Draft

Comprehensive Information Assurance Dictionary

Publication 0001d

National Information Assurance Training and Education Cener
Idaho State University

Director Corey D. Schou, PhD, CISSP
Professor, Information Systems
Associate Director, James Frost, PhD
Assistant Professor, Information Systems

Corey D. Schou, PhD
James Frost, PhD
Nathan Wingert
Jason Larsen
Herbert Lafond, Edward Munson

INTRODUCTION

This document was created at the Simplot Decision Support Center at Idaho State University. It origninated with the need to identify and catalog Knowledge, Skill and Ability categories for information assurance workers. These KSA's fromed the core of the Electronic Develop a Curriculum (eDACUM) research at Idaho State University. Items that have been included in all eDACUM work are marked with a pound sign (#)

During our eDACUM work, we noted a generation gap. Many of the slang terms used by younger team members were misunderstood by others. To overcome this communication problem we included portions of the Jargon File. The Jargon File is in the public domain, to be freely used, shared, and modified. Items from the Jargon file are marked with an asterisk (*).

With the establishment of the establishment of the National Information Assurance Training and Educaiton Center (NAITAEC), the work has been resumed.

We have included a section on abbreviations and documents. Many of the included terms were defined using the documents cited.

This draft document is being circulated for comment. The authors would appreciate suggestions for corrections, additions and deletions. In addition, we solicit authoratiaive definitions for terms that are included but not defined.

The Authors

Table of Contents

(TM) *

// [Usenet] ASCII rendition of the trademark-superscript symbol appended to phrases that the author feels should be recorded for posterity, perhaps in future editions of this lexicon. Sometimes used ironically as a form of protest against the recent spate of software and algorithm patents and `look and feel' lawsuits. See also UN*X.

*-Property Star Property

We have found at least four explanations of this term. We will include all authenticated versions received by 12/26/2001

/T/*

1. [From LISP terminology for `true'] Yes. Used in reply to a question (particularly one asked using The `-P' convention). In LISP, the constant T means `true', among other things. Some hackers use `T' and `NIL' instead of `Yes' and `No' almost reflexively. This sometimes causes misunderstandings. When a waiter or flight attendant asks whether a hacker wants coffee, he may well respond `T', meaning that he wants coffee; but of course he will be brought a cup of tea instead. As it happens, most hackers (particularly those who frequent Chinese restaurants) like tea at least as well as coffee -- so it is not that big a problem.
2. See time T (also since time T equals minus infinity).
3. [Techspeak] In transaction-processing circles, an abbreviation for the noun `transaction'.
4. A dialect of LISP developed at Yale.

@-Party*

/at'par`tee/ n. [from the @-sign in an Internet address] (alt. `@-sign party' /at'si:n par`tee/) A semi-closed party thrown for hackers at a science-fiction convention (esp. the annual Worldcon); one must have a network address to get in, or at least be in company with someone who does. One of the most reliable opportunities for hackers to meet face to face with people who might otherwise be represented by mere phosphor dots on their screens.

GNU Style'*

Used throughout GNU EMACS and the Free Software Foundation code, and just about nowhere else. Indents are always four spaces per level, with `' and `' halfway between the outer and inner indent levels. if (cond) <body> Surveys have shown the Allman and Whitesmiths styles to be the most common, with about equal mind shares. K&R/1TBS used to be nearly universal, but is now much less common (the opening brace tends to get lost against the right paren of the guard part in an `if' or `while', which is a Bad Thing). Defenders of 1TBS argue that any putative gain in readability is less important than their style's relative economy with vertical space, which enables one to see more code on one's screen at once. Doubtless these issues will continue to be the subject of holy wars.

Whitesmiths Style'*

popularized by the examples that came with Whitesmiths C, an early commercial C compiler. Basic indent per level shown here is eight spaces, but four spaces are occasionally seen. if (cond) <body>

0*

Numeric zero, as opposed to the letter `O' (the 15th letter of the English alphabet). In their unmodified forms they look a lot alike, and various kluges invented to make them visually distinct have compounded the confusion. If your zero is center-dotted and letter-O is not, or if letter-O looks almost rectangular but zero looks more like an American football stood on end (or the reverse), you're probably looking at a modern character display (though the dotted zero seems to have originated as an option on IBM 3270 controllers). If your zero is slashed but letter-O is not, you're probably looking at an old-style ASCII graphic set descended from the default typewheel on the venerable ASR-33 Teletype (Scandinavians, for whom Slashed-O is a letter, curse this arrangement). If letter-O has a slash across it and the zero does not, your display is tuned for a very old convention used at IBM and a few other early mainframe makers (Scandinavians curse *this* arrangement even more, because it means two of their letters collide). Some Burroughs/Unisys equipment displays a zero with a *reversed* slash. And yet another convention common on early line printers left zero unornamented but added a tail or hook to the letter-O so that it resembled an inverted Q or cursive capital letter-O (this was endorsed by a draft ANSI standard for how to draw ASCII characters, but the final standard changed the distinguisher to a tick-mark in the upper-left corner). Are we sufficiently confused yet?:

120 Reset*

/wuhn-twen'tee ree'set/ n. [from 120 volts, U. S. wall voltage] To cycle power on a machine in order to reset or unjam it. Compare Big Red Switch, power cycle.

4. 2*

n. Without a prefix, this almost invariably refers to BSD UNIX release 4. 2. Note that it is an indication of cluelessness to say “version 4. 2”, and “release 4. 2” is rare; the number stands on its own, or is used in the more explicit forms 4. 2BSD or (less commonly) BSD 4. 2. Similar remarks apply to “4. 3” and to earlier, less-widespread releases 4. 1 and 2. 9. , and will doubtless apply to 4. 4 in the near future.

A

A-Condition

For a start-stop teletypewriter system, synonym start signal.

A-D

Abbreviation for analog-to-digital.

A1

Abbreviation for analog-to-digital.

Abandoned Call

A call in which the caller disconnects or cancels the call after a connection has been made, but before the call is established.

*-Abbrev

/*-breev'/, /*-brev'/ n. Common abbreviation for `abbreviation'.

Abbreviated Dialing

A service feature permitting the user to dial fewer digits to establish a call than are required under the nominal numbering plan.

ABEND

/o'bend/, /*-bend'/ n. [ABnormal END] Abnormal termination (of software); crash; lossage. Derives from an error message on the IBM 360; used jokingly by hackers but seriously mainly by code grinders. Usually capitalized, but may appear as `abend'. Hackers will try to persuade you that ABEND is called `abend' because it is what system operators do to the machine late on Friday when they want to call it a day, and hence is from the German `Abend' = `Evening'.

Abort

1. In data transmission, a function invoked by a primary or secondary sending station causing the recipient to discard (and ignore) all bit sequences transmitted by the sender since the preceding flag sequence.
2. To terminate, in a controlled manner, a processing activity in a computer system because it is impossible or undesirable for the activity to proceed. (FP) (ISO)

Aborted Connection

Disconnection which does not follow established procedures. This may occasionally result from a bad phone connection, but more typically results when the user “hangs up” without attempting to issue the disconnect commands. Note: Some systems are sensitive to aborted connections, and do not detect the disconnect and reset for the next user. Continued aborts are considered [improper] and may result in a warning or revocation of access privileges. (BBD;)

Above Type 2 Magnetic Media

See Magnetic Media.

AC

See Magnetic Media.

AC Erasure

1. Using a magnetic field produced by an electromagnet powered by Alternating Current (AC) to degauss (purge) magnetic storage media.
2. The remnant or residual signal level after erasure with electrical degaussing equipment that should measure 90 decibels (dB) below saturated signal level. New equipment should be selected to meet the 90 dB standard. (*AFR* 205-16)

Accept

In data transmission, the condition assumed by a primary or secondary station upon correct receipt of a frame for processing.

Acceptable Level Of Risk

1. An assessment by the appropriate Designated Approving Authority that an Automated Information System meets the minimum requirements of applicable security directives. (*NCSC-WA*-001-85;)
2. A judicious and carefully considered assessment by the appropriate Designated Approving Authority (DAA) that an automatic data processing (ADP) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of ADP assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements. (*OPNAVINST* 5239. 1A;)
3. Judicious and carefully considered assessment by the appropriate Designated Approving Authority (DAA) that the residual risk inherent in operating the computer system or network after all proposed security features are implemented is acceptable and in the best interests of the Air Force.
4. An authority's determination of the level of protection deemed adequate to meet minimum level security requirements. *The level at which an Automated Information System is deemed to meet the minimum requirements of applicable security directives as determined by an assessment made by the appropriate designated approving authority (NSA, *National INFOSEC Glossary*, 10/88)

Acceptance

1. Indicates a facility or system generally meets technical and performance standards but may have minor exceptions which do not keep the facility from meeting operational and security requirements. (*AFR* 700-10;)
2. The condition that exists when a facility or system generally meets the technical performance stan-

dards and security requirements. (*NCSC-WA*-001-85;)

Acceptance Certification

Acceptance Inspection

The final inspection to determine if a facility or system meets the specified technical and performance standards. It is held immediately after facility and software testing and is the basis for commissioning or accepting the information system. The results are documented on AF Form 1261, Information Systems Acceptance, Commissioning, and Removal (*NCSC-WA*-001-85;; *AFR* 700-10;)

Acceptance Test

1. A test of a system or functional unit, usually performed by the user on the user's premises after installation, with the participation of the vendor to ensure that the contractual requirements are met. (FP) (ISO)
2. Operating and testing of a communication system, subsystem, or component, to ensure that the specified performance characteristics have been met. (~) Acceptance Trial A trial carried out by nominated representatives of the eventual military users of the weapon or equipment to determine if the specified performance and characteristics have been met. (JCS1-NATO)

Access

1. A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (CSC-STD-001-83;; *DCID* 1/16-1, Sup. ;)
2. The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system or network. (*DCID* 1/16-1;; DODD 5200. 28M;)
3. A specific type of interaction between a subject (i. e. , person, process or input device) and an object (i. e. , an AIS resource such as a record, file, program, output device) that results in the flow of information from one to the other. (DODD 5200. 28;)
4. The Ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any resource of an ADP system. (*FIPS PUB* 39;)
5. A user's ability to communicate with (input to or receive output from) a system to a specific area. Access does not include those persons (customers) who simply receive products created by the system and who do not communicate or interface with the system or its personnel. (*NCSC-WA*-001-85;)
6. The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system. Personnel only receiving output products from the ADP system and not inputting to or otherwise interacting with the system (i. e. , no “hands on” or other direct input or inquiry capability) are not considered to have ADP system access and are accordingly not subject to the personnel security requirements. Such output products, however, shall either be reviewed prior to dissemination or otherwise determined to be properly identified as to content and classification. (*OPNAVINST* 5239. 1A;; *AFR* 205-16;; *AFR* 700-10;)

Access Control List

A list of subjects which are authorized to have access to some object. (MTR-8201)

Access Control Measures

Hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these designed to detect or prevent unauthorized access to an ADP system and to enforce access control. (DOE 5637. 1)

Access Attempt

The process by which one or more users interact with a telecommunication system, to enable initiation of user information transfer. Note: An access attempt begins with an issuance of an access request by an access originator. An access attempt ends either in successful access or in access failure.

#-Access Authorization

Formal approval for access. (Source: NSAM 130-1)

Access Category

One of the classes to which a user, program or process in a system may be assigned on the basis of the resources or groups of resources that each is authorized to use. (*NCSC-WA*-001-85;; *AR* 380-380;; *FIPS PUB* 39;)

Access Code

The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line. (~)

Access Contention

In ISDN applications, synonymous with “contention. ”

Access Control

1. The process of limiting access to resources, to authorized users, programs, processes, or other networks. Access control is synonymous with controlled access and controlled accessibility. (*AR* 380-380;)

2. The process of limiting access to information or to resources of an ADP system to only authorized users. (DOE 5636. 2A;)
3. The process of limiting access to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks). Synonymous with controlled access, controlled accessibility. (*FIPS PUB* 39;; *NCSC-WA*-001-85;)

Access Control List(ACL)

1. A list of subjects which are authorized to have access to some object. (MTR-8201;)
2. Mechanism implementing discretionary access control in an AIS that identifies the users who may access an object and the type of access to the object that a user is permitted.

Access Control Measures

Hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these designed to detect or prevent unauthorized access to an ADP system and to enforce access control. (DOE 5636. 2A;)

Access Control Mechanism

1. Security safeguards designed to detect and prevent unauthorized access, and to permit authorized access in an AIS.
2. Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an automated system. (*AR* 380-380;; *NCSC-WA*-001-85;; *FIPS PUB* 39;)
3. Measure or procedure designed to prevent unauthorized access Hardware or software features, operating procedures, management procedures, and various combinations of these designed to prevent unauthorized access, and to permit authorized access to information within an automated system (NSA, *National INFOSEC Glossary*, 10/89)

Access Control Mechanism(s)

Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an automated system. (*AR* 380-380; *FIPS PUB* 39)

#-Access Control Models

1. DAC controls on the ability to assign access permission to an object by a user already possessing access permission. The ability to assign these permissions should be controlled with the same precision as the ability to access the objects themselves. (*NCSC-TG*-028 ver 1).
2. A model that gives rules of operation showing how access decisions are made. Traditionally, an access control model involves a set of states together with a set of primitive operations on states whose behavior is defined by rules of operation. Typically, each state contains a set of S of "SUBJECTS," a set O of "objects," and an access matrix A. For each subject s and object o, A[s,o] is a set of access rights, such as read, write, execute, and own. (*NCSC-TG*-010 ver 1).
3. A model which relates subjects, objects and access types.

#-Access Control Policies

1. A statement of intent with regard to control over access to, dissemination of, and modification on an information processing system. The policy must be precisely defined and implemented for each system that is used to process information. The policy must accurately reflect the laws, regulations, and general policies from which it is derived. (Panel of Experts, July 1994);
2. Operating and management procedures designed to detect or prevent the unauthorized access to an information system and enforce access control.

Access Control Roster

A list of personnel, users, computer, and so forth, who communicate or interface with an AIS, that documents the degree of access and control for each person. (*AFR* 205-16;)

#-Access Control Software

1. Security software designed to detect and prevent unauthorized access, and to permit authorized access in an AIS. (NSTISSI 4009*);
2. The control of system usage imposed by software controls. Such controls include system monitoring, user identification, user authentication and data integrity validations. (*ISDCST+LSC-1992*

#-Access Controls

Process of limiting access to the resources of an AIS only to authorized users, programs, processes, or other systems. (Source: NSTISSI 4009).

Access Level

The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. The access level, in conjunction with the non-hierarchical categories, form the sensitivity label of an object. (*NCSC-WA*-001-85;) NOTE: Access level, in conjunction with the non-hierarchical categories, forms the sensitivity label of an object.

Access Line

A transmission path between user terminal equipment and a switching center.

Access List

1. Roster of persons authorized admittance to a controlled area.

2. COMSEC Roster of persons authorized access to COMSEC material.
3. Compilation of users, programs, and/or processes and the access levels and types to which each is authorized. (AIS)
3. A catalog of users, programs, and/or processes and the specifications of access categories to which each is assigned. (*NCSC-WA*-001-85;; *AR* 380-380;; *FIPS PUB* 39;)

Access Mode

A distinct operation recognized by the protection mechanisms as a possible operation on an object. Read, write and append are possible modes of access to a file, while execute is an additional mode of access to a program. (MTR-8201;)

Access Node

In packet switching, the switching concentration point for the transaction of a subscriber's traffic to and from a network backbone system. Note: Protocol conversion may occur at this point of entry.

Access Originator

The functional entity responsible for initiating a particular access attempt. Note: An access attempt can be initiated by a source user, a destination user, or the telecommunication system.

Access Period

A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail. (*FIPS PUB* 39;; *NCSC-WA*-001-85;)

Access Permissions

Access Phase

Access Point

1. A class of junction points in a dedicated outside plant. They are semipermanent splice points at a junction between a branch feeder cable and distribution cables; points at which connections may be made for testing or using particular communication circuits. (~)
2. The point at which a user interfaces with a circuit or network.

Access Port

A logical or physical identifier that a computer uses to distinguish different terminal input/output data streams. (CSC-STD-002-85;; *NCSC-WA*-001-85;)

#-Access Privileges

The particular access permission (i. e. , read, write, append, execute, delete, create, modify) granted to a subject in relation to an object. (*ISDCST+LSC-1992*

Access Request

A control message issued by an access originator for the purpose of initiating an access attempt.

Access Time

1. In a telecommunication system, the elapsed time between the start of an access attempt and successful access. Note: Access time values are measured only on access attempts that result in successful access.
2. In a computer, the time interval between the instant at which an instruction control unit initiates a call for data and the instant at which delivery of the data is completed. (~)
3. The time interval between the instant at which storage of data is requested and the instant at which storage is started. (~)
4. In magnetic disk devices, the time for the access arm to reach the desired track and the delay for the rotation of the disk to bring the required sector under the read-write mechanism.

Access To Information

The function of providing to members of the public, upon their request, the government information to which they are entitled under law. (A-130;)

Access Type

1. The nature of an access right to a particular device, program, or file (such as read, write, execute, append, modify, delete, and create). (*AR* 380-380;; *NCSC-WA*-001-85;; *FIPS PUB* 39;)
2. Privilege to perform an action on a program or file. NOTE: Read, write, execute, append, modify, delete, and create are examples of access types.

Accessible Space

Area within which the user is aware of all persons entering and leaving, which denies the opportunity for concealed TEMPEST surveillance, and which delineates the closest point of potential TEMPEST intercept from a vehicle.

Accidental

A form of an event, contrasted with intentional, indicating that no agent or malice is involved in its realization. (RM;)

#-Account Administration

1. Maintenance of accounting files, tools, user accounts, and system statistics. (*NCSC-TG*-015);
2. Maintenance of user accounts entails verification of proper authorization (e. g. , clearance verification, need-to-know, and enforcement of least privilege) prior to adding a new account; updating access for users whose job requirements change; and timely deletion of accounts for users who no longer require or are authorized access. (Panel of Experts, July 1994).

Account Administrator

Individuals in an organization responsible carrying out the process of adding, updating and modifying user accounts.

Account Management

Accountability

1. The property that enables activities on an AIS to be traced to individuals who may be held responsible for their violations. (DODD 5200. 28;; *NCSC-WA*-001-85;)
2. The quality or state which enables violations or attempted violations of ADP system security to be traced who may then be held responsible. (*FIPS PUB* 39;; *AR* 380-380;)
3. The property which enables activities on an ADP system to be traced to individuals who can then be held responsible for their activities. (DOE 5636. 2A;)

#-Accountability For Sensitive Data

Functions to record the exercising of rights to perform security relevant actions and the quality or state which enables violations or attempted violations of information system security to be traced to individuals who may then be held responsible. (*ISDCST+LSC-1992*

Accountability Information

A set of records, often referred to as an audit trail, that collectively provide documentary evidence of the processing or other actions related to the security of an ADP system. (DOE 5636. 2A;)

Accounting

Accounting Legend

Numeric code used to indicate the code minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.

NOTE: National-level accounting legend codes are:

a. ALC-1 - continuously accountable by serial number.
b. ALC-2 - continuously accountable by quantity.
c. ALC-4 - report of initial receipt required. After acknowledging receipt, users may control in accordance with Service, department, or agency directives.

Accounting Legend Code (ALC)

1. (ALC) A numeric code used within the COMSEC Material Control System to indicate the minimum accounting controls required for items of TSEC-nomenclatured COMSEC material. ALC categories are specified in NACS1 4005. (NCSC-9)
   NOTE: National-level ALCs are:
   a. ALC-1: Continuously accountable by serial number.
   b. ALC-2: Continuously accountable by quantity.
   c. ALC-4: Report of initial receipt required.
2. After acknowledging receipt, the COMSEC manager and users will control according to AFKAG-1 or Air Force Systems Security Instruction (AFSSI) 4005, respectively. (AF9K_JBC. TXT) Numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.

Accounting Number

Number assigned to an item of COMSEC material to facilitate its control. Accreditation. Formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Accounting System

The system for recording, classifying, and summarizing information on financial position and operations

Accreditation

1. Official authorization, by the appropriate DAA, to place an automated system into operational use. This authorization is a statement that the level of residual risk in operating the system is sufficiently low to allow operation for a specified use. Accreditation is site specific and dependent on meeting local security measures and procedures. (*AFR* 205-16;)
2. The official authorization granted to an information system to process sensitive information in its operational environment based on comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel and communications security controls. (*AFR* 700-10;; CSC-STD-001-83;)
3. The authorization and approval granted to a system or network to process classified or sensitive data. Accreditation will be made on the basis of certification by a competent authority that designated technical personnel have verified that specified technical requirements for achieving adequate data security have been met. (*AR* 380-380;)
4. A formal declaration by the responsible SOIC, or his designee, as appropriate, that the ADP system or network provides an acceptable level of protection for processing and/or storing intelligence information. An accreditation should state the operating mode and other parameters peculiar to the ADP system or network being accredited. (*DCID* 1/16-1, Sup. ;)
5. A formal declaration by the DAA having accreditation responsibility that the AIS is approved to

operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (DODD 5200. 28;; *NCSC-WA*-001-85;)

6. The documented authorization, by the designated authority, granted to an organization or individual to operate an ADP system or network in a specific environment to process, store, transfer or provide access to classified information. (DOE 5636. 2A;)
7. The authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. (*FIPS PUB* 39;)
8. A policy decision by the responsible DAA resulting in a formal declaration that appropriate security countermeasures have been properly implemented for the ADP activity or network, so that the activity or network is operating at an acceptable level of risk. The accreditation should state the mode of operation and any operating limitations applicable to the ADP activity or network. (*OPNAVINST* 5239. 1A;)

Accreditation Authority

An official designated to accredit systems for the processing, use, storage, and production of . sensitive defense material. (*AR* 380-380)

See DESIGNATED APPROVING AUTHORITY.

Accumulator

1. A register in which one operand can be stored and subsequently replaced by the result of the store operation. (FP) (ISO)
2. A storage register. (~)
3. A storage battery. (~)

Accuracy

The degree of conformity of a measured or calculated value to its actual or specified value.

ACK

1. /ak/ interj. [from the ASCII mnemonic for 0000110] Acknowledge. Used to register one's presence (compare mainstream *Yo!*). An appropriate response to ping or ENQ.
2. [from the comic strip “Bloom County”] An exclamation of surprised disgust, esp. in “Ack pffft!” Semi-humorous. Generally this sense is not spelled in caps (ACK) and is distinguished by a following exclamation point.
3. Used to politely interrupt someone to tell them you understand their point (see NAK). Thus, for example, you might cut off an overly long explanation with “Ack. Ack. Ack. I get it now”. There is also a usage “ACK?” (from sense 1) meaning “Are you there?”, often used in email when earlier mail has produced no reply, or during a lull in talk mode to see if the person has gone away (the standard humorous response is of course NAK (sense
2. , i. e. , “I'm not here”).

Acknowledge Character

A transmission control character transmitted by the receiving station as an affirmative response to the sending station. (After FP) Note: An acknowledge character may also be used as an accuracy control character.

Acknowledgement

1. A protocol data unit, or element thereof, between peer entities to indicate the status of data units that have been previously received.
2. A message from the addressee informing the originator that his communication has been received and understood. (JCS1-DoD) (JCS1-NATO)

*Acme

n. The canonical supplier of bizarre, elaborate and non-functional gadgetry -- where Rube Goldberg and Heath Robinson shop. Describing some X as an “Acme X” either means “This is insanely great”, or, more likely, “This looks insanely great on paper, but in practice it's really easy to shoot yourself in the foot with it. ” Compare pistol. This term, specially cherished by American hackers and explained here for the benefit of our overseas brethren, comes from the Warner Brothers' series of “Roadrunner” cartoons. In these cartoons, the famished Wyl E. Coyote was forever attempting to catch up with, trap, and eat the Roadrunner. His attempts usually involved one or more high-technology Rube Goldberg devices -- rocket jetpacks, catapults, magnetic traps, high-powered slingshots, etc. These were usually delivered in large cardboard boxes, labeled prominently with the Acme name. These devices invariably malfunctioned in violent and improbable ways.

*Acolyte

n. ,obs. [TMRC] An OSU privileged enough to submit data and programs to a member of the priesthood.

Acoustic Coupler

1. A device for coupling electrical signals, by acoustical means, usually into and out of a telephone instrument. (~)
2. A terminal device used to link data terminals and radio sets with the telephone network. Note: The

link is achieved through acoustic (sound) signals rather than through direct electrical connection.

Acoustic Emanation

A signal transmitted mechanically via vibrations in either the air or some other conducting medium. (NACSEM 5106)

Acoustical Intelligence

1. (ACOUSTINT) Intelligence information derived from analysis of acoustic waves radiated either intentionally or unintentionally by the target. *
2. Intelligence information derived from analysis of acoustic waves radiated either intentionally or unintentionally by the target into surrounding medium;
3. In Naval usage, the acronym ACINT is used and usually refers to intelligence derived specifically from analysis of underwater acoustic waves from ships and submarines;
4. The technical and intelligence information derived from foreign sources that generate waves (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

ACOUSTINT

Acoustical Intelligence

Acquisition

1. In satellite communications, the process of locking tracking equipment on a signal from a communications satellite. (~)
2. The process of achieving synchronization.
3. In servo systems, the process of entering the boundary conditions that will allow the loop to capture the signal and achieve lock-on. (~)

Acquisition Program

A directed procurement effort. *A directed effort funded through procurement appropriations; the security assistance program; or through research, development, test, and evaluation (RDT&E) appropriations This program may include development or modifications to existing systems (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

Acquisition Specification

#-Acquisitions

The process of selecting and purchasing new information technology. Security and enforcement of the organization's security policy should be considerations in this process. (Panel of Experts, July 1994).

Active Attack

An attack that results in an unauthorized change in the system's state. Examples include modifying messages, inserting spurious messages, masquerading as an authorized user, and denying service.

Active Wiretapping

The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false signals, or by altering the communications of legitimate users. (*FIPS PUB* 39;)

Activity

A security model rule stating that once an object is made inactive, it cannot be accessed until it is made active again. (MTR-8201;)

Activity Log

A detective countermeasure that keeps track of all, or selected, activities. (RM;)

Ad Hoc Query

A method which allows the user in a data base environment to dynamically create his own view of the data and the method of retrieval for the information without intervention. (*AR* 380-380;)

*-Ad-Hockery

/ad-hok'*r-ee/ n. [Purdue]

1. Gratuitous assumptions made inside certain programs, esp. expert systems, which lead to the appearance of semi-intelligent behavior but are in fact entirely arbitrary. For example, fuzzy-matching against input tokens that might be typing errors against a symbol table can make it look as though a program knows how to spell.
2. Special-case code to cope with some awkward input that would otherwise cause a program to choke, presuming normal inputs are dealt with in some cleaner and more regular way. Also called `ad-hackery', `ad-hocity' (/ad-hos'*-tee/), `ad-crockery'. See also ELIZA effect.

Ada

1. (Ada®) The official, high-level computer language of DoD for embedded-computer, real-time applications as defined in MIL-STD-1815. Note: Ada® is a registered trademark of the U. S. Government (Ada Joint Program Office).
2. A Pascal-descended language that has been made mandatory for Department of Defense software projects by the Pentagon.
3. Lady Lovelace’s first name

Adaptive Channel Allocation

A method of multiplexing wherein the information-handling capacities of channels are not predetermined but are assigned on demand.

Adaptive Communication

Any communication system, or portion thereof, that automatically uses feedback information obtained from the system itself or from the signals carried by the system to modify dynamically one or more of the

system operational parameters to improve system performance or to resist degradation. (~) Note: The modification of a system parameter may be discrete, as in hard-switched diversity reception, or may be continuous, as in a predetection combining algorithm.

Adaptive Routing

Routing that is automatically adjusted to compensate for network changes such as traffic patterns, channel availability, or equipment failures. Note: The experience used for adaptation comes from the traffic being carried. See also , , , , , , .

Adaptive System

A system that has a means of monitoring its own performance and a means of varying its own parameters, by closed-loop action, to improve its performance. (~)

Add Mode

In addition and subtraction operations, a mode in which the decimal marker is placed at a predetermined location with respect to the last digit entered. (FP) (ISO)

Add-On Security

1. The retrofitting of protection mechanisms, implemented by hardware or software, after the ADP system has become operational. (*AR* 380-380;; *FIPS PUB* 39;)
2. The retrofitting of protection mechanisms, implemented by hardware or software. (*NCSC-WA*-001-85;)
3. Incorporation of new hardware, software, or firmware safeguards in an operational AIS.

Added Bit

A bit delivered to the intended destination user in addition to intended user information bits and delivered overhead bits.

Added Block

Any block, or other delimited bit group, delivered to the intended destination user in addition to intended user information bits and delivered overhead bits. Synonym extra block.

Adder

A device whose output data are a representation of the sum of the numbers represented by its input data. (FP) (ISO)

Adder-Subtracter

A device that acts as an adder or subtracter depending upon the control signal received; the adder-subtracter may be constructed so as to yield a sum and a difference at the same time. (FP) (ISO)

Address

1. In communications, the coded representation of the source or destination of a message. (~)
2. In data processing, a character or group of characters that identifies a register, a particular part of storage, or some other data source or destination. (~)
3. To assign to a device or item of data a label to identify its location. (~)
4. The part of a selection signal that indicates the destination of a call.
5. To refer to a device or data item by its address. (FP) (ISO)

Address Field

The portion of a message header that contains the destination address for the signal and the source of the signal. Note: In a communication network, the generally transmitted signal format contains a header, the data, and a trailer. See also , ,

Address Message Sequencing

In common-channel signaling, a procedure for ensuring that addressed messages are processed in the correct order when the order in which they are received is incorrect. See also queue, routing indicator.

Address Part

A part of an instruction that usually contains only an address or part of an address. (FP) (ISO) See also address.

Address Pattern

A prescribed structure of data used to represent the destination(s) of a block, message, packet, or other formalized data structure. See also address, frame synchronization pattern.

Address Separator

The character that separates the different addresses in a selection signal. See also character.

Address Space

The range of addresses that can be accessed by a process. Virtual address space is the range as though the addresses went from 0 to whatever upper limit is imposed by the virtual address manager. The actual address and location of the data may bear little resemblance to the address as seen by the process; there is no limit on the size of virtual address space other than secondary storage capacity. Physical or actual address space is the actual memory locations that may be referenced. The limit of the range is imposed by the physical memory implementation. For security purposes the address space allowed to a process must be limited to a set that has no physical intersection with the trusted computer base or other sensitive processes, or any other user's process(es).

Address Translation Unit

Addressability

1. In computer graphics, the number of addressable points on a display surface or in storage. (FP) (ISO)
2. In micrographics, the number of addressable points, within a specified film frame, written as follows: the number of addressable horizontal points by the number of addressable vertical points, for example, 3000 by 4000. (After FP)

Addressable Point

in computer graphics, any point of a device that can be addressed. (FP) (ISO)

Adequate Notice

*-Adger

/aj'r/ vt. [UCLA mutant of nadger] To make a bonehead move with consequences that could have been foreseen with even slight mental effort. E. g. , “He started removing files and promptly adgered the whole project”.

*-Admin

/ad-min'/ n. Short for `administrator'; very commonly used in speech or on-line to refer to the systems person in charge on a computer. Common constructions on this include `sysadmin' and `site admin' (emphasizing the administrator's role as a site contact for email and news) or `newsadmin' (focusing specifically on news). Compare postmaster, sysop, system mangler.

Administration

1. Any governmental department or service responsible for discharging the obligations undertaken in the convention of the International Telecommunication Union and the Regulations. (RR)
2. The management and execution of all military matters not included in tactics and strategy; primarily in the fields of logistics and personnel management. (JCS1-NATO)
3. Internal management of units. (JCS1-DoD) (JCS1-NATO)
4. The management and execution of all military matters not included in strategy and tactics. (JCS1-DoD)

Administrative Security

1. The management constraints and supplemental controls established to provide an acceptable level of protection for data. (*NCSC-WA*-001-85;)
2. The management constraints; operational, administrative, and accountability procedures and supplemental controls established to provide an acceptable level of protection for data. (*OPNAVINST* 5239. 1A;; *FIPS PUB* 39;; DOE 5636. 2A;)
3. Synonymous with Procedural Security.

#-Administrative Security Policies And Procedures

Written guidance necessary to implement administrative security. (Panel of Experts, July 1994).

Administrative User

Administratively Controlled Information

Privileged but unclassified material bearing designators to prevent disclosure to unauthorized persons. *Privileged but unclassified material bearing designations such as FOR OFFICIAL USE ONLY or LIMITED OFFICIAL USE, to prevent disclosure to unauthorized persons (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Administrator Of General Services

ADP Facility

One or more rooms, generally contiguous, containing the elements of an ADP system. (DOE 5636. 2A;)

ADP Security

Measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of ADP systems and data, and denial of service to process data. ADP security includes consideration of all hardware/software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the ADP system and for the data or information contained in the system. (*OPNAVINST* 5239. 1A;)

ADP Security Documentation

Documents which describe an activity's ADP security posture and include risk assessment plan and reports, security test and evaluation plans and reports, Inspector General inspection reports and findings, incident reports, contingency plans and test results, and standard operating procedures. (*OPNAVINST* 5239. 1A;)

ADP Security Staff

Individuals assigned and functioning as action officials for ADP security within their respective organization. (*OPNAVINST* 5239. 1A;)

ADP Storage Media

The physical substance(s) used by an ADP system upon which data is recorded. (CSD-STD-005-85)

ADP System

1. The central computer facility and any remote processors, terminals, or other in-

put/output/storage devices connected to it by communications links. Generally, all of the components of an ADP system will be under the authority of one SOIC or his designee. (*DCID* 1/16-1, Sup. ;)
2. An assembly of computer hardware, firmware, telecommunications, interconnections with other ADP equipment (e. g. , networks), and the entire collection of software that is executed on that hardware. Included in this definition are word processors, microprocessors, personal computers, controllers, automated office support systems (AOSS), or other stand-alone or special computer systems. (DOE 5636. 2A;)

ADP System Security

1. All of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy. (*FIPS PUB* 39;)
2. Includes all hardware/software functions, characteristics, and features, operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities and the management constraints, physical structures, and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system. (DODD 5200. 28M;)

Advanced Data Communication Control Procedure

(ADCCP) A bit-oriented Data-Link-Layer protocol used to provide point-to-point and point-to-multipoint transmission of a data frame with error control. Note: ADCCP closely resembles HDLC and SDLC. See also binary synchronous communications, frame, high-level data link control, link, synchronous data link control.

Advanced Development Model

1. Advanced Development Model;
2. A model of a complete COMSEC equipment for experimentation or tests intended to demonstrate the technical feasibility of the design and the ability to meet existing performance requirements; also to provide engineering data for further development. (NCSC " 9)

Advanced Intelligent Network

(AIN) A proposed intelligent-network (IN) architecture that includes both IN/1+ and IN/2 concepts. See also intelligent network.

*-ADVENT

/ad'vent/ n. The prototypical computer adventure game, first designed by Will Crowther on the PDP-10 in the mid-1970s as an attempt at computer-refereed fantasy gaming, and expanded into a puzzle-oriented game by Don Woods at Stanford in 1976. Now better known as Adventure, but the TOPS-10 operating system permitted only six-letter filenames. See also vadding, Zork, and Infocom. This game defined the terse, dryly humorous style since expected in text adventure games, and popularized several tag lines that have become fixtures of hacker-speak "A huge green fierce snake bars the way!" "I see no X here" (for some noun X). "You are in a maze of twisty little passages, all alike. " "You are in a little maze of twisty passages, all different. " The `magic words' xyzzy and plugh also derive from this game. Crowther, by the way, participated in the exploration of the Mammoth & Flint Ridge cave system; it actually *has* a `Colossal Cave' and a `Bedquilt' as in the game, and the `Y2' that also turns up is cavers' jargon for a map reference to a secondary entrance.

Adversary

1. An individual, group, organization, or government that must be denied critical information NOTE: Synonymous with Competitor. *
2. Those individuals, groups, or organizations that must be denied critical information to maintain friendly mission effectiveness (JCS, MOP 199, 3/89)

Adversary Scenario

1. A composite of adversary motivations, objectives, perceptions, and resources which threaten operational effectiveness through exploitation of sensitive/critical information. *
2. A composite of adversary mission objectives, adversary mission scenarios, and success criteria which could threaten each potential design of an operational or support system (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

Affirm

A formal methodology developed at the University of Southern California Information Sciences Institute (USC-ISI) for the specification and verification of abstract data types, incorporating algebraic specification techniques and hierarchical development. (MTR-8201;)

*-AFJ

// n. Written-only abbreviation for "April Fool's Joke". Elaborate April Fool's hoaxes are a long-established tradition on Usenet and Internet; see kremvax for an example. In fact, April Fool's Day is the 'only' seasonal holiday marked by customary observances on the hacker networks.

Agencies

Agency

Any executive department, military department, government corporation. Government controlled corporation, or other establishment in the executive branch of the government, or any independent regulatory agency. Within the Executive Off ice of the President, the term includes only the Off ice of Management and Budget and the Office of Administration. (A-1 30)

#-Agency-Specific Policies And Procedures

These are the local policies and procedures to supplement and implement higher level regulations, laws, procedures in the local environment. (Source: Panel of Experts, July 1994).

Agent

1. An individual entity of the external environment; when no human agent is involved, “nature” becomes the agent implicated in an event. (ET;)
2. The perpetrator of an intentional event. (RM;)
3. A person engaged in clandestine operations. *A person who engages in clandestine intelligence activity under the direction of an intelligence organization, but who is not an officer, employee, or coopted worker of that organization (*IC Staff, Glossary of Intelligence Terms and Definitions,* 6/89)

#-Aggregation

1. Individual data systems and data elements may be determined to be unclassified and to be of a specific sensitivity category. When those data are combined with other data, the totality of the information may be classified or in a higher sensitivity category, with higher protection requirements. (*AFR* 205-16;)
2. Collection or grouping of independent information where the sensitivity of the whole is greater than the sensitivity of the parts.

#-Aggregation Problem

An occurrence when a user's right to several pieces of information results in knowledge they do not have a right to. It can happen that a user is not allowed access to a collection of data items, but is allowed access to any given item in the collection. In this case, the aggregation problem is to prevent the user (or a subject acting on their behalf) from gaining access to the whole collection through repeated accesses to items in the collection. (Source: *NCSC-TG*-010).

AI

/A-I/ n. Abbreviation for `Artificial Intelligence', so common that the full form is almost never written or spoken among hackers.

*-AI-Complete

/A-I k*m-pleet'/ adj. [MIT, Stanfordby analogy with `NP-complete' (see NP-)] Used to describe problems or subproblems in AI, to indicate that the solution presupposes a solution to the `strong AI problem' (that is, the synthesis of a human-level intelligence). A problem that is AI-complete is, in other words, just too hard. Examples of AI-complete problems are `The Vision Problem' (building a system that can see as well as a human) and `The Natural Language Problem' (building a system that can understand and speak a natural language as well as a human). These may appear to be modular, but all attempts so far (1993) to solve them have foundered on the amount of context information and `intelligence' they seem to require. See also gedanken.

Air Conditioning

In the DoD, synonym for the term “environmental control,” which is the process of simultaneously controlling the temperature, relative humidity, air cleanliness, and air motion in a space to meet the requirements of the occupants, a process, or equipment. (~) See also critical areas.

*-Airplane Rule

n. “Complexity increases the possibility of failure; a twin-engine airplane has twice as many engine problems as a single-engine airplane. ” By analogy, in both software and electronics, the rule that simplicity increases robustness. It is correspondingly argued that the right way to build reliable systems is to put all your eggs in one basket, after making sure that you've built a really *good* basket. See also KISS Principle.

AIS Security

1. Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification, or destruction of AlSs and data, and denial of service. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable level of protection for an AIS and for data handled by an AIS. (DODD 5200. 28)

2 . See COMPUTER SECURITY.

Alarm Center

A location that receives local and remote alarms. It is generally located within a technical control facility. (~)

Alarm Indicator

A device that responds to a signal from an alarm sensor; e. g. , a bell, lamp, horn, gong, buzzer, or a combination thereof.

Allman Style'*

Named for Eric Allman, a Berkeley hacker who wrote a lot of the BSD utilities in it (it is sometimes called `BSD style'). Resembles normal indent style in Pascal and ALGOL. Basic indent per level shown here is eight spaces, but four spaces are just as common (esp. in C++ code). if (cond) Body>

Alarm Sensor

1. In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. (~) Note: The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle.
2. In a physical security system, any of a group of approved devices used to indicate a change in the physical environment of a facility, or part thereof. (~) Note: Sensors may also be redundant or chained as when one sensor is used to protect the housing, cabling, or power of another. See also communications security, variation monitor.

#-Alarms, Signals And Reports

A visual or audible signal indicating a security breach or a physical calamity such as a fire. (*ISDCST+LSC-1992*

Algorithm

In programming, a finite set of well-defined rules for the solution of a problem in a finite number of steps. (Data & Computer SECURITY Dictionary of Standards, Concepts and Terms)

Algorithmic Language

An artificial language established for expressing a given class of algorithms. (FP) (ISO)

*-Aliasing Bug

n. A class of subtle programming errors that can arise in code that does dynamic allocation, esp. via `malloc(3)' or equivalent. If several pointers address (`aliases for') a given hunk of storage, it may happen that the storage is freed or reallocated (and thus moved) through one alias and then referenced through another, which may lead to subtle (and possibly intermittent) lossage depending on the state and the allocation history of the malloc arena. Avoidable by use of allocation strategies that never alias allocated core, or by use of higher-level languages, such as LISP, which employ a garbage collector (see GC). Also called a stale pointer bug. See also precedence lossage, smash the stack, fandango on core, memory leak, memory smash, spam. Historical noteThough this term is nowadays associated with C programming, it was already in use in a very similar sense in the Algol-60 and FORTRAN communities in the 1960s.

*-All-Elbows

adj. [MS-DOS] Of a TSR (terminate-and-stay-resident) IBM PC program, such as the N pop-up calendar and calculator utilities that circulate on BBS systems unsociable. Used to describe a program that rudely steals the resources that it needs without considering that other TSRs may also be resident. One particularly common form of rudeness is lock-up due to programs fighting over the keyboard interrupt. See rude, also mess-dos.

Alpha Profile

See power-law index profile.

Alphabet

1. An ordered set of all the letters used in a language, including letters with diacritical signs where appropriate, but not including punctuation marks. (FP) (ISO)
2. An ordered set of symbols used in a language; e. g. , the Morse Code alphabet, the 128 ASCII (IA No. 5) characters. (~) Note: This definition includes punctuation marks, numeric digits, non-printing control characters, and other symbols. See also alphanumeric, ASCII, character, character set, code, coded set, digit, digital alphabet, EBCDIC, language.

Alphabet Translation

See alphabet transliteration.

Alphabet Transliteration

That process whereby the characters in one alphabet are converted to characters in a different alphabet. (~) See also code, language.

Alphabetic Character Set

A character set that contains letters and may contain control characters, special characters, and the space character, but not digits. (FP) (ISO)

Alphabetic Code

A code according to which data are represented through the use of an alphabetic character set. (FP) (ISO)

Alphabetic String

1. A string consisting solely of letters from the same alphabet. (FP) (ISO)
2. A character string consisting solely of letters and associated special characters from the same alphabet. (FP)

Alphabetic Word

1. A word consisting solely of letters from the same alphabet. (FP) (ISO)
2. A word that consists of letters and associated special characters, but not digits. (FP) See also word.

Alphanumeric

1. Pertaining to a character set that contains letters, digits, and, sometimes, other characters such as punctuation marks. (~)
2. A character set with unique bit configurations that comprise letters of the alphabet, digits of the decimal system, punctuation symbols, and sometimes special character symbols used in grammar, business, and science. See also alphabet (def. #2), character set, code, language.

Alphanumeric Character Set

A character set that contains both letters and digits, special characters, and the space character. (FP) (ISO)

Alphanumeric Code

A code whose application results in a code set whose elements are taken from an alphanumeric character set. (FP) (ISO)

Alphanumeric Data

Data represented by letters, digits, and sometimes by special characters and the space character. (FP) (ISO)

*-Alt /awlt/

1. n. The alt shift key on an IBM PC or clone keyboard; see bucky bits, sense 2 (though typical PC usage does not simply set the 0200 bit).
2. n. The `clover' or `Command' key on a Macintosh; use of this term usually reveals that the speaker hacked PCs before coming to the Mac (see also feature key). Some Mac hackers, confusingly, reserve `alt' for the Option key (and it is so labeled on some Mac II keyboards).
3. n. obs. [PDP-10; often capitalized to ALT] Alternate name for the ASCII ESC character (ASCII 0011011), after the keycap labeling on some older terminals; also `altmode' (/awlt'mohd/). This character was almost never pronounced `escape' on an ITS system, in TECO, or under TOPS-10 -- always alt, as in “Type alt alt to end a TECO command” or “alt-U onto the system” (for “log onto the [ITS] system”). This usage probably arose because alt is more convenient to say than `escape', especially when followed by another alt or a character (or another alt *and* a character, for that matter).
4. The alt hierarchy on Usenet, the tree of newsgroups created by users without a formal vote and approval procedure. There is a myth, not entirely, implausible, that alt is acronymic for “anarchists, lunatics, and terrorists”; but in fact it is simply short for “alternative”.

*-Alt Bit

/awlt bit/ [from alternate] adj. See meta bit.

Alternate COMSEC

Person designated by proper authority to custodian perform the duties of the COMSEC custodian during the temporary absence of the COMSEC custodian.

Alternate COMSEC Manager

Person designated by proper authority to perform the duties of the COMSEC manager during the temporary absence of the COMSEC manager.

Alternate Mark Inversion Signal

A pseudoternary signal, representing binary digits, in which successive “marks” are of alternate polarity (positive and negative) but normally equal in amplitude and in which “spaces” are of zero amplitude. See also AMI violation, bipolar signal, modified AMI, paired disparity code, return-to-zero code.

Alternate Routing

The routing of a call or message over a substitute route when a primary route is unavailable for immediate use. (~) See also adaptive routing, call, dispersion (def. #1), dual access, dual homing, heuristic routing, multiple access, multiple homing, routing.

Alternating Current

Alternating Current

Alternative

Synonym variant.

*-Altmode

n. Syn. alt sense 3.

*-Aluminum Book

n. [MIT] “Common LISPThe Language”, by Guy L. Steele Jr. (Digital Press, first edition 1984, second edition 1990). Note that due to a technical screwup some printings of the second edition are actually of a color the author describes succinctly as “yucky green”. See also book titles.

Ambient Level

Ambient levels may be classified into two categories: (a) Test Environment Ambient Level-Those levels of radiated and conduced noise existing at a specific test location and time when only the equipment under test is inoperative. Atmospherics, interference from other sources, and circuit noise or other interference generated within the test detection system comprise the “test environment ambient level. ” (b) Equipment-Under-Test Ambient Level - those levels of radiated and conducted noise which originate in the equipment under test and which are not compromising emanations.

Ambiguity

A condition which precludes positive identification of specific characters and functions utilizing the parameters of the detected signal. This condition exists when the intelligence-related signal emanation can be equated to more than one character or function.

American National Standard Code For Information Interchange
(ASCII) Standard and predominant seven-bit (eight bit with parity) character code used for data communications and data processing.

American National Standards Institute
American National Standards Institute (ANSI)

American Standard Code For Information Interchange (ASCII)
See ASCII.

***-Amp Off**
vt. [Purdue] To run in background. From the UNIX shell `&' operator.

***-Amper**
n. Common abbreviation for the name of the ampersand (`&', ASCII 0100110) character. See ASCII for other synonyms.

AMPS
Abbreviation for automatic message processing system.

Analog Computer
A device that performs operations on data that are represented, within the device, by continuous variables having some physical resemblance to the quantities being represented. Note: The earliest analog computers were purely mechanical devices with levers, cogs, cams, etc. , representing the data or operator values. Modern analog computers typically employ electrical parameters such as voltage, resistance, or current to represent the quantities being manipulated. See also computer, digital computer.

Analog Control
Synonym analog synchronization.

Analog Data
Data represented by a physical quantity that is considered to be continuously variable and whose magnitude is made directly proportional to the data or to a suitable function of the data. (~) See also data, digital data.

Analog Decoding
A process in which an analog signal is reconstructed from a digital signal that represents the original analog signal. (~) See also analog encoding, signal.

Analog Encoding
Any process by which a digital signal or signals, that represent a sample or samples taken of an analog signal at a given instant or consecutive instants, are generated. (~) See also analog decoding, signal, uniform encoding.

Analog Facsimile Equipment
Facsimile equipment that employs analog techniques to encode the image detected by the scanner. The output signal is analog. Note: Examples of analog facsimile equipment are CCITT Group 1 and CCITT Group 2.

ANALOG Signal
1. A signal that makes use of electrical or physical analogies; i. e. , varying voltages, frequencies, distances, etc. , to produce a signal of a continuous (rather than of a pulsed or discrete) nature. (~)
2. A nominally continuous electrical signal that varies in some direct correlation to another signal impressed on a transducer. (~) Note: The electrical signal may vary its frequency, phase, or amplitude, for instance, in response to changes in phenomena or characteristics such as sound, light, heat, position, or pressure. See also digital signal, signal.

Analog Synchronization
A synchronization control system in which the relationship between the actual phase error between clocks and the error signal device is a continuous function over a given range. Synonym analog control. See also synchronization.

#-Analog Technology
A form of measurement or representation in which an indicator is varied continuously, often reflect ongoing changes in the phenomenon being measured or represented. Analog representation is used, for example, in a thermometer: the hotter the patient, the longer the mercury. Analog techniques also are used for the reproduction of music in standard Lp records and audio cassettes. A computer that draws a comparison, or analogy, between the computer representation and the object being represented, making the object easy to measure. Analog computation is used widely in laboratory settings to monitor on-going, continuous changes and record these changes in charts or graphs. (*QCUS+Pf-90*

Analog Transmission
Transmission of a continuously varying signal as opposed to transmission of a discretely varying signal.

Analog-To-Digital

Analog-To-Digital Coder
See analog-to-digital converter.

Analog-To-Digital Converter
(ADC) A device that converts an analog input signal to a digital output signal carrying equivalent information. (~) Synonyms analog-to-digital coder, analog-to-digital encoder, coder. See also digital-to-analog converter, digital voice transmission, digitizer.

Analog-To-Digital Encoder
See analog-to-digital converter.

Analysis

The process by which information is examined to identify significant facts and derive conclusions. *A process in the production step of the intelligence cycle in which intelligence information is subject to systematic examination in order to identify significant facts and derive conclusions therefrom (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89) See Also COST-ANALYSIS, CRYPTOANALYSIS, and RISK ANALYSIS.

*-Angle Brackets

n. Either of the characters `<' (ASCII 0111100) and `>' (ASCII 0111110) (ASCII less-than or greater-than signs). Typographers in the Real World use angle brackets which are either taller and slimmer (the ISO `Bra' and `Ket' characters), or significantly smaller (single or double guillemets) than the less-than and greater-than signs. See broket, ASCII.

*-Angry Fruit Salad

n. A bad visual-interface design that uses too many colors. (This term derives, of course, from the bizarre day-glo colors found in canned fruit salad.) Too often one sees similar effects from interface designers using color window systems such as X; there is a tendency to create displays that are flashy and attention-getting but uncomfortable for long-term use.

Annual Loss Expectancy

The ALE of an ADP system or activity is the expected yearly dollar value loss from the hard to the system or activity by attacks against its assets. (*OPNAVINST* 5239. 1A;)

Annual Reports

ANSI

n. /an'see/

1. n. The American National Standards Institue. ANSI, along with the International Standards Organization (ISO) standardized the C programming language (see K&R, Classic C), and promulgates many other important software standards.
2. n. [BBS] The set of screen-painting codes that most MS-DOS and Amiga computers accept. This comes from the ANSI. SYS device driver that must be loaded on an MS-DOS computer to view such codes. Unfortunately, neither DOS ANSI nor the BBS ANSIs derived from it exactly match the ANSI terminal standard. For example, the ESC-[1m code turns on the bold highlight on large machines, but in IBM PC/MS-DOS ANSI, it turns on `intense' (bright) colors. Also, in BBS-land, the term `ANSI' is often used to imply that a particular computer uses or can emulate the IBM high-half character set from MS-DOS. Particular use depends on context. Occasionally, the vanilla ASCII character set is used with the color codes, but on BBSs, ANSI and `IBM characters' tend to go together.

Answer Back

A signal or tone sent by a receiving equipment or data set to the sending station to indicate that it is ready to accept transmission, or acknowledging receipt of a transmission. See also acknowledge character, call control signal.

Answer Signal

A supervisory signal, usually in the form of a closed loop, returned from the called telephone to the originating switch when the called party answers. Note: This signal stops the ringback signal from being returned to the caller. See also call control signal, loop, signal.

Anti-Jam

See Anti-Jamming.

Anti-Jamming

(AJ) Measures to ensure that intended transmitted information can be received despite deliberate jamming attempts.

Anti-Spoof

Measures to prevent an opponent's participation in a telecommunications network or operation/control of a cryptographic or COMSEC system.

Anti-Virus Program

Software program designed to protect an AIS from a virus attack.

*-AOS

1. /aws/ (East Coast), /ay-os/ (West Coast) vt. ,obs. To increase the amount of something. “AOS the campfire. ” [based on a PDP-10 increment instruction] Usage considered silly, and now obsolete. Now largely supplanted by bump. See SOS.
2. n. A Multics-derived OS supported at one time by Data General. This was pronounced /A-O-S/ or /A-os/. A spoof of the standard AOS system administrator's manual (“How to Load and Generate your AOS System”) was created, issued a part number, and circulated as photocopy folklore; it was called “How to Goad and Levitate your CHAOS System”.
3. n. Algebraic Operating System, in reference to those calculators which use infix instead of postfix (reverse Polish) notation.
4. A BSD-like operating system for the IBM RT. Historical note AOS in sense 1 was the name of a PDP-10 instruction that took any memory location in the computer and added 1 to it; AOS meant `Add One and do not Skip'. Why, you may ask, does the `S' stand for `do not Skip' rather than for `Skip'? Ah, here was a beloved piece of PDP-10 folklore. There were eight such instructionsAOSE added 1 and then skipped the next instruction if

the result was Equal to zero; AOSG added 1 and then skipped if the result was Greater than 0; AOSN added 1 and then skipped if the result was Not 0; AOSA added 1 and then skipped Always; and so on. Just plain AOS didn't say when to skip, so it never skipped. For similar reasons, AOJ meant `Add One and do not Jump'. Even more bizarre, SKIP meant `do not SKIP'! If you wanted to skip the next instruction, you had to say `SKIPA'. Likewise, JUMP meant `do not JUMP'; the unconditional form was JUMPA. However, hackers never did this. By some quirk of the 10's design, the JRST (Jump and ReSTore flag with no flag specified) was actually faster and so was invariably used. Such were the perverse mysteries of assembler programming.

*-App

/ap/ n. Short for `application program', as opposed to a systems program. Apps are what systems vendors are forever chasing developers to create for their environments so they can sell more boxes. Hackers tend not to think of the things they themselves run as apps; thus, in hacker parlance the term excludes compilers, program editors, games, and messaging systems, though a user would consider all those to be apps. (Broadly, an app is often a self-contained environment for performing some well-defined task such as `word processing'; hackers tend to prefer more general-purpose tools.) Oppose tool, operating system.

Append Access Mode

Application

Those portions of a system, including portions of the operating system, that are not responsible for enforcing the security policy. (CSC-STD-003-85;; CSC-STD-004-85;)

#-Application Development Control

Those processes aimed at ensuring that an application, viewed as a system, continues to operate according to its specifications and continues to be available. (*ISDCST+LSC-1992*

Application Layer

See Open Systems Interconnection--Reference Model.

Application Software

1. Routines and programs designed by, or for system (Functional) users and customers. Through the use of available automated system equipment and basic software, application software completes specific, mission-oriented tasks, jobs, or functions. It can be either general purpose packages, such as demand deposit accounting, payroll, machine tool control, and so forth, or specific application programs tailored to complete a single or limited number of user functions, for example, base-level personnel, depot maintenance, missile or satellite tracking, and so forth. Except for general purpose packages that are acquired directly from software vendors or from the original equipment manufacturers (OEM), this type of software is generally developed by users either with in-house resources or through contract services. (*AFR* 205-16;)
2. Mission support or mission specific software programs designed by, or for, system users and customers. By using available computer system equipment and operating system software, application software completes specific, mission-oriented tasks, jobs, or functions. It can be either general-purpose packages, such as demand deposit accounting, payroll, machine tool control, or specific application programs tailored to complete a single or limited number of user functions.

Application Software (functional)

Routines and programs designed by, or for system users and customers. By using available automated system equipment and basic software, application software completes specific, mission oriented tasks, jobs, or functions. It can be either general purpose packages, such as demand deposit accounting, payroll, machine too/ control, or specific application programs tailored to complete a single or limited number of user functions (base-level personnel, depot maintenance, missile or satellite tracking). Except for general purpose packages that are acquired directly from software vendors or from the original equipment manufacturers, this type of software is generally developed by the user either with in-house resources or through contract services. (*AFR* 205-16)

#-Applications Security

the state that exists when the source and object code are the same as originally developed and certified accredited or, have been modified and tested in accordance with established standards, and procedures and recertified reaccredited and have not been exposed to accidental or malicious alteration or destruction. (*ISDCST+LSC-92*.

Appreciations

Assumptions about another party's intentions, capabilities, and activities used in planning and decision making. *Personal conclusions, official estimates, and assumptions about another party's intentions, capabilities, and activities used in planning and decision making. (1) Desired Appreciations – Adversary personal conclusions and official estimates, valid or invalid, that result in adversary behaviors and official actions advantageous to friendly interests and objectives; (2) Harmful Appreciations – Adversary personal conclusions, official estimates, or assumptions, valid or invalid, that result in adversary behaviors and official

actions harmful to friendly interests and objectives. (JCS, MOP 199, 3/89)

Approval Accreditation

#-Approval To Operate

1. Concurrence by the DAA that a satisfactory level of security has been provided (minimum requirements are met and there is an acceptable level of risk). It authorizes the operation of an automated system or network at a computer facility. Approval results from an analysis of the computer facility, automated system and automatic data system certifications and the operational environment of the automated system entity by the DAA. (*AFR* 205-16;)
2. See ACCREDITATION.

Approval/accreditation

The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls. (CSC-STD-001-83;)

Approved Circuit

Synonymous with PROTECTED DISTRIBUTION SYSTEM.

Approving

See DESIGNATED APPROVING AUTHORITY.

Archive

Archivist

Area Code

See access code, code, country code, NXX code.

*-Arena

[UNIX] n. The area of memory attached to a process by `brk(2)' and `sbrk(2)' and used by `malloc(3)' as dynamic storage. So named from a `malloc corrupt arena' message emitted when some early versions detected an impossible value in the free block list. See aliasing bug, memory leak, memory smash, smash the stack.

*-Arg

/arg/ n. Abbreviation for `argument' (to a function), used so often as to have become a new word (like `piano' from `pianoforte'). “The sine function takes 1 arg, but the arc-tangent function can take either 1 or 2 args. ” Compare param, parm, var.

Argument

1. An independent variable. (FP) (ISO)
2. Any value of an independent variable: for example, a search key, or a number that identifies the location of a data item in a table. (FP) (ISO)

Arithmetic And Logic Unit

(ALU) A part of a computer that performs arithmetic, logic, and related operations. (FP) (ISO)

Arithmetic Operation

An operation performed according to the rules of arithmetic.

Arithmetic Overflow

Synonym overflow.

Arithmetic Register

A register that holds the operands or the results of operations such as arithmetic operations, logic operations, and shifts. (FP)

Arithmetic Shift

A shift, applied to the representation of a number in a fixed radix numeration system and in a fixed-point representation system, and in which only the characters representing the fixed-point part of the number are moved. An arithmetic shift is usually equivalent to multiplying the number by a positive or a negative integral power of the radix, except for the effect of any rounding; compare the logical shift with the arithmetic shift, especially in the case of floating-point representation. (FP) (ISO)

Arithmetic Underflow

Synonym underflow.

Arithmetic Unit

In a processor, the part that performs arithmetic operations; sometimes the unit performs both arithmetic and logic operations. (FP) (ISO)

*-ARMM

n. [acronym, `Automated Retroactive Minimal Moderation'] A Usenet robot created by Dick Depew of Munroe Falls, Ohio. ARMM was intended to automatically cancel posts from anonymous-posting sites. Unfortunately, the robot's recognizer for anonymous postings triggered on its own automatically-generated control messages! Transformed by this stroke of programming ineptitude into a monster of Frankensteinian proportions, it broke loose on the night of March 31, 1993 and proceeded to spam news. admin. policy with a recursive explosion of over 200 messages. ARMM's bug produced a recursive cascade of messages each of which mechanically added text to the ID and Subject and some other headers of its par-

ent. This produced a flood of messages in which each header took up several screens and each message ID and subject line got longer and longer and longer. Reactions varied from amusement to outrage. The pathological messages crashed at least one mail system, and upset people paying line charges for their Usenet feeds. One poster described the ARMM debacle as "instant Usenet history" (also establishing the term despew), and it has since been widely cited as a cautionary example of the havoc the combination of good intentions and incompetence can wreak on a network. Compare Great Worm, the; sorcerer's apprentice mode. See also software laser, network meltdown.

ARPANET

See Advanced Research Projects Agency NETwork.

Array

1. An arrangement of elements in one or more dimensions. (FP)
2. In a programming language, an aggregate that consists of data objects with identical attributes, each of which may be uniquely referenced by subscription. (FP) (ISO)

Array Processor

A processor capable of executing instructions in which the operands may be arrays rather than data elements. (FP) (ISO) Synonym vector processor.

Arrest

The discovery of user activity not necessary to the normal processing of data which might lead to a violation of system security and force termination of the processing. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; DODD 5200. 28M;)

Artificial Intelligence

The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement. (FP) Note: AI is the branch of computer science that attempts to approximate the results of human reasoning by organizing and manipulating factual and heuristic knowledge. Areas of AI activity include expert systems, natural language understanding, speech recognition, vision, and robotics.

ASCII

/as'kee/ n. [acronym American Standard Code for Information Interchange] The predominant character set encoding of present-day computers. The modern version uses 7 bits for each character, whereas most earlier codes (including an early version of ASCII) used fewer. This change allowed the inclusion of lowercase letters -- a major win -- but it did not provide for accented letters or any other letterforms not used in English (such as the German sharp-S or the ae-ligature which is a letter in, for example, Norwegian). It could be worse, though. It could be much worse. See EBCDIC to understand how. Computers are much pickier and less flexible about spelling than humans; thus, hackers need to be very precise when talking about characters, and have developed a considerable amount of verbal shorthand for them. Every character has one or more names -- some formal, some concise, some silly. Common jargon names for ASCII characters are collected here.

*-ASCIIbetical Order

/as'kee-be'-t*-kl or'dr/ adj. ,n. Used to indicate that data is sorted in ASCII collated order rather than alphabetical order. This lexicon is sorted in something close to ASCIIbetical order, but with case ignored and entries beginning with non-alphabetic characters moved to the end.

Assemble

To translate a computer program expressed in an assembly language into a machine language.

Assembler

A computer program that is used to assemble. (FP) (ISO) Synonym assembly program. See also compiler, translator.

Assembly

A group of parts, elements, subassemblies, and circuits assembled as a separately removable item of COMSEC equipment. (NCSC-9)

Assembly Language

A computer-oriented language whose instructions are symbolic and usually in one-to-one correspondence with computer instructions and that may provide facilities such as the use of macro instructions. (FP) (ISO) (~) Synonym computer-dependent language. See also compile, computer language, computer-oriented language, high-level language, language, machine language.

Assembly Phase

The logical subdivision of a run that includes the execution of an assembler. (FP) (ISO)

Assembly Program

Synonym assembler.

Assembly Time

The elapsed time taken for the execution of an assembler. (FP) (ISO) See also assembler, compiler.

Assertion

A compound predicate concerning the values of attributes of certain specified entities, and/or the existence of certain relationships among them. (ET;, MA;)

Assessing Controlled Access Protection

Assessment

1. An analysis of the vulnerabilities of Automated Information Systems. (*NCSC-WA*-001-85;)
2. An in-depth study of encrypted text, related traffic and collateral information to determine the adequacy of the technical design and security provided by a code, cipher or other manual cryptosystem. (NACSI 4007)
3. See Risk Assessment and Vulnerability Assessment.

#-Assessments (e. G. , Surveys, Inspections)

Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems in order to be successful in the mission. Assessments can be tailored to meet the needs of the requesting customer. Assessments normally review specific telecommunications and/or AIS', departmental, or organizational procedures or activities. (Source: Panel of Experts, July 1994).

Asset

1. Any software, data, hardware, administrative, physical, communications, or personnel resource within an ADP system or activity. (*OPNAVINST* 5239. 1A;)
2. An individual entity of the internal environment that must be protected from all types of peril. (ET;)
3. An item whose compromise, as the result of an event, causes a financial loss to its owner. (RM;)

Asset Category

A grouping of individual asset items. (RM;)

Asset Container

Asset Granularity

The degree to which assets are considered as individual assets or as a class. (MK;)

Association Description

A data structure that represents a collection of relationships between conceptual entities. (MA;)

Assurance

A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation. (DODD 5200. 28)

Assurance Testing

A process used to determine that the security features of a system are implemented as designed, and that they are adequate for the proposed environment. This process may include hands-on functional testing, penetration testing and/or verification. (DOE 5637. 1)

#-Asynchronous And Synchronous Communications

1. Asynchronous communications is a transmission method in which each transmitted data character is preceded by a start bit and followed by a stop bit. This permits the time interval between each character to vary. On the other hand synchronous communications does not require the start and stop bit, but do require synchronized clocks and data. (Panel of experts).
2. Pronounced “ay-sink' chroh-nuss. ” A method of data communication in which the transmission of bits of data is not synchronized by a clock signal but is accomplished by sending the bits on after another, with a start bit and a stop bit to mark the beginning and end of the data unit. (*QCUS+Pf-90*)

Asynchronous Attack

[An] asynchronous attack [.] is an attempt to exploit the interval between a defensive act and the attack in order to render inoperative the effect of the defensive act. For instance, an operating task may be interrupted at once following the checking of a stored parameter; the user regains control and malevolently changes the parameter; the operating system regains control and [continues] processing using the maliciously altered parameter. (JL;)

Asynchronous Network

Synonym nonsynchronous network.

Asynchronous Operation

Method of computer processing in which one operation is completed before the next one starts.

Asynchronous Transfer Mode

(ATM) A data-transfer mode in which a multiplexing technique for fast packet switching in CCITT broadband ISDN is used. This technique inserts information in small, fixed-size cells (32-120 octets) that are multiplexed and switched in a slotted operation, based upon header content, over a virtual circuit established immediately upon a request for service.

Asynchronous Transmission

Data transmission in which the instant that each character, or block of characters, starts is arbitrary; once started, the time of occurrence of each signal representing a bit within the character, or block, has the same relationship to significant instants of a fixed time frame. (~) See also block, character, intercharacter interval, isochronous, plesiochronous, synchronous transmission.

Asynchronous Working

Synonym asynchronous operation.

AT&T

American Telephone and Telegraph

*-Atomic

adj. [from Gk. `atomos', indivisible]

1. Indivisible; cannot be split up. For example, an instruction may be said to do several things `atomically', i. e. , all the things are done immediately, and there is no chance of the instruction being half-completed or of another being interspersed. Used esp. to convey that an operation cannot be screwed up by interrupts. “This routine locks the file and increments the file's semaphore atomically. ”
2. [primarily techspeak] Guaranteed to complete successfully or not at all, usu. refers to database transactions. If an error prevents a partially-performed transaction from proceeding to completion, it must be “backed out,” as the database must not be left in an inconsistent state. Computer usage, in either of the above senses, has none of the connotations that `atomic' has in mainstream English (i. e. of particles of matter, nuclear explosions etc.).

Attachment Unit Interface

In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (FP) (ISO)

Attack

1. The act of aggressively trying to bypass security controls on an Automated Information System. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (*NCSC-WA*-001-85;)
2. The realization of a threat. How often a threat is realized depends on such factors as the location, type, and value of information being processed. Thus, short of moving the system or facility or radically changing its mission, there is usually no way that the level of protection can affect the frequency of attack. The exceptions to this are certain human threats where effective security measures can have a deterrent effect. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (*OPNAVINST* 5239. 1A;)

Attack Time

The time interval between the instant that a signal at the input of a device or circuit exceeds the activation threshold of the device or circuit, and the instant that the device or circuit reacts in a specified manner, or to a specified degree, to the input. Note: The term often implies a protective action such as that provided by a clipper (peak limiter) or compressor, but may be used to describe the action of a device such as a vox, where the action is not protective.

Attempt

See access attempt, disengagement attempt.

Attention Character

In TCB design, a character that, when entered from a terminal, tells the TCB that the user wants a secure communications path from the terminal to some trusted code in order to provide a secure service for the user such as logging in or logging out. (MTR-8201;)

#-Attenuation

Reducing the amplitude of an electrical signal without appreciable distortion. (Source: Panel of Experts, July 1994); (2) the reduction in strength of an electrical signal as it passes through a circuity or an electromagnetic wave as it propagates through a transmission medium. (*ISDCST+LSC-1992*

*-Attoparsec

n. About an inch. `atto-' is the standard SI prefix for multiplication by 10^(-18). A parsec (parallax-second) is 3. 26 light-years; an attoparsec is thus 3. 26 * 10^(-18) light years, or about 3. 1 cm (thus, 1 attoparsec/microfortnight equals about 1 inch/sec). This unit is reported to be in use (though probably not very seriously) among hackers in the U. K. See micro-.

Attribute

1. A binary relation in which the first component of every pair is a conceptual entity and the second component of every pair is a value. (ET;)
2. A binary relation in which the first component of every pair is a conceptual entity and the second component of every pair is a descriptor (i. e. value). (MA;)

Attribute Of An Entity

A specific ordered pair in an attribute. (ET;, MA;)

Audit

1. To conduct an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures. (DODD 5200. 28;)
2. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure

compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures. a. Internal Security Audit. An audit conducted by personnel responsible to the management of the organization being audited. b. External Security Audit. An audit conducted by an organization independent of the one being audited. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; *FIPS PUB* 39;)

3. The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures. *The independent review and examination of records and activities in order to test for adequacy of system controls, to ensure compliance with established controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures NOTE: An audit may be conducted by personnel responsible to the management of the organization being audited (internal) or by an organization independent of the one being audited (external) (NSA, *National INFOSEC Glossary*, 10/88)

Audit Analysis Tools

#-Audit Collection Requirements

The ISSO must determine what auditable events will be collected based on mode of operation and levels of trust to meet the requirements defined in the information systems security policy. (Source: Panel of Experts, July 1994).

Audit Event

Audit Log

#-Audit Mechanism

The device used to collect, review, and/or examine system activities. (Source: *NCSC-TG*-001)

Audit Parameters

Audit Record

Audit Reduction Tools

Audit Review File

A file created by executing statements included in a program for the explicit purpose of providing data for auditing. (FP) (ISO)

Audit Trail

1. An automated or manual set of records that collectively provide documentary evidence of processing used to aid in tracing system activities. (*AFR* 205-16;)
2. A chronological record of activities which will enable the reconstruction, review and examination of the sequence of environments and activities concerning each event in the transaction. (*AR* 380-380;)
3. A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. (CSC-STD-001-83;)
4. A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in the path of a transaction from its inception to output of final results. (DODD 5200. 28;, *FIPS PUB* 39;)
5. A set of manual and/or automated produced records that provide documentary evidence of system use. (NCSC-wa-001-85;)
6. A special case of an activity log that is sufficient to enable reconstruction, review, and examination of the sequence of activities involved in every transaction. (RM;)
7. A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of events leading towards a particular final result. 8)
8. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results. (*OPNAVINST* 5239. 1A;)

#-Audit Trails And Logging

1. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event;
2. a chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. (NCSC TG 017). Note: Audit trail may apply to information in an AIS, to message routing in a communications system, or to the transfer of COMSEC material. (NSTISSI 4009).
3. A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from re-

cords and reports to their component source transactions. (*NCSC-TG*-001).

#-Audit Trails And Logging Policies

Written guidance defining howaudit collection requirements are to be implemented, to includewho has access to audit records, how often audits will bearchived and how long archives will be retained, and how oftenaudits will be reviewed. (Panel of Experts, July 1994).

#-Auditable Events

Any event that can be selected for inclusionin the audit trail. These events should include, in addition tosecurity-relevant events, events taken to recover the systemafter failure and any events that might prove to be securityrelevant at a later time. (Source: *NCSC-TG*-001 Version 2. .

#-Auditing Tools

Auditor

Represents the cognizant audit office designated by the DCAA or Service audit activities for conducing audit reviews of the contractor's accounting systme policies and procedures for compliance with the criteria

Authenticate

1. To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
2. To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.
3. To establish the validity of a claimed identity. (CSC-STD-001-83;; *NCSC-WA*-001-85;)
4. A challenge given by voice or electrical means to attest to the authenticity of a message or transmission. (JP 1-02)

Authenticated User

Authentication

1. A means of identifying individuals and verifying their eligibility to receive specific categories of information. (*AFR* 205-16)
2. The act of identifying or verifying the eligibility of a station, originator, or individual to access information. This measure is designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. (*AR* 380-380)
3. A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified. (*DCID* 1/1 6; *DCID* 1/1 6, Sup.)
4. The act of verifying the claimed identity of an individual, station or originator. (DOE 5637. 1)
5. The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. b. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. (*FIPS PUB* 39)
6. Measures designed to provide protection against fraudulent transmission and imitative communications deception by establishing the validity of transmission, message, station, or individual. (NCSC-9)

Authentication Data Base

Authentication Equipment

Equipment designed to provide protection against fraudulent transmissions and imitative communications deception or to establish the authenticity of a transmission, message, station, originator, or telecommunications system. (NACSIM 2002)

Authentication Period

Authentication period is the maximum acceptable period between any initial authentication process and subsequent reauthentication processes during a single terminal session or during the period data is being accessed. (*FIPS PUB* 112;)

Authentication Process

The actions involving: a. obtaining an identifier and a personal password from an ADP system user; b. comparing the entered password with the stored, valid password that was issued to, or selected by, the person associated with that identifier; and c. authenticating the identity if the entered password and the stored password are the same. (Note: If the enciphered password is stored, the entered password must be enciphered and compared with the stored ciphertext or the ciphertext must be deciphered and compared with the entered password.) (*FIPS PUB* 112;)

Authentication System

A cryptosystem or a cryptographic process used for authentication. (NCSC-9)

Authenticator

1. The means used to identify or verify the eligibility of a station, originator or individual to access specific categories of information. The authenticator may be a symbol, sequence of symbols, or series of prearranged bits that are usually inserted at a predetermined point within a message or transmission for the purpose of authentication. (*AR* 380-380;)

2. The means used to identify or verify the eligibility of a station, originator, or individual to access specific categories of information. b. A symbol, a sequence of symbols, or a series of bits that are arranged in a predetermined manner and are usually inserted at a predetermined point within a message or transmission for the purpose of an authentication of the message or transmission. (*FIPS PUB* 39;)
3. The means used to confirm the identity or verify the eligibility of a station, originator, or individual (*NCSC-WA*-001-85;)
4. A symbol or group of symbols, or a series of bits selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission. (NCSC-9)
5. The means used to confirm the identity or to verify the eligibility of a station, originator or individual. (*NCSC-TG*-004-88)

Authority Arrest

The discovery of user activity not necessary to the normal processing of data which might lead to a violation of system security and force termination of the processing. (*OPNAVINST*5239. lA; *AR* 380-380; *DOD* 5200. 28M)

Authorization

1. The privilege granted to an individual by a designated official to access information based upon the individual's clearance and need-to-know. (DOE 5637. 1)
2. The granting to a user, program, or process the right of access. (*AR* 380-380; Fl PS PUB 39)

Authorization Process

The actions involving: a. obtaining an access password from an ADP system user (whose identity has already been authenticated, perhaps using a personal password); b. comparing the access password with the password associated with the protected data; and c. authorizing access to the data if the entered password and the stored password are the same (*FIPS PUB* 112;)

Authorized Station

A station legitimately provided with all the current keys, procedures, and time information necessary to communicate with another station.

Authorized Vendor

1. Program in which a vendor, producing a Program COMSEC product under contract to the National Security Agency, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. NOTE: Eligible buyers are typically U. S. Government organizations or U. S. Government contractors. Products approved for marketing and sale through the Authorized Vendor Program are placed on the Endorsed Cryptographic Products List.
2. Manufacturer of existing COMSEC equipment who is authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers.

Authorized Vendor Program

(AVP) Program in which a vendor, producing a COMSEC product under contract to the National Security Agency, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. NOTE: Eligible buyers are typically U. S. Government organizations or U. S. Government contractors. Products approved for marketing and sale through the Authorized Vendor Program are placed on the Endorsed Cryptographic Products List.

Auto-Manual System

(AMS) Programmable, hand-held crypto-equipment used to perform encoding and decoding functions.

Autobogotiphobia*

/aw'toh-boh-got`*-foh'bee-*/ n. See bogotify.

AUTODIN

See AUTOmatic DIgital Network.

Automagically*

/aw-toh-maj'i-klee/ adv. Automatically, but in a way that, for some reason (typically because it is too complicated, or too ugly, or perhaps even too trivial), the speaker doesn't feel like explaining to you. See magic. "The C-INTERCAL compiler generates C, then automagically invokes `cc(1)' to produce an executable. "

Automated Data Medium

Synonym machine-readable medium.

Automated Data Processing

Automated Data Processing Equipment

(ADPE) See Automated Information System (AIS).

Automated Data Processing Security

See automated information systems security, Computer Security

Automated Decision Making Computer

Computer applications that issue checks, requisition supplies, or perform similar functions based on programmed criteria, with little human intervention. (*AFR* 205-16)

Automated Decision-Making System

Computer applications that perform decision making activities, such as issue checks or requisition supplies,

based on programmed criteria, with little human intervention.

Automated Information

1. An assembly of computer hardware, software, System (AIS) and firmware configured to collect, communicate, compute, disseminate, and/or control data. (DODD 5200. 28;)
2. Systems that create, prepare, or manipulate information in electronic form for purposes other than telecommunications or device control including computers, word processing systems, other electronic information handling systems, and associated equipment. (*NCSC-WA*-001-85;)
3. Systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment. (NSDD-145;)

Automated Information System

(AIS) Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes software, firmware, and hardware. NOTE: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment. See Computer, Computer Network, Computer System, Network, and System.

Automated Information System Security

Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS. See Computer Security

Automated Information Systems Security

1. Measures and controls that protect an AIS against denial of service and unauthorized, (accidental or intentional) disclosure, modification or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS. (*NCSC-TG*-004-88)
2. See COMPUTER SECURITY.

Automated Information Systems(s)

1. (AIS) An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data and information. (DODD 5200. 28)
2. Automated information systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment. (NSDD-145; NTISSP 200)
3. An information system (as defined in Section 6d of the Circular) that is automated. (A-1 30)

Automated Security

The use of automated procedures to ensure that automation security controls are not circumvented. (*AR* 380-380;; *NCSC-WA*-001-85;)

Automated Security Monitoring

1. The use of automated procedures to ensure that automation security controls are not circumvented. (*AR* 380-380)
2. The use of automated procedures to ensure that the security controls implemented within an ADP system are not circumvented. (*FIPS PUB* 39)

#-Automated Security Tools

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information. (Source: NSTISSI 4009).

Automated System Security

All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive unclassified or critical data, material, or processes in the system. It includes:

a. All hardware and software functions, characteristics and features;
b. Operational procedures;
c. Access controls at all computer facilities (includes those housing mainframes, terminals, minicomputers, or microcomputers);
d. Management constraints;
e. Physical protection;

f. Control of compromising emanations (TEMPEST);
g. Personnel and communications security (COMSEC); and
h. Other security disciplines. (*AFR* 205-16;)

Automatic

Pertaining to a process or device that, under specified conditions, functions without intervention by a human operator. (FP) (ISO)

Automatic Answering

A service feature in which the called terminal automatically responds to the calling signal and the call may be established whether or not the called terminal is attended by a human operator. See also call, data terminal equipment, facility, service feature.

Automatic Data Handling

A generalization of automatic data processing to include the aspect of data transfer. (JCS1-DoD) (JCS1-NATO) See also data.

Automatic Data Processing

1. An assembly of computer hardware, firmware, and (ADP) Systemsoftware, configured for the purpose of calculating, computing, sorting, transmitting, receiving, storing and retrieving data with a minimum of human intervention. (CSC-STD-005-85;; CSC-STD-001-83;) (F:\NEWDEFS. TXT)
2. An interacting assembly of procedures, processes, methods, personnel, and equipment to perform automatically a series of data processing operations that result in a change in the semantic content of the data. (~)
3. Data processing by means of one or more devices that use common storage for all or part of a computer program, and also for all or part of the data necessary for execution of the program; that execute user-written or user-designated programs; that perform user-designated symbol manipulation, such as arithmetic operations, logic operations, or character-string manipulations; and that can execute programs that modify themselves during their execution. Automatic data processing may be performed by a stand-alone unit or by several connected units. (FP)
4. Data processing largely performed by automatic means. (JCS1-DoD) (JCS1-NATO)
5. That branch of science and technology concerned with methods and techniques relating to data processing largely performed by automatic means. (JCS1-DoD) (JCS1-NATO)

Automatic Data Processing Equipment

Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information (i) by a Federal agency, or (ii) under a contract with a Federal agency which (I) requires the use of such equipment, or (II) requires the performance of a service or the furnishing of a product which is performed or produced making significant use of such equipment. Such term includes (i) computer, (ii) ancillary equipment, (iii) software, firmware, and similar procedures, (iv) services, including support services, and (v) related resources as defined by regulations issued by the Administrator for General Services. (Public Law 99-500, Title VII, Sec. 822 (a) Section 111(a) of the Federal Property and Administrative Services Act of 1949 (40 U. S. C. 759(a)) revised.)

Automatic Data Processing System

An assembly of computer hardware, firmware, and software, configured for the purpose of calculating, computing, sorting, transmitting, receiving, storing and retrieving data with a minimum of human intervention. (CSC-STD-005-85; *DOD* 5200. 28-STD; DOE 5635. l A)

Automatic Dialing

See automatic calling unit.

Automatic Message Accounting

A service feature that automatically records data of user-dialed calls. (~) See also audit trail, automatic number identification, call, call record, service feature.

Automatic Message Processing System

Any organized assembly of resources and methods used to collect, process, and distribute messages largely by automatic means. (JCS1-DoD)

Automatic Number Identification

A service feature whereby the directory number or equipment number of a calling station is obtained automatically, for use in message accounting. See also automatic message accounting, call, service feature.

Automatic Operation

The functioning of an apparatus, process, or system in a desired manner and at the proper time under control of mechanical or electronic devices that take the place of operators.

Automatic Remote

Procedure to rekey a distant crypto-rekeying equipment electronically without specific actions by the receiving terminal operator.

Automatic Remote Rekeying

Procedure to rekey a distant crypto-equipment electronically without specific actions by the receiving terminal operator.

Automatic Remote Reprogramming And Rekeying

The procedure by which distant equipment is reprogrammed or rekeyed electronically without specific actions by the receiving terminal.

Automatic Repeat-Request

Automatic Route Selection

Electronically or mechanically controlled selection and routing of outgoing calls without human intervention or assistance. See also adaptive routing, call, proration.

Automatic Secure Voice Communications Network (AUTOSEVOCOM)

A worldwide, switched, secure voice network developed to fulfill DoD long-haul, secure voice requirements. (JCS1-DoD) (~) See also Automatic Digital Network, Automatic Voice Network, communications, Federal Telecommunications System.

Automatic Voice Network

The principal long-haul, unsecure voice communications network within the Defense Communications System. (JCS1-DoD) (~) See also Automatic Digital Network, Automatic Secure Voice Communications Network, communications.

Automation

1. The implementation of processes by automatic means. (JCS1-DoD) (FP) (ISO)
2. The investigation, design, development, and application of methods of rendering processes automatic, self-moving, or self-controlling. (FP)
3. The conversion of a procedure, a process, or equipment to automatic operation. (JCS1-DoD)

Automation Security

The measures employed to protect automation and the information handled from both hostile and benign threats and to safeguard against unauthorized exploitation through espionage, sabotage, theft, fraud, misappropriation, or misuse. Automation security applies to all ADP systems and applies to the global aspects of the security problem. Therefore, it encompasses the security management, hardware, software, procedural, communications, personnel, physical and environmental, and all other security aspects contributing to the protection of automated systems (hardware and software), site, activity, facility, or operation as a potential target. (*AR* 380-380;)

Auxiliary Power

An alternate source of electric power, serving as backup for the primary power at the station main bus or prescribed sub-bus. (~) Note: An off-line unit provides electrical isolation between the primary power and the critical technical load; an on-line unit does not.

Class A power source is a primary power source; i. e. , a source that assures an essentially continuous supply of power.

Types of auxiliary power service include:

Class B: a standby power plant to cover extended outages (days);

Class C: a quick-start (10 to 60 seconds) unit to cover short-term outages (hours);

Class D: an uninterruptible (no-break) unit using stored energy to provide continuous power within specified voltage and frequency tolerances.

See also power, primary power, station battery.

Auxiliary Storage

1. Storage that is available to a processor only through input/output channels. (FP)
2. In a microcomputer, storage that is not memory; for example, storage on diskettes, on streaming tapes, or on magnetic tape cartridges. (FP)

#-Availability

1. That computer security characteristic that ensures the computer resources will be available to authorized users when they need them. This characteristic protects against denial of service. (*AFR* 205-16;);
2. The property of being accessible and usable upon demand by an authorized entity. (*NCSC-TG*-029).

Availability Of Data

1. The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.
2. Data that is in the place, at the time, and in the form needed by the user.

*-Avatar

n. Syn. [CMU, Tektronix] root, superuser. There are quite a few UNIX machines on which the name of the superuser account is `avatar' rather than `root'. This quirk was originated by a CMU hacker who disliked the term `superuser', and was propagated through an ex-CMU hacker at Tektronix.

Average Rate Of Transmission

Synonym effective speed of transmission.

Avoiding Information Monopolies

Awk*

1. /awk/ n. [UNIX techspeak] An interpreted language for massaging text data developed by Alfred Aho, Peter Weinberger, and Brian Kernighan (the name derives from their initials). It is characterized by C-like syntax, a declaration-free approach to variable typing and declarations, associative ar-

rays, and field-oriented text processing. See also Perl.

2. n. Editing term for an expression awkward to manipulate through normal regexp facilities (for example, one containing a newline).
3. vt. To process data using `awk(1)'.

B

B

Abbreviation for bit. See binary digit.

B Channel

The CCITT designation for a clear channel, 64-kbps service capability provided to a subscriber under the Integrated Services Digital Network offering. Note: The B channel is intended for transport of user information, as opposed to signaling information. See also Integrated Services Digital Network.

B1

B1FF*

/bif/ [Usenet] (alt. `BIFF') n. The most famous pseudo, and the prototypical newbie. Articles from BIFF feature by all uppercase letters sprinkled liberally with bangs, typos, `cute' misspellings (EVRY BUDY LUVS GOOD OLD BIFF CUZ HE”S A K00L DOOD AN HE RITES REEL AWESUM THINGZ IN CAPITULL LETTRS LIKE THIS!!!), use (and often misuse) of fragments of talk mode abbreviations, a long sig block (sometimes even a doubled sig), and unbounded naivete. BIFF posts articles using his elder brother's VIC-20. BIFF's location is a mystery, as his articles appear to come from a variety of sites. However, BITNET seems to be the most frequent origin. The theory that BIFF is a denizen of BITNET is supported by BIFF's (unfortunately invalid) electronic mail address BIFF@BIT. NET. [1993 how It Can Be Told! My spies inform me that BIFF was originally created by Joe Talmadge <jat@cup. hp. com>, also the author of the infamous and much-plagiarized “Flamer's Bible”. The BIFF filter he wrote was later passed to Richard Sexton, who posted BIFFisms much more widely. Versions have since been posted for the amusement of the net at large. -- ESR]

B2

See Orange Book

B3

See Orange Book

Back Door

n. A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers. Syn. trap door; may also be called a `wormhole'. See also iron box, cracker, worm, logic bomb. Historically, back doors have often lurked in systems longer than anyone expected or planned, and a few have become widely known. Ken Thompson's 1983 Turing Award lecture to the ACM suggested the possibility of a back door in early UNIX versions that may have qualified as the most fiendishly clever security hack of all time (Thompson's presentation managed to be unclear on whether it was ever actually implemented or not). In this scheme, the C compiler contained code that would recognize when the `login' command was being recompiled and insert some code recognizing a password chosen by Thompson, giving him entry to the system whether or not an account had been created for him. Normally such a back door could be removed by removing it from the source code for the compiler and recompiling the compiler. But to recompile the compiler, you have to *use* the compiler -- so Thompson also arranged that the compiler would *recognize when it was compiling a version of itself*, and insert into the recompiled compiler the code to insert into the recompiled `login' the code to allow Thompson entry -- and, of course, the code to recognize itself and do the whole thing again the next time around! And having done this once, he was then able to recompile the compiler from the original sources; the hack perpetuated itself invisibly, leaving the back door in place and active but with no trace in the sources. The talk that suggested this truly moby hack was published as “Reflections on Trusting Trust”, “Communications of the ACM 27”, 8 (August 1984), pp. 761--763.

Back-To-Back Connection

A connection between the output of a transmitting device and the input of an associated receiving device. (~) Note: When used for equipment measurements or testing purposes, this eliminates the effects of the transmission channel or medium. See also loopback (def. #2).

-Backbone Site

n. A key Usenet and email site; one that processes a large amount of third-party traffic, especially if it is the home site of any of the regional coordinators for the Usenet maps. Notable backbone sites as of early 1993 include uunet and the mail machines at Rutgers University, UC Berkeley, DEC's Western Research Laboratories, Ohio State University, and the University of Texas. Compare rib site, leaf site.

Backdoor

See Trap Door.

-Backgammon

See bignum (sense 3), moby (sense 4), and pseudoprime.

-Background

n. ,adj. ,vt. To do a task `in background' is to do it whenever foreground matters are not claiming your undivided attention, and `to background' something means to relegate it to a lower priority. “For now, we'll just print a list of nodes and links; I'm working on the graph-printing problem in background. ” Note that this implies ongoing activity but at a reduced level or in spare time, in contrast to mainstream `back burner' (which connotes benign neglect until some future resumption of activity). Some people prefer to use the term for processing that they have queued up for their unconscious minds (a tack that one can often fruitfully take upon encountering an obstacle in creative work). Compare amp off, slopsucker. Technically, a task running in background is detached from the terminal where it was started (and often running at a lower priority); oppose foreground. Nowadays this term is primarily associated with UNIX, but it appears to have been first used in this sense on OS/360.

#-Background Investigations #

Required review into a person's past in the determination of granting security clearance. (Source: Panel of Experts, July 1994).

Background Processing

The [automatic] execution of lower priority computer programs when higher priority programs are not using the system resources. (FP) See also batch processing.

-Backspace And Overstrike

interj. Whoa! Back up. Used to suggest that someone just said or did something wrong. Common among APL programmers.

Backup File

A copy of a file made for purposes of later reconstruction of the file, if necessary. (FP) (ISO) Synonym job-recovery control file.

Backup Plan

See Contingency Plan.

Backup Procedures

The provisions made for the recovery of data files and program libraries, and for restart or replacement of ADP equipment after a system failure or disaster. (*AR* 380-380; *FIPS PUB* 39;)

Backups#

Copy of files made for purposes of later reconstruction of the file, if necessary. (Federal Standard 1037B, per EKMS 004. 01); The provisions made for the recovery of data files and program libraries, and for restart or replacement of information systems after the occurrence of a failure or of a disaster (ISDCST+LSC-92).

Backward Channel

1. In data transmission, a secondary channel whose direction of transmission is constrained to be opposite to that of the primary (or forward) channel. Note: The direction of transmission in the backward channel is restricted by the control interchange circuit that controls the direction of transmission in the primary channel.
2. The channel of a data circuit that passes data in a direction opposite to that of its associated forward channel. (~) Note: The backward channel is usually used for transmission of supervisory, acknowledgement, or error-control signals. The direction of flow of these signals is opposite to that in which information is being transferred. The bandwidth of this channel is usually less than that of the forward channel; i. e. , the information channel. See also backward signal, data transmission, forward channel, forward signal, information-bearer channel.

-Backward Combatability

/bak'w*rd k*m-bat'*-bil'*-tee/ n. [CMU, Tektronix from `backward compatibility'] A property of hardware or software revisions in which previous protocols, formats, layouts, etc. are irrevocably discarded in favor of `new and improved' protocols, formats, and layouts, leaving the previous ones not merely deprecated but actively defeated. (Too often, the old and new versions cannot definitively be distinguished, such that lingering instances of the previous ones yield crashes or other infelicitous effects, as opposed to a simple “version mismatch” message.) A backwards compatible change, on the other hand, allows old versions to coexist without crashes or error messages, but too many major changes incorporating elaborate backwards compatibility processing can lead to extreme software bloat. See also flag day.

Backward Recovery

The reconstruction of an earlier version of a file by using a newer version of data recorded in a journal. (FP) (ISO)

Bacterium

A bacterium (also known as a chain letter) is a program which propagates itself by electronic mail to everyone in the victim's mailing list. It may also contain a logic bomb or trojan horse. (IC;)

-BAD

/B-A-D/ adj. [acronym, `Broken As Designed'] Said of a program that is bogus because of bad design and misfeatures rather than because of bugginess. See working as designed.

-Bad Thing

n. [from the 1930 Sellar & Yeatman parody “1066 And All That”] Something that can't possibly result in improvement of the subject. This term is always capitalized, as in “Replacing all of the 9600-baud mo-

dems with bicycle couriers would be a Bad Thing". Oppose Good Thing. British correspondents confirm that Bad Thing and Good Thing (and prob. therefore Right Thing and Wrong Thing) come from the book referenced in the etymology, which discusses rulers who were Good Kings but Bad Things. This has apparently created a mainstream idiom on the British side of the pond.

Balanced Code

1. In PCM systems, a code constructed such that the spectrum resulting from the transmission of any code word has no dc component. (~)
2. A code whose digital sum variation is finite. See also code, pulse-code modulation.

-Banana Label

n. The labels often used on the sides of macrotape reels, so called because they are shaped roughly like blunt-ended bananas. This term, like macrotapes themselves, is still current but visibly headed for obsolescence.

Band

1. In communications, the frequency spectrum between two defined limits. (~)
2. A group of tracks on a magnetic drum or on one side of a magnetic disk.
3. A designator used by common carriers to define geographical areas. See also common carrier, frequency guard band.

Bandwidth

A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second. (CSC-STD-001-83;)

Bandwidth Compression

Any technique to reduce the bandwidth needed to transmit a given amount of information in a given time, or to reduce the time needed to transmit a given amount of information in a given bandwidth. (~) Note: The term implies reducing the normal bandwidth of an information-carrying signal by some means that does not reduce its information content. See also biternary transmission, data compression, necessary bandwidth.

*-Bang

1. n. Common spoken name for `!' (ASCII 0100001), especially when used in pronouncing a bang path in spoken hackish. In elder days this was considered a CMUish usage, with MIT and Stanford hackers preferring excl or shriek; but the spread of UNIX has carried `bang' with it (esp. via the term bang path) and it is now certainly the most common spoken name for `!'. Note that it is used exclusively for non-emphatic written `!'; one would not say "Congratulations bang" (except possibly for humorous purposes), but if one wanted to specify the exact characters `foo!' one would speak "Eff oh oh bang". See shriek, ASCII.
2. interj. An exclamation signifying roughly "I have achieved enlightenment!", or "The dynamite has cleared out my brain!" Often used to acknowledge that one has perpetrated a thinko immediately after one has been called on it.

-Bang On

vt. To stress-test a piece of hardware or software "I banged on the new version of the simulator all day yesterday and it didn't crash once. I guess it is ready for release. " The term pound on is synonymous.

-Bang Path

n. An old-style UUCP electronic-mail address specifying hops to get from some assumed-reachable location to the addressee, so called because each hop is signified by a bang sign. Thus, for example, the path . !bigsite!foovax!barbox!me directs people to route their mail to machine bigsite (presumably a well-known location accessible to everybody) and from there through the machine foovax to the account of user me on barbox. In the bad old days of not so long ago, before autorouting mailers became commonplace, people often published compound bang addresses using the convention (see glob) to give paths from *several* big machines, in the hopes that one's correspondent might be able to get mail to one of them reliably (example . !seismo, ut-sally, ihnp4!rice!beta!gamma!me). Bang paths of 8 to 10 hops were not uncommon in 1981. Late-night dial-up UUCP links would cause week-long transmission times. Bang paths were often selected by both transmission time and reliability, as messages would often get lost. See Internet address, network, the, and sitename.

-Banner

1. n. The title page added to printouts by most print spoolers (see spool). Typically includes user or account ID information in very large character-graphics capitals. Also called a `burst page', because it indicates where to burst (tear apart) fan-fold paper to separate one user's printout from the next.
2. A similar printout generated (typically on multiple pages of fan-fold paper) from user-specified text, e. g. , by a program such as UNIX's `banner(1,6)'.
3. On interactive software, a first screen containing a logo and/or author credits and/or a copyright notice.

Bar Code

A code representing characters by sets of parallel bars of varying thickness and separation that are read optically by transverse scanning. (FP) (ISO)

-Bare Metal

1. n. New computer hardware, unadorned with such snares and delusions as an operating system, an HLL, or even assembler. Commonly used in the phrase `programming on the bare metal', which refers to the arduous work of bit bashing needed to create these basic tools for a new machine. Real bare-metal programming involves things like building boot proms and BIOS chips, implementing basic monitors used to test device drivers, and writing the assemblers that will be used to write the compiler back ends that will give the new machine a real development environment.
2. `Programming on the bare metal' is also used to describe a style of hand-hacking that relies on bit-level peculiarities of a particular hardware design, esp. tricks for speed and space optimization that rely on crocks such as overlapping instructions (or, as in the famous case described in The Story of Mel, a Real Programmer, interleaving of opcodes on a magnetic drum to minimize fetch delays due to the device's rotational latency). This sort of thing has become less common as the relative costs of programming time and machine resources have changed, but is still found in heavily constrained environments such as industrial embedded systems, and in the code of hackers who just can't let go of that low-level control. See Real Programmer. In the world of personal computing, bare metal programming (especially in sense 1 but sometimes also in sense is often considered a Good Thing, or at least a necessary evil (because these machines have often been sufficiently slow and poorly designed to make it necessary; see ill-behaved). There, the term usually refers to bypassing the BIOS or OS interface and writing the application to directly access device registers and machine addresses. “To get 19. 2 kilobaud on the serial port, you need to get down to the bare metal. ” People who can do this sort of thing well are held in high regard.

-Baroque

adj. Feature-encrusted; complex; gaudy; verging on excessive. Said of hardware or (esp.) software designs, this has many of the connotations of elephantine or monstrosity but is less extreme and not pejorative in itself. “Metafont even has features to introduce random variations to its letterform output. Now *that* is baroque!” See also rococo.

Base

1. In the numeration system commonly used in scientific papers, the number that is raised to the power denoted by the exponent and then multiplied by the coefficient to determine the real number represented, for example, the number 6. 25 in the expression 2. 7 ´ 6. 251. 5 = 42. 1875.
2. A reference value. (FP)
3. A number that is multiplied by itself as many times as indicated by an exponent. (FP)

Base Address

1. An address that is used as the origin in the calculation of addresses in the execution of a computer program. (FP) (ISO)
2. A given address from which an absolute address is derived by combination with a relative address. (FP)

Base C4 Systems Security Office

Office charged with the responsibility for managing and executing the C4 systems security program for a base or wing. The office reports to the MAJCOM C4 Systems Security Office and provides security guidance to Organization C4 Systems Security Offices or appropriate unit officials (COMSEC Managers, Computer Security Officers (CSOs), Network Security Officers (NSOs), ETAP Managers, TEMPEST users).

Base Computer Systems Security Officer

(BCSSO) Term no longer used. Prior to the Base C4 Systems Security Office, this was the individual charged with the responsibility for managing and executing the computer security program for a base or wing.

Baseband

1. The spectral band occupied by an unmodulated signal. (~) Note: Baseband transmission is usually characterized by being much lower in frequency than the signal that results if the baseband signal is used to modulate a carrier or subcarrier.
2. In facsimile, the frequency of a signal equal in width to that between zero frequency and maximum keying frequency. (~) See also baseband signaling, carrier (cxr), frequency, modulation, multiplex baseband, multiplexing.

Baseline

-BASIC

n. [acronymBeginner's All-purpose Symbolic Instruction Code] A programming language, originally designed for Dartmouth's experimental timesharing system in the early 1960s, which has since become the leading cause of brain-damage in proto-hackers. Edsger Dijkstra observed in “Selected Writings on Computing A Personal Perspective” that “It is practically impossible to teach good programming style to students that have had prior exposure to BASIC as po-

tential programmers they are mentally mutilated beyond hope of regeneration. ”

Basic Software

Routines and programs designed to extend or (Non-functional) facilitate the use of particular automated equipment. As a rule, the vendor provides basic software. It is usually essential for the system operation. Examples of basic software are executive and operating systems, diagnostic programs, compilers, assemblers, utility routines such as sort-merge and input or output conversion routines, file management programs, and data management programs. Data management programs are commonly linked to or under the control of the executive or operating system programs. (*AFR* 205-16;)

Basic Software (nonfunctional)

Routines and programs designed to extend or facilitate the use of particular automated equipment As a rule, the vendor provides basic software. It is usually essential for the system operation. Examples of bask software are executive and operating systems, diagnostic programs, compilers, assemblers, utility routines (such as sort-merge and input or output conversion routines), file management programs, and data management programs. (*AFR* 205-16)

Basic Status

In data transmission, a secondary station's capability to send or receive a frame containing an information field.

#-Basic/Generic Management Issues#

This KSA has no definition.

-Batch

1. adj. Non-interactive. Hackers use this somewhat more loosely than the traditional technical definitions justify; in particular, switches on a normally interactive program that prepare it to receive non-interactive command input are often referred to as `batch mode' switches. A `batch file' is a series of instructions written to be handed to an interactive program running in batch mode.

2. Performance of dreary tasks all at one sitting. “I finally sat down in batch mode and wrote out checks for all those bills; I guess they'll turn the electricity back on next week. ”
3. `batching up' Accumulation of a number of small tasks that can be lumped together for greater efficiency. “I'm batching up those letters to send sometime” “I'm batching up bottles to take to the recycling center. ”

Batch Processing

1. The processing of data or the accomplishment of jobs accumulated in advance in such a manner that the user cannot further influence the processing while it is in progress. (FP) (ISO) (~)
2. The processing of data accumulated over a period of time. (FP)
3. Loosely, the execution of computer programs serially. (FP)
4. Pertaining to the technique of executing a set of computer programs such that each is completed before the next program of the set is started. (FP)
5. Pertaining to the sequential input of computer programs or data. (FP)

See also background processing, remote batch processing.

Baterium

-Bathtub Curve

n. Common term for the curve (resembling an end-to-end section of one of those claw-footed antique bathtubs) that describes the expected failure rate of electronics with time initially high, dropping to near 0 for most of the system's lifetime, then rising again as it `tires out'. See also burn-in period, infant mortality.

Baud

1. A unit of modulation rate. One baud corresponds to a rate of one unit interval per second, where the modulation rate is expressed as the reciprocal of the duration in seconds of the shortest unit interval.
2. A unit of signaling speed equal to the number of discrete signal conditions, variations, or events per second. (~) Note: If the duration of the unit interval is 20 milliseconds, the signaling speed is 50 baud. If the signal transmitted during each unit interval can take on any one of M discrete states, the bit rate is equal to the rate in baud times log2M. The technique used to encode the allowable signal states may be any combination of amplitude, frequency, or phase modulation, but it cannot use a further time-division multiplexing technique to subdivide the unit intervals into multiple subintervals. In some signaling systems, non-information-carrying signals may be inserted to facilitate synchronization; e. g. , in certain forms of binary modulation coding, there is a forced inversion of the signal state at the center of the bit interval. In these cases, the synchronization signals are included in the calculation of the rate in baud but not in the computation of bit rate. See also bit rate, data signaling rate, unit interval.

Baud Rate

A measurement of the signaling speed of a data transmission device. A baud rate is equivalent to the maximum number of signaling elements, or symbols, per second that are generated.

Baudot Code

A synchronous code for the transmission of data, developed about ~0, in which five equal-length bits

represent one character. (~) Note 1: Baudot code has been replaced by the start-stop asynchronous International Alphabet No. 2 (IA No.

2. . Note 2: IA No. 2 should not be identified as “Baudot code. ” See also code.

-Bboard

1. /bee'bord/ n. [contraction of `bulletin board'] Any electronic bulletin board; esp. used of BBS systems running on personal micros, less frequently of a Usenet newsgroup (in fact, use of this term for a newsgroup generally marks one either as a newbie fresh in from the BBS world or as a real oldtimer predating Usenet).
2. At CMU and other colleges with similar facilities, refers to campus-wide electronic bulletin boards.
3. The term `physical bboard' is sometimes used to refer to an old-fashioned, non-electronic cork-and-thumbtack memo board. At CMU, it refers to a particular one outside the CS Lounge. In either of senses 1 or 2, the term is usually prefixed by the name of the intended board (`the Moonlight Casino bboard' or `market bboard'); however, if the context is clear, the better-read bboards may be referred to by name alone, as in (at CMU) “Don't post for-sale ads on general”.

BBS

/B-B-S/ n. [abbreviation, `Bulletin Board System'] An electronic bulletin board system; that is, a message database where people can log in and leave broadcast messages for others grouped (typically) into topic groups. Thousands of local BBS systems are in operation throughout the U. S. , typically run by amateurs for fun out of their homes on MS-DOS boxes with a single modem line each. Fans of Usenet and Internet or the big commercial timesharing bboards such as CompuServe and GEnie tend to consider local BBSes the low-rent district of the hacker culture, but they serve a valuable function by knitting together lots of hackers and users in the personal-micro world who would otherwise be unable to exchange code at all. See also bboard.

-Beam

vt. [from Star Trek Classic's “Beam me up, Scotty!”] To transfer softcopy of a file electronically; most often in combining forms such as `beam me a copy' or `beam that over to his site'. Compare blast, snarf, BLT.

-Beanie Key

n. [Mac users] See command key.

Bearer Channel

See B channel.

Bearer Service

In ISDN applications, a telecommunications service allowing transmission of user-information signals between user-network interfaces. See also interface.

-Beep

n. ,v. Syn. feep. This term seems to be preferred among micro hobbyists.

Bell-La Padula

Formal-state transition model of a security model computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations.

Bell-La Padula Security Model

Formal-state transition model of computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations. See Formal Security Policy Model, Simple Security Property, and Star Property (*-property).

Bell-LaPadula Model

A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined, and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving that the system is secure. A system state is defined as to “secure” if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. See *-PROPERTY and SIMPLE SECURITY PROPERTY. (*DOD* 5200. 28-STD)

-Bells And Whistles

n. [by analogy with the toyboxes on theater organs] Features added to a program or system to make it more flavorful from a hacker's point of view, without necessarily adding to its utility for its primary function. Distinguished from chrome, which is intended to attract users. “Now that we've got the basic program working, let's go back and add some bells and whistles. ” No one seems to know what distinguishes a bell from a whistle.

Benign

Condition of cryptographic data such that it cannot be compromised by human access to the data. NOTE: The term benign may be used to modify a variety of COMSEC-related terms, (e. g. , key, data, storage, fill, and key distribution techniques).

Benign Environment

1. A nonhostile envelope protected from external hostile elements by physical, personnel, and pro-

cedural security countermeasures. In this environment, the ADP system is protected at the system's highest level. All users are cleared for the highest level but a need-to-know is not required for all data. Reliance is placed on the ADP system for routing and need-to-know separation of data. (*AR* 380-380)

2. A nonhostile environment protected from external hostile elements by physical, personnel, and procedural security countermeasures. (*NCSC-WA*-001-85;)

-Beta

/bay't*/, /be't*/ or (Commonwealth) /bee't*/ n.

1. Mostly working, but still under test; usu. used with `in' `in beta'. In the Real World, systems (hardware or software) software often go through two stages of release testing Alpha (in-house) and Beta (outhouse?). Beta releases are generally made to a small number of lucky (or unlucky), trusted customers.
2. Anything that is new and experimental.
3. Flaky; dubious; suspect (since beta software is notoriously buggy). Historical note More formally, to beta-test is to test a pre-release (potentially unreliable) version of a piece of software by making it available to selected customers and users. This term derives from early 1960s terminology for product cycle checkpoints, first used at IBM but later standard throughout the industry. `Alpha Test' was the unit, module, or component test phase; `Beta Test' was initial system test. These themselves came from earlier A- and B-tests for hardware. The A-test was a feasibility and manufacturability evaluation done before any commitment to design and development. The B-test was a demonstration that the engineering model functioned as specified. The C-test (corresponding to today's beta) was the B-test performed on early samples of the production design.

Between-The-Lines Entry

1. Access obtained through active wiretapping by an unauthorized user to a momentarily inactive terminal of a legitimate user assigned to a communications channel. (*AR* 380-380; *FIPS PUB* 39)
2. Unauthorized access obtained by tapping the temporarily inactive terminal of a legitimate use. See PIGGYBACK. (*NCSC-TG*-004-88)

Beyond A1

A level of trust defined by the DoD Trusted Computer System Evaluation Criteria that is beyond the current state-of-the-art technology. It includes all the A1 level features plus features not required at the A1 level. These additional features may vary from system-to-system. This term is often used to describe capabilities not yet available, specifically, code verification. (*NCSC-WA*-001-85;).

Bi-Sync

Abbreviation for binary synchronous communication.

-Bible

1. n. One of a small number of fundamental source books such as Knuth and K&R.
2. The most detailed and authoritative reference for a particular language, operating system, or other complex software system.

-BiCapitalization

n. The act said to have been performed on trademarks (such as PostScript, NeXT, NeWS, VisiCalc, FrameMaker, TK!solver, EasyWriter) that have been raised above the ruck of common coinage by nonstandard capitalization. Too many marketroid types think this sort of thing is really cute, even the 2,317th time they do it. Compare studlycaps.

-Biff

/bif/ vt. To notify someone of incoming mail. From the BSD utility `biff(1)', which was in turn named after a friendly golden Labrador who used to chase frisbees in the halls at UCB while 4. 2BSD was in development. There was a legend that it had a habit of barking whenever the mailman came, but the author of `biff' says this is not true. No relation to B1FF.

-Big Gray Wall

n. What faces a VMS user searching for documentation. A full VMS kit comes on a pallet, the documentation taking up around 15 feet of shelf space before the addition of layered products such as compilers, databases, multivendor networking, and programming tools. Recent (since VMS version 5) DEC documentation comes with gray binders; under VMS version 4 the binders were orange (`big orange wall'), and under version 3 they were blue. See VMS. Often contracted to `Gray Wall'.

-Big Iron

n. Large, expensive, ultra-fast computers. Used generally of number-crunching supercomputers such as Crays, but can include more conventional big commercial IBMish mainframes. Term of approval; compare heavy metal, oppose dinosaur.

-Big Red Switch

n. [IBM] The power switch on a computer, esp. the `Emergency Pull' switch on an IBM mainframe or the power switch on an IBM PC where it really is large and red. “This !@%$% bitty box is hung again; time to hit the Big Red Switch. ” Sources at IBM report that, in tune with the company's passion for TLAs, this is often abbreviated as `BRS' (this has also become established on FidoNet and in the PC clone world). It is alleged that the emergency pull switch on an IBM 360/91 actually fired a non-conducting bolt into the main power feed; the BRSes on more recent

mainframes physically drop a block into place so that they can't be pushed back in. People get fired for pulling them, especially inappropriately (see also molly-guard). Compare power cycle, three-finger salute, 120 reset; see also scram switch.

-Big Room, The

n. The extremely large room with the blue ceiling and intensely bright light (during the day) or black ceiling with lots of tiny night-lights (during the night) found outside all computer installations. “He can't come to the phone right now, he's somewhere out in the Big Room. ”

-Big Win

n. Serendipity. “Yes, those two physicists discovered high-temperature superconductivity in a batch of ceramic that had been prepared incorrectly according to their experimental schedule. Small mistake; big win!” See win big.

-Big-Endian

adj. [From Swift's “Gulliver's Travels” via the famous paper “On Holy Wars and a Plea for Peace” by Danny Cohen, USC/ISI IEN 137, dated April 1, 1980]

1. Describes a computer architecture in which, within a given multi-byte numeric representation, the most significant byte has the lowest address (the word is stored `big-end-first'). Most processors, including the IBM 370 family, the PDP-10, the Motorola microprocessor families, and most of the various RISC designs current in mid-1993, are big-endian. See little-endian, middle-endian, NUXI problem, swab.
2. An Internet address the wrong way round. Most of the world follows the Internet standard and writes email addresses starting with the name of the computer and ending up with the name of the country. In the U. K. the Joint Networking Team had decided to do it the other way round before the Internet domain standard was established; e. g. , me@uk. ac. wigan. cs. Most gateway sites have ad-hockery in their mailers to handle this, but can still be confused. In particular, the address above could be in the U. K. (domain uk) or the domain cs (formerly, Czechoslovakia).

-Bignum

/big'nuhm/ n. [orig. from MIT MacLISP] [techspeak]

1. A multiple-precision computer representation for very large integers.
2. More generally, any very large number. “Have you ever looked at the United States Budget? There's bignums for you!”
3. [Stanford] In backgammon, large numbers on the dice especially a roll of double fives or double sixes (compare moby, sense 4). See also El Camino Bignum. Sense 1 may require some explanation. Most computer languages provide a kind of data called `integer', but such computer integers are usually very limited in size; usually they must be smaller than than 2^(31) (2,147,483,648) or (on a bitty box) 2^(15) (32,768). If you want to work with numbers larger than that, you have to use floating-point numbers, which are usually accurate to only six or seven decimal places. Computer languages that provide bignums can perform exact calculations on very large numbers, such as 1000! (the factorial of 1000, which is 1000 times 999 times 998 times . times 2 times 1). For example, this value for 1000! was computed by the MacLISP system using bignums

402387260077093773543702433923003985719374864210714632543799104299385123986290205920442084869694048004799886101971960586316668729948085589013238296699445909974245040870737599~23627727~73251977950595099527612087497546249704360141827809464649629102056393887437886487337119181045825783647849977012476328898359557354325131853239584630755574091142624174743493475534286465766116677973966688202912073791438537195882498081268678383745597317461360853795341524221586593201928090878297308431392844403281231558611036976801357304216168747609675871348312025478589320767169132448426236131412508780208000261683151027341827977704784635868170164365024153691398281264810213092761244896359928705114964975419909342221566832572080821333186116811553615836546984046708975 602900950537616475847728425~967964624494516076535340819890138544248798495995331910172335555660213941503997362807501378376153071277619268490343526252000158885351473316117021039681759215109077880193931781141945452572238655414610628921879602238389714760885062768629671466746975629112340824392081601537808898939645182632436716167621791689097799119037540312746222899880051954444142820121873617459926429565817466283029555702990243241531816172104658320367890611726015878352075151628422554026517048330422613974286933061690897968482590125458327168226458066526769958652682272807075781391858178889652208164348344825993266043367660176999612831860788386150279460595513115655203609398818061213855860030143569452724206344631797460594682573103790084024432438465651

7 24501440282~525247093519062092902313649327349756
5513958720559654228749774011413346962715422845862
3
7738753823048386568897646192738381490014076731044
6 6402598994902222217659043399 0~601856652648506179
97023561938970178600408 1~97299183110211712298459
0164192106888438712185564612496079872290851929681
9
3723886426148396573822911231250241866493531439701
3
7428531926649875337218940694281434118520158014123
3
4482801505139969429015348307764456909907315243327
8
2882698646027898643211390835062170950025973898635
5
4277196742822248757586765752344220207573630569498
8
2508796892816275384886339690995982628095612145099
4
8717012445164612603790293091208890869420285106401
8
2154399457156805941872748998094254742173582401063
6
7740459574178516082923013535808184009699637252423
0
5608559037006242712434169090041536901059339838357
7
7939410970027753472000000000000000000000000000000
0
0000000000000000000000000000000000000000000000000
0
0000000000000000000000000000000000000000000000000
0
0000000000000000000000000000000000000000000000000
0
0000000000000000000000000000000000000000000000000
0 000000000000000000.

-Bigot

n. A person who is religiously attached to a particular computer, language, operating system, editor, or other tool (see religious issues). Usually found with a specifier; thus, `cray bigot', `ITS bigot', `APL bigot', `VMS bigot', `Berkeley bigot'. Real bigots can be distiguished from mere partisans or zealots by the fact that they refuse to learn alternatives even when the march of time and/or technology is threatening to obsolete the favored tool. It is truly said “You can tell a bigot, but you can't tell him much. ” Compare weenie.

Binary

1. Pertaining to a selection, choice, or condition that has two possible different values or states. (FP) (ISO)
2. Pertaining to a fixed radix numeration system that has a radix of two. (FP) (ISO)

Binary Code

A code composed by selection and configuration of an entity that can assume either one of two possible states. (~) See also binary digit, code.

Binary Digit

1. A character used to represent one of the two digits in the numeration system with a base of two, each digit representing one of two, and only two, possible states of a physical entity or system.
2. In binary notation either of the characters 0 or 1. (FP) (ISO) (~)
3. A unit of information equal to one binary decision or the designation of one of two possible and equally likely states of anything used to store or convey information. (~) See also byte, code element, digital signal, octet alignment.

Binary Element

A constituent element of data that takes either of two values or states. (FP) (ISO)

Binary Exponential Backoff

See truncated binary exponential backoff.

Binary Notation

1. Any notation that uses two different characters, usually the binary digits 0 and 1. (After FP) (After ISO) Note: Data encoded in binary notation need not be in the form of a pure binary numeration sytem; e. g. , Gray code. Synonym pure binary numeration system.
2. A scheme for representing numbers characterized by the arrangements of digits in sequence, with the understanding that successive digits are interpreted as coefficients of successive powers of base (~)

See also binary coded decimal, binary digit, code, Gray code.

Binary Synchronous Communication

A character-oriented, data-link-layer protocol. Note: The bi-sync protocol is being phased out of most computer communication networks in favor of bit-oriented protocols such as SDLC, HDLC, and ADCCP. See also Advanced Data Communications Control Procedure, high-level data link control, synchronous data link control.

Binary-Coded Decimal

A numbering system wherein each digit of a given decimal number is represented separately by a unique arrangement of binary digits (usually four). (~) Note: BCD sometimes refers only to the 4-bit representation of the decimal digits 0 through 9.
See also binary digit, binary notation, code.

Binary-Coded Decimal Code

Synonym binary-coded decimal notation.

Binary-Coded Decimal Interchange Code

See binary-coded decimal notation.

Binary-Coded Decimal Notation

A binary notation in which each of the decimal digits is represented by a binary numeral. (After FP) (After ISO) Synonyms binary-coded decimal code, binary-coded decimal representation.

Binary-Coded Decimal Representation

Synonym binary-coded decimal notation.

Binding

Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.

#-Binding/Handshaking#

1. Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information. (NSTISSI 4009)
2. A cryptographic checkword used to detect whether an element of data or set of data has been altered. (EKMS 004. 01);
3. an effectiveness criterion in ITSEC. Although security functions may be suitable for their individual purposes it is possible that certain combinations of functions or mechanisms may interfere or conflict with each other. In evaluating the binding of functionality a study is undertaken of the interrelationships of security functions and mechanisms, to ensure that they are mutually supportive and provide an effective and integrated whole (handshaking). (ISDCST+LSC-92).

Biometric

The use of specific quantities that reflect unique personal characteristics (such as a fingerprint, an eye blood vessel print, or a voice print) to validate the identity of users. (WB;)

#-Biometrics#

In access control, automated methods of verifying or recognizing a person based upon a physical or behavioral characteristics. Biometric techniques may be classified on the basis of some passive attribute of an individual, e. g. , an eye retina pattern, or some unique manner in which an individual performs a task, e. g. , writing a signature. (Source: IS dictionary).

Bit

n. [from the mainstream meaning and `Binary digIT'] [techspeak]

1. The unit of information; the amount of information obtained by asking a yes-or-no question for which the two outcomes are equally probable.
2. [techspeak] A computational quantity that can take on one of two values, such as true and false or 0 and 1.
3. A mental flag a reminder that something should be done eventually. (Meaning “I think you were the last guy to hack on EMACS, and what I am about to say is predicated on this, so please stop me if this isn't true. ”) “I just need one bit from you” is a polite way of indicating that you intend only a short interruption for a question that can presumably be answered yes or no. A bit is said to be `set' if its value is true or 1, and `reset' or `clear' if its value is false or 0. One speaks of setting and clearing bits. To toggle or `invert' a bit is to change it, either from 0 to 1 or from 1 to 0. See also flag, trit, mode bit.
4. The term `bit' first appeared in print in the computer-science sense in 1949, and seems to have been coined by early computer scientist John Tukey. Tukey records that it evolved over a lunch table as a handier alternative to `bigit' or `binit'.

-Bit Bang

n. Transmission of data on a serial line, when accomplished by rapidly tweaking a single output bit, in software, at the appropriate times. The technique is a simple loop with eight OUT and SHIFT instruction pairs for each byte. Input is more interesting. And full duplex (doing input and output at the same time) is one way to separate the real hackers from the wannabees. Bit bang was used on certain early models of Prime computers, presumably when UARTs were too expensive, and on archaic Z80 micros with a Zilog PIO but no SIO. In an interesting instance of the cycle of reincarnation, this technique is now (1991) coming back into use on some RISC architectures because it consumes such an infinitesimal part of the processor that it actually makes sense not to have a UART.

-Bit Bashing

n. (alt. `bit diddling' or bit twiddling) Term used to describe any of several kinds of low-level programming characterized by manipulation of bit, flag, nybble, and other smaller-than-character-sized pieces of data; these include low-level device control, encryption algorithms, checksum and error-correcting codes, hash functions, some flavors of graphics programming (see bitblt), and assembler/compiler code generation. May connote either tedium or a real technical challenge (more usually the former). “The command decoding for the new tape driver looks pretty solid but the bit-bashing for the control registers still has bugs. ” See also bit bang, mode bit.

-Bit Bucket

1. n. The universal data sink (originally, the mythical receptacle used to catch bits when they fall off the end of a register during a shift instruction). Discarded, lost, or destroyed data is said to have `gone to the bit bucket'. On UNIX, often used for /dev/null. Sometimes amplified as `the Great Bit Bucket in the Sky'.
2. The place where all lost mail and news messages eventually go. The selection is performed according to Finagle's Law; important mail is much more likely to end up in the bit bucket than junk mail, which has an almost 100% probability of getting delivered. Routing to the bit bucket is automati-

cally performed by mail-transfer agents, news systems, and the lower layers of the network.

3. The ideal location for all unwanted mail responses "Flames about this article to the bit bucket. " Such a request is guaranteed to overflow one's mailbox with flames.
4. Excuse for all mail that has not been sent. "I mailed you those figures last week; they must have landed in the bit bucket. " Compare black hole. This term is used purely in jest. It is based on the fanciful notion that bits are objects that are not destroyed but only misplaced.
5. This appears to have been a mutation of an earlier term `bit box', about which the same legend was current; old-time hackers also report that trainees used to be told that when the CPU stored bits into memory it was actually pulling them `out of the bit box'. See also chad box.
6. Another variant of this legend has it that, as a consequence of the `parity preservation law', the number of 1 bits that go to the bit bucket must equal the number of 0 bits. Any imbalance results in bits filling up the bit bucket. A qualified computer technician can empty a full bit bucket as part of scheduled maintenance.

Bit Configuration

The order for encoding the bits of information that define a character. (FP) (ISO) See also binary digit.

-Bit Decay

n. See bit rot. People with a physics background tend to prefer this variant for the analogy with particle decay. See also computron, quantum bogodynamics.

Bit Density

1. A measure of the number of bits recorded per unit of length or area. (FP) (ISO) Synonym recording density.
2. The spacing along a magnetic medium of the bits that represent information. (FP) (ISO)

Bit Error Rate

Ratio between the number of bits incorrectly received and the total number of bits transmitted in a telecommunications system.

Bit Error Ratio

The number of erroneous bits divided by the total number of bits transmitted, received, or processed over some stipulated period of time. (~) Note: Two examples of bit error ratio are: (a) transmission BER--the number of erroneous bits received divided by the total number of bits transmitted; and (b) information BER--the number of erroneous decoded (corrected) bits divided by the total number of decoded (corrected) bits. The BER is usually expressed as a number and a power of 10; e. g. , 2. 5 erroneous bits out of 100,000 bits transmitted would be 2. 5 in 105 or 2. 5 ´ 10-5. See also binary digit, character-count and bit-count integrity, error, error budget, error burst, error control, error ratio, undetected error ratio.

Bit Error Ratio Tester

A testing device that compares a received data pattern with a known transmitted pattern to determine the level of transmission quality.

Bit Interval

See binary digit, character interval, unit interval.

Bit Inversion

The changing of the state of a bit to the opposite state. (~) See also character-count and bit-count integrity.

Bit Pairing

The practice of establishing, within a code set, a number of subsets that have an identical bit representation except for the state of a specified bit. (~) Note: In the International Alphabet No. 5 and the American Standard Code for Information Interchange (ASCII), the upper case letters are related to their respective lower case letters by the state of bit six. See also ASCII, binary digit.

Bit Position

A character position in a word in a binary notation. (FP) (ISO)

Bit Rate

In a bit stream, the number of bits occurring per unit time, usually expressed as bits per second. (~) Note: For M-ary operation, the bit rate is equal to log2M times the rate (in baud), where M is the number of significant conditions in the signal. See also baud, binary digit, bits per second, data signaling rate, modulation rate, multiplex aggregate bit rate.

Bit Robbing

The use of the least significant bit in a time slot or channel for conveying voice-related signaling or supervisory information.

-Bit Rot

n. Also bit decay. Hypothetical disease the existence of which has been deduced from the observation that unused programs or features will often stop working after sufficient time has passed, even if `nothing has changed'. The theory explains that bits decay as if they were radioactive. As time passes, the contents of a file or the code in a program will become increasingly garbled. There actually are physical processes that produce such effects (alpha particles generated by trace radionuclides in ceramic chip packages, for example, can change the contents of a computer memory unpredictably, and various kinds of subtle media failures can corrupt files in mass storage), but they are quite rare (and computers are built with error-detecting circuitry to compensate for them). The notion long favored among hackers that cosmic rays

are among the causes of such events turns out to be a myth; see the cosmic rays entry for details. The term software rot is almost synonymous. Software rot is the effect, bit rot the notional cause.

Bit Slip

The insertion or deletion of bits by a device to accommodate accumulated variations in the clock reference of the received waveform vs. the clock of the device. (~) See also binary digit, character-count and bit-count integrity, clock, error.

Bit Stream Transmission

The transmission of characters at fixed time intervals without stop and start elements. Note: The bits that make up the characters follow each other in sequence without interruption. See also binary digit, bit-sequence independence, data stream.

Bit String

A delimited sequence of bits. See also binary digit, byte, packet, word.

Bit Synchronization

The process whereby the decision time is brought into alignment with the received bit (or basic signaling element). (~) See also binary digit, decision instant, frame synchronization, synchronization, synchronization bit.

-Bit Twiddling

1. n. (pejorative) An exercise in tuning (see tune) in which incredible amounts of time and effort go to produce little noticeable improvement, often with the result that the code becomes incomprehensible.
2. Aimless small modification to a program, esp. for some pointless goal.
3. Approx. syn. for bit bashing; esp. used for the act of frobbing the device control register of a peripheral in an attempt to get it back to a known state.

Bit-By-Bit Asynchronous Operation

A mode of operation in which manual, semiautomatic, or automatic shifts in the data modulation rate are accomplished by gating or slewing the clock modulation rate. (~) Note: The equipment may, for example, be operated at 50 bps one moment and at 1200 bps the next moment. See also synchronous transmission.

Bit-Count Integrity

See character-count and bit-count integrity.

-Bit-Paired Keyboard

n. obs. (alt. `bit-shift keyboard') A non-standard keyboard layout that seems to have originated with the Teletype ASR-33 and remained common for several years on early computer equipment. The ASR-33 was a mechanical device (see EOU), so the only way to generate the character codes from keystrokes was by some physical linkage. The design of the ASR-33 assigned each character key a basic pattern that could be modified by flipping bits if the SHIFT or the CTRL key was pressed. In order to avoid making the thing more of a Rube Goldberg kluge than it already was, the design had to group characters that shared the same basic bit pattern on one key. Looking at the ASCII chart, we find high low bits bits 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 010 ! “ # $ % & ' () 011 0 1 2 3 4 5 6 7 8 9 This is why the characters !”#$%&'() appear where they do on a Teletype (thankfully, they didn't use shift-0 for space). This was *not* the weirdest variant of the QWERTY layout widely seen, by the way; that prize should probably go to one of several (differing) arrangements on IBM's even clunkier 026 and 029 card punches. When electronic terminals became popular, in the early 1970s, there was no agreement in the industry over how the keyboards should be laid out. Some vendors opted to emulate the Teletype keyboard, while others used the flexibility of electronic circuitry to make their product look like an office typewriter. These alternatives became known as `bit-paired' and `typewriter-paired' keyboards. To a hacker, the bit-paired keyboard seemed far more logical -- and because most hackers in those days had never learned to touch-type, there was little pressure from the pioneering users to adapt keyboards to the typewriter standard. The doom of the bit-paired keyboard was the large-scale introduction of the computer terminal into the normal office environment, where out-and-out technophobes were expected to use the equipment. The `typewriter-paired' standard became universal, `bit-paired' hardware was quickly junked or relegated to dusty corners, and both terms passed into disuse.

Bit-Sequence Independence

A characteristic of some digital data transmission systems that impose no restrictions on, or modification of, the transmitted bit sequence. Note: This is in contrast to some protocols that reserve certain bit sequences for special meaning, e. g. , the Flag sequence, 01111110, for HDLC, SDLC, and ADCCP protocols. See also binary digit, bit stream transmission.

Bit-Stepped

Control of digital equipment in which its operation is incremented one step at a time at the applicable bit rate. (~) See also character stepped.

Bit-Synchronous Operation

A mode of operation in which data circuit-terminating equipment, data terminal equipment, and transmitting circuits are all operated synchronously with a clock. (~)

1. Note 1: Clock timing is delivered at twice the modulation rate, and one bit is transmitted or received during each clock cycle.
2. Note 2: Bit-synchronous operation is sometimes erroneously referred to as “digital synchronization. ” See also binary digit, clock, data circuit-terminating equipment, data terminal equipment, synchronization, terminal.

-Bitblt

1. /bit'blit/ n. [from BLT, q. v.] Any of a family of closely related algorithms for moving and copying rectangles of bits between main and display memory on a bit-mapped device, or between two areas of either main or display memory (the requirement to do the Right Thing in the case of overlapping source and destination rectangles is what makes BitBlt tricky).
2. Synonym for blit or BLT. Both uses are borderline techspeak.

-BITNET

/bit'net/ n. [acronym Because It's Time NETwork] Everybody's least favorite piece of the network (see network, the). The BITNET hosts are a collection of IBM and VAX (the latter with comm hardware) that communicate using 80-character EBCDIC card images (see eighty-column mind); thus, they tend to mangle the headers and text of third-party traffic from the rest of the ASCII/RFC-822 world with annoying regularity. BITNET was also notorious as theapparent home of B1FF.

-Bits

1. n. pl. Information. Examples “I need some bits about file formats. ” (“I need to know about file formats. ”) Compare core dump, sense 2.
2. Machine-readable representation of a document, specifically as contrasted with paper”I have only a photocopy of the Jargon File; does anyone know where I can get the bits?”. See softcopy, source of all good bits See also bit.

Bits Per Inch

The density of data, expressed in binary digits per inch of a storage medium.

Bits Per Second

(BPS) Basic unit of measure for data transmission capacity; usually expressed as Kbps for thousands (kilo) of bits per second, Mbps for millions of bits per second, Gbps for billions (giga) of bits per second.

-Bixie

/bik'see/ n. Variant emoticons used on BIX (the Byte Information eXchange). The smiley bixie is <@_@>, apparently intending to represent two cartoon eyes and a mouth. A few others have been reported.

BLACK

1. Refers to unclassified information or equipment and wire lines that handle encrypted classified information. (*AFR* 205-16;);
2. Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, and equipment, in which only unclassified signals are processed. NOTE: Encrypted signals are unclassified.

-Black Art

n. A collection of arcane, unpublished, and (by implication) mostly ad-hoc techniques developed for a particular application or systems area (compare black magic). VLSI design and compiler code optimization were (in their beginnings) considered classic examples of black art; as theory developed they became deep magic, and once standard textbooks had been written, became merely heavy wizardry. The huge proliferation of formal and informal channels for spreading around new computer-related technologies during the last twenty years has made both the term `black art' and what it describes less common than formerly. See also voodoo programming.

BLACK Equipment Area (BEA)

A BLACK equipment area is located in a limited exclusion area. (NACSIM 5203)

-Black Hole

n. What a piece of email or netnews has fallen into if it disappears mysteriously between its origin and destination sites (that is, without returning a bounce message). “I think there's a black hole at foovax!” conveys suspicion that site foovax has been dropping a lot of stuff on the floor lately (see drop on the floor). The implied metaphor of email as interstellar travel is interesting in itself. Compare bit bucket.

Black Key

Encrypted key. See RED Key.

BLACK Line

Any line external to classified information-processing equipment, including power lines, which does not intentionally carry classified signals.

BLACK Signal

Any signal (e. g. , control signal or enciphered signal) which would not divulge classified information if recovered and analyzed.

Blanking

[In graphic display,] The suppression of the display of one or more display elements or display segments. (FP) (ISO)

-Blast

1. vt. ,n. Synonym for BLT, used esp. for large data sends over a network or comm line. Opposite of snarf. Usage uncommon. The variant `blat' has been reported.

2. vt. [HP/Apollo] Synonymous with nuke (sense 3). Sometimes the message `Unable to kill all processes. Blast them (y/n)?' would appear in the command window upon logout.

-Blink

v. ,n. To use a navigator or off-line message reader to minimize time spent on-line to a commercial network service. As of late 1994, this term was said to be in wide use in the U. K. , but is rare or unknown in the US.

-Blinkenlights

/blink'*n-li:tz/ n. Front-panel diagnostic lights on a computer, esp. a dinosaur. Derives from the last word of the famous blackletter-Gothic sign in mangled pseudo-German that once graced about half the computer rooms in the English-speaking world. One version ran in its entirety as follows ACHTUNG! ALLES LOOKENSPEEPERS! Das computermachine ist nicht fuer gefingerpoken und mittengrabben. Ist easy schnappen der springenwerk, blowenfusen und poppencorken mit spitzensparken. Ist nicht fuer gewerken bei das dumpkopfen. Das rubbernecken sichtseeren keepen das cotten-pickenen hans in das pockets muss; relaxen und watchen das blinkenlichten. This silliness dates back at least as far as 1959 at Stanford University and had already gone international by the early 1960s, when it was reported at London University's ATLAS computing site. There are several variants of it in circulation, some of which actually do end with the word `blinkenlights'. In an amusing example of turnabout-is-fair-play, German hackers have developed their own versions of the blinkenlights poster in fractured English, one of which is reproduced here ATTENTION This room is fullfilled mit special electronische equippment. Fingergrabbing and pressing the cnoeppkes from the computers is allowed for die experts only! So all the "lefthanders" stay away and do not disturben the brainstorming von here working intelligencies. Otherwise you will be out thrown and kicked anderswhere! Also please keep still and only watchen astaunished the blinkenlights. See also geef. Old-time hackers sometimes get nostalgic for blinkenlights because they were so much more fun to look at than a blank panel. Sadly, very few computers still have them (the three LEDs on a PC keyboard certainly don't count). The obvious reasons (cost of wiring, cost of front-panel cutouts, almost nobody needs or wants to interpret machine-register states on the fly anymore) are only part of the story. Another part of it is that radio-frequency leakage from the lamp wiring was beginning to be a problem as far back as transistor machines. But the most fundamental fact is that there are very few signals slow enough to blink an LED these days! With slow CPUs, you could watch the bus register or instruction counter tick, but at 33/66/150MHz it's all a blur.

Blinking

An intentional periodic change in the intensity of one or more display elements or display segments. (FP) (ISO)

-Blit

1. /blit/ vt. To copy a large array of bits from one part of a computer's memory to another part, particularly when the memory is being used to determine what is shown on a display screen. "The storage allocator picks through the table and copies the good parts up into high memory, and then blits it all back down again. " See bitblt, BLT, dd, cat, blast, snarf. More generally, to perform some operation (such as toggling) on a large array of bits while moving them.
2. Sometimes all-capitalized as `BLIT' an early experimental bit-mapped terminal designed by Rob Pike at Bell Labs, later commercialized as the AT&T 5620. (The folk etymology from `Bell Labs Intelligent Terminal' is incorrect. Its creators liked to claim that "Blit" stood for the Bacon, Lettuce, and Interactive Tomato.)

-Blitter

/blit'r/ n. A special-purpose chip or hardware system built to perform blit operations, esp. used for fast implementation of bit-mapped graphics. The Commodore Amiga and a few other micros have these, but in 1991 the trend is away from them (however, see cycle of reincarnation). Syn. raster blaster.

-Blivet

/bliv'*t/ n. [allegedly from a World War II military term meaning "ten pounds of manure in a five-pound bag"]

1. An intractable problem.
2. A crucial piece of hardware that can't be fixed or replaced if it breaks.
3. A tool that has been hacked over by so many incompetent programmers that it has become an unmaintainable tissue of hacks.
4. An out-of-control but unkillable development effort.
5. An embarrassing bug that pops up during a customer demo.
6. In the subjargon of computer security specialists, a denial-of-service attack performed by hogging limited resources that have no access controls (for example, shared spool space on a multi-user system). This term has other meanings in other technical cultures; among experimental physicists and hardware engineers of various kinds it seems to mean any random object of unknown purpose (similar to hackish use of frob). It has also been used to describe an amusing trick-the-eye drawing resembling a three-pronged fork that appears to

depict a three-dimensional object until one realizes that the parts fit together in an impossible way.

-BLOB

1. n. [acronymBinary Large OBject] Used by database people to refer to any random large block of bits that needs to be stored in a database, such as a picture or sound file. The essential point about a BLOB is that it's an object that cannot be interpreted within the database itself.
2. v. To mailbomb someone by sending a BLOB him/her; esp. used as a mild threat. “If that program crashes again, I'm going to BLOB the core dump to you. ”

Block

1. A group of bits or digits that are transmitted as a unit and that may be encoded for error-control purposes. (FP) (~)
2. A string of records, words, or characters, that for technical or logical purposes, are treated as a unit. (~) (FP) (ISO) Note: Blocks are separated by interblock gaps and each block may contain one or more records.
3. In programming languages, a subdivision of a program that serves to group related statements, delimit routines, specify storage allocation, delineate the applicability of labels, or segment parts of the program for other purposes. (FP)
4. [from process scheduling terminology in OS theory] vi. To delay or sit idle while waiting for something. “We're blocking until everyone gets here. ” Compare busy-wait.
5. `block on' vt. To block, waiting for (something). “Lunch is blocked on Phil's arrival. ”

Block Character

See end-of-transmission-block character.

Block Check

That part of the error control procedure that is used to determine whether a block of data is structured according to given rules. (~) See also block, block check character, block code, block parity, error control.

Block Check Character

A character added at the end of a message or transmission block to facilitate error detection. Note: In longitudinal redundancy checking and cyclic redundancy checking, a block check character is transmitted by the sender after each message block. This block check character is compared with a second block check character computed by the receiver to determine if the transmission is error free. See also block check, block parity, character, cyclic redundancy check, error control.

Block Code

An error detection and/or correction code in which the encoded block consists of N symbols, containing K information symbols (K<N) and N-K redundant check symbols, such that most naturally occurring errors can be detected and/or corrected. See also block, block parity, convolutional code, error control, error-correcting code, forward error correction.

Block Diagram

A diagram of a system, a computer, or a device in which the principal parts are represented by suitably annotated geometrical figures to show both the basic functions of the parts and their functional relationships. (FP) (ISO)

Block Length

The number of records, words, or characters in a block. (FP) (ISO)

Block Parity

The designation of one or more bits in a block as parity bits whose purpose is to ensure a designated parity, either odd or even. (~) Note: Used to assist in error detection or correction, or both. See also binary digit, block code, cyclic redundancy check, error control, error correcting code, error detecting code, parity, parity check.

Block Transfer

The process, initiated by a single action, of transferring one or more blocks of data. (FP) (ISO)

Block Transfer Attempt

A coordinated sequence of user and telecommunication system activities undertaken to effect transfer of an individual block from a source user to a destination user. Note: A block transfer attempt begins when the first bit of the block crosses the functional interface between the source user and the telecommunication system. A block transfer attempt ends either in successful block transfer or in block transfer failure. See also block transfer time, interface, successful block transfer.

-Block Transfer Computations

n. [from the television series “Dr. Who”] Computations so fiendishly subtle and complex that they could not be performed by machines. Used to refer to any task that should be expressible as an algorithm in theory, but isn't.

Block Transfer Efficiency

The average ratio of user information bits to total bits in successfully transferred blocks. See also overhead information, throughput.

Block Transfer Failure

Failure to deliver a block successfully. Note: Normally the principal block transfer failure outcomes

are: lost block, misdelivered block, and added block. See also added block, deleted block, failure, incorrect block, lost block, successful block delivery, successful block transfer.

Block Transfer Rate

The number of successful block transfers during a performance measurement period divided by the duration of the period. (~) See also data transfer rate, data transfer time, error ratio, maximum block transfer time.

Block Transfer Time

The average value of the duration of a successful block transfer attempt. A block transfer attempt is successful if a) the transmitted block is delivered to the intended destination user within the maximum allowable performance period and b) the contents of the delivered block are correct. See also block, block transfer attempt, successful block transfer.

Block-Error Probability

The ratio of the number of incorrectly received or missing blocks to the total number of blocks transmitted during a measurement period. (~) See also block-loss probability, incorrect block.

Block-Loss Probability

The ratio of the number of lost blocks to the total number of block transfer attempts during a specified period. (~) See also block error probability, block-misdelivery probability.

Block-Misdelivery Probability

The ratio of the number of misdelivered blocks to the total number of block transfer attempts during a specified period. (~) See also lost block, misdelivered block.

Blocking

1. The formatting of data into blocks for purposes of transmission, storage, checking, or other functions.
2. Denying access to, or use of, a facility, system, or component. See also classmark, lost call, system blocking signal.

Blocking Criterion

In telephone traffic engineering, a criterion that specifies the maximum number of calls or service demands that fail to receive immediate service. This value is normally expressed in a probabilistic notation (e. g. , P. 001).

Blocking Factor

The number of records in a block; the number is computed by dividing the size of the block by the size of each record contained therein. (FP) (ISO) Note: Each record in the block must be the same size. Synonym grouping factor.

Blocking Formulas

Specific probability distribution functions that closely approximate the call pattern of telephone users' probable behavior in failing to find idle facilities.

-Blow An EPROM

/bloh *n ee'prom/ v. (alt. `blast an EPROM', `burn an EPROM') To program a read-only memory, e. g. for use with an embedded system. This term arose because the programming process for the Programmable Read-Only Memories (PROMs) that preceded present-day Erasable Programmable Read-Only Memories (EPROMs) involved intentionally blowing tiny electrical fuses on the chip. The usage lives on (it's too vivid and expressive to discard) even though the write process on EPROMs is nondestructive.

-Blow Away

vt. To remove (files and directories) from permanent storage, generally by accident. “He reformatted the wrong partition and blew away last night's netnews. ” Oppose nuke.

-Blow Out

vi. [prob. from mining and tunneling jargon] Of software, to fail spectacularly; almost as serious as crash and burn. See blow past, blow up, die horribly.

-Blow Past

1. vt. To blow out despite a safeguard. “The server blew past the 5K reserve buffer. ”
2. To fool the uninitiated. “ I blew the explanation past the boss. ”

-Blow Up

1. vi. [scientific computation] To become unstable. Suggests that the computation is diverging so rapidly that it will soon overflow or at least go nonlinear.
2. Syn. blow out.

-BLT

/B-L-T/, /bl*t/ or (rarely) /belt/ n. ,vt. Synonym for blit. This is the original form of blit and the ancestor of bitblt. It referred to any large bit-field copy or move operation (one resource-intensive memory-shuffling operation done on pre-paged versions of ITS, WAITS, and TOPS-10 was sardonically referred to as `The Big BLT'). The jargon usage has outlasted the PDP-10 BLock Transfer instruction from which BLT derives; nowadays, the assembler mnemonic BLT almost always means `Branch if Less Than zero'.

-Blue Book

1. n. Informal name for one of the three standard references on the page-layout and graphics-control language PostScript (“PostScript Language Tuto-

rial and Cookbook", Adobe Systems, Addison-Wesley 1985, QA76. 73. P67P68, ISBN 0-201-10179-3); the other three official guides are known as the Green Book, the Red Book, and the White Book (sense 2).
2. Informal name for one of the three standard references on Smalltalk "Smalltalk-80 The Language and its Implementation", David Robson, Addison-Wesley 1983, QA76. 8. S635G64, ISBN 0-201-11371-63 (this book also has green and red siblings).
3. Any of the 1988 standards issued by the CCITT's ninth plenary assembly. These include, among other things, the X. 400 email spec and the Group 1 through 4 fax standards. See also book titles.

-Blue Box

1. n. obs. Once upon a time, before all-digital switches made it possible for the phone companies to move them out of the audible range, one could actually hear the switching tones used to route long-distance calls. Early phreakers built devices called `blue boxes' that could reproduce these tones, which could be used to commandeer portions of the phone network. (This was not as hard as it may sound; one early phreak acquired the sobriquet `Captain Crunch' after he proved that he could generate switching tones with a plastic whistle pulled out of a box of Captain Crunch cereal!)
2. n. An IBM machine, especially a large (non-PC) one.

-Blue Wire

n. [IBM] Patch wires added to circuit boards at the factory to correct design or fabrication problems. These may be necessary if there hasn't been time to design and qualify another board version. Compare purple wire, red wire, yellow wire.

-BNF

1. /B-N-F/ n. [techspeak] Acronym for `Backus-Naur Form', a metasyntactic notation used to specify the syntax of programming languages, command sets, and the like. Widely used for language descriptions but seldom documented anywhere, so that it must usually be learned by osmosis from other hackers. Consider this BNF for a U. S. postal address <postal-address>:= <name-part> <street-address> <zip-part> <personal-part>:= <name> | <initial> ". " <name-part>:= <personal-part> <last-name> [<jr-part>] <EOL> | <personal-part> <name-part> <street-address>:= [<apt>] <house-num> <street-name> <EOL> <zip-part>:= <town-name> "," <state-code> <ZIP-code> <EOL> This translates into English as "A postal-address consists of a name-part, followed by a street-address part, followed by a zip-code part. A personal-part consists of either a first name or an initial followed by a dot. A name-part consists of either a personal-part followed by a last name followed by an optional `jr-part' (Jr. , Sr. , or dynastic number) and end-of-line, or a personal part followed by a name part (this rule illustrates the use of recursion in BNFs, covering the case of people who use multiple first and middle names and/or initials). A street address consists of an optional apartment specifier, followed by a street number, followed by a street name. A zip-part consists of a town-name, followed by a comma, followed by a state code, followed by a ZIP-code followed by an end-of-line. " Note that many things (such as the format of a personal-part, apartment specifier, or ZIP-code) are left unspecified. These are presumed to be obvious from context or detailed somewhere nearby. See also parse.
2. Any of a number number of variants and extensions of BNF proper, possibly containing some or all of the regexp wildcards such as `*' or `+'. In fact the example above isn't the pure form invented for the Algol-60 report; it uses `[]', which was introduced a few years later in IBM's PL/I definition but is now universally recognized.
3. In science-fiction fandom, a `Big-Name Fan' (someone famous or notorious). Years ago a fan started handing out black-on-green BNF buttons at SF conventions; this confused the hacker contingent terribly.

-Boa

[IBM] n. Any one of the fat cables that lurk under the floor in a dinosaur pen. Possibly so called because they display a ferocious life of their own when you try to lay them straight and flat after they have been coiled for some time. It is rumored within IBM that channel cables for the 370 are limited to 200 feet because beyond that length the boas get dangerous -- and it is worth noting that one of the major cable makers uses the trademark `Anaconda'.

-Board

1. n. In-context synonym for bboard; sometimes used even for Usenet newsgroups (but see usage note under bboard, sense 1).
2. An electronic circuit board.

-Boat Anchor

1. n. Like doorstop but more severe; implies that the offending hardware is irreversibly dead or useless. "That was a working motherboard once. One lightning strike later, instant boat anchor!"
2. A person who just takes up space.
3. Obsolete but still working hardware, especially when used of an old S100-bus hobbyist system; originally a term of annoyance, but became more and more affectionate as the hardware became more and more obsolete.

-BOF

/B-O-F/ or /bof/ n. Abbreviation for the phrase “Birds Of a Feather” (flocking together), an informal discussion group and/or bull session scheduled on a conference program. It is not clear where or when this term originated, but it is now associated with the USENIX conferences for UNIX techies and was already established there by 1984. It was used earlier than that at DECUS conferences and is reported to have been common at SHARE meetings as far back as the early 1960s.

-Bogo-Sort

/boh`goh-sort'/ n. (var. `stupid-sort') The archetypical perversely awful algorithm (as opposed to bubble sort, which is merely the generic *bad* algorithm). Bogo-sort is equivalent to repeatedly throwing a deck of cards in the air, picking them up at random, and then testing whether they are in order. It serves as a sort of canonical example of awfulness. Looking at a program and seeing a dumb algorithm, one might say “Oh, I see, this program uses bogo-sort. ” Compare bogus, brute force, Lasherism.

Bogus Message

Communications transmitted for some purpose other than to pass information. NOTE: Bogus messages may consist of dummy groups or meaningless text.

-Bogus:

1. adj. Non-functional. “Your patches are bogus. ”
2. Useless. “OPCON is a bogus program. ”
3. False. “Your arguments are bogus. ”
4. Incorrect. “That algorithm is bogus. ”
5. Unbelievable. “You claim to have solved the halting problem for Turing Machines? That's totally bogus. ”
6. Silly. “Stop writing those bogus sagas. ” Astrology is bogus. So is a bolt that is obviously about to break. So is someone who makes blatantly false claims to have solved a scientific problem. (This word seems to have some, but not all, of the connotations of random -- mostly the negative ones.) It is claimed that `bogus' was originally used in the hackish sense at Princeton in the late 1960s. It was spread to CMU and Yale by Michael Shamos, a migratory Princeton alumnus. A glossary of bogus words was compiled at Yale when the word was first popularized (see autobogotiphobia under bogotify). The word spread into hackerdom from CMU and MIT. By the early 1980s it was also current in something like the hackish sense in West Coast teen slang, and it had gone mainstream by 1985. A correspondent from Cambridge reports, by contrast, that these uses of `bogus' grate on British nerves; in Britain the word means, rather specifically, `counterfeit', as in “a bogus 10-pound note”.

-Bohr Bug

/bohr buhg/ n. [from quantum physics] A repeatable bug; one that manifests reliably under a possibly unknown but well-defined set of conditions. Antonym of heisenbug; see also mandelbug, schroedinbug.

Bomb

1. v. General synonym for crash (sense 1) except that it is not used as a noun; esp. used of software or OS failures. “Don't run Empire with less than 32K stack, it'll bomb. ”
2. n. ,v. Atari ST and Macintosh equivalents of a UNIX `panic' or Amiga guru (sense2) in which icons of little black-powder bombs or mushroom clouds are displayed, indicating that the system has died. On the Mac, this may be accompanied by a decimal (or occasionally hexadecimal) number indicating what went wrong, similar to the Amiga guru meditation number. MS-DOS machines tend to get locked up in this situation. See Logic Bomb.

-Book Titles

There is a tradition in hackerdom of informally tagging important textbooks and standards documents with the dominant color of their covers or with some other conspicuous feature of the cover. Many of these are described in this lexicon under their own entries. See Aluminum Book, Blue Book, Cinderella Book, Devil Book, Dragon Book, Green Book, *Orange Book*, Pink-Shirt Book, Purple Book, Red Book, Silver Book, White Book, Wizard Book, Yellow Book, and bible; see also rainbow series.

Boolean Function

A switching function in which the number of possible values of the function and each of its independent variables is two. (FP) (ISO)

Boolean Operation

1. Any operation in which each of the operands and the result take one of two values. (FP) (ISO)
2. An operation that follows the rules of Boolean Algebra. (FP) (ISO)

-Boot

1. v. ,n. [techspeak; from `by one's bootstraps'] To load and initialize the operating system on a machine. This usage is no longer jargon (having passed into techspeak) but has given rise to some derivatives that are still jargon. The derivative `reboot' implies that the machine hasn't been down for long, or that the boot is a bounce (sense 4) intended to clear some state of wedgitude. This is sometimes used of human thought processes, as in the following exchange “You've lost me. ” “OK, reboot. Here's the theory. ” This term is also found in the variants `cold boot' (from power-off condition) and `warm boot' (with the CPU and all de-

vices already powered up, as after a hardware reset or software crash). Another variant `soft boot', reinitialization of only part of a system, under control of other software still running “If you're running the mess-dos emulator, control-alt-insert will cause a soft-boot of the emulator, while leaving the rest of the system running. ” Opposed to this there is `hard boot', which connotes hostility towards or frustration with the machine being booted “I'll have to hard-boot this losing Sun. ” “I recommend booting it hard. ” One often hard-boots by performing a power cycle.

2. Historical note this term derives from `bootstrap loader', a short program that was read in from cards or paper tape, or toggled in from the front panel switches. This program was always very short (great efforts were expended on making it short in order to minimize the labor and chance of error involved in toggling it in), but was just smart enough to read in a slightly more complex program (usually from a card or paper tape reader), to which it handed control; this program in turn was smart enough to read the application or operating system from a magnetic tape drive or disk drive. Thus, in successive steps, the computer `pulled itself up by its bootstraps' to a useful operating state. Nowadays the bootstrap is usually found in ROM or EPROM, and reads the first stage in from a fixed location on the disk, called the `boot block'. When this program gains control, it is powerful enough to load the actual OS and hand control over to it.

Bootstrap

1. A technique or device designed to bring about a desired state by means of its own action. (~)
2. That part of a computer program that may be used to establish another version of the computer program. (FP)
3. The automatic procedure whereby the basic operating system of a processor is reloaded following a complete shutdown or loss of memory.
4. A set of instructions that cause additional instructions to be loaded until the complete computer program is in storage. (FP) (ISO)
5. To use a bootstrap. (FP) (ISO) See also computer

-Bottom-Up Implementation

n. Hackish opposite of the techspeak term `top-down design'. It is now received wisdom in most programming cultures that it is best to design from higher levels of abstraction down to lower, specifying sequences of action in increasing detail until you get to actual code. Hackers often find (especially in exploratory designs that cannot be closely specified in advance) that it works best to *build* things in the opposite order, by writing and testing a clean set of primitive operations and then knitting them together.

-Bounce

1. v. [perhaps by analogy to a bouncing check] An electronic mail message that is undeliverable and returns an error notification to the sender is said to `bounce'. See also bounce message.
2. [Stanford] To play volleyball. The now-demolished D. C. Power Lab building used by the Stanford AI Lab in the 1970s had a volleyball court on the front lawn. From 5 P. M. to 7 P. M. was the scheduled maintenance time for the computer, so every afternoon at 5 would come over the intercom the cry “Now hear this bounce, bounce!”, followed by Brian McCune loudly bouncing a volleyball on the floor outside the offices of known volleyballers.
3. . To casually reboot a system in order to clear up a transient problem. Reported primarily among VMS users.
3. [VM/CMS programmers] *Automatic* warm-start of a machine after an error. “I logged on this morning and found it had bounced 7 times during the night”
4. [IBM] To power cycle a peripheral in order to reset it.

-Bounce Message

n. [UNIX] Notification message returned to sender by a site unable to relay email to the intended Internet address recipient or the next link in a bang path (see bounce, sense 1). Reasons might include a nonexistent or misspelled username or a down relay site. Bounce messages can themselves fail, with occasionally ugly results; see sorcerer's apprentice mode and software laser. The terms `bounce mail' and `barfmail' are also common.

Bounds Checking

1. Testing of computer program results for access to storage outside authorized limits. (*AR* 380-380; *FIPS PUB* 39)
2. Verifying a computer program address for access to storage outside authorized limits. Synonymous with Memory Bounds Checking. (*NCSC-WA*-001-85;)
3. Synonymous with MEMORY BOUNDS CHECKING.

Bounds Register

A hardware register which holds an address specifying a storage boundary. (*FIPS PUB* 39; *AR* 380-380)

-Boustrophedon

n. [from a Greek word for turning like an ox while plowing] An ancient method of writing using alternate left-to-right and right-to-left lines. This term is actually philologists' techspeak and typesetters' jargon. Erudite hackers use it for an optimization performed by some computer typesetting software and moving-

head printers. The adverbial form `boustrophedonically' is also found (hackers purely love constructions like this).

-Box

1. n. A computer; esp. in the construction `foo box' where foo is some functional qualifier, like `graphics', or the name of an OS (thus, `UNIX box', `MS-DOS box', etc.) “We preprocess the data on UNIX boxes before handing it up to the mainframe. ”
2. [IBM] Without qualification but within an SNA-using site, this refers specifically to an IBM front-end processor or FEP /F-E-P/. An FEP is a small computer necessary to enable an IBM mainframe to communicate beyond the limits of the dinosaur pen. Typically used in expressions like the cry that goes up when an SNA network goes down”Looks like the box has fallen over. ” (See fall over.) See also IBM, fear and loathing, fepped out, Blue Glue.

-Boxed Comments

n. Comments (explanatory notes attached to program instructions) that occupy several lines by themselves; so called because in assembler and C code they are often surrounded by a box in a style something like this

```
/*****************************************
This is a boxed comment in C style *
*****************************************/
```

Common variants of this style omit the asterisks in column 2 or add a matching row of asterisks closing the right side of the box. The sparest variant omits all but the comment delimiters themselves; the `box' is implied. Oppose winged comments.

-Boxen

/bok'sn/ pl. n. [by analogy with VAXen] Fanciful plural of box often encountered in the phrase `UNIX boxen', used to describe commodity UNIX hardware. The connotation is that any two UNIX boxen are interchangeable.

-Boxology

/bok-sol'*-jee/ n. Syn. ASCII art. This term implies a more restricted domain, that of box-and-arrow drawings. “His report has a lot of boxology in it. ” Compare macrology.

-Brain Dump

n. The act of telling someone everything one knows about a particular topic or project. Typically used when someone is going to let a new party maintain a piece of code. Conceptually analogous to an operating system core dump in that it saves a lot of useful state before an exit. “You'll have to give me a brain dump on FOOBAR before you start your new job at HackerCorp. ” See core dump (sense 4). At Sun, this is also known as `TOI' (transfer of information).

-Brain-Damaged

[generalization of `Honeywell Brain Damage' (HBD), a theoretical disease invented to explain certain utter cretinisms in Honeywell Multics]

1. adj. Obviously wrong; cretinous; demented. There is an implication that the person responsible must have suffered brain damage, because he should have known better. Calling something brain-damaged is really bad; it also implies it is unusable, and that its failure to work is due to poor design rather than some accident. “Only six monocase characters per file name? Now *that's* brain-damaged!”
2. [esp. in the Mac world] May refer to free demonstration software that has been deliberately crippled in some way so as not to compete with the commercial product it is intended to sell. Syn. crippleware.

-Brain-Dead

adj. Brain-damaged in the extreme. It tends to imply terminal design failure rather than malfunction or simple stupidity. “This comm program doesn't know how to send a break -- how brain-dead!”

Branch

1. In a computer program, a conditional jump or departure from the implicit or declared order in which instructions are being executed. (~)
2. To select a branch, as in definition #1.
3. A direct path joining two nodes of a network or graph.
4. In a power distribution system, a circuit from a distribution device (power panel) of a lower power handling capability than that of the input circuits to the device. (~) See also node.

Breach

The successful and repeatable defeat of security controls with or without an arrest, which if carried to consummation, could result in a penetration of the system. Examples of breaches are: a. Operation of user code in master mode. b. Unauthorized acquisition of identification password or file access passwords. c. Accessing a file without using prescribed operating system mechanisms. d. Unauthorized access to tape library. (*OPNAVINST* 5239. lA; *AR* 380-380; *DOD* 5200. 28M)

-Bread Crumbs

n. Debugging statements inserted into a program that emit output or log indicators of the program's state to a file so you can see where it dies or pin down the cause of surprising behavior. The term is probably a reference to the Hansel and Gretel story from the Brothers Grimm; in several variants, a character leaves a trail of bread crumbs so as not to get lost in the woods.

Breadboard

1. An assembly of circuits or parts used to prove the feasibility of a device, circuit, system, or principle with little or no regard to the final configuration or packaging of the parts. (~)
2. To prepare a breadboard.

-Break

1. vt. To cause to be broken (in any sense). “Your latest patch to the editor broke the paragraph commands. ”
2. v. (of a program) To stop temporarily, so that it may debugged. The place where it stops is a `breakpoint'.
3. [techspeak] vi. To send an RS-232 break (two character widths of line high) over a serial communication line.
4. [UNIX] vi. To strike whatever key currently causes the tty driver to send SIGINT to the current process. Normally, break (sense 3), delete or control-C does this.
5. ‘break break' may be said to interrupt a conversation (this is an example of verb doubling). This usage comes from radio communications, which in turn probably came from landline telegraph/teleprinter usage, as badly abused in the Citizen's Band craze a few years ago.

-Breath-Of-Life Packet

n. [XEROX PARC] An Ethernet packet that contains bootstrap (see boot) code, periodically sent out from a working computer to infuse the `breath of life' into any computer on the network that has happened to crash. Machines depending on such packets have sufficient hardware or firmware code to wait for (or request) such a packet during the reboot process. The notional `kiss-of-death packet', with a function complementary to that of a breath-of-life packet, is recommended for dealing with hosts that consume too many network resources. Though `kiss-of-death packet' is usually used in jest, there is at least one documented instance of an Internet subnet with limited address-table slots in a gateway machine in which such packets were routinely used to compete for slots, rather like Christmas shoppers competing for scarce parking spaces.

Brevity Code/brevity List

A code which has the sole purpose of shortening messages rather than the concealment of their content. (NCSC-9)

Brevity List

List containing words and phrases used to shorten messages.

Brevity Lists

1. A pseudo code system that is used to reduce the length of time required to transmit information by use of a few characters in place of long routine sentences. (*AR* 380-380;)
2. A code system that is used to reduce the length of time required to transmit information by the use of a few characters to represent long, stereotyped sentences. (*FIPS PUB* 39;)

Bridge

1. A functional unit that interconnects two local area networks that use the same logical link control procedure, but may use different medium access control procedures.
2. Device that connects local area networks at the data link layer. Browsing. Act of searching through AIS storage to locate or acquire information, without necessarily knowing the existence or format of information being sought. (FP) (ISO) See also gateway. See hybrid coil. (~)

Brightness

An attribute of visual perception, in accordance with which a source appears to emit more or less light. Note 1: Usage should be restricted to non-quantitative reference to physiological sensations and perceptions of light. Note 2: “Brightness” was formerly used as a synonym for the photometric term “luminance” and (incorrectly) for the radiometric term “radiance. ” See also irradiance, radiance, radiant intensity.

-Bring X To Its Knee

v. To present a machine, operating system, piece of software, or algorithm with a load so extreme or pathological that it grinds to a halt. “To bring a MicroVAX to its knees, try twenty users running vi -- or four running EMACS. ” Compare hog.

-Brittl

adj. Said of software that is functional but easily broken by changes in operating environment or configuration, or by any minor tweak to the software itself. Also, any system that responds inappropriately and disastrously to abnormal but expected external stimuli; e. g. , a file system that is usually totally scrambled by a power failure is said to be brittle. This term is often used to describe the results of a research effort that were never intended to be robust, but it can be applied to commercially developed software, which displays the quality far more often than it ought to. Oppose robust.

Broadband Emanation Or Emission

1. An acoustic emanation which is characterized by the following: a. The appearance of the observed emanation is definitely not sinusoidal. b. The duration of the impulse emanation is very short compared with the period between impulses. c. The peak value of the impulse emanation is very much greater (in order of 10 to 15 dB) than the average

"apparent r. m. s. " value of the overall emanation. (NACSEM 5103)
2. Any electromagnetic emanation or ambient signal detected with broadband tunable or broadband nontunable detection system. (NACSEM 5201)

Broadband ISDN

1. A CCITT proposed Integrated Services Digital Network offering broadband capabilities including many of the following features or services: (a) from 150 to 600 Mbps interfaces, (b) using ATM (asynchronous transfer mode) to carry all services over a single, integrated, high-speed packet-switched net, (c) LAN interconnection, (d) the ability to connect LANs at different locations, (e) access to a remote, shared disk server, (f) voice/video/data teleconferencing from one's desk, (g) transport for programming services (e. g. , cable TV), (h) single-user controlled access to remote video source, (i) voice/video telephone calls, and j) access to shop-at-home and other information services.
2. Note: Techniques involved in the B-ISDN include code conversion, information compression, multipoint connections, multiple-connection calls. Current proposals use service-independent call structure that allows flexible arrangement and modular control of access and transport edges, the service components of a connection which can provide each user in a connection with independent control of its access features and serve as the basis of a simplified control structure for multipoint and multiconnection calls. Such a network might be expected to offer a variety of ancillary information processing functions.
3. See also Integrated Services Digital Network. Synonym wideband

Broadband System

See wideband.

-Broadcast Storm

n. An incorrect packet broadcast on a network that causes most hosts to respond all at once, typically with wrong answers that start the process over again. See network meltdown; compare mail storm.

-Broken

1. adj. Not working properly (of programs).
2. Behaving strangely; especially (when used of people) exhibiting extreme depression.

-Broken Arrow

n. [IBM] The error code displayed on line 25 of a 3270 terminal (or a PC emulating a 3270) for various kinds of protocol violations and "unexpected" error conditions (including connection to a down computer). On a PC, simulated with `->/_', with the two center characters overstruck. Note to appreciate this term fully, it helps to know that `broken arrow' is also military jargon for an accident involving nuclear weapons.

-Broket

/broh'k*t/ or /broh'ket`/ n. [by analogy with `bracket' a `broken bracket'] Either of the characters `<' and `>', when used as paired enclosing delimiters. This word originated as a contraction of the phrase `broken bracket', that is, a bracket that is bent in the middle. (At MIT, and apparently in the Real World as well, these are usually called angle brackets.)

-Brooks's Law

prov. "Adding manpower to a late software project makes it later" -- a result of the fact that the expected advantage from splitting work among N programmers is O(N) (that is, proportional to N), but the complexity and communications cost associated with coordinating and then merging their work is O(N^2) (that is, proportional to the square of N). The quote is from Fred Brooks, a manager of IBM's OS/360 project and author of "The Mythical Man-Month" (Addison-Wesley, 1975, ISBN 0-201-00650-2), an excellent early book on software engineering. The myth in question has been most tersely expressed as "Programmer time is fungible" and Brooks established conclusively that it is not. Hackers have never forgotten his advice; too often, management still does. See also creationism, second-system effect, optimism.

Browsing

1. The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; *NCSC-WA*-001-85;; *FIPS PUB* 39;)
2. Browsing is 'the unauthorized looking through, identifying, and exploiting of data that are available but are supposed to be unknown'. (JL;)

-Brute Force

1. adj. Describes a primitive programming style, one in which the programmer relies on the computer's processing power instead of using his or her own intelligence to simplify the problem, often ignoring problems of scale and applying naive methods suited to small problems directly to large ones. The term can also be used in reference to programming style brute-force programs are written in a heavyhanded, tedious way, full of repetition and devoid of any elegance or useful abstraction (see also brute force and ignorance). The canonical example of a brute-force algorithm is associated with the `traveling salesman problem' (TSP), a classical NP-hard problem Suppose a person is in, say, Boston, and wishes to drive to N other cities. In what order should the cities be visited in

order to minimize the distance travelled? The brute-force method is to simply generate all possible routes and compare the distances; while guaranteed to work and simple to implement, this algorithm is clearly very stupid in that it considers even obviously absurd routes (like going from Boston to Houston via San Francisco and New York, in that order). For very small N it works well, but it rapidly becomes absurdly inefficient when N increases (for N = 15, there are already 1,307,674,368,000 possible routes to consider, and for N = 1000 -- well, see bignum). Sometimes, unfortunately, there is no better general solution than brute force. See also NP-.

2. A more simple-minded example of brute-force programming is finding the smallest number in a large list by first using an existing program to sort the list in ascending order, and then picking the first number off the front. Whether brute-force programming should actually be considered stupid or not depends on the context; if the problem is not terribly big, the extra CPU time spent on a brute-force solution may cost less than the programmer time it would take to develop a more `intelligent' algorithm. Additionally, a more intelligent algorithm may imply more long-term complexity cost and bug-chasing than are justified by the speed improvement. Ken Thompson, co-inventor of UNIX, is reported to have uttered the epigram “When in doubt, use brute force”. He probably intended this as a ha ha only serious, but the original UNIX kernel's preference for simple, robust, and portable algorithms over brittle `smart' ones does seem to have been a significant factor in the success of that OS. Like so many other tradeoffs in software design, the choice between brute force and complex, finely-tuned cleverness is often a difficult one that requires both engineering savvy and delicate esthetic judgment.

-Brute Force And Ignorance

n. A popular design technique at many software houses -- brute force coding unrelieved by any knowledge of how problems have been previously solved in elegant ways. Dogmatic adherence to design methodologies tends to encourage this sort of thing. Characteristic of early larval stage programming; unfortunately, many never outgrow it. Often abbreviated BFI “Gak, they used a bubble sort! That's strictly from BFI. ” Compare bogosity.

-BSD

/B-S-D/ n. [abbreviation for `Berkeley Software Distribution'] a family of UNIX versions for the DEC VAX and PDP-11 developed by Bill Joy and others at Berzerkeley starting around 1980, incorporating paged virtual memory, TCP/IP networking enhancements, and many other features. The BSD versions (4. 1, 4. 2, and 4. 3) and the commercial versions derived from them (SunOS, ULTRIX, and Mt. Xinu) held the technical lead in the UNIX world until AT&T's successful standardization efforts after about 1986, and are still widely popular. Note that BSD versions going back to 2. 9 are often referred to by their version numbers, without the BSD prefix. See 4. 2, UNIX, USG UNIX.

-Bubble Sort

n. Techspeak for a particular sorting technique in which pairs of adjacent values in the list to be sorted are compared and interchanged if they are out of order; thus, list entries `bubble upward' in the list until they bump into one with a lower sort value. Because it is not very good relative to other methods and is the one typically stumbled on by naive and untutored programmers, hackers consider it the canonical example of a naive algorithm. The canonical example of a really *bad* algorithm is bogo-sort. A bubble sort might be used out of ignorance, but any use of bogosort could issue only from brain damage or willful perversity.

-Bucky Bits

/buh'kee bits/ n. obs.

1. The bits produced by the CONTROL and META shift keys on a SAIL keyboard (octal 200 and 400 respectively), resulting in a 9-bit keyboard character set. The MIT AI TV (Knight) keyboards extended this with TOP and separate left and right CONTROL and META keys, resulting in a 12-bit character set; later, LISP Machines added such keys as SUPER, HYPER, and GREEK (see space-cadet keyboard).
2. By extension, bits associated with `extra' shift keys on any keyboard, e. g. , the ALT on an IBM PC or command and option keys on a Macintosh. It has long been rumored that `bucky bits' were named for Buckminster Fuller during a period when he was consulting at Stanford. Actually, bucky bits were invented by Niklaus Wirth when *he* was at Stanford in 1964--65; he first suggested the idea of an EDIT key to set the 8th bit of an otherwise 7-bit ASCII character). It seems that, unknown to Wirth, certain Stanford hackers had privately nicknamed him `Bucky' after a prominent portion of his dental anatomy, and this nickname transferred to the bit. Bucky-bit commands were used in a number of editors written at Stanford, including most notably TV-EDIT and NLS. The term spread to MIT and CMU early and is now in general use. Ironically, Wirth himself remained unaware of its derivation for nearly 30 years, until GLS dug up this history in early 1993! See double bucky, quadruple bucky.

Budget

Budget And Accounting Act

Budget And Accounting Procedures Act Of 1950

Buffer

1. A routine or storage used to compensate for a difference in rate of flow of data, or time of occurrence of events, when transferring data from one device to another. (FP) (~)
2. Note: Buffers are used for many purposes such as: (a) interconnecting two digital circuits operating at different rates, (b) holding data for use at a later time, (c) allowing timing corrections to be made on a data stream, (d) collecting binary data bits into groups that can then be operated on as a unit, (e) delaying the transit time of a signal in order to allow other operations to occur.
3. To allocate and schedule the use of buffers. (~)
4. An isolating circuit used to prevent a driven circuit from influencing the driving circuit. (~)
5. In an optical fiber cable, a component used to encapsulate an optical fiber, thus providing mechanical isolation and/or protection from physical damage. (~) Note: Cable fabrication techniques vary, some resulting in firm contact between fiber and protective buffering, others resulting in a loose fit, permitting the fiber to slide in the buffer tube. Multiple buffer layers may be used for added fiber protection. See also data, elastic buffer, first-in first-out, optical fiber cable, queueing, queueing delay, queue traffic, variable length buffer.

-Buffer Overflow

n. What happens when you try to stuff more data into a buffer (holding area) than it can handle. This may be due to a mismatch in the processing rates of the producing and consuming processes (see overrun and firehose syndrome), or because the buffer is simply too small to hold all the data that must accumulate before a piece of it can be processed. For example, in a text-processing tool that crunches a line at a time, a short line buffer can result in lossage as input from a long line overflows the buffer and trashes data beyond it. Good defensive programming would check for overflow on each character and stop accepting data when the buffer is full up. The term is used of and by humans in a metaphorical sense. “What time did I agree to meet you? My buffer must have overflowed. ” Or “If I answer that phone my buffer is going to overflow. ” See also spam.

Bug

1. A concealed microphone or listening device or other audiosurveillance device. (JCS1-DoD) See also communications security. (~)
2. To install means for audiosurveillance. (JCS1-DoD)
3. A semiautomatic telegraph key.
4. A mistake or malfunction. (FP) (~)
5. n. An unwanted and unintended property of a program or piece of hardware, esp. one that causes it to malfunction. Antonym of feature. Examples “There's a bug in the editor it writes things out backwards. ” “The system crashed because of a hardware bug. ” “Fred is a winner, but he has a few bugs” (i. e. , Fred is a good guy, but he has a few personality problems).
6. Historical note Admiral Grace Hopper (an early computing pioneer better known for inventing COBOL) liked to tell a story in which a technician solved a glitch in the Harvard Mark II machine by pulling an actual insect out from between the contacts of one of its relays, and she subsequently promulgated bug in its hackish sense as a joke about the incident (though, as she was careful to admit, she was not there when it happened). For many years the logbook associated with the incident and the actual bug in question (a moth) sat in a display case at the Naval Surface Warfare Center (NSWC). The entire story, with a picture of the logbook and the moth taped into it, is recorded in the “Annals of the History of Computing”, Vol. 3, No. 3 (July 1981), pp. 285--286. The text of the log entry (from September 9, 1947), reads “1545 Relay #70 Panel F (moth) in relay. First actual case of bug being found”. This wording establishes that the term was already in use at the time in its current specific sense -- and Hopper herself reports that the term `bug' was regularly applied to problems in radar electronics during WWII. Indeed, the use of `bug' to mean an industrial defect was already established in Thomas Edison's time, and a more specific and rather modern use can be found in an electrical handbook from 1896 (“Hawkin's New Catechism of Electricity”, Theo. Audel & Co.) which says “The term `bug' is used to a limited extent to designate any fault or trouble in the connections or working of electric apparatus. ” It further notes that the term is “said to have originated in quadruplex telegraphy and have been transferred to all electric apparatus. ” The latter observation may explain a common folk etymology of the term; that it came from telephone company usage, in which “bugs in a telephone cable” were blamed for noisy lines. Though this derivation seems to be mistaken, it may well be a distorted memory of a joke first current among *telegraph* operators more than a century ago! Actually, use of `bug' in the general sense of a disruptive event goes back to Shakespeare! In the first edition of Samuel Johnson's dictionary one meaning of `bug' is “A frightful object; a walking spectre”; this is traced to `bugbear', a Welsh term for a variety of mythological monster which (to

complete the circle) has recently been reintroduced into the popular lexicon through fantasy role-playing games. In any case, in jargon the word almost never refers to insects. Here is a plausible conversation that never actually happened "There is a bug in this ant farm!" "What do you mean? I don't see any ants in it. " "That's the bug. " A careful discussion of the etymological issues can be found in a paper by Fred R. Shapiro, 1987, "Entomology of the Computer Bug History and Folklore", American Speech 625. :376-378. [There has been a widespread myth that the original bug was moved to the Smithsonian, and an earlier version of this entry so asserted. A correspondent who thought to check discovered that the bug was not there. While investigating this in late 1990, your editor discovered that the NSWC still had the bug, but had unsuccessfully tried to get the Smithsonian to accept it -- and that the present curator of their History of American Technology Museum didn't know this and agreed that it would make a worthwhile exhibit. It was moved to the Smithsonian in mid-1991, but due to space and money constraints has not yet been exhibited. Thus, the process of investigating the original-computer-bug bug fixed it in an entirely unexpected way, by making the myth true! -- ESR]

-Bug-Of-The-Month Club

n. A mythical club which users of sendmail belong to; this was coined on the Usenet newsgroup comp. security. unix at a time when sendmail security holes, which allowed outside crackers access to the system, were uncovered at an alarming rate, forcing sysadmins to update very often. Also, more completely, `fatal security bug-of-the-month club'.

Bugging

Implanting a physical listening or transmittingdevice on or in AIS hardware to gain unauthorized access to data being processed. (JCS PUB 6-03. 7)

Bulk Encryption

Simultaneous encryption of all channels of a multichannel telecommunications trunk.

-Bulletproof

adj. Used of an algorithm or implementation considered extremely robust; lossage-resistant; capable of correctly recovering from any imaginable exception condition -- a rare and valued quality. Syn. armor-plated.

-Bum

1. vt. To make highly efficient, either in time or space, often at the expense of clarity. "I managed to bum three more instructions out of that code. " "I spent half the night bumming the interrupt code. " In elder days, John McCarthy (inventor of LISP) used to compare some efficiency-obsessed hackers among his students to "ski bums"; thus, optimization became "program bumming", and eventually just "bumming".
2. To squeeze out excess; to remove something in order to improve whatever it was removed from (without changing function; this distinguishes the process from a featurectomy).
3. n. A small change to an algorithm, program, or hardware device to make it more efficient. "This hardware bum makes the jump instruction faster. " Usage now uncommon, largely superseded by v. tune (and n. tweak, hack), though none of these exactly capture sense 2.
4. All these uses are rare in Commonwealth hackish, because in the parent dialects of English `bum' is a rude synonym for `buttocks'.

-Bump

vt. Synonym for increment. Has the same meaning as C's ++ operator. Used esp. of counter variables, pointers, and index dummies in `for', `while', and `do-while' loops.

-Burble

v. [from Lewis Carroll's "Jabberwocky"] Like flame, but connotes that the source is truly clueless and ineffectual (mere flamers can be competent). A term of deep contempt. "There's some guy on the phone burbling about how he got a DISK FULL error and it's all our comm software's fault. " This is mainstream slang in some parts of England.

-Buried Treasure

n. A surprising piece of code found in some program. While usually not wrong, it tends to vary from crufty to bletcherous, and has lain undiscovered only because it was functionally correct, however horrible it is. Used sarcastically, because what is found is anything *but* treasure. Buried treasure almost always needs to be dug up and removed. "I just found that the scheduler sorts its queue using bubble sort! Buried treasure!"

-Burn-In Period

1. n. A factory test designed to catch systems with marginal components before they get out the door; the theory is that burn-in will protect customers by outwaiting the steepest part of the bathtub curve (see infant mortality).
2. A period of indeterminate length in which a person using a computer is so intensely involved in his project that he forgets basic needs such as food, drink, sleep, etc. Warning Excessive burn-in can lead to burn-out. See hack mode, larval stage.

-Burst Page

n. Syn. banner, sense 1.

#-Burst Transmission#

A method of operating a data network by interrupting, at intervals, the data which are being transmitted. (Source: Panel of Experts, July 1994); (2) a sequence of transmission signals counted as a single entity in accordance with some defined criteria.

Bus

Transmission path or channel. A local area network topology, as used in Ethernet and the token bus, where all network nodes “listen” to all transmissions, selecting certain ones based on address identification.

Bus Interface Unit

See network interface device.

Bus Topology

A communication network topology in which nodes are connected serially, requiring all nodes except those at the ends of the bus to have the capability to transmit in, and receive from, two directions in order for all nodes to communicate with all other nodes on the bus; i. e. , with intermediate nodes acting as repeaters or passive transparent nodes. Note: The failure of a single transmission line (channel) linking any two nodes will result in the isolation of a minimum of one node from the rest of the network. (~) See also ring network, star topology, tree topology.

#-Business Aspects Of Information Security#

These aspects include protection of commercial proprietary information (eg, preliminary sales figures, strategic alliances, corporate plans and procedures, marketing strategies and end product development), the loss, alteration or destruction of which could adversely affect a business entity's financial stability or growth potential. (Source: Panel of experts).

Busy Back

Deprecated term. See busy signal.

-Busy-Wait

vi. Used of human behavior, conveys that the subject is busy waiting for someone or something, intends to move instantly as soon as it shows up, and thus cannot do anything else at the moment. “Can't talk now, I'm busy-waiting till Bill gets off the phone. ” Technically, `busy-wait' means to wait on an event by spinning through a tight or timed-delay loop that polls for the event on each pass, as opposed to setting up an interrupt handler and continuing execution on another part of the task. This is a wasteful technique, best avoided on time-sharing systems where a busy-waiting program may hog the processor.

-Buzz

1. vi. Of a program, to run with no indication of progress and perhaps without guarantee of ever finishing; esp. said of programs thought to be executing tight loops of code. A program that is buzzing appears to be catatonic, but never gets out of catatonia, while a buzzing loop may eventually end of its own accord. “The program buzzes for about 10 seconds trying to sort all the names into order. ” See spin; see also grovel.
2. [ETA Systems] To test a wire or printed circuit trace for continuity by applying an AC rather than DC signal. Some wire faults will pass DC tests but fail a buzz test.
3. To process an array or list in sequence, doing the same thing to each element. “This loop buzzes through the tz array looking for a terminator type. ”

-By Hand

1. adv. Said of an operation (especially a repetitive, trivial, and/or tedious one) that ought to be performed automatically by the computer, but which a hacker instead has to step tediously through. “My mailer doesn't have a command to include the text of the message I'm replying to, so I have to do it by hand. ” This does not necessarily mean the speaker has to retype a copy of the message; it might refer to, say, dropping into a subshell from the mailer, making a copy of one's mailbox file, reading that into an editor, locating the top and bottom of the message in question, deleting the rest of the file, inserting `>' characters on each line, writing the file, leaving the editor, returning to the mailer, reading the file in, and later remembering to delete the file. Compare eyeball search.
2. By extension, writing code which does something in an explicit or low-level way for which a pre-supplied library routine ought to have been available. “This cretinous B-tree library doesn't supply a decent iterator, so I'm having to walk the trees by hand. ”

Byte

/bi:t/ n. [techspeak] A unit of memory or data equal to the amount used to represent one character; on modern architectures this is usually 8 bits, but may be 9 on 36-bit machines. Some older architectures used `byte' for quantities of 6 or 7 bits, and the PDP-10 supported `bytes' that were actually bitfields of 1 to 36 bits! These usages are now obsolete, and even 9-bit bytes have become rare in the general trend toward power-of-2 word sizes. Historical note The term was coined by Werner Buchholz in 1956 during the early design phase for the IBM Stretch computer; originally it was described as 1 to 6 bits (typical I/O equipment of the period used 6-bit chunks of information). The move to an 8-bit byte happened in late 1956, and this size was later adopted and promulgated as a standard by the System/360. The word was coined by mutating the word `bite' so it would not be accidentally misspelled as bit. See also nybble.

C

-C

1. n. The third letter of the English alphabet.
2. ASCII 1000011.
3. The name of a programming language designed by Dennis Ritchie during the early 1970s and immediately used to reimplement UNIX; so called because many features derived from an earlier compiler named `B' in commemoration of *its* parent, BCPL. (BCPL was in turn descended from an earlier ALGOL-derived language, CPL. ) Before Bjarne Stroustrup settled the question by designing C++, there was a humorous debate over whether C's successor should be named `D' or `P'. C became immensely popular outside Bell Labs after about 1980 and is now the dominant language in systems and microcomputer applications programming. See also languages of choice, indent style. C is often described, with a mixture of fondness and disdain varying according to the speaker, as “a language that combines all the elegance and power of assembly language with all the readability and maintainability of assembly language”.

-C Programmer's Disease

n. The tendency of the undisciplined C programmer to set arbitrary but supposedly generous static limits on table sizes (defined, if you're lucky, by constants in header files) rather than taking the trouble to do proper dynamic storage allocation. If an application user later needs to put 68 elements into a table of size 50, the afflicted programmer reasons that he or she can easily reset the table size to 68 (or even as much as 70, to allow for future expansion) and recompile. This gives the programmer the comfortable feeling of having made the effort to satisfy the user's (unreasonable) demands, and often affords the user multiple opportunities to explore the marvelous consequences of fandango on core. In severe cases of the disease, the programmer cannot comprehend why each fix of this kind seems only to further disgruntle the user.

C-Language

A general-purpose, structured programming language, originally designed for and implemented on the UNIXTM operating system.

C4 Systems Security Vulnerability Reporting Program

(CVRP) Air Force program which implements the National-level reporting requirements of the Computer Security Technical Vulnerability Reporting Program (CSTVRP) as well as integrate COMPUSEC, TEMPEST, and COMSEC under a single threat driven program. The CVRP combines administrative controls, reporting procedures, specially developed software, and research and development efforts directed at known risks to Air Force communications and computer systems.

#-Cabling#

An assembly of electrical conductors insulated from each other but laid upon each other used to interconnect pieces of electrical equipment. (Source: Panel of Experts, July 1994).

Cache

Cache Memory

A special buffer storage, smaller and faster than main storage, that is used to hold a copy of instructions and data in main storage that are likely to be needed next by the processor, and that have been obtained automatically from main storage. (FP) (ISO)

Call

1. Any demand to set up a connection.
2. A unit of traffic measurement. (~) See also message.
3. In communications, the action performed by the calling party, or the operations necessary in making a call, or the effective use made of a connection between two stations.

Call Back

1. A procedure for identifying a remote terminal. The host system will disconnect the caller and then dial the authorized telephone number of the remote terminal to re-establish the connection. (*NCSC-WA*-001-85;; *AR* 380-380;)
2. Procedure where the system (after identifying the caller) disconnects the call and dials the caller's computer. Used in an attempt to ensure both the identity and location of the caller. (BBD;)
3. A procedure for identifying a remote terminal In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to re-establish the connection. (*NCSC-TG*-004-88)
4. Synonymous with DIAL BACK.

Call Forwarding

A service feature available in some switching systems where calls can be rerouted automatically from one line, i. e. , station number, to another or to an attendant. Note: This feature may be implemented in many forms. See also service feature, switching center.

Call Hold

A service feature, available in some switching systems, that permits a user to retain an existing call to accept or originate a second call using the same facilities. See also service feature.

Call Identifier

A network utility that is an identifying name assigned by the originating network for each established or

partially established virtual call and, when used in conjunction with the calling DTE address, uniquely identifies the virtual call over a period of time. See also data terminal equipment, virtual call.

Call Processing

Call Set-Up Time

Call Sign Cipher

1. Cryptosystem used to encipher/decipher call signs, address groups, and address indicating groups.
2. Canister Type of protective package used to contain and dispense key in punched or printed tape form.
3. Capability Unforgeable ticket that provides incontestable proof that the presenter is authorized access to the object named in the ticket.

#-Call-Back Security#

Procedure for identifying a remote AIS terminal, whereby the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to re-establish the connection. (Source: NSTISSI 4009).

Called-Party Camp-On

#-Caller ID#

1. A feature which lets the receiver of a call see the phone number of the caller before the call is answered. The number will appear on a display unit after the first ring. Caller ID requires additional equipment and a display unit. (Panel of Experts, July 1994);
2. AKA Automatic Number Identification (ANI) a technology that allow's a telephone caller's number to be displayed on the telephone instrument of the called party. (%).

Calling-Party Camp-On

Callsign

Any combination of characters or pronounceable words, which identifies a communication facility, a command, an authority, an activity, or a unit; used primarily for establishing and maintaining communications. (JP 1-02)

Callsign Cipher

Cryptosystem used to encipher or decipher callsigns, address groups, and address indicating groups.

CAMA

Acronym for Centralized Automatic Message Accounting.

Camp-On

Colloquial synonym for automatic callback.

Can

1. Abbreviation for cancel character.
2. vt. To abort a job on a time-sharing system. Used esp. when the person doing the deed is an operator, as in “canned from the console”. Frequently used in an imperative sense, as in “Can that print job, the LPT just popped a sprocket!” Synonymous with gun. It is said that the ASCII character with mnemonic CAN (0011000) was used as a kill-job character on some early OSes. Alternatively, this term may derive from mainstream slang `canned' for being laid off or fired.

-Can't Happen

The traditional program comment for code executed under a condition that should never be true, for example a file size computed as negative. Often, such a condition being true indicates data corruption or a faulty algorithm; it is almost always handled by emitting a fatal error message and terminating or crashing, since there is little else that can be done. Some case variant of “can't happen” is also often the text emitted if the `impossible' error actually happens! Although “can't happen” events are genuinely infrequent in production code, programmers wise enough to check for them habitually are often surprised at how frequently they are triggered during development and how many headaches checking for them turns out to head off. See also firewall code (sense2) .

Cancel Character

1. A control character used by some convention to indicate that the data with which it is associated are in error or are to be disregarded. (FP)
2. An accuracy control character used to indicate that the data with which it is associated are in error, are to be disregarded, or cannot be represented on a particular device. (FP) See also control character.

-Candygrammar

n. A programming-language grammar that is mostly syntactic sugar; the term is also a play on `candygram'. COBOL, Apple's Hypertalk language, and a lot of the so-called `4GL' database languages share this property. The usual intent of such designs is that they be as English-like as possible, on the theory that they will then be easier for unskilled people to program. This intention comes to grief on the reality that syntax isn't what makes programming hard; it's the mental effort and organization required to specify an algorithm precisely that costs. Thus the invariable result is that `candygrammar' languages are just as difficult to program in as terser ones, and far more painful for the experienced hacker.

Canister

Type of protective package used to contain and dispense key in punched or printed tape form.

-Canonical

1. adj. [historically, `according to religious law'] The usual or standard state or manner of something. This word has a somewhat more technical meaning in mathematics. Two formulas such as 9 + x and x + 9 are said to be equivalent because they mean the same thing, but the second one is in `canonical form' because it is written in the usual way, with the highest power of x first. Usually there are fixed rules you can use to decide whether something is in canonical form.
2. The jargon meaning, a relaxation of the technical meaning, acquired its present loading in computer-science culture largely through its prominence in Alonzo Church's work in computation theory and mathematical logic (see Knights of the Lambda Calculus). Compare vanilla. This word has an interesting history. Non-technical academics do not use the adjective `canonical' in any of the senses defined above with any regularity; they do however use the nouns `canon' and `canonicity' (not **canonicalness or **canonicality). The `canon' of a given author is the complete body of authentic works by that author (this usage is familiar to Sherlock Holmes fans as well as to literary scholars). `*The* canon' is the body of works in a given field (e. g. , works of literature, or of art, or of music) deemed worthwhile for students to study and for scholars to investigate. The word `canon' derives ultimately from the Greek `kanon' (akin to the English `cane') referring to a reed. Reeds were used for measurement, and in Latin and later Greek the word `canon' meant a rule or a standard. The establishment of a canon of scriptures within Christianity was meant to define a standard or a rule for the religion. The above non-techspeak academic usages stem from this instance of a defined and accepted body of work. Alongside this usage was the promulgation of `canons' (`rules') for the government of the Catholic Church. The techspeak usages (“according to religious law”) derive from this use of the Latin `canon'. Hackers invest this term with a playfulness that makes an ironic contrast with its historical meaning. A true story One Bob Sjoberg, new at the MIT AI Lab, expressed some annoyance at the incessant use of jargon. Over his loud objections, GLS and RMS made a point of using as much of it as possible in his presence, and eventually it began to sink in. Finally, in one conversation, he used the word `canonical' in jargon-like fashion without thinking. Steele “Aha! We've finally got you talking jargon too!” Stallman “What did he say?” Steele “Bob just used `canonical' in the canonical way. ” Of course, canonicality depends on context, but it is implicitly defined as the way *hackers* normally expect things to be. Thus, a hacker may claim with a straight face that `according to religious law' is *not* the canonical meaning of `canonical'.

Capability

1. In a computer system, an unforgeable ticket that is accepted by the system as incontestable proof that the presenter has authorized access to the object named by the ticket. It is often interpreted by the operating system and the hardware as an address for the object. Each capability also contains authorization information identifying the nature of the access mode (for example read mode, write mode). (MTR-8201;);
2. A protected identifier that both identifies the object and specifies the access rights to be allowed to the accessor who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be accessor possesses a capability for the object.

Capability-Based

AIS in which access to protected objects system is granted if the subject possesses a capability for the object.

Capability-Based System

AIS in which access to protected objects is granted if the subject possesses a capability for the object.

*-Card Walloper

n. An EDP programmer who grinds out batch programs that do stupid things like print people's paychecks. Compare code grinder. See also punched card, eighty-column mind.

#-Careless Employees

Negligent workers who may cause unintentional harm to information technology systems. Considered a threat to information systems due to the fact that they are “insiders” and are authorized users of the systems; they may perform acts harmful to the system or information processed, stored or transmitted by the system. (Source: Panel of Experts, July 1994).

*-Careware

/keir'weir/ n. A variety of shareware for which either the author suggests that some payment be made to a nominated charity or a levy directed to charity is included on top of the distribution charge. Syn. charityware; compare crippleware, sense 2.

*-Cargo Cult Programming

1. n. A style of (incompetent) programming dominated by ritual inclusion of code or program structures that serve no real purpose. A cargo cult programmer will usually explain the extra code as a way of working around some bug encountered in the past, but usually neither the bug nor the reason

the code apparently avoided the bug was ever fully understood (compare shotgun debugging, voodoo programming).

2. The term `cargo cult' is a reference to aboriginal religions that grew up in the South Pacific after World War II. The practices of these cults center on building elaborate mockups of airplanes and military style landing strips in the hope of bringing the return of the god-like airplanes that brought such marvelous cargo during the war. Hackish usage probably derives from Richard Feynman's characterization of certain practices as “cargo cult science” in his book “Surely You're Joking, Mr. Feynman” (W. W. Norton & Co, New York 1985, ISBN 0-393-01921-7).

Carrier

Synonym common carrier.

Carrier Sense Multiple Access With Collision Detection (CSMA/CD)

A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (FP) (ISO) See also local area network.

*-Cascade

1. n. A huge volume of spurious error-message output produced by a compiler with poor error recovery. Too frequently, one trivial syntax error (such as a missing `)' or `') throws the parser out of synch so that much of the remaining program text is interpreted as garbaged or ill-formed.
2. A chain of Usenet followups, each adding some trivial variation or riposte to the text of the previous one, all of which is reproduced in the new message; an include war in which the object is to create a sort of communal graffito.

Cascading

Downward flow of information across a range of security levels that is greater than the accreditation range of a component part of a network. An example is causing Top Secret data to flow through a network such that it comes to reside in a network component not accredited for Top Secret data and not protected as required.

*-Case And Paste

n. [from `cut and paste'] 1. The addition of a new feature to an existing system by selecting the code from an existing feature and pasting it in with minor changes. Common in telephony circles because most operations in a telephone switch are selected using `case' statements. Leads to software bloat. In some circles of EMACS users this is called `programming by Meta-W', because Meta-W is the EMACS command for copying a block of text to a kill buffer in preparation to pasting it in elsewhere. The term is condescending, implying that the programmer is acting mindlessly rather than thinking carefully about what is required to integrate the code for two similar cases. At DEC, this is sometimes called `clone-and-hack' coding.

*-Casters-Up Mode

n. [prob. fr. slang belly up] Yet another synonym for `broken' or `down'. Usually connotes a major failure. A system (hardware or software) which is `down' may be already being restarted before the failure is noticed, whereas one which is `casters up' is usually a good excuse to take the rest of the day off (as long as you're not responsible for fixing it).

*-Cat

1. [from `catenate' via UNIX `cat(1)'] vt.
2. [techspeak] To spew an entire file to the screen or some other output sink without pause.
3. By extension, to dump large amounts of data at an unprepared target or with no intention of browsing it carefully. Usage considered silly. Rare outside UNIX sites. See also dd, BLT. Among UNIX fans, `cat(1)' is considered an excellent example of user-interface design, because it delivers the file contents without such verbosity as spacing or headers between the files, and because it does not require the files to consist of lines of text, but works with any sort of data. Among UNIX haters, `cat(1)' is considered the canonical example of *bad* user-interface design, because of its woefully unobvious name. It is far more often used to blast a file to standard output than to concatenate two files. The name `cat' for the former operation is just as unintuitive as, say, LISP's cdr. Of such oppositions are holy wars made.

Catastrophe

An event which causes significant restructuring of an environment. (MK;)

*-Catatonic

adj. Describes a condition of suspended animation in which something is so wedged or hung that it makes no response. If you are typing on a terminal and suddenly the computer doesn't even echo the letters back to the screen as you type, let alone do what you're asking it to do, then the computer is suffering from catatonia (possibly because it has crashed). “There I was in the middle of a winning game of nethack and it went catatonic on me! Aaargh!”

Categories Of Data

In the context of perception management and its constituent approaches: Data obtained by adversary individuals, groups, intelligence systems, and officials are categorized in two ways: (1) Information A compilation of data provided by secret or open sources that would provide a substantially complete picture of

friendly intentions, capabilities, or activities. (2) Indicators. Data derived from open sources or from detectable actions that adversaries can piece together or interpret to reach personal conclusions or official estimates concerning friendly intentions, capabilities, or activities NOTE: For OPSEC purposes, actions that convey indicators exploitable by adversaries, but that must be carried out regardless to plan, prepare for, and execute activities, are called “observables. ”

Category

A restrictive label that has been applied to both classified and unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data.

1. NOTE: Examples include sensitive compartmented information, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special category information only after being granted formal access authorization. (NISTIR-4659)
2. Restrictive labels that have been applied to classified or unclassified data as a means of increasing the protection of and further restricting access to the data. Examples include Sensitive Compartmented Information (SCI), Proprietary Information (PROPIN), and NATO. Individuals may be given access to this information only if they have been granted formal access authorization. (*AFR* 205-16;)
3. A grouping of classified or unclassified but sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have appropriate authorization (CSC-STD-003-85;)
4. A grouping of classified or unclassified but sensitive information, to which an additional restrictive label is applied (e. g. , proprietary, compartmented information). (CSC-STD-004-85;)
5. A restrictive label that has been applied to classified or unclassified data as a means of increasing the protection of and further restricting access to the data. (*NCSC-WA*-001-85;)
6. A grouping of classified or unclassified sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have formal access approval or other appropriate authorization (e. g. , proprietary information, For Official Use Only (FOUO), Compartmented Information). (DODD 5200. 28;)
7. A grouping of information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have appropriate authorization (e. g. , Restricted Data [RD]). (DOE 5636. 2A;)

Caution Statement

1. A statement affixed to computer outputs which contains the highest classification being processed at the time the product was produced and a requirement that any data not requested be controlled at that level and returned immediately to the originating computer center. (*AR* 380-380;)
2. See SAFEGUARDING STATEMENT.

Caveats

See Special Markings.

CCI Assembly

Device embodying a cryptographic logic or other COMSEC design that the National Security Agency has approved as a controlled cryptographic item and performs the entire COMSEC function, but is dependent upon the host equipment to operate.

CCI Component

Device embodying a cryptographic logic or other COMSEC design, which the National Security Agency has approved as a controlled cryptographic item, that does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete and operate the COMSEC function.

CCI Equipment

Telecommunications or information handling equipment that embodies a controlled cryptographic item component or controlled cryptographic item assembly and performs the entire COMSEC function without dependence on a host equipment to operate.

*-Cd Tilde

/C-D til-d*/ vi. To go home. From the UNIX C-shell and Korn-shell command `cd ~', which takes one to one's `$HOME' (`cd' with no arguments happens to do the same thing). By extension, may be used with other arguments; thus, over an electronic chat link, `cd ~coffee' would mean “I'm going to the coffee machine. ”

CDR

1. Critical Design Review.
2. /ku'dr/ or /kuh'dr/ vt. [from LISP] To skip past the first item from a list of things (generalized from the LISP operation on binary tree structures, which returns a list consisting of all but the first element of its argument). In the form `cdr down', to trace down a list of elements “Shall we cdr down the agenda?” Usage silly. See also loop through. Historical note The instruction format of the IBM 7090 that hosted the original LISP implementation featured two 15-bit fields called the `address' and `decrement' parts. The term `cdr' was originally `Contents of Decrement part of Register'. Similarly, `car' stood for `Contents of Address part of Register'. The cdr and car operations have since become bases for formation of compound metaphors in non-LISP contexts. GLS recalls, for

example, a programming project in which strings were represented as linked lists; the get-character and skip-character operations were of course called CHAR and CHDR.

Cell

1. In cellular radio, the smallest geographic area defined for certain mobile communication systems. Note: Each cell has its own base station and a single controller interconnected with the public telephone network.
2. In OSI, a fixed-length block labeled at the Physical Layer of the Open Systems Interconnection Reference Model.
3. In computer systems, an addressable, internal hardware location.
4. In computer systems, a single location on a spreadsheet.
5. A group of individuals operating as part of a larger, unknown, group. Frequently for malicious intent.

Central Computer Facility

One or more computers with their peripherals and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links. (*DCID* 1/16-1;)

Central Office Of

Office of a federal department or agency record that keeps records of accountable COMSEC material held by elements subject to its oversight.

Central Office Of Record

(COR) Office of a federal department or agency that keeps records of accountable COMSEC material held by elements subject to its oversight. (AF9K_JBC. TXT)

Central Processing Unit

(CPU) Computer component with the circuitry to control the interpretation and execution of instructions. The CPU includes arithmetic-logic and control sections. (F:\NEWDEFS. TXT)

Central Processor

Synonym central processing unit.

Certificate Of Action

Statement attached to a COMSEC audit statement report by which a COMSEC custodian certifies that all actions have been completed.

Certificate Of Action Statement

Statement attached to a COMSEC audit report by which a COMSEC manager certifies that all actions have been completed.

Certification

1. A statement that specifies the extent to which the security measures meet specifications. Certification is based on the results of the risk analysis performed. It does not necessarily imply a guarantee that the described system is impenetrable. It is an input to the security approval process. (*AFR* 205-16;)
2. A statement based on detailed technical analysis that specifies the extent to which the security measures in the system or facility meet the security requirements. Certification is based on the results of the risk analysis performed. It does not necessarily imply a guarantee that the described system is impenetrable. It is an input to the security accreditation process. (*AFR* 700-10;)
3. The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements. (CSC-STD-001-83;)
4. The technical evaluation of an AIS's security features and other safeguards, made as part of and in support of the accreditation process, that establishes the extent to which a particular AIS design and implementation meet a set of specified security requirements. (DODD 5200. 28;)
5. An individual's formal written assurance that, based on evaluation of security tests, the classified ADP system and its environment meet the approved security specifications outlined by the ADP Security Plan (DOE 5636. 2A;)
6. The technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which the design and implementation of a computer system or network meet prespecified security requirements. (*FIPS PUB* 39;; *AR* 380-380;)
7. The resulting decision attesting to the system's ability to meet the specified security requirements. This decision is in support of the accreditation process and is based on the finding of a technical evaluation. (*NCSC-WA*-001-85;)
8. The technical process evaluation, made as part of and in support of the accreditation process, whereby a procedure, program, system, component, or system is shown to be secure; i. e. , that the security design specifications are correct and have been properly implemented. Certification is performed by independent technical personnel according to an acceptable standard of proof such that the level of security protection is identified with regard to a procedure, program, system component, or system. (*OPNAVINST* 5239. 1A;)
9. A reasonable assurance (based on a technical evaluation of a system test) and written acknowl-

edgment made by a CPPM, or an individual designated by the CPPM, that a proposed unclassified computer application processing sensitive information meets all applicable federal and departmental policies, regulations, and procedures, and that results of a systems test demonstrate installed security safeguards are adequate and functioning properly. (*DOE 1360. 2A*) 10) The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements. (*NCSC-TG*-004-88)

Certification And Accreditation Program

A program designed to ensure that critical decisions regarding the adequacy of Automated Information System security safeguards are made by authorized managers based on reliable technical information. (*NCSC-WA*-001-85;)

Certified TEMPEST

U. S. Government or U. S. Government technical authority contractor employee designated to review the TEMPEST countermeasures programs of a federal department or agency.

Certified Tempest Technical Authority

(CTTA) U. S. Government or U. S. Government contractor employee designated to review the TEMPEST countermeasures programs of a federal department or agency. NOTE: A CTTA is required to be an experienced, technically qualified individual who has met established certification requirements in accordance with NTISSC-approved criteria.

Chad

1. /chad/ n. The perforated edge strips on printer paper, after they have been separated from the printed portion. Also called selvage and perf.
2. obs. The confetti-like paper bits punched out of cards or paper tape; this has also been called `chaff', `computer confetti', and `keypunch droppings'. This use may now be mainstream; it has been reported seen (1993) in directions for a card-based voting machine in California. Historical noteOne correspondent believes `chad' (sense
3. derives from the Chadless keypunch (named for its inventor), which cut little u-shaped tabs in the card to make a hole when the tab folded back, rather than punching out a circle/rectangle; it was clear that if the Chadless keypunch didn't make them, then the stuff that other keypunches made had to be `chad'. There is an legend that the word was originally acronymic, standing for “Card Hole Aggregate Debris”, but this has all the earmarks of a bogus folk etymology.
4. Source of doisputed voting anomalies in Florida

*-Chad Box

1. n. A metal box about the size of a lunchbox (or in some models a large wastebasket), for collecting the chad (sense
2. that accumulated in Iron Age card punches. You had to open the covers of the card punch periodically and empty the chad box. The bit bucket was notionally the equivalent device in the CPU enclosure, which was typically across the room in another great gray-and-blue box.

Chad Tape

Punched tape used in telegraphy/teletypewriter operation. The perforations, called “chad,” are severed from the tape, making holes representing the characters. (~) See also reperforator, tape relay.

Chadless Tape

1. Punched tape that has been punched in such a way that chad is not formed.
2. A punched tape wherein only partial perforation is completed and the chad remains attached to the tape. (~) Note: This is a deliberate process and should not be confused with imperfect chadding. See also reperforator, tape relay.

*-Chain

1. vi. [orig. from BASIC's `CHAIN' statement] To hand off execution to a child or successor without going through the OS command interpreter that invoked it. The state of the parent program is lost and there is no returning to it. Though this facility used to be common on memory-limited micros and is still widely supported for backward compatibility, the jargon usage is semi-obsolescent; in particular, most UNIX programmers will think of this as an exec. Oppose the more modern `subshell'.
2. n. A series of linked data areas within an operating system or application. `Chain rattling' is the process of repeatedly running through the linked data areas searching for one which is of interest to the executing program. The implication is that there is a very large number of links on the chain.

Challenge And Reply

Prearranged procedure in which authenticationone communicator requests authentication of another and the latter establishes his/her validity with a correct reply.

Challenge And Reply Authentication

Prearranged procedure in which one communicator requests authentication of another and the latter establishes his/her validity with a correct reply.

#-Change Control Policies

Written guidance for implementation of change control. (Source: Panel of Experts, July 1994).

#-Change Controls

A management tool to provide control and traceability for all changes made to the system. Changes in progress are able to be monitored through configuration status accounting information in order to control the change and to evaluate its impact on other parts of the system. (Source: Panel of Experts, July 1994)

Channel

An information transfer path within a system. May also refer to the mechanism by which the path is effected. (CSC-STD-001-83;)

*-Channel Hopping

n. [IRC, GEnie] To rapidly switch channels on IRC, or a GEnie chat board, just as a social butterfly might hop from one group to another at a party. This term may derive from the TV watcher's idiom, `channel surfing'.

*-Channel Op

/chan'l op/ n. [IRC] Someone who is endowed with privileges on a particular IRC channel; commonly abbreviated `chanop' or `CHOP'. These privileges include the right to kick users, to change various status bits, and to make others into CHOPs.

*-Char

/keir/ or /char/; rarely, /kar/ n. Shorthand for `character'. Esp. used by C programmers, as `char' is C's typename for character data.

Character

1. A letter, digit, or other symbol that is used as part of the organization, control, or representation of data. (~)
2. One of the units of an alphabet. (~)

Character Check

A method of error detection using the preset rules for the formulation of characters. (~) See also character, cyclic redundancy check, error control, parity.

Character Generator

A functional unit that converts the coded representation of a character into the graphic representation of the character for display. (FP) (ISO)

Character Interval

The total number of unit intervals (including synchronizing, information, error checking, or control bits) required to transmit any given character in any given communication system. Extra signals that are not associated with individual characters are not included. Note: An example of an extra signal that is excluded in the above definition is any additional time added between the end of the stop element and the beginning of the next start element as a result of a speed change, buffering, etc. This additional time is defined as a part of the intercharacter interval. See also character, intercharacter interval, unit interval.

Character Recognition

The identification of characters by automatic means. (FP) (ISO)

Character Set

1. A finite set of different characters that is complete for a given purpose. (FP) (ISO) (~) Note 1: Examples are: each of the character sets in ISO Recommendation R646, 6- and 7-bit Coded Character Sets for Information Processing Interchange. Note 2: A character set may or may not include punctuation marks or other symbols.
2. An ordered set of unique representations called characters. (~) Note: Examples are: the 26 letters of the English alphabet, Boolean 0 and 1, and the 128 ASCII characters. See also alphabet, alphanumeric, binary digit, character, code, coded character set, coded set, digital alphabet, language.

Character Stepped

A form of operational control of start-stop teletypewriter equipment in which a device is stepped one character at a time. (~) Note: The step interval is equal to or greater than the character interval at the applicable signaling rate. See also bit-stepped, character.

Character-Count

Character-Count And Bit-Count Integrity

The preservation of the precise number of characters or bits that are originated per message or per unit time. (~) Note: Not to be confused with bit integrity or character integrity, which require that the characters or bits delivered are, in fact, as they were originated. See also added bit, binary digit, bit error ratio, bit inversion, bit slip, character, deleted bit, digital error, error.

*-Chase Pointers

1. vi. To go through multiple levels of indirection, as in traversing a linked list or graph structure. Used esp. by programmers in C, where explicit pointers are a very common data type. This is techspeak, but it remains jargon when used of human networks. “I'm chasing pointers. Bob said you could tell me who to talk to about. ” See dangling pointer and snap.
2. [Cambridge] `pointer chase' or `pointer hunt' The process of going through a core dump (sense 1), interactively or on a large piece of paper printed with hex runes, following dynamic data-structures. Used only in a debugging context.

*-Chawmp

n. [University of Florida] 16 or 18 bits (half of a machine word). This term was used by FORTH hackers during the late 1970s/early 1980s; it is said to have been archaic then, and may now be obsolete. It was coined in revolt against the promiscuous use of `word' for anything between 16 and 32 bits; `word' has an additional special meaning for FORTH hacks that made the overloading intolerable. For similar reasons, /gaw'bl/ (spelled `gawble' or possibly `gawbul') was in use as a term for 32 or 48 bits (presumably a full machine word, but our sources are unclear on this). These terms are more easily understood if one thinks of them as `chomp' and `gobble' pronounced in a Florida or other Southern U. S. dialect. For general discussion of similar terms, see nybble.

Check

1. A process for determining accuracy. (FP)
2. n. A hardware-detected error condition, most commonly used to refer to actual hardware failures rather than software-induced traps. E. g. , a `parity check' is the result of a hardware-detected parity error. Recorded here because the word often humorously extended to non-technical problems. For example, the term `child check' has been used to refer to the problems caused by a small child who is curious to know what happens when s/he presses all the cute buttons on a computer's console (of course, this particular problem could have been prevented with molly-guards).

Check Bit

A binary digit used for error detection, for example, a parity bit. (~) See also binary digit, error, error control, overhead information, parity check, redundancy check.

Check Character

A single character, derived from and appended to a data item, that can be used to detect errors in processing or transmitting a data item. (~) See also character, overhead information, parity check.

Check Digit

A single digit, derived from and appended to a data item, that can be used to detect errors in processing or transmitting a data item. (~) See also overhead information, parity check.

Check Word

Cipher text generated by a cryptographic logic to detect failures in the cryptography.

Checksum

Value computed, via some parity or hashing algorithm, on information requiring protection against error or manipulation. NOTE: Checksums are stored or transmitted with data and are intended to detect data integrity problems. See Hash Total and Integrity Check Value.

*-Chernobyl Packet

/cher-noh'b*l pak'*t/ n. A network packet that induces a broadcast storm and/or network meltdown, in memory of the April 1986 nuclear accident at Chernobyl in Ukraine. The typical scenario involves an IP Ethernet datagram that passes through a gateway with both source and destination Ether and IP address set as the respective broadcast addresses for the subnetworks being gated between. Compare Christmas tree packet.

*-Chiclet Keyboard

n. A keyboard with a small, flat rectangular or lozenge-shaped rubber or plastic keys that look like pieces of chewing gum. (Chiclets is the brand name of a variety of chewing gum that does in fact resemble the keys of chiclet keyboards.) Used esp. to describe the original IBM PCjr keyboard. Vendors unanimously liked these because they were cheap, and a lot of early portable and laptop products got launched using them. Customers rejected the idea with almost equal unanimity, and chiclets are not often seen on anything larger than a digital watch any more.

*-Chine Nual

/sheen'yu-*l/ n. ,obs. [MIT] The LISP Machine Manual, so called because the title was wrapped around the cover so only those letters showed on the front.

*-Choke

1. v. To reject input, often ungracefully. “NULs make System V's `lpr(1)' choke. ” “I tried building an EMACS binary to use X, but `cpp(1)' choked on all those `#define's. ” See barf, gag, vi.
2. [MIT] More generally, to fail at any endeavor, but with some flair or bravado; the popular definition is “to snatch defeat from the jaws of victory. ”

*-Chomp

vi. To lose; specifically, to chew on something of which more was bitten off than one can. Probably related to gnashing of teeth. See bagbiter. A hand gesture commonly accompanies this. To perform it, hold the four fingers together and place the thumb against their tips. Now open and close your hand rapidly to suggest a biting action (much like what Pac-Man does in the classic video game, though this pantomime seems to predate that). The gesture alone means `chomp chomp' (see “Verb Doubling” in the “Jargon Construction” section of the Prependices). The hand may be pointed at the object of complaint, and for real emphasis you can use both hands at once. Doing this to a person is equivalent to saying “You chomper!” If you point the gesture at yourself, it is a humble but humorous admission of some failure. You might do this if someone told you that a program you

had written had failed in some surprising way and you felt dumb for not having anticipated it.

*-CHOP

/chop/ n. [IRC] See channel op.

*-Christmas Tree

n. A kind of RS-232 line tester or breakout box featuring rows of blinking red and green LEDs suggestive of Christmas lights.

*-Christmas Tree Packet

n. A packet with every single option set for whatever protocol is in use. See kamikaze packet, Chernobyl packet. (The term doubtless derives from a fanciful image of each little option bit being represented by a different-colored light bulb, all turned on.)

*-Chrome

n. [from automotive slang via wargaming] Showy features added to attract users but contributing little or nothing to the power of a system. “The 3D icons in Motif are just chrome, but they certainly are *pretty* chrome!” Distinguished from bells and whistles by the fact that the latter are usually added to gratify developers' own desires for featurefulness. Often used as a term of contempt.

*-Chug

vi. To run slowly; to grind or grovel. “The disk is chugging like crazy. ”

*-Cinderella Book

[CMU] n. “Introduction to Automata Theory, Languages, and Computation”, by John Hopcroft and Jeffrey Ullman, (Addison-Wesley, 1979). So called because the cover depicts a girl (putatively Cinderella) sitting in front of a Rube Goldberg device and holding a rope coming out of it. On the back cover, the device is in shambles after she has (inevitably) pulled on the rope. See also book titles.

Cipher

Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text of regular length, usually single letters, or in which units of plain text are rearranged, or both, according to certain predetermined rules. (JP 1-02)

Cipher System

A cryptosystem in which the cryptographic treatment is applied to plain text elements of equal length. (*AR* 380-380; *FIPS PUB* 39;)

Cipher Text

(1) Enciphered information. ; (2) Unintelligible text or signals produced through the use of cipher systems. (*AR* 380-380;; *FIPS PUB* 39;)

Cipher Text Auto-Key

(CTAK) Cryptographic logic which uses previous cipher text to generate a key stream.

Ciphony

Process of enciphering audio information, resulting in encrypted speech.

Circuit

1. The complete path between two terminals over which one-way or two-way communications may be provided. (~)
2. An electronic path between two or more points, capable of providing a number of channels. (JCS1-DoD)
3. A number of conductors connected together for the purpose of carrying an electrical current. (JCS1-DoD)
4. An electronic closed-loop path among two or more points used for signal transfer. (~)

Circuit Breaker

A protective device for opening and closing a circuit between separable contacts under both normal and abnormal conditions. (~) Note: Circuit breakers may be of many types and sizes, and are usually classified according to the medium in which the interruption takes place; e. g. , oil (or other liquid), or air (or other gas). See also circuit, disconnect switch, protector, switch (def. #1).

#-Circuit-Switched Networks

Networks in which a connection is established on demand and maintained between data stations in order to allow the exclusive use of a data circuit until the connection is released. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Cladding

1. When referring to an optical fiber, a layer of material of lower refractive index, in intimate contact with a core material of higher refractive index. (~)
2. When referring to a metallic cable, a process of covering with a metal (usually achieved by pressure rolling, extruding, drawing, or swaging) until a bond is achieved. (~) See also cable, core, deeply depressed cladding fiber, depressed cladding fiber, doubly clad fiber, fiber optics, multimode optical fiber, normalized frequency, optical fiber, single-mode optical fiber, tolerance field.

Clandestine Operation

Activities to accomplish intelligence, counterintelligence, or similar activities in such a way as to maintain secrecy or concealment, especially for the purpose of deception or subversion. *A preplanned secret intelligence collection activity or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses both clandestine collection and covert action (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Class

1. A set of conceptual entities (individuals or other classes). (ET;)
2. A set of conceptual entities. (MA;)
3. Hierarchical ranking that denotes a certain level of computer operating system trust based on DoD Standard 5200. 28. See below and also Trusted Computing Base (TCB). Class A1, Verified Design See Verified Design. Class B1, Labeled Security Protection See Labeled Security Protection (Class B1). Class B2, Structured Protection See Structured Protection (Class B2). Class B3, Security Domains See Security Domains (Class B3). Class C1, Discretionary Security Protection See Discretionary Security Protection (Class C1). Class C2, Controlled Access Protection See Controlled Access Protection (Class C2). Class D, Minimal Protection See Minimal Protection (Class D).

Class A1, Verified Design

See Verified Design.

Class B1, Labeled Security Protection

See Labeled Security Protection. Class B2, Structured Protection. See Structured Protection.

Class B3, Security Domains

See Security Domains.

Class C1, Discretionary Security Protection

See Discretionary Security Protection.

Class C2, Controlled Access Protection

See Controlled Access Protection.

Class D, Minimal Protection

See Minimal Protection.

*-Classic C

/klas'ik C/ [a play on `Coke Classic'] n. The C programming language as defined in the first edition of K&R, with some small additions. It is also known as `K&R C'. The name came into use while C was being standardized by the ANSI X3J11 committee. Also `C Classic'. An analogous construction is sometimes applied elsewhere thus, `X Classic', where X = Star Trek (referring to the original TV series) or X = PC (referring to IBM's ISA-bus machines as opposed to the PS/2 series). This construction is especially used of product series in which the newer versions are considered serious losers relative to the older ones.

Classification

A determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made. Data classification is used along with categories in the calculation of risk index. (CSC-STD-004-85;)

Classification Guide

Directions by appropriate authority which identify general categories of information requiring protection, the level of classification to be applied, and associated downgrading instructions. *This is a document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specific information to be classified on a derivative basis (DoD 5220. 22-M, Industrial Security Manual, 3/89)

Classified Computer Security Program

All of the technological safeguards and managerial procedures established and applied to ADP facilities and ADP systems (including computer hardware, software, and data) in order to ensure the protection of classified information. (DOE 5636. 2A;)

Classified Data/information

1. Information or material that is (a) owned by, produced for or by, or under the control of the U. S. Government; and (b) determined under E. O. 12356, or prior orders, *DOD* 5200. 1-R, to require protection against unauthorized disclosure; and (c) so designated. (DODD 5200. 28)
2. Top Secret, Secret, and Confidential information of all categories (RD, FRD, NSI, etc.), including intelligence information, for which the Department is responsible and requires safeguarding in the interest of national security and defence. (DOE 5636. 2A;)
3. Official data which has been determined to require protection in the interests of national security. (*OPNAVINST* 5239. 1A;)

Classified Defence Information

Official information which requires protection against unauthorized disclosures in the interest of the national security and which has been so designated in accordance with the provision of Executive Order 12356: Top Secret, Secret, Confidential. (*AR* 380-380;)

Classified Defense Information

Official information which requires protection against unauthorized disclosures in the interest of national security and which has been so designated in accordance with the provision of Executive Order 12356: Top Secret, Secret, Confidential. (*AR* 380-380)

Classified Information

Official information regarding national security designated Top Secret, Secret, or Confidential in accordance with Executive Order. *Official information regarding the national security which has been designated Top Secret, Secret, or Confidential in accordance with Executive Order 12356 (NSA, *National INFOSEC Glossary*, 10/88) *Information or material that is: (1) owned by, produced by or for, or under the

control of the U. S. Government; (2) determined under E. O. 12356 or prior orders to require protection against unauthorized disclosure; and (3) so designated (DoD 5220. 22-M, Industrial Security Manual, 3/89)

#-Classified Materials Handling And Shipping

A structured method of handling COMSEC material from birth to death, from production through distribution to the end user to eventual disposition or destruction.

*-Clean

1. adj. Used of hardware or software designs, implies `elegance in the small', that is, a design or implementation that may not hold any surprises but does things in a way that is reasonably intuitive and relatively easy to comprehend from the outside. The antonym is `grungy' or crufty.
2. v. To remove unneeded or undesired files in a effort to reduce clutter “I'm cleaning up my account. ” “I cleaned up the garbage and now have 100 Meg free on that partition. ”

Clear

To cause one or more storage locations to be in a prescribed state, usually that corresponding to a zero or that corresponding to the space character. (FP) (ISO)

Clear Channel

A signal path that provides its full bandwidth for a user's service. Note: No control or signaling is performed on this path. See also bandwidth.

Clear Text

Synonym plain text.

Clearance Level

#-Clearance Verification

The act of ensuring that a user has the proper security clearance, authorizations prior to granting access to a facility or information technology system. (Source: Panel of Experts, July 1994).

Clearing

1. The overwriting of classified information on magnetic media such that the media may be reused. (This does not lower the classification level of the media.) (DOE 5636. 2A;)
2. Note: Volatile memory can be cleared by removing power to the unit for a minimum of one minute. (DOE 5637. 1)
3. Removal of data from an AIS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (i. e. , through the keyboard).
4. NOTE: An AIS need not be disconnected from any external network before clearing takes place. Clearing enables a product to be reused within, but not outside of, a secure facility. It does not produce a declassified product by itself, but may be the first step in the declassification process.

Clearing ADP Media

A procedure used to erase the classified information stored on the media, but lacking the totality of a declassification procedure. (CSC-STD-005-85;)

Clearing Magnetic Media

A procedure used to erase the sensitive information stored on the media, but lacking the totality of a declassification procedure. (*NCSC-WA*-001-85;)

#-Client/Server Security

measures taken to protect a distributed information system that consists of workstations connected to a unit at a node of a network that provides specific services for network users. (Source: panel of experts).

*-Clobber

vt. To overwrite, usually unintentionally “I walked off the end of the array and clobbered the stack. ” Compare mung, scribble, trash, and smash the stack.

Clock

1. A reference source of timing information. (~)
2. A device providing signals used in a transmission system to control the timing of certain functions such as the duration of signal elements or the sampling rate. (~)
3. A device that generates periodic, accurately spaced signals used for such purposes as timing, regulation of the operations of a processor, or generation of interrupts. (FP) (ISO) See also coordinated clock, Coordinated Universal Time, DoD master clock, master clock, precise time, reference clock.

*-Clocks

n. Processor logic cycles, so called because each generally corresponds to one clock pulse in the processor's timing. The relative execution times of instructions on a machine are usually discussed in clocks rather than absolute fractions of a second; one good reason for this is that clock speeds for various models of the machine may increase as technology improves, and it is usually the relative times one is interested in when discussing the instruction set. Compare cycle.

*-Clone

1. n. An exact duplicate “Our product is a clone of their product. ” Implies a legal reimplementation from documentation or by reverse-engineering. Also connotes lower price.
2. A shoddy, spurious copy “Their product is a clone of our product. ”

3. A blatant ripoff, most likely violating copyright, patent, or trade secret protections “Your product is a clone of my product. ” This use implies legal action is pending.
4. PC clone:' a PC-BUS/ISA or EISA-compatible 80x86-based microcomputer (this use is sometimes spelled `klone' or `PClone'). These invariably have much more bang for the buck than the IBM archetypes they resemble.
5. In the construction `UNIX clone' An OS designed to deliver a UNIX-lookalike environment without UNIX license fees, or with additional `mission-critical' features such as support for real-time programming.
6. v. To make an exact copy of something. “Let me clone that” might mean “I want to borrow that paper so I can make a photocopy” or “Let me get a copy of that file before you mung it”.

Closed Security

Environment that provides sufficient environment assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system. NOTE: Closed security is predicated upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control.

Closed Security Environment

1. An environment that includes those systems in which both the following conditions hold true.
   a) Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is Confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.
   b) Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during operation of system applications. (CSC-STD-003-85;; CSC-STD-004-85;)
2. An environment in which both of the following conditions hold true.
   a) Application developers (including maintainers) have sufficient clearances and authorizations to provide acceptable presumption that they have not introduced malicious logic.
   b) Configuration control provides sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during the operation of system applications. (*NCSC-WA*-001-85;)

Closed Shop

A computer operations area set up such that physical access controls restrict programmers, and others who do not have a need to be present, from being in the area. (WB;)

Closed User Group

A group of specified users of a data network that is assigned a facility that permits them to communicate with each other but precludes communications with all other users of the service or services. A user data terminal equipment may belong to more than one closed user group. (FP) (ISO) See also data, facility (defs. # 2 & 3).

Closed User Group With Outgoing Access

A closed user group in which at least one member of the group has a facility that permits communication with one or more users external to the closed user group.

*-Clover Key

n. [Mac users] See feature key.

Coax

Acronym for coaxial cable.

Coaxial Cable

A cable consisting of a center conductor surrounded by an insulating material and a concentric outer conductor. (~) Note: Used primarily for wideband, video, or radio frequency service. See also cable.

*-COBOL

/koh'bol/ n. [COmmon Business-Oriented Language] (Edsger Dijkstra's famous observation that “The use of COBOL cripples the mind; its teaching should, therefore, be regarded as a criminal offense. ” (from “Selected Writings on Computing A Personal Perspective”).

Code

Any system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. Coding has three distinctly different applications: a. In the broadest sense, coding is a means of converting information into a form suitable for communications or encryption; e. g. , coded speech, Morse code, teletypewriter codes, etc. No security is provided. b. Brevity lists are codes which are used to reduce the length of time necessary to transmit information; e. g. , long, stereotyped sentences may be reduced to a few characters which are transmitted. No security is provided. c. A cryptosystem in which the cryptographic equivalents (usually called code groups) typically consisting of letters or digits (or both) in otherwise meaningless combinations are substituted for-plain text information ele-

ments which are primarily words, phrases, or sentences. Security is provided. (NCSC-9)

Code Book

Book or other document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.

Code Character

The representation of a discrete value or symbol in accordance with a code. (~) See also alphabet, character, code, digital alphabet.

Code Conversion

1. Conversion of character signals or groups of character signals in one code into corresponding signals or groups of signals in another code. (~)
2. A process for converting a code of some predetermined bit structure; e. g. , 5, 7, or 14 bits per character interval, to a second code with the same or a different number of bits per character interval. No alphabetical significance is assumed in this process. See also binary digit, character, code, line code, pulse-code modulation, signal.

Code Element

1. One of a set of parts, of which the characters in a given code may be composed. (~)
2. See also binary digit, character, mark, space.

Code Freeze

See (CF)

*-Code Grinder

1. n. A suit-wearing minion of the sort hired in legion strength by banks and insurance companies to implement payroll packages in RPG and other such unspeakable horrors. In its native habitat, the code grinder often removes the suit jacket to reveal an underplumage consisting of button-down shirt (starch optional) and a tie. In times of dire stress, the sleeves (if long) may be rolled up and the tie loosened about half an inch. It seldom helps. The code grinder's milieu is about as far from hackerdom as one can get and still touch a computer; the term connotes pity. See Real World, suit.
2. Used of or to a hacker, a really serious slur on the person's creative ability; connotes a design style characterized by primitive technique, rule-boundedness, brute force, and utter lack of imagination. Compare card walloper; contrast hacker, Real Programmer.

Code Group

A group of letters or numbers, or both, assigned in a code system to represent a plain text element which may be a word, phrase or sentence. (NCSC-9)

Code Restriction

A service feature wherein certain terminals are prevented from having access to certain features of the network. See also classmark, restricted access, service feature.

Code System

1. Any system of communication in which groups of symbols are used to represent plain text elements of varying length.
2. in the broadest sense, a means of converting information into a form suitable for communications or encryption, for example, coded speech, Morse Code, teletypewriter codes.
3. A cryptographic system in which cryptographic equivalents (usually called code groups) typically consisting of letters, digits, or both in meaningless combinations are substituted for plain text elements which may be words, phrases, or sentences. (*FIPS PUB* 39) See BREVITY LISTS.

Code Vocabulary

Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.

Code Word

1. A sequence of symbols conforming to the rules of generation of a language, such as an error-detection-or-correction code. (~)
2. A cryptonym used to identify sensitive intelligence data. (JCS1-DoD) (JCS1-NATO) (~)
3. A word which has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. (JCS1-DoD) (JCS1-NATO) See also code, word.

Code-Excited Linear Prediction

An analog-to-digital voice coding scheme. See also linear predictive coding.

Code-Independent Data Communication

A mode of data communication that uses a character-oriented protocol that does not depend on the character set or the code used by the data source. (FP) (ISO) Synonym code-transparent data communication. See also code, data, data communication, data transmission, transparency.

CODEC

1. Acronym for coder-decoder.
2. An assembly comprising an encoder and a decoder in the same equipment. (~)
3. A circuit that converts analog signals to digital code and vice versa. See also code, pulse-code modulation.

Coded Character Set

1. A set of unambiguous rules that establish a character set and the one-to-one relationships between

the characters of the set and their coded representations. (~)
2. See also character, character set, code, digital alphabet.

Coded Image
A representation of a display image in a form suitable for storage and processing. (FP) (ISO)

Coded Set
A set of elements onto which another set of elements has been mapped according to a code, for example, the list of names of airports that is mapped onto a corresponding set of three-letter representations of airport names. (FP) (ISO) See also alphabet, character set, code, digital alphabet.

Coder
Synonym analog-to-digital converter.

*-Codes
n. [scientific computing] Programs. This usage is common in people who hack supercomputers and heavy-duty number-crunching, rare to unknown elsewhere (if you say “codes” to hackers outside scientific computing, their first association is likely to be “and cyphers”).

*-Codewalker
n. A program component that traverses other programs for a living. Compilers have codewalkers in their front ends; so do cross-reference generators and some database front ends. Other utility programs that try to do too much with source code may turn into codewalkers. As in “This new `vgrind' feature would require a codewalker to implement. ”

Coding Scheme
Synonym code

Coercive Force
A negative or reverse magnetic force applied for the purpose of reducing magnetic flux density. For example, the force applied to magnetic media by a degausser. (CSC-STD-005-85;)

Coercivity
The measure of the amount of coercive force required to reduce magnetic flux density to zero. Often used to represent the ease with which magnetic ADP media can be degaussed. Coercivity is measured in Oersteds (Oe). It is often used to represent the relative difficulty of degaussing various magnetic media. (CSC-STD-005-85;)

Cognizant Agent
A person who is authorized access to classified or sensitive unclassified information and who intentionally makes that information available to unauthorized recipients.

Cognizant Security Authority
(CSA)An individual, usually at the MAJCOM level, who is authorized to make COMSEC policy decisions based on current Air Force COMSEC doctrine.

Coherent
Pertaining to a fixed phase relationship between corresponding points on an electromagnetic wave. (~) Note: A truly coherent wave would be perfectly coherent at all points in space. In practice, however, the region of high coherence may extend over only a finite distance. See also phase, phase coherence.

*-Cokebottle
/kohk'bot-l/ n. Any very unusual character, particularly one you can't type because it it isn't on your keyboard. MIT people used to complain about the `control-meta-cokebottle' commands at SAIL, and SAIL people complained right back about the `altmode-altmode-cokebottle' commands at MIT. After the demise of the space-cadet keyboard, `cokebottle' faded away as serious usage, but was often invoked humorously to describe an (unspecified) weird or non-intuitive keystroke command. It may be due for a second inning, however. The OSF/Motif window manager, `mwm(1)', has a reserved keystroke for switching to the default set of keybindings and behavior. This keystroke is (believe it or not) `control-meta-bang' (see bang). Since the exclamation point looks a lot like an upside down Coke bottle, Motif hackers have begun referring to this keystroke as `cokebottle'. See also quadruple bucky.

*-Cold Boot
n. See boot.

Cold Start
1. (COMSEC) Procedure for initially keying crypto-equipment.
2. (AIS) Reloading an AIS with software and data known to be good.

Collaborative Computing
End user computing in a work group environment in which members of a work group may use a local area network to share hardware, software, and databases to accomplish group assignments.

Collateral
All national security information classified under the provisions of an Executive Order for which special intelligence community systems of compartmentation (i. e. , sensitive compartmented information) are not formally established. (NACSIM 5203)

Collusion
The act of two or more Agents or Perpetrators cooperating or conspiring to perpetrate an Intentional Event. (MK;)

Colours
Attributes, attached to users and objects within the system, that are used by access control mechanisms. (RM;)

Combinational Logic Element
A device having at least one output channel and one or more input channels, all characterized by discrete states, such that at any instant the state of each output channel is completely determined by the states of the input channels at the same instant.

COMINT
Communications Intelligence (CSC-STD-004-85;)

*-Comm Mode
/kom mohd/ n. [ITSfrom the feature supporting on-line chat; the term may spelled with one or two m's] Syn. for talk mode.

Comma-Free Code
A code constructed such that any partial code word, beginning at the start of a code word but terminating prior to the end of that code word, is not a valid code word. Note 1: The comma-free property permits the proper framing of transmitted code words, provided that: (a) external synchronization is provided to identify the start of the first code word in a sequence of code words, and (b) no uncorrected errors occur in the symbol stream. Note 2: Huffman codes (variable length) are examples of comma-free codes. Synonym prefix-free code. See also code, self-synchronizing code.

Command
1. An order for an action to take place. (FP)
2. A control signal. (FP)
3. That part of a computer instruction word that specifies the operation to be performed.
4. Loosely, a mathematical or logic operator. (FP) See also command frame.

Command And Control
The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JCS1-DoD)

Command And Control System
The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JCS1-DoD)

Command Authority
(CA) Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

*-Command Key
n. [Mac users] Syn. feature key.

Command Languages/interfaces

Command, Control And Communications
The capabilities required by commanders to exercise command and control of their forces. (JCS Pub 18, Operations Security, Dec. 1982.)

Command, Control, Communications, And Computer (C4) Systems
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, through all phases of the operational continuum. (JP 1-02)

Command, Control, Communications, And Computer (C4) Systems Security
The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and the information contained within the systems. Such protection is the integrated application of COMSEC, TEMPEST, and COMPUSEC.

Command, Control, Communications, And Computer System
(C4) A combination of facilities, computer equipment, software, communications equipment, transmission media, procedures, people, and other resources used for the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes base visual information support systems. This does not include embedded computers.

*-Comment Out
vt. To surround a section of code with comment delimiters or to prefix every line in the section with a comment marker; this prevents it from being compiled or interpreted. Often done when the code is redundant or obsolete, but is being left in the source to make the intent of the active code clearer; also when the code in that section is broken and you want to bypass it in order to debug some other part of the code. Compare condition out, usually the preferred technique in languages (such as C) that make it possible.

Commercial Carrier
Synonym common carrier.

Commercial COMSEC

1. Relationship between the National Endorsement Program Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (i. e. , standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product.
2. NOTE: Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices.

Commercial COMSEC Endorsement Program

Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (i. e. standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. NOTE: Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices. (AF9K_JBC. TXT) (CCEP) Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (i. e. standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. NOTE: Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices.

Common Carrier

1. An organization that provides telecommunication facilities, services, or classes of service to the public for hire. (~)
2. Any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to [this Act]; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier.
3. Note: “Person” means an individual, a corporation, a partnership, an association, a joint-stock company, a business trust, or any other organized group, or any receiver or trustee. (CFR 47) Synonyms carrier, commercial carrier. See also divestiture, other common carrier, resale carrier, specialized common carrier.

#-Common Carrier Security

The protection provided by a telecommunications service provider that comes under the jurisdiction of state organizations and the Federal Communications Commission (FCC). Common carrier security includes protective measures for services including facsimile, data messages, telemetry and television. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Common Fill Device

1. (CFD) One of a family of devices developed to read-in, transfer, or store key. NOTE: KYK-13 Electronic Transfer Device, KYX-15 Net Control Device, and KOI-18 General Purpose Tape Reader are examples of common fill devices. (F:\NEWDEFS. TXT) One of a family of devices developed to read-in, transfer, or store key.
2. NOTE: KYK-13 Electronic Transfer Device, KYX-15 Net Control Device, and KOI-18 General Purpose Tape Reader are examples of common fill devices.

Common Sense

Common-Channel Interoffice Signaling

In multichannel switched networks, a method of transmitting all signaling information for a group of trunks by encoding it and transmitting it over a separate voice channel using time-division digital techniques. See also channel, signal.

Communication Deception

Use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system. (JCS1-DoD)

Communications

1. Deliberate transmission, retransmission, deception or alteration of communications to mislead an adversary's interpretation of the communications.
2. Analytic model of communications profileassociated with an organization or activity. NOTE: The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.
3. Measures and controls taken to deny security unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Communications Center

1. An agency charged with the responsibility for handling and controlling communications traffic. The center normally includes message center, transmitting, and receiving facilities. (JCS1-DoD) (JCS1-NATO)

2. A facility that serves as a node for a communication network(s). It is equipped for technical control and maintenance of the circuits originating, transiting, or terminating at the node. It may be provided with message center facilities and may serve as a gateway between networks. (~) See also information processing center.

#-Communications Center Security

1. Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.
2. NOTE: Communications Security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (Source: NSTISSI 4009).
3. Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems transmitting national security or national security-related information. It also includes the application of physical security and other measures to COMSEC information or materials. (NSA/CSS Dir 10-27 per Sup 1 to NSAM 130-1).

Communications Channel

See channel.

Communications Cover

Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary. Communications Deception. Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications. See Imitative Communications Deception and Manipulative Communications Deception.

Communications Deception

Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications. See Imitative Communications Deception and Manipulative Communications Deception. (NSA, *National INFOSEC Glossary*, 10/88)

Communications Devices

An active or passive device dedicated to carry information among other devices and performs no processing except that necessary to carry the information (e. g. , networks, direct line connections). (JCS PUB 6-03. 7)

Communications Intelligence

1. (COMINT) Technical and intelligence information derived from foreign communications by other than the intended recipients. (JCS1-DoD)
2. Intelligence derived from interception of communications. *Technical and intelligence information derived from intercept of foreign communications by other than the intended recipients; it does not include the monitoring of foreign public media or the intercept of communications obtained during the course of counterintelligence investigations within the United States COMINT includes the fields of traffic analysis, cryptanalysis, and direction finding (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Communications Profile

1. An analytic model of communications associated with an organization or activity. *An analytic model of communications associated with an organization or activity
2. NOTE: The model is prepared from a systematic examination of communications content and patterns, the reflections they reflect, and the COMSEC measures applied (NSA, *National INFOSEC Glossary*, 10/88)

Communications Security

1. The protection resulting from all measures (COMSEC) designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. (*OPNAVINST* 5239. 1A;; *AFR* 700-10;; *AR* 380-380;)
2. The protection that insures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications. (*FIPS PUB* 39;)
3. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (DOE 5636. 2A;)
4. Protective measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications. (*NCSC-WA*-001-85;)
5. (COMSEC) Measures taken to deny unauthorized persons information derived from telecommunications or to ensure its authenticity. *Measures taken

to deny unauthorized persons information derived from telecommunications of the U. S. Government concerning national security, and to ensure the authenticity of such telecommunications NOTE: COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information See Telecommunications and Automated Information Systems Security (TAISS) (NSA, *National INFOSEC Glossary*, 10/88)

Communications Security (COMSEC)

1. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U. S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emission security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to communications security information or materials. (*AR* 380-380; NCSC-9)
2. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (DOE 5637. 1)
3. The protection that insures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications. (*FIPS PUB* 39)
4. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: a. Cryptosecurity. The component of communications security which results from the provision of technically sound cryptosystems and their proper use. b. Transmission security. The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. Emission security. The component of communications security which results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. Physical security. The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JCS PUB 1)
5. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. (*OPNAVINST* 5239. lA; *AFR* 700-10)

Communications Security Equipment

Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients, as well as equipment designed specifically to aid in, or as an essential element of, the conversion process. Communications security equipment is crytoequipment, cryptoancillary equipment, cryptoproduction equipment, and authentication equipment. (JCS1-DoD) See also communications security.

Communications Security Material

All documents, devices, equipment, or apparatus, including cryptomaterial, used in establishing or maintaining secure communications. (JCS1-DoD) See also communications security.

#-Communications Security Policy And Guidance

This KSA has no definition.

Communications Security Survey

The organized collection of COMSEC and communications data relative to a given operation, system, or organization (NSA, *National INFOSEC Glossary*, 10/88)

Communications System

A collection of individual communication networks, transmission systems, relay stations, tributary stations, and terminal equipment capable of interconnection and interoperation to form an integral whole. (~) Note: These individual components must serve a common purpose, be technically compatible, employ common procedures, respond to some form of control, and, in general, operate in unison. See also common control system, communications, error-correcting system, error-detecting system, hybrid

communication network, link, neutral direct current telegraph system, polarential telegraph system, protected distribution system, switching system, tactical communications system, wideband.

#-Communications Systems Abuse

This KSA has no definition.

Community Of Interest

A grouping of users who generate a majority of their traffic in calls to each other. It may be related to a geographic area or to an administrative organization. See also call, closed user group.

COMP

A function of the certainty measure of a statement that returns the certainty measure of the negation of the statement. A requirement of the Uncertainty Calculus. (MA;)

*-Compact

adj. Of a design, describes the valuable property that it can all be apprehended at once in one's head. This generally means the thing created from the design can be used with greater facility and fewer errors than an equivalent tool that is not compact. Compactness does not imply triviality or lack of power; for example, C is compact and FORTRAN is not, but C is more powerful than FORTRAN. Designs become non-compact through accreting features and cruft that don't merge cleanly into the overall design scheme (thus, some fans of Classic C maintain that ANSI C is no longer compact).

Companion Document Series

Unknown

Comparator

1. In analog computing, a functional unit that compares two analog variables and indicates the result of that comparison. (FP) (ISO)
2. A device that compares two items of data and indicates the result of that comparison. (FP) (ISO)
3. A device for determining the dissimilarity of two items such as two pulse patterns or words. (FP)

Compartment

Used to describe information that has need-to-know access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. (See also “Sensitive Compartment Information” and “Special Access Program”). (JCS PUB 6-03. 7)

Compartment “S” Variable

The variable held only by members of a select community of interest to ensure compartmentation of calls. (NACSI 8108)

Compartmentalization

The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs. This term also refers to the division of sensitive data into small, isolated blocks for the purpose of reducing risk to the data. (*AR* 380-380;; *FIPS PUB* 39;)

Compartmentation

1. A method employed to segregate information of different desired accessibilities from each other. (~) Note: It may be used for communications security purposes.
2. A formal system for restricting access to intelligence activities or information. *Formal system of restricted access to intelligence activities, such systems established by and/or managed under the cognizance of the Director of Central Intelligence to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. NOTE: See Decompartmentation (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Compartmented Information

Any information for which the responsible Office of Primary Interest (OPI) requires an individual needing access to that information to possess a special authorization. (CSC-STD-004-85;)

Compartmented Intelligence/sensitive Compartmented Information (SCI)

Includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentalization of handling are formally established. SI and TK are two types of SCI. (*OPNAVINST* 5239. 1A;; DODD 5200. 28M;)

Compartmented Mode

AIS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: a. Valid security clearance for the most restricted information processed in the system. b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access. c. Valid need-to-know for information to which a user is to have access.

Compartmented Security Mode

1. The mode of operation which allows the system to process two or more types of compartmented information (information requiring a special authorization) or any one type of compartmented information with other than compartmented information. In this mode, all system users need not be cleared for all types of compartmented information processed, but must be fully cleared for at least Top Secret information for unescorted access to the computer. (CSC-STD-003-85;)

2. The mode of operation that allows the system to process two or more types of compartmented information or any one type of compartmented information with non-compartmented information. In this mode, all system users need not be cleared for all types of compartmented information processed, but must be fully cleared for at least the highest level of information for unescorted access to the computer and peripherals. (*NCSC-WA*-001-85;)
3. Utilization of a resource-sharing computer system for the concurrent processing and storage of: a) two or more types of SCI; or b) one type of SCI with other than SCI. For DON purposes, the compartmented mode should be considered equivalent to multilevel mode. (*OPNAVINST* 5239. 1A;)

#-Compartmented/partitioned Mode

AIS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: a. Valid security clearance for the most restricted information processed in the system. b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access. c. Valid need-to-know for information to which a user is to have access. (Source: NSTISSI 4009).

Compelled Signaling

Competent Authority

Authority recognized by the DAA as having sufficient knowledge (individually or corporately) to make a valid determination. (*AFR* 205-16;)

Competitor

See Adversary.

Compile

1. To translate a computer program expressed in a high-level language into a program expressed in an intermediate language, assembly language, or a machine language. (FP) (ISO)
2. To prepare a machine language program from a computer program written in another programming language by making use of the overall logic structure of the program, or by generating more than one computer instruction for each symbolic statement, or both, as well as performing the function of an assembler. (FP)
3. See also Ada®, assembly language, computer, computer language, computer-oriented language, high-level language, machine language, programmer.

Compiler

A computer program for compiling. (FP) (ISO) Synonym compiling program. See also compile.

Compiling Program

Synonym compiler.

Compliance Review

Refers to a review and examination of records, procedures, and review activities at a site in order to assess the unclassified computer security posture and ensure compliance with this order. This review is normally conducted by the CPPC at an operations office having cognizance over the site and management responsibilities for implementing this order. For those sites not reporting to an operations office, this review is normally conducted by the Office of ADP Management. (*DOE 1360. 2A*)

Component

Hardware device, with its required firmware or software, that performs a specific AIS function. Components include modems, printers, communications controllers, tape drives, message switches, computers, gateways, peripheral controllers, etc.

*-Compress

[UNIX] vt. When used without a qualifier, generally refers to crunching of a file using a particular C implementation of compression by James A. Woods et al. and widely circulated via Usenet; use of crunch itself in this sense is rare among UNIX hackers. Specifically, compress is built around the Lempel-Ziv-Welch algorithm as described in “A Technique for High Performance Data Compression”, Terry A. Welch, “IEEE Computer”, vol. 17, no. 6 (June 1984), pp. 8--19.

Compression

1. A process in which the dynamic range of a signal is reduced by controlling it as a function of the inverse relationship of its instantaneous value relative to a specified reference level. (~)
   Note 1: Input levels that are low relative to the reference level thus realize a relative increase, and levels that are high relative to the reference level thus realize a relative decrease.
   Note 2: Compression is usually accomplished by separate devices called compressors and is used for many purposes, such as: improving signal-to-noise ratios, preventing overload of succeeding elements of a system, or matching the dynamic ranges of two devices.
   Note 3: The amount of compression (expressed in decibels) may be a linear or nonlinear function of the signal level across the frequency band of interest and may be essentially instantaneous or have fixed or variable delay times. Note 4: Compression always introduces distortion, which is usually not objectionable, provided the compression is limited to a few decibels.

2. In facsimile systems, a process wherein the number of pels scanned on the original is larger than the number of encoded bits of picture information transmitted. (~)
3. See also compander, compression ratio, compressor, expander, expansion, level, redundancy.

Compromise

1. The disclosure of classified data to persons who are not authorized to receive such data. (DOE 5636. 2A;)
2. An unauthorized disclosure or loss of sensitive information (*FIPS PUB* 39;)
3. [Passwords] Disclosing a password, or part of a password, to someone not authorized to know, have or use the password. (*FIPS PUB* 112;)
4. A violation of the security policy of a system such that an unauthorized disclosure, modification or destruction of sensitive information may have occurred. (*NCSC-WA*-001-85;)
5. An unauthorized disclosure or loss of sensitive defence data. (*OPNAVINST* 5239. 1A;; *AR* 380-380;)
6. The exposure of information or activities to persons not authorized access See Penetration. *The exposure of classified official information or activities to persons not authorized access thereto; hence, unauthorized disclosure NOTE: See Classified Information (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Compromising

Unintentional signals that, if emanations intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

Compromising Emanation Performance Requirement

(CEPR) The maximum emanation level permitted at the standard measurement point. When the CEPR is met, there will be minimal chance that a compromising emanation will be detected beyond the specified design radius.

Compromising Emanations

1. Electromagnetic emanations that may convey data and that, if intercepted and analyzed, may compromise sensitive information being processed by an ADP system (*FIPS PUB* 39;)
2. Unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmission received, handled or otherwise processed by any information processing equipment. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the "compromising emanations". (*OPNAVINST* 5239. 1A;; *AFR* 205-16;; *AFR* 700-10;; *AR* 380-380;; *NCSC-WA*-001-85;; DOE 5636. 2A;)
3. Unintentional intelligence-bearing signals emitted from information processing equipment See TEMPEST. *Unintentional data-related or intelligence-bearing signals emitted from telecommunications or information processing equipment or systems NOTE: If intercepted and analyzed, compromising emanations can disclose classified or sensitive unclassified information transmitted, received, or processed by an equipment or system Also referred to as TEMPEST (NSA, *National INFOSEC Glossary*, 10/88)

Computer

A machine capable of accepting, performing calculations on or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices. (DODD 5200. 28;) See Automated Information System

Computer Abuse

1. Willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service,and misappropriation. Levels of computer abuse are:
   a. Minor abuse - acts that represent management problems, such as printing calendars or running games that do not impact system availability for authorized applications;
   b. Major abuse - unauthorized use (possibly criminal), denial of service, and multiple instances of minor abuse to include waste;
   c. Criminal act - fraud, embezzlement, theft, malicious damage, misappropriation, conflict of interest, and unauthorized access to classified data. (*AFR* 205-16;)
2. The misuse, destruction, alteration, or disruption of data processing resources. The key aspects of computer related abuse are that it is intentional and improper and it may not involve the violation of a specific law. (*NCSC-WA*-001-85;)

Computer Conferencing

1. The ability for multiple users/groups to access a common information base mediated by a controlling computer.
2. The interconnection of two or more computers working in a distributed manner on a common application process. (~)

*-Computer Confetti

n. Syn. chad. Though this term is common, this use of punched-card chad is not a good idea, as the pieces

are stiff and have sharp corners that could injure the eyes. GLS reports that he once attended a wedding at MIT during which he and a few other guests enthusiastically threw chad instead of rice. The groom later grumbled that he and his bride had spent most of the evening trying to get the stuff out of their hair.

Computer Crime

Fraud, embezzlement, unauthorized access, and other "white collar" crimes committed with the aid of or directly involving a computer system and/or network. (GAO;)

Computer Cryptography

The use of a crypto algorithm in a computer, microprocessor or microcomputer to perform encryption/decryption to protect information or to authenticate users, sources or information. (*NCSC-WA*-001-85;)

#-Computer Emergency Response Team

This KSA has no definition.

Computer Facility

Physical resources that include structures or parts of structures to house and support capabilities. For small computers, stand-alone systems, and word processing equipment, it is the physical area where the computer is used. (*AFR* 205-16;)

Computer Fraud

Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or coverup of the act, or series of acts. A computer system might have been involved through improper manipulation of:

input data;
output or results;
applications programs;
data files;
computer operations;
communications; or
computer hardware, systems software, or firmware.

(*NCSC-WA*-001-85;)

Computer Fraud And Abuse Act

Public Law 99-474

Whoever knowingly or someone who exceeds authorization in subject to this act.

Computer Graphics

1. Methods and techniques for converting data to or from graphic displays via computers. (FP) (ISO)
2. That branch of science and technology that is concerned with methods and techniques for converting data to or from visual presentation using computers. (FP)

Computer Installation

The physical space which contains one or more computer systems. Computer installations may range from locations for large centralized computer centers to locations for individual standalone microcomputers. (*DOE 1360. 2A*)

Computer Language

A language that is used to program a computer. The language may be a high-level language, an assembly language, or a machine language. (~) See also assembly language, compile, high-level language, language, machine language.

#-Computer Matching

The comparison of two or more sets of data files to search for individuals included in both or all sets. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

#-Computer Matching Responsibilities

This KSA has no definition.

Computer Network

1. A complex consisting of two or more interconnected computers. (*AR* 380-380)
2. See NETWORK.

Computer Program

A sequence of instructions suitable for processing by a computer. Note: Processing may include the use of an assembler, a compiler, an interpreter, or a translator to prepare the program for execution, as well as the execution of the program. The sequence of instructions may include statements and necessary declarations. (FP) (ISO) See also assembler, compiler.

Computer Program Origin

The address assigned to the initial storage location of a computer program in main storage. (FP)

Computer Protection Plan

A document which serves as the single source management summary of information associated with the DOE unclassified computer security program as required on page 8, under paragraph 11d. It serves as a basis for estimating security needs, performing security assessments, performing compliance and management reviews, and facilitating risk management and certification efforts. (DOE 1369. 2A)

Computer Routine

See routine.

Computer Science

The branch of science and technology that is concerned with methods and techniques relating to data

processing performed by automatic means. (FP) (ISO)

#-Computer Science And Architecture

This KSA has no definition.

Computer Security

1. (COMPUSEC) The protection of the information and physical assets of a computer system. The protection of information aims to prevent the unauthorized disclosure, manipulation, destruction or alteration of data. The protection of physical assets implies security measures against theft, destruction or misuse of equipment, i. e. , processors, peripherals, data storage media, communication lines and interfaces. (MS)
2. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system. (NCSC-9)
3. All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive unclassified or critical data, material, or processes in the system. It includes: a. Hardware and software functions, characteristics, and features. b. Operational procedures. c. Accountability procedures. d. Access controls at computer facilities (includes those housing mainframes, terminals, minicomputers, or microcomputers). e. Management constraints. f. Physical protection. g. Control of compromising emanations (TEMPEST). h. Communications security (COMSEC). i. Personnel security. j. Other security disciplines. (*AFR* 205- 16)
4. See Adp Security, Adp System Security, Automated Data Processing Security, Automated Information Systems Security, Automation Security, Classified Computer Security Program, Data Security, Information Security, Information System Security, And Operational Data Security.

Computer Security Act

Computer Security Act Of 1987 100-235

Computer Security Incident

1. An adverse event associated with an ADP system(s): a. that is a failure to comply with security regulations or directives; b. that results in attempted, suspected or actual compromise of classified information; or c. that results in the waste, fraud, abuse, loss or damage of government property or information. (DOE 5637. 1)
2. The occurrence of an event which has or could adversely affect normal computer operations such as an unauthorized access, interruption to computer service or safeguarding controls, or discovery of a vulnerability. (*DOE 1360. 2A*)
3. See SIGNIFICANT COMPUTER SECURITY INCIDENT.

Computer Security Law

Computer Security Officer

(CSO) Individual responsible for the security of a specific computer system or grouping of computer systems. The CSO usually receives guidance from the Base C4 Systems Security Office and provides security assistance for assigned Terminal Area Security Officers (TASOs). See Network Security Officer (NSO).

Computer Security Policy

Set of laws, rules, and practices that regulate how an organization protects computer systems and the data within them. Computer Security Subsystem. Device designed to provide limited computer security features in a larger system environment.

Computer Security Subsystem

A device which is designed to provide limited Subsystem computer security features in a larger computer system environment. (*NCSC-WA*-001-85;)

Computer Security Subsystem Interpretation

Computer Security Technical Vulnerability Reporting Program

(CSTVRP) A program that focuses on technical vulnerabilities in commercially available hardware, firmware and software products acquired by DoD. CSTVRP provides for the reporting, cataloguing, and discreet dissemination of technical vulnerability and corrective measure information to DoD components on a need-to-know basis. (*NCSC-WA*-001-85;)

Computer Security Technical Vulnerability Reporting Program (CSTVRP)

A program that focuses on technical vulnerabilities in commercially available hardware, firmware and software products acquired by DoD. CSTVRP provides for the reporting, cataloging, and discreet dissemination of technical vulnerability and corrective measure information to DoD components on a need-to-know basis.

Computer Site

A geographic location where one or more computer installations is managed and operated. (*DOE 1360. 2A*)

Computer System

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and includes computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (PL 100-235)

Computer System Fault Tolerance

The ability of a computer system to continue to operate correctly even though one or more of its component parts are malfunctioning. The speed of performance, the throughput, or both may be diminished from normal until the faults are corrected. (FP) (ISO) Synonym computer system resilience.

Computer System Manager

Individual responsible for the operation of a computer system. See Network Manager (NM). (AF9K_JBC. TXT)

Computer System Resilience

Synonym Computer System Fault Tolerance.

Computer Systems Security Officer

(CSSO) Term no longer used, see Computer Security Officer (CSO).

Computer Word

In computing, a group of bits or characters treated by computer circuits as a unit. (~) Synonym machine word. See also binary digit, byte, character, word.

Computer-Dependent Language

Synonym assembly language.

Computer-Oriented Language

A programming language whose words and syntax are designed for use on a specific computer or class of computers. (~) Synonyms low-level language, machine-oriented language. See also assembly language, compile, high-level language.

#-Computers At Risk

Book title

Computing System

Synonym computer system.

*-Computron

1. /kom'pyoo-tron`/ n. A notional unit of computing power combining instruction speed and storage capacity, dimensioned roughly in instructions-per-second times megabytes-of-main-store times megabytes-of-mass-storage. “That machine can't run GNU EMACS, it doesn't have enough computrons!” This usage is usually found in metaphors that treat computing power as a fungible commodity good, like a crop yield or diesel horsepower. See bitty box, Get a real computer!, toy, crank.
2. A mythical subatomic particle that bears the unit quantity of computation or information, in much the same way that an electron bears one unit of electric charge (see also bogon). An elaborate pseudo-scientific theory of computrons has been developed based on the physical fact that the molecules in a solid object move more rapidly as it is heated. It is argued that an object melts because the molecules have lost their information about where they are supposed to be (that is, they have emitted computrons). This explains why computers get so hot and require air conditioning; they use up computrons. Conversely, it should be possible to cool down an object by placing it in the path of a computron beam. It is believed that this may also explain why machines that work at the factory fail in the computer room the computrons there have been all used up by the other hardware. (This theory probably owes something to the “Warlock” stories by Larry Niven, the best known being “What Good is a Glass Dagger?”, in which magic is fueled by an exhaustible natural resource called `mana'.)

COMSEC Account

(CA) Administrative entity, identified by an account number, used to maintain accountability, custody and control of COMSEC material.

COMSEC Account Audit

Examination of the holdings, records, and procedures of a COMSEC account to ensure that all accountable COMSEC material is properly handled and safeguarded.

#-COMSEC Accounting

Administrative entity, identified by an account number, used to maintain accountability, custody and control of COMSEC material. (Source: NSTISSI 4009).

COMSEC Aid

COMSEC material, other than an equipment or device, that assists in securing telecommunications and which is required in the production, operation, or maintenance of COMSEC systems and their components. NOTE: COMSEC keying material, callsign/frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.

COMSEC Boundary

Definable perimeter within a telecommunications equipment or system within which all hardware, firmware, and software components that perform critical COMSEC functions are located. NOTE: Key

generation and key handling and storage are critical COMSEC functions.

COMSEC Chip Set

Collection of National Security Agency approved microchips furnished to a manufacturer to secure or protect telecommunications equipment. See Protected Communications and Secure Communications.

COMSEC Control

Set of instructions or routines for program a computer that controls or affects the externally performed functions of key generation, key distribution, message encryption/decryption, or authentication.

COMSEC Control Program

Set of instructions or routines for a computer that controls or affects the externally performed functions of key generation, key distribution, message encryption/decryption, or authentication.

COMSEC Crypto-Algorithm

Well-defined procedure or sequence of rules or steps which are used to produce cipher-text from plain-text or vice versa. (NTISSI 4002)

#-COMSEC Custodian

Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account. NOTE: The term COMSEC manager is replacing the term COMSEC custodian. These terms are not synonymous, since the responsibilities of the COMSEC manager extend beyond the functions required for effective operation of a COMSEC account.

COMSEC End Item

Equipment or combination of components ready for its intended use in a COMSEC application. COMSEC Equipment. Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. NOTE: COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, cryptoproduction equipment, and authentication equipment.

COMSEC Equipment

Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. NOTE: COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, cryptoproduction equipment, and authentication equipment.

COMSEC Facility

Space employed primarily for the purpose of generating, storing, repairing, or using COMSEC material.

COMSEC Incident

Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information.

COMSEC Insecurity

COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

COMSEC Manager

Person designated by proper authority to be responsibile for the management of COMSEC material assigned to a COMSEC account.

COMSEC Material

1. Item designed to secure or authenticate telecommunications. NOTE: COMSEC material includes, but is not limited to, key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.
2. Logistics and accounting system Control System through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. NOTE: Included are the COMSEC central offices of record, cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the COMSEC Material Control System.

COMSEC Material Control System

(CMCS) Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. NOTE: Included are the COMSEC central offices of record, cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the COMSEC Material Control System. (F:\NEWDEFS. TXT)

#-COMSEC Material Destruction Procedures

Written guidance which defines the step-by-step methods for proper disposition of COMSEC materials. (Source: Panel of Experts, July 1994).

#-COMSEC Material Identification And Inventory

A method to identify COMSEC material known as TSEC Nomenclature. This system identifies the type

and purpose of certain items of COMSEC Equipment. Inventorying is a method to periodically physically inventory all items of COMSEC Material held by individual COMSEC Accounts.

COMSEC Modification

Electrical, mechanical, or software change to a National Security Agency approved COMSEC end item. NOTE: Categories of COMSEC modifications are: mandatory, optional, special mission mandatory, special mission optional, human safety mandatory, and repair actions.

COMSEC Module

Removable component that performs COMSEC functions in a telecommunications equipment or system.

COMSEC Monitoring

Act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis, so that the degree of security being provided to those transmissions may be determined.

COMSEC No-Lone Zone

Area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other. See Two Person Integrity.

COMSEC Profile

Statement of the COMSEC measures and materials used to protect a given operation, system, or organization.

COMSEC Responsible Officer

(CRO) Individual authorized by an orginization to order COMSEC aids from the COMSEC account and who is responsible for their protection. (UNTITLED. TXT)

COMSEC Survey

Organized collection of COMSEC and communications data relative to a given operation, system, or organization.

COMSEC System Data

Information required by a COMSEC equipment or system to enable it to properly handle and control key.

#-COMSEC Testing

Evaluation by the National Security Agency to test the telecommunications suitability for use with classified information. (Source: Panel of Experts, July 1994).

COMSEC Training

Teaching of hands-on skills relating to COMSEC accounting, the use of COMSEC aids, or the installation, use, maintenance, and repair of COMSEC equipment.

Concealment System

1. That computer security characteristic that ensures individuals are given access to computer resources based on security clearance and need-to-know. This characteristic protects against compromise and inadvertent disclosure. (*AFR* 205-16;)
2. A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for individuals or organizations. (*AR* 380-380;; *FIPS PUB* 39;)
3. A method of achieving confidentiality in which sensitive information is hidden by embedding it in irrelevant data. (*FIPS PUB* 39; *AR* 380-380)

Conceptual Entity

Anything about which we might want to say something. Examples of conceptual entities are physical objects, scenes, processes, and IF-THEN rules. (ET;, MA;)

*-Condition Out

vt. To prevent a section of code from being compiled by surrounding it with a conditional-compilation directive whose condition is always false. The canonical examples of these directives are `#if 0' (or `#ifdef notdef', though some find the latter bletcherous) and `#endif' in C. Compare comment out.

Conducted Signals

Electromagnetic or acoustic emissions of undesired signal data which become induced and propagated along wirelines or other conductors. (NACSEM 5106)

Confidential Source

Any individual or organization that has provided information with the understanding their identity will be protected. *Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence (DoD Directive 5200. 1R, Information Security Program Regulation)

Confidentiality

1. The computer security characteristic that makes sure individuals are given access to computer resources based on security clearance and need-to-know. This characteristic protects against compromise and inadvertent disclosure. (*AFR* 205-16)
2. A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for individuals or organizations. (*AR* 380-380; *FIPS PUB* 39)

3. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. (*NCSC-TG*-004-88)

Configuration
The arrangement of communication or computer systems as defined by the nature, number, and the chief characteristics of its functional units. Note 1: The term may refer to a hardware or a software configuration. Note 2: The configuration determines what the system will do and how well it will do it.

Configuration Control
1. Management of changes made to a system's hardware,software, firmware, and documentation throughout the development and operational life of the system. (CSC-STD-003-85;; CSC-STD-004-85;; COE 5636. 2A)
2. The process of controlling modifications to the system's hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification prior to, during, and after implementation. (*NCSC-WA*-001-85;)

Configuration Control Board
Unspecified

Configuration Management
1. Process of controlling modifications to the system's hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation. (*AFR* 205-16;)
2. The management of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system. (*NCSC-WA*-001-85;)
3. The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of insuring that such changes will not lead to decreased data security. (*OPNAVINST* 5239. 1A;)

Configuration Review Board
Unknown

Confinement
1. Allowing a process executing a borrowed program (in general, an arbitrary program) to have access to data, while ensuring that the data cannot be misused, altered, destroyed or released. (MTR-8201;)
2. The problem of preventing a program from leaking sensitive data. (*NCSC-WA*-001-85;)
3. The prevention of the leaking of sensitive data from a program.

Confinement Channel
See Covert Channel.

Confinement Property
See STAR PROPERTY (*-PROPERTY).

#-Conformance Testing
This KSA has no definition.

CONJ
A function of the certainty measures of two statements that returns the certainty measure of the conjunction of the statements. Required by the uncertainty calculus. (MA;)

Connection

Connectionless Data Transfer
See connectionless mode transmission.

Connectionless Mode Transmission
In packet data transmission, a mode of operation in which each packet is encoded with a header containing a destination address sufficient to permit the independent delivery of the packet without the aid of additional instructions. Note: A connectionless packet is frequently called a datagram. A connectionless service is inherently unreliable in the sense that the service provider usually cannot provide assurance against the loss, error insertion, misdelivery, duplication, or out-of-sequence delivery of a connectionless packet. However, it may be possible to protect against these anomalies by providing a reliable transmission service at a higher protocol layer, e. g. , Transport Layer. See also datagram, Open Systems Interconnection--Reference Model, packet switching.

#-Connectivity
Describe the connections your system has with external organizations. (Source: DACUM IV).

*-Connector Conspiracy
n. [probably came into prominence with the appearance of the KL-10 (one model of the PDP-10), none of whose connectors matched anything else] The tendency of manufacturers (or, by extension, programmers or purveyors of anything) to come up with new products that don't fit together with the old stuff, thereby making you buy either all new stuff or expensive interface devices. The KL-10 Massbus connector was actually *patented* by DEC, which reputedly refused to license the design and thus effectively locked third parties out of competition for the lucrative Massbus peripherals market. This policy is a source of never-ending frustration for the diehards who maintain older PDP-10 or VAX systems. Their CPUs work fine, but they are stuck with dying, obsolescent disk and tape drives with low capacity and high power requirements. (A closely related phenomenon,

with a slightly different intent, is the habit manufacturers have of inventing new screw heads so that only Designated Persons, possessing the magic screwdrivers, can remove covers and make repairs or install options. Older Apple Macintoshes took this one step further, requiring not only a hex wrench but a specialized case-cracking tool to open the box.) In these latter days of open-systems computing this term has fallen somewhat into disuse, to be replaced by the observation that “Standards are great! There are so *many* of them to choose from!” Compare backward combatability.

*-Cons

1. /konz/ or /kons/ [from LISP] vt. To add a new element to a specified list, esp. at the top. “OK, cons picking a replacement for the console TTY onto the agenda. ”
2. `cons up' vt. To synthesize from smaller pieces “to cons up an example”. In LISP itself, `cons' is the most fundamental operation for building structures. It takes any two objects and returns a `dot-pair' or two-branched tree with one object hanging from each branch. Because the result of a cons is an object, it can be used to build binary trees of any shape and complexity. Hackers think of it as a sort of universal constructor, and that is where the jargon meanings spring from.

#-Consequences

This KSA has no definition.

*-Considered Harmful

adj. Edsger W. Dijkstra's note in the March 1968 “Communications of the ACM”, “Goto Statement Considered Harmful”, fired the first salvo in the structured programming wars. Amusingly, the ACM considered the resulting acrimony sufficiently harmful that it will (by policy) no longer print an article taking so assertive a position against a coding practice. In the ensuing decades, a large number of both serious papers and parodies have borne titles of the form “X considered Y”. The structured-programming wars eventually blew over with the realization that both sides were wrong, but use of such titles has remained as a persistent minor in-joke (the `considered silly' found at various places in this lexicon is related).

*-Console

1. n. The operator's station of a mainframe. In times past, this was a privileged location that conveyed godlike powers to anyone with fingers on its keys. Under UNIX and other modern timesharing OSes, such privileges are guarded by passwords instead, and the console is just the tty the system was booted from. Some of the mystique remains, however, and it is traditional for sysadmins to post urgent messages to all users from the console (on UNIX, /dev/console).

2 On microcomputer UNIX boxes, the main screen and keyboard (as opposed to character-only terminals talking to a serial port). Typically only the console can do real graphics or run X. See also CTY.

Contained

“Contained” refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; DODD 5200. 28M;)

Container

A repository of data in a system. (MTR-8201;)

Containment

Being within limits, as within system bounds, regardless of prupose or functions, and includes any state of storage, use or processing. (*OPNAVINST* DOOD)

Contamination

1. The introduction of data of one sensitivity and need-to-know with data of a lower sensitivity or different need-to-know. This can result in the contaminating data not receiving the required level of protection. (*AFR* 205-16;)
2. The intermixing of data at different sensitivity and need-to-know levels. The lower level data is said to be contaminated by the higher level data. This can result in the contaminating data not receiving the required level of protection. (*NCSC-WA*-001-85;)
3. A peril involving the altering of an asset to behave in an improper manner (frequently the source of computer fraud). (RM;)

Content-Addressable Storage

Synonym associative storage.

Contention

*-Context. User-Friendly

adj. Programmer-hostile. Generally used by hackers in a critical tone, to describe systems that hold the user's hand so obsessively that they make it painful for the more experienced and knowledgeable to get any work done. See menuitis, drool-proof paper, Macintrash, user-obsequious.

Contingency Key

Key held for use under specific operational conditions or in support of specific contingency plans.

Contingency Management

Management of all the actions to be taken before, during, and after a disaster (emergency condition), along with a documented, tested procedures which, if followed, will ensure the availability of critical ADP systems and which will facilitate maintaining the con-

tinuity of operations in an emergency situation. (DOE 5636. 2A;)

Contingency Plan

1. A plan for emergency response, backup operations, and post-disaster recovery maintained by an ADP activity as a part of its security program. A comprehensive, consistent statement of all the actions (plans) to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical ADP resources and which will facilitate maintaining the continuity of operations in an emergency situation. (*OPNAVINST*5239. lA)
2. Documents, developed in conjunction with computer application owners and maintained at the primary and backup computer installation; they describe procedures and identify personnel necessary to respond to abnormal situations, and ensure that computer application owners can continue to process mission-essential applications in the event that computer support is interrupted (e. g. , appropriate automated and/or manual backup processing capabilities). (*DOE 1360. 2A*)
3. A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical -resources and facilitate the continuity of operations in an emergency situation. Also called disaster plan and emergency plan. (*NCSC-TG*-004-88)

#-Contingency Plan Testing

1. Aperiodic exercise of the Contingency Plan to ensure the plan's validity. The purpose of such testing is to assure that users can continue to perform essential functions in the event their information technology support is interrupted. (Panel of Experts, July 1994);
2. periodic testing of plans produced by an organization to respond to the range of incidents, accidents and disasters that could occur. (ISDCST+LSC-92).

#-Contingency Planning

Procedures for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan. (Source: *NCSC-TG*-004).

Continuity Of Operations

The maintenance of essential services for an information system after a major failure at an information center. The failure may result from natural causes (such as fire, flood or earthquakes) or from deliberate events (such as sabotage). (GAO;)

Continuity Plan

#-Continuity Planning

1. Procedures for maintenance of essential services for an information system after a major failure at an information center. The failure may result from natural causes (such as fire, flood or earthquakes) or from deliberate events (such as sabotage). (NISTIR 4659);
2. the maintenance of a plan to ensure essential services for an information system after a major failure at an information center. The failure may result from natural causes or from deliberate events.

Continuous Operation

1. A condition wherein certain nodes, facilities, circuits, or equipment are in an operational state at all times. (~) Note: This usually requires a fully redundant configuration or at least an X out of Y degree of redundancy for compatible equipment, where X is the number of spare components and Y is the number of operational components.
2. In data transmission, a type of operation in which the master station need not stop for a reply after transmitting each message or transmission block. See also cutover, degraded service state, downtime, dynamically adaptive routing, fail-safe operation, graceful degradation, operational service state, outage, redundancy (def. #2), survivability.

Contract

#-Contracting For Security Services

This KSA has no definition.

#-Contractor Security Safeguards

Contracts, Agreements, and Other Obligations- The process of agreeing to a specific course of action.

Contracts

A binding agreement between two or more parties for performing, or refraining from performing, some specified act(s) in exchange for lawful consideration. A consideration is something of value, such as money or personal services, given by one party to another in exchange for an act or promise.

#-Contracts, Agreements, And Other Obligations

The process of agreeing to a specific course of action;

Control Character

1. A character whose occurrence in a particular context specifies a control function. A control charac-

ter may be recorded for use in a subsequent action. A control character is not a graphic character but may have a graphic representation in some circumstances. (FP) (ISO) (~)
2. See also acknowledge character, call control signal, character, data link escape character, end-of-selection character, end-of-text character, end-of-transmission-block character, end-of-transmission character, enquiry character, idle character, negative acknowledge character, start-of-heading character, start-of-text character, stop signal.

Control Function
Synonym control operation.

Control Line
Line intended for the transmission of control signals, alarm indicators and fault determination between components of a system.

Control Zone
1. The space, expressed in feet of radius, surrounding equipment processing classified information which is under sufficient physical and technical control to preclude a successful hostile intercept attack. (*AR* 380-380;)
2. The space, expressed in feet of radius, surrounding equipment processing sensitive information which is under sufficient physical and technical control to preclude an unauthorized entry or compromise. (DOE 5636. 2A;) (*NCSC-WA*-001-85;)

*-Control-C
1. vi. “Stop whatever you are doing. ” From the interrupt character used on many operating systems to abort a running program. Considered silly.
2. interj. Among BSD UNIX hackers, the canonical humorous response to “Give me a break!”

*-Control-O
vi. “Stop talking. ” From the character used on some operating systems to abort output but allow the program to keep on running. Generally means that you are not interested in hearing anything more from that person, at least on that topic; a standard response to someone who is flaming. Considered silly. Compare control-S.

*-Control-Q
vi. “Resume. ” From the ASCII DC1 or XON character (the pronunciation /X-on/ is therefore also used), used to undo a previous control-S.

*-Control-S
vi. “Stop talking for a second. ” From the ASCII DC3 or XOFF character (the pronunciation /X-of/ is therefore also used). Control-S differs from control-O in that the person is asked to stop talking (perhaps because you are on the phone) but will be allowed to continue when you're ready to listen to him -- as opposed to control-O, which has more of the meaning of “Shut up. ” Considered silly.

Controllable Isolation
Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set of sphere of activity. (*FIPS PUB* 39;; *AR* 380-380;)

Controlled
Secure telecommunications or information cryptographic item handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. NOTE: Such items are marked “CONTROLLED CRYPTOGRAPHIC ITEM” or, where space is limited, “CCI. ”

Controlled Access
Log-in procedures, audit of security protection relevant events, and resource isolation as prescribed for class C2 in the *Orange Book*. See Access Control.

Controlled Access Area
1. (CAA) Part or all of an environment where all types and aspects of an access are checked and controlled. (*AFR* 205-16)
2. The complete building or facility area under direct physical control which can include one or more limited exclusion areas, controlled BLACK equipment areas, or any combination thereof. (NACSIM 5203)

Controlled Access Protection
(Class C2) Log-in procedures, audit of security relevant events, and resource isolation as prescribed for class C2 in the *Orange Book*. Is the C2 level of protection described in the Trusted Computer System Evaluation Criteria. The major characteristics of controlled access protection are addressed in Section IV. (NTISSP 200)

Controlled Accessibility
Synonymous with ACCESS CONTROL.

Controlled Area
1. An area within which uncontrolled movement does not permit access to classified information and which is designed for the principal purpose of providing administrative control, safety, or a buffer area of security restrictions for Limited Exclusion Areas. This area may be protected by physical security measures, such as sentries and fences. (*OPNAVINST* 5239. 1A;)
2. Any area, building, or structure specifically designated by the installation commander requiring limited entry for the protection of Air Force personnel or resources. (*AFR* 205-16;)

3. An area or space to which access is physically controlled. (NCSC-9)

Controlled BLACK Equipment Area(s) (CBEA)

A BLACK equipment area which is not located in limited exclusion area but is afforded the same physical entry control which would be required if it were within a limited exclusion area. (NACSIM 5203)

Controlled COMSEC Item

Unknown

Controlled Cryptographic Item

(CCI) Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. NOTE: Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI. "

Controlled Cryptographic Item (CCI)

A secure telecommunications or information handling equipment, or associated cryptographic component, which is unclassified but controlled. Equipments and components so designated shall bear the designator "controlled cryptographic item "or" CCI". Replaces the term "Controlled COMSEC Item (CCI) as defined in NCSC-9. (NTISSI 4001)

Controlled Cryptographic Item (CCI) Assembly

Device embodying a cryptographic logic or other COMSEC design that NSA has approved as a CCI and performs the entire COMSEC function, but is dependent upon the host equipment to operate.

Controlled Cryptographic Item (CCI) Component

Device embodying a cryptographic logic or other COMSEC design, that NSA has approved as a CCI, that does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete and operate the COMSEC function.

Controlled Cryptographic Item (CCI) Equipment

Telecommunications or information handling equipment that embodies a CCI component or CCI assembly and which performs the entire COMSEC function without dependence on a host equipment to operate.

Controlled Information

Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign official actions advantageous to U. S. interests/objectives (JCS PUB 3-54, 9/89) *Information conveyed to an adversary in a deception operation to evoke desired appreciations (JCS PUB 1-02, 12/89)

Controlled Security Mode

1. A mode of operation where internal security controls prevent inadvertent disclosure. Personnel, physical, and administrative controls prevent attempts to gain unauthorized access. The system may have users with access to the system who have neither the security clearance nor need-to-know for all classified information in the system. Access shall be limited to users with a minimal security clearance of one less than the highest classification information processed. (*AFR* 205-16;)
2. The mode of operation that is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware/software base of the system, with the resultant restrictions on the classification levels and clearance levels that may be supported. (CSC-STD-003-85;)
3. The mode of operation that is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware and software base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported. The system may have users who possess neither the security clearance nor the need-to-know for all information in the system, however, access shall be limited to users with a minimal clearance level of one less than the highest classification processed. (*NCSC-WA*-001-85;)
4. An ADP system is operating in the controlled security mode when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material then contained in the ADP system. However, the separation and controlof users and classified material on the basis, respectively, of security clearance and security classification is not essentially under operating system control as in the multilevel security mode. (*OPNAVINST* 5239. 1A;)

Controlled Sharing

The condition which exists when access control is applied to all users and components of a resource-sharing ADP system. (*FIPS PUB* 39;; *AR* 380-380; *NCSC-WA*-001-85;)

Controlled Space

1. The three-dimensional space surrounding equipment that processes national security information within which unauthorized personnel are1) denied unrestricted access; and
2. enter escorted by authorized personnel or under continual physical or electronic surveillance. (*AFR* 700-10;)

Controller
In an automated radio, the device that commands the radio transmitter and receiver, and that performs processes, such as automatic link establishment, channel scanning and selection, link quality analysis, polling, sounding, message store and forward, address protection, and anti-spoofing. See also automatic link establishment.

Controlling
Official responsible for directing authority the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.

Controlling Authority
(CA) Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.

Controlling Paperwork Burden On The Public

Conversational Mode
A mode of communication similar to a conversation between two persons. See also duplex operation, Hamming code, interactive data transaction, push-to-talk operation.

Conversational Service
Any two-way, interactive telecommunications service providing real-time, end-to-end information transfer.

***-Conway's Law**
prov. The rule that the organization of the software and the organization of the software team will be congruent; originally stated as “If you have four groups working on a compiler, you'll get a 4-pass compiler”. The law was named after Melvin Conway, an early proto-hacker who wrote an assembler for the Burroughs 220 called SAVE. The name `SAVE' didn't stand for anything; it was just that you lost fewer card decks and listings because they all had SAVE written on them.

***-Cookbook**
1. n. [from amateur electronics and radio] A book of small code segments that the reader can use to do various magic things in programs. One current example is the “PostScript Language Tutorial and Cookbook” by Adobe Systems, Inc (Addison-Wesley, ISBN 0-201-10179-3), also known as the Blue Book which has recipes for things like wrapping text around arbitrary curves and making 3D fonts.
2. Cookbooks, slavishly followed, can lead one into voodoo programming, but are useful for hackers trying to monkey up small programs in unknown languages. This function is analogous to the role of phrasebooks in human languages.

***-Cooked Mode**
n. [UNIX, by opposition from raw mode] The normal character-input mode, with interrupts enabled and with erase, kill and other special-character interpretations performed directly by the tty driver. Oppose raw mode, rare mode. This term is techspeak under UNIX but jargon elsewhere; other operating systems often have similar mode distinctions, and the raw/rare/cooked way of describing them has spread widely along with the C language and other UNIX exports. Most generally, `cooked mode' may refer to any mode of a system that does extensive preprocessing before presenting data to a program.

***-Cookie**
n. A handle, transaction ID, or other token of agreement between cooperating programs. “I give him a packet, he gives me back a cookie. ” The claim check you get from a dry-cleaning shop is a perfect mundane example of a cookie; the only thing it's useful for is to relate a later transaction to this one (so you get the same clothes back). Compare magic cookie; see also fortune cookie.

***-Cookie File**
n. A collection of fortune cookies in a format that facilitates retrieval by a fortune program. There are several different cookie files in public distribution, and site admins often assemble their own from various sources including this lexicon.

***-Cookie Jar**
n. An area of memory set aside for storing cookies. Most commonly heard in the Atari ST community; many useful ST programs record their presence by storing a distinctive magic number in the jar. Programs can inquire after the presence or otherwise of other programs by searching the contents of the jar.

Cooperative Key
Electronically exchanging functions of generation locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.

Cooperative Key Generation
(CKG) Electronically exchanged functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.

Cooperative Remote

Cooperative Remote Rekeying
See Manual Remote Rekeying.

#-Coordination With Related Disciplines

This KSA has no definition.

*-Copper

n. Conventional electron-carrying network cable with a core conductor of copper -- or aluminum! Opposed to light pipe or, say, a short-range microwave link.

Copy Protected

1. Software distributed on diskettes rendered “uncopyable” by physical means.
2. See UNPROTECT.

*-Copy Protection

n. A class of methods for preventing incompetent pirates from stealing software and legitimate customers from using it. Considered silly.

*-Copyleft

1. /kop'ee-left/ n. [play on `copyright'] The copyright notice (`General Public License') carried by GNU EMACS and other Free Software Foundation software, granting reuse and reproduction rights to all comers (but see also General Public Virus).
2. By extension, any copyright notice intended to achieve similar aims.

#-Copyright Protection And Licensing

The right of the copyright owner to prevent copying or and issue permission for a user to employ a particular computer program. (Source: panel of experts).

Core

1. The center region of an optical fiber through which light is transmitted. (~) Note 1: Strictly speaking, in certain cases a significant fraction of the energy in a bound mode does travel in the cladding. Note 2: The refractive index of the core must be higher than that of the cladding. See also cladding, core diameter, fiber optics, normalized frequency, optical fiber.
2. A piece of magnetic material, usually toroidal in shape, used for computer storage.
3 . The material at the center of an electromechanical relay or coil winding. (~)
4. n. Main storage or RAM. Dates from the days of ferrite-core memory; now archaic as techspeak most places outside IBM, but also still used in the UNIX community and by old-time hackers or those who would sound like them. Some derived idioms are quite current; `in core', for example, means `in memory' (as opposed to `on disk'), and both core dump and the `core image' or `core file' produced by one are terms in favor. Some varieties of Commonwealth hackish prefer store.

*-Core Cancer

n. A process that exhibits a slow but inexorable resource leak -- like a cancer, it kills by crowding out productive `tissue'.

*-Core Dump

n. [common Iron Age jargon, preserved by UNIX]

1. [techspeak] A copy of the contents of core, produced when a process is aborted by certain kinds of internal error.
2. By extension, used for humans passing out, vomiting, or registering extreme shock. “He dumped core. All over the floor. What a mess. ” “He heard about X and dumped core. ”
3. Occasionally used for a human rambling on pointlessly at great length; esp. in apology “Sorry, I dumped core on you”.
4. A recapitulation of knowledge (compare bits, sense 1). Hence, spewing all one knows about a topic (syn. brain dump), esp. in a lecture or answer to an exam question. “Short, concise answers are better than core dumps” (from the instructions to an exam at Columbia). See core.

*-Core Leak

n. Syn. memory leak.

Core Storage

See magnetic core storage.

*-Core Wars

n. A game between `assembler' programs in a simulated machine, where the objective is to kill your opponent's program by overwriting it. Popularized by A. K. Dewdney's column in “Scientific American” magazine, this was actually devised by Victor Vyssotsky, Robert Morris Sr. , and Dennis Ritchie in the early 1960s (their original game was called `Darwin' and ran on a PDP-1 at Bell Labs). See core.

#-Corrective Actions

The activities of detecting, isolating and correcting failures after occurrence. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Correctness

1. In a strict sense, the property of a system that is guaranteed as a result of formal verification activities. Correctness is not an absolute property of a system, rather it implies the mutual consistency of a specification and its implementation. (MTR-8201;)
2. See VERIFICATION.

Correctness Proof

A mathematical proof of consistency between a specification and its implementation. It may apply at the security model-to-formal specification level, at the formalspecification-to-HOL code level, at the compiler level or at the hardware level. For example, if a system has a verified design and implementation, then its overall correctness rests with the correctness of the compiler and hardware. Once a system is proved cor-

rect, it can be expected to perform as specified, but not necessarily as anticipated if the specifications are incomplete or inappropriate. (MTR-8201;)

Correlated Emanations

(CORR E) Detected emanations which correspond to or contain a discernible relationship to any signal or process of known characteristics. Correlated emanations may be compromising under the definition of "compromising emanations. "

Cost

The total money, time and resources associated with a purchase or activity

Cost Accounting

The process of identifying and evaluating production costs

Cost Benefit Analysis

1. A procedure that attempts to provide some form of financial justification for the expenditure of funds; the justification is obtained by comparing costs, both initial and maintenance (calculated using discount rates to derive their "present values") with the values, year by year, of the potential benefits to be expected. (ET;)
2. A technique used for evaluating protective mechanisms. (RM;)

Cost Distribution

Cost Of Major Failures

Cost Recovery

Cost-Analysis

Cost-Benefit Analysis

Assessment of the costs of providing protection or security to a telecommunications or AIS versus risk and cost associated with asset loss or damage.

Cost-Risk Analysis

1. The assessment of the costs of potential risk of loss or compromise without data protection versus the cost of providing data protection. (*FIPS PUB* 39;; *AR* 380-380;)
2. The assessment of the costs of providing data protection for an automated information system versus the cost of losing or compromising the data. (*NCSC-WA*-001-85;) See Cost-Benefit Analysis.

#-Cost/Benefit Analysis

1. The assessment of the costs of potential risk of loss of compromise without data protection versus the cost of providing data protection. ;
2. The assessment of the costs of providing data protection for a system versus the cost of losing or compromising the data. (Source: NISTIR 4659).

Cost/Time Contamination

1. A parameter indicating the impact of the contamination of an asset. (RM;)
2. A Parameter indicating the impact of the Contamination of an Asset. (MK;)

Cost/Time Interruption

A parameter indicating the impact of the interruption of an asset. (RM;)

Costing Function

The loss in dollars as the result of an event as a function of the severity of the event. (RM;)

Cots Software

Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project. (JCS PUB 6-03. 7)

Counterfeit Access Device And Computer Fraud Act

Counterintelligence

That phase of intelligence covering all activity devoted to neutralizing the effectiveness of hostile foreign intelligence collection activities. *Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or terrorist activities, but not including personnel, physical, document, or communications security programs. See Foreign Counterintelligence (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Countermeasure

1. That form of military science which by the use of devices and techniques has as its objective the impairment of the operational effectiveness of enemy activity. (*AR* 380-380;)
2. Any action, device, procedure, technique, or other measure that reduces the vulnerability of an ADP system or activity to the realization of a threat. (*OPNAVINST* 5239. 1A;; *NCSC-WA*-001-85;)
3. An act, device, procedure, etc. , that may be used in one or more of the three protective areas: detection, prevention and recovery. To be effective, the countermeasure should be complete, correct, and self-protecting. Also called a mechanism. (RM;)
4. Any thing that effectively negates an adversary's ability to exploit vulnerabilities. *A design or procedural measure taken in defense against a security threat or vulnerability (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

#-Countermeasures

Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system. (Source: *NCSC-TG*-0004).

Coupling

Cover

1. To convert the transmitted waveform into an unusable form by means of transmission security (TRANSEC) and cryptographic techniques.
2. To conceal or alter characteristic communications patterns to hide information that could be of value to an adversary.
3. The act of maintaining a continuous receiver watch with transmitter calibrated and available, but not necessarily available for immediate use. (JCS1-DoD) (JCS1-NATO)
4. Those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information. (JCS1-DoD) (JCS1-NATO)
5. Protective action taken to mask or conceal an operation or activity from an adversary. *Those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information (Definition #2, JCS PUB 1-02, 6/89)

#-Cover And Deception

Tools and techniques used to hide identification, location, true intent, and other facts from potential adversaries. (Source: Panel of Experts, July 1994).

Covert Channel

1. A communication channel that allows a process to transfer information in a manner that violates the system's security policy. (CSC-STD-001-83;; CSC-STD-004-85;)
2. A communication channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy. (*NCSC-WA*-001-85;)
3. Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an AIS security policy. See Exploitable Channel, Overt Channel. COVERT STORAGE CHANNEL and COVERT TIMING CHANNEL.

#-Covert Channels

Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an AIS security policy. (Source: NSTISSI 4009). Note: Covert channels may be storage or timing channels. A covert storage channel involves the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. A covert timing channel is one in which one process signals information to another process by modulating its own use of system resources in such a way that this manipulation affects the real response time observed by the second process. (Source: *NCSC-TG*-029).

Covert Storage

Covert channel that involves the channel direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. NOTE: Covert storage channels typically involve a finite resource (e. g. , sectors on a disk) that is shared by two subjects at different security levels.

Covert Storage Channel

1. A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert channels typically involve a finite resource (e. g. , sectors on a disk) that is shared by two subjects at different security levels. (CSC-STD-001-83;; *NCSC-WA*-001-85;)
2. A covert channel which involves writing information to a storage location by one process and reading that storage location by a different process. (*AFR* 205-16).

Covert Storage Channels

Covert Timing

Covert channel in which one channel process signals information to another process by modulating its own use of system resources (e. g. , central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.

Covert Timing Channel

1. A covert channel in which one process signals information to another by modulating its own use of system resources (e. g. , CPU time) in such a way that this manipulation affects the real response time observed by the second process. (CSC-STD-001-83;; *NCSC-WA*-001-85;)
2. A covert channel in which one process modulates its use of system resources (CPU time) to manipulate the real response time observed by a second process thereby signaling information to the second process. (*AFR* 205-16)

*-CP/M

/C-P-M/ n. [Control Program/Monitor; later retconned to Control Program for Microcomputers] An early microcomputer OS written by hacker Gary Kildall for 8080- and Z80-based machines, very popular in the late 1970s but virtually wiped out by MS-DOS after the release of the IBM PC in 1981. Legend has it that Kildall's company blew its chance

to write the OS for the IBM PC because Kildall decided to spend a day IBM's reps wanted to meet with him enjoying the perfect flying weather in his private plane. Many of CP/M's features and conventions strongly resemble those of early DEC operating systems such as TOPS-10, OS/8, RSTS, and RSX-11. See MS-DOS, operating system.

CPU Registers

*-CPU Wars

/C-P-U worz/ n. A 1979 large-format comic by Chas Andres chronicling the attempts of the brainwashed androids of IPM (Impossible to Program Machines) to conquer and destroy the peaceful denizens of HEC (Human Engineered Computers). This rather transparent allegory featured many references to ADVENT and the immortal line “Eat flaming death, minicomputer mongrels!” (uttered, of course, by an IPM stormtrooper). It is alleged that the author subsequently received a letter of appreciation on IBM company stationery from the head of IBM's Thomas J. Watson Research Laboratories (then, as now, one of the few islands of true hackerdom in the IBM archipelago). The lower loop of the B in the IBM logo, it is said, had been carefully whited out. See eat flaming death.

*-Crack Root

v. To defeat the security system of a UNIX machine and gain root privileges thereby; see cracking.

*-Cracker

n. One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker (q. v. , sense 8). An earlier attempt to establish `worm' in this sense around 1981--82 on Usenet was largely a failure. Use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done). Thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe *themselves* as hackers, most true hackers consider them a separate and lower form of life. Ethical considerations aside, hackers figure that anyone who can't imagine a more interesting way to play with their computers than breaking into someone else's has to be pretty losing. Some other reasons crackers are looked down on are discussed in the entries on cracking and phreaking. See also samurai, dark-side hacker, and hacker ethic, the. For a portrait of the typical teenage cracker, see warez.

*-Cracking

n. The act of breaking into a computer system; what a cracker does. Contrary to widespread myth, this does not usually involve some mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers.

*-Crank

vt. [from automotive slang] Verb used to describe the performance of a machine, especially sustained performance. “This box cranks (or, cranks at) about 6 megaflops, with a burst mode of twice that on vectorized operations. ”

*-Crash

1. n. A sudden, usually drastic failure. Most often said of the system (q. v. , sense 1), esp. of magnetic disk drives (the term originally described what happened when the air gap of a hard disk collapses). “Three lusers lost their files in last night's disk crash. ” A disk crash that involves the read/write heads dropping onto the surface of the disks and scraping off the oxide may also be referred to as a `head crash', whereas the term `system crash' usually, though not always, implies that the operating system or other software was at fault.
2. v. To fail suddenly. “Has the system just crashed?” “Something crashed the OS!” See down. Also used transitively to indicate the cause of the crash (usually a person or a program, or both). “Those idiots playing SPACEWAR crashed the system. ”
3. vi. Sometimes said of people hitting the sack after a long hacking run; see gronk out.

*-Crash And Burn

vi. ,n. A spectacular crash, in the mode of the conclusion of the car-chase scene in the movie “Bullitt” and many subsequent imitators (compare die horribly). Sun-3 monitors losing the flyback transformer and lightning strikes on VAX-11/780 backplanes are notable crash and burn generators. The construction `crash-and-burn machine' is reported for a computer used exclusively for alpha or beta testing, or reproducing bugs (i. e. , not for development). The implication is that it wouldn't be such a disaster if that machine crashed, since only the testers would be inconvenienced.

*-Cray

1. /kray/ n. (properly, capitalized) One of the line of supercomputers designed by Cray Research.
2. Any supercomputer at all.
3. The canonical number-crunching machine. The term is actually the lowercased last name of Seymour Cray, a noted computer architect and cofounder of the company. Numerous vivid legends surround him, some true and some admittedly invented by Cray Research brass to shape their corporate culture and image.

*-Cray Instability

1. A shortcoming of a program or algorithm that manifests itself only when a large problem is being run on a powerful machine (see cray). Generally more subtle than bugs that can be detected in smaller problems running on a workstation or mini.
2. More specifically, a shortcoming of algorithms which are well behaved when run on gentle floating point hardware (such as IEEE-standard or DEC) but which break down badly when exposed to a Cray's unique `rounding' rules.

*-Crayola

/kray-oh'l*/ n. A super-mini or -micro computer that provides some reasonable percentage of supercomputer performance for an unreasonably low price. Might also be a killer micro.

*-Crayola Books

n. The rainbow series of National Computer Security Center (NCSC) computer security standards (see *Orange Book*). Usagehumorous and/or disparaging.

*-Creationism

n. The (false) belief that large, innovative software designs can be completely specified in advance and then painlessly magicked out of the void by the normal efforts of a team of normally talented programmers. In fact, experience has shown repeatedly that good designs arise only from evolutionary, exploratory interaction between one (or at most a small handful of) exceptionally able designer(s) and an active user population --- and that the first try at a big new idea is always wrong. Unfortunately, because these truths don't fit the planning models beloved of management, they are generally ignored.

Credentials

1. Information, passed from one entity to another, that is used to establish the sending entity's access rights.
2. Data that is transferred to establish the claimed identity of an entity. (SS;)

*-Creep

v. To advance, grow, or multiply inexorably. In hackish usage this verb has overtones of menace and silliness, evoking the creeping horrors of low-budget monster movies.

*-Creeping Elegance

n. Describes a tendency for parts of a design to become elegant past the point of diminishing return, something which often happens at the expense of the less interesting parts of the design, the schedule, and other things deemed important in the Real World. See also creeping featurism, second-system effect, tense.

*-Creeping Featurism

1. /kree'ping fee'chr-izm/ n. Describes a systematic tendency to load more chrome and features onto systems at the expense of whatever elegance they may have possessed when originally designed. See also feeping creaturism. “You know, the main problem with BSD UNIX has always been creeping featurism. ”
2. More generally, the tendency for anything complicated to become even more complicated because people keep saying “Gee, it would be even better if it had this feature too”. (See feature.) The result is usually a patchwork because it grew one ad-hoc step at a time, rather than being planned. Planning is a lot of work, but it's easy to add just one extra little feature to help someone . and then another . and another. When creeping featurism gets out of hand, it's like a cancer. Usually this term is used to describe computer programs, but it could also be said of the federal government, the IRS 1040 form, and new cars. A similar phenomenon sometimes afflicts conscious redesigns; see second-system effect. See also creeping elegance.

*-Creeping Featuritis

/kree'ping fee'-chr-i:`t*s/ n. Variant of creeping featurism, with its own spoonerization `feeping creaturitis'. Some people like to reserve this form for the disease as it actually manifests in software or hardware, as opposed to the lurking general tendency in designers' minds. (After all, -ism means `condition' or `pursuit of', whereas -itis usually means `inflammation of'.)

#-Criminal Prosecution

Is a proceeding instituted and carried on by due course of law, before a competent tribunal, for the purpose of determining the guilt or innocence of a person charged with a crime. (Source Blacks).

Criteria

See *DOD* TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA.

Critical Information

Information about friendly intentions, capabilities, or activities that must be protected from loss to keep an adversary from gaining a significant military, eco-

nomic, political, or technological advantage. *Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (JCS MOP 199, 3/89)

*-Critical Mass

n. In physics, the minimum amount of fissionable material required to sustain a chain reaction. Of a software product, describes a condition of the software such that fixing one bug introduces one plus epsilon bugs. (This malady has many causes creeping featurism, ports to too many disparate environments, poor initial design, etc.) When software achieves critical mass, it can never be fixed; it can only be discarded and rewritten.

Critical Processing

Processing which must continue in a correct and uninterrupted manner to support DoD emergency or war plans, preserve human life or safety, or support the mission of the using organization.

Critical Resources

Those physical and information assets required for the performance of the site mission. (DOE 5637. 1)

Critical Severity

The severity at which altered recovery strategies change the costing function. (RM;)

#-Critical Systems

Systems determined by management to be important for correct and uninterrupted function for national security, human life or safety, or the mission of the using organization. (Source: Panel of Experts, July 1994).

Critical Technology

Technologies that consist of a) arrays of design and manufacturing know-how (including technical data); b) keystone manufacturing, inspection, and test equipment; c) keystone materials; and d) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States. (Also referred to as military critical technology.) (DODD 2040. 2;; DODD 5230. 24;; DODD 5230. 25;)

Criticality

1. A concept related to the mission the automated system supports and the degree that the mission is dependent upon the system. This degree of dependence corresponds to the effect on the mission in the event of denial of service, modification, or destruction of data or software. (*AFR* 205-16;)
2. A parameter indicating the degree of dependence of the organization on an asset. (RM;)
3. A measure of how important the correct and uninterrupted functioning of the system is to national security, human life or safety, or the mission of the using organization; the degree to which the system performs critical processing. (*AFR* 205-16)

*-CRLF

/ker'l*f/, sometimes /kru'l*f/ or /C-R-L-F/ n. (often capitalized as `CRLF') A carriage return (CR, ASCII 0001101) followed by a line feed (LF, ASCII 0001010). More loosely, whatever it takes to get you from the end of one line of text to the beginning of the next line. See newline, terpri. Under UNIX influence this usage has become less common (UNIX uses a bare line feed as its `CRLF').

Cross Assembler

An assembler that can run symbolic-language input on one type of computer and produce machine-language output for another type of computer. (FP)

*-Cross-Post

[Usenet] vi. To post a single article simultaneously to several newsgroups. Distinguished from posting the article repeatedly, once to each newsgroup, which causes people to see it multiple times (which is very bad form). Gratuitous cross-posting without a Follow-up-To line directing responses to a single follow-up group is frowned upon, as it tends to cause follow-up articles to go to inappropriate newsgroups when people respond to only one part of the original posting.

Cross-Talk

1. An unwanted transfer of energy from one communications channel to another channel. (*FIPS PUB* 39; *AR* 380-380)
2. Undesired energy appearing in one signal path as a result of coupling from other signal paths. Path implies wires, waveguides, or other localized transmission systems. (NACSIM 5203)
3. A terminal communications package derived from MITE by MYCROFT labs (Larry Hughes)

*-Cruft

1. /kruhft/ [back-formation from crufty] n. An unpleasant substance. The dust that gathers under your bed is cruft; the TMRC Dictionary correctly noted that attacking it with a broom only produces more.
2. n. The results of shoddy construction.
3. vt. [from `hand cruft', pun on `hand craft'] To write assembler code for something normally (and better) done by a compiler (see hand-hacking).
4. n. Excess; superfluous junk; used esp. of redundant or superseded code. 5. [University of Wisconsin] n. Cruft is to hackers as gaggle is to geese;

that is, at UW one properly says “a cruft of hackers”. This term is one of the oldest in the jargon and no one is sure of its etymology, but it is suggestive that there is a Cruft Hall at Harvard University which is part of the old physics building; it's said to have been the physics department's radar lab during WWII. To this day (early 1993) the windows appear to be full of random techno-junk. MIT or Lincoln Labs people may well have coined the term as a knock on the competition.

*-Crunch

1. vi. To process, usually in a time-consuming or complicated way. Connotes an essentially trivial operation that is nonetheless painful to perform. The pain may be due to the triviality's being embedded in a loop from 1 to 1,000,000,000. “FORTRAN programs do mostly number-crunching. ”
2. vt. To reduce the size of a file by a complicated scheme that produces bit configurations completely unrelated to the original data, such as by a Huffman code. (The file ends up looking something like a paper document would if somebody crunched the paper into a wad.) Since such compression usually takes more computations than simpler methods such as run-length encoding, the term is doubly appropriate. (This meaning is usually used in the construction `file crunch(ing)' to distinguish it from number-crunching.) See compress.
3. n. The character `#'. Used at XEROX and CMU, among other places. See ASCII.
4. vt. To squeeze program source into a minimum-size representation that will still compile or execute. The term came into being specifically for a famous program on the BBC micro that crunched BASIC source in order to make it run more quickly (it was a wholly interpretive BASIC, so the number of characters mattered). Obfuscated C Contest entries are often crunched; see the first example under that entry.

*-Cryppie

/krip'ee/ n. A cryptographer. One who hacks or implements cryptographic software or hardware.

Crypt/Crypto

See Cryptographic-related.

Cryptanalysis

(CA) 1) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext. (SS;)

2. Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Crypto

A marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying classified national security information and sensitive, but unclassified government or government-derived information, the loss of which could adversely affect the national security interest. (NTISSI 4002; NACSI 8104) NOTE: When written in all upper case letters, CRYPTO has the meaning stated above. When written in lower case as a prefix, crypto and crypt are abbreviations for cryptographic.

Crypto Key

Deprecated term. See key.

Crypto-Alarm

Circuit or device which detects failures or aberrations in the logic or operation of crypto-equipment. NOTE: Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm.

Crypto-Algorithm

A well-defined procedure or sequence of rules or steps used to produce a key stream or cipher text from plain text and vice versa.

Crypto-Ancillary

Equipment designed specifically to equipment facilitate efficient or reliable operation of crypto-equipment, but that does not perform cryptographic functions.

Crypto-Ancillary Equipment

Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but which does not perform cryptographic functions.

Crypto-Equipment

Equipment that embodies a cryptographic logic.

Crypto-Ignition Key

Device or electronic key used to unlock the secure mode of crypto-equipment.

Crypto-Operation

The functional application of cryptographic methods. a) Off-line. Encryption or decryption performed as a self-contained operation distinct from the transmission of the encrypted text, as by hand or by machines not electrically connected to a signal line. b) On-line. The use of crypto-equipment that is directly connected to a signal line, making continuous processes of encryption and transmission or reception and decryption. (*AR* 380-380;)

Cryptoanalysis

The steps and operations performed in converting encrypted messages into plain text without initial

knowledge of the key employed in the encryption algorithm. (*FIPS PUB* 39;; *AR* 380-380;)

Cryptochannel

A complete system of crypto-communications between two or more holders. The basic unit for naval cryptographic communication. It includes: (a) the cryptographic aids prescribed; (b) the holders thereof; (c) the indicators or other means of identification; (d) the area or areas in which effective; (e) the special purpose, if any, for which provided; and (f) pertinent notes as to distribution, usage, etc. A cryptochannel is analogous to a radio circuit. (JCS1-DoD) See also channel, cryptology.

Cryptographic

(1) Pertaining to, or concerned with, cryptography. (2) Hardware or firmware embodiment of the component cryptographic logic. NOTE: Cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items. (3) Function used to set the state of initialization a cryptographic logic prior to key generation, encryption, or other operating mode. (4) Function which randomly determines the randomization transmit state of a cryptographic logic.

Cryptographic Authentication

The use of encryption related techniques to provide authentication. (WB;)

Cryptographic Checkvalue

Information which is derived by performing a cryptographic transformation on the data unit. Note: The derivation of the checkvalue may be performed in one or more steps and is a result of mathematical function of the key and a data unit. It is usually used to check the integrity of a data unit. (SS;)

Cryptographic Component

The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or information handling equipment. A cryptographic component may be a modular assembly, a printed circuit board, a microcircuit, or a combination of these items. (NTISSI 4001)

Cryptographic Equipment

Any equipment employing cryptotechniques or containing cryptographic circuitry or logic. (NACSEM 5201)

Cryptographic Information

All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial. (JCS1-DoD) See also ciphony, cryptology, cryptomaterial.

Cryptographic Initialization

Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

Cryptographic Key

A parameter (e. g. , a secret 64-bit number for DES) used by a cryptographic process that makes the process completely defined and usable only by those having that key. (*FIPS PUB* 112;)

Cryptographic Logic

Well-defined procedure or sequence of rules or steps used to produce cipher text from plain text, and vice versa, or to produce a key stream, plus delays, alarms, and checks which are essential to effective performance of the cryptographic process. See Cryptoalgorithm.

Cryptographic Randomization

Function which randomly determines the transmit state of a cryptographic logic.

Cryptographic System

The documents, devices, equipment, and associated techniques that are used as a unit to provide a means of encryption (enciphering or encoding). (*FIPS PUB* 39;; *AR* 380-380;)

#-Cryptographic Techniques

The employment of crypto algorithms in a computer, microprocessor, or microcomputer, or any other information system to perform encryption or decryption in order to protect information or to authenticate users, sources, or information. (Source: Panel of Experts, July 1994).

Cryptography

1. The art or science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form. (*FIPS PUB* 39; *AR* 380-380)
2. The protection of telecommunications by rendering information unintelligible or unrecognizable until it reaches the intended recipient. b. The design and use of cryptosystems. (NCSC-9)
3. The principles, means and methods for rendering information unintelligible and for restoring encrypted information to intelligible form. (*NCSC-TG*-004-88)

Cryptologic

Cryptology

1. The field that encompasses both cryptography and cryptoanalysis. (*FIPS PUB* 39; *AR* 380-380)
2. The science that deals with hidden, disguised, or encrypted communications. It embraces communi-

cations security and communication intelligence. (NCSC-9)

Cryptomaterial

1. All material including documents, devices, equipment, and apparatus essential to the encryption, decryption, or authentication of telecommunications. When classified, it is designated CRYPTO and subject to special safeguards. (JCS1-DoD)
2. All material, including documents, devices, or equipment that contains crypto information and is essential to the encryption, decryption or authentication of telecommunications. (JCS1-NATO) See also ciphony, cryptographic information, cryptology.

Cryptonet

Stations that hold a specific key for use. NOTE: Activities that hold key for other than use, such as cryptologistic depots, are not cryptonet members for that key. Controlling authorities are defacto members of the cryptonets they control.

Cryptoperiod

Time span during which each key setting remains in effect.

Cryptosecurity

1. The security or protection resulting from the proper use of technically sound cryptosystems.
2. Component of communications security that results from the provision of technically sound cryptosystems and their proper use.

Cryptosynchronization

Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.

Cryptosystem

1. Associated COMSEC items interacting to provide a single means of encryption or decryption.
2. Process of establishing the assessment exploitability of a cryptosystem, normally by reviewing transmitted traffic protected or secured by the system under study.
3. Process of determining vulnerabilities evaluation of a cryptosystem.

Cryptosystem Assessment

Process of establishing the exploitability of a cryptosystem, normally by reviewing transmitted traffic protected or secured by the system under study.

Cryptosystem Evaluation

Process of determining vulnerability of a cryptosystem.

Cryptosystem Review

Examination of a cryptosystem by the controlling authority to ensure its adequacy of design and content, continued need, and proper distribution.

Cryptosystem Survey

Management technique in which actual holders of a cryptosystem express opinions on the system's suitability and provide usage information for technical evaluations.

#-Cryptovariable

The unknown and changeable portion of the cryptographic logic. (Source Panel of experts).

*-CTSS

/C-T-S-S/ n. Compatible Time-Sharing System. An early (1963) experiment in the design of interactive time-sharing operating systems, ancestral to Multics, UNIX, and ITS. The name ITS (Incompatible Time-sharing System) was a hack on CTSS, meant both as a joke and to express some basic differences in philosophy about the way I/O services should be presented to user programs.

*-CTY

/sit'ee/ or /C-T-Y/ n. [MIT] The terminal physically associated with a computer's system console. The term is a contraction of `Console tty', that is, `Console TeleTYpe'. This ITS- and TOPS-10-associated term has become less common, as most UNIX hackers simply refer to the CTY as `the console'.

*-Cube

1. n. [short for `cubicle'] A module in the open-plan offices used at many programming shops. “I've got the manuals in my cube. ”
2. A NeXT machine (which resembles a matte-black cube).

Custodian Of Data

The individual or group that has been entrusted with the possession of, and responsibility for, the security of specified data. (WB;)

Customer

1. A person or organization who receives products that an automated system produces, but who does not have access to the system. Input and output must be reviewed by cleared knowledgeable people. (*AFR* 205- 16)
2. A civil or military department or agency of the government which uses keying material, classified or unclassified. (NACSI 2002A)
3. See ACCESS.

#-Customer IT Security Needs

This KSA has no definition.

#-Customer Service Orientation

This KSA has no definition.

*-Cut A Tape

vi. To write a software or document distribution on magnetic tape for shipment. Has nothing to do with physically cutting the medium! Early versions of this lexicon claimed that one never analogously speaks of `cutting a disk', but this has since been reported as live usage. Related slang usages are mainstream business's `cut a check', the recording industry's `cut a record', and the military's `cut an order'. All of these usages reflect physical processes in obsolete recording and duplication technologies. The first stage in manufacturing an old-style vinyl record involved cutting grooves in a stamping die with a precision lathe. More mundanely, the dominant technology for mass duplication of paper documents in pre-photocopying days involved “cutting a stencil”, punching away portions of the wax overlay on a silk screen. More directly, paper tape with holes punched in it was an important early storage medium.

*-Cyberspace

1. /si:'ber-spays/ n. Notional `information-space' loaded with visual cues and navigable with brain-computer interfaces called `cyberspace decks'; a characteristic prop of cyberpunk SF. At the time of this writing (mid-1991), serious efforts to construct virtual reality interfaces modeled explicitly on Gibsonian cyberspace are already under way, using more conventional devices such as glove sensors and binocular TV headsets. Few hackers are prepared to deny outright the possibility of a cyberspace someday evolving out of the network (see network, the).
2. Occasionally, the metaphoric location of the mind of a person in hack mode. Some hackers report experiencing strong eidetic imagery when in hack mode; interestingly, independent reports from multiple sources suggest that there are common features to the experience. In particular, the dominant colors of this subjective `cyberspace' are often gray and silver, and the imagery often involves constellations of marching dots, elaborate shifting patterns of lines and angles, or moire patterns.

*-Cycle

1. n. The basic unit of computation. What every hacker wants more of (noted hacker Bill Gosper describes himself as a “cycle junkie”). One can describe an instruction as taking so many `clock cycles'. Often the computer can access its memory once on every clock cycle, and so one speaks also of `memory cycles'. These are technical meanings of cycle. The jargon meaning comes from the observation that there are only so many cycles per second, and when you are sharing a computer the cycles get divided up among the users. The more cycles the computer spends working on your program rather than someone else's, the faster your program will run. That's why every hacker wants more cycles so he can spend less time waiting for the computer to respond.
2. By extension, a notional unit of *human* thought power, emphasizing that lots of things compete for the typical hacker's think time. “I refused to get involved with the Rubik's Cube back when it was big. Knew I'd burn too many cycles on it if I let myself. ”
3. vt. Syn. bounce (sense 4), 120 reset; from the phrase `cycle power'. “Cycle the machine again, that serial port's still hung. ”

Cycle (for Overwriting Memory, Disk, Etc.)

One overwrite cycle is defined as follows: write one bit pattern or character, then write the complement of that pattern or character into every addressable location or sector. (CSC-STD-005-85;)

*-Cycle Crunch

n. A situation wherein the number of people trying to use a computer simultaneously has reached the point where no one can get enough cycles because they are spread too thin and the system has probably begun to thrash. This scenario is an inevitable result of Parkinson's Law applied to timesharing. Usually the only solution is to buy more computer. Happily, this has rapidly become easier since the mid-1980s, so much so that the very term `cycle crunch' now has a faintly archaic flavor; most hackers now use workstations or personal computers as opposed to traditional timesharing systems.

*-Cycle Drought

n. A scarcity of cycles. It may be due to a cycle crunch, but it could also occur because part of the computer is temporarily not working, leaving fewer cycles to go around. “The high moby is down, so we're running with only half the usual amount of memory. There will be a cycle drought until it's fixed. ”

*-Cycle Server

n. A powerful machine that exists primarily for running large batch jobs. Implies that interactive tasks such as editing are done on other machines on the network, such as workstations.

Cyclic Redundancy Check

(CRC) Error-checking mechanism which checks data integrity by computing a polynomial algorithm based checkvalue. The “as received” checkvalue must match the “as sent” checkvalue, or there has been an error.

*-Cypherpunk

n. [from cyberpunk] One interested in the uses of encryption using electronic cyphers for enhancing personal privacy and guarding against tyranny by centralized, authoritarian power structures, especially

tralized, authoritarian power structures, especially government. There is an active cypherpunks mailing list at cypherpunks-request@toad. com coordinating work on public-key encryption freeware, privacy, and digital cash. See also tentacle.

D

D-A

Abbreviation for digital-to-analog. See digital transmission system.

*-D. C. Power Lab

n. The former site of SAIL. Hackers thought this was very funny because the obvious connection to electrical engineering was nonexistent -- the lab was named for a Donald C. Power. Compare Marginal Hacks.

Daemon

(1) A program that is executed automatically (without an explicit invocation) immediately on the completion of specific operation on the knowledge base. (MA;) (2) /day'mn/ or /dee'mn/ n. [from the mythological meaning, later rationalized as the acronym `Disk And Execution MONitor'] A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The idea is that the perpetrator of the condition need not be aware that a daemon is lurking (though often a program will commit an action only because it knows that it will implicitly invoke a daemon). For example, under ITS writing a file on the LPT spooler's directory would invoke the spooling daemon, which would then print the file. The advantage is that programs wanting (in this example) files printed need neither compete for access to nor understand any idiosyncrasies of the LPT. They simply enter their implicit requests and let the daemon decide what to do with them. Daemons are usually spawned automatically by the system, and may either live forever or be regenerated at intervals. Daemon and demon are often used interchangeably, but seem to have distinct connotations. The term `daemon' was introduced to computing by CTSS people (who pronounced it /dee'mon/) and used it to refer to what ITS called a dragon. Although the meaning and the pronunciation have drifted, we think this glossary reflects current (1993) usage.

*-Daemon Book

n. “The Design and Implementation of the 4. 3BSD UNIX Operating System”, by Samuel J. Leffler, Marshall Kirk McKusick, Michael J. Karels, and John S. Quarterman (Addison-Wesley Publishers, 1989, ISBN 0-201-06196-1) -- the standard reference book on the internals of BSD UNIX. So called because the cover has a picture depicting a little devil (a visual play on daemon) in sneakers, holding a pitchfork (referring to one of the characteristic features of UNIX, the `fork(2)' system call). Also known as the Devil Book.

*-Dangling Pointer

n. A reference that doesn't actually lead anywhere (in C and some other languages, a pointer that doesn't actually point at anything valid). Usually this happens because it formerly pointed to something that has moved or disappeared. Used as jargon in a generalization of its techspeak meaning; for example, a local phone number for a person who has since moved to the other coast is a dangling pointer.

Dangling Threat

A set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk. (MK;)

Dangling Vulnerability

A set of properties about the internal environment for which there is no corresponding threat and therefore no implied risk. (MK;)

*-Dark-Side Hacker

n. A criminal or malicious hacker; a cracker. From George Lucas's Darth Vader, “seduced by the dark side of the Force”. The implication that hackers form a sort of elite of technological Jedi Knights is intended. Oppose samurai.

Data

1. Information with a specific physical representation. (CSC-STD-001-83;);
2. A representation of facts, concepts, information, or instructions in a manner suitable for communication, interpretation, or processing by humans or by an AIS. (DODD 5200. 28;);
3. Programs, files or other information stored in, or processed by, a computer system; (*FIPS PUB* 112;) or
4. Information with a specific representation (loosely used to denote any or all information that can be produced, processed, stored or produced by a computer). (CSC-STD-005-85;)
5. An asset category consisting of the information handled by the organization. (RM;) See Information.

Data Abstraction

#-Data Access Control

Data Arrangement

In the public switched telephone networks, a single item or group of items present at the customer side of the network interface for data transmission purposes,

including all equipment that may affect the characteristics of the interface. See also data, data circuit-terminating equipment, data terminal equipment, data transmission, interface.

Data Attribute

A characteristic of a data element such as length, value, or method of representation. (FP)

Data Authentication Algorithm

Data Bank

A set of data related to a given subject and organized in such a way that it can be consulted by users. (FP) (ISO)

Data Base

An extensive and comprehensive set of records collected and organized in a meaningful manner to serve a particular purpose. (*DODD 3200. 12*;)

Data Base Management System

DBMS

Data Burst

Synonym burst transmission.

Data Bus

A bus used to transfer data within or to and from a processing unit or storage device. See also bus.

Data Communication

The transfer of information between functional units by means of data transmission according to a protocol. (FP) (ISO) (~)

Data Communication Control Character

See control character.

Data Communication Control Procedure

A means used to control the orderly communication of information among stations in a data communication network. See also data, data transmission, serial access, serial transmission.

Data Communications Equipment

Deprecated term. See data circuit-terminating equipment.

Data Compaction

Synonym data compression.

Data Compression

1. The process of reducing (a) bandwidth, (b) cost, and (c) time for the generation, transmission, and storage of data by employing techniques designed to remove data redundancy.
2. The use of techniques such as null suppression, bit mapping, and pattern substitution for purposes of reducing the amount of space required for storage of textual files and data records. (FP) (ISO) Note: Some data compaction methods employ fixed tolerance bands, variable tolerance bands, slope-keypoints, sample changes, curve patterns, curve fitting, floating-point coding, variable precision coding, frequency analysis, and probability analysis. (Simply squeezing noncompacted data into a smaller space, e. g. , by transferring data on punched cards onto magnetic tape, is not considered data compression.) Synonym data compaction. See also concentrator, data, data transmission, redundancy.

Data Concentrator

A functional unit that permits a common transmission medium to serve more data sources than there are channels currently available within the transmission medium. (FP) (ISO) See also concentrator, multiplexer.

Data Contamination

A deliberate or accidental process or act that results in a change in the integrity of the original data. (*AR* 380-380;; *FIPS PUB* 39;). See Data Diddling.

Data Corruption

The violation of data integrity. (FP) (ISO) (~) Synonym data contamination. See also data, data integrity, data transmission.

Data Dictionary

1. A part of a database management system that provides a centralized repository of information about data, such as meaning, relationship to other data, origin, usage, and format. (~)
2. An inventory that describes, defines, and lists all of the data elements that are stored in a database (FP) (~) See also database management system.

Data Diddling

1. [.] the entering of false data into a computer system. (TC;).
2. Process of accidentally or maliciously changing data before or during the input or output to a computer. The changes can be made by anyone associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, or transforming the data. See Data Contamination.

Data Directory

An inventory that specifies the source, location, ownership, usage, and destination of all of the data elements that are stored in a database. (FP)

Data Element

1. A named unit of data that, in some contexts, is considered indivisible and in other contexts may consist of data items. (FP) (ISO)

2. A named identifier of each of the entities and their attributes that are represented in a database. (FP)
3. A basic unit of information having a unique meaning and subcategories (data items) of distinct units or values. Examples of data elements are military personnel grade, sex, race, geographic location, and military unit. (JCS1-DoD)

Data Encrypting Key

A cryptographic key used for encrypting (and decrypting) data. (*FIPS PUB* 112;)

Data Encryption

Cryptographic algorithm, designed for standard the protection of unclassified data and published by the National Institute of Standards and Technology in Federal Information Processing Standard Publication 46.

Data Encryption Standard

1. (DES) An unclassified crypto algorithm adopted by the National Bureau of Standards for public use. (*NCSC-WA*-001-85;)
2. A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use.

Data Flow Control

See Information Flow Control.

Data Integrity

1. The state that exists when data is being handled as intended and has not been exposed to accidental or malicious modification or destruction. (DODD 5200. 28;)
2. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. (*FIPS PUB* 39;)
3. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, disclosure, or destruction. (*OPNAVINST* 5239. 1A;; *AFR* 205-16;; *AR* 380-380;; CSC-STD-001-83;; *NCSC-WA*-001-85;)
4. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or willful alteration or destruction. (*AFR* 205-16)
5. The property that data meets an prior expectation of quality. (*NCSC-TG*-004-88)

Data Intelligence

(DATAINT) Intelligence information derived from the unauthorized acquisition of data or information stored or processed by Automated Information Systems (AIS).

Data Interface Capability

The designed capability of equipment to interface directly with equipment that conforms to other interfacing standards without the need for external modems.

Data Item

1. A named component of a data element; usually the smallest component. (FP)
2. A subunit of descriptive information or value classified under a data element. For example the data element “military personnel grade” contains data items such as sergeant, captain, and colonel. (JCS1-DoD)

Data Level

1. Level I. Classified data.
2. Level II. Unclassified data requiring special protection; for example Privacy Act, For Official Use Only, technical documents restricted to limited distribution.
3. Level III. All other unclassified data. (*OPNAVINST* 5239. 1A;) Note: There are several other levels of security classification of data, for example Classified, Secret, Top Secret, in use by various US Government agencies.

Data Link

1. The means of connecting one location to another for the purpose of transmitting and receiving data. (JCS1-DoD) (JCS1-NATO)
2. The assembly of parts of two DTEs that are controlled by a link protocol, and that, together with the interconnecting data circuit, enables data to be transferred from a data source to a data sink. (~) See also data, data terminal equipment, data transmission, link, Open Systems Interconnection--Reference Model, tactical data information link.

Data Link Control

See Advanced Data Communications Control Procedures, binary synchronous communication, high-level data-link control, Open Systems Interconnection--Reference Model, synchronous data link control.

Data Link Escape Character

A transmission control character that changes the meaning of a limited number of contiguously following characters or coded representations. (FP) (ISO) See also character, control character.

Data Link Layer

See Open Systems Interconnection--Reference Model.

Data Mode

The state of a DCE when connected to a communication channel but not in a talk or dial mode. See also

data, data circuit-terminating equipment, data transmission, mode.

Data Origin
Corroboration that the source of data is authentication as claimed.

Data Origin Authentication
The corroboration that the source of data received is as claimed. (SS;)

Data Owner
The authority, individual, or organization who has original responsibility for the data by statute, executive order, or directive. (DODD 5200. 28)

Data Processing
The systematic performance of operations upon data such as handling, merging, sorting, and computing. (FP) (ISO) (~) Note: The semantic content of the data may or may not be changed. Synonym information processing. See also automatic data processing, data.

#-Data Processing Center Security
This KSA has no definition.

Data Processing Fund

Data Protection Engineering
The methodology and tools used for designing and implementing data protection mechanisms. (*FIPS PUB* 39;) See Security Engineering.

Data Related Emanations
(DRE) Detected emanations which have a discernible relationship with a signal related to the data processed by the EUT, and have been analyzed and determined to be not compromising.

Data Scavenging

Data Scrambler
A device used in digital transmission systems to convert an input digital signal into a pseudorandom sequence free from long runs of marks, spaces, or other simple repetitive patterns. Note: This facilitates timing extraction and reduces the accumulation of jitter. See also randomizer, scrambler.

Data Security
1. The protection of data from accidental or malicious modification, destruction, or disclosure. (*FIPS PUB* 39;)
2. The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; *NCSC-WA*-001-85;)

Data Service Unit
1. A device used for interconnecting data terminal equipment for the public telephone network.
2. A type of short-haul, synchronous-data line driver, normally installed at a user location, that connects a user's synchronous equipment over a 4-wire circuit at a preset transmission rate to a servicing dial-central-office. Note: This service can be for a point-to-point or multipoint operation in a digital data network. See also customer service unit.

Data Set
Deprecated term. See data circuit-terminating equipment.

Data Sink
See communications sink.

Data Source
See communications source.

Data Station
The data terminal equipment, the data circuit-terminating equipment, and any intermediate equipment. Note: The data terminating equipment may be connected directly to a data processing system or may be a part of the latter. (FP) (ISO) See also data, data circuit-terminating equipment, data terminal equipment, and data transmission.

Data Stream
A sequence of digitally encoded signals used to represent information for transmission. See also bit stream transmission, code, data, data transmission, and serial transmission.

Data Terminal Equipment
1. Digital end instruments that convert the user information into data signals for transmission, or reconvert the received data signals into user information. (~)
2. The functional unit of a data station that serves as a data source or a data sink and provides for the data communication control function to be performed in accordance with link protocol. Note: The DTE may consist of a single piece of equipment that provides all the required functions necessary to permit the user to intercommunicate, or it may be an interconnected subsystem of multiple pieces of equipment, to perform all the required functions.

Data Transfer Rate
The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (FP) (ISO) (~) See also binary digit, block, block transfer rate, character, data signaling rate, data transmission, effective data transfer rate, throughput.

Data Transfer Request Signal
A call control signal transmitted by a DCE to a DTE to indicate that a distant DTE wants to exchange data. See also call, call control signal, data, data circuit-

terminating equipment, data terminal equipment, data transmission, signal.

Data Transfer Time

The time that elapses between the initial offering of a unit of user data to a network by transmitting data terminal equipment and the complete delivery of that unit to receiving data terminal equipment. (~) See also block transfer rate, data, data transmission, throughput, transmission time, transmit flow control.

Data Transmission

The conveying of data from one place for reception elsewhere by telecommunication means. (FP) (ISO) (~)

Data Transmission Circuit

The transmission media and intervening equipment used for the transfer of data between DTEs. (~) Note 1: A data transmission circuit includes any required signal conversion equipment. Note 2: A data transmission circuit may support the transfer of information in one direction only, in either direction alternately, or in both directions simultaneously. See also channel, circuit, data circuit, data phase, data terminal equipment, data transmission.

Data Volatility

Pertaining to the rate of change in the values of stored data over a period of time. (FP)

Data-Dependent Protection

Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements. (*FIPS PUB* 39; *AR* 380-380;)

Database

1. A set of data that is required for a specific purpose or is fundamental to a system, project, enterprise, or business. (~) Note: A database may consist of one or more data banks and be geographically distributed among several repositories.
2. An extensive and comprehensive set of records collected and organized in a meaningful manner to serve a particular purpose. (*DODD 3200. 12*)

#-Database Integrity

That attribute of data relating to the preservation of (a) its meaning and completeness, (b) the consistency of its representation(s), and (c) its correspondence to what it represents. (Source: *NCSC-TG*-029).

Database Management System

1. A computer-based system used to establish, make available, and maintain the integrity of a database. (~)
2. An integrated set of computer programs that collectively provide all of the capabilities required for centralized management, organization, and control of access to a database that is shared by many users. (FP) (~) See also data dictionary, facility.

Datagram

In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment to the destination data terminal equipment, without relying on earlier exchanges between the equipment and the network. (FP) (ISO) Note: Unlike virtual call service, there are no call establishment or clearing procedures, and the network does not generally provide protection against loss, duplication, or misdelivery. See also connectionless mode transmission, data, data transmission, packet switching, virtual call capability.

DATAINT

Data Intelligence

*-Datamation

/day`t*-may'sh*n/ n. A magazine that many hackers assume all suits read. Used to question an unbelieved quote, as in “Did you read that in “Datamation?”” It used to publish something hackishly funny every once in a while, like the original paper on COME FROM in 1973, and Ed Post's “Real Programmers Don't Use Pascal” ten years later, but it has since become much more exclusively suit-oriented and boring.

Date And Time Of Event

Dating Format

The format employed to express the time of an event. (~) Note: The time of an event on the UTC time scale is given in the following sequence: hour, day, month, year; e. g. , 0917 UT, 30 August 1997. The hour is designated by the 24-hour system. See also Coordinated Universal Time (UTC).

*-DAU

/dow/ [German FidoNet] n. German acronym for D”ummster Anzunehmender User (stupidest imaginable user). From the engineering-slang GAU for Gr”osster Anzunehmender Unfall, worst foreseeable accident, esp. of a LNG tank farm plant or something with similarly disastrous consequences. In popular German, GAU is used only to refer to worst-case nuclear acidents such as a core meltdown. See cretin, fool, loser and weasel.

*-Day Mode

n. See phase (sense 1). Used of people only.

DC Erasure

1. Using a magnetic field produced by an electromagnet operating on Direct Current (DC) to degauss (purge) magnetic storage media. See AC Erasure and Clear.

2. Degaussing with a hand-held permanent magnet or with DC electrical-powered equipment to saturate the media so the noise level is raised to mask the signal level There should be no signal level detectable above the noise level after DC erasure. (*AFR* 205-16)

*-Dd

/dee-dee/ vt. [UNIX from IBM JCL] Equivalent to cat or BLT. Originally the name of a UNIX copy command with special options suitable for block-oriented devices; it was often used in heavy-handed system maintenance, as in "Let's `dd' the root partition onto a tape, then use the boot PROM to load it back on to a new disk". The UNIX `dd(1)' was designed with a weird, distinctly non-UNIXy keyword option syntax reminiscent of IBM System/360 JCL (which had an elaborate DD `Dataset Definition' specification for I/O devices); though the command filled a need, the interface design was clearly a prank. The jargon usage is now very rare outside UNIX sites and now nearly obsolete even there, as `dd(1)' has been deprecated for a long time (though it has no exact replacement). The term has been displaced by BLT or simple English `copy'.

*-DDT

/D-D-T/ n.

1. Generic term for a program that assists in debugging other programs by showing individual machine instructions in a readable symbolic form and letting the user change them. In this sense the term DDT is now archaic, having been widely displaced by `debugger' or names of individual programs like `adb', `sdb', `dbx', or `gdb'.
2. [ITS] Under MIT's fabled ITS operating system, DDT (running under the alias HACTRN) was also used as the shell or top level command language used to execute other programs.
3. Any one of several specific DDTs (sense 1) supported on early DEC hardware. The DEC PDP-10 Reference Handbook (1969) contained a footnote on the first page of the documentation for DDT that illuminates the origin of the term Historical footnote DDT was developed at MIT for the PDP-1 computer in 1961. At that time DDT stood for "DEC Debugging Tape". Since then, the idea of an on-line debugging program has propagated throughout the computer industry. DDT programs are now available for all DEC computers. Since media other than tape are now frequently used, the more descriptive name "Dynamic Debugging Technique" has been adopted, retaining the DDT abbreviation. Confusion between DDT-10 and another well known pesticide, dichloro-diphenyl-trichloroethane (C14-H9-Cl5) should be minimal since each attacks a different, and apparently mutually exclusive, class of bugs. (The `tape' referred to was, incidentally, not magnetic but paper. ) Sadly, this quotation was removed from later editions of the handbook after the suits took over and DEC became much more `businesslike'. The history above is known to many old-time hackers. But there's more Peter Samson, compiler of the original TMRC lexicon, reports that he named `DDT' after a similar tool on the TX-0 computer, the direct ancestor of the PDP-1 built at MIT's Lincoln Lab in 1957. The debugger on that ground-breaking machine (the first transistorized computer) rejoiced in the name FLIT (FLexowriter Interrogation Tape).

*-De-Rezz

/dee-rez'/ [from `de-resolve' via the movie "Tron"] (also `derez')

1. vi. To disappear or dissolve; the image that goes with it is of an object breaking up into raster lines and static and then dissolving. Occasionally used of a person who seems to have suddenly `fuzzed out' mentally rather than physically. Usage extremely silly, also rare. This verb was actually invented as *fictional* hacker jargon, and adopted in a spirit of irony by real hackers years after the fact.
2. vt. The Macintosh resource decompiler. On a Macintosh, many program structures (including the code itself) are managed in small segments of the program file known as `resources'; `Rez' and `DeRez' are a pair of utilities for compiling and decompiling resource files. Thus, decompiling a resource is `derezzing'. Usagevery common.

*-Dead

1. adj. Non-functional; down; crashed. Especially used of hardware.
2. At XEROX PARC, software that is working but not undergoing continued development and support.
3. Useless; inaccessible. Antonym`live'. Compare dead code.

*-Dead Code

n. Routines that can never be accessed because all calls to them have been removed, or code that cannot be reached because it is guarded by a control structure that provably must always transfer control somewhere else. The presence of dead code may reveal either logical errors due to alterations in the program or significant changes in the assumptions and environment of the program (see also software rot); a good compiler should report dead code so a maintainer can think about what it means. (Sometimes it simply means that an *extremely* defensive programmer has inserted can't happen tests which really can't happen -- yet.) Syn. grunge. See also dead.

*-DEADBEEF

/ded-beef/ n. The hexadecimal word-fill pattern for freshly allocated memory (decimal -21524111) under a number of IBM environments, including the RS/6000. Some modern debugging tools deliberately fill freed memory with this value as a way of converting heisenbugs into Bohr bugs. As in “Your program is DEADBEEF” (meaning gone, aborted, flushed from memory); if you start from an odd half-word boundary, of course, you have BEEFDEAD. See also the anecdote under fool.

*-Deadlock

1. n. [techspeak] A situation wherein two or more processes are unable to proceed because each is waiting for one of the others to do something. A common example is a program communicating to a server, which may find itself waiting for output from the server before sending anything more to it, while the server is similarly waiting for more input from the controlling program before outputting anything. (It is reported that this particular flavor of deadlock is sometimes called a `starvation deadlock', though the term `starvation' is more properly used for situations where a program can never run simply because it never gets high enough priority. Another common flavor is `constipation', in which each process is trying to send stuff to the other but all buffers are full because nobody is reading anything.) See deadly embrace.
2. Also used of deadlock-like interactions between humans, as when two people meet in a narrow corridor, and each tries to be polite by moving aside to let the other pass, but they end up swaying from side to side without making any progress because they always move the same way at the same time.

*-Deadly Embrace

n. Same as deadlock, though usually used only when exactly two processes are involved. This is the more popular term in Europe, while deadlock predominates in the United States.

Deallocation

*-Death Code

n. A routine whose job is to set everything in the computer -- registers, memory, flags, everything -- to zero, including that portion of memory where it is running; its last act is to stomp on its own “store zero” instruction. Death code isn't very useful, but writing it is an interesting hacking challenge on architectures where the instruction set makes it possible, such as the PDP-8 (it has also been done on the DG Nova). Perhaps the ultimate death code is on the TI 990 series, where all registers are actually in RAM, and the instruction “store immediate 0” has the opcode “0”. The PC will immediately wrap around core as many times as it can until a user hits HALT. Any empty memory location is death code. Worse, the manufacturer recommended use of this instruction in startup code (which would be in ROM and therefore survive).

*-Death Square

n. The corporate logo of Novell, the people who acquired USL after AT&T let go of it. Coined by analogy with Death Star, because many people believe that Novell is bungling the lead in UNIX systems exactly as AT&T did for many years.

*-Death Star

n. [from the movie “Star Wars”]

1. The AT&T corporate logo, which appears on computers sold by AT&T and bears an uncanny resemblance to the Death Star in the movie. This usage is particularly common among partisans of BSD UNIX, who tend to regard the AT&T versions as inferior and AT&T as a bad guy. Copies still circulate of a poster printed by Mt. Xinu showing a starscape with a space fighter labeled 4. 2 BSD streaking away from a broken AT&T logo wreathed in flames.
2. AT&T's internal magazine, “Focus”, uses `death star' to describe an incorrectly done AT&T logo in which the inner circle in the top left is dark instead of light -- a frequent result of dark-on-light logo images.

Debug

To detect, trace, and eliminate mistakes. (~)

*-DEC

1. n. Digital Equipment Corporation. Before the killer micro revolution of the late 1980s, hackerdom was closely symbiotic with DEC's pioneering timesharing machines. The first of the group of cultures described by this lexicon nucleated around the PDP-1 (see TMRC. Subsequently, the PDP-6, PDP-10, PDP-20, PDP-11 and VAX were all foci of large and important hackerdoms, and DEC machines long dominated the ARPANET and Internet machine population. DEC was the technological leader of the minicomputer era (roughly 1967 to 1987), but its failure to embrace microcomputers and UNIX early cost it heavily in profits and prestige after silicon got cheap. However, the microprocessor design tradition owes a heavy debt to the PDP-11 instruction set, and every one of the major general-purpose microcomputer OSs so far (CP/M, MS-DOS, UNIX, OS/2) were either genetically descended from a DEC OS, or incubated on DEC hardware, or both. Accordingly, DEC is still regarded with a certain wry affection even among many hackers too

young to have grown up on DEC machines. The contrast with IBM is instructive.

2. /dek/ v. Verbal (and only rarely written) shorthand for decrement, i. e. `decrease by one'. Especially used by assembly programmers, as many assembly languages have a `dec' mnemonic. Antonym inc.

*-DEC Wars

n. A 1983 Usenet posting by Alan Hastings and Steve Tarr spoofing the “Star Wars” movies in hackish terms. Some years later, ESR (disappointed by Hastings and Tarr's failure to exploit a great premise more thoroughly) posted a 3-times-longer complete rewrite called “UNIX WARS”; the two are often confused.

*-Decay

n. ,vi [from nuclear physics] An automatic conversion which is applied to most array-valued expressions in C; they `decay into' pointer-valued expressions pointing to the array's first element. This term is borderline techspeak, but is not used in the official standard for the language.

Deception

Activities undertaken to mislead an adversary. *Those measures designed to mislead a foreign power, organization, or person by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89) See electronic deception.

Deception Means

Methods, resources, and techniques that can be used to control administrative, physical, and technical actions in order to convey or deny information and indicators to foreign targets.

1. Administrative Means Resources, methods, and techniques designed to convey or deny oral, pictorial, documentary or other physical evidence;
2. Physical Means Methods, resources, and techniques to convey or deny selected indicators derivable from foreign observations, imagery, or active sensor surveillance of physical entities and actions;
3. Technical Means Methods, resources, and techniques to convey or deny selected indicators derivable from electromagnetic, acoustic, or other forms of energy; the emission or suppression of nuclear particles; or other phenomena detectable by passive sensors (JCS PUB 3-54, 9/89)

Decertification

Revocation of the certification of an AIS item or equipment for cause.

Decipher

1. To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into plain text. (*AR* 380-380)
2. To convert, by use of the appropriate key, enciphered (encoded or enciphered) text into plain text. (*FIPS PUB* 39)
3. To convert enciphered text into its equivalent plain text by means of cipher system. (This does not include solution by cryptanalysis.) (NACSEM 5201; NCSC-9)

Decipherment

The reversal of a corresponding reversible encipherment. (SS;)

*-Deckle

/dek'l/ n. [from dec- and nybble; the original spelling seems to have been `decle'] Two nickles; 10 bits. Reported among developers for Mattel's GI 1600 (the Intellivision games processor), a chip with 16-bit-wide RAM but 10-bit-wide ROM. See nybble for other such terms.

Declassification

Administrative decision or procedure to remove or reduce the security classification of the subject media. See Clear and Purge.

Declassification (of Magnetic Storage Media)

An administrative action following purging of the AIS or magnetic storage media that is the audited step that the owner of the AIS or medium takes when the classification is lowered to UNCLASSIFIED. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities. (*NCSC-TG*-004-88)

Declassification Of AIS Storage Media

An administrative decision or procedure to remove or reduce the security classification of the subject media.

Declassification Of Magnetic Storage Media

A procedure which will totally remove all of the classified or sensitive information stored on magnetic media followed by a review of the procedure performed. A decision can then be made for (or against) actual removal of the classification level of the media. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities. (CSC-STD-005-85;; *NCSC-WA*-001-85;)

#-Declassification/Downgrade Of Media

1. An administrative decision or procedure to remove or reduce the security classification of the subject media. (Source: *NCSC-TG*-0004)
2. Process to lower classification of either mag media or storage devices in preparation for reuse or disposal. (Source: DACUM IV).

Decode

1. To convert encoded text into its equivalent plain text by means of code. (NCSC-9)

2. Synonymous with DECRYPT.

Decrypt

1. To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into plain text. (*AR* 380-380;)
2. To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into its equivalent plain text. (*FIPS PUB* 39;) Synonymous with DECODE.

*-DED

/D-E-D/ n. Dark-Emitting Diode (that is, a burned-out LED). Compare SED, LER, write-only memory. In the early 1970s both Signetics and Texas instruments released DED spec sheets as AFJs (suggested uses included "as a power-off indicator").

#-Dedicated Line

1. A communications circuit reserved for the exclusive use of a customer. (Source: Panel of Experts, July 1994);
2. a circuit or channel that has been reserved or committed for a specific use or application, eg, for emergency purposes.

#-Dedicated Mode

AIS security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

a. Valid security clearance for all information within the system.
b. Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).
c. Valid need-to-know for all information contained within the AIS.

NOTE: When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

.

Dedicated Security Mode

1. The mode of operation in which all users have the appropriate clearance and need-to-know for all data in the system. The system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information either for full-time operation or for a specified period of time. (*AFR* 205-16;)
2. A mode of operation in effect when all users with access have both a clearance and need-to-know for all information in the information system. Processing may be in this mode full time or for specific periods of time. (*AFR* 700-10;)
3. The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (CSC-STD-003-85;)
4. A mode of operation wherein all users have the clearance, formal access approval, and need-to-know for all data handled by the AIS. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. (DODD 5200. 28;; *NCSC-WA*-001-85;)
5. An ADP system is operating in a dedicated mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specified users or groups of users for the processing of a particular type(s) and category(ies) of classified information. (DODD 5200. 28M;)
6. The operation of an ADP system such that the central computer facility, the connected peripheral devices, the communications facilities, and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information. (*FIPS PUB* 39;)
7. An ADP system is operating in the dedicated security mode when the Central Computer Facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or group of users having a security clearance and need-to-know for the processing of a particular category(ies) and type(s) of classified material. (*OPNAVINST* 5239. 1A;)

*-Deep Hack Mode

n. See hack mode.

*-Deep Magic

n. [poss. from C. S. Lewis's "Narnia" books] An awesomely arcane technique central to a program or system, esp. one neither generally published nor available to hackers at large (compare black art); one that could only have been composed by a true wizard. Compiler optimization techniques and many aspects of OS design used to be deep magic; many techniques in cryptography, signal processing, graphics, and AI still are. Compare heavy wizardry. Esp. found in comments of the form "Deep magic begins here. ". Compare voodoo programming.

*-Deep Space

n.

Describes the notional location of any program that has gone off the trolley. Esp. used of programs that just sit there silently grinding long after either failure or some output is expected. "Uh oh. I should have

gotten a prompt ten seconds ago. The program's in deep space somewhere. ” Compare buzz, catatonic, hyperspace.
The metaphorical location of a human so dazed and/or confused or caught up in some esoteric form of bogosity that he or she no longer responds coherently to normal communication. Compare page out.

Default Classification

A temporary classification, reflecting the highest classification being processed in an automated system. The default classification is included in the safeguard statement affixed to the product. (*AR* 380-380;; *NCSC-WA*-001-85;)

Defence Industry Information

Technical planning, requirements, and acquisition information provided to industry through various programs to enable industry to meet defence weapons and support systems needs. The programs include *DOD* IACs, potential contractor programs of *DOD* components, advanced planning briefings for industry, technical meetings on special topics, and similar services initiated by the OUSDR&E and other *DOD* components. (*DODD 3200. 12*;)

*-Defenestration

1. n. [from the traditional Czechoslovakian method of assassinating prime ministers, via SF fandom] Proper karmic retribution for an incorrigible punster. “Oh, ghod, that was *awful*!” “Quick! Defenestrate him!”
2. The act of exiting a window system in order to get better response time from a full-screen program. This comes from the dictionary meaning of `defenestrate', which is to throw something out a window.
3. The act of discarding something under the assumption that it will improve matters. “I don't have any disk space left. ” “Well, why don't you defenestrate that 100 megs worth of old core dumps?”
4. [proposed] The requirement to support a command-line interface. “It has to run on a VT100. ” “Curses! I've been defenestrated!”

Defense Data Network

The Department of Defense integrated packet switching network capable of worldwide multilevel secure and non-secure data transmission.

*-Defined As

adj. In the role of, usually in an organization-chart sense. “Pete is currently defined as bug prioritizer. ” Compare logical.

Definition

A figure of merit for image quality. (~) Note: For video-type displays, it is normally expressed in terms of the smallest resolvable element of the reproduced received image, e. g. , lines per inch, pels per square inch. See also facsimile, resolution.

Definition Of Security Features

Degauss

1. To reduce magnetic flux density to zero by applying a reverse (coercive) magnetizing force. Commonly referred to as demagnetizing. (CSC-STD-005-85;; *NCSC-WA*-001-85;)
2. To apply a variable, aternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; *FIPS PUB* 39;)
3. To demagnetize, thereby removing magnetic memory. (JCS PUB 6-03. 7)
4. To reduce magnetic flux density to zero by applying a reverse magnetizing field. Also referred to as demagnetizing. (*NCSC-TG*-004-88)

Degausser

1. An electrical device (AC or DC) or a hand-held magnet assembly which can generate coercive magnetic force for the purpose of degaussing magnetic storage media or other magnetic material. (CSC-STD-005-85)
2. An electrical device that can generated magnetic field for the purpose of degauss in a magnetic storage media. (*NCSC-TG*-004-88)

Degausser Products List (DPL)

1. A list of commercially produced degaussers that meet National Security Agency specifications. This list is included in the NSA Information Systems Security Products and Services Catalogue, and is available through the Government Printing Office. (AF9K_JBC. TXT)
2. List of commercially produced degaussers that meet National Security Agency (NSA) specifications. This list is included in the NSA Information Systems Security Products and Services Catalogue, and is available through the Government Printing Office. Degree of Trust. Level of confidence in security mechanisms and procedures to correctly enforce a specified security policy. Delegated Development Program. Information systems security program in which the Director, National Security Agency, delegates the development and/or production of the entire telecommunications product, including the information systems security portion, to a lead department or agency.

Degree Of Trust

The level of confidence that can be placed in security mechanisms to correctly enforce the security policy. (*AFR* 205-16;)

*-Dehose

/dee-hohz/ vt. To clear a hosed condition.

Delegated Development

Information systems security program program in which the Director, National Security Agency, delegates the development and/or production of the entire telecommunica-tions product, including the information systems security portion, to a lead department or agency.

Delegated Development Program

Information systems security program in which the NSA Director delegates the development and, or production of the entire telecommunications product, including the information systems security portion, to a lead department or agency.

#-Delegation Of Authority

This KSA has no definition.

Deleted Bit

A bit not delivered to the intended destination. (~) See also added bit, binary digit, character-count and bit-count integrity, error.

Deleted Block

A block not delivered to the intended destination. (~) See also added block, block, block transfer failure.

#-Deletion Of Accounts

*-Delint

/dee-lint/ v. To modify code to remove problems detected when linting. Confusingly, this process is also referred to as `linting' code.

Delivered Block

A successfully transferred block. See also binary digit, block.

Delivered Overhead Bit

A bit transferred to a destination user, but having its primary functional effect within the telecommunication system. See also binary digit, overhead information, user information.

Delivered Overhead Block

A successfully transferred block that contains no user information bits. See also block, overhead information, user information.

Delivery Confirmation

Information returned to the originator indicating that a given unit of information has been delivered to the intended addressee(s). See also acknowledge character.

*-Delta

1. n. [techspeak] A quantitative change, especially a small or incremental one (this use is general in physics and engineering). “I just doubled the speed of my program!” “What was the delta on program size?” “About 30 percent. ” (He doubled the speed of his program, but increased its size by only 30 percent.)
2. [UNIX] A diff, especially a diff stored under the set of version-control tools called SCCS (Source Code Control System) or RCS (Revision Control System).
3. n. A small quantity, but not as small as epsilon. The jargon usage of delta and epsilon stems from the traditional use of these letters in mathematics for very small numerical quantities, particularly in `epsilon-delta' proofs in limit theory (as in the differential calculus). The term delta is often used, once epsilon has been mentioned, to mean a quantity that is slightly bigger than epsilon but still very small. “The cost isn't epsilon, but it's delta” means that the cost isn't totally negligible, but it is nevertheless very small. Common constructions include `within delta of ---', `within epsilon of ---' that is, `close to' and `even closer to'.

Demarcation Point

*-Demented

adj. Yet another term of disgust used to describe a program. The connotation in this case is that the program works as designed, but the design is bad. Said, for example, of a program that generates large numbers of meaningless error messages, implying that it is on the brink of imminent collapse. Compare wonky, bozotic.

*-Demigod

n. A hacker with years of experience, a national reputation, and a major role in the development of at least one design, tool, or game used by or known to more than half of the hacker community. To qualify as a genuine demigod, the person must recognizably identify with the hacker community and have helped shape it. Major demigods include Ken Thompson and Dennis Ritchie (co-inventors of UNIX and C), Richard M. Stallman (inventor of EMACS), and Linus Torvalds (inventor of Linux). In their hearts of hearts, most hackers dream of someday becoming demigods themselves, and more than one major software project has been driven to completion by the author's veiled hopes of apotheosis. See also net. god, true-hacker.

*-Demo

/de'moh/ [short for `demonstration']

1. v. To demonstrate a product or prototype. A far more effective way of inducing bugs to manifest than any number of test runs, especially when important people are watching.

2. n. The act of demoing. “I've gotta give a demo of the drool-proof interface; how does it work again?”
3. n. Esp. as `demo version', can refer either to an early, barely-functional version of a program which can be used for demonstration purposes as long as the operator uses *exactly* the right commands and skirts its numerous bugs, deficiencies, and unimplemented portions, or to a special version of a program (frequently with some features crippled) which is distributed at little or no cost to the user for enticement purposes.

*-Demo Mode

1. [Sun] n. The state of being heads down in order to finish code in time for a demo, usually due yesterday.
2. A mode in which video games sit by themselves running through a portion of the game, also known as `attract mode'. Some serious apps have a demo mode they use as a screen saver, or may go through a demo mode on startup (for example, the Microsoft Windows opening screen -- which lets you impress your neighbors without actually having to put up with Microsloth Windows).

*-Demon

1. n. [MIT] A portion of a program that is not invoked explicitly, but that lies dormant waiting for some condition(s) to occur. See daemon. The distinction is that demons are usually processes within a program, while daemons are usually programs running on an operating system.
2. [outside MIT] Often used equivalently to daemon -- especially in the UNIX world, where the latter spelling and pronunciation is considered mildly archaic. Demons in sense 1 are particularly common in AI programs. For example, a knowledge-manipulation program might implement inference rules as demons. Whenever a new piece of knowledge was added, various demons would activate (which demons depends on the particular piece of data) and would create additional pieces of knowledge by applying their respective inference rules to the original piece. These new pieces could in turn activate more demons as the inferences filtered down through chains of logic. Meanwhile, the main program could continue with whatever its primary task was.

*-Demon Dialer

n. A program which repeatedly calls the same telephone number. Demon dialing may be benign (as when a number of communications programs contend for legitimate access to a BBS line) or malign (that is, used as a prank or denial-of-service attack). This term dates from the blue box days of the 1970s and early 1980s and is now semi-obsolescent among phreakers; see war dialer for its contemporary progeny.

Denial Of Service

1. Action or actions which prevent any part of an AIS from functioning in accordance with its intended purpose. This includes any action which causes the unauthorized destruction, modification, or delay of service (DODD 5200. 28;; *NCSC-WA*-001-85;)
2. The prevention of authorized access to resources or the delaying of time-critical operations. (SS;)
3. Result of any action or series of actions that prevents any part of a telecommunications or AIS from functioning.
4. Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Also called interdiction. (*NCSC-TG*-004-88)
5. See INTERDICTION.

Denial Time

The average length of time that an affected asset is denied to the organisation. [Jones 87a]. (N. B. this could be represented as a statistical distribution). (MK;)

Department Of Commerce

DOC

Department Of Defence

Department of Defence (DOD)

Department Of State

*-Depeditate

/dee-ped'*-tayt/ n. [by (faulty) analogy with `decapitate'] Humorously, to cut off the feet of. When one is using some computer-aided typesetting tools, careless placement of text blocks within a page or above a rule can result in chopped-off letter descenders. Such letters are said to have been depeditated.

Deployable Computer System

Computer system able to temporarily operate in different locations to satisfy the mission. These systems vary from large communications processors to laptop computers.

*-Deprecated

adj. Said of a program or feature that is considered obsolescent and in the process of being phased out, usually in favor of a specified replacement. Deprecated features can, unfortunately, linger on for many years. This term appears with distressing frequency in standards documents when the committees writing the documents realize that large amounts of extant (and presumably happily working) code depend on the fea-

ture(s) that have passed out of favor. See also dusty deck.

*-Derf

v. ,n. [PLATO] The act of exploiting a terminal which someone else has absent-mindedly left logged on, to use that person's account, especially to post articles intended to make an ass of the victim you're impersonating.

Descriptive Top Level Specification

Descriptive Top-Level

1. A top-level specification that is written in a Specification (DTLS) natural language (e. g. , English), an informal program design notation, or a combination of the two. (CSC-STD-001-83;)
2. NOTE: Descriptive top-level specification, required for a class B2 and B3 AIS, completely and accurately describes a trusted computing base.

Descriptive Top-Level Specification

1. (DTLS) Top-level specification that is written in a natural language (e. g. , English), an informal design notation, or a combination of the two.
2. NOTE: Descriptive top-level specification, required for a class B2 or B3 AIS, completely and accurately describes a trusted computing base. See Formal Top-Level Specification (FTLS).

Design Analysis Phase

Design Controlled

Part or subassembly for a COMSEC spare part equipment or device with a National Security Agency controlled design.

Design Controlled Spare Part

(DCSP) Part or subassembly for a COMSEC equipment or device with a NSA-controlled design.

Design Controlled Spare Pary

Part or subassembly for a COMSEC equipment or device with a National Security Agency controlled design.

Design Documentation

Design Flaws

Design Objective

Any desired performance characteristic for communication circuits and equipment which is based on engineering judgment but, for a number of reasons, is not considered feasible to establish as a system standard at the time the standard is written. (~) Note: Examples of reasons for designating a performance characteristic as a DO rather than as a standard are:

a. it may be bordering on an advancement in the state of the art;
b. the requirement may not have been fully confirmed by measurement or experience with operating circuits;
c. it may not have been demonstrated that it can be met considering other constraints such as cost and size.

A DO must be considered as guidance for DoD agencies in preparation of specifications for development or procurement of new equipment or systems and must be used if technically and economically practicable at the time such specifications are written. See also specification, standard.

Design Radius

The radius of the sphere within which compromising emanations from an equipment located at its center will be contained when the equipment meets the compromising emanation performance requirements.

Design Reviews

Design Verification

The use of verification techniques, usually computer assisted, to demonstrate a mathematical correspondence between an abstract (security) model and a formal system specification. (MTR-8201;)

Designated Approving

Official with the authority to formally authority assume responsibility for operating an AIS or network at an acceptable level of risk.

Designated Approving Authority

1. (DAA) A designated official who approves the (DAA) operation of automated systems at the computer facilities under his or her jurisdiction for processing of information or for critical processing. (*AFR* 205-16;)
2. A senior policy official who has the authority and the responsibility to make the management decision to accept or not accept the security safeguards prescribed for an AIS; the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. (DODD 5200. 28;; *NCSC-WA*-001-85;)
3. An official assigned responsibility to accredit ADP elements, activities, and networks under the official's jurisdiction. (*OPNAVINST* 5239. 1A;)
4. The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. (*NCSC-TG*-004-88)

Designated Development Activity

(DDA) The activity assigned responsibility by the Joint Chiefs of Staff for development of a standard software capability. (JCS PUB 19)

*-Desk Check

n. ,v. To grovel over hardcopy of source code, mentally simulating the control flow; a method of catching bugs. No longer common practice in this age of on-screen editing, fast compiles, and sophisticated debuggers -- though some maintain stoutly that it ought to be. Compare eyeball search, vdiff, vgrep.

Destruction

1. The physical alteration of ADP system media or ADP system components such that they can no longer be used for storage or retrieval of information. (DOE 5636. 2A;)
2. A peril involving the denial of an asset to its owner without acquisition by an agent. (RM;)

Detectable Actions

Activities or entities that can be heard, observed, or imaged. *Physical actions or entities that can be observed, imaged, or detected by human senses or by active and passive technical sensors, including emissions that can be intercepted (JCS MOP 199, 3/89)

Detection

1. The process of identifying the occurrence of an event and possibly the agent involved in the purpose of some protective mechanisms. (RM;)
2. The act of determining the presence of TEMPEST emanations by technical surveillance techniques. (NACSEM 5106)

Detection System

The total instrumentation used in performing an acoustic TEMPEST test which includes the transducer, detector, and display devices. Recording devices are also included if they are the only means of displaying the emanations during the test. (NACSEM 5103; NACSEM 51 06; NACSEM 5201)

#-Detective Controls

This KSA has no definition.

#-Development (Life Cycle)

This KSA has no definition.

*-Devil Book

n. See daemon book, the term preferred by its authors.

*-Devo

/dee'voh/ n. [orig. in-house jargon at Symbolics] A person in a development group. See also doco and mango.

Diagnostic Program

A computer program that recognizes, locates, and/or explains (a) a fault in equipment, networks, or systems, (b) a predefined error in input data, or (c) a syntax error in another computer program. (~)

Dial Back

See Call Back.

#-Dial Number Indicator

This KSA has no definition.

Dial-Up

The service whereby a telephone can be used to initiate and effect communication with a computer. (*NCSC-WA*-001-85;)

Dial-Up Diagnostic

Service whereby a remote diagnostic facility or source can communicate and perform diagnostic functions on computers or a computer system.

#-Dial-Up Security

The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer. (Source: *NCSC-TG*-0004).

Dibit

A group of two bits. Note: The four possible states for a dibit are 00, 01, 10, and 11. (~) Synonym diad. See also binary digit.

*-Dictionary Flame

n. [Usenet] An attempt to sidetrack a debate away from issues by insisting on meanings for key terms that presuppose a desired conclusion or smuggle in an implicit premise. A common tactic of people who prefer argument over definitions to disputes about reality. Compare spelling flame.

*-Diddle

1. vt. To work with or modify in a not particularly serious manner. “I diddled a copy of ADVENT so it didn't double-space all the time. ” “Let's diddle this piece of code and see if the problem goes away. ” See tweak and twiddle.
2. n. The action or result of diddling. See also tweak, twiddle, frob.

*-Die

v. Syn. crash. Unlike crash, which is used primarily of hardware, this verb is used of both hardware and software. See also go flatline, casters-up mode.

*-Die Horribly

v. The software equivalent of crash and burn, and the preferred emphatic form of die. “The converter choked on an FF in its input and died horribly”.

*-Diff

1. /dif/ n. A change listing, especially giving differences between (and additions to) source code or documents (the term is often used in the plural

`diffs'). “Send me your diffs for the Jargon File!” Compare vdiff.
2. Specifically, such a listing produced by the `diff(1)' command, esp. when used as specification input to the `patch(1)' utility (which can actually perform the modifications; see patch). This is a common method of distributing patches and source updates in the UNIX/C world.
3. v. To compare (whether or not by use of automated tools on machine-readable files); see also vdiff, mod.

Digit

1. A symbol, numeral, or graphic character that represents an integer, e. g. , one of the decimal characters “0” to “9,” or one of the binary characters “0” or “1. ” (~) Note: In a given numeration system, the number of allowable different digits, including zero, is always equal to the radix (base). See also alphabet, binary digit, character, character set.
2. n. An employee of Digital Equipment Corporation. See also VAX, VMS, PDP-10, TOPS-10, DEChead, double DECkers, field circus.

Digit Time Slot

In a digital data stream, a time interval that can be recognized and defined uniquely, and which is allocated to a single digit. (~) See also signaling time slot, time-division multiplexing, time slot (def. #2).

Digital

Characterized by discrete states.

Digital Alphabet

A coded character set in which the characters of an alphabet have a one-to-one relationship with their digitally coded representations. (~) See also alphabet, character, character set, code, coded character set, coded set.

Digital Combining

A method of interfacing digital data signals, in either synchronous or asynchronous mode, without converting the data into a quasi-analog signal. (~) See also digital alphabet, diversity combiner, interface, multiplexing.

Digital Computer

A device that performs operations on data that are represented by discrete values only. Note: Digital computers commonly employ electrical signals having two permissible states or levels, which represent the two possible characters (numerals) in the binary number system. See also analog computer, computer.

Digital Data

1. Data represented by discrete values or conditions, as opposed to analog data. (~)
2. A discrete representation of a quantized value of a variable, i. e. , the representation of a number by digits, perhaps with special characters and the “space” character. See also analog data, data, data transmission.

Digital Error

A single-digit inconsistency between the signal actually received and the signal that should have been received. (~) See also character-count and bit-count integrity, error, error control.

Digital Facsimile Equipment

1. Facsimile equipment that employs digital techniques to encode the image detected by the scanner. The output signal may be either digital or analog (~).
2. Note: Examples of digital facsimile equipment are CCITT Group 3, CCITT Group 4, STANAG 5000 Type I and STANAG 5000 Type II.

Digital Filter

A filter (usually linear), in discrete time, that is normally implemented through digital electronic computation. (~) Note: Digital filters differ from continuous time filters only in application. The parameters of digital filters are generally more stable than the parameters of commonly used analog (continuous) filters. Digital filters can be applied as optimal estimators. Commonly used forms are finite impulse response (FIR) and infinite impulse response (IIR). See also Kalman filter.

Digital Modulation

The process of varying one or more parameters of a carrier wave as a function of two or more finite and discrete states of a signal. (~) See also carrier (cxr), digital data, frequency-shift keying, modulation, phase-shift keying.

Digital Signal

A nominally discontinuous electrical signal that changes from one state to another in discrete steps.

Digital Signature

Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit and protect against forgery e. g. by the recipient. (SS;);

Digital-To-Analog Converter

1. A device that converts a digital input signal to an analog output signal carrying equivalent information. (~)
2. A functional unit that converts data from a digital representation to an analog representation. (FP) (ISO) See also analog-to-digital converter, digital voice transmission, digitize.

#-Digital/Analog Technology

A form of representation in which discrete (separate) objects (digits) are used to stand for something so that counting and other operations can be performed precisely. Information represented digitally can be manipulated to produce a calculation, a sort, or some other computation. In an abacus,for example, quantities are represented by positioning beads on a wire. A trained abacus operator can perform calculations at high rates of speed by following an algorithm, a recipe for solving the problem. In digital electronic computers, two electrical states correspond to the 1s and 0s of binary numbers, and the algorithm is embodied in a computer program. (*QCUS+Pf-90*)

Digitize

To convert an analog signal to a digital signal carrying equivalent information. (~) See also analog-to-digital converter, digital-to-analog converter.

Digitizer

1. A device that converts an analog signal into a digital representation of that signal. (~) Note: Usually implemented by sampling the analog signal at a regular rate and encoding each sample into a numeric representation of the amplitude value of the sample.
2. A device that converts the position of a point on a surface into digital coordinate data. (~) See also analog-to-digital converter.

Digraphic Processing

Processing where the data (bits) are parallel processed, and the characters are processed two at a time.

*-Dike

vt. To remove or disable a portion of something, as a wire from a computer or a subroutine from a program. A standard slogan is “When in doubt, dike it out”. (The implication is that it is usually more effective to attack software problems by reducing complexity than by increasing it.) The word `dikes' is widely used among mechanics and engineers to mean `diagonal cutters', esp. the heavy-duty metal-cutting version, but may also refer to a kind of wire-cutters used by electronics techs. To `dike something out' means to use such cutters to remove something. Indeed, the TMRC Dictionary defined dike as “to attack with dikes”. Among hackers this term has been metaphorically extended to informational objects such as sections of code.

*-Ding

1. n. ,vi. Synonym for feep. Usage rare among hackers, but commoner in the Real World.
2. `dinged' What happens when someone in authority gives you a minor bitching about something, esp. something trivial. “I was dinged for having a messy desk. ”

*-Dink

/dink/ adj. Said of a machine that has the bitty box nature; a machine too small to be worth bothering with --- sometimes the system you're currently forced to work on. First heard from an MIT hacker working on a CP/M system with 64K, in reference to any 6502 system, then from fans of 32-bit architectures about 16-bit machines. “GNUMACS will never work on that dink machine. ” Probably derived from mainstream `dinky', which isn't sufficiently pejorative. See macdink.

*-Dinosaur

1. n. Any hardware requiring raised flooring and special power. Used especially of old minis and mainframes, in contrast with newer microprocessor-based machines. In a famous quote from the 1988 UNIX EXPO, Bill Joy compared the liquid-cooled mainframe in the massive IBM display with a grazing dinosaur “with a truck outside pumping its bodily fluids through it”. IBM was not amused. Compare big iron; see also mainframe.
2. [IBM] A very conservative user; a zipperhead.

*-Dinosaur Pen

n. A traditional mainframe computer room complete with raised flooring, special power, its own ultra-heavy-duty air conditioning, and a side order of Halon fire extinguishers. See boa.

*-Dinosaurs Mating

n. Said to occur when yet another big iron merger or buyout occurs; reflects a perception by hackers that these signal another stage in the long, slow dying of the mainframe industry. In its glory days of the 1960s, it was `IBM and the Seven Dwarves' Burroughs, Control Data, General Electric, Honeywell, NCR, RCA, and Univac. RCA and GE sold out early, and it was `IBM and the Bunch' (Burroughs, Univac, NCR, Control Data, and Honeywell) for a while. Honeywell was bought out by Bull; Burroughs merged with Univac to form Unisys (in 1984 --- this was when the phrase `dinosaurs mating' was coined); and in 1991 AT&T absorbed NCR. More such earth-shaking unions of doomed giants seem inevitable.

DIP

Abbreviation for dual in-line package. See dual in-line package switch.

Direct Access

1. The capability to obtain data from a storage device or to enter data into a storage device in a sequence independent of their relative positions, by means of addresses that indicate the physical location of the data. (FP) (ISO)
2. Pertaining to the organization and access method that must be used for a storage structure in which locations of records are determined by their keys, without reference to an index or to other records

that may have been previously accessed. (FP) See also browsing.

Direct Address

[In computing,] An address that designates the storage location of an item of data to be treated as an operand. (FP)

Direct Memory Access

Direct Memory Access Controllers

Direct Memory Access Devices

Direct Shipment

Shipment of COMSEC material directly from the National Security Agency to user COMSEC accounts.

Direct Support

COMSEC monitor support provided to combat commanders under wartime, simulated wartime conditions, or as specified in agreements between the Air Intelligence Agency (HQ AIA) and other agencies.

Direction Finding

(DF) A procedure for obtaining bearings on radio frequency (RF) emitters. *A procedure for obtaining bearings on radio frequency emitters with the use of a directional antenna and a display unit with an intercept receiver or ancillary equipment (*IC Staff, Glossary of Intelligence Terms and Definitions,* 6/89)

Directionalization

Director Of The Office Of Management And Budget

*-Dirtball

n. [XEROX PARC] A small, perhaps struggling outsider; not in the major or even the minor leagues. For example, “Xerox is not a dirtball company”. [Outsiders often observe in the PARC culture an institutional arrogance which usage of this term exemplifies. The brilliance and scope of PARC's contributions to computer science have been such that this superior attitude is not much resented. -- ESR]

*-Dirty Power

n. Electrical mains voltage that is unfriendly to the delicate innards of computers. Spikes, drop-outs, average voltage significantly higher or lower than nominal, or just plain noise can all cause problems of varying subtlety and severity (these are collectively known as power hits).

Disaster Plan

See Contingency Plan.

#-Disaster Recovery

1. The ability to provide continuity of operations in the event that information technology support is interrupted for any reason. (Source: Panel of Experts, July 1994);
2. the planned sequence of events that allows for the recovery of a computer facility and or the applications processed there. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992

#-Disaster Recovery Plan Testing

Exercising the Disaster Recovery Plan to provide reasonable continuity of data processing support should events occur that prevent normal operations. Plans should be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information technology support. (Source: *OMB Circular A-130*).

#-Disaster Recovery Planning

1. Documents containing procedures for emergency response, extended backup operations, and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objectives of these plans, in conjunction with contingency plans, are to provide reasonable assurance that a computer installation can recover from such incidents, continue to process mission-essential applications in a degraded mode (i. e. , as a minimum, process computer applications previously identified as most essential), and return to a normal mode of operation within a reasonable amount of time. Such plans are a protective measure generally applied based on assessments of risk, cost, benefit, and feasibility as well as the other protective measures in place. (Source: NISTIR 4659);
2. planning for any event that causes significant disruption to operations thereby threatening the business survival. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Disaster Recovery Plans

1. Documents containing procedures for emergency response, extended backup operations, and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objectives of these plans, in conjunction with contingency plans, are to provide reasonable assurance that a computer installation can recover from such incidents, continue to process mission essential applications in a degraded mode (i. e. , as a minimum process computer applications previously

identified as most essential), and return to a normal mode of operation within a reasonable amount of time. Such plans are a protective measure generally applied based on assessments of risk, cost, benefit, and feasibility as well as the other protective measures in place. (*DOE 1360. 2A*)
2. See CONTINGENCY PLAN(S).

*-Disclaimer

n. [Usenet] Statement ritually appended to many Usenet postings (sometimes automatically, by the posting software) reiterating the fact (which should be obvious, but is easily forgotten) that the article reflects its author's opinions and not necessarily those of the organization running the machine through which the article entered the network.

Disclosure

1. A peril involving the acquisition of an asset by an agent without direct loss to the owner. (RM;)
2. The authorized release of information through approved channels. *The authorized release of classified information through approved channels (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

#-Disclosure Of Sensitive Data

The unauthorized acquisition of sensitive information (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992, et al)

Disconnect

*-Discordianism

/dis-kor'di-*n-ism/ n. The veneration of Eris, a. k. a. Discordia; widely popular among hackers. Discordianism was popularized by Robert Shea and Robert Anton Wilson's novel “Illuminatus!” as a sort of self-subverting Dada-Zen for Westerners -- it should on no account be taken seriously but is far more serious than most jokes. Consider, for example, the Fifth Commandment of the Pentabarf, from “Principia Discordia” “A Discordian is Prohibited of Believing What he Reads. ” Discordianism is usually connected with an elaborate conspiracy theory/joke involving millennia-long warfare between the anarcho-surrealist partisans of Eris and a malevolent, authoritarian secret society called the Illuminati. See Religion in Appendix B, Church of the SubGenius, and ha ha only serious.

Discretionary Access

Means of restricting access to control objects based on the identity and need-to-know of users and/or groups to which the object belongs. NOTE: Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

#-Discretionary Access Control

1. (DAC) A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. (NSTISSI 4009) NOTE: Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (DODD 5200. 28-STD;)
2. A means of restricting access to objects based on the identity and need-to-know of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare MANDATORY ACCESS CONTROL. (*NCSC-WA*-001-85;; CSC-STD-001-83;; CSC-STD-004-85;)

Discretionary Access Control Mechanism

Trusted Computing Base (TCB) routines or algorithms which use Discretionary Access Controls to provide Discretionary Protection.

Discretionary Protection

Access control that identifies individual users and their need-to-know and limits users to the information that they are allowed to see. It is used on systems that process information with the same level of sensitivity. (*AFR* 205-16;)

Discretionary Security Protection

(Class C1) Trusted Computing Base (TCB) which provides elementary Discretionary Access Control protection features that separate users from data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis; i. e. , suitable for allowing users to be able to protect private data and to keep other users from accidentally reading or destroying that data.

Disengagement Attempt

#-Disgruntled Employees

Dissatisfied workers who may cause intentional harm to information technology systems. Considered the biggest threat to information systems due to the fact that they are “insiders” and are authorized users of the systems; they may perform acts harmful to the system or information processed, stored or transmitted by the system. (Source: Panel of Experts, July 1994).

DISJ

A function of the certainty measures of two statements that returns the certainty measure of the dis-

junction of the statements. Required by the Uncertainty Calculus. (MA;)

***-Disk Farm**

n. (also laundromat) A large room or rooms filled with disk drives (esp. washing machines).

Disk Pack

An assembly of magnetic disks that can be removed as a whole from a disk drive together with a container from which the assembly must be separated when operating. (FP) (ISO)

Disk Sectors

Diskette

A small magnetic disk enclosed in a jacket. (FP) (ISO)

#-Diskless Workstations

Workstations to which access to the disk drive mechanism is either not present or has been disabled for the general user. (Source: Panel of Experts, July 1994).

Display Device

An output unit that gives a visual representation of data.

***-Display Hack**

n. A program with the same approximate purpose as a kaleidoscope to make pretty pictures. Famous display hacks include munching squares, smoking clover, the BSD UNIX `rain(6)' program, `worms(6)' on miscellaneous UNIXes, and the X `kaleid(1)' program. Display hacks can also be implemented without programming by creating text files containing numerous escape sequences for interpretation by a video terminal; one notable example displayed, on any VT100, a Christmas tree with twinkling lights and a toy train circling its base. The hack value of a display hack is proportional to the esthetic value of the images times the cleverness of the algorithm divided by the size of the code. Syn. psychedelicware.

#-Disposition Of Classified Information

Disposition of Media and Data

#-Disposition Of Media And Data

This KSA has no definition.

Dissemination

Dissemination Control

See Special Markings

Dissemination Controls

See Special Markings.

Dissemination Of Information

The function of distributing government information to the public, whether through printed documents, or electronic or other media. Does not include intra-agency use of information, interagency sharing of information, or responding to requests for “access to information”. (A-130;)

***-Dissociated Press**

n. [play on `Associated Press'; perhaps inspired by a reference in the 1949 Bugs Bunny cartoon “What's Up, Doc?”] An algorithm for transforming any text into potentially humorous garbage even more efficiently than by passing it through a marketroid. The algorithm starts by printing any N consecutive words (or letters) in the text. Then at every step it searches for any random occurrence in the original text of the last N words (or letters) already printed and then prints the next word or letter. EMACS has a handy command for this. Here is a short example of word-based Dissociated Press applied to an earlier version of this Jargon File wart n. A small, crocky feature that sticks out of an array (C has no checks for this). This is relatively benign and easy to spot if the phrase is bent so as to be not worth paying attention to the medium in question. Here is a short example of letter-based Dissociated Press applied to the same source

DIST

A specific metric (q. v.). (MA;)

Distributed AIS

An AIS that is physically and/or electrically connected to one or more AISs. (DODD 5200. 28;)

Distributed Computer System

Computer system that is geographically separated but electrically connected to one or more other systems.

Distributed Processing

A technique for implementing an integrated set of information processing functions within multiple, physically separated devices. (~) See also distributed network.

Distributed Processing

A form of decentralization of information processing made possible by a network of computers dispensed throughout an organization. Processing of user applications is accomplished by several computers interconnected by a telecommunications network rather than relying on one large centralized omputer facility or on the decentralized operation of several independent computers.

#-Distributed Systems Security

This KSA has no definition.

***-Distribution**

1. n. A software source tree packaged for distribution; but see kit.

2. A vague term encompassing mailing lists and Usenet newsgroups (but not BBS fora); any topic-oriented message channel with multiple recipients.
3. An information-space domain (usually loosely correlated with geography) to which propagation of a Usenet message is restricted; a much-underutilized feature.

Distribution Statement

A statement used in marking a technical document to denote the extent of its availability for distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking assigned in accordance with *DOD* 5200. 1-R. (DODD 5230. 24;)

Distribution System

The metallic wirepaths or fiber optic transmission paths providing interconnection between components of the protected system. (NACSIM 5203)

*-Disusered

adj. [Usenet] Said of a person whose account on a computer has been removed, esp. for cause rather than through normal attrition. “He got disusered when they found out he'd been cracking through the school's Internet access. ” The verbal form `disuser' is live but less common. Both usages probably derive from the DISUSER account status flag on VMS; setting it disables the account. Compare star out.

*-Do Protocol

vi. [from network protocol programming] To perform an interaction with somebody or something that follows a clearly defined procedure. For example, “Let's do protocol with the check” at a restaurant means to ask for the check, calculate the tip and everybody's share, collect money from everybody, generate change as necessary, and pay the bill. See protocol.

*-Doc

/dok/ n. Common spoken and written shorthand for `documentation'. Often used in the plural `docs' and in the construction `doc file' (i. e. , documentation available on-line).

*-Doco

/do'koh/ n. [orig. in-house jargon at Symbolics] A documentation writer. See also devo and mango.

Document

1. Any record information regardless of its medium, physical form, or characteristics. a) Technical document. Any document that presents STI. b) Technical report. Any preliminary or final technical document prepared to record, document, or share results obtained from, or recommendations made on, or relating to, DOD-sponsored or co-sponsored scientific and technical work. (*DODD 3200. 12*;)
2. Any record of information regardless of physical form or characteristics, including, but not limited to, the following: a. Handwritten, printed, or typed matter. b. Painted, drawn, or engraved matter. c. Sound, magnetic, optical or electro-mechanical recordings. d. Photographic prints and exposed or developed film or still or motion pictures. e. Automatic data processing input and contents of equipment and/or media including memory, punch cards, tapes, diskettes, and visual displays. f. Reproductions of the foregoing by any process. (DOE 5635. lA)

#-Document Labeling

Security markings on the document to identify the sensitivity of the information in the document.

#-Documentation

The internal technical records used throughout the information system's life cycle and the external written guidance for users of software applications and hardware. Internal documentation includes system and design specifications; management plans, architectural, prototype and detail design documents; test specifications and reports, and engineering change requests and results. External documentation includes customer reference and usage information. (Sources - *Encyclopedia of Software Eng*).

#-Documentation Policies

This KSA has no definition.

DoD Directive 5200. 28 Automated Information System Security.

Trsusted Facility Manual. A manual shall be available that provides the following: be addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility; give procedures examining and maintaining the audit files; give the detailed audit record structure for each type of audit event; describe the operator and administrator functions related to security, to include changing the security characteristics of a user; provide guidelines on the consistent and effective use of the protection features of the system; explain how the protection features of the system interact; show how to securely generate a new TCB; provide guidelines on facility procedures, warinings, and privileges that need to be controlled in order to operate the facility in a secure manner; identify the TCB modules that contain the reference validation mechanism; describe the procedures for secure generation of a new TCB from source after modification of any modules in the TCB.

DoD Information Analysis Center

(IAC) An activity that acquires, digests, analyzes, evaluates, synthesizes, stores, publishes, and provides advisory and other user services concerning available worldwide scientific and technical information and

engineering data in a clearly defined, specialized field or subject area of significant *DOD* interest or concern. IACs are distinguished from technical information centers and libraries whose functions are primarily concerned with providing reference or access to the documents themselves rather than the STI information contained in the documents. (*DODD 3200. 12*;)

DoD TCSEC

See Department of Defense Trusted Computer System Evaluation Criteria.

DOD Technology Transfer

Programs to promote military-civilian technology transfer and cooperative development on a systematic basis, including appropriate transfer of technology developed by the *DOD* to the US civilian sector where such technology can be utilized profitably, and identification of new technologies of both military and civilian interest. (*DODD 3200. 12*;)

DoD Trusted Computer

Document containing basic requirements, System Evaluation and evaluation classes for assessing Criteria degrees of effectiveness of hardware and software security controls built into AIS. NOTE: This document, *DoD 5200. 28 STD*, is frequently referred to as the *Orange Book*.

DoD Trusted Computer System Evaluation Criteria

(TCSEC) A document published by the National Computer Security Center (NCSC) containing a uniform set of basic requirements and evaluation classes for assessing the effectiveness of hardware and software security controls built into automated information systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is frequently referred to as "The Criteria" or "The *Orange Book*". (*NCSC-WA*-001-85;) See Object and Subject.

DoD Trusted Computer System Evaluation Criteria (TCSEC)

A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is Government Standard DoD 5200. 28-STD and is frequently referred to as "The Criteria" or "The *Orange Book*. "

*-Dodgy

adj. Syn. with flaky. Preferred outside the U. S.

*-Dogcow

/dog'kow/ n. See Moof. The dogcow is a semi-legendary creature that lurks in the depths of the Macintosh Technical Notes Hypercard stack V3. 1. The full story of the dogcow is told in technical note #31 (the particular Moof illustrated is properly named `Clarus'). Option-shift-click will cause it to emit a characteristic `Moof!' or `!fooM' sound. *Getting* to tech note 31 is the hard part; to discover how to do that, one must needs examine the stack script with a hackerly eye. Clue rot13 is involved. A dogcow also appears if you choose `Page Setup. ' with a LaserWriter selected and click on the `Options' button.

*-Dogpile

v. [Usenet prob. fr. mainstream "puppy pile"] When many people post unfriendly responses in short order to a single posting, they are sometimes said to "dogpile" or "dogpile on" the person to whom they're responding. For example, when a religious missionary posts a simplistic appeal to alt. atheism, he can expect to be dogpiled.

*-Dogwash

/dog'wosh/ [From a quip in the `urgency' field of a very optional software change request, ca. 1982. It was something like "Urgency Wash your dog first".]

1. n. A project of minimal priority, undertaken as an escape from more serious work.
2. v. To engage in such a project. Many games and much freeware get written this way.

Domain

1. The set of objects that a subject has the ability to access. (CSC-STD-001-83;)
2. The set of objects that a subject or resources in an automated information system has the ability to access. (*NCSC-WA*-001-85;)
3. The unique context (e. g. , access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access.

*-Domainist

1. /doh-mayn'ist/ adj. Said of an Internet address (as opposed to a bang path) because the part to the right of the `@' specifies a nested series of `domains'; for example, esr@snark. thyrsus. com specifies the machine called snark in the subdomain called thyrsus within the top-level domain called com. See also big-endian, sense
2. Said of a site, mailer, or routing program which knows how to handle domainist addresses.
3. Said of a person (esp. a site admin) who prefers domain addressing, supports a domainist mailer, or proselytizes for domainist addressing and disdains bang paths. This term is now (1993) semi-obsolete, as most sites have converted.

Dominate

Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the nonhierarchical categories of S1 include all those of S2 as a subset. NOTE: Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than, or equal to, that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset. (CSC-STD-001-83;)

Dominate Security Level

Dominated By

Dominates

*-Don't Do That, Then!

[from an old doctor's office joke about a patient with a trivial complaint] Stock response to a user complaint. “When I type control-S, the whole system comes to a halt for thirty seconds. ” “Don't do that, then!” (or “So don't do that!”). Compare RTFM.

*-Dongle

1. /dong'gl/ n. A security or copy protection device for commercial microcomputer programs consisting of a serialized EPROM and some drivers in a D-25 connector shell, which must be connected to an I/O port of the computer while the program is run. Programs that use a dongle query the port at startup and at programmed intervals thereafter, and terminate if it does not respond with the dongle's programmed validation code. Thus, users can make as many copies of the program as they want but must pay for each dongle. The idea was clever, but it was initially a failure, as users disliked tying up a serial port this way. Almost all dongles on the market today (1993) will pass data through the port and monitor for magic codes (and combinations of status lines) with minimal if any interference with devices further down the line -- this innovation was necessary to allow daisy-chained dongles for multiple pieces of software. The devices are still not widely used, as the industry has moved away from copy-protection schemes in general.
2. By extension, any physical electronic key or transferable ID required for a program to function. Common variations on this theme have used parallel or even joystick ports. See dongle-disk. [Note in early 1992, advertising copy from Rainbow Technologies (a manufacturer of dongles) included a claim that the word derived from “Don Gall”, allegedly the inventor of the device. The company's receptionist will cheerfully tell you that the story is a myth invented for the ad copy. Nevertheless, I expect it to haunt my life as a lexicographer for at least the next ten years. --- ESR]

*-Dongle-Disk

/don'gl disk/ n. A special floppy disk that is required in order to perform some task. Some contain special coding that allows an application to identify it uniquely, others *are* special code that does something that normally-resident programs don't or can't. (For example, AT&T's “Unix PC” would only come up in root mode with a special boot disk.) Also called a `key disk'. See dongle.

*-Donuts

n. obs. A collective noun for any set of memory bits. This usage is extremely archaic and may no longer be live jargon; it dates from the days of ferrite-core memories in which each bit was implemented by a doughnut-shaped magnetic flip-flop.

*-Doorstop

n. Used to describe equipment that is non-functional and halfway expected to remain so, especially obsolete equipment kept around for political reasons or ostensibly as a backup. “When we get another Wyse-50 in here, that ADM 3 will turn into a doorstop. ” Compare boat anchor.

DOS

1. Disk Operating System
2. Denial of Service Attack

*-Dot File

[UNIX] n. A file that is not visible by default to normal directory-browsing tools (on UNIX, files named with a leading dot are, by convention, not normally presented in directory listings). Many programs define one or more dot files in which startup or configuration information may be optionally recorded; a user can customize the program's behavior by creating the appropriate file in the current or home directory. (Therefore, dot files tend to creep -- with every non-trivial application program defining at least one, a user's home directory can be filled with scores of dot files, of course without the user's really being aware of it.) See also profile (sense 1), rc file.

*-Double Bucky

adj. Using both the CTRL and META keys. “The command to burn all LEDs is double bucky F. ” This term originated on the Stanford extended-ASCII keyboard, and was later taken up by users of the space-cadet keyboard at MIT. A typical MIT comment was that the Stanford bucky bits (control and meta shifting keys) were nice, but there weren't enough of them; you could type only 512 different characters on a Stanford keyboard. An obvious way to address this was simply to add more shifting keys, and this was eventually done; but a keyboard with that many shifting keys is hard on touch-typists, who don't like to

move their hands away from the home position on the keyboard. It was half-seriously suggested that the extra shifting keys be implemented as pedals; typing on such a keyboard would be very much like playing a full pipe organ. This idea is mentioned in a parody of a very fine song by Jeffrey Moss called “Rubber Duckie”, which was published in “The Sesame Street Songbook” (Simon and Schuster 1971, ISBN 0-671-21036-X). These lyrics were written on May 27, 1978, in celebration of the Stanford keyboard Double Bucky Double bucky, you're the one! You make my keyboard lots of fun. Double bucky, an additional bit or two (Vo-vo-de-o!) Control and meta, side by side, Augmented ASCII, nine bits wide! Double bucky! Half a thousand glyphs, plus a few! Oh, I sure wish that I Had a couple of Bits more! Perhaps a Set of pedals to Make the number of Bits four Double double bucky! Double bucky, left and right OR'd together, outta sight! Double bucky, I'd like a whole word of Double bucky, I'm happy I heard of Double bucky, I'd like a whole word of you! --- The Great Quux (with apologies to Jeffrey Moss) [This, by the way, is an excellent example of computer filk -- ESR] See also meta bit, cokebottle, and quadruple bucky.

*-Double DECkers

n. Used to describe married couples in which both partners work for Digital Equipment Corporation.

*-Doubled Sig

[Usenet] n. A sig block that has been included twice in a Usenet article or, less commonly, in an electronic mail message. An article or message with a doubled sig can be caused by improperly configured software. More often, however, it reveals the author's lack of experience in electronic communication. See B1FF, pseudo.

*-Down

1. adj. Not operating. “The up escalator is down” is considered a humorous thing to say, and “The elevator is down” always means “The elevator isn't working” and never refers to what floor the elevator is on. With respect to computers, this term has passed into the mainstream; the extension to other kinds of machine is still hackish.
2. `go down' vi. To stop functioning; usually said of the system. The message from the console that every hacker hates to hear from the operator is “System going down in 5 minutes”.
3. `take down', `bring down' vt. To deactivate purposely, usually for repair work or PM. “I'm taking the system down to work on that bug in the tape drive. ” Occasionally one hears the word `down' by itself used as a verb in this vt. sense. See crash; oppose up.

*-Download

vt. To transfer data or (esp.) code from a larger `host' system (esp. a mainframe) over a digital comm link to a smaller `client' system, esp. a microcomputer or specialized peripheral. Oppose upload. However, note that ground-to-space communications has its own usage rule for this term. Space-to-earth transmission is always `down' and the reverse `up' regardless of the relative size of the computers involved. So far the in-space machines have invariably been smaller; thus the upload/download distinction has been reversed from its usual sense.

Downtime

The time during which a functional unit is inoperable. (~) See also continuous operation, failure, fault, mean time between failures, mean time between outages, mean time to repair, mean time to service restoral, uptime.

*-DP

/D-P/ n. 1. Data Processing. Listed here because, according to hackers, use of the term marks one immediately as a suit. See DPer.

*-DPB

/d*-pib'/ vt. [from the PDP-10 instruction set] To plop something down in the middle. Usagesilly. “DPB yourself into that couch there. ” The connotation would be that the couch is full except for one slot just big enough for one last person to sit in. DPB means `DePosit Byte', and was the name of a PDP-10 instruction that inserts some bits into the middle of some other bits. Hackish usage has been kept alive by the Common LISP function of the same name.

*-Dper

/dee-pee-er/ n. Data Processor. Hackers are absolutely amazed that suits use this term self-referentially. *Computers* process data, not people! See DP.

DPL

See Degausser Products List (A section in the Information Systems Security Products and Services Catalogue).

*-Dragon

n. [MIT] A program similar to a daemon, except that it is not invoked at all, but is instead used by the system to perform various secondary tasks. A typical example would be an accounting program, which keeps track of who is logged in, accumulates load-average statistics, etc. Under ITS, many terminals displayed a list of people logged in, where they were, what they were running, etc. , along with some random picture (such as a unicorn, Snoopy, or the Enterprise), which was generated by the `name dragon'. Usage rare outside MIT -- under UNIX and most other OSes this would be called a `background demon' or daemon. The best-known UNIX example of a dragon is

`cron(1)'. At SAIL, they called this sort of thing a `phantom'.

*-Dragon Book

n. The classic text “Compilers Principles, Techniques and Tools”, by Alfred V. Aho, Ravi Sethi, and Jeffrey D. Ullman (Addison-Wesley 1986; ISBN 0-201-10088-6), so called because of the cover design featuring a dragon labeled `complexity of compiler design' and a knight bearing the lance `LALR parser generator' among his other trappings. This one is more specifically known as the `Red Dragon Book' (1986); an earlier edition, sans Sethi and titled “*Principles Of Compiler Design*” (Alfred V. Aho and Jeffrey D. Ullman; Addison-Wesley, 1977; ISBN 0-201-00022-9), was the `Green Dragon Book' (1977). (Also `New Dragon Book', `Old Dragon Book'.) The horsed knight and the Green Dragon were warily eying each other at a distance; now the knight is typing (wearing gauntlets!) at a terminal showing a video-game representation of the Red Dragon's head while the rest of the beast extends back in normal space. See also book titles.

*-Drain

1. v. [IBM] Syn. for flush (sense
2. . Has a connotation of finality about it; one speaks of draining a device before taking it offline. dread high-bit disease
2. n. A condition endemic to PRIME (a. k. a. PR1ME) minicomputers that results in all the characters having their high (0x80) bit ON rather than OFF. This of course makes transporting files to other systems much more difficult, not to mention talking to true 8-bit devices. Folklore had it that PRIME adopted the reversed-8-bit convention in order to save 25 cents per serial line per machine; PRIME old-timers, on the other hand, claim they inherited the disease from Honeywell via customer NASA's compatibility requirements and struggled heroically to cure it. Whoever was responsible, this probably qualifies as one of the most cretinous design tradeoffs ever made. See meta bit. A few other machines have exhibited similar brain damage.

*-DRECNET

/drek'net/ n. [from Yiddish/German `dreck', meaning filth] Deliberate distortion of DECNET, a networking protocol used in the VMS community. So called because DEC helped write the Ethernet specification and then (either stupidly or as a malignant customer-control tactic) violated that spec in the design of DRECNET in a way that made it incompatible. See also connector conspiracy.

*-Driver

1. n. The main loop of an event-processing program; the code that gets commands and dispatches them for execution.
2. [techspeak] In `device driver', code designed to handle a particular peripheral device such as a magnetic disk or tape unit. 3. In the TeX world and the computerized typesetting world in general, a program that translates some device-independent or other common format to something a real device can actually understand.

*-Droid

n. [from `android', SF terminology for a humanoid robot of essentially biological (as opposed to mechanical/electronic) construction] A person (esp. a low-level bureaucrat or service-business employee) exhibiting most of the following characteristics (a) naive trust in the wisdom of the parent organization or `the system'; (b) a blind-faith propensity to believe obvious nonsense emitted by authority figures (or computers!); (c) a rule-governed mentality, one unwilling or unable to look beyond the `letter of the law' in exceptional situations; (d) a paralyzing fear of official reprimand or worse if Procedures are not followed No Matter What; and (e) no interest in doing anything above or beyond the call of a very narrowly-interpreted duty, or in particular in fixing that which is broken; an “It's not my job, man” attitude. Typical droid positions include supermarket checkout assistant and bank clerk; the syndrome is also endemic in low-level government employees. The implication is that the rules and official procedures constitute software that the droid is executing; problems arise when the software has not been properly debugged. The term `droid mentality' is also used to describe the mindset behind this behavior. Compare suit, marketroid; see -oid.

*-Drool-Proof Paper

n. Documentation that has been obsessively dumbed down, to the point where only a cretin could bear to read it, is said to have succumbed to the `drool-proof paper syndrome' or to have been `written on drool-proof paper'. For example, this is an actual quote from Apple's LaserWriter manual”Do not expose your LaserWriter to open fire or flame. ”

Drop Accountability

Procedure under which a COMSEC account custodian initially receipts for COMSEC material, and then provides no further accounting for it to its central office of record. NOTE: Local accountability of the COMSEC material may continue to be required.

Drop And Insert

That process wherein a part of the information carried in a transmission system is demodulated (dropped) at an intermediate point and different information is entered (inserted) for subsequent transmission in the same position, e. g. , time, frequency, or phase, previously occupied by the terminated information. (~) Note: Information not of interest at the drop-and-

insert location is not demodulated. See also drop repeater, radio relay system.

*-Drop On The Floor

vt. To react to an error condition by silently discarding messages or other valuable data. “The gateway ran out of memory, so it just started dropping packets on the floor. ” Also frequently used of faulty mail and netnews relay sites that lose messages. See also black hole, bit bucket.

*-Drop-Ins

n. [prob. by analogy with drop-outs] Spurious characters appearing on a terminal or console as a result of line noise or a system malfunction of some sort. Esp. used when these are interspersed with one's own typed input. Compare drop-outs, sense 2.

#-Drop-Off/Add-On Protection

This KSA has no definition.

*-Drop-Outs

1. n. A variety of `power glitch' (see glitch); momentary 0 voltage on the electrical mains.
2. Missing characters in typed input due to software malfunction or system saturation (one cause of such behavior under UNIX when a bad connection to a modem swamps the processor with spurious character interrupts; see screaming tty).
3. Mental glitches; used as a way of describing those occasions when the mind just seems to shut down for a couple of beats. See glitch, fried.

*-Drugged

1. adj. (also `on drugs') Conspicuously stupid, heading toward brain-damaged. Often accompanied by a pantomime of toking a joint.
2. Of hardware, very slow relative to normal performance.

*-Drum

adj, n. Ancient techspeak term referring to slow, cylindrical magnetic media that were once state-of-the-art storage devices. Under BSD UNIX the disk partition used for swapping is still called `/dev/drum'; this has led to considerable humor and not a few straight-faced but utterly bogus `explanations' getting foisted on newbies. See also “The Story of Mel, a Real Programmer” in Appendix A.

*-Drunk Mouse Syndrome

n. (also `mouse on drugs') A malady exhibited by the mouse pointing device of some computers. The typical symptom is for the mouse cursor on the screen to move in random directions and not in sync with the motion of the actual mouse. Can usually be corrected by unplugging the mouse and plugging it back again. Another recommended fix for optical mice is to rotate your mouse pad 90 degrees. At Xerox PARC in the 1970s, most people kept a can of copier cleaner (isopropyl alcohol) at their desks. When the steel ball on the mouse had picked up enough cruft to be unreliable, the mouse was doused in cleaner, which restored it for a while. However, this operation left a fine residue that accelerated the accumulation of cruft, so the dousings became more and more frequent. Finally, the mouse was declared `alcoholic' and sent to the clinic to be dried out in a CFC ultrasonic bath.

Dry Line

An interface line of the equipment under test which does not carry any signals while TEMPEST tests are in progress.

Dual Control

The process of utilizing two or more separate entities (usually persons) operating in concert, to protect sensitive functions or information. Both (all) entities are equally responsible. This approach generally involves the split knowledge [of the] physical or logical protection of security parameters. (WB;)

Dual Homing

The connection of a terminal so that it is served by either of two switching centers. Note: This service uses a single directory number or a single routing indicator. (~) See also alternate routing, dual access, multiple access, multiple homing.

Dual In-Line Package Switch

A subminiature switch compatible with standard integrated-circuit sockets.

#-Due Care

Requires just, proper and sufficient care, so far as the circumstances demand. The absence of negligence. That degree of care that a reasonable person can be expected to exercise to avoid harm reasonable foreseeable if such care is not taken. That care which an ordinarily prudent person would have exercised under the same or similar circumstances. “Due Care” is care proportioned to any given situation, its surroundings, peculiarities, and hazards. (Source Blacks);

*-Duff's Device

n. The most dramatic use yet seen of fall through in C, invented by Tom Duff when he was at Lucasfilm. Trying to bum all the instructions he could out of an inner loop that copied data serially onto an output port, he decided to unroll it. He then realized that the unrolled version could be implemented by *interlacing* the structures of a switch and a loop register n = (count + 7) / 8; /* count > 0 assumed */ switch (count % 8) case 0 do *to = *from++; case 7 *to = *from++; case 6 *to = *from++; case 5 *to = *from++; case 4 *to = *from++; case 3 *to = *from++; case 2 *to = *from++; case 1 *to = *from++; while (--n > 0); Shocking though it appears to all who encounter it for the first time, the device is

actually perfectly valid, legal C. C's default fall through in case statements has long been its most controversial single feature; Duff observed that “This code forms some sort of argument in that debate, but I'm not sure whether it's for or against. ” [For maximal obscurity, the outermost pair of braces above could be actually be removed -- GLS]

Dumb Terminal

1. Terminal (or computer using dumb terminal software) which allows communications with other computers, but does not enhance the data exchanged, or provide additional features such as upload/download. (BBD;)
2. n. A terminal that is one step above a glass tty, having a minimally addressable cursor but no on-screen editing or other features normally supported by a smart terminal. Once upon a time, when glass ttys were common and addressable cursors were something special, what is now called a dumb terminal could pass for a smart terminal.

*-Dumbed Down

adj. Simplified, with a strong connotation of *over*simplified. Often, a marketroid will insist that the interfaces and documentation of software be dumbed down after the designer has burned untold gallons of midnight oil making it smart. This creates friction. See user-friendly.

Dummy Group

Textual group having the appearance of a valid code or cipher group which has no plain text significance. ?

*-Dump

1. n. An undigested and voluminous mass of information about a problem or the state of a system, especially one routed to the slowest available output device (compare core dump), and most especially one consisting of hex or octal runes describing the byte-by-byte state of memory, mass storage, or some file. In elder days, debugging was generally done by `groveling over' a dump (see grovel); increasing use of high-level languages and interactive debuggers has made such tedium uncommon, and the term `dump' now has a faintly archaic flavor.
2. A backup. This usage is typical only at large time-sharing installations.

*-Dumpster Diving

1. /dump'-ster di:'-ving/ n. The practice of sifting refuse from an office or technical installation to extract confidential data, especially security-compromising information (`dumpster' is an Americanism for what is elsewhere called a `skip'). Back in AT&T's monopoly days, before paper shredders became common office equipment, phone phreaks (see phreaking) used to organize regular dumpster runs against phone company plants and offices. Discarded and damaged copies of AT&T internal manuals taught them much. The technique is still rumored to be a favorite of crackers operating against careless targets.
2. The practice of raiding the dumpsters behind buildings where producers and/or consumers of high-tech equipment are located, with the expectation (usually justified) of finding discarded but still-valuable equipment to be nursed back to health in some hacker's den. Experienced dumpster-divers not infrequently accumulate basements full of moldering (but still potentially useful) cruft.

*-Dup Killer

/d[y]oop kill'r/ n. [FidoNet] Software that is supposed to detect and delete duplicates of a message that may have reached the FidoNet system via different routes.

*-Dup Loop

/d[y]oop loop/ (also `dupe loop') n. [FidoNet] An infinite stream of duplicated, near-identical messages on a FidoNet echo, the only difference being unique or mangled identification information applied by a faulty or incorrectly configured system or network gateway, thus rendering dup killers ineffective. If such a duplicate message eventually reaches a system through which it has already passed (with the original identification information), all systems passed on the way back to that system are said to be involved in a dup loop.

*-Dusty Deck

n. Old software (especially applications) which one is obliged to remain compatible with, or to maintain (DP types call this `legacy code', a term hackers consider smarmy and excessively reverent). The term implies that the software in question is a holdover from card-punch days. Used esp. when referring to old scientific and number-crunching software, much of which was written in FORTRAN and very poorly documented but is believed to be too expensive to replace. See fossil; compare crawling horror.

*-DWIM

1. /dwim/ [acronym, `Do What I Mean'] adj. Able to guess, sometimes even correctly, the result intended when bogus input was provided.
2. n. ,obs. The BBNLISP/INTERLISP function that attempted to accomplish this feat by correcting many of the more common errors. See hairy.
3. Occasionally, an interjection hurled at a balky computer, esp. when one senses one might be tripping over legalisms (see legalese). Warren Teitelman originally wrote DWIM to fix his typos and spelling errors, so it was somewhat idiosyncratic to his style, and would often make hash of anyone else's typos if they were stylistically different.

Some victims of DWIM thus claimed that the acronym stood for `Damn Warren's Infernal Machine!'. In one notorious incident, Warren added a DWIM feature to the command interpreter used at Xerox PARC. One day another hacker there typed `delete *$' to free up some disk space. (The editor there named backup files by appending `$' to the original file name, so he was trying to delete any backup files left over from old editing sessions. ) It happened that there weren't any editor backup files, so DWIM helpfully reported `*$ not found, assuming you meant 'delete *'. ' It then started to delete all the files on the disk! The hacker managed to stop it with a Vulcan nerve pinch after only a half dozen or so files were lost. The disgruntled victim later said he had been sorely tempted to go to Warren's office, tie Warren down in his chair in front of his workstation, and then type `delete *$' twice. DWIM is often suggested in jest as a desired feature for a complex program; it is also occasionally described as the single instruction the ideal computer would have. Back when proofs of program correctness were in vogue, there were also jokes about `DWIMC' (Do What I Mean, Correctly). A related term, more often seen as a verb, is DTRT (Do The Right Thing); see Right Thing.

Dynamically Adaptive Routing

*-Dynner

/din'r/ 32 bits, by analogy with nybble and byte. Usagerare and extremely silly. See also playte, tayste, crumb. General discussion of such terms is under nybble.

E

E Model

See Engineering development Model.

E-Mail

See Electronic Mail.

Earth Ground

See ground.

*-Earthquake

n. [IBM] The ultimate real-world shock test for computer hardware. Hackish sources at IBM deny the rumor that the Bay Area quake of 1989 was initiated by the company to test quality-assurance procedures at its California plants.

*-Easter Egg

n. [from the custom of the Easter Egg hunt observed in the U. S. and many parts of Europe]

1. A message hidden in the object code of a program as a joke, intended to be found by persons disassembling or browsing the code.
2. A message, graphic, or sound effect emitted by a program (or, on a PC, the BIOS ROM) in response to some undocumented set of commands or keystrokes, intended as a joke or to display program credits. One well-known early Easter egg found in a couple of OSes caused them to respond to the command `make love' with `not war?'. Many personal computers have much more elaborate eggs hidden in ROM, including lists of the developers' names, political exhortations, snatches of music, and (in one case) graphics images of the entire development team.

*-Easter Egging

n. [IBM] The act of replacing unrelated components more or less at random in hopes that a malfunction will go away. Hackers consider this the normal operating mode of field circus techs and do not love them for it. See also the jokes under field circus. Compare shotgun debugging.

Eavesdropping

The unauthorized interception of information- bearing emanations through the use of methods other than wiretapping. (*FIPS PUB* 39;; *AR* 380-380;) (NSA, *National INFOSEC Glossary*, 10/88)

EBCDIC

/eb's*-dik/, /eb'see`dik/, or /eb'k*-dik/ n. [abbreviation, Extended Binary Coded Decimal Interchange Code] An alleged character set used on IBM mainframes. It exists in at least six mutually incompatible versions, all featuring such delights as non-contiguous letter sequences and the absence of several ASCII punctuation characters fairly important for modern computer languages (exactly which characters are absent varies according to which version of EBCDIC you're looking at). IBM adapted EBCDIC from punched card code in the early 1960s and promulgated it as a customer-control tactic, spurning the already established ASCII standard. Today, IBM claims to be an open-systems company, but IBM's own description of the EBCDIC variants and how to convert between them is still internally classified top-secret, burn-before-reading. Hackers blanch at the very *name* of EBCDIC and consider it a manifestation of purest.

ECCM

See Electronic Counter-CounterMeasures.

Echo

1. A wave that has been reflected or otherwise returned with sufficient magnitude and delay to be perceived. (~) Note 1: Echoes are frequently measured in decibels relative to the directly

transmitted wave. Note 2: Echoes may be desirable (as in radar usage) or undesirable (as in telephone usage). See also echo attenuation, echo suppressor, feeder echo noise, forward echo, ghost, return loss.

2. In computing, to print or display characters (a) as they are entered from an input device, (b) as instructions are executed, or (c) as retransmitted characters are received from a remote terminal.
3. For an interactive computer graphics display, the immediate notification of the current value for a graphics parameter or operation as selected by the user.

Economic Assessment

A detailed study of security measures, their operational and technical feasibility, and their costs and benefits. Economic assessment aids in planning and selecting security measures. (*AFR* 205-16;; *AFR* 700-10;)

Economic Intelligence

Intelligence regarding economic resources, activities, and policies. *Intelligence regarding foreign economic resources, activities, and policies including the production, distribution, and consumption of goods and services, labor, finance, taxation, and other aspects of the international economic system (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

#-Education, Training And Awareness

This KSA has no definition.

EIA Interface

Any of a number of equipment interfaces compliant with voluntary industry standards developed by the Electronic Industries Association (EIA) to define interface parameters. Note 1: Some of these standards have been adopted by the Federal Government as Federal standards. Note 2: The telecommunication-standards-developing bodies of the EIA are now part of the Telecommunications Industry Association (TIA), and the standards are designated EIA/TIA-XXX. See also interface.

Eight-Hundred Service

(800) Synonym Inward Wide-Area Telephone service.

*-Eighty-Column Mind

n. [IBM] The sort said to be possessed by persons for whom the transition from punched card to tape was traumatic (nobody has dared tell them about disks yet). It is said that these people, including (according to an old joke) the founder of IBM, will be buried `face down, 9-edge first' (the 9-edge being the bottom of the card). This directive is inscribed on IBM's 1402 and 1622 card readers and is referenced in a famous bit of doggerel called “The Last Bug”, the climactic lines of which are as follows He died at the console Of hunger and thirst. Next day he was buried, Face down, 9-edge first. The eighty-column mind is thought by most hackers to dominate IBM's customer base and its thinking. See IBM, fear and loathing, card walloper.

*-El Camino Bignum

/el' k*-mee'noh big'nuhm/ n. The road mundanely called El Camino Real, a road through the San Francisco peninsula that originally extended all the way down to Mexico City and many portions of which are still intact. Navigation on the San Francisco peninsula is usually done relative to El Camino Real, which defines logical north and south even though it isn't really north-south many places. El Camino Real runs right past Stanford University and so is familiar to hackers. The Spanish word `real' (which has two syllables /ray-ol'/) means `royal'; El Camino Real is `the royal road'. In the FORTRAN language, a `real' quantity is a number typically precise to seven significant digits, and a `double precision' quantity is a larger floating-point number, precise to perhaps fourteen significant digits (other languages have similar `real' types). When a hacker from MIT visited Stanford in 1976, he remarked what a long road El Camino Real was. Making a pun on `real', he started calling it `El Camino Double Precision' -- but when the hacker was told that the road was hundreds of miles long, he renamed it `El Camino Bignum', and that name has stuck. (See bignum. ) In recent years, the synonym `El Camino Virtual' has been reported as an alternate at IBM and Amdahl sites in the Valley. [GLS has since let slip that the unnamed hacker in this story was in fact him -- ESR]

*-Elder Days

n. The heroic age of hackerdom (roughly, pre-1980); the era of the PDP-10, TECO, ITS, and the ARPANET. This term has been rather consciously adopted from J. R. R. Tolkien's fantasy epic “The Lord of the Rings”. Compare Iron Age; see also elvish and Great Worm, the.

Electro-Optical Intelligence

(ELECTRO-OPTINT) Intelligence information derived from the optical monitoring of the electromagnetic spectrum. *Intelligence information derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0. 01 micrometers) through far (long wavelength) infrared (1,000 micrometers) NOTE: See Optical Intelligence (IC Staff, Glossary of Intelligence Terms and Definition, 6/89)

Electrochemical Recording

Facsimile recording by means of a chemical reaction brought about by the passage of a signal-controlled current through the sensitized portion of the record sheet. (~) See also direct recording, facsimile, recording.

Electrographic Recording
See electrostatic recording.

#-Electromagnetic Countermeasures
This KSA has no definition.

Electromagnetic Emanations
Signals transmitted as radiation through the air and through conductors. (*FIPS PUB* 39;; *AR* 380-380;)

#-Electromagnetic Interference
This KSA has no definition.

#-Electronic Data Interchange
The transmission of documents from one computer to another over a network. (Source *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Electronic Emission Security
Those measures taken to protect all transmissions from interception and electronic analysis. (~) See also electromagnetic interference control, electronics security, electronic warfare, emanations security, TEMPEST.

#-Electronic Funds Transfer
(EFT) In data communications, an automated system for transferring funds from one bank account to another using electronic equipment and data communications rather than paper media and the postal system. (Data & Computer SECURITY Dictionary of Standards, Concepts and Terms)

Electronic Intelligence
(ELINT) Technical and intelligence information derived from foreign non-communications transmissions by other than the intended recipients. *Technical and intelligence information derived from foreign non-communications transmissions by other than the intended recipients Technical and intelligence information derived from foreign non-communications electromagnetic radiations emanating from other than atomic detonation or radioactive sources (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

#-Electronic Key Management System
Interoperable collection of systems being developed by services and agencies of the US Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material. (Source: EKMS 004. 01).

Electronic Mail
An electronic means for communicating information (primarily text) by a method of sending, storing, processing, and retrieving the information. This allows users to communicate under specified conditions. Note: Messages are held in storage until called for by the addressee. (~) See also data transmission, Integrated Services Digital Network, store-and-forward.

Electronic Message System
An electronic mail system incorporating the additional feature in which the central facility assumes active responsibility for delivering the message to the intended addressee(s) rather than the passive role of an electronic mail system, which merely delivers messages in response to a request by an addressee.

#-Electronic Monitoring
The acquisition of any electronic command or communication by other than the sender or intended receiver (Source Panel of experts);

#-Electronic Records Management
Is the responsibility of the head of each Federal agency. It includes:

a. assigning responsibility to develop and implement an agency wide program for the management of all electronic records,
b. integrating the management of electronic records with other agency records,
c having and disseminating agency directives that address records management requirements;
d establishing procedures for addressing records management requirements;
e ensuring adequate training is provided with regard to electronic records management;
f developing and maintaining up to date documentation about all electronic records systems;
g specifying how electronic records are to be maintained and an inventory of such records;
h developing and securing approval from the national archive and records administration (NARA) of records disposition schedules, and implementation of their provisions;
i specifying the methods of implementing controls over national security classified, sensitive, proprietary, and Privacy Act records stored and used electronically;
j establishing procedures that these requirements are implemented and applied to contractors;
k ensuring compliance with applicable Government wide policies; and
l reviewing electronic records systems periodically for conformance to established agency procedures, standards, and policies. (Source 36 CFR Part 1234).

Electronic Seals

Electronic Security
Protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and

analysis of non-communications electromagnetic radiations, such as radar.

Electronic Security Assessment

One of three levels of capability to improve communications-computer systems security posture by accurately measuring the posture and recommending countermeasures where deficiencies exist.

Electronic Signature

Process that operates on a message to assure message source authenticity and integrity, and source non-repudiation.

#-Electronic Sources Of Security Information

This KSA has no definition.

Electronic Surveillance

The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. (NACSI 4000A)

Electronic Switching System

Any switching system whose major components use semiconductor devices. This includes semielectronic systems that have reed relays or crossbar matrices. (~) See also crossbar switch, switching system.

#-Electronic-Mail Privacy

measures taken to protect the confidentiality and sensitivity of electronic mail messages from the threat or unauthorized surveillance. Measures include the use of data encryption and authentication programs. (Source: Panel of experts)

#-Electronic-Mail Security

security in electronic mail systems introduced to ensure the confidentiality and or integrity of electronic mail messages. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992

Electronically

Key produced only in non-physical generated key form. NOTE: Electronically generated key stored magnetically (e. g. , on a floppy disc) is not considered hard copy key.

Electronically Generated Key

Key produced only in non-physical form. NOTE: Electronically generated key stored magnetically (e. g. , on a floppy disc) is not considered hard copy key. See Hard Copy Key.

Electronics Intelligence

Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JCS1-DoD) See also electromagnetic environment, electromagnetic interference, electronic warfare, intercept, interference.

Electronics Security

1. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception, and study of noncommunications electromagnetic radiations, e. g. , radar. (JCS1-DoD)
2. (ELSEC) The protection resulting from measures designed to deny unauthorized persons information of value from the interception and analysis of non-communications electromagnetic radiations. *The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and analysis of non-communications electromagnetic radiations, such as radar. (NSA, *National INFOSEC Glossary*, 10/88)

Electrosensitive Recording

A method of recording by means of impressing an electrical signal directly on the record medium. See also facsimile, recording.

Electrostatic Recording

1. Recording by means of a signal-controlled electrostatic field. (~)
2. Note: Subsequent processing is usually required to make the image visible. See also direct recording, facsimile, recording.

Electrothermal Recording

That type of recording produced principally by signal-controlled thermal action. (~) See also facsimile, recording.

*-Elegant

adj. [from mathematical usage] Combining simplicity, power, and a certain ineffable grace of design. Higher praise than `clever', `winning', or even cuspy. The French aviator, adventurer, and author Antoine de Saint-Exup'ery, probably best known for his classic children's book "The Little Prince", was also an aircraft designer. He gave us perhaps the best definition of engineering elegance when he said "A designer knows he has achieved perfection not when there is nothing left to add, but when there is nothing left to take away. "

Element

Removable item of COMSEC equipment, assembly, or subassembly which normally consists of a single piece or group of replaceable parts.

*-Elephantine

adj. Used of programs or systems that are both conspicuous hogs (owing perhaps to poor design founded on brute force and ignorance) and exceedingly hairy in source form. An elephantine program may be func-

tional and even friendly, but (as in the old joke about being in bed with an elephant) it's tough to have around all the same (and, like a pachyderm, difficult to maintain). In extreme cases, hackers have been known to make trumpeting sounds or perform expressive proboscatory mime at the mention of the offending program. Usage semi-humorous. Compare `has the elephant nature' and the somewhat more pejorative monstrosity. See also second-system effect and baroque.

*-Elevator Controller

n. An archetypal dumb embedded-systems application, like toaster (which superseded it). During one period (1983--84) in the deliberations of ANSI X3J11 (the C standardization committee) this was the canonical example of a really stupid, memory-limited computation environment. “You can't require `printf(3)' to be part of the default runtime library -- what if you're targeting an elevator controller?” Elevator controllers became important rhetorical weapons on both sides of several holy wars.

*-Elite

adj. Clueful. Plugged-in. One of the cognoscenti. Also used as a general positive adjective. This term is not actually hacker slang in the strict sense; it is used primarily by crackers and warez d00dz. Cracker usage is probaby related to a 19200cps modem called the `Courier Elite' that was widely popular on pirate boards before the V. 32bis standard. A true hacker would be more likely to use `wizardly'. Oppose lamer.

*-ELIZA Effect

/*-li:'z* *-fekt'/ n. [AI community] The tendency of humans to attach associations to terms from prior experience. For example, there is nothing magic about the symbol `+' that makes it well-suited to indicate addition; it's just that people associate it with addition. Using `+' or `plus' to mean addition in a computer language is taking advantage of the ELIZA effect. This term comes from the famous ELIZA program by Joseph Weizenbaum, which simulated a Rogerian psychotherapist by rephrasing many ofthe patient's statements as questions and posing them to the patient. It worked by simple pattern recognition and substitution of key words into canned phrases. It was so convincing, however, that there are many anecdotes about people becoming very emotionally caught up in dealing with ELIZA. All this was due to people's tendency to attach to words meanings which the computer never put there. The ELIZA effect is a Good Thing when writing a programming language, but it can blind you to serious shortcomings when analyzing an Artificial Intelligence system. Compare ad-hockery; see also AI-complete.

*-Elvish

1. n. The Tengwar of Feanor, a table of letterforms resembling the beautiful Celtic half-uncial hand of the “Book of Kells”. Invented and described by J. R. R. Tolkien in “The Lord of The Rings” as an orthography for his fictional `elvish' languages, this system (which is both visually and phonetically elegant) has long fascinated hackers (who tend to be intrigued by artificial languages in general). It is traditional for graphics printers, plotters, window systems, and the like to support a Feanorian typeface as one of their demo items. See also elder days.
2. By extension, any odd or unreadable typeface produced by a graphics device.
3. The typeface mundanely called `B”ocklin', an art-decoish display font.

*-EMACS

/ee'maks/ n. [from Editing MACroS] The ne plus ultra of hacker editors, a programmable text editor with an entire LISP system inside it. It was originally written by Richard Stallman in TECO under ITS at the MIT AI lab; AI Memo 554 described it as “an advanced, self-documenting, customizable, extensible real-time display editor”. It has since been reimplemented any number of times, by various hackers, and versions exist that run under most major operating systems. Perhaps the most widely used version, also written by Stallman and now called “GNU EMACS” or GNUMACS, runs principally under UNIX. It includes facilities to run compilation subprocesses and send and receive mail; many hackers spend up to 80% of their tube time inside it. Other variants include GOSMACS, CCA EMACS, UniPress EMACS, Montgomery EMACS, jove, epsilon, and MicroEMACS. Some EMACS versions running under window managers iconify as an overflowing kitchen sink, perhaps to suggest the one feature the editor does not (yet) include. Indeed, some hackers find EMACS too heavyweight and baroque for their taste, and expand the name as `Escape Meta Alt Control Shift' to spoof its heavy reliance on keystrokes decorated with bucky bits. Other spoof expansions include `Eight Megabytes And Constantly Swapping', `Eventually `malloc()'s All Computer Storage', and `EMACS Makes A Computer Slow' (see recursive acronym). See also vi.

*-Email

1. /ee'mayl/ (also written `e-mail') n. Electronic mail automatically passed through computer networks and/or via modems over common-carrier lines. Contrast snail-mail, paper-net, voice-net. See network address.
2. vt. To send electronic mail. Oddly enough, the word `emailed' is actually listed in the OED; it means “embossed (with a raised pattern) or perh. arranged in a net or open work”. A use from 1480 is given. The word is derived from Old French `emmaill”ure', network. A French correspondent tells us that in modern French, `email' is a hard

enamel obtained by heating special paints in a furnace; an `emailleur' (no final e) is a craftsman who makes email (he generally paints some objects like jewels and cook them in a furnace).

Emanation

Unintended signals or noise appearing external to an equipment.

Emanation Security

The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations. (*FIPS PUB* 39;)

Emanations

See COMPROMISING EMANATIONS And ELECTROMAGNETIC EMANATIONS.

#-Emanations Security

Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose the information transmission received, handled, or otherwise processed by any information processing equipment. (Source: *NCSC-TG*-0004).

Embedded Computer

Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or in part.

Embedded Computers

Computer hardware and software that are an integral part of a product, where the principal function of the product is not the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. An embedded computer would require major modification to be used for general purpose computing and is managed as a component of the system in which it is embedded. (Federal Information Resources Management Regulation [FIRMR]).

Embedded Cryptographic

Cryptosystem that performs or controls system a function, either in whole or in part, as an integral element of a larger system or subsystem.

Embedded Cryptographic System

Cryptosystem that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem.

Embedded Cryptography

Cryptography which is engineered into an equipment or system the basic function of which is not cryptographic. NOTE: Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed or identifiable as a separate module within the host.

Embedded System

1. An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e. g. , ground support equipment, flight simulators, engine test stands, or fire control systems. (DODD 5200. 28)
2. Computers which are dedicated elements, subsystems, or components of more extensive Air Force systems. (*AFR* 205-16)

Emergency

A sudden, generally unexpected event, that does or could do harm to people, the environment, resources, property, or institutions. Note: Emergencies range from relatively local events to regional and national events and may be caused by natural or technological factors, human actions, or national security-related events.

#-Emergency Destruction

#-Emergency Destruction Procedures

A structured set of guidelines developed in accordance with doctrinal guidance for controlling and possible disposition of material in emergency situations, i. e. , hostilities towards embassies worldwide and potential takeover, potential over run of troops during wartime, etc.

Emergency Plan

See Contingency Plan.

Emission Security

1. A component of COMSEC that results from all measures to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from electrically operated classified information processing equipment and systems. (*AR* 380-380)
2. That component of communications security (COMSEC) which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. (NCSC-9; JCS PUB 1)
3. The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations fromsystems. (*NCSC-TG*-004-88)

Emissions Security

(EMSEC) The protection resulting from measures taken to deny unauthorized persons information of

value from interception and analysis of compromising emanations. *The protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems, and telecommunications systems (NSA, *National INFOSEC Glossary*, 10/88)

*-Emoticon

/ee-moh'ti-kon/ n. An ASCII glyph used to indicate an emotional state in email or news. Although originally intended mostly as jokes, emoticons (or some other explicit humor indication) are virtually required under certain circumstances in high-volume text-only communication forums such as Usenet; the lack of verbal and visual cues can otherwise cause what were intended to be humorous, sarcastic, ironic, or otherwise non-100%-serious comments to be badly misinterpreted (not always even by newbies), resulting in arguments and flame wars. Hundreds of emoticons have been proposed, but only a few are in common use. These include -) `smiley face' (for humor, laughter, friendliness, occasionally sarcasm) -(`frowney face' (for sadness, anger, or upset) ;-) `half-smiley' (ha ha only serious); also known as `semi-smiley' or `winkey face'. -/ `wry face' (These may become more comprehensible if you tilt your head sideways, to the left.) The first two listed are by far the most frequently encountered. Hyphenless forms of them are common on CompuServe, GEnie, and BIX; see also bixie. On Usenet, `smiley' is often used as a generic term synonymous with emoticon, as well as specifically for the happy-face emoticon. It appears that the emoticon was invented by one Scott Fahlman on the CMU bboard systems around 1980. He later wrote “I wish I had saved the original post, or at least recorded the date for posterity, but I had no idea that I was starting something that would soon pollute all the world's communication channels. ” [GLS confirms that he remembers this original posting]. Note for the newbie Overuse of the smiley is a mark of loserhood! More than one per paragraph is a fairly sure sign that you've gone over the line.

*-Empire

n. Any of a family of military simulations derived from a game written by Peter Langston many years ago. Five or six multi-player variants of varying degrees of sophistication exist, and one single-player version implemented for both UNIX and VMS; the latter is even available as MS-DOS freeware. CDC supported a version on PLATO. It and Moria were said to be the largest money makers in terms of connect time on the educational system. All are notoriously addictive.

Emulate

To duplicate the functions of one system with a different system, so that the second system appears to behave like the first system. Note: For example, a computer emulates another, different computer by accepting the same data, executing the same programs, and achieving the same results. Contrast with simulate.

Emulator

A combination of hardware and software that permits programs written for one computer to be run on another computer. In computer security terminology, the emulator is the portion of the system responsible for creating an operating system compatible environment out of the environment provided by the kernel. In KSOS, the emulator maps the kernel environment into the UNIX environment. (MTR-8201;)

En-Bloc Signaling

Encipher

1. To convert plain text into an unintelligible form by means of a cipher system. (*FIPS PUB* 39; *AR* 380-380)
2. To convert plain text into enciphered text by means of a cipher system. (NCSC-9)encode

Encipherment

The cryptographic transformation of data to produce ciphertext. Note: Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed. (SS;)

Encode

To convert plain text into an unintelligible form by means of a code system. (*FIPS PUB* 39;; *AR* 380-380;)

Encoder

See analog-to-digital converter.

Encoding

See analog encoding.

Encoding Law

The law defining the relative values of the quantum steps used in quantizing and encoding signals. See also code, segmented encoding law.

Encrypt

1. To convert plain text into unintelligible form by means of a cryptosystem. (*AFR* 700-10;; *AR* 380-380;; *FIPS PUB* 39;)
2. Note: The term encrypt encompasses the terms “encipher' and “encode. ” (NCSC-9)

Encryption

1. Transforming a text into code in order to conceal its meaning. a) End-to-end encryption. Encryption of information at the origin within a communications network and postponing decryption to the fi-

nal destination point. b) Link encryption. The application of on-line crypto operations to a link of a communications system so that all information passing over the link is encrypted. (*AR* 380-380;)
2. The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process. (*FIPS PUB* 112;)
3. See END-TO-END ENCRYPTION and LINK ENCRYPTION.

Encryption Algorithm

1. A set of mathematical rules for rendering information unintelligible by effecting a series of transformations to the normal representation of the information through the use of variable elements controlled by a key. (*AR* 380-380;)
2. A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a key to the normal representation of the information. Synonymous with Privacy Transformation. (*FIPS PUB* 39;)

#-Encryption Codes

A method of converting plain text to an equivalent cipher text by means of a code.

End System

A system containing the application processes that are the ultimate sources and destinations of user oriented message flows. Note: The functions of an end system can be distributed among more than one processor/computer.

End User

The ultimate consumer of a telecommunication service. See also destination user, source user.

#-End User Computing Security

This KSA has no definition.

End-Item Accounting

Accounting for all the accountable components of a COMSEC equipment configuration by a single short title.

End-Of-Message Function

In tape relay procedure, the letter and key functions, including the end-of-message indicator, that constitute the last format line. (~) See also relay, reperforator, tape relay, torn-tape relay.

End-Of-Selection Character

The character that indicates the end of the selection signal. See also binary synchronous communication, character.

End-Of-Text Character

A transmission control character used to terminate text. (FP) (ISO) See also binary synchronous communication, character.

End-Of-Transmission Character

A transmission control character used to indicate the conclusion of a transmission that may have included one or more texts and any associated message headings. (FP) (ISO) Note: Often used to initiate other functions such as releasing circuits, disconnecting terminals, or placing receive terminals in a standby condition. See also binary synchronous communication, character.

End-Of-Transmission-Block Character

A transmission control character used to indicate the end of a transmission block of data when data are divided into such blocks for transmission purposes. (FP) (ISO) See also binary synchronous communication, block, character.

End-To-End

1. Encryption of information at the origin within a encryption communications network and postponing decryption to the final destination point. (*FIPS PUB* 39)
2. The protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination. (*NCSC-TG*-004-88)
3. See ENCRYPTION and LINK ENCRYPTION.

End-To-End Encipherment

Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (SS;)

End-To-End Encryption

1. Encryption of information at the origin within a communications network and postponing decryption to the final destination point. (*FIPS PUB* 39;)
2. The protection of information passed in a secure telecommunications system by cryptographic means, from point of origin to point of destination. (*NCSC-WA*-001-85;)

End-To-End Security

Safeguarding information in a secure telecommunications system by cryptographic or protected distribution system means from point of origin to point of destination.

Endorsed DES

Unclassified equipment that embodies equipment unclassified data encryption standard cryptographic logic and has been endorsed by the National Security Agency for the protection of national security information.

Endorsed DES Equipment

Unclassified equipment that embodies unclassified data encryption standard cryptographic logic and has been endorsed by the National Security Agency for the protection of national security information.

Endorsed For Unclassified

Unclassified cryptographic equipment cryptographic item that embodies U. S. Government classified cryptographic logic and is endorsed by the National Security Agency for the protection of national security information.

Endorsed For Unclassified Cryptographic Item

Unclassified cryptographic equipment which embodies a U. S. Government classified cryptographic logic and is endorsed by the National Security Agency for the protection of national security information. See Type 2 Product.

Endorsed Tools List

The list of formal verification tools endorsed by the NCSC for the development of systems with high levels of trust. (AF9K_JBC. TXT) (ETL) List of formal verification tools endorsed by the National Computer Security Center (NCSC) for the development of systems with high levels of trust.

Endorsement

National Security Agency approval of a commercially-developed telecommunications or automated information systems protection equipment or system for safeguarding national security information.

*-Engine

1. n. A piece of hardware that encapsulates some function but can't be used without some kind of front end. Today we have, especially, `print engine' the guts of a laser printer.
2. An analogous piece of software; notionally, one that does a lot of noisy crunching, such as a `database engine'. The hackish senses of `engine' are actually close to its original, pre-Industrial-Revolution sense of a skill, clever device, or instrument (the word is cognate to `ingenuity'). This sense had not been completely eclipsed by the modern connotation of power-transducing machinery in Charles Babbage's time, which explains why he named the stored-program computer that he designed in 1844 the `Analytical Engine'.

Engineering Development Model

(EDM) Model of COMSEC equipment used for engineering or operational tests under service conditions for evaluation of performance and operational suitability.

*-English

1. n. ,obs. The source code for a program, which may be in any language, as opposed to the linkable or executable binary produced from it by a compiler. The idea behind the term is that to a real hacker, a program written in his favorite programming language is at least as readable as English. Usage mostly by old-time hackers, though recognizable in context.
2. The official name of the database language used by the Pick Operating System, actually a sort of crufty, brain-damaged SQL with delusions of grandeur. The name permits marketroids to say “Yes, and you can program our computers in English!” to ignorant suits without quite running afoul of the truth-in-advertising laws.

Enhanced Hierarchical Development Methodology

A software development methodology which makes use of the language REVISED SPECIAL to formally prove design specifications. REVISED SPECIAL is a language developed by SRI International. (*NCSC-WA*-001-85;)

2. An integrated set of tools designed to aid in creating, analyzing, modifying, managing, and documenting program specifications and proofs. This methology includes a specification parser and typechecker, a theorem prover, and a multi-level security checker. Note: This methodology is not based upon the Hierarchical Development Methodology.

*-Enhancement

n. Common marketroid-speak for a bug fix. This abuse of language is a popular and time-tested way to turn incompetence into increased revenue. A hacker being ironic would instead call the fix a feature -- or perhaps save some effort by declaring the bug itself to be a feature.

*-ENQ

/enkw/ or /enk/ [from the ASCII mnemonic ENQuire for 0000101] An on-line convention for querying someone's availability. After opening a talk mode connection to someone apparently in heavy hack mode, one might type `SYN SYN ENQ?' (the SYNs representing notional synchronization bytes), and expect a return of ACK or NAK depending on whether or not the person felt interruptible. Compare ping, finger, and the usage of `FOO?' listed under talk mode.

Entrapment

1. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations. (*AR* 380-380;; *NCSC-WA*-001-85;)
2. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit. (*FIPS PUB* 39;)

Entry

See BETWEEN-THE-LINES ENTRY and PIGGY BACK ENTRY.

Environment

1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. (CSC-STD-004-85;; CSC-STD-003-85;; *NCSC-WA*-001-85;)
2. Those factors, both internal and external, of an ADP system that help to define the risks associated with its operation, e. g. , the interfaces within the ADP system, the associated software, the type and level of information contained within the ADP system, the access control mechanisms used to restrict access, and the physical characteristics of the operational area. (DOE 5636. 2A;)

#-Environmental Controls

The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system. (Source: *NCSC-TG*-004.)

#-Environmental/Natural Threats

This KSA has no definition.

*-EOF

/E-O-F/ n. [abbreviation, `End Of File']

1. [techspeak] The out-of-band value returned by C's sequential character-input functions (and their equivalents in other environments) when end of file has been reached. This value is -1 under C libraries postdating V6 UNIX, but was originally 0.
2. [UNIX] The keyboard character (usually control-D, the ASCII EOT (End Of Transmission) character) that is mapped by the terminal driver into an end-of-file condition.
3. Used by extension in non-computer contexts when a human is doing something that can be modeled as a sequential read and can't go further. “Yeah, I looked for a list of 360 mnemonics to post as a joke, but I hit EOF pretty fast; all the library had was a JCL manual. ” See also EOL.

*-EOL

/E-O-L/ n. [End Of Line] Syn. for newline, derived perhaps from the original CDC6600 Pascal. Now rare, but widely recognized and occasionally used for brevity. Used in the example entry under BNF. See also EOF.

*-EOU

/E-O-U/ n. The mnemonic of a mythical ASCII control character (End Of User) that would make an ASR-33 Teletype explode on receipt. This construction parodies the numerous obscure delimiter and control characters left in ASCII from the days when it was associated more with wire-service teletypes than computers (e. g. , FS, GS, RS, US, EM, SUB, ETX, and esp. EOT). It is worth remembering that ASR-33s were big, noisy mechanical beasts with a lot of clattering parts; the notion that one might explode was nowhere near as ridiculous as it might seem to someone sitting in front of a tube or flatscreen today.

*-Epoch

n. [UNIX prob. from astronomical timekeeping] The time and date corresponding to 0 in an operating system's clock and timestamp values. Under most UNIX versions the epoch is 00:00:00 GMT, January 1, 1970; under VMS, it's 00:00:00 of November 17, 1858 (base date of the U. S. Naval Observatory's ephemerides); on a Macintosh, it's the midnight beginning January 1 1904. System time is measured in seconds or ticks past the epoch. Weird problems may ensue when the clock wraps around (see wrap around), which is not necessarily a rare event; on systems counting 10 ticks per second, a signed 32-bit count of ticks is good only for 6. 8 years. The 1-tick-per-second clock of UNIX is good only until January 18, 2038, assuming at least some software continues to consider it signed and that word lengths don't increase by then. See also wall time.

EPROM

See Erasable Programmable Read Only Memory.

*-Epsilon

1. [see delta] n. A small quantity of anything. “The cost is epsilon. ”
2. adj. Very small, negligible; less than marginal. “We can get this feature for epsilon cost. ”
3. `within epsilon of' close enough to be indistinguishable for all practical purposes, even closer than being `within delta of'. “That's not what I asked for, but it's within epsilon of what I wanted. ” Alternatively, it may mean not close enough, but very little is required to get it there “My program is within epsilon of working. ”

*-Epsilon Squared

n. A quantity even smaller than epsilon, as small in comparison to epsilon as epsilon is to something normal; completely negligible. If you buy a supercomputer for a million dollars, the cost of the thousand-dollar terminal to go with it is epsilon, and the cost of the ten-dollar cable to connect them is epsilon squared. Compare lost in the underflow, lost in the noise.

Equipment Radiation Tempest Zone

(ERTZ) A zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

Equipment Under Test

(EUT) An equipment or group of equipments subjected to TEMPEST testing.

*-Era

the Syn. epoch. Webster's Unabridged makes these words almost synonymous, but `era' more often connotes a span of time rather than a point in time, whereas the reverse is true for epoch. The epoch usage is recommended.

Eradication

Erase

1. To obliterate information from any storage medium, e. g. , to clear or to overwrite. (~)
2. To remove all previous data from magnetic storage by changing it to a specified condition that may be an unmagnetized state or predetermined magnetized state. See also read-only storage, storage.

Erasure

1. A security model rule stating that objects must be purged before being activated or reassigned. This ensures that no information is retained within an object when it is reassigned to a subject at a different security level. (MTR-8201;)
2. A process by which a signal recorded on magnetic media is removed (i. e. , degaussed). Erasure may be accomplished in two ways: in AC erasure, the media are degaussed by applying an alternating field which is reduced in amplitude from an initial high value (i. e. , AC powered); in DC erasure, the media are saturated by applying a unidirectional field (i. e. , DC powered or by employing a permanent magnet). (CSC-STD-005-85;; *NCSC-WA*-001-85;)

*-Eric Conspiracy

n. A shadowy group of mustachioed hackers named Eric first pinpointed as a sinister conspiracy by an infamous talk. bizarre posting ca. 1986; this was doubtless influenced by the numerous `Eric' jokes in the Monty Python oeuvre. There do indeed seem to be considerably more mustachioed Erics in hackerdom than the frequency of these three traits can account for unless they are correlated in some arcane way. Well-known examples include Eric Allman (he of the `Allman style' described under indent style) and Erik Fair (co-author of NNTP); your editor has heard from about fifteen others by email, and the organization line `Eric Conspiracy Secret Laboratories' now emanates regularly from more than one site.

*-Eris

/e'ris/ n. The Greek goddess of Chaos, Discord, Confusion, and Things You Know Not Of; her name was latinized to Discordia and she was worshiped by that name in Rome. Not a very friendly deity in the Classical original, she was reinvented as a more benign personification of creative anarchy starting in 1959 by the adherents of Discordianism and has since been a semi-serious subject of veneration in several `fringe' cultures, including hackerdom. See Discordianism, Church of the SubGenius.

*-Erotics

/ee-ro'tiks/ n. [Helsinki University of Technology, Finland] n. English-language university slang for electronics. Often used by hackers in Helsinki, maybe because good electronics excites them and makes them warm.

Error

*-Error 33

1. [XEROX PARC] n. Predicating one research effort upon the success of another.
2. Allowing your own research effort to be placed on the critical path of some other project (be it a research effort or not).

Error Budget

The allocation of a bit-error-ratio requirement to the segments of a circuit, e. g. , trunking, switching, access lines, terminal devices, in a manner that permits the specified system end-to-end bit-error-ratio requirements to be satisfied for traffic transmitted over a postulated reference circuit. (~) See also binary digit, bit error ratio, error.

#-Error Logs

A file created by the operating system which may be useful for review as part of the audit process. (Source: Panel of Experts, July 1994).

Error Rate Deprecated Term

See Error Ratio.

Error Ratio

The ratio of the number of bits, elements, characters, or blocks incorrectly received to the total number of bits, elements, characters, or blocks sent in a specified time interval. (~) See also binary digit, bit error ratio, block, block transfer rate, character, error.

Error-Correcting Code

A code in which each telegraph or data signal conforms to specific rules of construction so that departures from this construction in the received signals can generally be automatically detected and corrected. If the number of errors is not greater than the maximum correctable threshold of the code, then all errors are corrected. (~) Note 1: Such codes require more signal elements than are necessary to convey the basic information. Note 2: The two main classes of error-correction codes are block codes and convolutional codes. See also block code, code, convolutional code, error control, forward error correction, Hagelbarger code, Hamming code.

Error-Correcting System

In digital data transmission, a system employing either forward error correction (FEC) or automatic repeat-request (ARQ) techniques such that most transmission errors are automatically removed from the data unit prior to delivery to the destination facility. (~) See also ARQ, code, communications system, error, error control, error correcting code, error-detecting code, forward error correction.

Error-Detecting Code

A code in which each telegraph or data signal conforms to specific rules of construction, so that departures from this construction in the received signals can be detected automatically. (~) Note: Such codes require more signal elements than are necessary to convey the basic information. See also block parity, code, error, error control, error-correcting code, error-correcting system.

Error-Detecting System

A system employing an error-detecting code and so arranged that any signal detected as being in error is either deleted from the data delivered to the data sink, in some cases with an indication that such deletion has taken place, or delivered to the data sink together with an indication that the signal is in error. See also code, cyclic redundancy check, error, error control.

Error-Detecting-And-Feedback System

Synonym ARQ.

Escort(s)

Duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted. (*OPNAVINST* 5239. 1A; *AR* 380-380; *DCID* 1/16; *DCID* 1/16, Sup. ; 380; *DCID* 1/16; *DCID* 1/16, Sup. ; *DOD* 5200. 28M)

Espionage

Intelligence activity directed toward the acquisition of information through clandestine or covert means. *Intelligence activity directed toward the acquisition of information through clandestine means and proscribed by the laws of the country against which it is committed (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Essential Elements Of Friendly Information

(EEFI) Key questions about friendly intentions and military capabilities asked by opposing planners and decision makers. This information if acquired by hostile interests by any means, might jeopardize the successful execution of an operation. (*AFR* 205-16) Key questions are likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness (JCS MOP 199, 3/89)

Essential Elements Of Friendly Information (EERI)

Information concerning a plan, project, or activity which, if acquired by hostile interests by any means, might jeopardize the successful execution of an operation. (*AFR* 205-16;)

Essential Elements Of Information

(EEI) Key questions likely to be asked by friendly planners about specific adversaries' intentions, capabilities, and activities. *

1. Items of intelligence information essential for timely decisions and for enhancement of operations that relate to foreign powers, forces, targets, or the physical environments;
2. Targets (documents, instruments, etc.) that intelligence and/or security services attempt to obtain;
3. (Military usage) The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Essential Secrecy

The condition achieved from the denial of critical information to an adversary. *The condition achieved from the denial of critical information (Navy, *OPNAVINST* 3070. 1B) (JCS Pub 3-54, 9/89)

Essentially Rating

An importance-time-related designation assigned to a computer application that indicates when an application must be back in operation to avoid mission impacts after a disaster or interruption in computer support services at a multiuser installation. To facilitate prioritized recovery procedures and for operating at offsite backup facilities in a degraded mode (i. e. , only most essential applications), computer applications should be assigned essentiality ratings of varying importance (e. g. , most essential, essential, important, defferable). Applications with the same essentiality rating (i. e. , most essential) should be additionally ranked (e. g. , numerically) according to installation or site determined processing priorities and perceptions of importance. (*DOE 1360. 2A*)

#-Ethics

The principles of conduct governing an individual or group. (Source: Panel of Experts, July 1994).

Eut Exerciser Equipment

Any equipment or device (not part of the EUT) used during TEMPEST testing to make the equipment under test (EUT) operate; e. g. , a similar or complementary equipment for back-to back operation or an external clock source. This term may be used interchangeably with EUT stimulus equipment.

#-Evaluated Products

1. A documented inventory of commercially available trusted computer hardware and software that has been evaluated against the Department of Defense Trusted Computer System Evaluation Criteria by the National Computer Security Center.
2. A documented inventory of equipments, hardware, software, and/or firmware that has been evaluated against the evaluation criteria found in *DOD* 5200. 28. STD. (NISTIR 4658).

Evaluated Products List

1. (EPL) A documented inventory of commercially available trusted computer hardware and software that has been evaluated against the Department of Defense Trusted Computer System Evaluation Criteria by the National Computer Security Center. (AFR 205-16; DODD 5215. 1)
2. A documented inventory of equipments, hardware, software, and/or firmware that has been evaluated against the evaluation criteria found in DOD 5200. 28-STD. (DODD 5200. 28)
3. A list of equipments, hardware, software, and or firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DoD TCSEC by the NCSC. The EPL is included in the National Security Agency In formation Systems Security Products and Services Catalogue, which is available through the Government Printing Office. (NCSC-TG-004-88)

Evaluation

The evaluator's report to the Designated Approving Authority describing the investigative and test procedures used in the analysis of the ADP system security features with a description and results of tests used to support or refute specific system weaknesses that would permit the acquisition of identifiable classified material from secure or protecteddata files. (DODD 5200. 28M;)

#-Evaluation Techniques (Evaluation)

The technical analysis of a component's, product's, subsystem's, or system's security that establishes whether or not the component, product, subsystem, or system meets a specific set of requirements.

Evaluator

Personnel specifically designated to participate in the test team review, analysis, testing, and evaluation of the security features of an automated system. (*AR* 380-380;)

Event

1. An abstract entity that represents an impact on one or more assets by one or more agents. Every event has a distinguished component a timestamp. (ET;)
2. A realization of a threat; that is, one possible instance or occurrence of the threat. (RM;)
3. An abstract entity that represents an impact on one or more assets. Event properties include impact area (the assets affected), perpetrator (external entities that cause the impact), and event cost. (MK;)

Event Cost

1. The financial loss incurred by the owner of an asset resulting from an event. (RM;)
2. An Evaluation, possibly in more than one unit, or the “loss” to the organisation if the event occurs. (MK;)

Event Value

The result of an evaluation by an agent of the costs and benefits of an event. (RM;)

Event-Reporting Systems

#-Evidence Acceptability

This KSA has no definition.

#-Evidence Collection And Preservation

This KSA has no definition.

*-Evil

adj. As used by hackers, implies that some system, program, person, or institution is sufficiently maldesigned as to be not worth the bother of dealing with. Unlike the adjectives in the cretinous/losing/brain-damaged series, `evil' does not imply incompetence or bad design, but rather a set of goals or design criteria fatally incompatible with the speaker's. This usage is more an esthetic and engineering judgment than a moral one in the mainstream sense. “We thought about adding a Blue Glue interface but decided it was too evil to deal with. ” “TECO is neat, but it can be pretty evil if you're prone to typos. ” Often pronounced with the first syllable lengthened, as /eeee'vil/. Compare evil and rude.

*-Evil And Rude

adj. Both evil and rude, but with the additional connotation that the rudeness was due to malice rather than incompetence. Thus, for exampleMicrosoft's Windows NT is evil because it's a competent implementation of a bad design; it's rude because it's gratuitously incompatible with UNIX in places where compatibility would have been as easy and effective to do; but it's evil and rude because the incompatibilities are apparently there not to fix design bugs in UNIX but rather to lock hapless customers and developers

into the Microsoft way. Hackish evil and rude is close to the mainstream sense of `evil'.

*-Exa

/ek's*/ pref. [SI] See quantifiers.

*-Examining The Entrails

n. The process of grovelling through a core dump or hex image in an attempt to discover the bug that brought a program or system down. The reference is to divination from the entrails of a sacrified animal. Compare runes, incantation, black art, desk check.

*-EXCH

/eks'ch*/ or /eksch/ vt. To exchange two things, each for the other; to swap places. If you point to two people sitting down and say “Exch!”, you are asking them to trade places. EXCH, meaning EXCHange, was originally the name of a PDP-10 instruction that exchanged the contents of a register and a memory location. Many newer hackers are probably thinking instead of the PostScript exchange operator (which is usually written in lowercase).

Exclusion Area

A security area for the protection of classified matter where mere access to the area would result in access to classified matter. See DOE 5632. 4 for further information. (DOE 5637. 1)

*-EXE

/eks'ee/ or /eek'see/ or /E-X-E/ n. An executable binary file. Some operating systems (notably MS-DOS, VMS, and TWENEX) use the extension . EXE to mark such files. This usage is also occasionally found among UNIX programmers even though UNIX executables don't have any required suffix.

*-Exec

/eg-zek'/ or /eks'ek/ vt. , n.

1. [UNIX from `execute'] Synonym for chain, derives from the `exec(2)' call.
2. [from `executive'] obs. The command interpreter for an OS (see shell); term esp. used around mainframes, and prob. derived from UNIVAC's archaic EXEC 2 and EXEC 8 operating systems.
3. At IBM and VM/CMS shops, the equivalent of a shell command file (among VM/CMS users). The mainstream `exec' as an abbreviation for (human) executive is *not* used. To a hacker, an `exec' is a always a program, never a person. exercise, left as an [from technical books] Used to complete a proof when one doesn't mind a handwave, or to avoid one entirely. The complete phrase is “The proof [or `the rest'] is left as an exercise for the reader. ” This comment *has* occasionally been attached to unsolved research problems by authors possessed of either an evil sense of humor or a vast faith in the capabilities of their audiences.

Execute Access Mode

Executing Ring

Execution Of The Budget

Executive Order No. 12046 Of March 27, 1978

Executive Order No. 12472 Or April 3, 1984

Executive State

One of several states in which a system may operate and the only one in which certain privileged instructions may be executed. Such instructions cannot be executed when the system is operating in other (e. g. , user) states. Synonymous with supervisor state.

Exemption

Exercise Key

Key intended to safeguard transmissions associated with exercises.

Exhaustive Attack

1. [An] exhaustive attack consists of discovering secret data by trying all possibilities and checking for correctness. For a four digit password, one might start with 0000 and move on to 0001, 0002 till 9999. (JL;).
2. See SCANNING.

Expected Lifetime

A parameter indicating the length of time an asset is operative or has value to its owners. (RM;)

Expenditure

#-Expert Security/Audit Tools

This KSA has no definition.

#-Expert Systems

This KSA has no definition.

Expired Password

A password that must be changed by the user before login may be completed. (CSC-STD-002-85;)

Exploitable Channel

1. Any channel that is usable or detectable by subjects external to the Trusted Computing Base.
2. Covert channel that is intended to violate the security policy governing an AIS and is useable or detectable by subjects external to the trusted comput-

ing base. (CSC-STD-001-83;) See Covert Channel.

Exploitation

The process of obtaining information from any source and taking advantage of collected information. *The process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes NOTE: See Source (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Exploratory Development

Assembly of preliminary circuits or parts model in line with commercial practice to investigate, test, or evaluate the soundness of a concept, device, circuit, equipment, or system in a “breadboard” or rough experimental form, without regard to eventual overall physical form or layout.

Exploratory Development Model

Assembly of preliminary circuits or parts in line with commercial practice to investigate, test, or evaluate the soundness of a concept, device, circuit, equipment, or system in a “breadboard” or rough experimental form, without regard to eventual overall physical form or layout.

#-Export Controls

Mechanisms, eg, license and reporting requirements, by which the government regulates the flow of goods, services, and technology to non-U. S. destinations including the domestic transfer of such items to foreign nationals.

Exposure

1. A specific instance of the condition of being unduly exposed to losses resulting from the occurrence of one or more threat events. (WB;)
2. A numerical evaluation of the degree of vulnerability of an asset to an event or threat. Computed in terms of statistically expected cost per time unit. (RM;)

External Label

Visible marking on the outside of media, or the cover of media, that reflects the classification and sensitivity of the information resident within media. See Internal Label and Label.

*-External Memory

n. A memo pad or written notes. “Hold on while I write that to external memory”. The analogy is with store or DRAM versus nonvolatile disk storage on computers.

External Protected Distribution System

That portion of a protected distribution system extending beyond a controlled access area (CAA). (NACSIM 5203)

External Security Audit

A security audit conducted by an organization independent of the one being audited. (*FIPS PUB* 39;)

Extra Bit

Synonym added bit.

Extra Block

Synonym added block.

Extraction Resistance

Capability of a crypto-equipment or a secure telecommunications system or equipment to resist efforts to extract key.

*-Eyeball Search

n. ,v. To look for something in a mass of code or data with one's own native optical sensors, as opposed to using some sort of pattern matching software like grep or any other automated search tool. Also called a vgrep; compare vdiff, desk check.

F

*-Face Time

n. Time spent interacting with somebody face-to-face (as opposed to via electronic links). “Oh, yeah, I spent some face time with him at the last Usenix. ”

Facilities

Buildings, structures, or other real property improvements separately identified on real property records and including items of real property Facilities are categorized as technical support real property, critical subsystems, non-technical support real property (NSRP), and industrial facilities (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

#-Facilities Planning

This KSA has no definition.

Facility

1. A building or other structure, either fixed or transportable in nature, with its utilities, ground networks, and electrical supporting structures. Note: All wiring and cabling required to be provided are considered to be part of the facility. Any electrical and electronic equipment required to be supplied and installed are also part of the facility. (~)
2. A service provided by a telecommunication network or equipment for the benefit of the users or the operating administration.
3. A general term for the communication transmission pathway and associated equipment.
4. In a data protocol context, an additional item of information or a constraint encoded within the protocol data unit to provide the requested control.
5. A real property entity consisting of one or more of the following: a building, a structure, a utility sys-

tem, pavement, and underlying land. (JCS1-DoD) See also technical control facility.

#-Facility Management

This KSA has no definition.

Facsimile

1. A form of telegraphy for the transmission of fixed images, with or without half-tones, with a view to their reproduction in a permanent form. In this definition the term telegraphy has the same general meaning as defined in the Convention. (RR)
2. A system of telecommunication for the transmission of fixed images with a view to their reception in a permanent form. (JCS1-DoD) (JCS1-NATO)
3. The process, or the result of the process, by which fixed graphic material, including pictures or images, is scanned and the information converted into electrical signals that may be transmitted over a telecommunication system and used to record a copy of the original. (~)
4. Note 1: Wirephoto and telephoto are facsimile via wire circuits; radiophoto is facsimile via radio. Note 2: Current facsimile systems are designated and defined as follows: (a) group 1 facsimile: A mode of black/white facsimile operation as defined in CCITT Recommendation T. 2, which uses double sideband modulation without any special measures to compress the bandwidth. Note 1: A 216 ´ 279 mm document (8½ ´ 11 inches) may be transmitted in approximately 6 minutes via a telephone-type circuit. Additional modes in this group may be designed to operate at a lower resolution suitable for the transmission of documents 216 ´ 279 mm in a time between 3 and 6 minutes. Note 2: The CCITT frequencies used are 1300 Hz for white and 2300 Hz for black. The North American standard is 1500 Hz for white and either 2300 or 2400 Hz for black. (b) group 2 facsimile: A mode of black/white facsimile operation as defined in CCITT Recommendation T. 3, which accomplishes bandwidth compression by using encoding and vestigial sideband, but excludes processing of the document signal to reduce redundancy. Note: A 216 ´ 279 mm document (8½ ´ 11 inches) may be transmitted in approximately 3 minutes using a 2100-Hz AM/PM/VSB, over a telephone-type circuit. (c) group 3 facsimile: A mode of black/white facsimile operation as defined in CCITT Recommendation T. 4, which incorporates means for reducing the redundant information in the document signal using a one-dimensional run-length coding scheme prior to the modulation process.
5. Note 1: A 216 ´ 279 mm document (8½ ´ 11 inches) may be transmitted in approximately 1 minute or less over a telephone-type circuit with twice the group 2 horizontal resolution; vertical resolution may also be doubled.
6. Note 2: Group 3 machines have integral digital modems. Note 3: An optional two-dimensional bandwidth compression scheme is also defined within the group 3 facsimile specification. (d) group 4 facsimile: A mode of black/white facsimile operation as defined in CCITT Recommendations T. 5 and T. 6. Note: Uses bandwidth compression techniques to transmit an essentially error-free 216 ´ 279 mm (8½ ´ 11 inches) document at a nominal resolution of 8 lines/mm in less than 1 minute over a public data network voice-grade circuit.

Facsimile Converter

1. [Receiving,] A facsimile device that changes the type of modulation from frequency shift to amplitude. (~)
2. [Transmitting,] A facsimile device that changes the type of modulation from amplitude to frequency shift. (~)

Facsimile Recorder

That part of the facsimile receiver that performs the final conversion of the facsimile picture signal to an image of the original subject copy on the record medium. (~) See also facsimile.

Facsimile Transmission

See black facsimile transmission, facsimile, white facsimile transmission.

*-Factor

n. See coefficient of X.

Fail

See failure, graceful degradation.

Fail Safe

Automatic termination and protection of programs and/or processing systems when a hardware or software failure is detected in an automated information system. (*NCSC-WA*-001-85;; *AR* 380-380;; *FIPS PUB* 39;)

Fail Soft

The selective termination of affected non essential processing when a hardware or software failure is detected in an automated system. (*AR* 380-380;; *NCSC-WA*-001-85;; *FIPS PUB* 39;)

Fail-Safe Operation

Any mode of operation designed to ensure that a failure of equipment, process, or system does not propagate beyond the immediate environs of the failing entity. (~) See also continuous operation, endurability, graceful degradation.

Failure

The temporary or permanent termination of the ability of an entity to perform its required function. (~) Note: Catastrophic failures are both sudden and complete. Degradation failures are both gradual and partial.

Failure Access

An unauthorized and usually inadvertent access to data resulting from a hardware or software failure in the automated system. (*AR* 380-380;; *FIPS PUB* 39;; *NCSC-WA*-001-85;)

Failure Control

The methodology used to detect and provide fail-safe or fail-soft recovery from hardware and software failures in an automated system. (*AR* 380-380;; *FIPS PUB* 39;; *NCSC-WA*-001-85;)

*-Fall Over

vi. [IBM] Yet another synonym for crash or lose. `Fall over hard' equates to crash and burn.

*-Fall Through

1. v. (n. `fallthrough', var. `fall-through') To exit a loop by exhaustion, i. e. , by having fulfilled its exit condition rather than via a break or exception condition that exits from the middle of it. This usage appears to be *really* old, dating from the 1940s and 1950s.
2. To fail a test that would have passed control to a subroutine or some other distant portion of code.
3. In C, `fall-through' occurs when the flow of execution in a switch statement reaches a `case' label other than by jumping there from the switch header, passing a point where one would normally expect to find a `break'. A trivial example switch (color) case GREEN do_green(); break; case PINK do_pink(); /* FALL THROUGH */ case RED do_red(); break; default do_blue(); break; The variant spelling `/* FALL THRU */' is also common. The effect of the above code is to `do_green()' when color is `GREEN', `do_red()' when color is `RED', `do_blue()' on any other color other than `PINK', and (and this is the important part) `do_pink()' *and then* `do_red()' when color is `PINK'. Fall-through is considered harmful by some, though there are contexts (such as the coding of state machines) in which it is natural; it is generally considered good practice to include a comment highlighting the fall-through where one would normally expect a break. See also Duff's device.

*-Fan

n. Without qualification, indicates a fan of science fiction, especially one who goes to cons and tends to hang out with other fans. Many hackers are fans, so this term has been imported from fannish slang; however, unlike much fannish slang it is recognized by most non-fannish hackers. Among SF fans the plural is correctly `fen', but this usage is not automatic to hackers. “Laura reads the stuff occasionally but isn't really a fan. ”

*-Fandango On Core

n. [UNIX/C hackers, from the Mexican dance] In C, a wild pointer that runs out of bounds, causing a core dump, or corrupts the `malloc (3)' arena in such a way as to cause mysterious failures later on, is sometimes said to have `done a fandango on core'. On low-end personal machines without an MMU, this can corrupt the OS itself, causing massive lossage. Other frenetic dances such as the rhumba, cha-cha, or watusi, may be substituted. See aliasing bug, precedence lossage, smash the stack, memory leak, memory smash, core.

*-FAQ

1. /F-A-Q/ or /fak/ n. [Usenet] A Frequently Asked Question.
2. A compendium of accumulated lore, posted periodically to high-volume newsgroups in an attempt to forestall such questions. Some people prefer the term `FAQ list' or `FAQL' /fa'kl/, reserving `FAQ' for sense 1. This lexicon itself serves as a good example of a collection of one kind of lore, although it is far too big for a regular FAQ posting. Examples “What is the proper type of NULL?” and “What's that funny name for the `#' character?” are both Frequently Asked Questions. Several FAQs refer readers to this file.

*-FAQ List

/F-A-Q list/ or /fak list/ n. [Usenet] Syn FAQ, sense 2.

*-Faradize

/far'*-di:z/ v. [US Geological Survey] To start any hyper-addictive process or trend, or to continue adding current to such a trend. Telling one user about a new octo-tetris game you compiled would be a faradizing act -- in two weeks you might find your entire department playing the faradic game.

*-Farkled

/far'kld/ adj. [DeVry Institute of Technology, Atlanta] Syn. hosed. Poss. owes something to Yiddish `farblondjet' and/or the `Farkle Family' skits on “Rowan and Martin's Laugh-In”, a popular comedy show of the early 1970s.

*-Farming

n. [Adelaide University, Australia] What the heads of a disk drive are said to do when they plow little furrows in the magnetic media. Associated with a crash. Typically used as follows “Oh no, the machine has just crashed; I hope the hard drive hasn't gone farming again. ”

*-Fat Electrons

n. Old-time hacker David Cargill's theory on the causation of computer glitches. Your typical electric utility draws its line current out of the big generators with a pair of coil taps located near the top of the dynamo. When the normal tap brushes get dirty, they take them off line to clean them up, and use special auxiliary taps on the *bottom* of the coil. Now, this is a problem, because when they do that they get not

ordinary or `thin' electrons, but the fat'n'sloppy electrons that are heavier and so settle to the bottom of the generator. These flow down ordinary wires just fine, but when they have to turn a sharp corner (as in an integrated-circuit via), they're apt to get stuck. This is what causes computer glitches. [Fascinating. Obviously, fat electrons must gain mass by bogon absorption -- ESR] Compare bogon, magic smoke.

Fault

1. A condition that causes a device or system component to fail to perform in a required manner (such as, a short circuit, broken wire or intermittent connection). (*AR* 380-380;; *NCSC-WA*-001-85;)
2. Synonymous with Loophole.

#-Fault Tolerance

1. The ability of a system or component to continue normal operation despite the presence or hardware or software faults.
2. The number of faults a system or component can withstand before normal operation is impaired. (Source - Marciniak, vol 1).

*-Faulty

adj. Non-functional; buggy. Same denotation as bletcherous, losing, q. v. , but the connotation is much milder.

FAX

See facsimile.

#-Fax Security

The methods used to protect the transmission of images over communications links from the threats of unauthorized disclosure and misrouting. (Source panel of experts).

*-Fd Leak

/F-D leek/ n. A kind of programming bug analogous to a core leak, in which a program fails to close file descriptors (`fd's) after file operations are completed, and thus eventually runs out of them. See leak.

*-Fear And Loathing

n. [from Hunter S. Thompson] A state inspired by the prospect of dealing with certain real-world systems and standards that are totally brain-damaged but ubiquitous -- Intel 8086s, or COBOL, or EBCDIC, or any IBM machine except the Rios (a. k. a. the RS/6000). “Ack! They want PCs to be able to talk to the AI machine. Fear and loathing time!”

*-Feature

1. n. A good property or behavior (as of a program). Whether it was intended or not is immaterial.
2. An intended property or behavior (as of a program). Whether it is good or not is immaterial (but if bad, it is also a misfeature).
3. A surprising property or behavior; in particular, one that is purposely inconsistent because it works better that way -- such an inconsistency is therefore a feature and not a bug. This kind of feature is sometimes called a miswart; see that entry for a classic example.
4. A property or behavior that is gratuitous or unnecessary, though perhaps also impressive or cute. For example, one feature of Common LISP's `format' function is the ability to print numbers in two different Roman-numeral formats (see bells, whistles, and gongs).
5. A property or behavior that was put in to help someone else but that happens to be in your way.
6. A bug that has been documented. To call something a feature sometimes means the author of the program did not consider the particular case, and that the program responded in a way that was unexpected but not strictly incorrect. A standard joke is that a bug can be turned into a feature simply by documenting it (then theoretically no one can complain about it because it's in the manual), or even by simply declaring it to be good. “That's not a bug, that's a feature!” is a common catchphrase. See also feetch feetch, creeping featurism, wart, green lightning. The relationship among bugs, features, misfeatures, warts, and miswarts might be clarified by the following hypothetical exchange between two hackers on an airliner A “This seat doesn't recline. ” B “That's not a bug, that's a feature. There is an emergency exit door built around the window behind you, and the route has to be kept clear. ” A “Oh. Then it's a misfeature; they should have increased the spacing between rows here. ” B “Yes. But if they'd increased spacing in only one section it would have been a wart -- they would've had to make nonstandard-length ceiling panels to fit over the displaced seats. ” A “A miswart, actually. If they increased spacing throughout they'd lose several rows and a chunk out of the profit margin. So unequal spacing would actually be the Right Thing. ” B “Indeed. ” `Undocumented feature' is a common, allegedly humorous euphemism for a bug.

*-Feature Creature

n. [poss. fr. slang `creature feature' for a horror movie]

1. One who loves to add features to designs or programs, perhaps at the expense of coherence, concision, or taste.
2. Alternately, a mythical being that induces otherwise rational programmers to perpetrate such crocks. See also feeping creaturism, creeping featurism.

*-Feature Key

n. The Macintosh key with the cloverleaf graphic on its keytop; sometimes referred to as `flower', `pretzel', `clover', `propeller', `beanie' (an apparent reference to the major feature of a propeller beanie), splat, or the `command key'. The Mac's equivalent of an alt key (and so labeled on on some Mac II keyboards). The proliferation of terms for this creature may illustrate one subtle peril of iconic interfaces. Many people have been mystified by the cloverleaf-like symbol that appears on the feature key.
Its oldest name is `cross of St. Hannes', but it occurs in pre-Christian Viking art as a decorative motif. Throughout Scandinavia today the road agencies use it to mark sites of historical interest. Apple picked up the symbol from an early Mac developer who happened to be Swedish. Apple documentation gives the translation “interesting feature”! There is some dispute as to the proper (Swedish) name of this symbol. It technically stands for the word `sev”ardhet' (interesting feature) many of these are old churches. Some Swedes report as an idiom for it the word `kyrka', cognate to English `church' and Scots-dialect `kirk' but pronounced /shir'k*/ in modern Swedish. Others say this is nonsense. Another idiom reported for the sign is `runsten' /roon'stn/, derived from the fact that many of the interesting sites are Viking rune-stones.

*-Feature Shock

n. [from Alvin Toffler's book title “Future Shock”] A user's (or programmer's!) confusion when confronted with a package that has too many features and poor introductory material.

*-Featurectomy

/fee`ch*r-ek't*-mee/ n. The act of removing a feature from a program. Featurectomies come in two flavors, the `righteous' and the `reluctant'. Righteous featurectomies are performed because the remover believes the program would be more elegant without the feature, or there is already an equivalent and better way to achieve the same end. (Doing so is not quite the same thing as removing a misfeature.) Reluctant featurectomies are performed to satisfy some external constraint such as code size or execution speed.

Features

See SECURITY FEATURES.

FEC

Federal

Federal Agency

Federal Computer Criminals

Federal Computer System

A computer system operated by a federal agency or by a contractor of a federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a federal function;, and includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. (PL 100-235)

Federal Data Processing Centers

*-Feep

1. /feep/ n. The soft electronic `bell' sound of a display terminal (except for a VT-52); a beep (in fact, the microcomputer world seems to prefer beep).
2. vi. To cause the display to make a feep sound. ASR-33s (the original TTYs) do not feep; they have mechanical bells that ring. Alternate forms beep, `bleep', or just about anything suitably onomatopoeic. (Jeff MacNelly, in his comic strip “Shoe”, uses the word `eep' for sounds made by computer terminals and video games; this is perhaps the closest written approximation yet.) The term `breedle' was sometimes heard at SAIL, where the terminal bleepers are not particularly soft (they sound more like the musical equivalent of a raspberry or Bronx cheer; for a close approximation, imagine the sound of a Star Trek communicator's beep lasting for five seconds). The `feeper' on a VT-52 has been compared to the sound of a '52 Chevy stripping its gears. See also ding.

*-Feeper

/fee'pr/ n. The device in a terminal or workstation (usually a loudspeaker of some kind) that makes the feep sound.

*-Feeping Creature

n. [from feeping creaturism] An unnecessary feature; a bit of chrome that, in the speaker's judgment, is the camel's nose for a whole horde of new features.

*-Feeping Creaturism

/fee'ping kree`ch*r-izm/ n. A deliberate spoonerism for creeping featurism, meant to imply that the system or program in question has become a misshapen creature of hacks. This term isn't really well defined, but it sounds so neat that most hackers have said or heard it. It is probably reinforced by an image of terminals prowling about in the dark making their customary noises.

*-Fence

1. n. A sequence of one or more distinguished (out-of-band) characters (or other data items), used to delimit a piece of data intended to be treated as a

unit (the computer-science literature calls this a `sentinel'). The NUL (ASCII 0000000) character that terminates strings in C is a fence. Hex FF is also (though slightly less frequently) used this way. See zigamorph.

2. An extra data value inserted in an array or other data structure in order to allow some normal test on the array's contents also to function as a termination test. For example, a highly optimized routine for finding a value in an array might artificially place a copy of the value to be searched for after the last slot of the array, thus allowing the main search loop to search for the value without having to check at each pass whether the end of the array had been reached.
3. [among users of optimizing compilers] Any technique, usually exploiting knowledge about the compiler, that blocks certain optimizations. Used when explicit mechanisms are not available or are overkill. Typically a hack “I call a dummy procedure there to force a flush of the optimizer's register-coloring info” can be expressed by the shorter “That's a fence procedure”.

*-Fencepost Error

1. n. A problem with the discrete equivalent of a boundary condition, often exhibited in programs by iterative loops. From the following problem “If you build a fence 100 feet long with posts 10 feet apart, how many posts do you need?” (Either 9 or 11 is a better answer than the obvious 10.) For example, suppose you have a long list or array of items, and want to process items m through n; how many items are there? The obvious answer is n - m, but that is off by one; the right answer is n - m + 1. A program that used the `obvious' formula would have a fencepost error in it. See also zeroth and off-by-one error, and note that not all off-by-one errors are fencepost errors. The game of Musical Chairs involves a catastrophic off-by-one error where N people try to sit in N - 1 chairs, but it's not a fencepost error. Fencepost errors come from counting things rather than the spaces between them, or vice versa, or by neglecting to consider whether one should count one or both ends of a row.
2. [rare] An error induced by unexpected regularities in input values, which can (for instance) completely thwart a theoretically efficient binary tree or hash table implementation. (The error here involves the difference between expected and worst case behaviors of an algorithm.)

*-Fepped Out

/fept owt/ adj. The Symbolics 3600 LISP Machine has a Front-End Processor called a `FEP' (compare sense 2 of box). When the main processor gets wedged, the FEP takes control of the keyboard and screen. Such a machine is said to have `fepped out' or `dropped into the fep'.

FER

Fetch Protection

A system-provided restriction to prevent a program from accessing data in another user's segment of storage. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

Fiber Distributed Data Interface

An optical-fiber token-ring network (defined by four ANSI standards) with highly reliable data transfer, active link monitoring, station management, large-bandwidth capabilities (100 Mbps transmission rate), and survivability features. Note 1: The four standards are: ANSI X3T9. 5 (Physical Media Dependent [PMD] specifications), ANSI X3T9. 5 (addressing the PHY [physical] specifications), ANSI X3. 139 (addressing the Media Access Control [MAC] parameters), and ANSI X3T9. 5 (addressing Station Management [SMT] parameters). Note 2: FDDI-2, a second-generation FDDI network is under development.

Fiber Optics

The branch of optical technology concerned with the transmission of radiant power through fibers made of transparent materials such as glass (including fused silica) or plastic. (~) Note 1: Telecommunications applications of fiber optics employ flexible low-loss fibers, using a single fiber per information channel(s). Note 2: Various industrial and medical applications employ (typically high-loss) flexible fiber bundles in which individual fibers are spatially aligned, permitting optical relay of an image, such as in an endoscope. Note 3: Some specialized industrial applications employ rigid (fused) aligned fiber bundles for image transfer, such as in the fiber optics faceplate used on some high-speed oscilloscopes.

Fiber Pigtail

A short length of optical fiber, permanently fixed to a component, used to couple power between the component and the transmission fiber. (~) See also fiber optics, optical fiber.

*-FidoNet

n. A worldwide hobbyist network of personal computers which exchanges mail, discussion groups, and files. Founded in 1984 and originally consisting only of IBM PCs and compatibles, FidoNet now includes such diverse machines as Apple][s, Ataris, Amigas, and UNIX systems. Though it is much younger than Usenet, FidoNet is already (in early 1991) a significant fraction of Usenet's size at some 8000 systems.

Field

1. The volume of influence of a physical phenomenon, expressed vectorially.
2. On a data medium or in storage, a specified area used for a particular class of data, e. g. , a group of character positions used to enter or display wage rates on a screen. (FP) (ISO)
3. Defined logical data that are part of a record. (FP)
4. The elementary unit of a record that may contain a data item, a data aggregate, a pointer, or a link. (FP) See also address field, information field.

*-Field Circus

n. [a derogatory pun on `field service'] The field service organization of any hardware manufacturer, but especially DEC. There is an entire genre of jokes about DEC field circus engineers Q How can you recognize a DEC field circus engineer with a flat tire? A He's changing one tire at a time to see which one is flat. Q How can you recognize a DEC field circus engineer who is out of gas? A He's changing one tire at a time to see which one is flat. [See Easter egging for additional insight on these jokes.] There is also the `Field Circus Cheer' (from the plan file for DEC on MIT-AI) Maynard! Maynard! Don't mess with us! We're mean and we're tough! If you get us confused (DEC's service HQ is located in Maynard, Massachusetts.)

*-Field Servoid

[play on `android'] /fee'ld ser'voyd/ n. Representative of a field service organization (see field circus). This has many of the implications of droid.

Fielded Equipment

COMSEC end-item shipped to the user subsequent to first article testing on the initial production contract.

FIFO

Abbreviation for first-in first-out.

File

1. The largest unit of storage structure that consists of a named collection of all occurrences in a database of records of a particular record type. (FP)
2. A set of related records treated as a unit, for example, in stock control, a file could consist of a set of invoices. (FP) (ISO)

*-File Attach

1. [FidoNet] n. A file sent along with a mail message from one BBS to another.
2. vt. Sending someone a file by using the File Attach option in a BBS mailer.

File Authentication Code

In a manner similar to that used for the computation of a Message Authentication Code, certain authentication techniques can be used to provide assurance that data held ina file has not been altered or deleted. This term is also applied to databases. (WB;)

File Management System

File Protection

The aggregate of all processes and procedures established in an automated system and designed to inhibit unauthorized access, contamination, or elimination of a file. (*AR* 380-380;; *NCSC-WA*-001-85;; *FIPS PUB* 39;)

*-File Request

1. [FidoNet] n. The FidoNet equivalent of FTP, in which one BBS system automatically dials another and snarfs one or more files. Often abbreviated `FReq'; files are often announced as being “available for FReq” in the same way that files are announced as being “available for/by anonymous FTP” on the Internet.
2. vt. The act of getting a copy of a file by using the File Request option of the BBS mailer.

File Security

The means by which access to computer files is limited to authorized users only. (*NCSC-WA*-001-85;)

*-File Signature

n. A magic number, sense 3.

File Transfer Protocol

File Transfer, Access, And Management

An application's service and protocol based on the concept of virtual file store. This service/protocol allows remote access to various levels in a file structure and provides a comprehensive set of file management capabilities.

Fill

See bit stuffing.

Fill Device

COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment.

*-Film At 11

1. [MIT in parody of TV newscasters] Used in conversation to announce ordinary events, with a sarcastic implication that these events are earth-shattering. “ITS crashes; film at 11. ” “Bug found in scheduler; film at 11. ”
2. Also widely used outside MIT to indicate that additional information will be available at some future time, *without* the implication of anything particularly ordinary about the referenced event. For example, “The mail file server died this morning; we found garbage all over the root directory. Film at 11. ” would indicate that a major failure had occurred but that the people working on it

have no additional information about it as yet; use of the phrase in this way suggests gently that the problem is liable to be fixed more quickly if the people doing the fixing can spend time doing the fixing rather than responding to questions, the answers to which will appear on the normal “11:00 news”, if people will just be patient.

Filter

1. A device for use on power, signal, telephone or other wirelines, specifically designed to pass only selected frequencies and to attenuate substantially all other frequencies. There are two basic types of filters: a) active filters - Those which are active components and require the application of power for the utilization of their filtering properties. b) passive filters - Those which use passive components having properties of inductance, capacitance or resistance and which do not require the application of power for the utilization of their filtering properties. (NACSIM 5203)
2. See Front-End Security Filter and Guard.
3. n. [orig. UNIX, now also in MS-DOS] A program that processes an input data stream into an output data stream in some well-defined way, and does no I/O to anywhere else except possibly on error conditions; one designed to be used as a stage in a “pipeline” (see plumbing). Compare sponge.

#-Filtered Power

Power which has been processed by a filter device. The filter device is designed to pass only specifically selected frequencies and to attenuate substantially all other frequencies. (Source: Panel of Experts, July 1994).

*-Finagle's Law

n. The generalized or `folk' version of Murphy's Law, fully named “Finagle's Law of Dynamic Negatives” and usually rendered “Anything that can go wrong, will”. One variant favored among hackers is “The perversity of the Universe tends towards a maximum” (but see also Hanlon's Razor). The label `Finagle's Law' was popularized by SF author Larry Niven in several stories depicting a frontier culture of asteroid miners; this `Belter' culture professed a religion and/or running joke involving the worship of the dread god Finagle and his mad prophet Murphy.

Final Evaluation Report

Unknown

Financial Management Information

information on Federal spending, collections, assets, liabilities, equity, and related budgetary transactions and balances. This also includes data used to develop information for decisionmaking regarding unit costs, average pay rates, user charges, etc. (Key words - Day 3)

Financial Management System

the total of agency financial systems, both manual and automated, for planning, budget formulation and execution, program and administrative accounting, and audit; as well as all other systems for recording and classifying financial data and reporting financial management information, including purchasing, property, inventory, etc. (Key words - Day 3)

*-Fine

adj. [WPI] Good, but not good enough to be cuspy. The word `fine' is used elsewhere, of course, but without the implicit comparison to the higher level implied by cuspy.

*-Finger

1. [WAITS, via BSD UNIX] n. A program that displays information about a particular user or all users logged on the system, or a remote system. Typically shows full name, last login time, idle time, terminal line, and terminal location (where applicable). May also display a plan file left by the user (see also Hacking X for Y).
2. vt. To apply finger to a username.
3. vt. By extension, to check a human's current state by any means. “Foodp?” “T!” “OK, finger Lisa and see if she's idle. ”
4. Any picture (composed of ASCII characters) depicting `the finger'. Originally a humorous component of one's plan file to deter the curious fingerer (sense 2). , it has entered the arsenal of some flamers.

*-Finger Trouble

n. Mistyping, typos or generalized keyboard incompetence (this is surprisingly common among hackers, given the anount of time they spend at keyboards). “I keep putting colons at the end of statements instead of semicolons”, “Finger-trouble again, eh?”.

*-Finger-Pointing Syndrome

n. All-too-frequent result of bugs, esp. in new or experimental configurations. The hardware vendor points a finger at the software. The software vendor points a finger at the hardware. All the poor users get is the finger.

Fingerprint Signal

A unique emanation caused by the processing or transfer of an information unit (e. g. , character, byte, etc.) by the EUT. (Also called signature.)

*-Finn

v. [IRC] To pull rank on somebody based on the amount of time one has spent on IRC. The term derives from the fact that IRC was originally written in Finland in 1987. There may be some influence from the `Finn' character in William Gibson's seminal cyberpunk novel “Count Zero”, who at one point says to

another (much younger) character “I have a pair of shoes older than you are, so shut up!”

#-Fire Prevention And Protection

This KSA has no definition.

*-Firebottle

n. A large, primitive, power-hungry active electrical device, similar in function to a FET but constructed out of glass, metal, and vacuum. Characterized by high cost, low density, low reliability, high-temperature operation, and high power dissipation. Sometimes mistakenly called a `tube' in the U. S. or a `valve' in England; another hackish term is glassfet.

*-Firefighting

1. n. What sysadmins have to do to correct sudden operational problems. An opposite of hacking. “Been hacking your new newsreader?” “No, a power glitch hosed the network and I spent the whole afternoon fighting fires. ”
2. The act of throwing lots of manpower and late nights at a project, esp. to get it out before deadline. See also gang bang, Mongolian Hordes technique; however, the term `firefighting' connotes that the effort is going into chasing bugs rather than adding features.

FIREFLY

Key management protocol based on public key cryptography.

*-Firehose Syndrome

n. In mainstream folklore it is observed that trying to drink from a firehose can be a good way to rip your lips off. On computer networks, the absence or failure of flow control mechanisms can lead to situations in which the sending system sprays a massive flood of packets at an unfortunate receiving system, more than it can handle. Compare overrun, buffer overflow.

*-Firewall Code

1. n. The code you put in a system (say, a telephone switch) to make sure that the users can't do any damage. Since users always want to be able to do everything but never want to suffer for any mistakes, the construction of a firewall is a question not only of defensive coding but also of interface presentation, so that users don't even get curious about those corners of a system where they can burn themselves.
2. Any sanity check inserted to catch a can't happen error. Wise programmers often change code to fix a bug twice once to fix the bug, and once to insert a firewall which would have arrested the bug before it did quite as much damage.

*-Firewall Machine

n. A dedicated gateway machine with special security precautions on it, used to service outside network connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind it from crackers. The typical firewall is an inexpensive micro-based UNIX box kept clean of critical data, with a bunch of modems and public network ports on it but just one carefully watched connection back to the rest of the cluster. The special precautions may include threat monitoring, callback, and even a complete iron box keyable to particular incoming IDs or activity patterns. Syn. flytrap, Venus flytrap.

Firmware

1. Software that is permanently stored in a hardware device which allows reading of the software but not writing or modifying. The most common device for firmware is read only memory (ROM). (*AFR* 205-16;)
2. Computer programs recorded in a permanent or semi-permanent physical medium incorporated in the computer equipment. (*AR* 380-380;) See Read-Only Memory

#-Firmware Security

The security provided to an information processing system by firmware. Firmware is software that is permanently stored in a hardware device which allows reading but not writing or modifying. The most common device for firmware is read only memory. Alternately, firmware are computer programs recorded in a permanent or semipermanent physical medium incorporated in the information processing system. (Source: Panel of Experts, July 1994).

*-Firmy

/fer'mee/ Syn. stiffy (a 3. 5-inch floppy disk).

First-In First-Out

A queueing discipline in which arriving entities leave in the same order in which they arrived. (~) Note 1: Service is offered first to the entity that has been in the file the longest. Note 2: Commonly used in message switching. See also buffer, elastic buffer, last-in first-out, queue traffic, variable length buffer.

*-FISH Queue

n. [acronym, by analogy with FIFO (First In, First Out)] `First In, Still Here'. A joking way of pointing out that processing of a particular sequence of events or requests has stopped dead. Also `FISH mode' and `FISHnet'; the latter may be applied to any network that is running really slowly or exhibiting extreme flakiness.

FISINT

See foreign instrumentation signals intelligence.

*-FITNR

// [Thinking Machines, Inc.] Fixed In the Next Release. A written-only notation attached to bug reports. Often wishful thinking.

Five-Year Plan

*-Fix

n. ,v. What one does when a problem has been reported too many times to be ignored.

Fixed COMSEC Facility

COMSEC facility that is located in an immobile structure or aboard a ship.

Fixed Storage

Synonym read-only storage.

*-FIXME

imp. A standard tag often put in C comments near a piece of code that needs work. The point of doing so is that a `grep' or a similar pattern-matching tool can find all such places quickly. FIXMEnote this is common in GNU code. Compare XXX.

Flag

1. In data transmission, an indicator, such as a signal, symbol, character, or digit, used for identification. Note: An example is a word mark, a group mark, or letter that signals the occurrence of some condition or event such as the end of a word or block. See also block, character, word.
2. n. A variable or quantity that can take on one of two values; a bit, particularly one that is used to indicate one of two outcomes or is used to control which of two things is to be done. “This flag controls whether to clear the screen before printing the message. ” “The program status word contains several flag bits. ” Used of humans analogously to bit. See also hidden flag, mode bit.

*-Flag Day

n. A software change that is neither forward- nor backward-compatible, and which is costly to make and costly to reverse. “Can we install that without causing a flag day for all users?” This term has nothing to do with the use of the word flag to mean a variable that has two values. It came into use when a massive change was made to the Multics timesharing system to convert from the old ASCII code to the new one; this was scheduled for Flag Day (a U. S. holiday), June 14, 1966. See also backward combatability.

Flag Sequence

1. A sequence of bits used in a bit-oriented link protocol, e. g. , ADCCP, SDLC, and HDLC, to delimit the beginning and end of a frame. Note: An 8-bit sequence is generally used as the flag sequence.
2. In data transmission, the sequence of bits employed to delimit the beginning and end of a frame. Note: In one standard data transmission system, the 8-bit sequence 01111110 is used as the flag sequence. See also abort, binary digit, data transmission, frame.

*-Flaky

adj. (var sp. `flakey') Subject to frequent lossage. This use is of course related to the common slang use of the word to describe a person as eccentric, crazy, or just unreliable. A system that is flaky is working, sort of -- enough that you are tempted to try to use it -- but fails frequently enough that the odds in favor of finishing what you start are low. Commonwealth hackish prefers dodgy or wonky.

*-Flame

1. vi. To post an email message intended to insult and provoke.
2. vi. To speak incessantly and/or rabidly on some relatively uninteresting subject or with a patently ridiculous attitude.
3. vt. Either of senses 1 or 2, directed with hostility at a particular person or people.
4. n. An instance of flaming. When a discussion degenerates into useless controversy, one might tell the participants “Now you're just flaming” or “Stop all that flamage!” to try to get them to cool down (so to speak). The term may have been independently invented at several different places. It has been reported from MIT, Carleton College and RPI (among many other places) from as far back as 1969. It is possible that the hackish sense of `flame' is much older than that. The poet Chaucer was also what passed for a wizard hacker in his time; he wrote a treatise on the astrolabe, the most advanced computing device of the day. In Chaucer's “Troilus and Cressida”, Cressida laments her inability to grasp the proof of a particular mathematical theorem; her uncle Pandarus then observes that it's called “the fleminge of wrecches. ” This phrase seems to have been intended in context as “that which puts the wretches to flight” but was probably just as ambiguous in Middle English as “the flaming of wretches” would be today. One suspects that Chaucer would feel right at home on Usenet.

*-Flame On

1. vi. ,interj. To begin to flame. The punning reference to Marvel Comics's Human Torch is no longer widely recognized.
2. To continue to flame. See rave, burble.

*-Flame War

n. (var. `flamewar') An acrimonious dispute, especially when conducted on a public electronic forum such as Usenet.

*-Flamer

n. One who habitually flames. Said esp. of obnoxious Usenet personalities.

*-Flap

1. vt. To unload a DECtape (so it goes flap, flap, flap.). Old-time hackers at MIT tell of the days when the disk was device 0 and microtapes were 1, 2,. and attempting to flap device 0 would instead start a motor banging inside a cabinet near the disk.
2. By extension, to unload any magnetic tape. See also macrotape. Modern cartridge tapes no longer actually flap, but the usage has remained. (The term could well be re-applied to DEC's TK50 cartridge tape drive, a spectacularly misengineered contraption which makes a loud flapping sound, almost like an old reel-type lawnmower, in one of its many tape-eating failure modes.)

*-Flat

1. adj. Lacking any complex internal structure. “That bitty box has only a flat filesystem, not a hierarchical one. ” The verb form is flatten.
2. Said of a memory architecture (like that of the VAX or 680x0) that is one big linear address space (typically with each possible value of a processor register corresponding to a unique core address), as opposed to a `segmented' architecture (like that of the 80x86) in which addresses are composed from a base-register/offset pair (segmented designs are generally considered cretinous). Note that sense 1 (at least with respect to filesystems) is usually used pejoratively, while sense 2 is a Good Thing.

*-Flat-ASCII

adj. Said of a text file that contains only 7-bit ASCII characters and uses only ASCII-standard control characters (that is, has no embedded codes specific to a particular text formatter markup language, or output device, and no meta-characters). Syn. plain-ASCII. Compare flat-file.

*-Flat-File

adj. A flattened representation of some database or tree or network structure as a single file from which the structure could implicitly be rebuilt, esp. one in flat-ASCII form. See also sharchive.

*-Flatten

vt. To remove structural information, esp. to filter something with an implicit tree structure into a simple sequence of leaves; also tends to imply mapping to flat-ASCII. “This code flattens an expression with parentheses into an equivalent canonical form. ”

*-Flavor

1. n. Variety, type, kind. “DDT commands come in two flavors. ” “These lights come in two flavors, big red ones and small green ones. ” See vanilla.
2. The attribute that causes something to be flavorful. Usually used in the phrase “yields additional flavor”. “This convention yields additional flavor by allowing one to print text either right-side-up or upside-down. ” See vanilla. This usage was certainly reinforced by the terminology of quantum chromodynamics, in which quarks (the constituents of, e. g. , protons) come in six flavors (up, down, strange, charm, top, bottom) and three colors (red, blue, green) -- however, hackish use of `flavor' at MIT predated QCD.
3. The term for `class' (in the object-oriented sense) in the LISP Machine Flavors system. Though the Flavors design has been superseded (notably by the Common LISP CLOS facility), the term `flavor' is still used as a general synonym for `class' by some LISP hackers.

*-Flavorful

1. adj. Full of flavor (sense 2)
2. esthetically pleasing. See random and losing for antonyms. See also the entries for taste and elegant.

Flaw

1. An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed. (CSC-STD-001-83;; *NCSC-WA*-001-85;)
2. See loophole 3) See PSEUDO-FLAW.

Flaw Hypothesis

System analysis and penetration methodology technique in which the specification and documentation for an AIS are analyzed and then flaws in the system are hypothesized. NOTE: List of hypothesized flaws is prioritized on the basis of the estimated probability that a flaw exists and, assuming a flaw does exist, on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.

Flaw Hypothesis Methodology

A system analysis and penetration technique where specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually exists and, assuming a flaw does exist, on theease of exploiting it on the extent of control or compromise it would provide. The prioritized list is used to direct the actual testing of the system. (CSC-STD-001-83;; *NCSC-WA*-001-85;)

Flexible Disk

Synonym floppy disk.

*-Flippy

/flip'ee/ n. A single-sided floppy disk altered for double-sided use by addition of a second write-notch, so called because it must be flipped over for the second side to be accessible. No longer common.

*-Flood

v. [IRC] To dump large amounts of text onto an IRC channel. This is especially rude when the text is uninteresting and the other users are trying to carry on a serious conversation.

Floppy Disk

A flexible magnetic disk enclosed in a container. (FP) Synonym flexible disk.

Flow Control

1. A strategy for protecting the contents of information objects from being transferred to objects at improper security levels. It is more restrictive than access control. (MTR-8201;)
2. See Information Flow Control.

Flow Control Procedure

The procedure for controlling the rate of transfer of data among elements of a network, e. g. , between a DTE and a data switching exchange network, to prevent overload. See also data terminal equipment, data transmission, network.

Flow Diagram

Synonym flowchart.

Flowchart

A graphical representation in which symbols are used to represent such things as operations, data, flow direction, and equipment, for the definition, analysis, or solution of a problem. (FP) (ISO) Synonym flow diagram.

*-Flower Key

n. [Mac users] See feature key.

*-Flush

1. v. To delete something, usually superfluous, or to abort an operation. “All that nonsense has been flushed. ”
2. [UNIX/C] To force buffered I/O to disk, as with an `fflush(3)' call. This is *not* an abort or deletion as in sense 1, but a demand for early completion!
3. To leave at the end of a day's work (as opposed to leaving for a meal). “I'm going to flush now. ” “Time to flush. ”
4. To exclude someone from an activity, or to ignore a person. `Flush' was standard ITS terminology for aborting an output operation; one spoke of the text that would have been printed, but was not, as having been flushed. It is speculated that this term arose from a vivid image of flushing unwanted characters by hosing down the internal output buffer, washing the characters away before they could be printed. The UNIX/C usage, on the other hand, was propagated by the `fflush(3)' call in C's standard I/O library (though it is reported to have been in use among BLISS programmers at DEC and on Honeywell and IBM machines as far back as 1965). UNIX/C hackers find the ITS usage confusing, and vice versa.

Flux

1. Number of particles crossing a unit area per unit of time.
2. Magnetic field that exists between the poles of a magnet.

*-Flypage

/fli:'payj/ n. (alt. `fly page') A banner, sense 1.

*-Flyspeck 3

n. Standard name for any font that is so tiny as to be unreadable (by analogy with names like `Helvetica 10' for 10-point Helvetica). Legal boilerplate is usually printed in Flyspeck 3.

*-Flytrap

n. See firewall machine.

*-FOAF

// n. [Usenet] Acronym for `Friend Of A Friend'. The source of an unverified, possibly untrue story. This term was not originated by hackers (it is used in Jan Brunvand's books on urban folklore), but is much better recognized on Usenet and elsewhere than in mainstream English.

*-Fold Case

v. See smash case. This term tends to be used more by people who don't mind that their tools smash case. It also connotes that case is ignored but case distinctions in data processed by the tool in question aren't destroyed.

*-Followup

n. On Usenet, a posting generated in response to another posting (as opposed to a reply, which goes by email rather than being broadcast). Followups include the ID of the parent message in their headers; smart news-readers can use this information to present Usenet news in `conversation' sequence rather than order-of-arrival. See thread.

*-Fontology

n. [XEROX PARC] The body of knowledge dealing with the construction and use of new fonts (e. g. , for window systems and typesetting software). It has been said that fontology recapitulates file-ogeny. [Unfortunately, this reference to the embryological dictum that “Ontogeny recapitulates phylogeny” is not merely a joke. On the Macintosh, for example, System 7 has to go through contortions to compensate for an earlier design error that created a whole different set of abstractions for fonts parallel to `files' and `folders' -- ESR]

*-Foonly

1. n. The PDP-10 successor that was to have been built by the Super Foonly project at the Stanford

Artificial Intelligence Laboratory along with a new operating system. The intention was to leapfrog from the old DEC timesharing system SAIL was then running to a new generation, bypassing TENEX which at that time was the ARPANET standard. ARPA funding for both the Super Foonly and the new operating system was cut in 1974. Most of the design team went to DEC and contributed greatly to the design of the PDP-10 model KL10.

2. The name of the company formed by Dave Poole, one of the principal Super Foonly designers, and one of hackerdom's more colorful personalities. Many people remember the parrot which sat on Poole's shoulder and was a regular companion.
3. Any of the machines built by Poole's company. The first was the F-1 (a. k. a. Super Foonly), which was the computational engine used to create the graphics in the movie "TRON". The F-1 was the fastest PDP-10 ever built, but only one was ever made. The effort drained Foonly of its financial resources, and the company turned towards building smaller, slower, and much less expensive machines. Unfortunately, these ran not the popular TOPS-20 but a TENEX variant called Foonex; this seriously limited their market. Also, the machines shipped were actually wire-wrapped engineering prototypes requiring individual attention from more than usually competent site personnel, and thus had significant reliability problems. Poole's legendary temper and unwillingness to suffer fools gladly did not help matters. By the time of the Jupiter project cancellation in 1983, Foonly's proposal to build another F-1 was eclipsed by the Mars, and the company never quite recovered. See the Mars entry for the continuation and moral of this story.

*-Footprint

1. n. The floor or desk area taken up by a piece of hardware.
2. [IBM] The audit trail (if any) left by a crashed program (often in plural, `footprints'). See also toeprint.

*-For Free

adj. Said of a capability of a programming language or hardware equipment that is available by its design without needing cleverness to implement "In APL, we get the matrix operations for free. " "And owing to the way revisions are stored in this system, you get revision trees for free. " The term usually refers to a serendipitous feature of doing things a certain way (compare big win), but it may refer to an intentional but secondary feature.

For Official Use Only (FOUO) Data

1. Data that is unclassified official information of a sensitive, proprietary, or personal nature which must be protected against unauthorized public release. (*AFR* 205-16;; *AR* 380-380;)
2. Unclassified official information of a sensitive proprietary, or personal nature which must be protected against unauthorized public release as defined in *AFR* 12-30. (*AFR* 205-16; *AR* 380-380)

*-For The Rest Of Us

1. adj. [from the Mac slogan "The computer for the rest of us"] Used to describe a spiffy product whose affordability shames other comparable products, or (more often) used sarcastically to describe spiffy but very overpriced products.
2. Describes a program with a limited interface, deliberately limited capabilities, non-orthogonality, inability to compose primitives, or any other limitation designed to not `confuse' a naive user. This places an upper bound on how far that user can go before the program begins to get in the way of the task instead of helping accomplish it. Used in reference to Macintosh software which doesn't provide obvious capabilities because it is thought that the poor lusers might not be able to handle them. Becomes `the rest of *them*' when used in third-party reference; thus, "Yes, it is an attractive program, but it's designed for The Rest Of Them" means a program that superficially looks neat but has no depth beyond the surface flash. See also WIMP environment, Macintrash, point-and-drool interface, user-friendly.

*-For Values Of

[MIT] A common rhetorical maneuver at MIT is to use any of the canonical random numbers as placeholders for variables. "The max function takes 42 arguments, for arbitrary values of 42. " "There are 69 ways to leave your lover, for 69 = 50. " This is especially likely when the speaker has uttered a random number and realizes that it was not recognized as such, but even `non-random' numbers are occasionally used in this fashion. A related joke is that pi equals 3 -- for small values of pi and large values of 3. Historical note this usage probably derives from the programming language MAD (Michigan Algorithm Decoder), an Algol-like language that was the most common choice among mainstream (non-hacker) users at MIT in the mid-60s. It had a control structure FOR VALUES OF X = 3, 7, 99 DO . that would repeat the indicated instructions for each value in the list (unlike the usual FOR that only works for arithmetic sequences of values). MAD is long extinct, but similar for-constructs still flourish (e. g. , in UNIX's shell languages).

*-Fora

pl. n. Plural of forum.

*-Foreground

vt. [UNIX] To bring a task to the top of one's stack for immediate processing, and hackers often use it in this sense for non-computer tasks. “If your presentation is due next week, I guess I'd better foreground writing up the design document. ” Technically, on a time-sharing system, a task executing in foreground is one able to accept input from and return output to the user; oppose background. Nowadays this term is primarily associated with UNIX, but it appears first to have been used in this sense on OS/360. Normally, there is only one foreground task per terminal (or terminal window); having multiple processes simultaneously reading the keyboard is a good way to lose.

Foreign Government Information

1. Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or information produced by the United States pursuant to or as a result of joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence. (EO 12356)
2. Information that is: a. Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation either expressed or implied, that the information or the source of information, or both be held in confidence. b. Produced by the United States following or as a result of a joint arrangement with a foreign government or governments or an international organization of governments or any element thereof, requiring that the information or the arrangement or both be held in confidence. Information described in subparagraphs above and in the possession of the *DOD* is classified information in accordance with *DOD* 5200. 1 -R. (DODD 5230. 24; DOE 5635. 1 A)

Foreign Intelligence Service

The intelligence organization of a foreign country capable of executing all or part of the intelligence cycle.

*-Fork Bomb

n. [UNIX] A particular species of wabbit that can be written in one line of C (`main() for(;;)fork();') or shell (`$0 & $0 &') on any UNIX system, or occasionally created by an egregious coding bug. A fork bomb process `explodes' by recursively spawning copies of itself (using the UNIX system call `fork(2)'). Eventually it eats all the process table entries and effectively wedges the system. Fortunately, fork bombs are relatively easy to spot and kill, so creating one deliberately seldom accomplishes more than to bring the just wrath of the gods down upon the perpetrator. See also logic bomb.

*-Forked

adj. [UNIX; prob. influenced by a mainstream expletive] Terminally slow, or dead. Originated when one system was slowed to a snail's pace by an inadvertent fork bomb.

Formal Access

Documented approval by a data approval owner to allow access to a particular category of information.

Formal Access Approval

Documented approval by a data owner to allow access to a particular type or category of information. (DODD 5200. 28;; *NCSC-WA*-001-85;)

Formal Cryptographic Access (FCA)

Formal approval permitting access to COMSEC keying material and prior consent to a non-lifestyle, counterintelligence-scope polygraph examination. (AF9K_JBC. TXT)

Formal Development Methodology (FDM)

1. A software development methodology which makes use of the language, Ina Jo, to formally prove design specifications. Ina Jo is a language developed by System Development Corporation. (*NCSC-WA*-001-85;) (F:\NEWDEFS. TXT)
2. Collection of languages and tools enforcing a rigorous method of verification. This methodology uses the Ina Jo specification language for successive stages of system development, including identification and modeling of requirements, high-level design, and program design.

#-Formal Methods For Security Design

A collection of languages and tools that enforces a rigorous method of verification. This methodology uses the Ina Jo specification language for successive stages of system development, including identification and modeling of requirements, high-level design, and program design. (Source: *NCSC-TG*-0004).

Formal Proof

A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and for showing that computer programs satisfy their specifications. (CSC-STD-001-83;)

Formal Security Policy

Mathematically precise statement of a model security policy. NOTE: Such a model must define a secure state, an initial state, and how the model represents

changes in state. The model must be shown to be secure by proving that the initial state is secure and that all possible subsequent states remain secure.

Formal Security Policy Model

1. A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a TCB, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modelling techniques include: state transition models, temporal logic models, denotational semantics models, algebraic specification models. An example is the model described by Bell and LaPadula. (CSC-STD-001-83;; *NCSC-WA*-001-85;)
2. See BELL-LAPADULA MODEL and SECURITY POLICY MODEL.

Formal Top-Level

1. Top-level specification that is written specification in a formal mathematical language to allow theorems, showing the correspon-dence of the system specification to its formal requirements, to be hypothesized and formally proven.
2. NOTE: Formal top-level specification, required for a class A1 AIS, completely and accurately describes the trusted computing base.

Formal Top-Level Specification

(FTLS) A Top-Level Specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven. (CSC-STD-001-83;; *NCSC-WA*-001-85;);

Formal Verification

The process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model or (implementation verification) between the formal specification and its program implementation. (CSC-STD-001-83;)

Format

1. Arrangement of bits or characters within a group, such as a word, message, or language. (~) See also packet format.
2. Shape, size, and general makeup of a document. (~)

Formerly Restricted Data

(FRD) Classified information jointly determined by DOE and the Department of Defense (DOD) to be related primarily to the military utilization of atomic weapons, and removed by DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act, as amended, and safeguarded as national security information subject to the restrictions of transmission to other countries and regional defense organizations that apply to Restricted Data. (DOE 5635. 1 A)

Formulary

A technique for permitting the decision to grant or deny access to be determined dynamically at access time rather than at the time of creation of the access list. (*FIPS PUB* 39;)

*-Fortrash

/for'trash/ n. Hackerism for the FORTRAN (FORmula TRANslator) language, referring to its primitive design, gross and irregular syntax, limited control constructs, and slippery, exception-filled semantics.

Fortuitous Conduction

Emanations in the form of signals propagated along any unintended conductor. Such emanations may be compromising under the definition of "compromising emanations. "

Fortuitous Conductor

Any conductor which may provide an unintended path for signals. Fortuitous conductors include cables, wires, pipes, conduits, and structural metal work in the vicinity of a radiation source.

*-Fortune Cookie

n. [WAITS, via UNIX] A random quote, item of trivia, joke, or maxim printed to the user's tty at login time or (less commonly) at logout time. Items from this lexicon have often been used as fortune cookies. See cookie file.

*-Forum

n. [Usenet, GEnie, CI$; pl. `fora' or `forums'] Any discussion group accessible through a dial-in BBS, a mailing list, or a newsgroup (see network, the). A forum functions much like a bulletin board; users submit postings for all to read and discussion ensues. Contrast real-time chat via talk mode or point-to-point personal email.

Forward Error Correction

1. A system of error control for data transmission wherein the receiving device has the capability to detect and correct any character or code block that contains fewer than a predetermined number of symbols in error. (~)
2. Note: FEC is accomplished by adding bits to each transmitted character or code block using a predetermined algorithm. See also binary digit, block

code, character, code, convolutional code, data transmission, error, error control, error-detecting code, information feedback.

*-Fossil

1. n. In software, a misfeature that becomes understandable only in historical context, as a remnant of times past retained so as not to break compatibility. Example the retention of octal as default base for string escapes in C, in spite of the better match of hexadecimal to ASCII and modern byte-addressable architectures. See dusty deck.
2. More restrictively, a feature with past but no present utility. Example the force-all-caps (LCASE) bits in the V7 and BSD UNIX tty driver, designed for use with monocase terminals. (In a perversion of the usual backward-compatibility goal, this functionality has actually been expanded and renamed in some later USG UNIX releases as the IUCLC and OLCUC bits.)
3. The FOSSIL (Fido/Opus/Seadog Standard Interface Level) driver specification for serial-port access to replace the brain-dead routines in the IBM PC ROMs. Fossils are used by most MS-DOS BBS software in preference to the `supported' ROM routines, which do not support interrupt-driven operation or setting speeds above 9600; the use of a semistandard FOSSIL library is preferable to the bare metal serial port programming otherwise required. Since the FOSSIL specification allows additional functionality to be hooked in, drivers that use the hook but do not provide serial-port access themselves are named with a modifier, as in `video fossil'.

*-Four-Color Glossies

1. n. Literature created by marketroids that allegedly contains technical specs but which is in fact as superficial as possible without being totally content-free. “Forget the four-color glossies, give me the tech ref manuals. ” Often applied as an indication of superficiality even when the material is printed on ordinary paper in black and white. Four-color-glossy manuals are *never* useful for finding a problem.
2. [rare] Applied by extension to manual pages that don't contain enough information to diagnose why the program doesn't produce the expected or desired output.

*-Fragile

adj. Syn brittle.

Frame

1. A Data Structure that represents the attributes of an entity and other information about an entity. (ET;)
2. A data structure that represents attributes of an entity and other information about the entity. (MA;)

#-Fraud

Is an intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him, or to surrender a legal right. (Source - Blacks).

Fraud Or Abuse

#-Fraud, Waste And Abuse

Fraud is an intentional deception designed to deprive the USG unlawfully of something of value or to secure from the USG for an individual benefit, privilege, allowance or consideration to which he or she is not entitled. Waste is an extravagant, careless, or needless expenditure of government funds, or the consumption of government property that results from deficient practices, systems, controls or decisions. Abuse is an intentional or improper use of government resources, including misuse or resources such as tools, vehicles or copying machines. (Source Office of the Inspector General).

*-Frednet

/fred'net/ n. Used to refer to some random and uncommon protocol encountered on a network. “We're implementing bridging in our router to solve the frednet problem. ”

Freedom Of Information Act

Freeware

n. Free software, often written by enthusiasts and distributed by users' groups, or via electronic mail, local bulletin boards, Usenet, or other electronic media. At one time, `freeware' was a trademark of Andrew Fluegelman, the author of the well-known MS-DOS comm program PC-TALK III. It wasn't enforced after his mysterious disappearance and presumed death in 1984. See shareware.

*-Freeze

v. To lock an evolving software distribution or document against changes so it can be released with some hope of stability. Carries the strong implication that the item in question will `unfreeze' at some future date. “OK, fix that bug and we'll freeze for release. ” There are more specific constructions on this term. A `feature freeze', for example, locks out modifications intended to introduce new features but still allows bugfixes and completion of existing features; a `code freeze' connotes no more changes at all. At Sun Microsystems and elsewhere, one may also hear references to `code slush' -- that is, an almost-but-not-quite frozen state.

Frequency

The average number of event occurrences per year. (RM;)

Frequency Hopping

Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications.

Frequency Of Major Failure

*-Fried

1. adj. Non-working due to hardware failure; burnt out. Especially used of hardware brought down by a `power glitch' (see glitch), drop-outs, a short, or some other electrical event. (Sometimes this literally happens to electronic circuits! In particular, resistors can burn out and transformers can melt down, emitting noxious smoke -- see friode, SED and LER. However, this term is also used metaphorically.) Compare frotzed.
2. Of people, exhausted. Said particularly of those who continue to work in such a state. Often used as an explanation or excuse. “Yeah, I know that fix destroyed the file system, but I was fried when I put it in. ” Esp. common in conjunction with `brain' “My brain is fried today, I'm very short on sleep. ”

Friendly

Those individuals or organizations involved in the specific sensitive operation or activity who have a need-to-know (NSDD-298, 1/88) *A contact positively identified as friendly (JCS PUB 1-02, 12/89)

*-Frink

/frink/ v. The unknown ur-verb, fill in your own meaning. Found esp. on the Usenet newsgroup alt. fan. lemurs, where it is said that the lemurs know what `frink' means, but they aren't telling. Compare gorets.

*-Friode

/fri:'ohd/ n. [TMRC] A reversible (that is, fused or blown) diode. Compare fried; see also SED, LER.

*-Fritterware

n. An excess of capability that serves no productive end. The canonical example is font-diddling software on the Mac (see macdink); the term describes anything that eats huge amounts of time for quite marginal gains in function but seduces people into using it anyway. See also window shopping.

*-Frob

1. /frob/ 1. n. [MIT] The TMRC definition was “FROB = a protruding arm or trunnion”; by metaphoric extension, a `frob' is any random small thing; an object that you can comfortably hold in one hand; something you can frob (sense
2. . See frobnitz.
2. vt. Abbreviated form of frobnicate.
3. [from the MUD world] A command on some MUDs that changes a player's experience level (this can be used to make wizards); also, to request wizard privileges on the `professional courtesy' grounds that one is a wizard elsewhere. The command is actually `frobnicate' but is universally abbreviated to the shorter form.

*-Frobnicate

/frob'ni-kayt/ vt. [Poss. derived from frobnitz, and usually abbreviated to frob, but `frobnicate' is recognized as the official full form. ] To manipulate or adjust, to tweak. One frequently frobs bits or other 2-state devices. Thus “Please frob the light switch” (that is, flip it), but also “Stop frobbing that clasp; you'll break it”. One also sees the construction `to frob a frob'. See tweak and twiddle. Usage frob, twiddle, and tweak sometimes connote points along a continuum. `Frob' connotes aimless manipulation; `twiddle' connotes gross manipulation, often a coarse search for a proper setting; `tweak' connotes fine-tuning. If someone is turning a knob on an oscilloscope, then if he's carefully adjusting it, he is probably tweaking it; if he is just turning it but looking at the screen, he is probably twiddling it; but if he's just doing it because turning a knob is fun, he's frobbing it. The variant `frobnosticate' has been recently reported.

*-Frobnitz

/frob'nits/, pl. `frobnitzem' /frob'nit-zm/ or `frobni' /frob'ni:/ n. [TMRC] An unspecified physical object, a widget. Also refers to electronic black boxes. This rare form is usually abbreviated to `frotz', or more commonly to frob. Also used are `frobnule' (/frob'n[y]ool/) and `frobule' (/frob'yool/). Starting perhaps in 1979, `frobozz' /fr*-boz'/ (plural `frobbotzim' /fr*-bot'zm/) has also become very popular, largely through its exposure as a name via Zork. These variants can also be applied to nonphysical objects, such as data structures. Pete Samson, compiler of the original TMRC lexicon, adds, “Under the TMRC [railroad] layout were many storage boxes, managed (in 1958) by David R. Sawyer. Several had fanciful designations written on them, such as `Frobnitz Coil Oil'. Perhaps DRS intended Frobnitz to be a proper name, but the name was quickly taken for the thing”. This was almost certainly the origin of the term.

*-Front End

1. n. An intermediary computer that does set-up and filtering for another (usually more powerful but less friendly) machine (a `back end').
2. What you're talking to when you have a conversation with someone who is making replies without paying attention. “Look at the dancing elephants!” “Uh-huh. ” “Do you know what I just said?” “Sorry, you were talking to the front end. ” See also fepped out.

3. Software that provides an interface to another program `behind' it, which may not be as user-friendly. Probably from analogy with hardware front-ends (see sense 1) that interfaced with mainframes.

Front-End Processing

The transformation of information prior to a processing operation. Note: Front-end processing may include such service as serial-to-parallel conversion, packetizing, multiplexing and concentration, network access signaling/supervision, protocol conversion, error control, and diagnosis.

Front-End Processor

A programmed-logic or stored-program device that interfaces data communication equipment with an input/output bus or memory of a data processing computer. See also computer.

Front-End Security

Security filter, which could be filter implemented in hardware or software, that is logically separated from the remainder of an AIS to protect the integrity of the system.

Front-End Security Filter

1. A process that is invoked to process data according to a specified security policy prior to releasing the data outside the processing environment or upon receiving data from an external source. (DODD 5200. 28-STD;)
2. A security filter, which could be implemented in hardware or software, that is logically separated from the remainder of the system to protect its integrity. (*NCSC-WA*-001-85;)

*-Frotz

1. /frots/ 1. n. See frobnitz.
2. `mumble frotz'An interjection of mildest disgust.

*-Frotzed

/frotst/ adj. down because of hardware problems. Compare fried. A machine that is merely frotzed may be fixable without replacing parts, but a fried machine is more seriously damaged.

*-Frowney

n. (alt. `frowney face') See emoticon.

*-Fry

1. vi. To fail. Said especially of smoke-producing hardware failures. More generally, to become non-working. Usage never said of software, only of hardware and humans. See fried, magic smoke.
2. vt. To cause to fail; to roach, toast, or hose a piece of hardware. Never used of software or humans, but compare fried.

1. /F-T-P/, *not* /fit'ip/ [techspeak] n. The File Transfer Protocol for transmitting files between systems on the Internet.

2. vt. To beam a file using the File Transfer Protocol.
3. Sometimes used as a generic even for file transfers not using FTP. “Lemme get a copy of “Wuthering Heights” ftp'd from uunet. ”

*-FUBAR

1. n. The Failed UniBus Address Register in a VAX. A good example of how jargon can occasionally be snuck past the suits; see foobar, and foo for a fuller etymology.
2. Fouled up beyond repair

*-FUD Wars

/fuhd worz/ n. [from FUD] Political posturing engaged in by hardware and software vendors ostensibly committed to standardization but actually willing to fragment the market to protect their own shares. The UNIX International vs. OSF conflict is but one outstanding example. fudge

1. vt. To perform in an incomplete but marginally acceptable way, particularly with respect to the writing of a program. “I didn't feel like going through that pain and suffering, so I fudged it -- I'll fix it later. ”
2. n. The resulting code.

*-Fudge Factor

n. A value or parameter that is varied in an ad hoc way to produce the desired result. The terms `tolerance' and slop are also used, though these usually indicate a one-sided leeway, such as a buffer that is made larger than necessary because one isn't sure exactly how large it needs to be, and it is better to waste a little space than to lose completely for not having enough. A fudge factor, on the other hand, can often be tweaked in more than one direction. A good example is the `fuzz' typically allowed in floating-point calculations two numbers being compared for equality must be allowed to differ by a small amount; if that amount is too small, a computation may never terminate, while if it is too large, results will be needlessly inaccurate. Fudge factors are frequently adjusted incorrectly by programmers who don't fully understand their import. See also coefficient of X.

*-Fuel Up

vi. To eat or drink hurriedly in order to get back to hacking. “Food-p?” “Yeah, let's fuel up. ” “Time for a great-wall!” See also oriental food.

Full Bit Emanation

An emanation which correlates on a one-to-one basis with the bits of the message code signal.

Full Financial Disclosure

Full Maintenance

Complete diagnostic repair, modification, and overhaul of information systems security equipment, including repair of defective assemblies by piece part replacement.

*-Full Monty, The

n. See monty, sense 2.

Functional Testing

1. The portion of security testing in which the advertised features of a system are tested for correct operation. (CSC-STD-001-83;)
2. The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation. (*NCSC-WA*-001-85;)

Funds

*-Funky

adj. Said of something that functions, but in a slightly strange, klugey way. It does the job and would be difficult to change, so its obvious non-optimality is left alone. Often used to describe interfaces. The more bugs something has that nobody has bothered to fix because workarounds are easier, the funkier it is. TECO and UUCP are funky. The Intel i860's exception handling is extraordinarily funky. Most standards acquire funkiness as they age. “The new mailer is installed, but is still somewhat funky; if it bounces your mail for no reason, try resubmitting it. ” “This UART is pretty funky. The data ready line is active-high in interrupt mode and active-low in DMA mode. ”

*-Funny Money

1. n. Notional `dollar' units of computing time and/or storage handed to students at the beginning of a computer course; also called `play money' or `purple money' (in implicit opposition to real or `green' money). In New Zealand and Germany the odd usage `paper money' has been recorded; in Germany, the particularly amusing synonym `transfer ruble' commemmorates the funny money used for trade between COMECON countries back when the Soviet Bloc still existed. When your funny money ran out, your account froze and you needed to go to a professor to get more. Fortunately, the plunging cost of timesharing cycles has made this less common. The amounts allocated were almost invariably too small, even for the non-hackers who wanted to slide by with minimum work. In extreme cases, the practice led to small-scale black markets in bootlegged computer accounts.
2. By extension, phantom money or quantity tickets of any kind used as a resource-allocation hack within a system. Antonym `real money'.

Fuzz

A small quantity, associated with “distance” between values, such that if the distance is less than Fuzz, the two values may be said to be acceptably close. (MA;)

*-Fuzzball

n. [TCP/IP hackers] A DEC LSI-11 running a particular suite of homebrewed software written by Dave Mills and assorted co-conspirators, used in the early 1980s for Internet protocol testbedding and experimentation. These were used as NSFnet backbone sites in its early 56KB-line days; a few are still active on the Internet as of mid 1993, doing odd jobs such as network time service.

*-G

pref. ,suff. [SI] See quantifiers.

*-G-File

n. [Commodore BBS culture] Any file that is written with the intention of being read by a human rather than a machine, such asthe Jargon File, documentation, humor files, hacker lore and technical files. This term survives from the nearly-forgotten Commodore 64underground and BBS community. In the early 80s, C-Net had emerged as the mostpopular C64 BBS software for systems which encouraged messaging (as opposedto file transfer). There were three main options for files Program files (p-files), which served the same function as `doors' in today'ssystems, UD files (the user upload/download section), and G-files. Anythingthat was meant to be read was included in G-files.

*-Gabriel

/gay'bree-*l/ n. [for Dick Gabriel, SAIL LISP hacker and volleyball fanatic] An unnecessary (in the opinion of the opponent) stalling tactic, e. g. , tying one's shoelaces or combing one's hair repeatedly, asking the time, etc. Also used to refer to the perpetrator of such tactics. Also, `pulling a Gabriel', `Gabriel mode'.

G

*-Gag

vi. Equivalent to choke, but connotes more disgust. “Hey, this is FORTRAN code. No wonder the C compiler gagged. ” See also barf.

*-Garbage Collect

vi. (also `garbage collection', n.) See GC.

Garble

An error in transmission, reception, encryption, or decryption that changes the text of a message or any portion thereof in such a manner that it is incorrect or undecryptable. (JCS1-DoD) See also decrypt, encrypt, error.

*-Gas

As in ORKIN Termite Control

1. interj. A term of disgust and hatred, implying that gas should be dispensed in generous quantities, thereby exterminating the source of irritation. “Some loser just reloaded the system for no reason! Gas!”
2. interj. A suggestion that someone or something ought to be flushed out of mercy. “The system's getting wedged every few minutes. Gas!”
3. vt. To flush (sense 1). “You should gas that old crufty software. ”
4. [IBM] n. Dead space in nonsequentially organized files that was occupied by data that has since been deleted; the compression operation that removes it is called `degassing' (by analogy, perhaps, with the use of the same term in vacuum technology).
5. [IBM] n. Empty space on a disk that has been clandestinely allocated against future need.

*-Gaseous

adj. Deserving of being gassed. Disseminated by Geoff Goodfellow while at SRI; became particularly popular after the Moscone-Milk killings in San Francisco, when it was learned that the defendant Dan White (a politician who had supported Proposition 7) would get the gas chamber under Proposition 7 if convicted of first-degree murder (he was eventually convicted of manslaughter).

Gate

1. A device having one output channel and one or more input channels, such that the output channel state is completely determined by the input channel states, except during switching transients.
2. One of many types of combinational logic elements having at least two inputs; e. g. , AND, OR, NAND, and NOR. (~)

Gateway

An interface between two networks. (JCS PUB 6-03. 7)

Gating

1. The process of selecting only those portions of a wave between specified time intervals or between specified amplitude limits. See also limiting, synchronizing.
2. The controlling of signals by means of combinational logic elements. (~) See also gate.
3. A process in which a predetermined set of conditions, when established, permits a second process to occur. (~) See also decision circuit, synchronizing.

Gauss

A unit measure of the magnetic flux density produced by a magnetizing force. (CSC-STD-005-85;)

*-Gawble

n. See chawmp.

*-GC

/G-C/ [from LISP terminology; `Garbage Collect']

1. vt. To clean up and throw away useless things. “I think I'll GC the top of my desk today. ” When said of files, this is equivalent to GFR.
2. vt. To recycle, reclaim, or put to another use.
3. n. An instantiation of the garbage collector process. `Garbage collection' is computer-science techspeak for a particular class of strategies for dynamically but transparently reallocating computer memory (i. e. , without requiring explicit allocation and deallocation by higher-level software). One such strategy involves periodically scanning all the data in memory and determining what is no longer accessible; useless data items are then discarded so that the memory they occupy can be recycled and used for another purpose. Implementations of the LISP language usually use garbage collection. In jargon, the full phrase is sometimes heard but the abbrev is more frequently used because it is shorter. Note that there is an ambiguity in usage that has to be resolved by context “I'm going to garbage-collect my desk” usually means to clean out the drawers, but it could also mean to throw away or recycle the desk itself.

*-GCOS

/jee'kohs/ n. A quick-and-dirty clone of System/360 DOS that emerged from GE around 1970; originally called GECOS (the General Electric Comprehensive Operating System). Later kluged to support primitive timesharing and transaction processing. After the buyout of GE's computer division by Honeywell, the name was changed to General Comprehensive Operating System (GCOS). Other OS groups at Honeywell began referring to it as `God's Chosen Operating System', allegedly in reaction to the GCOS crowd's uninformed and snotty attitude about the superiority of their product. All this might be of zero interest, except for two facts (1) The GCOS people won the political war, and this led in the orphaning and eventual death of Honeywell Multics, and (2) GECOS/GCOS left one permanent mark on UNIX. Some early UNIX systems at Bell Labs used GCOS machines for print spooling and various other services; the field added to `/etc/passwd' to carry GCOS ID information was called the `GECOS field' and survives today as the `pw_gecos' member used for the user's full name and other human-ID information. GCOS later played a major role in keeping Honeywell a dismal also-ran in the mainframe market, and was itself ditched for UNIX in the late 1980s when Honeywell retired its aging big iron designs.

*-GECOS

/jee'kohs/ n. See GCOS.

***-Gedanken**

/g*-dahn'kn/ adj. Ungrounded; impractical; not well-thought-out; untried; untested. `Gedanken' is a German word for `thought'. A thought experiment is one you carry out in your head. In physics, the term `gedanken experiment' is used to refer to an experiment that is impractical to carry out, but useful to consider because it can be reasoned about theoretically. (A classic gedanken experiment of relativity theory involves thinking about a man in an elevator accelerating through space.) Gedanken experiments are very useful in physics, but must be used with care. It's too easy to idealize away some important aspect of the real world in constructing the `apparatus'. Among hackers, accordingly, the word has a pejorative connotation. It is typically used of a project, especially one in artificial intelligence research, that is written up in grand detail (typically as a Ph. D. thesis) without ever being implemented to any great extent. Such a project is usually perpetrated by people who aren't very good hackers or find programming distasteful or are just in a hurry. A `gedanken thesis' is usually marked by an obvious lack of intuition about what is programmable and what is not, and about what does and does not constitute a clear specification of an algorithm. See also AI-complete, DWIM.

***-Geef**

v. [ostensibly from `gefingerpoken'] vt. Syn. mung. See also blinkenlights.

***-Geek Code**

n. A set of codes commonly used in sig blocks to broadcast the interests, skills, and aspirations of the poster. Features a G at the left margin followed by numerous letter codes, often suffixed with plusses or minuses. Because many net users are involved in computer science, the most common prefix is `GCS'. To see a copy of the current Code of the Geeks, finger hayden@vax1. mankato. msus. edu. See also computer geek.

***-Geek Out**

vi. To temporarily enter techno-nerd mode while in a non-hackish context, for example at parties held near computer equipment. Especially used when you need to do or say something highly technical and don't have time to explain “Pardon me while I geek out for a moment. ” See computer geek; see also propeller head.

***-Gen**

/jen/ n. ,v. Short for generate, used frequently in both spoken and written contexts.

***-Gender Mender**

n. A cable connector shell with either two male or two female connectors on it, used to correct the mismatches that result when some loser didn't understand the RS232C specification and the distinction between DTE and DCE. Used esp. for RS-232C parts in either the original D-25 or the IBM PC's bogus D-9 format. Also called `gender bender', `gender blender', `sex changer';

***-General Public Virus**

n. Pejorative name for some versions of the GNU project copyleft or General Public License (GPL), which requires that any tools or apps incorporating copylefted code must be source-distributed on the same counter-commercial terms as GNU stuff. Thus it is alleged that the copyleft `infects' software generated with GNU tools, which may in turn infect other software that reuses any of its code. The Free Software Foundation's official position as of January 1991 is that copyright law limits the scope of the GPL to “programs textually incorporating significant amounts of GNU code”, and that the `infection' is not passed on to third parties unless actual GNU source is transmitted (as in, for example, use of the Bison parser skeleton). Nevertheless, widespread suspicion that the copyleft language is `boobytrapped' has caused many developers to avoid using GNU tools and the GPL. Recent (July 1991) changes in the language of the version 2. 00 license may eliminate this problem.

General Purpose Network

See common user network.

General Purpose System

A computer system that is designed to aid in solving a wide variety of problems. (CSC-STD-001-93)

General Services Administration

Generla Services Administration

#-Generally Accepted Systems Security Principles (GSSP)

This KSA has no definition.

***-Generate**

vt. To produce something according to an algorithm or program or set of rules, or as a (possibly unintended) side effect of the execution of an algorithm or program. The opposite of parse. This term retains its mechanistic connotations (though often humorously) when used of human behavior. “The guy is rational most of the time, but mention nuclear energy around him and he'll generate infinite flamage. ”

Generatrix

the set of letters which are considered to be the cause of a particular received TEMPEST signal, arranged in order of probability.

Generatrix Family

The groups (sets of generatrices) into which the letters of the alphabet are assigned by the TEMPEST encoder. Also, the groups into which the letters are

assigned at the output of the detector for analysis purposes.

Generatrix Sequence

The sequence of generatrices resulting from a test, where a representative test message for the EUT is processed; one generatrix for each received signal.

#-Generic Accreditation

1. (aka type accreditation) (1) Official authorization by the DAA to employ a system in a specified environment. (Note: Type accreditation includes a statement of residual risk, delineates the operating environment, and identifies the specific use. It may be performed when multiple copies of a system are to be fielded in similar environments.) (Source: *NCSC-TG*-029). (2)
2. Accreditation provided with end product delivered by the Design and Implementation organization. Sometimes referred to as “Type accreditation”. (Source: DACUM IV).

*-Genius From Mars Technique

n. [TMRC] A visionary quality which enables one to ignore the standard approach and come up with a totally unexpected new algorithm. To approach a problem from an offbeat angle that no one has ever thought of before, but that in retrospect makes total sense. Compare grok, zen.

*-Gensym

/jen'sim/ [from MacLISP for `generated symbol']

1. v. To invent a new name for something temporary, in such a way that the name is almost certainly not in conflict with one already in use.
2. n. The resulting name. The canonical form of a gensym is `Gnnnn' where nnnn represents a number; any LISP hacker would recognize G0093 (for example) as a gensym.
3. A freshly generated data structure with a gensymmed name. Gensymmed names are useful for storing or uniquely identifying crufties (see cruft).

*-Get A Life!

imp. Hacker-standard way of suggesting that the person to whom it is directed has succumbed to terminal geekdom (see computer geek). Often heard on Usenet, esp. as a way of suggesting that the target is taking some obscure issue of theology too seriously. This exhortation was popularized by William Shatner on a “Saturday Night Live” episode in a speech that ended “Get a *life*!”, but some respondents believe it to have been in use before then. It was certainly in wide use among hackers for at least five years before achieving mainstream currency in early 1992.

*-Get A Real Computer!

imp. Typical hacker response to news that somebody is having trouble getting work done on a system that (a) is single-tasking, (b) has no hard disk, or (c) has an address space smaller than 16 megabytes. This is as of mid-1993; note that the threshold for `real computer' rises with time, and it may well be (for example) that machines with character-only displays will be generally considered `unreal' in a few years (GLS points out that they already are in some circles). See bitty box and toy.

*-GFR

/G-F-R/ vt. [ITS from `Grim File Reaper', an ITS and LISP Machine utility] To remove a file or files according to some program-automated or semi-automatic manual procedure, especially one designed to reclaim mass storage space or reduce name-space clutter (the original GFR actually moved files to tape). Often generalized to pieces of data below file level. “I used to have his phone number, but I guess I GFRed it. ” See also prowler, reaper. Compare GC, which discards only provably worthless stuff.

*-Gig

/jig/ or /gig/ n. [SI] See quantifiers.

*-Giga

/ji'ga/ or /gi'ga/ pref. [SI] See quantifiers.

*-GIGO

1. /gi:'goh/ [acronym] `Garbage In, Garbage Out' --- usually said in response to lusers who complain that a program didn't “do the right thing” when given imperfect input or otherwise mistreated in some way. Also commonly used to describe failures in human decision making due to faulty, incomplete, or imprecise data.
2. `Garbage In, Gospel Out' this more recent expansion is a sardonic comment on the tendency human beings have to put excessive trust in `computerized' data.

*-Gilley

n. [Usenet] The unit of analogical bogosity. According to its originator, the standard for one gilley was “the act of bogotoficiously comparing the shutting down of 1000 machines for a day with the killing of one person”. The milligilley has been found to suffice for most normal conversational exchanges.

*-Gillion

/gil'y*n/ or /jil'y*n/ n. [formed from giga- by analogy with mega/million and tera/trillion] 10^9. Same as an American billion or a British `milliard'. How one pronounces this depends on whether one speaks giga- with a hard or soft `g'.

*-GIPS

/gips/ or /jips/ n. [analogy with MIPS] Giga-Instructions per Second (also possibly `Gillions of Instructions per Second'; see gillion). In 1991, this is used of only a handful of highly parallel machines, but this is expected to change. Compare KIPS.

***-Glark**

/glark/ vt. To figure something out from context. “The System III manuals are pretty poor, but you can generally glark the meaning from context. ” Interestingly, the word was originally `glork'; the context was “This gubblick contains many nonsklarkish English flutzpahs, but the overall pluggandisp can be glorked [sic] from context” (David Moser, quoted by Douglas Hofstadter in his “Metamagical Themas” column in the January 1981 “Scientific American”). It is conjectured that hackish usage mutated the verb to `glark' because glork was already an established jargon term. Compare grok, zen.

***-Glass**

n. [IBM] Synonym for silicon.

***-Glass Tty**

/glas T-T-Y/ or /glas ti'tee/ n. A terminal that has a display screen but which, because of hardware or software limitations, behaves like a teletype or some other printing terminal, thereby combining the disadvantages of both like a printing terminal, it can't do fancy display hacks, and like a display terminal, it doesn't produce hard copy. An example is the early `dumb' version of Lear-Siegler ADM 3 (without cursor control). See tube, tty; compare dumb terminal, smart terminal. See “TV Typewriters” (Appendix A) for an interesting true story about a glass tty.

***-Glassfet**

/glas'fet/ n. [by analogy with MOSFET, the acronym for `Metal-Oxide-Semiconductor Field-Effect Transistor'] Syn. firebottle, a humorous way to refer to a vacuum tube.

***-Glitch**

1. /glich/ [from German `glitzschig' to slip, via Yiddish `glitshen', to slide or skid] n. A sudden interruption in electric service, sanity, continuity, or program function. Sometimes recoverable. An interruption in electric service is specifically called a `power glitch' (also power hit), of grave concern because it usually crashes all the computers. In jargon, though, a hacker who got to the middle of a sentence and then forgot how he or she intended to complete it might say, “Sorry, I just glitched”.
2. vi. To commit a glitch. See gritch.
3. vt. [Stanford] To scroll a display screen, esp. several lines at a time. WAITS terminals used to do this in order to avoid continuous scrolling, which is distracting to the eye.
4. obs. Same as magic cookie, sense 2. All these uses of `glitch' derive from the specific technical meaning the term has in the electronic hardware world, where it is now techspeak. A glitch can occur when the inputs of a circuit change, and the outputs change to some random value for some very brief time before they settle down to the correct value. If another circuit inspects the output at just the wrong time, reading the random value, the results can be very wrong and very hard to debug (a glitch is one of many causes of electronic heisenbugs).

***-Glob**

/glob/, *not* /glohb/ vt. ,n. [UNIX] To expand special characters in a wildcarded name, or the act of so doing (the action is also called `globbing'). The UNIX conventions for filename wildcarding have become sufficiently pervasive that many hackers use some of them in written English, especially in email or news on technical topics. Those commonly encountered include the following * wildcard for any string (see also UN*X) ? wildcard for any single character (generally read this way only at the beginning or in the middle of a word) [] delimits a wildcard matching any of the enclosed characters alternation of comma-separated alternatives; thus, `foobaz,qux' would be read as `foobaz' or `fooqux' Some examples “He said his name was [KC]arl” (expresses ambiguity). “I don't read talk. politics. *” (any of the talk. politics subgroups on Usenet). Other examples are given under the entry for X. Note that glob patterns are similar, but not identical, to those used in regexps. Historical note The jargon usage derives from `glob', the name of a subprogram that expanded wildcards in archaic pre-Bourne versions of the UNIX shell.

***-Glork**

1. /glork/ interj. Term of mild surprise, usually tinged with outrage, as when one attempts to save the results of two hours of editing and finds that the system has just crashed.
2. Used as a name for just about anything. See foo.
3. vt. Similar to glitch, but usually used reflexively. “My program just glorked itself. ” See also glark.

***-Glue**

n. Generic term for any interface logic or protocol that connects two component blocks. For example, Blue Glue is IBM's SNA protocol, and hardware designers call anything used to connect large VLSI's or circuit blocks `glue logic'.

***-Gnarly**

/nar'lee/ adj. Both obscure and hairy (sense 1). “Yow! -- the tuned assembler implementation of BitBlt is really gnarly!” From a similar but less specific usage in surfer slang.

***-GNU**

1. /gnoo/, *not* /noo/ [acronym `GNU's Not UNIX!', see recursive acronym] A UNIX-workalike development effort of the Free Software Foundation headed by Richard Stallman <rms@gnu. ai. mit. edu>. GNU EMACS and the GNU C compiler, two tools designed for this project, have become very popular in hackerdom and elsewhere. The

GNU project was designed partly to proselytize for RMS's position that information is community property and all software source should be shared. One of its slogans is “Help stamp out software hoarding!” Though this remains controversial (because it implicitly denies any right of designers to own, assign, and sell the results of their labors), many hackers who disagree with RMS have nevertheless cooperated to produce large amounts of high-quality software for free redistribution under the Free Software Foundation's imprimatur. See EMACS, copyleft, General Public Virus, Linux.

2. Noted UNIX hacker John Gilmore <gnu@toad.com>, founder of Usenet's anarchic alt. * hierarchy.

*-GNUMACS

/gnoo'maks/ n. [contraction of `GNU EMACS'] Often-heard abbreviated name for the GNU project's flagship tool, EMACS. Used esp. in contrast with GOSMACS.

*-Go Flatline

1. v. [from cyberpunk SF, refers to flattening of EEG traces upon brain-death] (also adjectival `flatlined'). To die, terminate, or fail, esp. irreversibly. In hacker parlance, this is used of machines only, human death being considered somewhat too serious a matter to employ jargon-jokes about.
2. To go completely quiescent; said of machines undergoing controlled shutdown. “You can suffer file damage if you shut down UNIX but power off before the system has gone flatline. ”
3. Of a video tube, to fail by losing vertical scan, so all one sees is a bright horizontal line bisecting the screen.

*-Go Root

vi. [UNIX] To temporarily enter root mode in order to perform a privileged operation.

*-Go-Faster Stripes

[UK] Syn. chrome. Mainstream in some parts of UK.

*-Gobble

1. vt. To consume, usu. used with `up'. “The output spy gobbles characters out of a tty output buffer. ”
2. To obtain, usu. used with `down'. “I guess I'll gobble down a copy of the documentation tomorrow. ” See also snarf.

*-Godwin's Law

prov. [Usenet] “As a Usenet discussion grows longer, the probability of a comparison involving Nazis or Hitler approaches one. ” There is a tradition in many groups that, once this occurs, that thread is over, and whoever mentioned the Nazis has automatically lost whatever argument was in progress. Godwin's Law thus guarantees the existence of an upper bound on thread length in those groups.

*-Godzillagram

1. /god-zil'*-gram/ n. [from Japan's national hero] A network packet that in theory is a broadcast to every machine in the universe. The typical case is an IP datagram whose destination IP address is [255. 255. 255. 255]. Fortunately, few gateways are foolish enough to attempt to implement this case!
2. A network packet of maximum size. An IP Godzillagram has 65,536 octets. Compare super source quench.

*-Golden

adj. [prob. from folklore's `golden egg'] When used to describe a magnetic medium (e. g. , `golden disk', `golden tape'), describes one containing a tested, up-to-spec, ready-to-ship software version. Compare platinum-iridium.

*-Golf-Ball Printer

n. The IBM 2741, a slow but letter-quality printing device and terminal based on the IBM Selectric typewriter. The `golf ball' was a little spherical frob bearing reversed embossed images of 88 different characters arranged on four parallels of latitude; one could change the font by swapping in a different golf ball. This was the technology that enabled APL to use a non-EBCDIC, non-ASCII, and in fact completely non-standard character set. This put it 10 years ahead of its time -- where it stayed, firmly rooted, for the next 20, until character displays gave way to programmable bit-mapped devices with the flexibility to support other character sets.

*-Gonk

1. /gonk/ vt. ,n. To prevaricate or to embellish the truth beyond any reasonable recognition. In German the term is (mythically) `gonken'; in Spanish the verb becomes `gonkar'. “You're gonking me. That story you just told me is a bunch of gonk. ” In German, for example, “Du gonkst mir” (You're pulling my leg). See also gonkulator.
2. [British] To grab some sleep at an odd time; compare gronk out.

*-Gonkulator

/gon'kyoo-lay-tr/ n. [from the old “Hogan's Heroes” TV series] A pretentious piece of equipment that actually serves no useful purpose. Usually used to describe one's least favorite piece of computer hardware. See gonk.

*-Gonzo

1. /gon'zoh/ adj. [from Hunter S. Thompson] Overwhelming; outrageous; over the top; very large, esp. used of collections of source code, source files, or individual functions. Has some of the connotations of moby and hairy, but without the implication of obscurity or complexity. Good

Thing n. ,adj. Often capitalized; always pronounced as if capitalized. 1. Self-evidently wonderful to anyone in a position to notice “The Trailblazer's 19. 2Kbaud PEP mode with on-the-fly Lempel-Ziv compression is a Good Thing for sites relaying netnews. ”
2. Something that can't possibly have any ill side-effects and may save considerable grief later “Removing the self-modifying code from that shared library would be a Good Thing. ”
3. When said of software tools or libraries, as in “YACC is a Good Thing”, specifically connotes that the thing has drastically reduced a programmer's work load. Oppose Bad Thing.

Goods

Any articles, materials, supplies, or manufactured products, including inspection and test equipment. The term excludes technical data. (DODD 2040. 2;)

*-Gopher

n. A type of Internet service first floated around 1991 and now (1994) being obsolesced by the World-Wide Web. Gopher presents a menuing interface to a tree or graph of links; the links can be to documents, runnable programs, or other gopher menus arbitrarily far across the net. Some claim that the gopher software, which was originally developed at the University of Minnesota, was named after the Minnesota Gophers (a sports team). Others claim the word derives from American slang `gofer' (from “go for”, dialectical “go fer”), one whose job is to run and fetch things. Finally, observe that gophers (aka woodchucks) dig long tunnels, and the idea of tunneling through the net to find information was a defining metaphor for the developers. Probably all three things were true, but with the first two coming first and the gopher-tunnel metaphor serendipitously adding flavor and impetus to the project as it developed out of its concept stage.

*-Gopher Hole

1. n. Any access to a gopher.
2. [Amateur Packet Radio] The terrestrial analogue of a wormhole (sense 2. ,from which this term was coined. A gopher hole links two amateur packet relays through some non-ham radio medium.

*-Gorets

/gor'ets/ n. The unknown ur-noun, fill in your own meaning. Found esp. on the Usenet newsgroup alt. gorets, which seems to be a running contest to redefine the word by implication in the funniest and most peculiar way, with the understanding that no definition is ever final. [A correspondent from the Former Soviet Union informs me that `gorets' is Russian for `mountain dweller' -- ESR] Compare frink.

*-Gorilla Arm

n. The side-effect that destroyed touch-screens as a mainstream input technology despite a promising start in the early 1980s. It seems the designers of all those spiffy touch-menu systems failed to notice that humans aren't designed to hold their arms in front of their faces making small motions. After more than a very few selections, the arm begins to feel sore, cramped, and oversized -- the operator looks like a gorilla while using the touch screen and feels like one afterwards. This is now considered a classic cautionary tale to human-factors designers; “Remember the gorilla arm!” is shorthand for “How is this going to fly in *real* use?”.

GOSIP

Acronym for Government Open Systems Interconnection Profile.

*-GOSMACS

/goz'maks/ n. [contraction of `Gosling EMACS'] The first EMACS-in-C implementation, predating but now largely eclipsed by GNUMACS. Originally freeware; a commercial version is now modestly popular as `UniPress EMACS'. The author (James Gosling) went on to invent NeWS.

*-Gosperism

/gos'p*r-izm/ n. A hack, invention, or saying due to arch-hacker R. William (Bill) Gosper. This notion merits its own term because there are so many of them. Many of the entries in HAKMEM are Gosperisms; see also life.

*-Gotcha

n. A misfeature of a system, especially a programming language or environment, that tends to breed bugs or mistakes because it both enticingly easy to invoke and completely unexpected and/or unreasonable in its outcome. For example, a classic gotcha in C is the fact that `if (a=b) code;' is syntactically valid and sometimes even correct. It puts the value of `b' into `a' and then executes `code' if `a' is non-zero. What the programmer probably meant was `if (a==b) code;', which executes `code' if `a' and `b' are equal.

Government Agency

1. Any executive department, commission, independent establishment, or corporation, wholly or partly owned by the United States of America and which is an instrumentality of the United States, or any board, bureau, division, service, office, authority, administration, or other establishment in the executive branch of the government. (DOE 5635. lA)
2. Synonymous with AGENCY.

Government Contractor

An individual, corporation, partnership, association, or other entity performing work under a U. S. Government contract, either as a prime contractor, or as a subcontractor. (NTISSI 3005; NACSI 6002)

Government Contractor Telecommunications

Telecommunications between or among departments or agencies and their contractors, and telecommunications of, between, or among government contractors and their subcontractors, of whatever level, which relate to government business or performance of a government contract. (NACSI 6002)

Government Information

Information created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government. (A-130;)

Government Open Systems Interconnection Profile (GOSIP)

A definition of Federal Government functional requirements for open systems computer network products. A common set of Open System Interconnection (OSI) data communication protocols that enables systems developed by different vendors to interoperate and enable the users of different applications on these systems to exchange information. Note 1: These OSI protocols were developed primarily by ISO and CCITT. Note 2: The GOSIP is a subset of the OSI protocols and is based on agreements reached by vendors and users of computer networks participating in the National Institute of Standards and Technology (NIST) Implementors Workshop. Note 3: The GOSIP is promulgated as *FIPS PUB* 146. See also Open Systems Interconnection.

Government Publication

Informational matter which is published as an individual document at government expense, or as required by law. (A-130;)

Government Telecommunications

Telecommunications of any employee, officer, contractor, or other entity of the U. S. Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the U. S. government or a government contractor. (See Telecommunications and Telecommunications System.) (NACSI 4000A)

Granularity

1. The relative fineness or coarseness by which a mechanism can be adjusted. The phrase “the granularity of a single user” means the access control mechanism can be adjusted to include or exclude any single user. (DODD 5200. 28-STD;)
2. An expression of the relative size of a data object, e. g. , protection at the file level is considered coarse granularity, whereas protection at the field level is considered to be a finer granularity. (*NCSC-WA*-001-85;)

Gray Scale

An optical pattern consisting of discrete steps or shades of gray between black and white. (~) See also facsimile.

*-Great Renaming

n. The flag day in 1985 on which all of the non-local groups on the Usenet had their names changed from the net. - format to the current multiple-hierarchies scheme. Used esp. in discussing the history of newsgroup names. “The oldest sources group is comp. sources. misc; before the Great Renaming, it was net. sources. ”

*-Great Runes

n. Uppercase-only text or display messages. Some archaic operating systems still emit these. See also runes, smash case, fold case. Decades ago, back in the days when it was the sole supplier of long-distance hardcopy transmittal devices, the Teletype Corporation was faced with a major design choice. To shorten code lengths and cut complexity in the printing mechanism, it had been decided that teletypes would use a monocase font, either ALL UPPER or all lower. The Question Of The Day was therefore, which one to choose. A study was conducted on readability under various conditions of bad ribbon, worn print hammers, etc. Lowercase won; it is less dense and has more distinctive letterforms, and is thus much easier to read both under ideal conditions and when the letters are mangled or partly obscured. The results were filtered up through management. The chairman of Teletype killed the proposal because it failed one incredibly important criterion “It would be impossible to spell the name of the Deity correctly. ” In this way (or so, at least, hacker folklore has it) superstition triumphed over utility. Teletypes were the major input devices on most early computers, and terminal manufacturers looking for corners to cut naturally followed suit until well into the 1970s. Thus, that one bad call stuck us with Great Runes for thirty years.

*-Great Worm, The

n. The 1988 Internet worm perpetrated by RTM. This is a play on Tolkien (compare elvish, elder days). In the fantasy history of his Middle Earth books, there were dragons powerful enough to lay waste to entire regions; two of these (Scatha and Glaurung) were known as “the Great Worms”. This usage expresses the connotation that the RTM hack was a sort of devastating watershed event in hackish history; certainly it did more to make non-hackers nervous about the Internet than anything before or since.

*-Great-Wall

vi. ,n. [from SF fandom] A mass expedition to an oriental restaurant, esp. one where food is served family-style and shared. There is a common heuristic about the amount of food to order, expressed as “Get N - 1 entrees”; the value of N, which is the number of people in the group, can be inferred from context (see

ple in the group, can be inferred from context (see N). See oriental food, ravs, stir-fried random.

*-Green Book

1. n. One of the three standard PostScript references “PostScript Language Program Design”, bylined `Adobe Systems' (Addison-Wesley, 1988; QA76. 73. P67P66 ISBN 0-201-14396-8); see also Red Book, Blue Book, and the White Book (sense 2. .
2. Informal name for one of the three standard references on SmallTalk “Smalltalk-80 Bits of History, Words of Advice”, by Glenn Krasner (Addison-Wesley, 1983; QA76. 8. S635S58; ISBN 0-201-11669-3) (this, too, is associated with blue and red books).
3. The “X/Open Compatibility Guide”, which defines an international standard UNIX environment that is a proper superset of POSIX/SVID; also includes descriptions of a standard utility toolkit, systems administrations features, and the like. This grimoire is taken with particular seriousness in Europe. See Purple Book.
4. The IEEE 1003. 1 POSIX Operating Systems Interface standard has been dubbed “The Ugly Green Book”.
5. Any of the 1992 standards issued by the CCITT's tenth plenary assembly. These include, among other things, the X. 400 email standard and the Group 1 through 4 fax standards. See also book titles.

*-Green Bytes

1. n. (also `green words') Meta-information embedded in a file, such as the length of the file or its name; as opposed to keeping such information in a separate description file or record. The term comes from an IBM user's group meeting (ca. 1962) at which these two approaches were being debated and the diagram of the file on the blackboard had the `green bytes' drawn in green.
2. By extension, the non-data bits in any self-describing format. “A GIF file contains, among other things, green bytes describing the packing method for the image. ” Compare out-of-band, zigamorph, fence (sense 1).

*-Green Card

n. [after the “IBM System/360 Reference Data” card] A summary of an assembly language, even if the color is not green. Less frequently used now because of the decrease in the use of assembly language. “I'll go get my green card so I can check the addressing mode for that instruction. ” Some green cards are actually booklets. The original green card became a yellow card when the System/370 was introduced, and later a yellow booklet. An anecdote from IBM refers to a scene that took place in a programmers' terminal room at Yorktown in 1978. A luser overheard one of the programmersask another “Do you have a green card?” The other grunted and passed the first a thick yellow booklet. At this point the luser turned a delicate shade of olive and rapidly left the room, never to return.

*-Green Lightning

1. n. [IBM] Apparently random flashing streaks on the face of 3278-9 terminals while a new symbol set is being downloaded. This hardware bug was left deliberately unfixed, as some genius within IBM suggested it would let the user know that `something is happening'. That, it certainly does. Later microprocessor-driven IBM color graphics displays were actually *programmed* to produce green lightning!
2. [proposed] Any bug perverted into an alleged feature by adroit rationalization or marketing. “Motorola calls the CISC cruft in the 88000 architecture `compatibility logic', but I call it green lightning”. See also feature (sense 6).

*-Green Machine

n. A computer or peripheral device that has been designed and built to military specifications for field equipment (that is, to withstand mechanical shock, extremes of temperature and humidity, and so forth). Comes from the olive-drab `uniform' paint used for military equipment.

*-Green's Theorem

prov. [TMRC] For any story, in any group of people there will be at least one person who has not heard the story. A refinement of the theorem states that there will be *exactly* one person (if there were more than one, it wouldn't be as bad to re-tell the story). [The name of this theorem is a play on a fundamental theorem in calculus. -- ESR]

*-Grep

/grep/ vt. [from the qed/ed editor idiom g/re/p , where re stands for a regular expression, to Globally search for the Regular Expression and Print the lines containing matches to it, via UNIX `grep(1)'] To rapidly scan a file or set of files looking for a particular string or pattern (when browsing through a large set of files, one may speak of `grepping around'). By extension, to look for something by pattern. “Grep the bulletin board for the system backup schedule, would you?” See also vgrep.

*-Grilf

// n. Girl-friend. Like newsfroup and filk, a typo reincarnated as a new word. Seems to have originated sometime in 1992.

*-Grind

1. vt. [MIT and Berkeley] To prettify hardcopy of code, especially LISP code, by reindenting lines,

printing keywords and comments in distinct fonts (if available), etc. This usage was associated with the MacLISP community and is now rare; prettyprint was and is the generic term for such operations.
2. [UNIX] To generate the formatted version of a document from the nroff, troff, TeX, or Scribe source.
3. To run seemingly interminably, esp. (but not necessarily) if performing some tedious and inherently useless task. Similar to crunch or grovel. Grinding has a connotation of using a lot of CPU time, but it is possible to grind a disk, network, etc. See also hog.
4. To make the whole system slow. “Troff really grinds a PDP-11. ” 5. `grind grind' excl. Roughly, “Isn't the machine slow today!”

*-Grind Crank

n. A mythical accessory to a terminal. A crank on the side of a monitor, which when operated makes a zizzing noise and causes the computer to run faster. Usually one does not refer to a grind crank out loud, but merely makes the appropriate gesture and noise. See grind and wugga wugga. Historical note At least one real machine actually had a grind crank -- the R1, a research machine built toward the end of the days of the great vacuum tube computers, in 1959. R1 (also known as `The Rice Institute Computer' (TRIC) and later as `The Rice University Computer' (TRUC)) had a single-step/free-run switch for use when debugging programs. Since single-stepping through a large program was rather tedious, there was also a crank with a cam and gear arrangement that repeatedly pushed the single-step button. This allowed one to `crank' through a lot of code, then slow down to single-step for a bit when you got near the code of interest, poke at some registers using the console typewriter, and then keep on cranking.

*-Gripenet

n. [IBM] A wry (and thoroughly unofficial) name for IBM's internal VNET system, deriving from its common use by IBMers to voice pointed criticism of IBM management that would be taboo in more formal channels.

*-Gritch

1. /grich/ [MIT] n. A complaint (often caused by a glitch).
2. vi. To complain. Often verb-doubled “Gritch gritch”.
3. A synonym for glitch (as verb or noun). Interestingly, this word seems to have a separate history from glitch, with which it is often confused. Back in the early 1960s, when `glitch' was strictly a hardware-tech's term of art, the Burton House dorm at M. I. T. maintained a “Gritch Book”, a blank volume, into which the residents hand-wrote complaints, suggestions, and witticisms. Previous years' volumes of this tradition were maintained, dating back to antiquity. The word “gritch” was described as a portmanteau of “gripe” and “bitch”. Thus, sense 3 above is at least historically incorrect.

*-Grok

/grok/, var. /grohk/ vt. [from the novel “Stranger in a Strange Land”, by Robert A. Heinlein, where it is a Martian word meaning literally `to drink' and metaphorically `to be one with'] The emphatic form is `grok in fullness'.
1. To understand, usually in a global sense. Connotes intimate and exhaustive knowledge. Contrast zen, which is similar supernal understanding experienced as a single brief flash. See also glark.
2. Used of programs, may connote merely sufficient understanding. “Almost all C compilers grok the `void' type these days. ”

*-Gronk

1. /gronk/ vt. [popularized by Johnny Hart's comic strip “B. C. ” but the word apparently predates that] 1. To clear the state of a wedged device and restart it. More severe than `to frob' (sense2. .
2. [TMRC] To cut, sever, smash, or similarly disable.
3. The sound made by many 3. 5-inch diskette drives. In particular, the microfloppies on a Commodore Amiga go “grink, gronk”.

*-Gronk Out

vi. To cease functioning. Of people, to go home and go to sleep. “I guess I'll gronk out now; see you all tomorrow. ”

*-Gronked

1. adj. Broken. “The teletype scanner was gronked, so we took the system down. ”
2. Of people, the condition of feeling very tired or (less commonly) sick. “I've been chasing that bug for 17 hours now and I am thoroughly gronked!” Compare broken, which means about the same as gronk used of hardware, but connotes depression or mental/emotional problems in people.

#-Grounding

To place an electric circuit to ground. A ground is a portion of an electric circuit is at zero potential with respect to the earth. (Source Panel of experts).

Group Identification

Group Userid

A USERID snared by numerous authorized users. Also implies sharing of the associated Top Secret password. (JCS PUB 6-03. 7)

***-Grovel**

1. vi. to work interminably and without apparent progress. Often used transitively with `over' or `through'. “The file scavenger has been groveling through the /usr directories for 10 minutes now. ” Compare grind and crunch. Emphatic form `grovel obscenely'.
2. To examine minutely or in complete detail. “The compiler grovels over the entire source program before beginning to translate it. ” “I grovelled through all the documentation, but I still couldn't find the command I wanted. ”

***-Grunge**

1. /gruhnj/ n. That which is grungy, or that which makes it so.
2. [Cambridge] Code which is inaccessible due to changes in other parts of the program. The preferred term in North America is dead code.

Guard

A processor that provides a filter between two systems operating at different security levels or between a user terminal and a data base to filter our data that the user is not authorized to access. (*NCSC-WA*-001-85;)

***-Gubbish**

/guhb'*sh/ n. [a portmanteau of `garbage' and `rubbish'; may have originated with SF author Philip K. Dick] Garbage; nonsense. “What is all this gubbish?” The opposite portmanteau `rubbage' is also reported.

#-Guidelines

This KSA has no definition.

***-Guiltware**

1. /gilt'weir/ n. A piece of freeware decorated with a message telling one how long and hard the author worked on it and intimating that one is a no-good freeloader if one does not immediately send the poor suffering martyr gobs of money.
2. A piece of shareware that works.

***-Gumby**

1. /guhm'bee/ n. [from a class of Monty Python characters, poss. with some influence from the 1960s claymation character] An act of minor but conspicuous stupidity, often in `gumby maneuver' or `pull a gumby'.
2. [NRL] n. A bureaucrat, or other technical incompetent who impedes the progress of real work.
3. adj. Relating to things typically associated with people in sense 2. (e. g. “Ran would be writing code, but Richard gave him gumby work that's due on Friday”, or, “Dammit! Travel screwed up my plane tickets. I have to go out on gumby patrol. ”)

***-Gun**

vt. [ITSfrom the `:GUN' command] To forcibly terminate a program or job (computer, not career). “Some idiot left a background process running soaking up half the cycles, so I gunned it. ” Usagenow rare. Compare can, blammo.

***-Gunch**

/guhnch/ vt. [TMRC] To push, prod, or poke at a device that has almost (but not quite) produced the desired result. Implies a threat to mung.

***-Gurfle**

/ger'fl/ interj. An expression of shocked disbelief. “He said we have to recode this thing in FORTRAN by next week. Gurfle!” Compare weeble.

***-Guru**

n. [UNIX] An expert. Implies not only wizard skill but also a history of being a knowledge resource for others. Less often, used (with a qualifier) for other experts on other systems, as in `VMS guru'. See source of all good bits.

***-Guru Meditation**

n. Amiga equivalent of `panic' in UNIX (sometimes just called a `guru' or `guru event'). When the system crashes, a cryptic message of the form “GURU MEDITATION #XXXXXXXX. YYYYYYYY” may appear, indicating what the problem was. An Amiga guru can figure things out from the numbers. Generally a guru event must be followed by a Vulcan nerve pinch. This term is (no surprise) an in-joke from the earliest days of the Amiga. There used to be a device called a `Joyboard' which was basically a plastic board built onto a joystick-like device; it was sold with a skiing game cartridge for the Atari game machine. It is said that whenever the prototype OS crashed, the system programmer responsible would calm down by concentrating on a solution while sitting cross-legged on a Joyboard trying to keep the board in balance. This position resembled that of a meditating guru. Sadly, the joke was removed in AmigaOS 2. 04 (actually in 2. 00, a buggy post-2. 0 release on the A3000 only).

***-Gweep**

1. /gweep/ [WPI] v. To hack, usually at night. At WPI, from 1977 onwards, one who gweeped coud often be found at the College Computing Center punching cards or crashing the PDP-10 or, later, the DEC-20. The term has survived the demise of those technologies, however, and is still alive in late 1991. “I'm going to go gweep for a while. See you in the morning. ” “I gweep from 8 PM till 3 AM during the week. ”
2. n. One who habitually gweeps in sense 1; a hacker. “He's a hard-core gweep, mumbles code in his sleep. ”

GWEN

See Ground Wave Emergency Network.

Gypsy

A combined formal program specification language and a verifiable high order language, developed at the University of Texas, and designed in conjunction with a complete verification system. (MTR-8201;) See Formal Verification.

Gypsy Verification Environment

A software development methodology which makes use of the Gypsy language, to formally prove design specification and code implementation. Gypsy is a language developed by the University of Texas. (*NCSC-WA*-001-85;)

2. An integrated set of tools for specifying, coding, and verifying programs written in the Gypsy language, a language similar to Pascal which has both specification and programming features. This methology includes an editor, a specification processor, a verification condition generator, a user-directed theorem prover, and an information flow tool.

H

*-H

[from SF fandom] A method of `marking' common words, i. e. , calling attention to the fact that they are being used in a nonstandard, ironic, or humorous way. Originated in the fannish catchphrase “Bheer is the One True Ghod!” from decades ago. H-infix marking of `Ghod' and other words spread into the 1960s counterculture via underground comix, and into early hackerdom either from the counterculture or from SF fandom (the three overlapped heavily at the time). More recently, the h infix has become an expected feature of benchmark names (Dhrystone, Rhealstone, etc.); this is prob. patterning on the original Whetstone (the name of a laboratory) but influenced by the fannish/counterculture h infix.

*-Ha Ha Only Serious

[from SF fandom, orig. as mutation of HHOK, `Ha Ha Only Kidding'] A phrase (often seen abbreviated as HHOS) that aptly captures the flavor of much hacker discourse. Applied especially to parodies, absurdities, and ironic jokes that are both intended and perceived to contain a possibly disquieting amount of truth, or truths that are constructed on in-joke and self-parody. This lexicon contains many examples of ha-ha-only-serious in both form and content. Indeed, the entirety of hacker culture is often perceived as ha-ha-only-serious by hackers themselves; to take it either too lightly or too seriously marks a person as an outsider, a wannabee, or in larval stage. For further enlightenment on this subject, consult any Zen master. See also Humor, Hacker, and AI koans.

*-Hack

1. n. Originally, a quick job that produces what is needed, but not well.
2. n. An incredibly good, and perhaps very time-consuming, piece of work that produces exactly what is needed.
3. vt. To bear emotionally or physically. “I can't hack this heat!”
4. vt. To work on something (typically a program). In an immediate sense “What are you doing?” “I'm hacking TECO. ” In a general (time-extended) sense “What do you do around here?” “I hack TECO. ” More generally, “I hack `foo'“ is roughly equivalent to “`foo' is my major interest (or project)”. “I hack solid-state physics. ” See Hacking X for Y.
5. vt. To pull a prank on. See sense 2 and hacker (sense 5).
6. vi. To interact with a computer in a playful and exploratory rather than goal-directed way. “Whatcha up to?” “Oh, just hacking. ”
7. n. Short for hacker.
8. See nethack.
9. [MIT] v. To explore the basements, roof ledges, and steam tunnels of a large, institutional building, to the dismay of Physical Plant workers and (since this is usually performed at educational institutions) the Campus Police. This activity has been found to be eerily similar to playing adventure games such as Dungeons and Dragons and Zork. See also vadding. Constructions on this term abound. They include `happy hacking' (a farewell), `how's hacking?' (a friendly greeting among hackers) and `hack, hack' (a fairly content-free but friendly comment, often used as a temporary farewell). For more on this totipotent term see “The Meaning of `Hack'”. See also neat hack, real hack.

*-Hack Attack

n. [poss. by analogy with `Big Mac Attack' from ads for the McDonald's fast-food chain; the variant `big hack attack' is reported] Nearly synonymous with hacking run, though the latter more strongly implies an all-nighter.

*-Hack Mode

1. n. What one is in when hacking, of course.
2. More specifically, a Zen-like state of total focus on The Problem that may be achieved when one is hacking (this is why every good hacker is part mystic). Ability to enter such concentration at will correlates strongly with wizardliness; it is one of the most important skills learned during larval stage. Sometimes amplified as `deep hack mode'. Being yanked out of hack mode (see priority interrupt) may be experienced as a physical shock, and the sensation of being in hack mode is more than a

little habituating. The intensity of this experience is probably by itself sufficient explanation for the existence of hackers, and explains why many resist being promoted out of positions where they can code. See also cyberspace (sense 2. . Some aspects of hackish etiquette will appear quite odd to an observer unaware of the high value placed on hack mode. For example, if someone appears at your door, it is perfectly okay to hold up a hand (without turning one's eyes away from the screen) to avoid being interrupted. One may read, type, and interact with the computer for quite some time before further acknowledging the other's presence (of course, he or she is reciprocally free to leave without a word). The understanding is that you might be in hack mode with a lot of delicate state (sense 2. in your head, and you dare not swap that context out until you have reached a good point to pause. See also juggling eggs.

*-Hack On

vt. To hack; implies that the subject is some pre-existing hunk of code that one is evolving, as opposed to something one might hack up.

*-Hack Together

vt. To throw something together so it will work. Unlike `kluge together' or cruft together, this does not necessarily have negative connotations.

*-Hack Up

vt. To hack, but generally implies that the result is a hack in sense 1 (a quick hack). Contrast this with hack on. To `hack up on' implies a quick-and-dirty modification to an existing system. Contrast hacked up; compare kluge up, monkey up, cruft together.

*-Hack Value

n. Often adduced as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack. For example, MacLISP had features for reading and printing Roman numerals, which were installed purely for hack value. See display hack for one method of computing hack value, but this cannot really be explained, only experienced. As Louis Armstrong once said when asked to explain jazz “Man, if you gotta ask you'll never know. ” (Feminists please note Fats Waller's explanation of rhythm “Lady, if you got to ask you ain't got it. ”)

*-Hacked Off

adj. Said of system administrators who have become annoyed, upset, or touchy owing to suspicions that their sites have been or are going to be victimized by crackers, or used for inappropriate, technically illegal, or even overtly criminal activities. For example, having unreadable files in your home directory called `worm', `lockpick', or `goroot' would probably be an effective (as well as impressively obvious and stupid) way to get your sysadmin hacked off at you. It has been pointed out that there is precedent for this usage in U. S. Navy slang, in which officers under discipline are sometimes said to be “in hack” and one may speak of “hacking off the C. O. ”.

*-Hacked Up

adj. Sufficiently patched, kluged, and tweaked that the surgical scars are beginning to crowd out normal tissue (compare critical mass). Not all programs that are hacked become `hacked up'; if modifications are done with some eye to coherence and continued maintainability, the software may emerge better for the experience. Contrast hack up.

Hacker

Originally, a computer enthusiast who spent significant time learning the functions of the computer without benefit of formal training (and often without the technical manuals) by trying combinations of commands at random to determine their effect. Common usage today is from the press which uses the word to describe people who “break into” computers for various purposes. (BBD;)

*-Hacker Ethic, The

1. n. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible.
2. The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality. Both of these normative ethical principles are widely, but by no means universally, accepted among hackers. Most hackers subscribe to the hacker ethic in sense 1, and many act on it by writing and giving away free software. A few go further and assert that *all* information should be free and *any* proprietary control of it is bad; this is the philosophy behind the GNU project. Sense 2 is more controversial some people consider the act of cracking itself to be unethical, like breaking and entering. But the belief that `ethical' cracking excludes destruction at least moderates the behavior of people who see themselves as `benign' crackers (see also samurai). On this view, it may be one of the highest forms of hackerly courtesy to (a) break into a system, and then (b) explain to the sysop, preferably by email from a superuser account, exactly how it was done and how the hole can be plugged -- acting as an unpaid (and unsolicited) tiger team. The most reliable manifestation of either version of the hacker ethic is that almost all hackers are actively willing to share technical tricks, software, and (where possible) computing resources with other hackers. Huge cooperative networks such as Usenet, FidoNet and Internet (see

Internet address) can function without central control because of this trait; they both rely on and reinforce a sense of community that may be hackerdom's most valuable intangible asset.

#-Hackers (and Unauthorized Users)

Originally, “hacker” referred to a computer enthusiast who spends significant time learning the functions of a computer without the benefit of formal training, and often without the technical manuals, by trying combinations of commands at random to determine their effect. Common usage today is from the press, which uses the word to describe “people who break into” computers for various purposes. (Source: NISTIR 4659). An unauthorized user is anyone (or a process acting on someone's) behalf who attempts to gain access or perform an operation on an information technology system that has not been formally granted access to do so. (Source: Panel of Experts, July 1994)

*-Hacking Run

n. [analogy with `bombing run' or `speed run'] A hack session extended long outside normal working times, especially one longer than 12 hours. May cause you to `change phase the hard way' (see phase).

*-Hacking X For Y

n. [ITS] Ritual phrasing of part of the information which ITS made publicly available about each user. This information (the INQUIR record) was a sort of form in which the user could fill out various fields. On display, two of these fields were always combined into a project description of the form “Hacking X for Y” (e. g. , `”Hacking perceptrons for Minsky”'). This form of description became traditional and has since been carried over to other systems with more general facilities for self-advertisement (such as UNIX plan files).

*-Hackintosh

1. n. An Apple Lisa that has been hacked into emulating a Macintosh (also called a `Mac XL').
2. A Macintosh assembled from parts theoretically belonging to different models in the line.

*-Hackish

1. /hak'ish/ adj. (also hackishness n.) Said of something that is or involves a hack.
2. Of or pertaining to hackers or the hacker subculture. See also true-hacker.

*-Hackishness

n. The quality of being or involving a hack. This term is considered mildly silly. Syn. hackitude.

*-Hackitude

n. Syn. hackishness; this word is considered sillier.

*-Hair

n. [back-formation from hairy] The complications that make something hairy. “Decoding TECO commands requires a certain amount of hair. ” Often seen in the phrase `infinite hair', which connotes extreme complexity. Also in `hairiferous' (tending to promote hair growth) “GNUMACS elisp encourages lusers to write complex editing modes. ” “Yeah, it's pretty hairiferous all right. ” (or just “Hair squared!”)

*-Hairball

n. [Fidonet] A large batch of messages that a store-and-forward network is failing to forward when it should. Often used in the phrase “Fido coughed up a hairball today”, meaning that the stuck messages have just come unstuck, producing a flood of mail where there had previously been drought.

*-Hairy

1. adj. Annoyingly complicated. “DWIM is incredibly hairy. ”
2. Incomprehensible. “DWIM is incredibly hairy. ”
3. Of people, high-powered, authoritative, rare, expert, and/or incomprehensible. Hard to explain except in context “He knows this hairy lawyer who says there's nothing to worry about. ” See also hirsute. A well-known result in topology called the Brouwer Fixed-Point Theorem states that any continuous transformation of a surface into itself has at least one fixed point. Mathematically literate hackers tend to associate the term `hairy' with the informal version of this theorem; “You can't comb a hairy ball smooth. ” The adjective `long-haired' is well-attested to have been in slang use among scientists and engineers during the early 1950s; it was equivalent to modern `hairy' senses 1 and 2, and was very likely ancestral to the hackish use. In fact the noun `long-hair' was at the time used to describe a person satisfying sense 3. Both senses probably passed out of use when long hair was adopted as a signature trait by the 1960s counterculture, leaving hackish `hairy' as a sort of stunted mutant relic.

*-HAKMEM

/hak'mem/ n. MIT AI Memo 239 (February 1972). A legendary collection of neat mathematical and programming hacks contributed by many people at MIT and elsewhere. (The title of the memo really is “HAKMEM”, which is a 6-letterism for `hacks memo'.) Some of them are very useful techniques, powerful theorems, or interesting unsolved problems, but most fall into the category of mathematical and computer trivia. Here is a sampling of the entries (with authors), slightly paraphrased Item 41 (Gene Salamin) There are exactly 23,000 prime numbers less than 2^18. Item 46 (Rich Schroeppel) The most *probable* suit distribution in bridge hands is 4-4-3-2, as compared to 4-3-3-3, which is the most *evenly* distributed. This is because the world likes to have unequal numbers a thermodynamic effect saying

things will not be in the state of lowest energy, but in the state of lowest disordered energy. Item 81 (Rich Schroeppel) Count the magic squares of order 5 (that is, all the 5-by-5 arrangements of the numbers from 1 to 25 such that all rows, columns, and diagonals add up to the same number). There are about 320 million, not counting those that differ only by rotation and reflection. Item 154 (Bill Gosper) The myth that any given programming language is machine independent is easily exploded by computing the sum of powers of

2. If the result loops with period = 1 with sign +, you are on a sign-magnitude machine. If the result loops with period = 1 at -1, you are on a twos-complement machine. If the result loops with period greater than 1, including the beginning, you are on a ones-complement machine. If the result loops with period greater than 1, not including the beginning, your machine isn't binary -- the pattern should tell you the base. If you run out of memory, you are on a string or bignum system. If arithmetic overflow is a fatal error, some fascist pig with a read-only mind is trying to enforce machine independence. But the very ability to trap overflow is machine dependent. By this strategy, consider the universe, or, more precisely, algebra Let X = the sum of many powers of 2 = . 111111 (base

2. . Now add X to itself X + X = . 111110. Thus, 2X = X - 1, so X = -1. Therefore algebra is run on a machine (the universe) that is two's-complement. Item 174 (Bill Gosper and Stuart Nelson) 21963283741 is the only number such that if you represent it on the PDP-10 as both an integer and a floating-point number, the bit patterns of the two representations are identical. Item 176 (Gosper) The “banana phenomenon” was encountered when processing a character string by taking the last 3 letters typed out, searching for a random occurrence of that sequence in the text, taking the letter following that occurrence, typing it out, and iterating. This ensures that every 4-letter string output occurs in the original. The program typed BANANANANANANANA. We note an ambiguity in the phrase, “the Nth occurrence of. ” In one sense, there are five 00's in 0000000000; in another, there are nine. The editing program TECO finds five. Thus it finds only the first ANA in BANANA, and is thus obligated to type N next. By Murphy's Law, there is but one NAN, thus forcing A, and thus a loop. An option to find overlapped instances would be useful, although it would require backing up N - 1 characters before seeking the next N-character string. Note This last item refers to a Dissociated Press implementation. See also banana problem. HAKMEM also contains some rather more complicated mathematical and technical items, but these examples show some of its fun flavor.

*-Hakspek

/hak'speek/ n. A shorthand method of spelling found on many British academic bulletin boards and talker systems. Syllables and whole words in a sentence are replaced by single ASCII characters the names of which are phonetically similar or equivalent, while multiple letters are usually dropped. Hence, `for' becomes `4'; `two', `too', and `to' become `2'; `ck' becomes `k'. “Before I see you tomorrow” becomes “b4 i c u 2moro”. First appeared in London about 1986, and was probably caused by the slowness of available talker systems, which operated on archaic machines with outdated operating systems and no standard methods of communication. Has become rarer since. See also talk mode.

Half-Duplex Operation

That mode of operation in which communication between two terminals occurs in either direction, but in only one direction at a time. (~) Note: Half-duplex operation may occur on a half-duplex circuit or on a duplex circuit, but it may not occur on a simplex circuit (def. #1). Synonyms one-way reversible operation, two-way alternate operation. See also circuit, duplex circuit, duplex operation, one-way communication, simplex circuit.

Halftone

Any photomechanical printing surface or the impression therefrom in which detail and tone values are represented by a series of evenly spaced dots in varying size and shape, varying in direct proportion to the intensity of tones they represent. (JCS1-DOD) (JCS1-NATO) See also continuous tone copy, facsimile.

Halftone Characteristic

In facsimile systems, a relationship between the density of the recorded copy and the density of the original copy. (~) Note: The term may also be used to relate the amplitude of the facsimile signal to the density of the original copy or the record copy when only a portion of the system is under consideration. In a frequency modulation system, an appropriate parameter is to be used instead of the amplitude. See also facsimile.

*-Hammer

vt. Commonwealth hackish syn. for bang on.

Hamming Code

An error-detecting and -correcting binary code used in data transmission that can detect all single and double bit errors and can correct all single bit errors. Note: Hamming codes must satisfy $2m \geq n+1$ and $m = n-k$ where n is the number of bits in the block, k is the number of information bits in the block, and m is the number of check bits in the block. See also binary digit, block, code, convolutional code, error-correcting code, error-detecting code.

Hamming Distance

Synonym signal distance (def. #1).

Hamming Weight

The number of non-zero symbols in a symbol sequence. Note: For binary signaling, it is the number of “1” bits in the binary sequence. See also binary code, binary digit, Hamming code.

*-Hamster

1. n. [Fairchild] A particularly slick little piece of code that does one thing well; a small, self-contained hack. The image is of a hamster happily spinning its exercise wheel.
2. A tailless mouse; that is, one with an infrared link to a receiver on the machine, as opposed to the conventional cable.
3. [UK] Any item of hardware made by Amstrad, a company famous for its cheap plastic PC-almost-compatibles.

*-Hand Cruft

vt. [pun on `hand craft'] See cruft, sense 3.

*-Hand-Hacking

1. n. The practice of translating hot spots from an HLL into hand-tuned assembler, as opposed to trying to coerce the compiler into generating better code. Both the term and the practice are becoming uncommon. See tune, bum, by hand; syn. with v. cruft.
2. More generally, manual construction or patching of data sets that would normally be generated by a translation utility and interpreted by another program, and aren't really designed to be read or modified by humans.

*-Hand-Roll

v. [from obs. mainstream slang `hand-rolled' in opposition to `ready-made', referring to cigarettes] To perform a normally automated software installation or configuration process by hand; implies that the normal process failed due to bugs in the configurator or was defeated by something exceptional in the local environment. “The worst thing about being a gateway between four different nets is having to hand-roll a new sendmail configuration every time any of them upgrades. ”

*-Handle

1. n. [from CB slang] An electronic pseudonym; a `nom de guerre' intended to conceal the user's true identity. Network and BBS handles function as the same sort of simultaneous concealment and display one finds on Citizen's Band radio, from which the term was adopted. Use of grandiose handles is characteristic of warez d00dz, crackers, weenies, spods, and other lower forms of network life; true hackers travel on their own reputations rather than invented legendry. Compare nick.
2. [Mac] A pointer to a pointer to dynamically-allocated memory; the extra level of indirection allows on-the-fly memory compaction (to cut down on fragmentation) or aging out of unused resources, with minimal impact on the (possibly multiple) parts of the larger program containing references to the allocated memory. Compare snap (to snap a handle would defeat its purpose); see also aliasing bug, dangling pointer.

Handled

The term “handled by” denotes the activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating and controlling. (DODD 5200. 28;)

Handled By

The term “handled by” denotes the activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating and controlling. (DODD 5200. 28)

Handling Caveats

Handling Restrictions

Handshaking

1. In data communication, a sequence of events governed by hardware or software, requiring mutual agreement of the state of the operational modes prior to change.
2. The process used to establish communications parameters between two stations. (~) Note: Handshaking follows the establishment of a circuit between the stations and precedes information transfer. It is used to agree upon such parameters as information transfer rate, alphabet, parity, interrupt procedure, and other protocol features. See also protocol.

Handshaking Procedure

A dialogue between two entities (e. g. , a user and a computer, a computer and another computer, or a program and another program) for the purpose of identifying and authenticating the entities to one another.

Handshaking Procedures

1. A dialogue between a user and a computer, a computer and another computer, a program and another program for the purpose of identifying a user and authenticating identity. A sequence of questions and answers is used based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue. (*AR* 380-380;; *FIPS PUB* 39;)

2. A dialogue between a user and a computer, or a program and another program for the purpose of identifying a user and authenticating identity. (*NCSC-WA*-001-85;)
3. Synonymous with Password Dialogue.

*-Handwave

[poss. from gestures characteristic of stage magicians]

1. v. To gloss over a complex point; to distract a listener; to support a (possibly actually valid) point with blatantly faulty logic.
2. n. The act of handwaving. “Boy, what a handwave!” If someone starts a sentence with “Clearly. ” or “Obviously. ” or “It is self-evident that. ”, it is a good bet he is about to handwave (alternatively, use of these constructions in a sarcastic tone before a paraphrase of someone else's argument suggests that it is a handwave). The theory behind this term is that if you wave your hands at the right moment, the listener may be sufficiently distracted to not notice that what you have said is bogus. Failing that, if a listener does object, you might try to dismiss the objection with a wave of your hand. The use of this word is often accompanied by gestures both hands up, palms forward, swinging the hands in a vertical plane pivoting at the elbows and/or shoulders (depending on the magnitude of the handwave); alternatively, holding the forearms in one position while rotating the hands at the wrist to make them flutter. In context, the gestures alone can suffice as a remark; if a speaker makes an outrageously unsupported assumption, you might simply wave your hands in this way, as an accusation, far more eloquent than words could express, that his logic is faulty.

*-Hang

1. v. To wait for an event that will never occur. “The system is hanging because it can't read from the crashed drive”. See wedged, hung.
2. To wait for some event to occur; to hang around until something happens. “The program displays a menu and then hangs until you type a character. ” Compare block.
3. To attach a peripheral device, esp. in the construction `hang off' “We're going to hang another tape drive off the file server. ” Implies a device attached with cables, rather than something that is strictly inside the machine's chassis.

*-Hanlon's Razor

prov. A corollary of Finagle's Law, similar to Occam's Razor, that reads “Never attribute to malice that which can be adequately explained by stupidity. ” The derivation of the common title Hanlon's Razor is unknown; a similar epigram has been attributed to William James. Quoted here because it seems to be a particular favorite of hackers, often showing up in sig blocks, fortune cookie files and the login banners of BBS systems and commercial networks. This probably reflects the hacker's daily experience of environments created by well-intentioned but short-sighted people. Compare Sturgeon's Law.

*-Happily

adv. Of software, used to emphasize that a program is unaware of some important fact about its environment, either because it has been fooled into believing a lie, or because it doesn't care. The sense of `happy' here is not that of elation, but rather that of blissful ignorance. “The program continues to run, happily unaware that its output is going to /dev/null. ” Also used to suggest that a program or device would really rather be doing something destructive, and is being given an opportunity to do so. “If you enter a `o' here instead of a zero, the program will happily erase all your data. ”

*-Haque

/hak/ n. [Usenet] Variant spelling of hack, used only for the noun form and connoting an elegant hack. that is a hack in sense 2.

*-Hard Boot

n. See boot.

Hard Copy

In computer graphics or telecommunications, a permanent reproduction of the data displayed or transmitted. The reproduction may be on any media suitable for direct use by a person. (~)
Note 1: Teletypewriter pages, continuous printed tapes, facsimile pages, computer printouts, and radiophoto prints are all examples of hard copy.
Note 2: Magnetic tapes or diskettes or nonprinted punched paper tapes are not hard copy.

Hard Copy Key

Physical keying material, such as printed key lists, punched or printed key tapes, or programmable, read-only memories.

*-Hardcoded

1. adj. Said of data inserted directly into a program, where it cannot be easily modified, as opposed to data in some profile, resource (see de-rezz sense
2. , or environment variable that a user or hacker can easily modify.
3. In C, this is esp. applied to use of a literal instead of a `#define' macro (see magic number).

Hardware

The electric, electronic, and mechanical equipment used for processing data. (DOE 5636. 2A;)
An asset category consisting of the machinery, devices, tools, etc. (RM;)

#-Hardware Asset Management

This KSA has no definition.

Hardware Handshaking

The passing of control characters between two devices such as ACK, NAK, XON, XOFF, for the purpose of controlling the flow of information between the devices. (*AFR* 205-16;)

Hardware Isolation Mechanisms

Hardware Protection Mechanisms

Hardware Security

1. Computer equipment features or devices used in an ADP system to preclude unauthorized data access. (*AR* 380-380;)
2. Equipment features or devices used in an automated information system to preclude unauthorized data access or support a Trusted Computing Base. (*NCSC-WA*-001-85;)

*-Hardwarily

/hard-weir'*-lee/ adv. In a way pertaining to hardware. “The system is hardwarily unreliable. ” The adjective `hardwary' is *not* traditionally used, though it has recently been reported from the U. K. See softwarily.

Hardwire

1. To connect equipment or components permanently in contrast to using switches, plugs, or connectors. (~)
2. The wiring-in of fixed logic or read-only storage that cannot be altered by program changes. (~) See also firmware.

*-Hardwired

1. adj. In software, syn. for hardcoded.
2. By extension, anything that is not modifiable, especially in the sense of customizable to one's particular needs or tastes.

Hardwired Key

Key that is permanently installed.

*-Has The X Nature

[seems to derive from Zen Buddhist koans of the form “Does an X have the Buddha-nature?”] adj. Common hacker construction for `is an X', used for humorous emphasis. “Anyone who can't even use a program with on-screen help embedded in it truly has the loser nature!” See also the X that can be Y is not the true X.

*-Hash Bucket

n. A notional receptacle, a set of which might be used to apportion data items for sorting or lookup purposes. When you look up a name in the phone book (for example), you typically hash it by extracting its first letter; the hash buckets are the alphabetically ordered letter sections. This term is used as techspeak with respect to code that uses actual hash functions; in jargon, it is used for human associative memory as well. Thus, two things `in the same hash bucket' are more difficult to discriminate, and may be confused. “If you hash English words only by length, you get too many common grammar words in the first couple of hash buckets. ” Compare hash collision.

*-Hash Collision

n. [from the techspeak] (var. `hash clash') When used of people, signifies a confusion in associative memory or imagination, especially a persistent one (see thinko). True story One of us [ESR] was once on the phone with a friend about to move out to Berkeley. When asked what he expected Berkeley to be like, the friend replied “Well, I have this mental picture of naked women throwing Molotov cocktails, but I think that's just a collision in my hash tables. ” Compare hash bucket.

Hash Total

The use of specific mathematical formulae to produce a quantity that is (often appended to and) used as a check-sum or validation parameter for the data that it protects. (WB;)

Hashing

Iterative process that computes a value (referred to as a hashword) from a particular data unit in a manner that, when a hashword is protected, manipulation of the data is detectable.

Hashword

See Checksum.

*-Hat

n. Common (spoken) name for the circumflex (`^', ASCII 1011110) character. See ASCII for other synonyms.

Hazard

A measure of both the existence and the compromising nature of an emanation. A hazard exists if and only if compromising emanations are detectable beyond the controlled space.

*-HCF

/H-C-F/ n. Mnemonic for `Halt and Catch Fire', any of several undocumented and semi-mythical machine instructions with destructive side-effects, supposedly included for test purposes on several well-known architectures going as far back as the IBM 360. The MC6800 microprocessor was the first for which an HCF opcode became widely known. This instruction caused the processor to toggle a subset of the bus lines as rapidly as it could; in some configurations this could actually cause lines to burn up.

Head-On Collision

A condition that can occur on a data circuit when two or more nodes seize the circuit at approximately the same instant. Note: This condition may occur on other types of circuits. See also call collision, lockout (def. #4).

Header

The portion of a message that contains information that will guide the message to the correct destination. (~) Note: This information contains such things as the sender's and receiver's addresses, precedence level, routing instructions, and synchronization pulses. See also address field, overhead information.

*-Heads Down

[Sun] adj. Concentrating, usually so heavily and for so long that everything outside the focus area is missed. See also hack mode and larval stage, although this mode is hardly confined to fledgling hackers.

*-Heartbeat

1. n. The signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.
2. A periodic synchronization signal used by software or hardware, such as a bus clock or a periodic interrupt.
3. The `natural' oscillation frequency of a computer's clock crystal, before frequency division down to the machine's clock rate.
4. A signal emitted at regular intervals by software to demonstrate that it is still alive. Sometimes hardware is designed to reboot the machine if it stops hearing a heartbeat. See also breath-of-life packet.

*-Heatseeker

n. [IBM] A customer who can be relied upon to buy, without fail, the latest version of an existing product (not quite the same as a member of the lunatic fringe). A 1993 example of a heatseeker is someone who, owning a 286 PC and Windows 3. 0, goes out and buys Windows 3. 1 (which offers no worthwhile benefits unless you have a 386). If all customers were heatseekers, vast amounts of money could be made by just fixing the bugs in each release (n) and selling it to them as release (n+1).

*-Heavy Metal

n. [Cambridge] Syn. big iron.

*-Heavy Wizardry

1. n. Code or designs that trade on a particularly intimate knowledge or experience of a particular operating system or language or complex application interface. Distinguished from deep magic, which trades more on arcane *theoretical* knowledge. Writing device drivers is heavy wizardry; so is interfacing to X (sense
2. without a toolkit. Esp. found in source-code comments of the form “Heavy wizardry begins here”. Compare voodoo programming.

*-Heavyweight

adj. High-overhead; baroque; code-intensive; featureful, but costly. Esp. used of communication protocols, language designs, and any sort of implementation in which maximum generality and/or ease of implementation has been pushed at the expense of mundane considerations such as speed, memory utilization, and startup time. EMACS is a heavyweight editor; X is an *extremely* heavyweight window system. This term isn't pejorative, but one hacker's heavyweight is another's elephantine and a third's monstrosity. Oppose `lightweight'. Usage now borders on techspeak, especially in the compound `heavyweight process'.

*-Heisenbug

/hi:'zen-buhg/ n. [from Heisenberg's Uncertainty Principle in quantum physics] A bug that disappears or alters its behavior when one attempts to probe or isolate it. (This usage is not even particularly fanciful; the use of a debugger sometimes alters a program's operating environment significantly enough that buggy code, such as that which relies on the values of uninitialized memory, behaves quite differently.) Antonym of Bohr bug; see also mandelbug, schroedinbug. In C, nine out of ten heisenbugs result from uninitialized auto variables, fandango on core phenomena (esp. lossage related to corruption of the malloc arena) or errors that smash the stack.

*-Hello, Sailor!

interj. Occasional West Coast equivalent of hello, world; seems to have originated at SAIL, later associated with the game Zork (which also included “hello, aviator” and “hello, implementor”). Originally from the traditional hooker's greeting to a swabbie fresh off the boat, of course.

*-Hello, Wall!

excl. See wall.

*-Hello, World

1. interj. The canonical minimal test message in the C/UNIX universe.
2. Any of the minimal programs that emit this message. Traditionally, the first program a C coder is supposed to write in a new environment is one that just prints “hello, world” to standard output (and indeed it is the first example program in K&R). Environments that generate an unreasonably large executable for this trivial test or which require a hairy compiler-linker invocation to generate it are considered to lose (see X).
3. Greeting uttered by a hacker making an entrance or requesting information from anyone present. “Hello, world! Is the VAX back up yet?”

Hertz

The frequency of a periodic phenomenon for which the period is one second. (~) Note: The SI unit for frequency, where one hertz corresponds to one cycle per second. See also frequency, SI, spectrum designation of frequency.

Heuristic

A procedure or rule of thumb which reduces the number of steps (applications of IF-THEN rules or primitive knowledge-base operations) required to solve a problem. (ET;)

A procedure or rule of thumb that reduces the number of steps (such as primitive KP operations or applications of production rules) required to solve a problem. (MA;)

*-Hex

1. n. Short for hexadecimal, base 16.
2. A 6-pack of anything (compare quad, sense
3. Neither usage has anything to do with magic or black art, though the pun is appreciated and occasionally used by hackers. True story As a joke, some hackers once offered some surplus ICs for sale to be worn as protective amulets against hostile magic. The chips were, of course, hex inverters.

Hexadecimal

n. Base 16. Coined in the early 1960s to replace earlier `sexadecimal', which was too racy and amusing for stuffy IBM, and later adopted by the rest of the industry. Actually, neither term is etymologically pure. If we take `binary' to be paradigmatic, the most etymologically correct term for base 10, for example, is `denary', which comes from `deni' (ten at a time, ten each), a Latin `distributive' number; the corresponding term for base-16 would be something like `sendenary'. `Decimal' is from an ordinal number; the corresponding prefix for 6 would imply something like `sextidecimal'. The `sexa-' prefix is Latin but incorrect in this context, and `hexa-' is Greek. The word `octal' is similarly incorrect; a correct form would be `octaval' (to go with decimal), or `octonary' (to go with binary). If anyone ever implements a base-3 computer, computer scientists will be faced with the unprecedented dilemma of a choice between two *correct* forms; both `ternary' and `trinary' have a claim to this throne.

*-Hexit

/hek'sit/ n. A hexadecimal digit (0--9, and A--F or a--f). Used by people who claim that there are only *ten* digits, dammit; sixteen-fingered human beings are rather rare, despite what some keyboard designs might seem to imply (see space-cadet keyboard).

*-Hidden Flag

n. [scientific computation] An extra option added to a routine without changing the calling sequence. For example, instead of adding an explicit input variable to instruct a routine to give extra diagnostic output, the programmer might just add a test for some otherwise meaningless feature of the existing inputs, such as a negative mass. The use of hidden flags can make a program very hard to debug and understand, but is all too common wherever programs are hacked on in a hurry.

Hidden Sections

Menu options or entire sub-menus not visible or accessible to a user due to lack of adequate authorization. (BBD;)

Hierarchical Computer Network

A computer network in which processing and control functions are performed at several levels by computers specially suited for the functions performed; e. g. , industrial process control, inventory control, database control, or hospital automation. See also distributed control.

Hierarchical Development Methodology (HDM)

1. A formal specification and verification methodology developed at SRI International. HDM is based on a nonprocedural, state transition specification language, SPECIAL, and provides a security flow analysis tool, MLS, for verifying the multilevel security properties of a user-interface specification. (MTR-8201;)
2. A software development methodology which makes use of the language SPECIAL to formally prove design specifications. SPECIAL is a language developed by SRI International. (*NCSC-WA*-001-85;)

Hierarchically Synchronized Network

A mutually synchronized network in which some clocks exert more control than others, the network operating frequency being a weighted mean of the natural frequencies of the population of clocks. See also democratically synchronized network, master-slave timing, mutually synchronized network, mutual synchronization, oligarchically synchronized network.

*-High Bit

1. n. [from `high-order bit'] 1. The most significant bit in a byte.
2. By extension, the most significant part of something other than a data byte “Spare me the whole saga, just give me the high bit. ” See also meta bit, hobbit, dread high-bit disease, and compare the mainstream slang `bottom line'.

*-High Moby

/hi:' mohb'ee/ n. The high half of a 512K PDP-10's physical address space; the other half was of course the low moby. This usage has been generalized in a

way that has outlasted the PDP-10; for example, at the 1990 Washington D. C. Area Science Fiction Conclave (Disclave), when a miscommunication resulted in two separate wakes being held in commemoration of the shutdown of MIT's last ITS machines, the one on the upper floor was dubbed the `high moby' and the other the `low moby'. All parties involved grokked this instantly. See moby.

High Order Language

Programming languages designed to easily achieve varying degrees of machine independence. HOLs are designed for programming convenience and are intended to more readily communicate procedures to individuals who develop, review, or maintain such procedures. (AF9K_JBC. TXT) (HOL) Programming languages designed to easily achieve varying degrees of machine independence. HOLs are designed for programming convenience and are intended to more readily communicate procedures to individuals who develop, review, or maintain such procedures.

High Risk Environment

Specific location or geographic area where there are insufficient friendly security forces to ensure the safeguarding of information systems security equipment.

High-Level Control

In data transmission, the conceptual level of control or processing logic existing in the hierarchical structure of a primary or secondary station, which level is above the Link Level and upon which the performance of Link Level functions is dependent or is controlled; e. g. , device control, buffer allocation, or station management. See also level (def. #2), Open Systems Interconnection--Reference Model.

High-Level Data Link Control

A link-level protocol used to provide reliable point-to-point transmission of a data packet. Note: A subset of HDLC, known as “LAP-B,” is the layer-two protocol for CCITT Recommendation X. 25. See also Advanced Data Communication Control Procedure, data, data transmission, level, link, Open Systems Interconnection--Reference Model, synchronous data link control, X. -series Recommendations.

High-Level Language

A computer programming language that does not reflect the structure of any one given computer or that of any one given class of computers. A statement in a high-level language must be interpreted and corresponding intermediate, assembly, or machine language statements compiled for use by a computer. (~) Note: Ada® is the DoD high-level language. FORTRAN, BASIC, C, and COBOL are common commercial high-level languages. See also Ada®, assembly language, compile, computer, computer language, computer-oriented language, language, level, machine language.

*-Highly

adv. [scientific computation] The preferred modifier for overstating an understatement. As in `highly nonoptimal', the worst possible way to do something; `highly nontrivial', either impossible or requiring a major research project; `highly nonlinear', completely erratic and unpredictable; `highly nontechnical', drivel written for lusers, oversimplified to the point of being misleading or incorrect (compare drool-proof paper). In other computing cultures, postfixing of in the extreme might be preferred.

*-Hing

// n. [IRC] Fortuitous typo for `hint', now in wide intentional use among players of initgame. Compare newsfroup, filk.

*-Hirsute

adj. Occasionally used humorously as a synonym for hairy.

#-History Of Information Security

This KSA has no definition.

HLL

/H-L-L/ n. [High-Level Language (as opposed to assembler)] Found primarily in email and news rather than speech. Rarely, the variants `VHLL' and `MLL' are found. VHLL stands for `Very-High-Level Language' and is used to describe a bondage-and-discipline language that the speaker happens to like; Prolog and Backus's FP are often called VHLLs. `MLL' stands for `Medium-Level Language' and is sometimes used half-jokingly to describe C, alluding to its `structured-assembler' image.

*-Hobbit

1. n. The High Order Bit of a byte; same as the meta bit or high bit.
2. The non-ITS name of vad@ai. mit. edu (*Hobbit*), master of lasers.

*-Hog

1. n. ,vt. Favored term to describe programs or hardware that seem to eat far more than their share of a system's resources, esp. those which noticeably degrade interactive response. *Not* used of programs that are simply extremely large or complex or that are merely painfully slow themselves (see pig, run like a). More often than not encountered in qualified forms, e. g. , `memory hog', `core hog', `hog the processor', `hog the disk'. “A controller that never gives up the I/O bus gets killed after the bus-hog timer expires. ”
2. Also said of *people* who use more than their fair share of resources (particularly disk, where it seems that 10% of the people use 90% of the disk,

no matter how big the disk is or how many people use it). Of course, once disk hogs fill up one file-system, they typically find some other new one to infect, claiming to the sysadmin that they have an important new project to complete.

*-Hole

n. A region in an otherwise flat entity which is not actually present. For example, some UNIX filesystems can store large files with holes so that unused regions of the file are never actually stored on disk. (In tech-speak, these are referred to as `sparse' files. ) As another example, the region of memory in IBM PCs reserved for memory-mapped I/O devices which may not actually be present is called `the I/O hole', since memory-management systems must skip over this area when filling user requests for memory.

*-Holy Wars

[from Usenet, but may predate it] n. flame wars over religious issues. The paper by Danny Cohen that popularized the terms big-endian and little-endian in connection with the LSB-first/MSB-first controversy was entitled “On Holy Wars and a Plea for Peace”. Other perennial Holy Wars have included EMACS vs. vi, my personal computer vs. everyone else's personal computer, ITS vs. UNIX, UNIX vs. VMS, BSD UNIX vs. USG UNIX, C vs. Pascal, C vs. FORTRAN, etc. , ad nauseam. The characteristic that distinguishes holy wars from normal technical disputes is that in a holy war most of the participants spend their time trying to pass off personal value choices and cultural attachments as objective technical evaluations. See also theology.

*-Home Box

n. A hacker's personal machine, especially one he or she owns. “Yeah? Well, *my* home box runs a full 4. 2 BSD, so there!”

*-Home Machine

1. n. Syn. home box.
2. The machine that receives your email. These senses might be distinct, for example, for a hacker who owns one computer at home, but reads email at work.

*-Hook

n. A software or hardware feature included in order to simplify later additions or changes by a user. For example, a simple program that prints numbers might always print them in base 10, but a more flexible version would let a variable determine what base to use; setting the variable to 5 would make the program print numbers in base 5. The variable is a simple hook. An even more flexible program might examine the variable and treat a value of 16 or less as the base to use, but treat any other number as the address of a user-supplied routine for printing a number. This is a hairy but powerful hook; one can then write a routine to print numbers as Roman numerals, say, or as Hebrew characters, and plug it into the program through the hook. Often the difference between a good program and a superb one is that the latter has useful hooks in judiciously chosen places. Both may do the original job about equally well, but the one with the hooks is much more flexible for future expansion of capabilities (EMACS, for example, is *all* hooks). The term `user exit' is synonymous but much more formal and less hackish.

*-Hop

1. n. One file transmission in a series required to get a file from point A to point B on a store-and-forward network. On such networks (including UUCPNET and FidoNet), an important inter-machine metric is the number of hops in the shortest path between them, which can be more significant than their geographical separation. See bang path.
2. v. To log in to a remote machine, esp. via rlogin or telnet. “I'll hop over to foovax to FTP that. ”

*-Hose

1. vt. To make non-functional or greatly degraded in performance. “That big ray-tracing program really hoses the system. ” See hosed.
2. n. A narrow channel through which data flows under pressure. Generally denotes data paths that represent performance bottlenecks.
3. n. Cabling, especially thick Ethernet cable. This is sometimes called `bit hose' or `hosery' (play on `hosiery') or `etherhose'. See also washing machine.

*-Hosed

adj. Same as down. Used primarily by UNIX hackers. Humorous also implies a condition thought to be relatively easy to reverse. Probably derived from the Canadian slang `hoser' popularized by the Bob and Doug Mackenzie skits on SCTV, but this usage predated SCTV by years in hackerdom (it was certainly already live at CMU in the 1970s). See hose. It is also widely used of people in the mainstream sense of `in an extremely unfortunate situation'. Once upon a time, a Cray that had been experiencing periodic difficulties crashed, and it was announced to have been hosed. It was discovered that the crash was due to the disconnection of some coolant hoses. The problem was corrected, and users were then assured that everything was OK because the system had been rehosed. See also dehose.

Host

1. Computer providing processing power for attached terminals and peripheral devices.
2. Controlling computer of a network.

Host Computer

In a computer network, a computer that provides end users with services such as computation and database access and that usually performs network control functions. (FP) (ISO) Synonym host.

Host To Front-End

Set of conventions governing the protocol format and control of data that is passed from a host to a front-end machine.

Host To Front-End Protocol

A set of conventions governing the format and control of data that are passed from a host to a front-end machine.

Hostile Code

Hostile Cognizant Agent

Person, authorized access to national security information, who intentionally makes that information available to an intelligence service or other group, the goals of which are inimical to the interests of the United States Government or its allies.

#-Hostile Intelligence Sources

A foreign government or quasi government agency that seeks, either overtly or covertly, to gather classified national security and other sensitive information, the disclosure of which could potentially cause grave harm to the national security. These services represent nations whose political and military aims and inimical to those of the United States. (Source panel of experts).

Hostile Threat Environment

An area that contains known threats and possesses little or no control over the surrounding area such as experienced by some diplomatic facilities. (*AFR* 205-16;)

*-Hot Spot

1. n. [primarily used by C/UNIX programmers, but spreading] It is received wisdom that in most programs, less than 10% of the code eats 90% of the execution time; if one were to graph instruction visits versus code addresses, one would typically see a few huge spikes amidst a lot of low-level noise. Such spikes are called `hot spots' and are good candidates for heavy optimization or hand-hacking. The term is especially used of tight loops and recursions in the code's central algorithm, as opposed to (say) initial set-up costs or large but infrequent I/O operations. See tune, bum, hand-hacking.
2. The active location of a cursor on a bit-map display. “Put the mouse's hot spot on the `ON' widget and click the left button. ”
3. A screen region that is sensitive to mouse clicks, which trigger some action. Hypertext help screens are an example, in which a hot spot exists in the vicinity of any word for which additional material is available.
4. In a massively parallel computer with shared memory, the one location that all 10,000 processors are trying to read or write at once (perhaps because they are all doing a busy-wait on the same lock). 5. More generally, any place in a hardware design that turns into a performance bottleneck due to resource contention.

Hot-Standby

Equipment and other information system components that are electrically activated and so configured such that production operations can be quickly and easily switched to such components. (WB;)

*-House Wizard

n. [prob. from ad-agency tradetalk, `house freak'] A hacker occupying a technical-specialist, R&D, or systems position at a commercial shop. A really effective house wizard can have influence out of all proportion to his/her ostensible rank and still not have to wear a suit. Used esp. of UNIX wizards. The term `house guru' is equivalent.

#-Housekeeping Procedures

This KSA has no definition.

*-HP-SUX

/H-P suhks/ n. Unflattering hackerism for HP-UX, Hewlett-Packard's UNIX port, which features some truly unique bogosities in the filesystem internals and elsewhere (these occasionally create portability problems). HP-UX is often referred to as `hockey-pux' inside HP, and one respondent claims that the proper pronunciation is /H-P ukkkhhhh/ as though one were about to spit. Another such alternate spelling and pronunciation is “H-PUX” /H-puhks/. Hackers at HP/Apollo (the former Apollo Computers which was swallowed by HP in 1989) have been heard to complain that Mr. Packard should have pushed to have his name first, if for no other reason than the greater eloquence of the resulting acronym. Compare AIDX, buglix. See also Nominal Semidestructor, Telerat, Open DeathTrap, ScumOS, sun-stools.

*-Huff

v. To compress data using a Huffman code. Various programs that use such methods have been called `HUFF' or some variant thereof. Oppose puff. Compare crunch, compress.

#-Human Intelligence

1. The product resulting from the collection evaluation, analysis, integration and interpretation of agent (covert and overt) information concerning one or more aspects of foreign countries or areas, that is immediately or potentially significant to the

development and execution of plans, policies, and operations. (Source Langley).

2. (HUMINT) A category of intelligence information derived from human sources (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Human Interface Functions

TCB operations that require human intervention or judgement. Untrusted processes would not be able to invoke them. (MTR-8201;)

Human Source

A person who wittingly or unwittingly conveys by any means information of potential intelligence value (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

#-Human Threats

This KSA has no definition.

*-Humma

// excl. A filler word used on various `chat' and `talk' programs when you had nothing to say but felt that it was important to say something. The word apparently originated (at least with this definition) on the MECC Timeshare System (MTS, a now-defunct educational time-sharing system running in Minnesota during the 1970s and the early 1980s) but was later sighted on early UNIX systems. Compare the U. K's wibble.

*-Humor, Hacker

1. n. A distinctive style of shared intellectual humor found among hackers, having the following marked characteristics 1. Fascination with form- vs. -content jokes, paradoxes, and humor having to do with confusion of metalevels (see meta). One way to make a hacker laugh hold a red index card in front of him/her with “GREEN” written on it, or vice-versa (note, however, that this is funny only the first time).
2. Elaborate deadpan parodies of large intellectual constructs, such as specifications (see write-only memory), standards documents, language descriptions (see INTERCAL), and even entire scientific theories (see quantum bogodynamics, computron).
3. Jokes that involve screwily precise reasoning from bizarre, ludicrous, or just grossly counter-intuitive premises.
4. Fascination with puns and wordplay. 5. A fondness for apparently mindless humor with subversive currents of intelligence in it -- for example, old Warner Brothers and Rocky & Bullwinkle cartoons, the Marx brothers, the early B-52s, and Monty Python's Flying Circus. Humor that combines this trait with elements of high camp and slapstick is especially favored. 6. References to the symbol-object antinomies and associated ideas in Zen Buddhism and (less often) Taoism. See has the X nature, Discordianism, zen, ha ha only serious, AI koans. See also filk, retrocomputing, and A Portrait of J. Random Hacker in Appendix B. If you have an itchy feeling that all 6 of these traits are really aspects of one thing that is incredibly difficult to talk about exactly, you are (a) correct and (b) responding like a hacker. These traits are also recognizable (though in a less marked form) throughout science-fiction fandom.

*-Hung

adj. [from `hung up'] Equivalent to wedged, but more common at UNIX/C sites. Not generally used of people. Syn. with locked up, wedged; compare hosed. See also hang. A hung state is distinguished from crashed or down, where the program or system is also unusable but because it is not running rather than because it is waiting for something. However, the recovery from both situations is often the same.

*-Hungry Puppy

n. Syn. slopsucker.

*-Hungus

/huhng'g*s/ adj. [perhaps related to slang `humongous'] Large, unwieldy, usually unmanageable. “TCP is a hungus piece of code. ” “This is a hungus set of modifications. ”

Hybrid Computer

A computer that processes both analog and digital data. (FP)

*-Hyperspace

/hi:'per-spays/ n. A memory location that is *far* away from where the program counter should be pointing, often inaccessible because it is not even mapped in. “Another core dump -- looks like the program jumped off to hyperspace somehow. ” (Compare jump off into never-never land.) This usage is from the SF notion of a spaceship jumping `into hyperspace', that is, taking a shortcut through higher-dimensional space -- in other words, bypassing this universe. The variant `east hyperspace' is recorded among CMU and Bliss hackers.

*-Hysterical Reasons

n. (also `hysterical raisins') A variant on the stock phrase “for historical reasons”, indicating specifically that something must be done in some stupid way for backwards compatibility, and moreover that the feature it must be compatible with was the result of a bad design in the first place. “All IBM PC video adapters have to support MDA text mode for hysterical reasons. ” Compare bug-for-bug compatible.

I

*-I Didn't Change Anything!

interj. An aggrieved cry often heard as bugs manifest during a regression test. The canonical reply to this assertion is “Then it works just the same as it did before, doesn't it?” See also one-line fix. This is also heard from applications programmers trying to blame an obvious applications problem on an unrelated systems software change, for example a divide-by-0 fault after terminals were added to a network. Usually, their statement is found to be false. Upon close questioning, they will admit some major restructuring of the program that shouldn't have broken anything, in their opinion, but which actually hosed the code completely.

*-I See No X Here

Hackers (and the interactive computer games they write) traditionally favor this slightly marked usage over other possible equivalents such as “There's no X here!” or “X is missing. ” or “Where's the X?”. This goes back to the original PDP-10 ADVENT, which would respond in this wise if you asked it to do something involving an object not present at your location in the game.

*-IBM Discount

n. A price increase. Outside IBM, this derives from the common perception that IBM products are generally overpriced (see clone); inside, it is said to spring from a belief that large numbers of IBM employees living in an area cause prices to rise.

*-ICBM Address

n. (Also `missile address') The form used to register a site with the Usenet mapping project includes a blank for longitude and latitude, preferably to seconds-of-arc accuracy. This is actually used for generating geographically-correct maps of Usenet links on a plotter; however, it has become traditional to refer to this as one's `ICBM address' or `missile address', and many people include it in their sig block with that name. (A real missile address would include target altitude.)

*-Ice

n. [coined by Usenetter Tom Maddox, popularized by William Gibson's cyberpunk SF novels a contrived acronym for `Intrusion Countermeasure Electronics'] Security software (in Gibson's novels, software that responds to intrusion by attempting to literally kill the intruder). Also, `icebreaker' a program designed for cracking security on a system. Neither term is in serious use yet as of mid-1993, but many hackers find the metaphor attractive, and each may develop a denotation in the future. In the meantime, the speculative usage could be confused with `ICE', an acronym for “in-circuit emulator”.

*-Idempotent

adj. [from mathematical techspeak] Acting as if used only once, even if used multiple times. This term is often used with respect to C header files, which contain common definitions and declarations to be included by several source files. If a header file is ever included twice during the same compilation (perhaps due to nested #include files), compilation errors can result unless the header file has protected itself against multiple inclusion; a header file so protected is said to be idempotent. The term can also be used to describe an initialization subroutine that is arranged to perform some critical action exactly once, even if the routine is called several times.

Identification

1. The process that enables recognition of a user described to an ADP system. This is generally by the use of unique machine-readable names. (*AR* 380-380;; *NCSC-WA*-001-85;)
2. The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to an ADP system. (*FIPS PUB* 39;)

Identification And Authentication

Identity Token

A smart card, a metal key, or some other physical token carried by a systems user that allows user identity validation. (WB;)

Identity Validation

1. The performance of tests, such as the checking of a password, that enables an information system to recognize users or resources as identical to those previously described to the system. (WB;) The entity (individual or class) from the internal environment that is subject to the peril named in the risk. (ET;)
2. An entity (individual or class) in the internal environment affected by an event. (MK;)
3. See AUTHENTICATE and AUTHENTICATION.

Identity-Based

Identity-Based Security Policy

A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. (SS;)

*-If You Want X, You Know Where To Find It.

There is a legend that Dennis Ritchie, inventor of C, once responded to demands for features resembling those of what at the time was a much more popular language by observing “If you want PL/I, you know

where to find it. ” Ever since, this has been hackish standard form for fending off requests to alter a new design to mimic some older (and, by implication, inferior and baroque) one. The case X = Pascal manifests semi-regularly on Usenet's comp. lang. c newsgroup. Indeed, the case X = X has been reported in discussions of graphics software (see X).

*-Ifdef Out

/if'def owt/ v. Syn. for condition out, specific to C.

*-Ill-Behaved

1. adj. [numerical analysis] Said of an algorithm or computational method that tends to blow up because of accumulated roundoff error or poor convergence properties.
2. Software that bypasses the defined OS interfaces to do things (like screen, keyboard, and disk I/O) itself, often in a way that depends on the hardware of the machine it is running on or which is nonportable or incompatible with other pieces of software. In the IBM PC/MS-DOS world, there is a folk theorem (nearly true) to the effect that (owing to gross inadequacies and performance penalties in the OS interface) all interesting applications are ill-behaved. See also bare metal. Oppose well-behaved, compare PC-ism. See mess-dos.

Imagery

Representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Imagery Intelligence

(IMINT) The products of imagery and photographic interpretation processed for intelligence use (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Imagery Interpretation

(II) The process of locating, recognizing, identifying, and describing objects, activities, and terrain represented by imagery; it includes photographic interpretation (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

*-IMHO

// abbrev. [from SF fandom via Usenet; abbreviation for `In My Humble Opinion'] “IMHO, mixed-case C names should be avoided, as mistyping something in the wrong case can cause hard-to-detect errors -- and they look too Pascalish anyhow. ” Also seen in variant forms such as IMNSHO (In My Not-So-Humble Opinion) and IMAO (In My Arrogant Opinion).

Imitative Communications

Introduction of deceptive messages or deception signals into an adversary's telecommunications signals.

Imitative Communications Deception

Introduction of deceptive messages or signals into an adversary's telecommunications signals. (NSA, *National INFOSEC Glossary*, 10/88) See Communications Deception and Manipulative Communications Deception.

*-Imminent Death Of The Net Predicted!

prov. [Usenet] Since Usenet first got off the ground in 1980-10-81, it has grown exponentially, approximately doubling in size every year. On the other hand, most people feel the signal-to-noise ratio of Usenet has dropped steadily. These trends led, as far back as mid-1983, to predictions of the imminent collapse (or death) of the net. Ten years and numerous doublings later, enough of these gloomy prognostications have been confounded that the phrase “Imminent Death Of The Net Predicted!” has become a running joke, hauled out any time someone grumbles about the S/N ratio or the huge and steadily increasing volume, or the possible loss of a key node or link, or the potential for lawsuits when ignoramuses post copyrighted material, etc. , etc. , etc.

Impact Area 1

Impact Delay Interval

A parameter indicating the length of time that the loss of an asset has no impact. (RM;)

Impact Percent

The average proportion of an asset affected by an event. (MK;)

Impacted Assets

A subset of the asset category involved in a threat which has relevance to a particular event. (RM;)

Impersonating

See Spoofing.

Impersonation

1. An attempt to gain access to a system by posing as an authorized user. (*FIPS PUB* 39;)
2. Synonymous with MASQUERADING and MIMICKING. Also see Spoofing.

Implant

Electronic device or component modification to electronic equipment that is designed to gain unauthorized interception of information-bearing energy via technical means.

#-Implementation (Life Cycle)

The phase of the system development process in which the detailed specifications are translated into actual system components. (Source: *NCSC-TG*-029).

Implementation Verification

The use of verification techniques, usually computer assisted, to demonstrate a mathematical correspon-

dence between a formal specification and its implementation in program code. (MTR-8201;)

Impulsive Emanation

An emanation composed of impulses.

*-In The Extreme

adj. A preferred superlative suffix for many hackish terms. See, for example, `obscure in the extreme' under obscure, and compare highly.

IN/1

A proposed intelligent network targeted toward services that allow increased customer control and that can be provided by centralized switching vehicles serving a large customer base.

IN/1+

A proposed intelligent network targeted toward services that can be provided by centralized switching vehicles, e. g. , access tandems, serving a large customer base.

IN/2

A proposed, advanced intelligent-network concept that extends the distributed IN/1 architecture to accommodate the concept called “service independence. ” Note: Traditionally, service logic has been localized at individual switching systems. The IN/2 architecture provides flexibility in the placement of service logic, requiring the use of advanced techniques to manage the distribution of both network data and service logic across multiple IN/2 modules.

Ina Jo

A software language developed by the Systems Development Corporation used in formal development methodology.

Ina Jo (formal Development Methodology)

System Development Corporation's specification and verification methodology, based on a nonprocedural state-transition specification language, Ina Jo. The Ina Jo methodology incorporates user-supplied invariants to produce a formal demonstration that security properties are met. (MTR-8201;)

Inadvertent

Accidental exposure of information disclosure to a person not authorized access.

Inadvertent Disclosure

Accidental exposure of sensitive defence information to a person not authorized access. This may result in a compromise or a need-to-know violation (*AR* 380-380;) (NSA, *National INFOSEC Glossary*, 10/88) See Failure Access.

*-Inc

/ink/ v. Verbal (and only rarely written) shorthand for increment, i. e. `increase by one'. Especially used by assembly programmers, as many assembly languages have an `inc' mnemonic. Antonymdec.

*-Incantation

n. Any particularly arbitrary or obscure command that one must mutter at a system to attain a desired result. Not used of passwords or other explicit security features. Especially used of tricks that are so poorly documented that they must be learned from a wizard. “This compiler normally locates initialized data in the data segment, but if you mutter the right incantation they will be forced into text space. ”

Incident

See COMPUTER SECURITY INCIDENT

#-Incident Response

This KSA has no definition.

*-Include

1. vt. [Usenet] To duplicate a portion (or whole) of another's message (typically with attribution to the source) in a reply or followup, for clarifying the context of one's response. See the discussion of inclusion styles under “Hacker Writing Style”.
2. [from C] `#include <disclaimer. h>' has appeared in sig blocks to refer to a notional `standard disclaimer file'.

*-Include War

n. Excessive multi-leveled including within a discussion thread, a practice that tends to annoy readers. In a forum with high-traffic newsgroups, such as Usenet, this can lead to flames and the urge to start a kill file.

Incomplete Parameter

AIS design flaw that results when checking all parameters have not been fully anticipated for accuracy and consistency, thus making the system vulnerable to penetration.

Incomplete Parameter Checking

A system fault which exists when all parameters have not been fully checked for accuracy and consistency by the operating system, thus making the system vulnerable to penetration. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

*-Indent Style

n. [C programmers] The rules one uses to indent code in a readable fashion. There are four major C indent styles, described below; all have the aim of making it easier for the reader to visually track the scope of control constructs. The significant variable is the placement of `' and `' with respect to the statement(s) they enclose and to the guard or controlling statement (`if', `else', `for', `while', or `do') on the block, if any.

***-Index**

n. See coefficient of X.

Indicator

An event, observation, or value used to measure an abstract concept An item of information that reflects the intention or capability of a potential enemy to adopt or reject a course of action An action – specific, generalized, or theoretical – that an enemy might be expected to take in preparation for an aggressive act (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Individual

A conceptual entity which the human experts, from which knowledge is being elicited for the purposes of constructing a knowledge base, consider in some sense to be primitive or atomic. (ET;, MA;)

Individual Accountability

The ability to positively associate the identity of a user with the time, method, and degree of access to an Automated Information System. (*NCSC-WA*-001-85;; *AR* 380-380;)

#-Industrial Espionage

The gathering, transmitting, or losing of information with respect to industrial (trade) secrets, with intent or reason to believe that the information is to be used to the injury or a specific company or the United States industry in general, or to the advantage of any foreign nation or foreign nation's industry. (Source Blacks).

#-Industrial Security

Security measures taken to protect a company's or other enterprises proprietary and other trade secrets from competitors and other hostile elements. (Source - panel of experts).

***-Infant Mortality**

n. It is common lore among hackers (and in the electronics industry at large; this term is possibly techspeak by now) that the chances of sudden hardware failure drop off exponentially with a machine's time since first use (that is, until the relatively distant time at which enough mechanical wear in I/O devices and thermal-cycling stress in components has accumulated for the machine to start going senile). Up to half of all chip and wire failures happen within a new system's first few weeks; such failures are often referred to as `infant mortality' problems (or, occasionally, as `sudden infant death syndrome'). See bathtub curve, burn-in period.

Infection

#-Inference

The deduction of confidential information relating to an individual by correlation of statistical evidence relating to a group of individuals. (Source Langley).

#-Inference Engine

A logical inference based mechanism which operates a knowledge base (a set of rules). Inference engines are used in artificial intelligence applications. (Source - *Encyclopedia of Software Eng*).

***-Infinite**

adj. Consisting of a large number of objects; extreme. Used very loosely as in “This program produces infinite garbage. ” “He is an infinite loser. ” The word most likely to follow `infinite', though, is hair. (It has been pointed out that fractals are an excellent example of infinite hair. ) These uses are abuses of the word's mathematical meaning. The term `semi-infinite', denoting an immoderately large amount of some resource, is also heard. “This compiler is taking a semi-infinite amount of time to optimize my program. ” See also semi.

***-Infinite Loop**

n. One that never terminates (that is, the machine spins or buzzes forever and goes catatonic). There is a standard joke that has been made about each generation's exemplar of the ultra-fast machine”The Cray-3 is so fast it can execute an infinite loop in under 2 seconds!”

***-Infinite-Monkey Theorem**

n. “If you put an infinite number of monkeys at typewriters, eventually one will bash out the script for Hamlet. ” (One may also hypothesize a small number of monkeys and a very long period of time.) This theorem asserts nothing about the intelligence of the one random monkey that eventually comes up with the script (and note that the mob will also type out all the possible *incorrect* versions of Hamlet). It may be referred to semi-seriously when justifying a brute force method; the implication is that, with enough resources thrown at it, any technical challenge becomes a one-banana problem. This theorem was first popularized by the astronomer Sir Arthur Eddington. It became part of the idiom of through the classic short story “Inflexible Logic” by Russell Maloney, and many younger hackers know it through a reference in Douglas Adams's “Hitchhiker's Guide to the Galaxy”.

***-Infinity**

1. n. The largest value that can be represented in a particular type of variable (register, memory location, data type, whatever).
2. `minus infinity' The smallest such value, not necessarily or even usually the simple negation of plus infinity. In N-bit twos-complement arithmetic, infinity is 2^(N-1) - 1 but minus infinity is -(2^(N-1)), not -(2^(N-1) - 1). Note also that this is different from “time T equals minus infinity”,

which is closer to a mathematician's usage of infinity.

*-Infix

In translation software written by hackers, infix 2 often represents the syllable *to* with the connotation `translate to' as in dvi2ps (DVI to PostScript), int2string (integer to string), and texi2roff (Texinfo to [nt]roff).

*-Infocom

n. A now-legendary games company, active from 1979 to 1989, that commercialized the MDL parser technology used for Zork to produce a line of text adventure games that remain favorites among hackers. Infocom's games were intelligent, funny, witty, erudite, irreverent, challenging, satirical, and most thoroughly hackish in spirit. The physical game packages from Infocom are now prized collector's items. The software, thankfully, is still extant; Infocom games were written in a kind of P-code and distributed with a P-code interpreter core, and freeware emulators for that interpreter have been written to permit the P-code to be run on platforms the games never originally graced.

Information

1. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. (A-130;; DODD 5200. 28;)
2. The terms “data”, “information”, “material”, “documents”, and “matter” are considered synonymous and used interchangeably in this order. They refer to all data regardless of its physical form (e. g. , data on paper printouts, tapes, disks or disk packs, in memory chips, random access memory (RAM), in read only memory (ROM), microfilm or microfiche, on communication lines, and on display terminals). (DOE 5636. 2A;)
3. Unevaluated material of every description, at all levels of reliability, and from any source that may contain intelligence information (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89).
4. Any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. (EO 12356; DOE 5635. lA)
5. Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium. (DODD 5200. 28)
6. The end product of communication. (NACSEM 5100)
7. See Data

Information And Indicator Sources

In the context of perception management and its constituent approaches: Material, data, and actions that provide information and indicators The sources are categorized as follows:

1. Secret Sources Friendly personnel, documents, material, etc. , possessing classified or sensitive information;
2. Open Sources Overt contacts between people or oral, documentary, pictorial, and physical materials accessible by the public;
3. Detectable Actions Physical actions or entities that can be observed, imaged, or detected by human senses or by active and passive technical sensors Also includes emissions that can be interpreted (JCS MOP 199, 3/89)

#-Information Availability

The computer security characteristic that makes sure the computer resources are available to authorized users when they need them. This characteristic protects against denial of service. (Source: NISTIR 4659).

Information Bit

See user information bit.

#-Information Categorization

This KSA has no definition.

Information Channel

Path through which information actually flows within and external to an organization, project, program, activity, or operation.

#-Information Classification

A determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made. Data classification is used along with categories in the calculation of risk index. (Source: NISTIR 4659).

Information Collection

Information Collection And Sharing

#-Information Confidentiality

1. The computer security characteristic that makes sure individuals are given access to computer resources based on security clearance and need-to-know. This characteristic protects against compromise and inadvertent disclosure.
2. A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for individuals or organizations.

3. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. (NISTIR 4659).

Information Control

A procedure to ensure that information transfers within a system be made from a higher security level object to an object of a lower security level. (*NCSC-WA*-001-85;)

#-Information Criticality

A measure of how important the correct and uninterrupted functioning of the system is to national security, human life or safety, or the mission of the using organization; the degree to which the system performs critical processing. (Source: NISTIR 4659).

Information Feedback

The sending of data back to a source, usually for the purpose of checking the accuracy of transmission of data, the received data being returned to the sending end for comparison with the original data. See also echo check, feedback, forward error correction.

Information Field

In data transmission, a field assigned to contain user information. Note: The contents of the information field are not interpreted at the link level. See also data transmission, Open Systems Interconnection--Reference Model, user information bit.

Information Flow

Procedure to ensure that information control transfers within an AIS are not made from a higher security level object to an object of a lower security level.

Information Flow Analysis

Tracing the flow of specific information types through an information system to determine whether the controls applied to this information are appropriate. (WB;)

Information Flow Control

1. A procedure to ensure that information transfers within a system are not made from a higher security level object to an object of a lower security level. See Covert Channel, Simple Security Property, and Star Property (*-property).
2. Synonymous with DATA FLOW CONTROL and FLOW CONTROL.

#-Information Integrity

A characteristic that ensures computer resources operate correctly and that the data in the data bases are correct. This characteristic protects against deliberate or inadvertent unauthorized manipulations. This characteristic is applicable to hardware, software, firmware, and the data bases used by the system. (Source: NISTIR 4659).

Information Label

Piece of information that accurately and completely represents the sensitivity of the data in a subject or object. NOTE: Information label consists of a security label as well as other required security markings (e. g. , codewords, dissemination control markings, and handling caveats), to be used for data information security labeling purposes. See Label.

#-Information Ownership

This KSA has no definition.

Information Perishability

See Intelligence Life.

Information Processing

Synonym data processing.

Information Processing Center

A facility staffed and equipped for processing and distributing information. (~) Note: An IPC may be geographically distributed.

Information Ratio

(IR) A measure of the amount of information which can be derived from a detected signal. It is the ratio of the amount of information contained in a signal to the amount of information necessary for 100 percent recovery of plaintext information.

Information Resource Management

The process of managing all hardware, software, data and information assets of an organization. [CDS]

#-Information Resource Owner/Custodian

This KSA has no definition.

#-Information Resources Management

Planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology. (Source: *OMB Circular A-130*).

Information Security

1. The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute. (*DOD* 5200. I-R)
2. An Automated Information System and communication security system of administrative policies and procedures for identifying, controlling, and protecting information from unauthorized disclosure. (*NCSC-WA*-001-85;)
3. (INFOSEC) The discipline covering the protection of classified national security information by the application of the rules and procedures established by Executive Order. *
4. The discipline covering the protection of classified national security information by the application of the rules and procedures established by Executive

Order 12356 It includes classification, declassification, marking, mandatory review, oversight, etc The procedures pertaining to both communications security and computer security (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

#-Information Security Policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (Source: *NCSC-TG*-004).

#-Information Sensitivity

The relative worth of information to an organization that claims ownership. Identifying the sensitivity of information is the first step in planning for and developing a secure system. (Source: Panel of Experts, July 1994).

Information Source

Synonym source user.

#-Information States

This KSA has no definition.

Information System

1. (IS) Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.
2. Person responsible to the designated security officer approving authority who ensures that security of an information system is implemented through its design, development, operation, maintenance, and secure disposal stages.
3. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. (A-130;; DODD 5200. 28;) See Automated Information System (AIS). (F:\NEWDEFS. TXT) Any telecommunications and/or computer related equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. See Automated Information System (AIS).

Information System Abuse

Willful or negligent activity that affects the availability, confidentiality, or integrity of information systems resources. Includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation. (*AFR* 700-10;)

Information System Security

Information System Security Officer

The Automated Information System Security Officer (ISSO). The title and the division of duties varies between agencies. In this assessment form the term ISSO is intended to apply to the person(s) responsible for automated information security for the information center(s) and Information System(s). The title could be ISSO, ADPSO, ADPSSO, Security Administrator, OISSO, CESSO, CSSO, etc. (GAO;) () (ISSO) Person responsible to the designated approving authority who ensures that security of an information system is implemented through its design, developement, operation, maintenance, and secure disposal stages. See Computer Security Officer (CSO) and Network Security Officer (NSO).

Information Systems

1. The protection of information systemssecurity (INFOSEC) against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.
2. Item (chip, module, assembly, or security product equipment), technique, or service that performs or relates to information systems security. (Abbreviation - IS)

Information Systems Security

1. (INFOSEC) The protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and information contained within the systems. Such protection is the application of the combination of all security disciplines which will, at a minimum, include COMSEC, TEMPEST, computer security, OPSEC, information security, personnel security, industrial security, resource protection, and physical security. (*AFR* 700-10;)
2. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.
3. The protection afforded information systems in order to preserve the availability, integrity, and confidentiality of the systems and the information they contain. *The protection afforded information systems in order to preserve the availability, integrity, and confidentiality of the systems and the information contained within the systems Such protection is the application of the combination of

tection is the application of the combination of all security disciplines that will at a minimum include: COMSEC, TEMPEST, COMPUSEC, personnel security, industrial security, resource protection, and physical security (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89) (NOTE: Others define this as INFOSEC. See Telecommunications and Automated Information Systems Security (TAISS)), Computer Security (COMPUSEC), Computer Security

#-Information Systems Security Officer

The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal. (Source: DoD Dir 5200. 28).

Information Systems Security Product

Item (chip, module, assembly, or equipment), technique, or service that performs or relates to information systems security.

Information Systems Security Products And Services Catalogue

A catalogue issued quarterly by the National Security Agency that incorporates the DPL, EPL, ETL, PPL and other security product and service lists. This catalogue is available through the U. S. Government Printing Office, Washington, DC 20402, (202) 783-3238.

Information Technology

The hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, or others. Automatic data processing and telecommunications activities related to certain critical national security missions as defined in 44 U. S. C. 3502 (2) and 10 U. S. C. 2315 are excluded. (A-130;)

Information Technology Facility

An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. (A-130;)

Information Technology Installation

One or more computer or office automation systems including related telecommunications, peripheral and storage units, central processing units, and operating and support system software. Information technology installations may range from information technology facilities such as large centralized computer centers to individual stand-alone microprocessors such as personal computers. (A-130)

Information Transfer

The process of moving messages containing user information from a source to a sink. (~) Note: The information transfer rate may or may not be equal to the transmission modulation rate. See also information-bearer channel, information-transfer transaction, isochronous burst transmission.

#-Information Valuation

This KSA has no definition.

Information-Transfer Phase

In an information-transfer transaction, the phase during which user information blocks are transferred from the source user to a destination user. See also access phase, disengagement phase, information-transfer transaction, phase, successful disengagement.

Information-Transfer Transaction

A coordinated sequence of user and telecommunication system activities whose ultimate purpose is to cause user information present at a source user to become present at a destination user. Note: An information-transfer transaction is typically divided into three consecutive phases: the access phase, the information-transfer phase, and the disengagement phase. See also access phase, disconnect, disconnect signal, disengagement attempt, disengagement phase, information transfer, information-transfer phase.

Initial Cost

A parameter indicating the original amount paid to obtain the asset. (RM;)

Initial Product Assessment Report

Unknown

Initial State

The state of the system under analysis prior to the occurrence of any event. (MK;)

Initialize

Setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

Input

1. Pertaining to a point in a device, process, or channel, which point accepts data.
2. An input state, or a sequence of states. (FP) See also input data.

Input Data

1. Data being received or to be received by a device or a computer program. (FP)
2. Data to be processed. (FP)

Input-Output Channel

[For a computer,] A device that handles the transfer of data between internal memory and peripheral equipment. (FP) (ISO)

Input-Output Controller

A functional unit that controls one or more input-output channels. (FP) (ISO) Synonym I/O controller. (FS1037S1. TXT) (IOC) A functional unit that controls one or more input-output channels. (FP) (ISO) See I/O controller.

Input/output Device

(I/O) A device that introduces data into or extracts data from a system. (~) See also terminal.

*-Insanely Great

adj. [Mac community, from Steve Jobs; also BSD UNIX people via Bill Joy] Something so incredibly elegant that it is imaginable only to someone possessing the most puissant of hacker-natures.

Inspectable Space

The three-dimensional space surrounding equipment that process classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation existsA CTTA shall determine the Inspectable Space.

Instruction

In a programming language, an expression that specifies one operation and identifies its operands, if any. (FP) (ISO) See also operand, operation.

Instruction Processor

Instrumentation Signals Intelligence

(ISINT) Intelligence information derived from interception of instrumentation signals.

#-Insurance

Is a contract whereby, for a stipulated consideration, one party undertakes to compensate the other for loss on a specified subject by specified perils. (Source - Blacks).

Integrated Digital Network

A network employing both digital transmission and digital switching. See also Integrated Services Digital Network. (FS1037S1. TXT) (IDN) A network employing both digital transmission and digital switching. See also Integrated Services Digital Network.

Integrated Services Digital Network

Standardized operating parameters and interfaces for a network that will allow mixed digital transmission services (audio, video, and data) simultaneously. (AF9K_JBC. TXT) (ISDN) An integrated digital network in which the same time-division switches and digital transmission paths are used to establish connections for different services. Note 1: Such services include telephone, data, electronic mail, and facsimile. Note 2: How a connection is accomplished is often specified. For example, switched connection, nonswitched connection, exchange connection, ISDN connection. See also communications, electronic mail, integrated digital network.

Integrated Station

A terminal device in which a telephone and one or more other devices, such as a video display unit, keyboard, or printer, are integrated into one unit and used over a single circuit.

Integrated System

A telecommunication system that transfers analog and digital traffic over the same switched network. (~) See also communications system, hybrid communication network, network.

Integrated Voice Data Terminal

See integrated station. (FS1037S1. TXT) (IVDT) See integrated station.

Integrity

1. That computer security characteristic that ensures that computer resources operate correctly and that the data in the data bases are correct. This characteristic protects against deliberate or inadvertent unauthorized manipulation of the system and ensures and maintains the security of entities of a computer system under all conditions. (*AFR* 205-16;)
2. The quality or state of being unimpaired; soundness. a) The capability of an automated system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. b) Inherent quality of protection that ensures and maintains the security of entities of a computer system under all conditions. (*AR* 380-380;)
3. The assurance, under all conditions, that a system will reflect the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection mechanisms; and the consistency of the data structures and accuracy of the stored data. In a formal security model, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (MTR-8201;)
4. The capability of an Automated Information System to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Inherent quality of protection that ensures and maintains the security of entities of an Automated Information System. (*NCSC-WA*-001-85;)
5. See DATA INTEGRITY and SYSTEM INTEGRITY.

Integrity Check Value

Checksum that is capable of detecting malicious modification of an AIS.

INTEGRITY:D1

INTEGRITY:D2

#-Intellectual Property Rights

Right to that body of knowledge, ideas , or concepts produced by an entity which is claimed by that entity to be original and of copyright-type quality. (Source: DACUM IV).

Intelligence

1. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas which is immediately or potentially significant to the development and execution of plans, policies, and operations. (DODD 5200. 28M;)
2. A compilation and analysis of data provided by any/all source(s) that could provide a picture of intentions, capabilities, or activities. *The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of collected information. (Definition #3, *IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89) *The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas (JCS PUB 1-02, 12/89)

Intelligence Collection

Acquisition of information or intelligence information and the provision of this to processing and/or production elements.

Intelligence Cycle

The direction and planning by which information is collected, processed, intelligence produced, and disseminated. *The processes by which information is acquired and converted into intelligence and made available to customers There are usually five steps in the cycle:

1. Planning and Direction. Determination of intelligence requirements, preparation of a collection plan, issuance of orders, and requests to information collection entities, and a continuous check on the productivity of collection entities;
2. Collection. Acquisition of information or intelligence information and the provision of information to processing and/or production elements;
3. Processing. Conversion of collected information and/or intelligence information into a form more suitable for the production of intelligence;
4. Production. Conversion of information or intelligence information into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated customer requirements;
5. Dissemination. Timely conveyance of intelligence in suitable form to customers (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Intelligence Estimate

Intelligence product that predicts the degree of likelihood of possible future events, developments, and/or courses of action and their implications and consequences. *The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption (JCS PUB 1-02, 12/89)

Intelligence Information

Classified information defined as intelligence information by Director of Central Intelligence Directive 1/16. (DOE 5636. 2A;)

Intelligence Life

Length of time during which information has value Synonymous with Information Perishability. *The length of time during which information remains important enough to protect (NSA, *National INFOSEC Glossary*, 10/88)

Intelligence Processing

Conversion of collected information and/or intelligence information into a form more suitable for the production of intelligence.

Intelligence Production

Conversion of material into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated customer requirements.

Intelligence System

Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action The term is not limited to intelligence organizations or services, but includes any system, in all its parts, that accomplishes the listed tasks (JCS PUB 3-54, 9/89)

Intelligent Network

A network that allows functionality to be distributed flexibly at a variety of nodes on and off the network and allows the architecture to be modified to control the services; [in North America] an advanced network concept that is envisioned to offer such things as (a) distributed call-processing capabilities across multi-

ple network modules, (b) real-time authorization code verification, (c) one-number services, and (d) flexible private network services [including (1) reconfiguration by subscriber, (2) traffic analyses, (3) service restrictions, (4) routing control, and (5) data on call histories]. Levels of IN development are identified below:--IN/1 A proposed intelligent network targeted toward services that allow increased customer control and that can be provided by centralized switching vehicles serving a large customer base. --IN/1+ A proposed intelligent network targeted toward services that can be provided by centralized switching vehicles, e. g. , access tandems, serving a large customer base. --IN/2 A proposed, advanced intelligent-network concept that extends the distributed IN/1 architecture to accommodate the concept called "service independence. " Note: Traditionally, service logic has been localized at individual switching systems. The IN/2 architecture provides flexibility in the placement of service logic, requiring the use of advanced techniques to manage the distribution of both network data and service logic across multiple IN/2 modules. (FS1037S1. TXT) (IN) A network that allows functionality to be distributed flexibly at a variety of nodes on and off the network and allows the architecture to be modified to control the services; [in North America] an advanced network concept that is envisioned to offer such things as (a) distributed call-processing capabilities across multiple network modules, (b) real-time authorization code verification, (c) one-number services, and (d) flexible private network services [including (1) reconfiguration by subscriber, (2) traffic analyses, (3) service restrictions, (4) routing control, and (5) data on call histories]. Levels of IN development are identified below:

Intelligent Peripheral

1. Functional components that may be used most efficiently when accessed locally.
2. An intelligent-network feature that provides specialized telecommunication capabilities required by IN/2 service logic programs. See also intelligent network (FS1037S1. TXT) (IP) 1. Functional components that may be used most efficiently when accessed locally.
3. An intelligent-network feature that provides specialized telecommunication capabilities required by IN/2 service logic programs. See also intelligent network

Intelligent Terminal

A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics. (DODD 5200. 28)

Intention

An aim or design (as distinct from capability) to execute a specific course of action (JCS PUB 1-02, 12/89)

Intentional

A form of an event, contrasted with accidental, indicating that a malicious agent is involved in its realization. (RM;)

Interactive Computing

Use of a computer such that the user is in control and may enter data or make other demands on the system which responds by the immediate processing of user requests and returning appropriate replies to these requests. (*FIPS PUB* 39;)

Interactive Data Transaction

A single (one-way) message, transmitted via a data channel, to which a reply is required in order for work to proceed logically. See also data transmission.

Interagency Sharing Of Information Technology Facilities

*-INTERCAL

/in't*r-kal/ n. [said by the authors to stand for `Compiler Language With No Pronounceable Acronym'] A computer language designed by Don Woods and James Lyons in 1972. INTERCAL is purposely different from all other computer languages in all ways but one; it is purely a written language, being totally unspeakable. An excerpt from the INTERCAL Reference Manual will make the style of the language clear It is a well-known and oft-demonstrated fact that a person whose work is incomprehensible is held in high esteem. For example, if one were to state that the simplest way to store a value of 65536 in a 32-bit INTERCAL variable is DO 1 <- #0$#256 any sensible programmer would say that that was absurd. Since this is indeed the simplest method, the programmer would be made to look foolish in front of his boss, who would of course have happened to turn up, as bosses are wont to do. The effect would be no less devastating for the programmer having been correct. INTERCAL has many other peculiar features designed to make it even more unspeakable. The Woods-Lyons implementation was actually used by many (well, at least several) people at Princeton. The language has been recently reimplemented as C-INTERCAL and is consequently enjoying an unprecedented level of unpopularity; there is even an alt. lang. intercal newsgroup devoted to the study and . appreciation of the language on Usenet.

Interdiction

1. The act of impeding or denying the use of system resources to a user. (*FIPS PUB* 39;; *AR* 380-380;)
2. See Denial of Service.

*-Interesting

adj. In hacker parlance, this word has strong connotations of `annoying', or `difficult', or both. Hackers relish a challenge, and enjoy wringing all the irony possible out of the ancient Chinese curse “May you live in interesting times”. Oppose trivial, uninteresting.

Interface

The common boundary between independent systems or modules where communications take place. (MTR-8201;)

Interim Approval

1. The temporary authorization granted an information system to process sensitive or critical information in its operational environment based on preliminary results of a comprehensive security evaluation of the information system. (*AFR* 700-10;; *NCSC-WA*-001-85;)
2. Temporary authorization granted by a designated approving authority for an AIS to process classified information and information governed by 10 U. S. C. Section 2315 or 44 U. S. C. 3502
3. in its operational environment based on preliminary results of a security evaluation of the system.

Interim Approval To Operate

Internal Control Documentation

Written policies, organization charts, procedural write-ups, manuals, memoranda, flow charts, decision tables, completed questionnaires, software, and related written materials used to describe the internal control methods and measures, to communicate responsibilities and authorities for operating such methods and measures, and to serve as a reference for persons reviewing the internal controls and their functioning. (A-123;; DODD 7040. 6;)

Internal Control Report

Internal Control Review

A detailed examination of internal control to determine whether adequate control measures exist and are implemented to prevent or detect the occurrence of potential risks in a cost effective manner. (A-123;; DODD 7040. 6;)

Internal Control System

The totality of the methods and measures of internal control. (A-123;; DODD 7040. 6;)

Internal Controls

The plan of organization and all of the methods and measures adopted within an agency to safeguard its resources, assure the accuracy and reliability of its information, assure adherence to applicable laws, regulations and policies, and promote operational economy and efficiency. (A-123;; DODD 7040. 6;)

#-Internal Controls And Security

Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices). (Source: *NCSC-TG*-0004).

Internal Label

Marking of an item of information, to reflect the classification and sensitivity of the information, within the confines of the media containing the information. See External Label and Label.

Internal Memory

See internal storage.

Internal Protected Distribution System

That portion of a protected distribution system located entirely within a controlled access area (CAA). (NACSIM 5203)

Internal Security Audit

A security audit conducted by personnel responsible to the management of the organization being audited. (*FIPS PUB* 39;)

Internal Security Controls

Hardware, firmware, and software features within an automated system that restrict access to resources (hardware, software, and data) to only authorized subjects (persons, programs, or devices). Controls will also provide limit checks, reasonability checks, and so forth. (*AFR* 205-16;; *NCSC-WA*-001-85;)

Internal Storage

Storage that is accessible by a processor without the use of input-output channels. Note: It includes main storage, and may include other kinds of storage, such as cache memory and special registers, that can be accessed by the processor. (FP) (ISO) Synonym internal memory.

#-International Espionage

Is the crime of “gathering, transmitting, or losing” information respecting the national defense with intent or reason to believe that the information is to be sued to the injury of the United States, or to the advantage of any foreign nation. (Source Blacks).

#-International Security Considerations

This KSA has no definition.

*-Internet Address

1. n. [techspeak] An absolute network address of the form foo@bar. baz, where foo is a user name, bar is a sitename, and baz is a `domain' name, possibly including periods itself. Contrast with bang path;

see also network, the and network address. All Internet machines and most UUCP sites can now resolve these addresses, thanks to a large amount of behind-the-scenes magic and PD software written since 1980 or so. See also bang path, domainist.

2. More loosely, any network address reachable through Internet; this includes bang path addresses and some internal corporate and government networks. Reading Internet addresses is something of an art. Here are the four most important top-level functional Internet domains followed by a selection of geographical domains com commercial organizations edu educational institutions gov U. S. government civilian sites mil U. S. military sites Note that most of the sites in the com and edu domains are in the U. S. or Canada. us sites in the U. S. outside the functional domains su sites in the ex-Soviet Union (see kremvax). uk sites in the United Kingdom Within the us domain, there are subdomains for the fifty states, each generally with a name identical to the state's postal abbreviation. Within the uk domain, there is an ac subdomain for academic sites and a co domain for commercial ones. Other top-level domains may be divided up in similar ways.

Internet Private Line

Network cryptographic unit thatinterfaceprovides secure connections, singularly or in simultaneous multiple connections, between a host and a predetermined set of corresponding hosts.

Internet Private Line Interface

A network cryptographic unit that provides secure connections between a host and a predetermined set of correspondent hosts. It is capable of maintaining a number of connections simultaneously. (*NCSC-WA-*001-85;)

Internet Protocol

(IP) A DoD standard protocol designed for use in interconnected systems of packet-switched computer communication networks. Note: The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small-packet networks. See also block, communications, protocol.

#-Internet Security

This KSA has no definition.

Internet Worm

Internetwork Connection

See gateway.

Internetworking

The process of interconnection of a number of individual networks to provide a path from one network to another network. Note: The networks involved may be of the same type, or they may be of different types; the important thing is that each network is distinct, with its own addresses, internal protocols, access methods, and administration. See also bridge, communications, gateway.

Interoperability

1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (JCS1-DoD) (JCS1-NATO)
2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JCS1-DoD) (~)
3. The ability to exchange data in a prescribed manner and the processing of such data to extract intelligible information which can be used to control/coordinate operations. (JCS Pub. 12, Vol. I, Change I, Information Exchange Planning Guidance [FOUO], May 1979) See also commonality, compatibility, interchangeability, mobile service, mobile station, portability, transportability.

Interoperability Standard

A document that establishes engineering and technical requirements that are necessary to be employed in the design of systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

Interoperation

The use of interoperable systems, units, or forces. (JCS1-DoD)

Interpret

To translate and to execute each source language statement of a computer program before translating and executing the next statement. (FP) (ISO)

Interprocess Communication (IPC)

Communication between two different processes using system-supplied constructs; for example, shared files. (MTR-8201;)

Interrogation

1. The process whereby a signal or combination of signals is intended to trigger a response.
2. The process whereby a station or device requests another station or device to identify itself or to give its status. (~) See also master station.

Interrupt

1. A suspension of a process, such as the execution of a computer program, caused by an event external to that process, and performed in such a way that the process can be resumed. (FP) (ISO)
2. n. On a computer, an event that interrupts normal processing and temporarily diverts flow-of-control through an “interrupt handler” routine. See interruption.

Interrupt Handlers

***-Interrupt List, The**

n. [MS-DOS] The list of all known software interrupt calls (both documented and undocumented) for IBM PCs and compatibles, maintained and made available for free redistribution by Ralf Brown <ralf@cs. cmu. edu>. As of late 1992, it had grown to approximately two megabytes in length.

Interrupted Isochronous Transmission

See isochronous burst transmission.

Interruption

A peril involving the temporary lack of availability of an asset. (RM;)

Interrupts And Traps

(hardware and software)

***-Interrupts Locked Out**

adj. When someone is ignoring you. In a restaurant, after several fruitless attempts to get the waitress's attention, a hacker might well observe “She must have interrupts locked out”. The synonym `interrupts disabled' is also common. Variations abound; “to have one's interrupt mask bit set” and “interrupts masked out” are also heard. See also spl.

Introduction To Certification And Accredidation

#-Intrusion Detection

Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of security logs or audit data. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

#-Intrusion Deterrents

This KSA has no definition.

Investigation

Review and analysis of system security features (e. g. , the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system.

#-Investigation Of Security Breaches

This KSA has no definition.

Investigation(s)

The review and analysis of system security features (e. g. , the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system. (*OPNAVINST* 5239. 1A;; DODD 5200. 28M;)

#-Investigative Authorities

Specifically authorized organizations or individuals who conduct investigations, for example, the Office of the Inspector General.

***-IRC**

/I-R-C/ n. [Internet Relay Chat] A worldwide “party line” network that allows one to converse with others in real time. IRC is structured as a network of Internet servers, each of which accepts connections from client programs, one per user. The IRC community and the Usenet and MUD communities overlap to some extent, including both hackers and regular folks who have discovered the wonders of computer networks. Some Usenet jargon has been adopted on IRC, as have some conventions such as emoticons. There is also a vigorous native jargon, represented in this lexicon by entries marked `[IRC]'. See also talk mode.

***-Iron**

n. Hardware, especially older and larger hardware of mainframe class with big metal cabinets housing relatively low-density electronics (but the term is also used of modern supercomputers). Often in the phrase big iron. Oppose silicon. See also dinosaur.

***-Iron Age**

n. In the history of computing, 1961--1971 -- the formative era of commercial mainframe technology, when ferrite-core dinosaurs ruled the earth. The Iron Age began, ironically enough, with the delivery of the first minicomputer (the PDP-1) and ended with the introduction of the first commercial microprocessor (the Intel 4004) in 1971. See also Stone Age; compare elder days.

***-Iron Box**

n. [UNIX/Internet] A special environment set up to trap a cracker logging in over remote connections long enough to be traced. May include a modified shell restricting the cracker's movements in unobvious ways, and `bait' files designed to keep him interested and logged on. See also back door, firewall machine, Venus flytrap, and Clifford Stoll's account in “The Cuckoo's Egg” of how he made and used one (see the Bibliography in Appendix C). Compare padded cell.

*-Ironmonger

n. [IBM] A hardware specialist (derogatory). Compare sandbender, polygon pusher.

#-IS Program Budgeting

This KSA has no definition.

#-IS Security Program Planning

This KSA has no definition.

Isochronous

1. That characteristic of a periodic signal in which the time interval separating any two corresponding transitions is equal to the unit interval or to a multiple of the unit interval. (~)
2. Pertaining to data transmission in which corresponding significant instants of two or more sequential signals have a constant phase relationship. Note: “Isochronous” and “anisochronous” are characteristics, while “synchronous” and “asynchronous” are relationships. See also anisochronous, asynchronous transmission, heterochronous, homochronous, isochronous burst transmission, isochronous distortion, isochronous modulation, isochronous signal, mesochronous, plesiochronous.

Isochronous Burst Transmission

A transmission process that may be used where the information-bearer channel rate is higher than the input data signaling rate. Note 1: The binary digits are transferred at the information-bearer channel rate, and the transfer is interrupted at intervals in order to produce the required average data signaling rate. Note 2: The interruption is always for an integral number of digit periods. (~) Note 3: The isochronous burst condition has particular application where envelopes are being transmitted and received by the data circuit-terminating equipment, but only the bytes contained within the envelopes are being transferred between data circuit-terminating equipment and the data terminal equipment. Synonyms burst isochronous (deprecated), interrupted isochronous transmission. See also information transfer, isochronous.

Isolation

The containment of users and resources in an automated system in such a way that users and processes are separate from one another as well as from the protection controls of the operating system. (*AR* 380-380;; *FIPS PUB* 39;; *NCSC-WA*-001-85;)

#-Isolation And Mediation

This KSA has no definition.

Isolation Of User Programs

#-IT Asset Valuation

This KSA has no definition.

Items Of Intrinsic Military Utility

End items other than those identified in the *DOD* Militarily Critical Technologies List whose transfer to potential adversaries shall be controlled for the following reasons: a) the end product in question could significantly enhance the recipient's military or war making capability either because of its technology content or because of the quantity to be sold; or b) the product could be analyzed to reveal U. S. system characteristics and thereby contribute to the development of countermeasures to equivalent U. S. equipment. (DODD 2040. 2;)

*-ITS

1. /I-T-S/ n. Incompatible Time-sharing System, an influential but highly idiosyncratic operating system written for PDP-6s and PDP-10s at MIT and long used at the MIT AI Lab. Much AI-hacker jargon derives from ITS folklore, and to have been `an ITS hacker' qualifies one instantly as an old-timer of the most venerable sort. ITS pioneered many important innovations, including transparent file sharing between machines and terminal-independent I/O. After about 1982, most actual work was shifted to newer machines, with the remaining ITS boxes run essentially as a hobby and service to the hacker community. The shutdown of the lab's last ITS machine in May 1990 marked the end of an era and sent old-time hackers into mourning nationwide (see high moby). The Royal Institute of Technology in Sweden is maintaining one `live' ITS site at its computer museum (right next to the only TOPS-10 system still on the Internet), so ITS is still alleged to hold the record for OS in longest continuous use (however, WAITS is a credible rival for this palm).
2. A mythical image of operating-system perfection worshiped by a bizarre, fervent retro-cult of old-time hackers and ex-users (see troglodyte, sense
3. ITS worshipers manage somehow to continue believing that an OS maintained by assembly-language hand-hacking that supported only mono-case 6-character filenames in one directory per account remains superior to today's state of commercial art (their venom against UNIX is particularly intense). See also holy wars, Weenix.

J

*-J. Random

/J rand'm/ n. [generalized from J. Random Hacker] Arbitrary; ordinary; any one; any old. `J. Random' is often prefixed to a noun to make a name out of it. It means roughly `some particular' or `any specific one'. “Would you let J. Random Loser marry your daughter?” The most common uses are `J. Random Hacker', `J. Random Loser', and `J. Random Nerd' (“Should J. Random Loser be allowed to gun down other people?”), but it can be used simply as an elaborate version of random in any sense.

***-J. Random Hacker**

/J rand'm hak'r/ n. [MIT] A mythical figure like the Unknown Soldier; the archetypal hacker nerd. See random, Suzie COBOL. This may originally have been inspired by `J. Fred Muggs', a show-biz chimpanzee whose name was a household word back in the early days of TMRC, and was probably influenced by `J. Presper Eckert' (one of the co-inventors of the electronic computer).

***-Jack In**

v. To log on to a machine or connect to a network or BBS, esp. for purposes of entering a virtual reality simulation such as a MUD or IRC (leaving is "jacking out"). This term derives from cyberpunk SF, in which it was used for the act of plugging an electrode set into neural sockets in order to interface the brain directly to a virtual reality. It is primarily used by MUD and IRC fans and younger hackers on BBS systems.

***-Jaggies**

/jag'eez/ n. The `stairstep' effect observable when an edge (esp. a linear edge of very shallow or steep slope) is rendered on a pixel device (as opposed to a vector display).

#-Jamming

This KSA has no definition.

***-JCL**

1. n. /J-C-L/. IBM's supremely rude Job Control Language. JCL is the script language used to control the execution of programs in IBM's batch systems. JCL has a very fascist syntax, and some versions will, for example, barf if two spaces appear where it expects one. Most programmers confronted with JCL simply copy a working file (or card deck), changing the file names. Someone who actually understands and generates unique JCL is regarded with the mixed respect one gives to someone who memorizes the phone book. It is reported that hackers at IBM itself sometimes sing "Who's the breeder of the crud that mangles you and me? I-B-M, J-C-L, M-o-u-s-e" to the tune of the "Mickey Mouse Club" theme to express their opinion of the beast.
2. A comparative for any very rude software that a hacker is expected to use. "That's as bad as JCL. " As with COBOL, JCL is often used as an archetype of ugliness even by those who haven't experienced it. See also IBM, fear and loathing.

***-JEDR**

// n. Synonymous with IYFEG. At one time, people in the Usenet newsgroup rec. humor. funny tended to use `JEDR' instead of IYFEG or `<ethnic>'; this stemmed from a public attempt to suppress the group once made by a loser with initials JEDR after he was offended by an ethnic joke posted there. (The practice was retconned by the expanding these initials as `Joke Ethnic/Denomination/Race'. ) After much sound and fury JEDR faded away; this term appears to be doing likewise. JEDR's only permanent effect on the net. culture was to discredit `sensitivity' arguments for censorship so thoroughly that more recent attempts to raise them have met with immediate and near-universal rejection.

***-JFCL**

/jif'kl/, /jaf'kl/, /j*-fi'kl/ vt. , obs. (alt. `jfcl') To cancel or annul something. "Why don't you jfcl that out?" The fastest do-nothing instruction on older models of the PDP-10 happened to be JFCL, which stands for "Jump if Flag set and then CLear the flag"; this does something useful, but is a very fast no-operation if no flag is specified. Geoff Goodfellow, one of the jargon-1 co-authors, had JFCL on the license plate of his BMW for years. Usage rare except among old-time PDP-10 hackers.

***-Jiffy**

1. n. The duration of one tick of the system clock on the computer (see tick). Often one AC cycle time (1/60 second in the U. S. and Canada, 1/50 most other places), but more recently 1/100 sec has become common. "The swapper runs every 6 jiffies" means that the virtual memory management routine is executed once for every 6 ticks of the clock, or about ten times a second.
2. Confusingly, the term is sometimes also used for a 1-millisecond wall time interval. Even more confusingly, physicists semi-jokingly use `jiffy' to mean the time required for light to travel one foot in a vacuum, which turns out to be close to one *nanosecond*.
3. Indeterminate time from a few seconds to forever. "I'll do it in a jiffy" means certainly not now and possibly never. This is a bit contrary to the more widespread use of the word. Oppose nano. See also Real Soon Now.

JMSNS

See Justification for Major System New Start.

Job

A unit of work that is defined by a user and that is to be accomplished by a computer. Note: This term is sometimes used to refer to a representation of a job; the representation may include a set of computer programs, files, and control statements to the operating system.

***-Job Security**

n. When some piece of code is written in a particularly obscure fashion, and no good reason (such as time or space optimization) can be discovered, it is often said that the programmer was attempting to increase his job security (i. e. , by making himself indispensable for maintenance). This sour joke seldom has to be said in full; if two hackers are looking over

some code together and one points at a section and says “job security”, the other one may just nod.

Job-Recovery Control File

See backup file.

*-Jock

1. A programmer who is characterized by large and somewhat brute-force programs. See brute force.
2. When modified by another noun, describes a specialist in some particular computing area. The compounds `compiler jock' and `systems jock' seem to be the best-established examples.

*-Joe Code

1. /joh' kohd`/ n. Code that is overly tense and unmaintainable. “Perl may be a handy program, but if you look at the source, it's complete joe code. ”
2. Badly written, possibly buggy code. Correspondents wishing to remain anonymous have fingered a particular Joe at the Lawrence Berkeley Laboratory and observed that usage has drifted slightly; the original sobriquet `Joe code' was intended in sense 1. 1994 update This term has now generalized to `<name> code', used used to designate cose that has distinct characteristics traceable to its author. “This section doesn't check for a NULL return from malloc! Oh! no wonder! It's Ed code!”. Used most often with a programmer who has left the shop and thus is a convenient scapegoat for anything that is wrong with the project.

*-Jolix

n. /joh'liks/ n. ,adj. 386BSD, the freeware port of the BSD Net/2 release to the Intel i386 architecture by Bill Jolitz and friends. Used to differentiate from BSDI's port based on the same source tape, which is called BSD/386. See BSD.

Journal

1. A chronological record of data processing operations that may be used to reconstruct a previous or an updated version of a file. (FP) (ISO) See log.
2. In database management systems, the record of all stored data items whose values are changed as a result of processing and manipulation of the data. (FP)

Joy Stick

In computer graphics, a lever with at least two degrees of freedom that is used as an input unit, normally as a locator. (FP) (ISO)

*-JR

[LN] /J-R-L/, /J-R-N/ n. The names JRL and JRN were sometimes used as example names when discussing a kind of user ID used under TOPS-10 and WAITS; they were understood to be the initials of (fictitious) programmers named `J. Random Loser' and `J. Random Nerd' (see J. Random). For example, if one said “To log in, type log one comma jay are en” (that is, “log 1,JRN”), the listener would have understood that he should use his own computer ID in place of `JRN'.

*-JRST

/jerst/ v. ,obs. [based on the PDP-10 jump instruction] To suddenly change subjects, with no intention of returning to the previous topic. Usage rather rare except among PDP-10 diehards, and considered silly. See also AOS.

*-Juggling Eggs

vi. Keeping a lot of state in your head while modifying a program. “Don't bother me now, I'm juggling eggs”, means that an interrupt is likely to result in the program's being scrambled. In the classic first-contact SF novel “The Mote in God's Eye”, by Larry Niven and Jerry Pournelle, an alien describes a very difficult task by saying “We juggle priceless eggs in variable gravity. ” See also hack mode.

Julian Date

1. The sequential day count, reckoned consecutively from the epoch beginning January 1, 4713 B. C. The Julian date on January 1, 1990, was 2,446,89
2. The true meaning of Julian date has been corrupted in modern times to refer also to an annual day numbering system in which days of the year are numbered in sequence, i. e. , the first day of the year is 001, the second 002, the last day of the year is 365 (366 in leap years). (~) Note: To avoid ambiguity, “day of year” rather than “Julian date” should be used for this purpose. See also Coordinated Universal Time.

*-Jump Off Into Never-Never Land

v. [from J. M. Barrie's “Peter Pan”] Same as branch to Fishkill, but more common in technical cultures associated with non-IBM computers that use the term `jump' rather than `branch'. Compare hyperspace.

*-Jupiter

vt. [IRC] To kill an IRC robot or user and then take its place by adopting its nick so that it cannot reconnect. Named after a particular IRC user who did this to NickServ, the robot in charge of preventing people from inadvertently using a nick claimed by another user.

Justification

See bit stuffing, de-stuffing, justify.

Justify

1. To shift the contents of a register or a field so that the significant character at the specified end of the data is at a particular position. (FP) (ISO)
2. To align text horizontally or vertically so that the first and last characters of every line or the first

and last line of the text are aligned with their corresponding margins. The last line of a paragraph is often not justified. (FP) (ISO)

K

*-K

/K/ n. [from kilo-] A kilobyte. Used both as a spoken word and a written suffix (like meg and gig for megabyte and gigabyte). See quantifiers.

*-K&R

[Kernighan and Ritchie] n. Brian Kernighan and Dennis Ritchie's book "The C Programming Language", esp. the classic and influential first edition (Prentice-Hall 1978; ISBN 0-113-110163-3). Syn. White Book, Old Testament. See also New Testament.

*-K

pref. Extremely. Not commonly used among hackers, but quite common among crackers and warez d00dz in compounds such as `k-kool' /K'-kool'/, `k-rad' /K'-rad'/, and `k-awesome' /K-aw'sm/. Also used to intensify negatives; thus, `k-evil', `k-lame', `k-screwed', and `k-annoying'. Overuse of this prefix, or use in more formal or technical contexts, is consideredan indicator of lamer status.

K&R Style*

Named after Kernighan & Ritchie, because the examples in K&R are formatted this way. Also called `kernel style' because the UNIX kernel is written in it, and the `One True Brace Style' (abbr. 1TBS) by its partisans. The basic indent shown here is eight spaces (or one tab) per level; four spaces are occasionally seen, but are much less common. if (cond) <body>

*-Kahuna

/k*-hoo'n*/ n. [IBMfrom the Hawaiian title for a shaman] Synonym for wizard, guru.

*-Kamikaze Packet

n. The `official' jargon for what is more commonly called a Christmas tree packet. RFC-1025, "TCP and IP Bake Off" says 10 points for correctly being able to process a "Kamikaze" packet (AKA nastygram, christmas tree packet, lamp test segment, et al.). That is, correctly handle a segment with the maximum combination of features at once (e. g. , a SYN URG PUSH FIN segment with options and data). See also Chernobyl packet.

*-Kangaroo Code

n. Syn. spaghetti code.

KEEPER

Knowledge Engineering applied to the Evaluation of Potential Environmental Risks. The supershell to be used for Risk Assessment.

*-Ken

1. /ken/ n. [UNIX] Ken Thompson, principal inventor of UNIX. In the early days he used to hand-cut distribution tapes, often with a note that read "Love, ken". Old-timers still use his first name (sometimes uncapitalized, because it's a login name and mail address) in third-person reference; it is widely understood (on Usenet, in particular) that without a last name `Ken' refers only to Ken Thompson. Similarly, Dennis without last name means Dennis Ritchie (and he is often known as dmr). See also demigod, UNIX.
2. A flaming user. This was originated by the Software Support group at Symbolics because the two greatest flamers in the user community were both named Ken.

Kerberos

#-Kernel

1. The hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. It must mediate all accesses, be protected from modification and be verifiable as correct. (Source: *Orange Book*)
2. An implementation of a reference monitor. See Security Kernel.

Kernelized Secure Operating System

(KSOS) Project to strengthen the UNIX operating system with a security kernel to make it suitable for multilevel operations.

Kernelized VM/370

Kernelized version of IBM's VM/370 for S/370 series architecture, being built by System Development Corporation.

Key

1. in cryptography, a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) which control the operations of encryption and decryption. (*AR* 380-380; *FIPS PUB* 39)
2. A sequence of symbols or their electrical or mechanical equivalents which, in machine or auto-manual cryptosystems, is combined with plain text to produce ciphertext. (Often used informally as a synonym for keying material or cryptovariable). (NCSC-9)
3. A sequence of random binary bits used to initially set up and periodically change the encryption/decryption function in a protection equipment for purposes of the encryption, decryption or authentication of information. (NTISSI 3005)
4. A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text

in order to encrypt or decrypt. Also, an element of the arrangement of a cryptoequipment which must be known before encryption or decryption can be carried out. (NACSEM 5201)

Key Card

Paper card, containing a pattern of punched holes, which establishes the key for a specific cryptonet at a specific time.

#-Key Certificate Administration

This KSA has no definition.

Key Distribution Center

A COMSEC facility that generates and distributes key in electrical form. (~) See also cryptology (def. #2). (FS1037S1. TXT) (KDC)

Key Encrypting Key

A cryptographic key used for encrypting (and decrypting) data encrypting keys or other key encrypting keys. (*FIPS PUB* 112;)

Key Encryption Key

(KEK) Key that encrypts or decrypts other key for transmission or storage. (F:\NEWDEFS. TXT) Key that encrypts or decrypts other key for transmission or storage.

Key Generation

The origination of a key or a set of distinct keys. (*FIPS PUB* 39;; *AR* 380-380;)

Key List

Printed series of key settings for a specific cryptonet. NOTE: Key lists may be produced in list, pad, or printed tape format.

Key Loader

An ancillary device used to transfer, store, or load key into a protection equipment. (NTISSI 3005)

Key Management

1. Specific manual and computer procedures for the generation, dissemination, replacement, storage, archive, and destruction of secret keys that control encryption or authentication processes. (WB;)
2. The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy. (SS;)

Key Management Device

A unit that provides for secure electronic distribution of data encryption keys to authorized users. In the DES case, these keys are essentially 56 bits in a 64 bit block, therefore, 64 bit blocks can be electronically distributed by a key management (trusted) center. (GAO;)

Key Production Key

(KPK) Key that is used to initialize a keystream generator for the production of other electronically generated key. (F:\NEWDEFS. TXT) Key that is used to initialize a keystream generator for the production of other electronically generated keys.

Key Stream

Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.

Key Tag

Identification information associated with certain types of electronic key.

Key Tape

Punched or magnetic tape containing key. NOTE: Printed key in tape form is referred to as a key list.

Key Updating

Irreversible cryptographic process for modifying key automatically or manually.

Key-Auto-Key

(KAK) Cryptographic logic which uses previous key to produce key. (F:\NEWDEFS. TXT) Cryptographic logic which uses previous key to produce key.

Keyboard

An input device used to enter data by manual depression of keys, which causes the generation of the selected code element. (~)

Keyboard Punch

See keypunch.

Keying

The generating of signals by the interruption or modulation of a steady signal or carrier. (~)

Keying Material

Key, code, or authentication information in physical or magnetic form.

Keying Variable

Deprecated synonym for key.

Keypunch

A keyboard-actuated punch that punches holes in a data medium. (FP) (ISO) Synonym keyboard punch.

Keystone Equipment

Includes manufacturing, inspection, or test equipment and is the required equipment for the effective application of technical information and know how. Keystone materials have the same significant application. (DODD 2040. 2;)

#-Keystroke Monitoring

1. A specialized form of audit trail software, or a specially designed device, that records every key

struck by a user and every character of the response that the host computer returns to the suer. Unlike audit trail software that may only record specific events such as long ins, keystroke monitoring software could be used to target specific users or terminals due to suspicious unauthorized activity. Personnel employing keystroke monitoring devices would have the ability to access the contents of users' files. Database management and spreadsheet systems may also perform keystroke monitoring to allow the system to recreate transactions for recovery purposes. This form of keystroke monitoring is generally referred to as journaling. (Source panel of experts).

2. A detailed level of monitoring which assess and records all information generated or received by a particular terminal or computer.

Keyword

See Password.

*-Kgbvax

/K-G-B'vaks/ n. See kremvax.

*-KIBO

1. /ki:'boh/ 1. [acronym] Knowledge In, Bull Out. A summary of what happens whenever valid data is passed through an organization (or person) that deliberately or accidentally disregards or ignores its significance. Consider, for example, what an advertising campaign can do with a product's actual specifications. Compare GIGO; see also SNAFU principle.
2. James Parry <kibo@world. std. com>, a Usenetter infamous for various surrealist net. pranks and an uncanny, machine-assisted knack for joining any thread in which his nom de guerre is mentioned.

*-Kiboze

v. [Usenet] To grep the Usenet news for a string, especially with the intention of posting a follow-up. This activity was popularised by Kibo (see KIBO, sense 2).

*-Kick

v. [IRC] To cause somebody to be removed from a IRC channel, an option only available to CHOPs. This is an extreme measure, often used to combat extreme flamage or flooding, but sometimes used at the chop's whim. Compare gun.

*-Kill File

n. [Usenet] (alt. `KILL file') Per-user file(s) used by some Usenet reading programs (originally Larry Wall's `rn(1)') to discard summarily (without presenting for reading) articles matching some particularly uninteresting (or unwanted) patterns of subject, author, or other header lines. Thus to add a person (or subject) to one's kill file is to arrange for that person to be ignored by one's newsreader in future. By extension, it may be used for a decision to ignore the person or subject in other media. See also plonk.

*-Killer Micro

n. [popularized by Eugene Brooks] A microprocessor-based machine that infringes on mini, mainframe, or supercomputer performance turf. Often heard in "No one will survive the attack of the killer micros!", the battle cry of the downsizers. Used esp. of RISC architectures. The popularity of the phrase `attack of the killer micros' is doubtless reinforced by the movie title "Attack Of The Killer Tomatoes" (one of the canonical examples of so-bad-it's-wonderful among hackers). This has even more flavor now that killer micros have gone on the offensive not just individually (in workstations) but in hordes (within massively parallel computers).

*-Killer Poke

n. A recipe for inducing hardware damage on a machine via insertion of invalid values (see poke) into a memory-mapped control register; used esp. of various fairly well-known tricks on bitty boxes without hardware memory management (such as the IBM PC and Commodore PET) that can overload and trash analog electronics in the monitor. See also HCF.

*-Kilo

pref. [SI] See quantifiers.

*-KIPS

/kips/ n. [abbreviation, by analogy with MIPS using K] Thousands (*not* 1024s) of Instructions Per Second. Usagerare.

*-KISS Principle

/kis' prin'si-pl/ n. "Keep It Simple, Stupid". A maxim often invoked when discussing design to fend off creeping featurism and control development complexity. Possibly related to the marketroid maxim on sales presentations, "Keep It Short and Simple".

*-Kit

n. [Usenet; poss. fr. DEC slang for a full software distribution, as opposed to a patch or upgrade] A source software distribution that has been packaged in such a way that it can (theoretically) be unpacked and installed according to a series of steps using only standard UNIX tools, and entirely documented by some reasonable chain of references from the top-level README file. The more general term distribution may imply that special tools or more stringent conditions on the host environment are required.

*-Klone

/klohn/ n. See clone, sense 4.

*-Kludge

1. /klooj/ n. Incorrect (though regrettably common) spelling of kluge (US). These two words have been confused in American usage since the early 1960s, and widely confounded in Great Britain since the end of World War II.
2. [TMRC] A crock that works. (A long-ago “Datamation” article by Jackson Granholme similarly said “An ill-assorted collection of poorly matching parts, forming a distressing whole. ”)
3. v. To use a kludge to get around a problem. “I've kludged around it for now, but I'll fix it up properly later. ” This word appears to have derived from Scots `kludge' or `kludgie' for a common toilet, via British military slang. It apparently became confused with U. S. kluge during or after World War II; some Britons from that era use both words in definably different ways, but kluge is now uncommon in Great Britain. `Kludge' in Commonwealth hackish differs in meaning from `kluge' in that it lacks the positive senses; a kludge is something no Commonwealth hacker wants to be associated too closely with. Also, `kludge' is more widely known in British mainstream slang than `kluge' is in the U. S.

*-Kluge

1. /klooj/ [from the German `klug', clever] 1. n. A Rube Goldberg (or Heath Robinson) device, whether in hardware or software.
2. n. A clever programming trick intended to solve a particular nasty case in an expedient, if not clear, manner. Often used to repair bugs. Often involves ad-hockery and verges on being a crock.
3. n. Something that works for the wrong reason.
4. vt. To insert a kluge into a program. “I've kluged this routine to get around that weird bug, but there's probably a better way. ”
5. [WPI] n. A feature that is implemented in a rude manner. Nowadays this term is often encountered in the variant spelling `kludge'. Reports from old farts are consistent that `kluge' was the original spelling, reported around computers as far back as the mid-1950s and, at that time, used exclusively of *hardware* kluges. In 1947, the “New York Folklore Quarterly” reported a classic shaggy-dog story `Murgatroyd the Kluge Maker' then current in the Armed Forces, in which a `kluge' was a complex and puzzling artifact with a trivial function. Other sources report that `kluge' was common Navy slang in the WWII era for any piece of electronics that worked well on shore but consistently failed at sea. However, there is reason to believe this slang use may be a decade older. Several respondents have connected it to the brand name of a device called a “Kluge paper feeder”, an adjunct to mechanical printing presses. Legend has it that the Kluge feeder was designed before small, cheap electric motors and control electronics; it relied on a fiendishly complex assortment of cams, belts, and linkages to both power and synchronize all its operations from one motive driveshaft. It was accordingly tempermental, subject to frequent breakdowns, and devilishly difficult to repair -- but oh, so clever! People who tell this story also aver that `Kluge' was the the name of a design engineer. There is in fact a Brandtjen & Kluge Inc. , an old family business that manufactures printing equipment -- interestingly, their name is pronounced /kloo'gee/! Henry Brandtjen, president of the firm, told me (ESR, 1994) that his company was co-founded by his father and an engineer named Kluge /kloo'gee/, who built and co-designed the original Kluge automatic feeder in 1919. Mr. Brandtjen claims, however, that this was a *simple* device (with only four cams); he says he has no idea how the myth of its complexity took hold. TMRC and the MIT hacker culture of the early '60s seems to have developed in a milieu that remembered and still used some WWII military slang (see also foobar). It seems likely that `kluge' came to MIT via alumni of the many military electronics projects that had been located in Cambridge (many in MIT's venerable Building 20, in which TMRC is also located) during the war. The variant `kludge' was apparently popularized by the Datamation article mentioned above; it was titled “How to Design a Kludge” (February 1962, pp. 30, 31). This spelling was probably imported from Great Britain, where kludge has an independent history (though this fact was largely unknown to hackers on either side of the Atlantic before a mid-1993 debate in the Usenet group alt. folklore. computers over the First and Second Edition versions of this entry; everybody used to think kludge was just a mutation of kluge). It now appears that the British, having forgotten the etymology of their own `kludge' when `kluge' crossed the Atlantic, repaid the U. S. by lobbing the `kludge' orthography in the other direction and confusing their American cousins' spelling! The result of this history is a tangle. Many younger U. S. hackers pronounce the word as /klooj/ but spell it, incorrectly for its meaning and pronunciation, as `kludge'. British hackers mostly learned /kluhj/ orally and use it in a restricted negative sense and are at least consistent. European hackers have mostly learned the word from written American sources and tend to pronounce it /kluhj/ but use the wider American meaning! Some observers consider this mess appropriate in view of the word's meaning.

*-Kluge Around

vt. To avoid a bug or difficult condition by inserting a kluge. Compare workaround.

*-Kluge Up

vt. To lash together a quick hack to perform a task; this is milder than cruft together and has some of the connotations of hack up (note, however, that the construction `kluge on' corresponding to hack on is never used). “I've kluged up this routine to dump the buffer contents to a safe place. ”

*-Knights Of The Lambda Calculus

n. A semi-mythical organization of wizardly LISP and Scheme hackers. The name refers to a mathematical formalism invented by Alonzo Church, with which LISP is intimately connected. There is no enrollment list and the criteria for induction are unclear, but one well-known LISPer has been known to give out buttons and, in general, the *members* know who they are.

Know How

Includes both the know how of design and manufacturing and the know how and related technical information that is needed to achieve a significant development, production, or use. The term know how includes services, processes, procedures, specifications, design data and criteria, and testing techniques. (DODD 2040. 2;)

Knowledge Base

A data structure, consisting of a set of frames and a set of association descriptions, that represents (possibly uncertain) knowledge about a universe of discourse. (MA;)

*-Knuth

/knooth/ n. [Donald E. Knuth's “The Art of Computer Programming”] Mythically, the reference that answers all questions about data structures or algorithms. A safe answer when you do not know “I think you can find that in Knuth. ” Contrast literature, the. See also bible.

*-Kremvax

/krem-vaks/ n. [from the then large number of Usenet VAXen with names of the form foovax] Originally, a fictitious Usenet site at the Kremlin, announced on April 1, 1984 in a posting ostensibly originated there by Soviet leader Konstantin Chernenko. The posting was actually forged by Piet Beertema as an April Fool's joke. Other fictitious sites mentioned in the hoax were moskvax and kgbvax. This was probably the funniest of the many April Fool's forgeries perpetrated on Usenet (which has negligible security against them), because the notion that Usenet might ever penetrate the Iron Curtain seemed so totally absurd at the time. In fact, it was only six years later that the first genuine site in Moscow, demos. su, joined Usenet. Some readers needed convincing that the postings from it weren't just another prank. Vadim Antonov, senior programmer at Demos and the major poster from there up to mid-1991, was quite aware of all this, referred to it frequently in his own postings, and at one point twitted some credulous readers by blandly asserting that he *was* a hoax! Eventually he even arranged to have the domain's gateway site *named* kremvax, thus neatly turning fiction into fact and demonstrating that the hackish sense of humor transcends cultural barriers. [Mr. Antonov also contributed the Russian-language material for this lexicon. -- ESR] In an even more ironic historical footnote, kremvax became an electronic center of the anti-communist resistance during the bungled hardline coup of August 1991. During those three days the Soviet UUCP network centered on kremvax became the only trustworthy news source for many places within the USSR. Though the sysops were concentrating on internal communications, cross-border postings included immediate transliterations of Boris Yeltsin's decrees condemning the coup and eyewitness reports of the demonstrations in Moscow's streets. In those hours, years of speculation that totalitarianism would prove unable to maintain its grip on politically-loaded information in the age of computer networking were proved devastatingly accurate -- and the original kremvax joke became a reality as Yeltsin and the new Russian revolutionaries of `glasnost' and `perestroika' made kremvax one of the timeliest means of their outreach to the West.

KVM/370

Kernelized VM/370. The kernelized version of IBM's VM/370 for the S/370 series architecture being built and verified by System Development Corporation. (MTR-8201;)

*-Kyrka

/shir'k*/ n. [Swedish] See feature key.

L

Label

1. A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object. (CSC-STD-004-85;; *NCSC-WA*-001-85;)
2. The marking of an item of information to reflect its classification and its set of categories that represent the sensitivity of the information.
3. Internal Label. The marking of an item of information to reflect the classification and sensitivity of the information within the confines of the medium containing the information.
4. External Label. The visible marking on the outside of the medium or the cover of the medium that reflects the classification and sensitivity of the information resident within the medium. (DOE 5636. 2A;) See External Label, Information Label, Internal Label, Security Label, Security Level, and Sensitivity Label.

Labeled Security Protection

(Class B1) Trusted Computing Base (TCB) which provides elementary-level Mandatory Access Control protection features, as well as intermediate-level Discretionary Access Control features. Sensitivity labels are used to make access control decisions based on an informal security policy model that states the rules for how named subjects (users, programs) may access named objects (files, records).

#-Labeling

1. A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object. (Source Information Security: A Dictionary of Concepts, standards);
2. A means to identify the sensitivity of a unit of information (object) or a process (subject);
3. In a system supporting mandatory access controls, the assignment of sensitivity labels to every subject or object in the system. (CSB+RG-92).

*-Lace Card

n. ,obs. A punched card with all holes punched (also called a `whoopee card' or `ventilator card'). Card readers tended to jam when they got to one of these, as the resulting card had too little structural strength to avoid buckling inside the mechanism. Card punches could also jam trying to produce these things owing to power-supply problems. When some practical joker fed a lace card through the reader, you needed to clear the jam with a `card knife' -- which you used on the joker first.

*-Lamer

n. [prob. originated in skateboarder slang] Synonym for luser, not used much by hackers but common among warez d00dz, crackers, and phreakers. Oppose elite. Has the same connotations of self-conscious elitism that use of luser does among hackers. Crackers also use it to refer to cracker wannabees. In phreak culture, a lamer is one who scams codes off others rather than doing cracks or really understanding the fundamental concepts. In warez d00dz culture, where the ability to obtained cracked commercial software within days of (or before) release to the commercial market is much esteemed, the lamer might try to upload garbage or shareware or something incredibly old (old in this context is read as a few years to anything older than 3 days).

Land Mobile Service

A mobile service between base stations and land mobile stations, or between land mobile stations. (RR)

Land Mobile Station

A mobile station in the land mobile service capable of surface movement within the geographical limits of a country or continent. (RR)

Land Station

A station in the mobile service not intended to be used while in motion. (RR)

Landscape Mode

1. In facsimile, the mode for scanning lines across the longer dimension of a rectangular original.
2. In computer graphics, the orientation of a page in which the longer dimension is horizontal. See also portrait mode.

Language

A set of characters, conventions, and rules that is used for conveying information. (FP) (ISO) (~) See also alphabet.

*-Language Lawyer

n. A person, usually an experienced or senior software engineer, who is intimately familiar with many or most of the numerous restrictions and features (both useful and esoteric) applicable to one or more computer programming languages. A language lawyer is distinguished by the ability to show you the five sentences scattered through a 200-plus-page manual that together imply the answer to your question “if only you had thought to look there”. Compare wizard, legal, legalese.

Language Processor

A program that performs such functions as translating, interpreting, and other tasks required for processing a specified programming language, for example, a FORTRAN processor, a COBOL processor. (FP) (ISO)

*-Languages Of Choice

n. C, LISP, and Perl. Nearly every hacker knows one of C or Lisp, and most good ones are fluent in both. Over the last years, Perl has rapidly been gaining favor, especially as a tool for systems-administration utilities and rapid prototyping. Smalltalk and Prolog are also popular in small but influential communities. There is also a rapidly dwindling category of older hackers with FORTRAN, or even assembler, as their language of choice. They often prefer to be known as Real Programmers, and other hackers consider them a bit odd (see “The Story of Mel, a Real Programmer” in Appendix A). Assembler is generally no longer considered interesting or appropriate for anything but HLL implementation, glue, and a few time-critical and hardware-specific uses in systems programs. FORTRAN occupies a shrinking niche in scientific programming. Most hackers tend to frown on languages like Pascal and Ada, which don't give them the near-total freedom considered necessary for hacking (see bondage-and-discipline language), and to regard everything even remotely connected with COBOL or other traditional card walloper languages as a total and unmitigated loss.

Laptop Computer

Large hand-carried computer, typically weighing over seven pounds. See Notebook Computer.

*-Larval Stage

n. Describes a period of monomaniacal concentration on coding apparently passed through by all fledgling hackers. Common symptoms include the perpetration of more than one 36-hour hacking run in a given week; neglect of all other activities including usual basics like food, sleep, and personal hygiene; and a chronic case of advanced bleary-eye. Can last from 6 months to 2 years, the apparent median being around 18 months. A few so afflicted never resume a more `normal' life, but the ordeal seems to be necessary to produce really wizardly (as opposed to merely competent) programmers. See also wannabee. A less protracted and intense version of larval stage (typically lasting about a month) may recur when one is learning a new OS or programming language.

*-Lase

/layz/ vt. To print a given document via a laser printer. “OK, let's lase that sucker and see if all those graphics-macro calls did the right things. ”

Laser

Acronym for light amplification by stimulated emission of radiation. A device that produces an intense, coherent, directional beam of optical radiation by stimulating electronic, ionic, or molecular transitions to higher energy levels so that when they return to lower energy levels they emit energy. Note: Laser radiation may be highly coherent temporally, or spatially, or both. (~) See also active laser medium, injection laser diode, optical cavity.

*-Laser Chicken

n. Kung Pao Chicken, a standard Chinese dish containing chicken, peanuts, and hot red peppers in a spicy pepper-oil sauce. Many hackers call it `laser chicken' for two reasons It can zap you just like a laser, and the sauce has a red color reminiscent of some laser beams. In a variation on this theme, it is reported that some Australian hackers have redesignated the common dish `lemon chicken' as `Chernobyl Chicken'. The name is derived from the color of the sauce, which is considered bright enough to glow in the dark (as, mythically, do some of the inhabitants of Chernobyl).

Laser Intelligence

(LASINT) Intelligence information derived from laser systems. *Technical and intelligence information derived from laser systems; it is a subcategory of electro-optical intelligence (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

*-Lasherism

n. [Harvard] A program that solves a standard problem (such as the Eight Queens puzzle or implementing the life algorithm) in a deliberately nonstandard way. Distinguished from a crock or kluge by the fact that the programmer did it on purpose as a mental exercise. Such constructions are quite popular in exercises such as the Obfuscated C Contest, and occasionally in retrocomputing. Lew Lasher was a student at Harvard around 1980 who became notorious for such behavior.

Last-In, First-Out

A queueing discipline in which arriving entities leave in the reverse order from which they arrived. Note: Service is offered to the entity that has been in the file the least time. Synonyms cellar, push-down file, spike file. (FS1037S1. TXT) (LIFO) A queueing discipline in which arriving entities leave in the reverse order from which they arrived. Note: Service is offered to the entity that has been in the file the least time. See s cellar, push-down file, spike file.

Lattice

A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound. (CSC-STD-001-83;)

#-Lattice Model

In data base security, a model of the data in a statistical database useful for studying inference controls. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

*-Laundromat

n. Syn. disk farm; see washing machine.

#-Law Enforcement Interfaces

Interfaces between the computer networks of various law enforcement agencies for purposes of criminal investigation and database matching. Examples include the FBI's Nation Crime Information Center (NCIC) which links FBI headquarters to police department networks around the country. (Source panel of experts).

#-Laws, Regulations, And Other Public Policies

This KSA has no definition.

*-LDB

/l*'d*b/ vt. [from the PDP-10 instruction set] To extract from the middle. “LDB me a slice of cake, please. ” This usage has been kept alive by Common LISP's function of the same name. Considered silly. See also DPB.

*-Leaf Site

n. A machine that merely originates and reads Usenet news or mail, and does not relay any third-party traffic. Often uttered in a critical tone; when the ratio of leaf sites to backbone, rib, and other relay sites gets

too high, the network tends to develop bottlenecks. Compare backbone site, rib site.

*-Leak

n. With qualifier, one of a class of resource-management bugs that occur when resources are not freed properly after operations on them are finished, so they effectively disappear (leak out). This leads to eventual exhaustion as new allocation requests come in. memory leak and fd leak have their own entries; one might also refer, to, say, a `window handle leak' in a window system.

*-Leaky Heap

n. [Cambridge] An arena with a memory leak.

*-Leapfrog Attack

n. Use of userid and password information obtained illicitly from one host (e. g. , downloading a file of account IDs and passwords, tapping TELNET, etc.) to compromise another host. Also, the act of TELNETting through one or more hosts in order to confuse a trace (a standard cracker procedure).

#-Leased-Line Networks

This KSA has no definition.

Least Privilege

1. The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. NOTE: Application of this principle limits the damage that can result from accident, error, or unauthorized use of an AIS.
2. This principle requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. (*NCSC-WA*-001-85;; CSC-STD-001-83;)

*-Leech

n. Among BBS types, crackers and warez d00dz, one who consumes knowledge without generating new software, cracks or techniques. BBS culture specifically defines a leech as someone who downloads files with few or no uploads in return, and who does not contribute to the message section. Cracker culture extends this definition to someone (a lamer, usually) who constantly presses informed sources for information and/or assistance, but has nothing to contribute.

*-Legal

adj. Loosely used to mean `in accordance with all the relevant rules', esp. in connection with some set of constraints defined by software. “The older =+ alternate for += is no longer legal syntax in ANSI C. ” “This parser processes each line of legal input the moment it sees the trailing linefeed. ” Hackers often model their work as a sort of game played with the environment in which the objective is to maneuver through the thicket of `natural laws' to achieve a desired objective. Their use of `legal' is flavored as much by this game-playing sense as by the more conventional one having to do with courts and lawyers. Compare language lawyer, legalese.

#-Legal And Liability Issues

Are issues that have to be analyzed to determine if criminal or civil liability may result if a specific or general course of action is pursued. (Source panel of experts).

*-Legalese

n. Dense, pedantic verbiage in a language description, product specification, or interface standard; text that seems designed to obfuscate and requires a language lawyer to parse it. Though hackers are not afraid of high information density and complexity in language (indeed, they rather enjoy both), they share a deep and abiding loathing for legalese; they associate it with deception, suits, and situations in which hackers generally get the short end of the stick.

Legitimate User

*-LER

/L-E-R/ n. [TMRC, from `Light-Emitting Diode'] A light-emitting resistor (that is, one in the process of burning up). Ohm's law was broken. See also SED.

*-LERP

/lerp/ vi. ,n. Quasi-acronym for Linear Interpolation, used as a verb or noun for the operation. “Bresenham's algorithm lerps incrementally between the two endpoints of the line. ”

#-Lessons Learned

This KSA has no definition.

*-Let The Smoke Out

v. To fry hardware (see fried). See magic smoke for a discussion of the underlying mythology.

*-Letterbomb

1. n. A piece of email containing live data intended to do nefarious things to the recipient's machine or terminal. It is possible, for example, to send letterbombs that will lock up some specific kinds of terminals when they are viewed, so thoroughly that the user must cycle power (see cycle, sense 3) to unwedge them. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to tragic. See also Trojan horse; compare nastygram.
2. Loosely, a mailbomb.

Level

1. The absolute or relative voltage, current, or power at a particular point in a circuit or system. (~)
2. A tier or layer of a hierarchical system, e. g. , the Link-Level protocol, high-level computer language. (~)

Level I/II/III

See DATA LEVEL.

Level Of Trust

*-Lexer

/lek'sr/ n. Common hacker shorthand for `lexical analyzer', the input-tokenizing stage in the parser for a language (the part that breaks it into word-like pieces). “Some C lexers get confused by the old-style compound ops like `=-'. ”

*-Lexiphage

/lek'si-fayj`/ n. A notorious word chomper on ITS. See bagbiter. This program would draw on a selected victim's bitmapped terminal the words “THE BAG” in ornate letters, followed a pair of jaws biting pieces of it off.

*-Life

1. n. A cellular-automata game invented by John Horton Conway and first introduced publicly by Martin Gardner (“Scientific American”, October 1970); the game's popularity had to wait a few years for computers on which it could reasonably be played, as it's no fun to simulate the cells by hand. Many hackers pass through a stage of fascination with it, and hackers at various places contributed heavily to the mathematical analysis of this game (most notably Bill Gosper at MIT, who even implemented life in TECO!; see Gosperism). When a hacker mentions `life', he is much more likely to mean this game than the magazine, the breakfast cereal, or the human state of existence.
2. The opposite of Usenet. As in “Get a life!”

Life Cycle

The total phases through which an item passes from the time it is initially developed until the time it is either consumed in use or disposed of as being excess to all known materiel requirements. (JP 1-02)

Life Cycle Security

Protecting a system over its full life, including research, development, test, evaluation, production, procurement, operation, support and, where pertinent, disposal.

#-Life Cycle System Security Planning

This KSA has no definition.

Life Cycle

*-Life Is Hard

1. prov. [XEROX PARC] This phrase has two possible interpretations (1) “While your suggestion may have some merit, I will behave as though I hadn't heard it. ”
2. “While your suggestion has obvious merit, equally obvious circumstances prevent it from being seriously considered. ” The charm of the phrase lies precisely in this subtle but important ambiguity.

Life-Cycle

Duration of a project, from when a requirement is proposed till the equipment is disposed of. A computer's life-cycle begins with the user deciding that a new system is needed, and ends when the last computer aquired under that program is scrapped through DRMO or given to another organization through inter-agency reutilization.

Life-Cycle Security

*-Light Pipe

n. Fiber optic cable. Oppose copper.

*-Lightweight

adj. Opposite of heavyweight; usually found in combining forms such as `lightweight process'.

*-Like Kicking Dead Whales Down The Beach

adj. Describes a slow, difficult, and disgusting process. First popularized by a famous quote about the difficulty of getting work done under one of IBM's mainframe OSes. “Well, you *could* write a C compiler in COBOL, but it would be like kicking dead whales down the beach. ” See also fear and loathing.

*-Like Nailing Jelly To A Tree

adj. Used to describe a task thought to be impossible, esp. one in which the difficulty arises from poor specification or inherent slipperiness in the problem domain. “Trying to display the `prettiest' arrangement of nodes and arcs that diagrams a given graph is like nailing jelly to a tree, because nobody's sure what `prettiest' means algorithmically. ”:line 666 [from Christian eschatological myth] n. The notional line of source at which a program fails for obscure reasons, implying either that *somebody* is out to get it (when you are the programmer), or that it richly deserves to be so gotten (when you are not). “It works when I trace through it, but seems to crash on line 666 when I run it. ” “What happens is that whenever a large batch comes through, mmdf dies on the Line of the Beast. Probably some twit hardcoded a buffer size. ”

Limited Access

Limiting access to the resources of a system only to authorized personnel, users, programs, processes, or

other systems, for instance computer networks. (*AFR* 205-16;) See Access Control.

Limited Access Area

An area in which uncontrolled movement of persons would allow access to classified information, but in which such access is prevented by escort or other internal restrictions or controls (NSA, *National INFOSEC Glossary*, 10/88)

Limited Access Security Mode

The type of data being processed is categorized as unclassified and requires the implementation of special access controls to restrict the access to the data only to individuals who, by their job function, have a need to access the data. (*NCSC-WA*-001-85;)

Limited ADP Access Security Mode

An ADP system or network is operating in the limited access security mode when the type of data being processed is categorized as unclassified and requires the implementation of special access controls to restrict the access to the data only to individuals who, by their job function, have a need to access the data. (*OPNAVINST* 5239. 1A;)

Limited Area

A security area for the protection of classified matter where guards, security inspectors, or other internal controls can prevent access. See 5632. 4 for further information. (DOE 5637. 1)

Limited Exclusion Area

(LEA) A room or enclosed area to which security controls have been applied to provide protection to a RED information processing systems equipment and wire lines equivalent to that required for the information transmitted through the system. An LEA must contain a RED equipment area. (NACSIM 5203)

Limited Maintenance

COMSEC maintenance restricted to fault isolation, removal, and replacement of plug-in assemblies. NOTE: Soldering or unsoldering usually is prohibited in limited maintenance. See Full Maintenance.

Limited Protection

1. A form of short-term communications security applied to the electromagnetic or acoustic transmission of unclassified information which warrants protection against simple analysis and easy exploitation but does not require the level of protection needed for classified information. (*AR* 380-380)
2. A form of short-term COMSEC protection applied to the electromagnetic or acoustic transmission of national security-related information. (NCSC-9)

Line

#-Line Authentication

This KSA has no definition.

Line Conduction

1. Unintentional signals or noise induced or conducted on a telecommunications or automated information system signal, power, control, indicator, or other external interface line.
2. (TEMPEST) Emanations produced on any external or interface line of an equipment, which, in any way, alter the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and AC or DC power lines.
3. Line conduction emanations include all signals or noise which are induced or conducted on the external interface linesThe external interface lines include signal lines, control and indicator lines, power lines and any lines which interface an equipment to other equipment or systems.

Line Conductors

Line conduction emanations include all signals or noise which are induced or conducted on the external interface linesThe external interface lines include signal lines, control and indicator lines, power lines and any lines which interface an equipment to other equipment or systems.

*-Line Eater, The

1. n. [Usenet] A bug in some now-obsolete versions of the netnews software that used to eat up to BUFSIZ bytes of the article text. The bug was triggered by having the text of the article start with a space or tab. This bug was quickly personified as a mythical creature called the `line eater', and postings often included a dummy line of `line eater food'. Ironically, line eater `food' not beginning with a space or tab wasn't actually eaten, since the bug was avoided; but if there *was* a space or tab before it, then the line eater would eat the food *and* the beginning of the text it was supposed to be protecting. The practice of `sacrificing to the line eater' continued for some time after the bug had been nailed to the wall, and is still humorously referred to. The bug itself is still (in mid-1991) occasionally reported to be lurking in some mail-to-netnews gateways.
2. See NSA line eater.

Line Load Control

*-Line Noise

1. n. [techspeak] Spurious characters due to electrical noise in a communications link, especially an RS-232 serial connection. Line noise may be induced by poor connections, interference or crosstalk from other circuits, electrical storms, cosmic rays, or (notionally) birds crapping on the phone wires.

2. Any chunk of data in a file or elsewhere that looks like the results of line noise in sense 1.
3. Text that is theoretically a readable text or program source but employs syntax so bizarre that it looks like line noise in senses 1 or 2. Yes, there are languages this ugly. The canonical example is TECO; it is often claimed that “TECO's input syntax is indistinguishable from line noise. ” Other non-WYSIWYG editors, such as Multics `qed' and Unix `ed', in the hands of a real hacker, also qualify easily, as do deliberately obfuscated languages such as INTERCAL.

#-Line Of Sight

This KSA has no definition.

*-Line Starve

1. vi. [MIT] To feed paper through a printer the wrong way by one line (most printers can't do this). On a display terminal, to move the cursor up to the previous line of the screen. “To print `X squared', you just output `X', line starve, `2', line feed. ” (The line starve causes the `2' to appear on the line above the `X', and the line feed gets back to the original line.)
2. n. A character (or character sequence) that causes a terminal to perform this action. ASCII 0011010, also called SUB or control-Z, was one common line-starve character in the days before microcomputers and the X3. 64 terminal standard. Unlike `line feed', `line starve' is *not* standard ASCII terminology. Even among hackers it is considered a bit silly.
3. [proposed] A sequence such as \c (used in System V echo, as well as nroff and troff) that suppresses a newline or other character(s) that would normally be emitted.

Linear Analog Synchronization

A synchronization control system in which the functional relationships used to obtain synchronization are of simple proportionality. Synonym linear analog control. See also synchronization.

Linear Predictive Coding

A method of digitally encoding analog signals, which method uses a single-level or multilevel sampling system in which the value of the signal at each sample time is predicted to be a linear function of the past values of the quantized signal. Note: LPC is related to adaptive predictive coding (APC) in that both use adaptive predictors. However, LPC uses more prediction coefficients to permit use of a lower information bit rate than APC, and thus requires a more complex processor. See also adaptive predictive coding, code, level. (FS1037S1. TXT) (LPC) A method of digitally encoding analog signals, which method uses a single-level or multilevel sampling system in which the value of the signal at each sample time is predicted to be a linear function of the past values of the quantized signal. Note: LPC is related to adaptive predictive coding (APC) in that both use adaptive predictors. However, LPC uses more prediction coefficients to permit use of a lower information bit rate than APC, and thus requires a more complex processor. See also adaptive predictive coding, code, level.

Linear Programming

In operations research, a procedure for locating the maximum or minimum of a linear function of variables that are subject to linear constraints. (FP) Synonym linear optimization. (FS1037S1. TXT) (LP) In operations research, a procedure for locating the maximum or minimum of a linear function of variables that are subject to linear constraints. (FP) See linear optimization.

*-Linearithmic

adj. Of an algorithm, having running time that is O(N log N). Coined as a portmanteau of `linear' and `logarithmic' in “Algorithms In C” by Robert Sedgewick (Addison-Wesley 1990, ISBN 0-201-51425-7).

Link

1. The communication facilities existing between adjacent nodes of a network. (~)
2. A portion of a circuit designed to be connected in tandem with other portions.
3. A radio path between two points, called a radio link, which may be unidirectional, half-duplex, or (full) duplex. (~)
4. In communications, a general term used to indicate the existence of communications facilities between two points. (JCS1-DoD) (JCS1-NATO)
5. In computer programming, the part of a computer program, in some cases a single instruction or address, that passes control and parameters between separate portions of the computer program. Note: The term “link” should be defined or qualified when used.
6. A conceptual (or logical) circuit between two users of a packet-switched (or other) network permitting them to communicate, although different physical paths may be used. (FS1037S1. TXT)
7. The communication facilities existing between adjacent nodes of a network. (~)
8. A portion of a circuit designed to be connected in tandem with other portions.
9. A radio path between two points, called a radio link, which may be unidirectional, half-duplex, or (full) duplex. (~)
10. In communications, a general term used to indicate the existence of communications facilities between two points. (JCS1-DoD) (JCS1-NATO)
11. In computer programming, the part of a computer program, in some cases a single instruction

or address, that passes control and parameters between separate portions of the computer program. Note: The term “link” should be defined or qualified when used.

12. A conceptual (or logical) circuit between two users of a packet-switched (or other) network permitting them to communicate, although different physical paths may be used.

Link Encryption

1. The application of online crypto-operations to a link of a communications sytem so that all information passing over the link is encrypted in its entirety. (*FIPS PUB* 39;)
2. End-to-end encryption within each link in a communications network. (*FIPS PUB* 39;)

*-Link Farm

n. [UNIX] A directory tree that contains many links to files in a master directory tree of files. Link farms save space when one is maintaining several nearly identical copies of the same source tree -- for example, when the only difference is architecture-dependent object files. “Let's freeze the source and then rebuild the FROBOZZ-3 and FROBOZZ-4 link farms. ” Link farms may also be used to get around restrictions on the number of `-I' (include-file directory) arguments on older C preprocessors. However, they can also get completely out of hand, becoming the filesystem equivalent of spaghetti code.

Link Layer

Deprecated term for Data Link Layer. See Open Systems Interconnection--Reference Model.

Link Level

In data transmission, the conceptual level of control or data processing logic existing in the hierarchical structure of a primary or secondary station that is responsible for maintaining control of the data link. Note: The link level functions provide an interface between the station high-level logic and the data link; these functions include transmit bit injection and receive bit extraction, address/control field interpretation, command response generation, transmission and interpretation, and frame check sequence computation and interpretation. See also data transmission, level, link.

Link Protocol

A set of rules for data communication over a data link, which rules are specified in terms of a transmission code, a transmission mode, and control and recovery procedures. See also code, link, protocol.

Link-By-Link Encipherment

The individual application of encipherment to data on each link of a communications system. Note: The implication of link-by-link encipherment is that data will be in cleartext form in relay entities. (SS;)

Link-By-Link Encryption

*-Link-Dead

adj. [MUD] Said of a MUD character who has frozen in place because of a dropped Internet connection.

Linkage

The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information; in particular, the combination of computer files from two or more sources. (*FIPS PUB* 39;)

*-Lint

1. [from UNIX's `lint(1)', named for the bits of fluff it supposedly picks from programs] 1. vt. To examine a program closely for style, language usage, and portability problems, esp. if in C, esp. if via use of automated analysis tools, most esp. if the UNIX utility `lint(1)' is used. This term used to be restricted to use of `lint(1)' itself, but (judging by references on Usenet) it has become a shorthand for desk check at some non-UNIX shops, even in languages other than C. Also as v. delint.
2. n. Excess verbiage in a document, as in “This draft has too much lint”.

*-Linux

n. The free UNIX workalike created by Linus Torvalds and friends starting about 1990. This may be the most remarkable hacker project in history -- an entire clone of UNIX for 386 and 486 micros, distributed for free with sources over the net. This is what GNU aimed to be, but the Free Software Foundation never produced the kernel to go with its UNIX toolset (which Linux uses). Other, similar efforts like FreeBSD and NetBSD have been much less successful. The secret of Linux's success may be that Linus worked much harder early on to keep the development process open and recruit other hackers, creating a snowball effect.

*-Lion Food

n. [IBM] Middle management or HQ staff (or, by extension, administrative drones in general). From an old joke about two lions who, escaping from the zoo, split up to increase their chances but agree to meet after 2 months. When they finally meet, one is skinny and the other overweight. The thin one says “How did you manage? I ate a human just once and they turned out a small army to chase me -- guns, nets, it was terrible. Since then I've been reduced to eating mice, insects, even grass. ” The fat one replies “Well, *I* hid near an IBM office and ate a manager a day. And nobody even noticed!”

*-Lions Book

n. “Source Code and Commentary on UNIX level 6”, by John Lions. The two parts of this book contained

(1) the entire source listing of the UNIX Version 6 kernel, and (2) a commentary on the source discussing the algorithms. These were circulated internally at the University of New South Wales beginning 1976--77, and were, for years after, the *only* detailed kernel documentation available to anyone outside Bell Labs. Because Western Electric wished to maintain trade secret status on the kernel, the Lions book was never formally published and was only supposed to be distributed to affiliates of source licensees (it is still possible to get a Bell Labs reprint of the book by sending a copy of a V6 source license to the right person at Bellcore, but *real* insiders have the UNSW edition). In spite of this, it soon spread by samizdat to a good many of the early UNIX hackers.

*-LISP

n. [from `LISt Processing language', but mythically from `Lots of Irritating Superfluous Parentheses'] AI's mother tongue, a language based on the ideas of (a) variable-length lists and trees as fundamental data types, and (b) the interpretation of code as data and vice-versa. Invented by John McCarthy at MIT in the late 1950s, it is actually older than any other HLL still in use except FORTRAN. Accordingly, it has undergone considerable adaptive radiation over the years; modern variants are quite different in detail from the original LISP 1. 5. The dominant HLL among hackers until the early 1980s, LISP now shares the throne with C. See languages of choice. All LISP functions and programs are expressions that return values; this, together with the high memory utilization of LISPs, gave rise to Alan Perlis's famous quip (itself a take on an Oscar Wilde quote) that “LISP programmers know the value of everything and the cost of nothing”. One significant application for LISP has been as a proof by example that most newer languages, such as COBOL and Ada, are full of unnecessary crocks. When the Right Thing has already been done once, there is no justification for bogosity in newer languages.

List Oriented

A computer protection system in which each protected object has a list of all subjects authorized to access it Compare ticket-oriented. (*NCSC-TG*-004-88)

#-List-Based Access Controls

This KSA has no definition.

List-Oriented

A computer protection system in which each protected object has a list of all subjects authorized to access it. Compare ticket-oriented. See Ticket-Oriented.

Literature Intelligence

(LITINT) A category of intelligence information derived from written/printed/graphic and computer database sources.

*-Literature, The

n. Computer-science journals and other publications, vaguely gestured at to answer a question that the speaker believes is trivial. Thus, one might answer an annoying question by saying “It's in the literature. ” Oppose Knuth, which has no connotation of triviality.

*-Lithium Lick

n. [NeXT] Steve Jobs. Employees who have gotten too much attention from their esteemed founder are said to have `lithium lick' when they begin to show signs of Jobsian fervor and repeat the most recent catch phrases in normal conversation --- for example, “It just works, right out of the box!”

LITINT

Literature Intelligence

*-Little-Endian

adj. Describes a computer architecture in which, within a given 16- or 32-bit word, bytes at lower addresses have lower significance (the word is stored `little-end-first'). The PDP-11 and VAX families of computers and Intel microprocessors and a lot of communications and networking hardware are little-endian. See big-endian, middle-endian, NUXI problem. The term is sometimes used to describe the ordering of units other than bytes; most often, bits within a byte.

*-Live

/li:v/ adj. ,adv. Opposite of `test'. Refers to actual real-world data or a program working with it. For example, theresponse to “I think the record deleter is finished. ” might be “Is it liveyet?” “Have you tried it out on live data?” This usage usually carriesthe connotation that live data is more fragile and must not becorrupted, or bad things will happen. So a more appropriate response mightbe “Well, make sure it works perfectly before we throw live data at it. ” The implication here is that record deletion is something pretty significant, and a haywire record-deleter running amok live would probably cause great harm.

*-Live Data

1. n. Data that is written to be interpreted and takes over program flow when triggered by some unobvious operation, such as viewing it. One use of such hacks is to break security. For example, some smart terminals have commands that allow one to download strings to program keys; this can be used to write live data that, when listed to the terminal, infects it with a security-breaking virus that is triggered the next time a hapless user strikes that key. For another, there are some well-known bugs in vi that allow certain texts to send arbitrary

commands back to the machine when they are simply viewed.
2. In C code, data that includes pointers to function hooks (executable code).
3. An object, such as a trampoline, that is constructed on the fly by a program and intended to be executed as code.

*-Live Free Or Die!

1. imp. The state motto of New Hampshire, which appears on that state's automobile license plates.
2. A slogan associated with UNIX in the romantic days when UNIX aficionados saw themselves as a tiny, beleaguered underground tilting against the windmills of industry. The “free” referred specifically to freedom from the fascist design philosophies and crufty misfeatures common on commercial operating systems. Armando Stettner, one of the early UNIX developers, used to give out fake license plates bearing this motto under a large UNIX, all in New Hampshire colors of green and white. These are now valued collector's items. Recently (1994) an inferior imitation of these has been put in circulation with a red corporate logo added.

*-Livelock

/li:v'lok/ n. A situation in which some critical stage of a task is unable to finish because its clients perpetually create more work for it to do after they have been serviced but before it can clear its queue. Differs from deadlock in that the process is not blocked or waiting for anything, but has a virtually infinite amount of work to do and can never catch up.

*-Liveware

1. /li:v'weir/ n. Synonym for wetware. Less common.
2. [Cambridge] Vermin. “Waiter, there's some liveware in my salad. ”

*-Lobotomy

1. n. What a hacker subjected to formal management training is said to have undergone. At IBM and elsewhere this term is used by both hackers and low-level management; the latter doubtless intend it as a joke.
2. The act of removing the processor from a microcomputer in order to replace or upgrade it. Some very cheap clone systems are sold in `lobotomized' form -- everything but the brain.

Local Area Network

(LAN) A short-haul data communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways. (JCS PUB 6-03. 7) Note 1: A LAN is not subject to public telecommunications regulations. See also bus topology, metropolitan area network, node (def. #1), ring network, star network, star topology, tree topology.

#-Local Area Network Security

Provision of access, integrity and availability controls for a high bandwidth bidirectional communications network which operates over a limited geographic area. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Local Exchange Loop

Local Nationals

A non-U. S. citizen who is normally resident in the country in which employed, though not necessarily a citizen of that country, and who is employed by the U. S. Government. (*AR* 380-380;)

*-Locals, The

pl. n. The users on one's local network (as opposed, say, to people one reaches via public Internet or UUCP connects). The marked thing about this usage is how little it has to do with real-space distance. “I have to do some tweaking on this mail utility before releasing it to the locals. ”

LOCK

See LOgical Co-processing Kernel.

Lock-And-Key Protection System

A protection system that involves matching a key or password with a specific access requirement. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

*-Locked And Loaded

adj. [from military slang for an M-16 rifle with magazine inserted and prepared for firing] Said of a removable disk volume properly prepared for use -- that is, locked into the drive and with the heads loaded. Ironically, because their heads are `loaded' whenever the power is up, this description is never used of Winchester drives (which are named after a rifle).

*-Locked Up

adj. Syn. for hung, wedged.

Lockout

1. In a telephone circuit controlled by two voice-operated devices, the inability of one or both users to get through, either because of excessive local circuit noise or because of continuous speech from either or both users. (~) See also head-on collision.
2. In mobile communications, an arrangement of control circuits whereby only one receiver can feed the system at a time. (~) Synonym receiver lockout system.

3. In telephone systems, treatment of a user's line or trunk that is in trouble or in a permanent off-hook condition, by automatically disconnecting the line from the switching equipment. (~)
4. In public telephone systems, a process that denies an attendant or other users the ability to reenter an established connection. See also call spill-over, head-on collision, not-ready condition.
5. An arrangement for restricting access to use of all, or part of, a computer system. (FP) (ISO) Synonym protection.

Log

See journal (def. #1).

Log-Off

The procedure that is followed by a user in closing a session, i. e. , a period of terminal operation.

Log-On

The procedure that is followed by a user in beginning a session, i. e. , a period of terminal operation.

Logic Bomb

1. A resident computer program which, when executed, checks for particular conditions or particular states of the system which, when satisfied, triggers the perpetration of an unauthorized act. (*NCSC-WA*-001-85;)
2. A logic bomb is a program that causes damage when a certain event takes place. For example, files may be destroyed whenever a “Friday the 13th” comes around. (IC;)

*-Logical

adj. [from the technical term `logical device', wherein a physical device is referred to by an arbitrary `logical' name] Having the role of. If a person (say, Les Earnest at SAIL) who had long held a certain post left and were replaced, the replacement would for a while be known as the `logical' Les Earnest. (This does not imply any judgment on the replacement. ) Compare virtual. At Stanford, `logical' compass directions denote a coordinate system in which `logical north' is toward San Francisco, `logical west' is toward the ocean, etc. , even though logical north varies between physical (true) north near San Francisco and physical west near San Jose. (The best rule of thumb here is that, by definition, El Camino Real always runs logical north-and-south.) In giving directions, one might say “To get to Rincon Tarasco restaurant, get onto El Camino Bignum going logical north. ” Using the word `logical' helps to prevent the recipient from worrying about that the fact that the sun is setting almost directly in front of him. The concept is reinforced by North American highways which are almost, but not quite, consistently labeled with logical rather than physical directions. A similar situation exists at MIT Route 128 (famous for the electronics industry that has grown up along it) is a 3-quarters circle surrounding Boston at a radius of 10 miles, terminating near the coastline at each end. It would be most precise to describe the two directions along this highway as `clockwise' and `counterclockwise', but the road signs all say “north” and “south”, respectively. A hacker might describe these directions as `logical north' and `logical south', to indicate that they are conventional directions not corresponding to the usual denotation for those words. (If you went logical south along the entire length of route 128, you would start out going northwest, curve around to the south, and finish headed due east, passing along one infamous stretch of pavement that is simultaneously route 128 south and Interstate 93 north, and is signed as such!)

Logical Access Control

The use of information-related mechanisms (such as passwords) rather than physical mechanisms for the provision of access control. (WB;)

Logical Circuit

See virtual circuit.

Logical Completeness

Means for assessing the effectiveness measure and degree to which a set of security and access control mechanisms meets the requirements of security specifications.

Logical Completeness Measure

A means for assessing the effectiveness and degree to which a set of security and access control mechanisms meet the requirements of security specifications. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

Logical Link Control Sublayer

(LLC) In a LAN/MAN system, that part of the OSI Data Link Layer that supports medium-independent data link functions, and uses the services of the medium access control sublayer to provide services to the network layer. See also link, Open Systems Interconnection--Reference Model.

Logical Signaling Channel

A logical channel that provides a signaling path within an information channel or a physical signaling channel. See also signaling path.

Logical Topology

The connection configuration of a network that reflects the network's function, use, or implementation without reference to the physical interconnection of elements. See also physical topology.

Login

Login History

Login/log In
See Logon/Log On.

Logoff/log Off
Procedure used to terminate connections. (BBD;)

Logon

Logon/log On
1. Procedure used to establish the identity of the user and the levels of authorization and access permitted. (BBD;)
2. An error of omission or oversight in software or hardware which permits circumventing the access control process. (*AR* 380-380;; *NCSC-WA*-001-85;)
3. Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the non hierarchical categories. (*DCID* 1/16-1, Sup. ;) See Login, SIGNIN, SIGNON, Loophole, Fault, Flaw, Low Water Mark

#-Logs And Journals
This KSA has no definition.

Long Title
Descriptive title of a COMSEC item.

Long-Haul Communication
Any communication line, whether government owned or controlled by a common carrier, extending outside the geographic perimeter of the installation.

Long-Range Plan
A written description of the strategy for implementing the Classified Computer Security Program that covers the 5 years beginning at the date of the plan. (DOE 5637. 1)

Loop
1. A communication channel from a switching center or an individual message distribution point to the user terminal. (~) Synonym subscriber line.
2. In telephone systems, a pair of wires from a central office to a subscriber's telephone. (~) Synonyms local loop, user's line. See also local exchange loop.
3. Go and return conductors of an electric circuit; a closed circuit.
4. A closed path under measurement in a resistance test. 5. A type of antenna used extensively in direction-finding equipment and in UHF reception. (~) 6. A sequence of instructions that may be executed iteratively while a certain condition prevails. In some implementations, no test is made to discover whether the condition prevails until the loop has been executed once. (FP) (ISO)

*-Loop Through
vt. To process each element of a list of things. “Hold on, I've got to loop through my paper mail. ” Derives from the computer-language notion of an iterative loop; compare `cdr down' (under cdr), which is less common among C and UNIX programmers. ITS hackers used to say `IRP over' after an obscure pseudo-op in the MIDAS PDP-10 assembler (the same IRP op can nowadays be found in Microsoft's assembler).

Loop-Back
1. A method of performing transmission tests of access lines from the serving switching center, a method that usually does not require the assistance of personnel at the served terminal. (~)
2. A method of testing between stations (not necessarily adjacent) wherein two lines are used, with the testing being done at one station and the two lines interconnected at the distant station. (~) See also back-to-back connection, loop (def. #2), loop test.

Loophole
1. An error of omission or oversight in software or hardware that permits circumventing the system security policy.
2. Synonymous with FAULT and FLAW.

*-Loose Bytes
n. Commonwealth hackish term for the padding bytes or shims many compilers insert between members of a record or structure to cope with alignment requirements imposed by the machine architecture.

*-Lord High Fixer
n. [primarily British, from Gilbert & Sullivan's `lord high executioner'] The person in an organization who knows the most about some aspect of a system. See wizard.

*-Lose
1. [MIT] vi. To fail. A program loses when it encounters an exceptional condition or fails to work in the expected manner.
2. To be exceptionally unesthetic or crocky.
3. Of people, to be obnoxious or unusually stupid (as opposed to ignorant). See also deserves to lose.
4. n. Refers to something that is losing, especially in the phrases “That's a lose!” and “What a lose!”

*-Lose Lose
interj. A reply to or comment on an undesirable situation. “I accidentally deleted all my files!” “Lose, lose. ”

*-Loser
n. An unexpectedly bad situation, program, programmer, or person. Someone who habitually loses. (Even winners can lose occasionally.) Someone who knows not and knows not that he knows not. Emphatic forms

are `real loser', `total loser', and `complete loser' (but not **`moby loser', which would be a contradiction in terms). See luser.

*-Losing

adj. Said of anything that is or causes a lose or lossage.

*-Loss

n. Something (not a person) that loses; a situation in which something is losing. Emphatic forms include `moby loss', and `total loss', `complete loss'. Common interjections are “What a loss!” and “What a moby loss!” Note that `moby loss' is OK even though **`moby loser' is not used; applied to an abstract noun, moby is simply a magnifier, whereas when applied to a person it implies substance and has positive connotations. Compare lossage.

*-Lossage

/los'*j/ n. The result of a bug or malfunction. This is a mass or collective noun. “What a loss!” and “What lossage!” are nearly synonymous. The former is slightly more particular to the speaker's present circumstances; the latter implies a continuing lose of which the speaker is currently a victim. Thus (for example) a temporary hardware failure is a loss, but bugs in an important tool (like a compiler) are serious lossage.

Lost Call

*-Lost In The Noise

adj. Syn. lost in the underflow. This term is from signal processing, where signals of very small amplitude cannot be separated from low-intensity noise in the system. Though popular among hackers, it is not confined to hackerdom; physicists, engineers, astronomers, and statisticians all use it.

*-Lost In The Underflow

adj. Too small to be worth considering; more specifically, small beyond the limits of accuracy or measurement. This is a reference to `floating underflow', a condition that can occur when a floating-point arithmetic processor tries to handle quantities smaller than its limit of magnitude. It is also a pun on `undertow' (a kind of fast, cold current that sometimes runs just offshore and can be dangerous to swimmers). “Well, sure, photon pressure from the stadium lights alters the path of a thrown baseball, but that effect gets lost in the underflow. ” Compare epsilon, epsilon squared; see also overflow bit.

*-Lots Of MIPS But No I/O

adj. Used to describe a person who is technically brilliant but can't seem to communicate with human beings effectively. Technically it describes a machine that has lots of processing power but is bottlenecked on input-output (in 1991, the IBM Rios, a. k. a. RS/6000, is a notorious recent example).

#-Low Power

The minimum level of power required for proper operation of equipment.

Low Probability Of

(1) Result of measures used to hide or detection disguise intentional electromagnetic transmissions. (2) Result of measures to prevent the intercept of intentional electromagnetic transmissions.

Low Probability Of Detection

(LPD) (1) Result of measures used to hide or disguise intentional electromagnetic transmissions. (2) Result of measures used to hide or disguise intentional electromagnetic transmissions. (3) Measures used to hide or disguise intentional electromagnetic transmissions (NSA, *National INFOSEC Glossary*, 10/88)

Low Probability Of Intercept

Result of measures to prevent the intercept of intentional electromagnetic transmissions. (AF9K_JBC. TXT) (LPI) Result of measures to prevent the intercept of intentional electromagnetic transmissions.

Low Water Mark

Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the nonhierarchical categories. (*DCID* 1/16, Sup.)

*-Low-Bandwidth

adj. [from communication theory] Used to indicate a talk that, although not content-free, was not terribly informative. “That was a low-bandwidth talk, but what can you expect for an audience of suits!” Compare zero-content, bandwidth, math-out.

*-LPT

/L-P-T/ or /lip'it/ or /lip-it'/ n. Line printer, of course. Rare under UNIX, more common among hackers who grew up with ITS, MS-DOS, CP/M and other operating systems that were strongly influenced by early DEC conventions.

LTHE

Shorthand for Less Than or Equal, an ordering relation on the set of certainty measures. A requirement of the Uncertainty Calculus. (MA;)

*-Lubarsky's Law Of Cybernetic Entomology

prov. “There is *always* one more bug. ”

*-Lunatic Fringe

n. [IBM] Customers who can be relied upon to accept release 1 versions of software.

*-Lurker

n. One of the `silent majority' in a electronic forum; one who posts occasionally or not at all but is known to read the group's postings regularly. This term is not

pejorative and indeed is casually used reflexively "Oh, I'm just lurking. " Often used in `the lurkers', the hypothetical audience for the group's flamage-emitting regulars.

*-Luser

n. /loo'zr/ A user; esp. one who is also a loser. (luser and loser are pronounced identically.) This word was coined around 1975 at MIT. Under ITS, when you first walked up to a terminal at MIT and typed Control-Z to get the computer's attention, it printed out some status information, including how many people were already using the computer; it might print "14 users", for example. Someone thought it would be a great joke to patch the system to print "14 losers" instead. There ensued a great controversy, as some of the users didn't particularly want to be called losers to their faces every time they used the computer. For a while several hackers struggled covertly, each changing the message behind the back of the others; any time you logged into the computer it was even money whether it would say "users" or "losers". Finally, someone tried the compromise "lusers", and it stuck. Later one of the ITS machines supported `luser' as a request-for-help command. ITS died the death in mid-1990, except as a museum piece; the usage lives on, however, and the term `luser' is often seen in program comments.

M

*-M

pref. (on units) suff. (on numbers) [SI] See quantifiers.

M-Ary Code

The generic name applied to all multilevel codes. (~) Note: A numeric digit may be substituted for "M" to indicate the specific number of quantization states. Thus an 8-ary code has eight distinct states and could convey three bits per code symbol. See also binary digit, code, level.

*-Macdink

/mak'dink/ vt. [from the Apple Macintosh, which is said to encourage such behavior] To make many incremental and unnecessary cosmetic changes to a program or file. Often the subject of the macdinking would be better off without them. "When I left at 11 P. M. last night, he was still macdinking the slides for his presentation. " See also fritterware, window shopping.

*-Machinable

adj. Machine-readable. Having the softcopy nature.

Machine Cryptosystem

Cryptosystem in which cryptographic processes are performed by crypto-equipment.

Machine Instruction

An instruction that can be executed by the processor of the computer for which it has been designed as part of the machine language. (FP) (ISO)

Machine Language

A computer language composed of machine instructions that can be executed directly by a computer without further modification. (~) See also assembly language, compile, computer, computer language, high-level language.

Machine Learning

The ability of a device to improve its performance based on its past performance. (FP)

Machine Word

See computer word.

Machine-Oriented Language

See computer-oriented language.

Machine-Readable Medium

A medium that can convey data to a given sensing device. (FP) See automated data medium.

*-Machoflops

/mach'oh-flops/ n. [pun on `megaflops', a coinage for `millions of FLoating-point Operations Per Second'] Refers to artificially inflated performance figures often quoted by computer manufacturers. Real applications are lucky to get half the quoted speed. See Your mileage may vary, benchmark.

*-Macintoy

/mak'in-toy/ n. The Apple Macintosh, considered as a toy. Less pejorative than Macintrash.

*-Macintrash

/mak'in-trash`/ n. The Apple Macintosh, as described by a hacker who doesn't appreciate being kept away from the *real computer* by the interface. The term maggotbox has been reported in regular use in the Research Triangle area of North Carolina. Compare Macintoy. See also beige toaster, WIMP environment, point-and-drool interface, drool-proof paper, user-friendly.

*-Macro

/mak'roh/ [techspeak] n. A name (possibly followed by a formal arg list) that is equated to a text or symbolic expression to which it is to be expanded (possibly with the substitution of actual arguments) by a macro expander. This definition can be found in any technical dictionary; what those won't tell you is how the hackish connotations of the term have changed over time. The term `macro' originated in early assemblers, which encouraged the use of macros as a structuring and information-hiding device. During the

early 1970s, macro assemblers became ubiquitous, and sometimes quite as powerful and expensive as HLLs, only to fall from favor as improving compiler technology marginalized assembler programming (see languages of choice). Nowadays the term is most often used in connection with the C preprocessor, LISP, or one of several special-purpose languages built around a macro-expansion facility (such as TeX or UNIX's [nt]roff suite). Indeed, the meaning has drifted enough that the collective `macros' is now sometimes used for code in any special-purpose application control language (whether or not the language is actually translated by text expansion), and for macro-like entities such as the `keyboard macros' supported in some text editors (and PC TSR or Macintosh INIT/CDEV keyboard enhancers).

*-Macro

pref. Large. Opposite of micro-. In the mainstream and among other technical cultures (for example, medical people) this competes with the prefix mega-, but hackers tend to restrict the latter to quantification.

*-Macrology

1. /mak-rol'*-jee/ n. Set of usually complex or crufty macros, e. g. , as part of a large system written in LISP, TECO, or (less commonly) assembler.
2. The art and science involved in comprehending a macrology in sense 1. Sometimes studying the macrology of a system is not unlike archeology, ecology, or theology, hence the sound-alike construction. See also boxology.

*-Macrotape

/mak'roh-tayp/ n. An industry-standard reel of tape, as opposed to a microtape. See also round tape.

*-Maggotbox

/mag'*t-boks/ n. See Macintrash. This is even more derogatory.

*-Magic

1. adj. As yet unexplained, or too complicated to explain; compare automagically and (Arthur C.) Clarke's Third Law “Any sufficiently advanced technology is indistinguishable from magic. ” “TTY echoing is controlled by a large number of magic bits. ” “This routine magically computes the parity of an 8-bit byte in three instructions. ”
2. Characteristic of something that works although no one really understands why (this is especially called black magic).
3. [Stanford] A feature not generally publicized that allows something otherwise impossible, or a feature formerly in that category but now unveiled. Compare black magic, wizardly, deep magic, heavy wizardry. For more about hackish `magic', see A Story About `Magic' in Appendix A.

*-Magic Cookie

1. n. [UNIX] Something passed between routines or programs that enables the receiver to perform some operation; a capability ticket or opaque identifier. Especially used of small data objects that contain data encoded in a strange or intrinsically machine-dependent way. E. g. , on non-UNIX OSes with a non-byte-stream model of files, the result of `ftell(3)' may be a magic cookie rather than a byte offset; it can be passed to `fseek(3)', but not operated on in any meaningful way. The phrase `it hands you a magic cookie' means it returns a result whose contents are not defined but which can be passed back to the same or some other program later.
2. An in-band code for changing graphic rendition (e. g. , inverse video or underlining) or performing other control functions (see also cookie). Some older terminals would leave a blank on the screen corresponding to mode-change magic cookies; this was also called a glitch (or occasionally a `turd'; compare mouse droppings). See also cookie.

*-Magic Number

1. n. [UNIX/C] In source code, some non-obvious constant whose value is significant to the operation of a program and that is inserted inconspicuously in-line (hardcoded), rather than expanded in by a symbol set by a commented `#define'. Magic numbers in this sense are bad style.
2. A number that encodes critical information used in an algorithm in some opaque way. The classic examples of these are the numbers used in hash or CRC functions, or the coefficients in a linear congruential generator for pseudo-random numbers. This sense actually predates and was ancestral to the more common sense 1.
3. Special data located at the beginning of a binary data file to indicate its type to a utility. Under UNIX, the system and various applications programs (especially the linker) distinguish between types of executable file by looking for a magic number. Once upon a time, these magic numbers were PDP-11 branch instructions that skipped over header data to the start of executable code; 0407, for example, was octal for `branch 16 bytes relative'. Nowadays only a wizard knows the spells to create magic numbers. How do you choose a fresh magic number of your own? Simple -- you pick one at random. See? It's magic! *The* magic number, on the other hand, is 7+/
4. See “The magical number seven, plus or minus two some limits on our capacity for processing information” by George Miller, in the “Psychological Review” 63:81-97 (1956). This classic paper established the number of distinct items (such as numeric digits) that humans can hold in short-term memory. Among other things, this strongly influenced the interface design of the phone system.

*-Magic Smoke

n. A substance trapped inside IC packages that enables them to function (also called `blue smoke'; this is similar to the archaic `phlogiston' hypothesis about combustion). Its existence is demonstrated by what happens when a chip burns up -- the magic smoke gets let out, so it doesn't work any more. See smoke test, let the smoke out. Usenetter Jay Maynard tells the following story “Once, while hacking on a dedicated Z80 system, I was testing code by blowing EPROMs and plugging them in the system, then seeing what happened. One time, I plugged one in backwards. I only discovered that *after* I realized that Intel didn't put power-on lights under the quartz windows on the tops of their EPROMs -- the die was glowing white-hot. Amazingly, the EPROM worked fine after I erased it, filled it full of zeros, then erased it again. For all I know, it's still in service. Of course, this is because the magic smoke didn't get let out. ” Compare the original phrasing of Murphy's Law.

Magnetic Card

A card with a magnetizable layer on which data can be stored. (FP) (ISO) (~) See also band, magnetic tape.

Magnetic Core Storage

A storage device that uses magnetic properties of such materials as iron, iron oxide, or ferrite and in such shapes as wires, tapes, toroids, rods, or thin film.

Magnetic Disk

A flat circular plate with a magnetizable surface layer on one or both sides of which data can be stored. (FP) (ISO)

Magnetic Disk Unit

A device that contains magnetic disks, a disk drive, one or more magnetic heads, and associated controls. (FP) (ISO)

Magnetic Drum

A right circular cylinder with a magnetizable layer on which data can be stored. (FP) (ISO)

Magnetic Drum Unit

A device that contains a magnetic drum, the mechanism for moving it, magnetic heads, and associated controls. (FP) (ISO)

Magnetic Field

Area where magnetic forces can be detected.

Magnetic Field Intensity

The magnetic force required to produce a desired magnetic flux given as the symbol H. (CSC-STD-005-85;) See Oersted.

Magnetic Flux

Lines of force representing a magnetic field. (CSC-STD-005-85;)

Magnetic Flux Density

1. Flux per unit area perpendicular to the direction of the flux.
2. Representation of the strength of a magnetic field, given as the symbol B.
3. The representation of the strength of a magnetic field, given as the symbol B. (CSC-STD-005-85;) See Flux.

Magnetic Media

1. Media used to store computer data using magnetic force. There are currently three types of magnetic media. They are defined based on their coercivity as: 1. Type 1. Media whose coercivity is no greater than 350 Oersteds (Oe).
2. Type 2. Media whose coercivity lies in the range of 351 to 750 Oe.
3. Above Type 2. Media whose coercivity is 751 Oe or higher.

Magnetic Oxide

Surface coating on magnetic media which is sensitive to magnetic forces and allows the media to retain data images.

Magnetic Remanence

1. A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.
2. Magnetic representation of residual information that remains on a magnetic medium after the medium has been erased or overwritten. NOTE: Magnetic remanence refers to data remaining on magnetic storage media after removal of the power or after degaussing.
3. A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on storage media after removal of the power. (*NCSC-WA*-001-85;)

Magnetic Saturation

The condition in which an increase in magnetizing force will produce or result in little or no increase in magnetic flux. (CSC-STD-005-85;)

Magnetic Tape

1. A tape with a magnetizable layer on which data can be stored. (FP) (ISO)
2. A tape or ribbon of any material impregnated or coated with magnetic or other material on which information may be placed in the form of magnetically polarized spots. (JCS1-DoD) See also band (def. #2), interblock gap, magnetic card, phase-encoded recording.

Magnetic Tapes

*-Mail Storm

n. [from broadcast storm, influenced by `maelstrom'] What often happens when a machine with an Internet connection and active users re-connects after extended downtime --- a flood of incoming mail that brings the machine to its knees.

*-Mailbomb

1. v. (also mail bomb) [Usenet] To send, or urge others to send, massive amounts of email to a single system or person, esp. with intent to crash or spam the recipient's system. Sometimes done in retaliation for a perceived serious offense. Mailbombing is itself widely regarded as a serious offense -- it can disrupt email traffic or other facilities for innocent users on the victim's system, and in extreme cases, even at upstream sites.
2. n. An automatic procedure with a similar effect.
3. n. The mail sent. Compare letterbomb, nastygram, BLOB (sense 2) .

Mailbox

*-Mailing List

1. n. (often shortened in context to `list') 1. An email address that is an alias (or macro, though that word is never used in this connection) for many other email addresses. Some mailing lists are simple `reflectors', redirecting mail sent to them to the list of recipients. Others are filtered by humans or programs of varying degrees of sophistication; lists filtered by humans are said to be `moderated'.
2. The people who receive your email when you send it to such an address. Mailing lists are one of the primary forms of hacker interaction, along with Usenet. They predate Usenet, having originated with the first UUCP and ARPANET connections. They are often used for private information-sharing on topics that would be too specialized for or inappropriate to public Usenet groups. Though some of these maintain almost purely technical content (such as the Internet Engineering Task Force mailing list), others (like the `sf-lovers' list maintained for many years by Saul Jaffe) are recreational, and many are purely social. Perhaps the most infamous of the social lists was the eccentric bandykin distribution; its latter-day progeny, lectroids and tanstaafl, still include a number of the oddest and most interesting people in hackerdom. Mailing lists are easy to create and (unlike Usenet) don't tie up a significant amount of machine resources (until they get very large, at which point they can become interesting torture tests for mail software). Thus, they are often created temporarily by working groups, the members of which can then collaborate on a project without ever needing to meet face-to-face. Much of the material in this lexicon was criticized and polished on just such a mailing list (called `jargon-friends'), which included all the co-authors of Steele-1983.

*-Main Loop

n. The top-level control flow construct in an input- or event-driven program, the one which receives and acts or dispatches on the program's input. See also driver.

*-Mainframe

n. Term originally referring to the cabinet containing the central processor unit or `main frame' of a room-filling Stone Age batch machine. After the emergence of smaller `minicomputer' designs in the early 1970s, the traditional big iron machines were described as `mainframe computers' and eventually just as mainframes. The term carries the connotation of a machine designed for batch rather than interactive use, though possibly with an interactive timesharing operating system retrofitted onto it; it is especially used of machines built by IBM, Unisys, and the other great dinosaurs surviving from computing's Stone Age. It has been common wisdom among hackers since the late 1980s that the mainframe architectural tradition is essentially dead (outside of the tiny market for number-crunching supercomputers (see cray)), having been swamped by the recent huge advances in IC technology and low-cost personal computing. As of 1993, corporate America is just beginning to figure this out -- the wave of failures, takeovers, and mergers among traditional mainframe makers have certainly provided sufficient omens (see dinosaurs mating).

Maintainability

1. A characteristic of design and installation which is expressed as the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources. (~)
2. The ease with which maintenance of a functional unit can be performed in accordance with prescribed requirements. (FP) (ISO) See also availability, failure, mean time between failures, mean time to repair, mean time to service restoral.

Maintenance

1. All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (JCS1-NATO)
2. All supply and repair action taken to keep a force in condition to carry out its mission. (JCS1-NATO)
3. The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it may be continuously utilized, at its

original or designed capacity and efficiency, for its intended purpose. (JCS1-NATO)

4. Any activity intended to restore or retain a functional unit in a state in which the unit can perform its required functions. Maintenance includes keeping a functional unit in a specified state by performing activities such as tests, measurements, replacements, adjustments, and repairs. (FP) (ISO) (~) See also corrective maintenance, preventive maintenance.

Maintenance Hook

Special instructions in software to allow easy maintenance and additional feature development. These are not clearly defined during access for design specification. Hooks frequently allow entry into the code at unusual points or without the usual checks so they are a serious security risk if they are not removed prior to live implementation. Maintenance hooks are simply special types of trap doors. (*NCSC-WA*-001-85;)

Maintenance Key

Key intended only for off-the-air in-shop use.

#-Maintenance Of Configuration Documentation

The ISSO must know what the current architecture is as a basis for configuration management. (Source: DACUM IV).

#-Maintenance Procedures, Contract Employee

The procedures to be followed when a contract employee does the maintenance. (Source: DACUM IV).

#-Maintenance Procedures, Local Employee

The procedures to be followed when one of your employees does maintenance. (Source: DACUM IV).

MAJCOM

Major Command

MAJCOM C4 Systems Security Office

Office charged with the responsibility for managing and executing the C4 systems security program for a MAJCOM, Field Operating Agency, or Direct Reporting Unit. The office reports to the MAJCOM Designated Approving Authority (DAA) and provides security guidance to the Base C4 Systems Security Offices.

MAJCOM Computer System Security Manager

(MCSSM) Term no longer used. Prior to the MAJCOM C4 Systems Security Office, this was the individual charged with the responsibility for managing and executing the computer security program for a Major Command, Separate Operating Agency, or Direct Reporting Unit.

MAJCOM Computer System Security Manager (MCSSM)

Term no longer used. Prior to the MAJCOM C4 Systems Security Office, this was the individual charged with the responsibility for managing and executing the computer security program for a Major Command, Separate Operating Agency, or Direct Reporting Unit.

Major Information System

An information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources. (A-130)

#-Malicious Code

Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e. g. , a Trojan horse. (Source: *NCSC-TG*-0004).

Malicious Logic

Hardware, software, or firmware that are intentionally included in a system for an unauthorized purpose. An example is a Trojan Horse. (*NCSC-WA*-001-85;; CSC-STD-003-85;; CSC-STD-004-85;)

*-Management

1. n. Corporate power elites distinguished primarily by their distance from actual productive work and their chronic failure to manage (see also suit). Spoken derisively, as in "*Management* decided that . ".
2. Mythically, a vast bureaucracy responsible for all the world's minor irritations. Hackers' satirical public notices are often signed `The Mgt'; this derives from the "Illuminatus" novels (see the Bibliography in Appendix C).

Management Control Process

Management Information System

(MIS) An organized assembly of resources and procedures required to collect, process, and distribute data for use in decision making. (~)

#-Management Of The Security Function

This KSA has no definition.

Manchester Encoding

A means by which data and clock signals can be combined into a single self-synchronizing data stream. Each encoded bit contains a transition at the midpoint of a bit period; the direction of transition determines whether the bit is a "0" or a "1. " The first half is the true bit value; the second half is the com-

plement of the true bit value. (~) See also alternate mark inversion signal.

Mandatory

Change to a COMSEC end item that the modification National Security Agency requires to be completed and reported by a specified date. NOTE: This type of modification should not be confused with modifications that are optional to the National Security Agency, but have been adjudged mandatory by a given department or agency. The latter modification may have an installation deadline established and controlled solely by the user's headquarters.

Mandatory Access

Means of restricting access to objects control based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i. e. , clearance) of subjects to access information of such sensitivity.

Mandatory Access Control

(MAC) A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i. e. , clearance) of subjects to access information of such sensitivity. (CSC-STD-001-83;; CSC-STD-004-85;; *NCSC-WA*-001-85;)

Mandatory Access Control (MAC)

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i. e. , clearance) of subjects to access information of such sensitivity. (*DOD* 5200. 28-STD; CSC-STD-004-85)

#-Mandatory Access Controls

A means of restricting access to objects based on the sensitively (as represented by a label) of the information contained in the objects and the formal authorization (i. e. , clearance) of subjects to access information of such sensitivity. Compare discretionary access control. (Source: *NCSC-TG*-0004).

Mandatory Modification

(MAN) Change to a COMSEC end item that the National Security Agency requires to be completed and reported by a specified date. NOTE: This type of modification should not be confused with modifications which are optional to the National Security Agency, but have been adjudged mandatory by a given department or agency. The latter modification may have an installation deadline established and controlled solely by the user's headquarters.

Mandatory Protection

Result of a system that preserves the sensitivity labels of major data structures in the system and uses them to enforce mandatory access controls.

*-Mandelbug

/man'del-buhg/ n. [from the Mandelbrot set] A bug whose underlying causes are so complex and obscure as to make its behavior appear chaotic or even nondeterministic. This term implies that the speaker thinks it is a Bohr bug, rather than a heisenbug. See also schroedinbug.

*-Manged

/mahnjd/ n. [probably from the French `manger' or Italian `mangiare', to eat; perhaps influenced by English `mange', `mangy'] adj. Refers to anything that is mangled or damaged, usually beyond repair. “The disk was manged after the electrical storm. ” Compare mung.

*-Mangle

vt. Used similarly to mung or scribble, but more violent in its connotations; something that is mangled has been irreversibly and totally trashed.

*-Mangler

n. [DEC] A manager. Compare mango; see also management. Note that system mangler is somewhat different in connotation.

*-Mango

/mang'go/ n. [orig. in-house jargon at Symbolics] A manager. Compare mangler. See also devo and doco.

Manipulation Detection

A mechanism which is used to detect whether a data unit has been modified (either accidently or intentionally). (SS;)

Manipulative

Alteration or simulation of friendly communications telecommunications for the purpose of deception. NOTE: Manipulative communications deception may involve establishment of bogus communications structures, transmission of deception messages, and expansion or creation of communications schedules on existing structures to display an artificial volume of messages.

Manipulative Communications Deception

1. Alteration or simulation of friendly telecommunications for the purpose of deception. NOTE: Manipulative communications deception may involve establishment of bogus communications structures, transmission of deception messages, and expansion or creation of communications schedules on existing structures to display an artificial volume of messages.
2. The alteration or simulation of friendly telecommunications for the purpose of deception

NOTE: May consist of any or all of the following: establishment of bogus communications structures, transmission of deception messages, expansion or creation of communications schedules on existing structures to display an artificial volume of messages (NSA, *National INFOSEC Glossary*, 10/88) See Communications Deception and Imitative Communications Deception.

Manual Cryptosystem

Cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment or auto-manual devices.

Manual Remote

Procedure by which a distant crypto-rekeying equipment is rekeyed electrically, with specific actions required by the receiving terminal operator.

Manual Remote Rekeying

Procedure by which a distant crypto-equipment is rekeyed electrically, with specific actions required by the receiving terminal operator.

*-Manularity

/man`yoo-la'ri-tee/ n. [prob. fr. techspeak `manual' + `granularity'] A notional measure of the manual labor required for some task, particularly one of the sort that automation is supposed to eliminate. “Composing English on paper has much higher manularity than using a text editor, especially in the revising stage. ” Hackers tend to consider manularity a symptom of primitive methods; in fact, a true hacker confronted with an apparent requirement to do a computing task by hand will inevitably seize the opportunity to build another tool (see toolsmith).

MAPLESS

Mixed paradigm APL-based Expert System Shell. The basic system used in creating supershells.

*-Marbles

pl. n. [from mainstream “lost all his/her marbles”] The minimum needed to build your way further up some hierarchy of tools or abstractions. After a bad system crash, you need to determine if the machine has enough marbles to come up on its own, or enough marbles to allow a rebuild from backups, or if you need to rebuild from scratch. “This compiler doesn't even have enough marbles to compile hello, world. ”

*-Marginal

1. adj. Extremely small. “A marginal increase in core can decrease GC time drastically. ” In everyday terms, this means that it is a lot easier to clean off your desk if you have a spare place to put some of the junk while you sort through it.
2. Of extremely small merit. “This proposed new feature seems rather marginal to me. ”
3. Of extremely small probability of winning. “The power supply was rather marginal anyway; no wonder it fried. ”

*-Marginal Hacks

n. Margaret Jacks Hall, a building into which the Stanford AI Lab was moved near the beginning of the 1980s (from the D. C. Power Lab).

*-Marginally

adv. Slightly. “The ravs here are only marginally better than at Small Eating Place. ” See epsilon.

Mark

1. In binary communications, one of the two significant conditions of encoding. (~) Synonyms marking pulse, marking signal. See also space.
2. A symbol or symbols that indicate the beginning or the end of a field, of a word, or of a data item in a file, record, or block. (FP) (ISO) See also code element, marking bias, modulation, neutral operation, pulse, signal transition.

*-Marketroid

/mar'k*-troyd/ n. alt. `marketing slime', `marketeer', `marketing droid', `marketdroid'. A member of a company's marketing department, esp. one who promises users that the next version of a product will have features that are not actually scheduled for inclusion, are extremely difficult to implement, and/or are in violation of the laws of physics; and/or one who describes existing features (and misfeatures) in ebullient, buzzword-laden adspeak. Derogatory. Compare droid.

Marking

1. The process of placing a sensitivity designator (e. g. , “confidential”) with data such that its sensitivity is communicated. Marking is not restricted to the physical placement of a sensitivity designator, as might be done with a rubber stamp, but can involve the use of headers for network messages, special fields in databases, etc. (WB)
2. See LABEL.

#-Marking Of Media

The physical marking of all storage media (i. e. , floppies, tapes) to reflect proper classification, to facilitate control and storage. The marking must be in accordance with national and local policies.

#-Marking Of Sensitive Information

This KSA has no definition.

Marking Pulse

See mark.

Marking Signal

See mark.

*-Mars

n. A legendary tragic failure, the archetypal Hacker Dream Gone Wrong. Mars was the code name for a family of PDP-10 compatible computers built by Sys-

tems Concepts (now, The SC Group) the multiprocessor SC-30M, the small uniprocessor SC-25M, and the never-built superprocessor SC-40M. These machines were marvels of engineering design; although not much slower than the unique Foonly F-1, they were physically smaller and consumed less power than the much slower DEC KS10 or Foonly F-2, F-3, or F-4 machines. They were also completely compatible with the DEC KL10, and ran all KL10 binaries (including the operating system) with no modifications at about 2--3 times faster than a KL10. When DEC cancelled the Jupiter project in 1983, Systems Concepts should have made a bundle selling their machine into shops with a lot of software investment in PDP-10s, and in fact their spring 1984 announcement generated a great deal of excitement in the PDP-10 world. TOPS-10 was running on the Mars by the summer of 1984, and TOPS-20 by early fall. Unfortunately, the hackers running Systems Concepts were much better at designing machines than at mass producing or selling them; the company allowed itself to be sidetracked by a bout of perfectionism into continually improving the design, and lost credibility as delivery dates continued to slip. They also overpriced the product ridiculously; they believed they were competing with the KL10 and VAX 8600 and failed to reckon with the likes of Sun Microsystems and other hungry startups building workstations with power comparable to the KL10 at a fraction of the price. By the time SC shipped the first SC-30M to Stanford in late 1985, most customers had already made the traumatic decision to abandon the PDP-10, usually for VMS or UNIX boxes. Most of the Mars computers built ended up being purchased by CompuServe. This tale and the related saga of Foonly hold a lesson for hackers if you want to play in the Real World, you need to learn Real World moves.

*-Martian

n. A packet sent on a TCP/IP network with a source address of the test loopback interface [127. 0. 0. 1]. This means that it will come back labeled with a source address that is clearly not of this earth. “The domain server is getting lots of packets from Mars. Does that gateway have a martian filter?”

MASINT

Measurement and Signature Intelligence

Masquerade

The pretence by an entity to be a different entity. (SS;)

Masquerading

1. An attempt to gain access to a system by posing as an authorized user. (*AR* 380-380)
2. Synonymous with MIMICKING and IMPERSONATION.

*-Massage

vt. Vague term used to describe `smooth' transformations of a data set into a different form, esp. transformations that do not lose information. Connotes less pain than munch or crunch. “He wrote a program that massages X bitmap files into GIF format. ” Compare slurp.

Master Crypto-Ignition Key

Crypto-ignition key that is able to initialize crypto-ignition key, when interacting with its associated crypto-equipment.

Master Station

1. In a data network, the station that has been designated by the control station to ensure data transfer to one or more slave stations. Note: A master station has control of one or more data links of the data communication network at a given instant. The assignment of master status to a given station is temporary and is controlled by the control station according to the procedures set forth in the operational protocol. Master status is normally conferred upon a station so that it may transmit a message, but a station need not have a message to send to be nominated as master.
2. In navigation systems employing precise time dissemination, a station whose clock is used to synchronize the clocks of subordinate stations.
3. In basic mode link control, the data station that has accepted an invitation to ensure a data transfer to one or more slave stations. At a given instant, there can be only one master station on a data link. (FP) (ISO) See also contention, control station, data communication, data transmission, interrogation, network, primary station, secondary station, slave station, tributary station.

Matching Programs

Material

“Material” refers to data processed, stored, or used in, and information produced by an ADP system regardless of form or medium, e. g. , programs, reports, data sets or files, records, and data elements. (*DOD* 5200-28M; *AR* 380-380; *AFR* 205-16)

Material Symbol

Communications circuit identifier used for key card resupply purposes. (AF9K_JBC. TXT) (MATSYM) Communications circuit identifier used for key card resupply purposes.

*-Math-Out

n. [poss. from `white-out' (the blizzard variety)] A paper or presentation so encrusted with mathematical or other formal notation as to be incomprehensible. This may be a device for concealing the fact that it is

actually content-free. See also numbers, social science number.

*-Matrix

1. n. [FidoNet] What the Opus BBS software and sysops call FidoNet.
2. Fanciful term for a cyberspace expected to emerge from current networking experiments (see network, the).
3. The totality of present-day computer networks.

MATSYM

See MATerial SYMbol.

Maximum Access Time

*-Maximum Maytag Mode

n. What a washing machine or, by extension, any hard disk is in when it's being used so heavily that it's shaking like an old Maytag with an unbalanced load. If prolonged for any length of time, can lead to disks becoming walking drives.

*-Mbogo, Dr. Fred

/*m-boh'goh, dok'tr fred/ n. [Stanford] The archetypal man you don't want to see about a problem, esp. an incompetent professional; a shyster. “Do you know a good eye doctor?” “Sure, try Mbogo Eye Care and Professional Dry Cleaning. ” The name comes from synergy between bogus and the original Dr. Mbogo, a witch doctor who was Gomez Addams' physician on the old “Addams Family” TV show. Compare Bloggs Family, the, see also fred.

Measure Of Effectiveness

Any mutually agreeable parameter of a problem which induces a rank ordering on the perceived set of goals. (MK;)

Measurement And Signature Intelligence

(MASINT) Information derived from technical sensors for the purpose of identifying distinctive features associated with the source, emitter, or sender to facilitate subsequent identification and/or measurement of the same. *Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source emitter, or sender, and to facilitate subsequent identification and/or measurement of the same. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

*-Meatware

n. Synonym for wetware. Less common.

Media

The peripheral device related physical components used for the storage of data such as tape reels, floppy diskettes, etc. (WB;)

#-Media Convergence

This KSA has no definition.

Mediation

Medium

1. In telecommunications, the transmission path along which a signal is propagated, such as wire pair, coaxial cable, waveguide, optical fiber, or radio path. (~) See also circuit, communications, link, loop, transmission channel.
2. The material on which data are recorded, e. g. , paper tape, punched card, magnetic tape or disk. (~)

Medium Access Control Sublayer

(MAC) In a local area network, that part of the OSI Data Link Layer that supports topology-dependent functions and uses the services of the Physical Layer to provide services to the logical link control sublayer. See also layer (def. #2), link, Open Systems Interconnection--Reference Model.

*-Meeces

/mees'*z/ n. [TMRC] Occasional furry visitors who are not urchins. [That is, mice. This may no longer be in live use; it clearly derives from the refrain of the early-1960s cartoon character Mr. Jinx “I hate meeces to *pieces*!” --- ESR]

MEECN

See Minimum Essential Emergency Communications Network.

*-Meg

/meg/ n. See quantifiers.

*-Mega

/me'g*/ pref. [SI] See quantifiers.

*-Megapenny

/meg'*-pen`ee/ n. $10,000 (1 cent * 10^6). Used semi-humorously as a unit in comparing computer cost and performance figures.

*-MEGO

1. /me'goh/ or /mee'goh/ [`My Eyes Glaze Over', often `Mine Eyes Glazeth (sic) Over', attributed to the futurologist Herman Kahn] Also `MEGO factor'. 1. n. A handwave intended to confuse the listener and hopefully induce agreement because the listener does not want to admit to not understanding what is going on. MEGO is usually directed at senior management by engineers and contains a high proportion of TLAs.
2. excl. An appropriate response to MEGO tactics.

3. Among non-hackers, often refers not to behavior that causes the eyes to glaze, but to the eye-glazing reaction itself, which may be triggered by the mere threat of technical detail as effectively as by an actual excess of it.

*-Meltdown, Network

n. See network meltdown.

*-Meme

/meem/ n. [coined by analogy with `gene', by Richard Dawkins] An idea considered as a replicator, esp. with the connotation that memes parasitize people into propagating them much as viruses do. Used esp. in the phrase `meme complex' denoting a group of mutually supporting memes that form an organized belief system, such as a religion. This lexicon is an (epidemiological) vector of the `hacker subculture' meme complex; each entry might be considered a meme. However, `meme' is often misused to mean `meme complex'. Use of the term connotes acceptance of the idea that in humans (and presumably other tool- and language-using sophonts) cultural evolution by selection of adaptive ideas has superseded biological evolution by selection of hereditary traits. Hackers find this idea congenial for tolerably obvious reasons.

*-Meme Plague

n. The spread of a successful but pernicious meme, esp. one that parasitizes the victims into giving their all to propagate it. Astrology, BASIC, and the other guy's religion are often considered to be examples. This usage is given point by the historical fact that `joiner' ideologies like Naziism or various forms of millennarian Christianity have exhibited plague-like cycles of exponential growth followed by collapses to small reservoir populations.

*-Memetics

/me-met'iks/ n. [from meme] The study of memes. As of mid-1994, this is still an extremely informal and speculative endeavor, though the first steps towards at least statistical rigor have been made by H. Keith Henson and others. Memetics is a popular topic for speculation among hackers, who like to see themselves as the architects of the new information ecologies in which memes live and replicate.

Memory

1. All of the addressable storage space in a processing unit and other internal memory that is used to execute instructions. (FP) (ISO)
2. Main storage, when used in reference to calculators, microcomputers, and some minicomputers.
3. Computer component used to hold information in electrical, magnetic, or optical form. See Nonvolatile Memory and Volatile Memory, read-only storage, register.

#-Memory (Non-Volatile)

Memory that retains its information after the power has been removed. (Source: NSAM 130-1).

#-Memory (Random)

1. A storage technique in which the access time to obtain information is independent of the location of the information most recently accessed. (Source Panel of experts)
2. (RAM's) memory which any unit of addressable information can be accessed in an identical amount of time.

#-Memory (Sequential)

1. A storage technique in which the stored information becomes available only in a sequential manner, regardless of whether or not all the information is needed, eg, a magnetic tape.
2. Memory in which information must be addressed and accessed in a bit stream manner.

#-Memory (Volatile)

1. Memory that does not retain its information after the primary power has been removed. (Source Panel of experts).
2. A memory which looses its information when all power is removed.

Memory Address Translation Unit

Memory Bounds

The limits in the range of storage addresses for a protected region in memory. (*FIPS PUB* 39;; *AR* 380-380;)

Memory Bounds Checking

See Bounds Checking.

*-Memory Leak

n. An error in a program's dynamic-store allocation logic that causes it to fail to reclaim discarded memory, leading to eventual collapse due to memory exhaustion. Also (esp. at CMU) called core leak. These problems were severe on older machines with small, fixed-size address spaces, and special “leak detection” tools were commonly written to root them out. With the advent of virtual memory, it is unfortunately easier to be sloppy about wasting a bit of memory (although when you run out of memory on a VM machine, it means you've got a *real* leak!). See aliasing bug, fandango on core, smash the stack, precedence lossage leaky heap, leak.

Memory Mapping

Memory Page Cache

***-Memory Smash**

n. [XEROX PARC] Writing through a pointer that doesn't point to what you think it does. This occasionally reduces your machine to a rubble of bits. Note that this is subtly different from (and more general than) related terms such as a memory leak or fandango on core because it doesn't imply an allocation error or overrun condition.

Menu

A displayed list of options from which a user selects actions to be performed. (FP)

***-Menuitis**

/men`yoo-i:'tis/ n. Notional disease suffered by software with an obsessively simple-minded menu interface and no escape. Hackers find this intensely irritating and much prefer the flexibility of command-line or language-style interfaces, especially those customizable via macros or a special-purpose language in which one can encode useful hacks. See user-obsequious, drool-proof paper, WIMP environment, for the rest of us.

***-Mess-Dos**

/mes-dos/ n. Derisory term for MS-DOS. Often followed by the ritual banishing “Just say No!” See MS-DOS. Most hackers (even many MS-DOS hackers) loathe MS-DOS for its single-tasking nature, its limits on application size, its nasty primitive interface, and its ties to IBMness (see fear and loathing). Also `mess-loss', `messy-dos', `mess-dog', `mess-dross', `mush-dos', and various combinations thereof. In Ireland and the U. K. it is even sometimes called `Domestos' after a brand of toilet cleanser.

Message

1. Any thought or idea expressed briefly in a plain, coded, or secret language, prepared in a form suitable for transmission by any means of communication. (JCS1-NATO) Note: A message may be a one-unit message or a multiunit message.
2. [In telecommunications,] Record information expressed in plain or encrypted language and prepared in a format specified for intended transmission by a telecommunications system. (JCS1-DoD)
3. An arbitrary amount of information whose beginning and end are defined or implied. (FP) See also signal (def. #4), signal message.

Message Alignment Indicator

In a signal message, data transmitted between the user part and the message transfer part to identify the boundaries of the signal message. See also signal message.

Message Authentication

Data element associated with an code authenticated message which allows a receiver to verify the integrity of the message.

Message Authentication Code

(MAC) A data-authenticator specifically designed for messages traveling on computer networks, which is implemented as an encryption-generated and (often) truncated quantity that accompanies the message it protects. (WB)

#-Message Authentication Codes

Data element associated with an authenticated message which allows a receiver to verify the integrity of the message. (Source: NSTISSI 4009).

Message Broadcast

An electronic-mail conference capability using data terminals. Note: Control can be maintained by the user or by the network.

Message Distribution Center

Message Externals

Non-textual (outside the message text) characteristics of transmitted messages.

Message Format

A predetermined or prescribed spatial or time-sequential arrangement of the parts of a message that is recorded in or on a data storage medium. Note: Messages prepared for electrical transmission are usually composed on a printed blank form with spaces for each part of the message and for administrative entries.

Message Handling Systems

The CCITT X. 400 family of services and protocols that provides the functions for global electronic-mail transfer among local mail systems. (FS1037S1. TXT) (MHS) The CCITT X. 400 family of services and protocols that provides the functions for global electronic-mail transfer among local mail systems.

Message Indicator

Sequence of bits transmitted over a telecommunications system for the purpose of crypto-equipment synchronization. NOTE: Some off-line cryptosystems, such as the KL-51 and one-time pad systems, employ message indicators to establish decryption starting points.

Message Register Leads

Terminal equipment leads at the interface used solely for receiving dc message register pulses from a central office at a PBX so that message unit information normally recorded at the central office only is also recorded at the PBX. (After CFR 47)

***-Meta Bit**

n. The top bit of an 8-bit character, which is on in character values 128--255. Also called high bit, alt bit, or hobbit. Some terminals and consoles (see

space-cadet keyboard) have a META shift key. Others (including, *mirabile dictu*, keyboards on IBM PC-class machines) have an ALT key. See also bucky bits. Historical note although in modern usage shaped by a universe of 8-bit bytes the meta bit is invariably hex 80 (octal 0200), things were different on earlier machines with 36-bit words and 9-bit bytes. The MIT and Stanford keyboards (see space-cadet keyboard) generated hex 100 (octal 400) from their meta keys.

Metadata

Metal Particle Tape

Type of tape whose surface coating is produced from pure iron and having very high coercivity in the range of 850 to 1250 Oe (above Type II).

*-Metasyntactic Variable

n. A name used in examples and understood to stand for whatever thing is under discussion, or any random member of a class of things under discussion. The word foo is the canonical example. To avoid confusion, hackers never (well, hardly ever) use `foo' or other words like it as permanent names for anything. In filenames, a common convention is that any filename beginning with a metasyntactic-variable name is a scratch file that may be deleted at any time. To some extent, the list of one's preferred metasyntactic variables is a cultural signature. They occur both in series (used for related groups of variables or objects) and as singletons. Here are a few common signatures foo, bar, baz, quux, quuux, quuuux. MIT/Stanford usage, now found everywhere (thanks largely to early versions of this lexicon!). At MIT (but not at Stanford), baz dropped out of use for a while in the 1970s and '80s. A common recent mutation of this sequence inserts qux before quux. bazola, ztesch Stanford (from mid-'70s on). foo, bar, thud, grunt This series was popular at CMU. Other CMU-associated variables include gorp. foo, bar, fum This series is reported to be common at XEROX PARC. fred, barney See the entry for fred. These tend to be Britishisms. corge, grault, flarp Popular at Rutgers University and among GOSMACS hackers. zxc, spqr, wombat Cambridge University (England). shme Berkeley, GeoWorks, Ingres. Pronounced /shme/ with a short /e/. foo, bar, zot Helsinki University of Technology, Finland. blarg, wibble New Zealand. toto, titi, tata, tutu France. pippo, pluto, paperino Italy. Pippo /pee'po/ and Paperino /pa-per-ee'-no/ are the Italian names for Goofy and Donald Duck. aap, noot, mies The Netherlands. These are the first words a child used to learn to spell on a Dutch spelling board. Of all these, only `foo' and `bar' are universal (and baz nearly so). The compounds foobar and `foobaz' also enjoy very wide currency. Some jargon terms are also used as metasyntactic names; barf and mumble, for example. See also Commonwealth Hackish for discussion of numerous metasyntactic variables found in Great Britain and the Commonwealth.

Method

1. A special kind of slot which specifies (as the slot's value) an activity that can be invoked explicitly; the activity must be expressed in APL or STAPLE and may be one of the predefined rule-chaining methods applied to a specific class of rules. (ET;)
2. A special kind of Slot (q. v.) that specifies as the value of the Slot an activity that can be invoked explicitly. Methods can take the form of applying one of the predefined rule-chaining methods to a specific class of rules. (MA;)

Metric

A function, often denoted “Dist”, of two values from a particular type that returns the “distance” between the values. (MA;)

#-Metrics

This KSA has no definition.

Metropolitan Area Network MAN

A loosely defined term generally understood to describe a network covering an area larger than a local area network. (~) Note: It typically interconnects two or more local area networks, may operate at a higher speed, may cross administrative boundaries, and may use multiple access methods. See also communications, local area network, medium interface connector, medium interface point, wide area network. (FS1037S1. TXT) (MAN)

*-MFTL

/M-F-T-L/ [abbreviation`My Favorite Toy Language']

1. adj. Describes a talk on a programming language design that is heavy on the syntax (with lots of BNF), sometimes even talks about semantics (e. g. , type systems), but rarely, if ever, has any content (see content-free). More broadly applied to talks --- even when the topic is not a programming language -- in which the subject matter is gone into in unnecessary and meticulous detail at the sacrifice of any conceptual content. “Well, it was a typical MFTL talk”.
2. n. Describes a language about which the developers are passionate (often to the point of prosyletic zeal) but no one else cares about. Applied to the language by those outside the originating group. “He cornered me about type resolution in his MFTL. ” The first great goal in the mind of the designer of an MFTL is usually to write a compiler for it, then bootstrap the design away from contamination by lesser languages by writing a compiler for it in itself. Thus, the standard put-down question at an MFTL talk is “Has it been used for anything besides its own compiler?”. On the other hand, a language that *cannot* be used

to write its own compiler is beneath contempt. See break-even point. (On a related note, Doug McIlroy once proposed a test of the generality and utility of a language and the operating system under which it is compiled “Is the output of a FORTRAN program acceptable as input to the FORTRAN compiler?” In other words, can you write programs that write programs? (See toolsmith.) Alarming numbers of (language, OS) pairs fail this test, particularly when the language is FORTRAN; aficionados are quick to point out that UNIX (even using FORTRAN) passes it handily. That the test could ever be failed is only surprising to those who have had the good fortune to have worked only under modern systems which lack OS-supported and -imposed “file types”.)

*-Mickey

n. The resolution unit of mouse movement. It has been suggested that the `disney' will become a benchmark unit for animation graphics performance.

*-Mickey Mouse Program

n. North American equivalent of a noddy (that is, trivial) program. Doesn't necessarily have the belittling connotations of mainstream slang “Oh, that's just mickey mouse stuff!”; sometimes trivial programs can be very useful.

*-Micro

1. pref. Very small; this is the root of its use as a quantifier prefix.
2. A quantifier prefix, calling for multiplication by 10^(-6) (see quantifiers). Neither of these uses is peculiar to hackers, but hackers tend to fling them both around rather more freely than is countenanced in standard English. It is recorded, for example, that one CS professor used to characterize the standard length of his lectures as a microcentury -- that is, about 52. 6 minutes (see also attoparsec, nanoacre, and especially microfortnight).
3. Personal or human-scale -- that is, capable of being maintained or comprehended or manipulated by one human being. This sense is generalized from `microcomputer', and is esp. used in contrast with `macro-' (the corresponding Greek prefix meaning `large').
4. Local as opposed to global (or macro-). Thus a hacker might say that buying a smaller car to reduce pollution only solves a microproblem; the macroproblem of getting to work might be better solved by using mass transit, moving to within walking distance, or (best of all) telecommuting.

Microcode

A sequence of microinstructions that is fixed in storage that is not program-addressable, and that performs specific processing functions. (FP)

Microcomputer

A computer system whose processing unit is a microprocessor. A basic microcomputer includes a microprocessor, storage, and an input/output facility which may or may not be on one chip. (FP) See also computer.

Microengine

*-Microfloppies

n. 3. 5-inch floppies, as opposed to 5. 25-inch vanilla or mini-floppies and the now-obsolete 8-inch variety. This term may be headed for obsolescence as 5. 25-inchers pass out of use, only to be revived if anybody floats a sub-3-inch floppy standard. See stiffy, minifloppies.

*-Microfortnight

n. 1/1000000 of the fundamental unit of time in the Furlong/Firkin/Fortnight system of measurement; 1. 2096 sec. (A furlong is 1/8th of a mile; a firkin is 1/4th of a barrel; the mass unit of the system is taken to be a firkin of water). The VMS operating system has a lot of tuning parameters that you can set with the SYSGEN utility, and one of these is TIMEPROMPTWAIT, the time the system will wait for an operator to set the correct date and time at boot if it realizes that the current value is bogus. This time is specified in microfortnights! Multiple uses of the millifortnight (about 20 minutes) and nanofortnight have also been reported.

Microinstruction

An instruction that controls data flow and sequencing in a processor at a more fundamental level than machine instructions. Individual machine instructions and perhaps other functions may be implemented by microprograms. (FP)

*-MicroLenat

/mi:`-kroh-len'-*t/ n. The unit of bogosity, written uL; the consensus is that this is the largest unit practical for everyday use. The microLenat, originally invented by David Jefferson, was promulgated as an attack against noted computer scientist Doug Lenat by a tenured graduate student at CMU. Doug had failed the student on an important exam for giving only “AI is bogus” as his answer to the questions. The slur is generally considered unmerited, but it has become a running gag nevertheless. Some of Doug's friends argue that *of course* a microLenat is bogus, since it is only one millionth of a Lenat. Others have suggested that the unit should be redesignated after the grad student, as the microReid.

Microprocessor
A central processing unit implemented on a single chip. (~) See also computer.

Microprogram
A sequence of microinstructions that are in special storage where they can be dynamically accessed to perform various functions. (FP)

***-MicroReid**
/mi:'kroh-reed/ n. See bogosity.

Microsequencer

***-Microtape**
/mi:'kroh-tayp/ n. Occasionally used to mean a DECtape, as opposed to a macrotape. A DECtape is a small reel, about 4 inches in diameter, of magnetic tape about an inch wide. Unlike those for today's macrotapes, microtape drivers allowed random access to the data, and therefore could be used to support file systems and even for swapping (this was generally done purely for hack value, as they were far too slow for practical use). In their heyday they were used in pretty much the same ways one would now use a floppy disk as a small, portable way to save and transport files and programs. Apparently the term `microtape' was actually the official term used within DEC for these tapes until someone coined the word `DECtape', which, of course, sounded sexier to the marketroids; another version of the story holds that someone discovered a conflict with another company's `microtape' trademark.

Microwave mw
A term loosely applied to those radio frequency wavelengths that are sufficiently short to exhibit some of the properties of light, e. g. , they are easily concentrated into a beam. Commonly used for frequencies from about 1 GHz to 30 GHz. (~) See also frequency, spectrum designation of frequency. (FS1037S1. TXT) (mw)

#-Microwave/Wireless Communications Security
This KSA has no definition.

***-Middle-Endian**
adj. Not big-endian or little-endian. Used of perverse byte orders such as 3-4-1-2 or 2-1-4-3, occasionally found in the packed-decimal formats of minicomputer manufacturers who shall remain nameless. See NUXI problem. Non-US hackers use this term to describe the American mm/dd/yy style of writing dates.

Militarily Critical Technology
Goods accompanied by sophisticated operation, application, or maintenance know how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States. (DODD 2040. 2;)

***-MilliLampson**
/mil'*-lamp`sn/ n. A unit of talking speed, abbreviated mL. Most people run about 200 milliLampsons. The eponymous Butler Lampson (a CS theorist and systems implementor highly regarded among hackers) goes at 1000. A few people speak faster. This unit is sometimes used to compare the (sometimes widely disparate) rates at which people can generate ideas and actually emit them in speech. For example, noted computer architect C. Gordon Bell (designer of the PDP-11) is said, with some awe, to think at about 1200 mL but only talk at about 300; he is frequently reduced to fragments of sentences as his mouth tries to keep up with his speeding brain.

Mimicking
Synonymous with IMPERSONATION and MASQUERADING.

Minicomputer
See computer.

***-Minifloppies**
n. 5. 25-inch vanilla floppy disks, as opposed to 3. 5-inch or microfloppies and the now-obsolescent 8-inch variety. At one time, this term was a trademark of Shugart Associates for their SA-400 minifloppy drive. Nobody paid any attention. See stiffy.

Minimal Protection
(Class D) Class reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation.

Minor Change

Minor Change To A System Of Records
A change that does not significantly change the system; that is, does not affect the character or purpose of the system and does not affect the ability of an individual to gain access to his or her record or to any information pertaining to him or her which is contained in the system; e. g. , changing the title of the system manager. (A-1 30)

***-MIPS**
1. /mips/ n. [abbreviation] 1. A measure of computing speed; formally, `Million Instructions Per Second' (that's 10^6 per second, not 2^(20)!); often rendered by hackers as `Meaningless Indication of Processor Speed' or in other unflattering ways. This joke expresses a nearly universal attitude about the value of most benchmark claims, said attitude being one of the great cultural divides between hackers and marketroids. The singular is

sometimes `1 MIP' even though this is clearly etymologically wrong. See also KIPS and GIPS.

2. Computers, especially large computers, considered abstractly as sources of computrons. “This is just a workstation; the heavy MIPS are hidden in the basement. ”
3. The corporate name of a particular RISC-chip company; among other things, they designed the processor chips used in DEC's 3100 workstation series.
4. Acronym for `Meaningless Information per Second' (a joke, prob. from sense 1).

*-Misbug

/mis-buhg/ n. [MIT] An unintended property of a program that turns out to be useful; something that should have been a bug but turns out to be a feature. Usage rare. Compare green lightning. See miswart.

*-Misfeature

/mis-fee'chr/ or /mis'fee`chr/ n. A feature that eventually causes lossage, possibly because it is not adequate for a new situation that has evolved. Since it results from a deliberate and properly implemented feature, a misfeature is not a bug. Nor is it a simple unforeseen side effect; the term implies that the feature in question was carefully planned, but its long-term consequences were not accurately or adequately predicted (which is quite different from not having thought ahead at all). A misfeature can be a particularly stubborn problem to resolve, because fixing it usually involves a substantial philosophical change to the structure of the system involved. Many misfeatures (especially in user-interface design) arise because the designers/implementors mistake their personal tastes for laws of nature. Often a former feature becomes a misfeature because trade-offs were made whose parameters subsequently change (possibly only in the judgment of the implementors). “Well, yeah, it is kind of a misfeature that file names are limited to six characters, but the original implementors wanted to save directory space and we're stuck with it for now. ”

*-Missed'em-Five

n. Pejorative hackerism for AT&T System V UNIX, generally used by BSD partisans in a bigoted mood. (The synonym `SysVile' is also encountered.) See software bloat, Berzerkeley.

*-Missile Address

n. See ICBM address.

Mission-Critical

Mission-Essential Unclassified Information

Plain text or machine-encoded unclassified data that, as determined by competent authority (e. g. , information owners), has high importance related to accomplishing a DOE mission and requires a degree of protection because unnecessary delays in processing could adversely affect the ability of an owner organization, site, or the Department to accomplish such missions. (*DOE 1360. 2A*)

*-Miswart

/mis-wort/ n. [from wart by analogy with misbug] A feature that superficially appears to be a wart but has been determined to be the Right Thing. For example, in some versions of the EMACS text editor, the `transpose characters' command exchanges the character under the cursor with the one before it on the screen, *except* when the cursor is at the end of a line, in which case the two characters before the cursor are exchanged. While this behavior is perhaps surprising, and certainly inconsistent, it has been found through extensive experimentation to be what most users want. This feature is a miswart.

Mobile COMSEC Facility

COMSEC facility that can be readily moved from one location to another.

#-Mobile Workstation Security

This KSA has no definition.

*-Moby

1. /moh'bee/ [MIT seems to have been in use among model railroad fans years ago. Derived from Melville's “Moby Dick” (some say from `Moby Pickle'). ] 1. adj. Large, immense, complex, impressive. “A Saturn V rocket is a truly moby frob. ” “Some MIT undergrads pulled off a moby hack at the Harvard-Yale game. ” (See “The Meaning of `Hack'”).
2. n. obs. The maximum address space of a machine (see below). For a 680[234]0 or VAX or most modern 32-bit architectures, it is 4,294,967,296 8-bit bytes (4 gigabytes).
3. A title of address (never of third-person reference), usually used to show admiration, respect, and/or friendliness to a competent hacker. “Greetings, moby Dave. How's that address-book thing for the Mac going?”
4. adj. In backgammon, doubles on the dice, as in `moby sixes', `moby ones', etc. Compare this with bignum (sense 3) double sixes are both bignums and moby sixes, but moby ones are not bignums (the use of `moby' to describe double ones is sarcastic). Standard emphatic forms `Moby foo', `moby win', `moby loss'. `Foby moo' a spoonerism due to Richard Greenblatt. 5. The largest available unit of something which is available in discrete increments. Thus, ordering a “moby Coke” at the local fast-food joint is not just a request for a large Coke, it's an explicit request for the largest size they sell. This term entered hackerdom with the Fabritek 256K memory added to the MIT AI PDP-

6 machine, which was considered unimaginably huge when it was installed in the 1960s (at a time when a more typical memory size for a timesharing system was 72 kilobytes). Thus, a moby is classically 256K 36-bit words, the size of a PDP-6 or PDP-10 moby. Back when address registers were narrow the term was more generally useful, because when a computer had virtual memory mapping, it might actually have more physical memory attached to it than any one program could access directly. One could then say “This computer has 6 mobies” meaning that the ratio of physical memory to address space is 6, without having to say specifically how much memory there actually is. That in turn implied that the computer could timeshare six `full-sized' programs without having to swap programs between memory and disk. Nowadays the low cost of processor logic means that address spaces are usually larger than the most physical memory you can cram onto a machine, so most systems have much *less* than one theoretical `native' moby of core. Also, more modern memory-management techniques (esp. paging) make the `moby count' less significant. However, there is one series of widely-used chips for which the term could stand to be revived --- the Intel 8088 and 80286 with their incredibly brain-damaged segmented-memory designs. On these, a `moby' would be the 1-megabyte address span of a segment/offset pair (by coincidence, a PDP-10 moby was exactly 1 megabyte of 9-bit bytes).

Mockingbird

A computer program or process which mimics the legitimate behaviour of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user. (ed. ;)

*-Mod

1. vt. ,n. Short for `modify' or `modification'. Very commonly used -- in fact the full terms are considered markers that one is being formal. The plural `mods' is used esp. with reference to bug fixes or minor design changes in hardware or software, most esp. with respect to patch sets or a diff.
2. Short for modulo but used *only* for its techspeak sense.

*-Mode

n. A general state, usually used with an adjective describing the state. Use of the word `mode' rather than `state' implies that the state is extended over time, and probably also that some activity characteristic of that state is being carried out. “No time to hack; I'm in thesis mode. ” In its jargon sense, `mode' is most often attributed to people, though it is sometimes applied to programs and inanimate objects. In particular, see hack mode, day mode, night mode, demo mode, fireworks mode, and yoyo mode; also talk mode. One also often hears the verbs `enable' and `disable' used in connection with jargon modes. Thus, for example, a sillier way of saying “I'm going to crash” is “I'm going to enable crash mode now”. One might also hear a request to “disable flame mode, please”. In a usage much closer to techspeak, a mode is a special state that certain user interfaces must pass into in order to perform certain functions. For example, in order to insert characters into a document in the UNIX editor `vi', one must type the “i” key, which invokes the “Insert” command. The effect of this command is to put vi into “insert mode”, in which typing the “i” key has a quite different effect (to wit, it inserts an “i” into the document). One must then hit another special key, “ESC”, in order to leave “insert mode”. Nowadays, modeful interfaces are generally considered losing but survive in quite a few widely used tools built in less enlightened times.

*-Mode Bit

n. A flag, usually in hardware, that selects between two (usually quite different) modes of operation. The connotations are different from flag bit in that mode bits are mainly written during a boot or set-up phase, are seldom explicitly read, and seldom change over the lifetime of an ordinary program. The classic example was the EBCDIC-vs. -ASCII bit (#12) of the Program Status Word of the IBM 360. Another was the bit on a PDP-12 that controlled whether it ran the PDP-8 or the LINC instruction set.

Mode Of Operation

Description of the conditions under which an AIS operates, based on the sensitivity of data processed and the clearance levels and authorizations of the users. NOTE: Five modes of operation are authorized for an AIS processing information and for networks transmitting information. See Compartmented Mode, Dedicated Security Mode, Multilevel Security Mode, Partitioned Security Mode, and System-High Security Mode.

Modem

1. `See modulator-demodulator. A device that modulates and demodulates signals. (~) Note 1: Modems are primarily used for converting digital signals into quasi-analog signals for transmission over analog communication channels and for reconverting the quasi-analog signals into digital signals. Note 2: Many additional functions may be added to a modem to provide for customer service and control features. See signal conversion equipment. See also acoustic coupler, data circuit-terminating equipment, input/output device, narrowband modem, peripheral equipment, quasi-analog signal, wideband modem.
2. A device which connects to a telephone line and transforms a digital bit stream into an analog sig-

nal and vice versa. Modems may be internal or external to the hardware of a computer. (NSAM 130-1).

#-Modes Of Operation

1. The security environment and method of operating an ADP system or network. (*OPNAVINST* 5239. lA)
2. The definition of the security environment and approved methods of operating a system. (*NCSC-TG*-004-88)
3. A description of the conditions under which an AIS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. Four modes of operation are authorized: Dedicated Mode - An AIS is operating in the dedicated mode when each user with direct or indirect individual access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following: a. A valid personnel clearance for all information on the system. b. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs). c. A valid need-to-know for all information contained within the system.
4. System-High Mode An AIS is operating in the system-high mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following: a. A valid personnel clearance for all information on the AIS. b. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs). c. A valid need-to-know for some of the information contained within the AIS.
5. Compartmented Mode An AIS is operating in the compartmented mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following: a. A valid personnel clearance for the most restricted information processed in the AIS. b. Formal access approval for, and has signed nondisclosure agreements for that information to which he/she is to have access. c. A valid need-to-know for that information to which he/she is to have access.
6. Multilevel Mode An AIS is operating in the multilevel mode when all the following statements are satisfied concerning the users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts: a. Some do not have a valid personnel clearance for all the information processed in the AIS. b. All have the proper clearance and have the appropriate formal access approval for that information to which he/she is to have access. c. All have a valid need-to-know for that information to which they are to have access.
7. The definition of the security environment and approved methods of operating an Automated Information System. (*NCSC-WA*-001-85;; *OPNAVINST* 5239. 1A;)

Modification

Modularity

*-Modulo

/mod'yu-loh/ prep. Except for. An overgeneralization of mathematical terminology; one can consider saying that 4 equals 22 except for the 9s (4 = 22 mod 9). “Well, LISP seems to work okay now, modulo that GC bug. ” “I feel fine today modulo a slight headache. ”

*-Molly-Guard

/mol'ee-gard/ n. [University of Illinois] A shield to prevent tripping of some Big Red Switch by clumsy or ignorant hands. Originally used of the plexiglass covers improvised for the BRS on an IBM 4341 after a programmer's toddler daughter (named Molly) frobbed it twice in one day. Later generalized to covers over stop/reset switches on disk drives and networking equipment.

*-Mongolian Hordes Technique

n. Implies that large numbers of inexperienced programmers are being put on a job better performed by a few skilled ones. Also called `Chinese Army technique'; see also Brooks's Law.

Monitor

1. Software or hardware that scrutinizes and then displays, records, supervises, controls, or verifies the operations of a system. Note: Possible uses of monitors are to indicate significant departures from the norm, or to determine levels of utilization of particular functional units.
2. See visual display unit.
3. CRT

Monitor Signal

The signal to which a detected emanation is compared for determining correlation; a monitor is usually a RED signal.

#-Monitoring

1. The act of listening, carrying out surveillance on, and/or recording the emissions of one's own or allied forces for the purpose of maintaining and improving procedural standards and security, or for reference, as applicable. (JCS1-DoD) (JCS1-NATO)
2. The act of listening, carrying out surveillance on, and/or recording of enemy emissions for intelli-

gence purposes. (JCS1-DoD) (JCS1-NATO) See also electronic reconnaissance, intercept.
3. The act of detecting the presence of signals, such as electromagnetic radiation, sound, and visual signals, and the measurement thereof with appropriate measuring instruments.
4. The act of detecting the presence of radiation and the measurement thereof with radiation measuring instruments. See radiological monitoring. (JCS1-DoD) (JCS1-NATO)

#-Monitoring (e. g. , Data, Line)

This KSA has no definition.

*-Monkey Up

vt. To hack together hardware for a particular task, especially a one-shot job. Connotes an extremely crufty and consciously temporary solution. Compare hack up, kluge up, cruft together.

*-Monkey, Scratch

n. See scratch monkey.

Monochromatic

In optics, consisting of a single wavelength or color. Note: In practice, radiation is never perfectly monochromatic but, at best, displays a narrow band of wavelengths. See also coherent, line source, spectral width.

Monographic Processing

Processing where each character is sequentially processed in a bit parallel format.

Monolithic TCB

*-Monstrosity

1. n. A ridiculously elephantine program or system, esp. one that is buggy or only marginally functional.
2. adj. The quality of being monstrous (see `Overgeneralization' inthe discussion of jargonification). See also baroque.

*-Monty

1. /mon'tee/ n. [US Geological Survey] A program with a ludicrously complex user interface written to perform extremely trivial tasks. An example would be a menu-driven, button clicking, pull-down, pop-up windows program for listing directories. The original monty was an infamous weather-reporting program, Monty the Amazing Weather Man, written at the USGS. Monty had a widget-packed X-window interface with over 200 buttons; and all monty actually *did* was FTP files off the network.
2. [Great Britain; commonly capitalized as `Monty' or as `the Full Monty'] 16 megabytes of memory, when fitted to an IBM-PC or compatible. A standard PC-compatible using the AT- or ISA-bus with a normal BIOS cannot access more than 16 megabytes of RAM. Generally used of a PC, UNIX workstation etc. to mean `fully populated with' memory, disk-space or some other desirable resource. This usage is possibly derived from a TV commercial for Del Monte fruit juice, in which one of the characters insisted on “the full Del Monte”. Compare American moby.

*-Moof

1. /moof/ [MAC users] n. The call of a semi-legendary creature, properly called the dogcow. (Some previous version of this entry claimed, incorrectly, that Moof was the name of the *creature*.)
2. adj. Used to flag software that's a hack, something untested and on the edge. On one Apple CD-ROM, certain folders such as “Tools & Apps (Moof!)” and “Development Platforms (Moof!)”, are so marked to indicate that they contain software not fully tested or sanctioned by the powers that be. When you open these folders you cross the boundary into hackerland.

*-Moore's Law

/morz law/ prov. The observation that the logic density of silicon integrated circuits has closely followed the curve (bits per square inch) = 2^((t - 1962)) where t is time in years; that is, the amount of information storable on a given amount of silicon has roughly doubled every year since the technology was invented. See also Parkinson's Law of Data.

*-Moose Call

n. See whalesong.

*-Moria

/mor'ee-*/ n. Like nethack and rogue, one of the large PD Dungeons-and-Dragons-like simulation games, available for a wide range of machines and operating systems. The name is from Tolkien's Mines of Moria; compare elder days, elvish. The game is extremely addictive and a major consumer of time better used for hacking.

Mouse

A hand-held computer input device that generates the coordinates of a position indicator and is operated by being moved on a flat surface.

*-Mouse Ahead

vi. Point-and-click analog of `type ahead'. To manipulate a computer's pointing device (almost always a mouse in this usage, but not necessarily) and its selection or command buttons before a computer program is ready to accept such input, in anticipation of the program accepting the input. Handling this properly is rare, but it can help make a WIMP environment much

more usable, assuming the users are familiar with the behavior of the user interface.

*-Mouse Around

vi. To explore public portions of a large system, esp. a network such as Internet via FTP or TELNET, looking for interesting stuff to snarf.

*-Mouse Belt

n. See rat belt.

*-Mouse Droppings

n. [MS-DOS] Pixels (usually single) that are not properly restored when the mouse pointer moves away from a particular location on the screen, producing the appearance that the mouse pointer has left droppings behind. The major causes for this problem are programs that write to the screen memory corresponding to the mouse pointer's current location without hiding the mouse pointer first, and mouse drivers that do not quite support the graphics mode in use.

*-Mouse Elbow

n. A tennis-elbow-like fatigue syndrome resulting from excessive use of a WIMP environment. Similarly, `mouse shoulder'; GLS reports that he used to get this a lot before he taught himself to be ambimoustrous.

*-Mouso

/mow'soh/ n. [by analogy with `typo'] An error in mouse usage resulting in an inappropriate selection or graphic garbage on the screen. Compare thinko, braino.

*-MS-DOS

/M-S-dos/ n. [MicroSoft Disk Operating System] A clone of CP/M for the 8088 crufted together in 6 weeks by hacker Tim Paterson, who is said to have regretted it ever since. Numerous features, including vaguely UNIX-like but rather broken support for subdirectories, I/O redirection, and pipelines, were hacked into 2. 0 and subsequent versions; as a result, there are two or more incompatible versions of many system calls, and MS-DOS programmers can never agree on basic things like what character to use as an option switch or whether to be case-sensitive. The resulting mess is now the highest-unit-volume OS in history. Often known simply as DOS, which annoys people familiar with other similarly abbreviated operating systems (the name goes back to the mid-1960s, when it was attached to IBM's first disk operating system for the 360). The name further annoys those who know what the term operating system does (or ought to) connote; DOS is more properly a set of relatively simple interrupt services. Some people like to pronounce DOS like “dose”, as in “I don't work on dose, man!”, or to compare it to a dose of brain-damaging drugs (a slogan button in wide circulation among hackers exhorts “MS-DOSJust say No!”). See mess-dos, ill-behaved.

*-Mu

/moo/ The correct answer to the classic trick question “Have you stopped beating your wife yet?”. Assuming that you have no wife or you have never beaten your wife, the answer “yes” is wrong because it implies that you used to beat your wife and then stopped, but “no” is worse because it suggests that you have one and are still beating her. According to various Discordians and Douglas Hofstadter the correct answer is usually “mu”, a Japanese word alleged to mean “Your question cannot be answered because it depends on incorrect assumptions”. Hackers tend to be sensitive to logical inadequacies in language, and many have adopted this suggestion with enthusiasm. The word `mu' is actually from Chinese, meaning `nothing'; it is used in mainstream Japanese in that sense, but native speakers do not recognize the Discordian question-denying use. It almost certainly derives from overgeneralization of the answer in the following well-known Rinzei Zen teaching riddle A monk asked Joshu, “Does a dog have the Buddha nature?” Joshu retorted, “Mu!” See also has the X nature, AI Koans, and Douglas Hofstadter's “G”odel, Escher, BachAn Eternal Golden Braid” (pointer in the Bibliography in Appendix C.

*-MUD

/muhd/ n. [acronym, Multi-User Dungeon; alt. Multi-User Dimension]

1. A class of virtual reality experiments accessible via the Internet. These are real-time chat forums with structure; they have multiple `locations' like an adventure game, and may include combat, traps, puzzles, magic, a simple economic system, and the capability for characters to build more structure onto the database that represents the existing world.
2. vi. To play a MUD. The acronym MUD is often lowercased and/or verbed; thus, one may speak of `going mudding', etc. Historically, MUDs (and their more recent progeny with names of MU-form) derive from a hack by Richard Bartle and Roy Trubshaw on the University of Essex's DEC-10 in the early 1980s; descendants of that game still exist today and are sometimes generically called BartleMUDs. There is a widespread myth (repeated, unfortunately, by earlier versions of this lexicon) that the name MUD was trademarked to the commercial MUD run by Bartle on British Telecom (the motto “You haven't *lived* 'til you've *died* on MUD!”); however, this is false -- Richard Bartle explicitly placed `MUD' in PD in 1985. BT was upset at this, as they had already printed trademark claims on some maps and posters, which were released and created the myth. Students on the European academic networks

quickly improved on the MUD concept, spawning several new MUDs (VAXMUD, AberMUD, LPMUD). Many of these had associated bulletin-board systems for social interaction. Because these had an image as `research' they often survived administrative hostility to BBSs in general. This, together with the fact that Usenet feeds have been spotty and difficult to get in the U. K. , made the MUDs major foci of hackish social interaction there. AberMUD and other variants crossed the Atlantic around 1988 and quickly gained popularity in the U. S. ; they became nuclei for large hacker communities with only loose ties to traditional hackerdom (some observers see parallels with the growth of Usenet in the early 1980s). The second wave of MUDs (TinyMUD and variants) tended to emphasize social interaction, puzzles, and cooperative world-building as opposed to combat and competition. In 1991, over 50% of MUD sites are of a third major variety, LPMUD, which synthesizes the combat/puzzle aspects of AberMUD and older systems with the extensibility of TinyMud. The trend toward greater programmability and flexibility will doubtless continue. The state of the art in MUD design is still moving very rapidly, with new simulation designs appearing (seemingly) every month. There is now (early 1991) a move afoot to deprecate the term MUD itself, as newer designs exhibit an exploding variety of names corresponding to the different simulation styles being explored. See also bonk/oif, FOD, link-dead, mudhead, talk mode.

*-Muddie

n. Syn. mudhead. More common in Great Britain, possibly because system administrators there like to mutter “bloody muddies” when annoyed at the species.

*-Mudhead

n. Commonly used to refer to a MUD player who eats, sleeps, and breathes MUD. Mudheads have been known to fail their degrees, drop out, etc. , with the consolation, however, that they made wizard level. When encountered in person, on a MUD, or in a chat system, all a mudhead will talk about is three topics the tactic, character, or wizard that is supposedly always unfairly stopping him/her from becoming a wizard or beating a favorite MUD; why the specific game he/she has experience with is so much better than any other; and the MUD he or she is writing or going to write because his/her design ideas are so much better than in any existing MUD. See also wannabee. To the anthropologically literate, this term may recall the Zuni/Hopi legend of the mudheads or `koyemshi', mythical half-formed children of an unnatural union. Figures representing them act as clowns in Zuni sacred ceremonies. Others may recall the `High School Madness' sequence from the Firesign Theater album “Don't Crush That Dwarf, Hand Me the Pliers”, in which there is a character named “Mudhead”.

Multi-Level

Multi-Satellite Link

A radio link between a transmitting Earth station and a receiving Earth station through two or more satellites, without any intermediate Earth station. A multi-satellite link comprises one uplink, one or more satellite-to-satellite links, and one downlink. (RR)

Multi-User Hosts

Host computers that perform processing for more than one user simultaneously. (JCS PUB 6-03. 7)

Multi-User Mode Of Operation

A mode of operation designed for systems that process sensitive unclassified information in which users ma y not have a need-to-know for all information processed in the system. this mode is also for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation. (*NCSC-TG*-004-88)

Multi-User Security Mode

A mode of operation designed for sensitive unclassified systems in which users may or may have the need-to-know for all sensitive information processed, may simultaneously access the system. (*AFR* 205-16)

Multi-User Security Mode Of Operation

This mode of operation is designed for systems which process sensitive unclassified information in which users may not have a need-to-know for all information processed in the system. This mode is also for microcomputers processing sensitive unclassified information which cannot meet the requirements of the stand alone mode of operation. (*AFR* 205-16;)

Multichannel Information

Information which results when emanations from multiple TEMPEST channels are used to extract information correlating to a single message being processed.

*-Multician

/muhl-ti'shn/ n. [coined at Honeywell, ca. 1970] Competent user of Multics. Perhaps oddly, no one has ever promoted the analogous `Unician'.

*-Multics

/muhl'tiks/ n. [from “MULTiplexed Information and Computing Service”] An early (late 1960s) timesharing operating system co-designed by a consortium including MIT, GE, and Bell Laboratories. Multics was very innovative for its time --- among other things, it introduced the idea of treating all devices uniformly as special files. All the members but GE eventually

pulled out after determining that second-system effect had bloated Multics to the point of practical unusability (the `lean' predecessor in question was CTSS). Honeywell commercialized Multics after buying out GE's computer group, but it was never very successful (among other things, on some versions one was commonly required to enter a password to log out). One of the developers left in the lurch by the project's breakup was Ken Thompson, a circumstance which led directly to the birth of UNIX. For this and other reasons, aspects of the Multics design remain a topic of occasional debate among hackers. See also brain-damaged and GCOS.

Multilevel

Multilevel Device

A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i. e. , machine-readable or human-readable) as the data being processed. (CSC-STD-001-83;)

Multilevel Mode

AIS security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:(a)Some users do not have a valid security clearance for all the information processed in the AIS. (b)All users have the proper security clearance and appropriate formal access approval for that information to which they have access. (c)All users have a valid need-to-know only for information to which they have access.

Multilevel Mode Or Multilevel Security Mode

AIS security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:

1. Some users do not have a valid security clearance for all the information processed in the AIS.
2. All users have the proper security clearance and appropriate formal access approval for that information to which they have access.
3. All users have a valid need-to-know only for information to which they have access. NOTE: See Modes of Operation.

#-Multilevel Processing

A system that processes information of two or more different classification levels or intelligence compartments.

Multilevel Secure

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization. (CSC-STD-001-83;)

Multilevel Security

Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

Multilevel Security Mode

1. A mode of operation that provides a capability for various levels and categories or compartments of data to be concurrently stored and processed in an automated system and permits selective access to such material concurrently by users who have differing security clearances and need-to-know. Internal controls, as well as personnel, physical, and administrative controls, separate users and data on the basis of security clearance. The internal security controls must be thoroughly demonstrated to be effective in preventing unauthorized access to information. (*AFR* 205-16;)
2. A mode of operation in effect when at least some users with access to the system do not have a security clearance or need-to-know for all classified material in the information system. This mode provides the capability for the concurrent access to and use of the information system by uncleared users and users having different security clearances and need-to-know. The identification, segregation, and control of users and sensitive material on the basis of security clearance, and material classification category, and need-to-know must be essentially under automated control. Operation in this mode should be predicated on a comprehensive demonstration that the internal security controls can effectively prevent malicious attempts to bypass these controls. (*AFR* 700-10;)
3. The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. (CSC-STD-003-85;; *NCSC-WA*-001-85;)
4. A mode of operation wherein not all users have a clearance, formal access approval, and/or need-to-know for all data handled by the AIS. (DODD 5200. 28;)
5. A mode of operation under an operating system (supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP system. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipu-

lated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of: a) two or more levels of classified data, or b) one or more levels of classified data with unclassified data depending upon the constraints placed on the system by the Designated Approving Authority. (DODD 5200. 28M;)

6. An operation under an operating system (supervisor or executive program) which provides a capability permitting various categories and types of classified materials to be stored and processed concurrently in an ADP system and permitting selective access to such material concurrently by uncleared users having differing security clearances and need-to-know is accordingly accomplished by the operating system and associated system software. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and need-to-know. This mode of operation can accommodate the concurrent processing and storage of: a) two or more levels of classified data, or b) one or more levels of classified data with unclassified data depending upon constraints placed on the system by the DAA (*OPNAVINST* 5239. 1A;)

Multilevel Systems

Systems/networks that incorporate the mode of operation that allows two or more classification levels (including unclassified) of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. (DOE 5637. 1)

Multiple Access

1. The connection of a user or subscriber end-instrument to two or more switching centers by separate access lines using a single-message routing indicator or telephone number.
2. In satellite communications, the capability of a communication satellite to function as a portion of a communication link between more than one pair of satellite terminals simultaneously. (~) Note: Three types of multiple access are presently employed with communication satellites: code-division, frequency-division, and time-division. See also alternate routing, dual access, dual homing, extension facility, multiple homing, pulse-address multiple access, satellite.

Multiple Access Rights Terminal

A terminal that may be used by more than one class of users; for example, users with different access rights to data. (*FIPS PUB* 39;; *NCSC-WA*-001-85;)

Multiple Call

See conference call.

Multiplexing

(MUXing) The combining of two or more information channels onto a common transmission medium. (~)

Multiprocessing

1. A mode of operation that provides for parallel processing by two or more processors of a multiprocessor. (FP) (ISO)
2. The simultaneous execution of two or more computer programs or sequences of instructions by a computer. (FP)
3. Loosely, parallel processing. (FP) See also central processing unit, computer, distributed control, multiprogramming, on-line computer system, time-sharing.

Multiprocessor

A computer that has two or more processors that have common access to a main storage. (FP) (ISO)

Multiprogramming

A mode of operation that provides for the interleaved execution of two or more computer programs by a single processor. (FP) (ISO) (~) See also multiprocessing, time-sharing.

*-Multitask

n. Often used of humans in the same meaning it has for computers, to describe a person doing several things at once (but see thrash). The term `multiplex', from communications technology (meaning to handle more than one channel at the same time), is used similarly.

Multitasking

A mode of operation that provides for concurrent performance or interleaved execution of two or more tasks. (FP) (ISO)

Multiuser Mode Of Operation

A mode of operation designed for systems that process sensitive unclassified information in which users may not have a need-to-know for all information processed in the system. This mode is also for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation.

*-Mumblage

/muhm'bl*j/ n. The topic of one's mumbling (see mumble). “All that mumblage” is used like “all that stuff” when it is not quite clear how the subject of discussion works, or like “all that 'stuff" “ when `mumble' is being used as an implicit replacement for pejoratives.

*-Munch

vt.

[often confused with mung, q. v.] To transform information in a serial fashion, often requiring large amounts of computation. To trace down a data structure. Related to crunch and nearly synonymous with grovel, but connotes less pain.

*-Munching

n.

Exploration of security holes of someone else's computer for thrills, notoriety, or to annoy the system manager. Compare cracker. See also hacked off.

*-Munching Squares

n. A display hack dating back to the PDP-1 (ca. 1962, reportedly discovered by Jackson Wright), which employs a trivial computation (repeatedly plotting the graph Y = X XOR T for successive values of T -- see HAKMEM items 146--148) to produce an impressive display of moving and growing squares that devour the screen. The initial value of T is treated as a parameter, which, when well-chosen, can produce amazing effects.

*-Munchkin

/muhnch'kin/ n.

[from the squeaky-voiced little people in L. Frank Baum's "The Wizard of Oz"] A teenage-or-younger micro enthusiast hacking BASIC or something else equally constricted. A term of mild derision -- munchkins are annoying but some grow up to be hackers after passing through a larval stage. The term urchin is also used. See also wannabee, bitty box.

*-Mundane

n. [from SF fandom]

1. A person who is not in science fiction fandom.
2. A person who is not in the computer industry. In this sense, most often an adjectival modifier as in "in my mundane life. " See also Real World.

*-Mung

/muhng/ vt.

[in 1960 at MIT, `Mash Until No Good'; sometime after that the derivation from the recursive acronym `Mung Until No Good' became standard; but see munge]

1. To make changes to a file, esp. large-scale and irrevocable changes. See BLT.
2. To destroy, usually accidentally, occasionally maliciously. The system only mungs things maliciously; this is a consequence of Finagle's Law. See scribble, mangle, trash, nuke. Reports from Usenet suggest that the pronunciation /muhnj/ is now usual in speech, but the spelling `mung' is still common in program comments (compare the widespread confusion over the proper spelling of kluge).
3. The kind of beans of which the sprouts are used in Chinese food. (That's their real name! Mung beans! Really!) Like many early hacker terms, this one seems to have originated at TMRC; it was already in use there in 1958. Peter Samson (compiler of the original TMRC lexicon) thinks it may originally have been onomatopoeic for the sound of a relay spring (contact) being twanged. However, it is known that during the World Wars, `mung' was army slang for the ersatz creamed chipped beef better known as `SOS', and it seems quite likely that the word in fact goes back to Scots-dialect munge.

*-Munge

/muhnj/ vt.

1. [derogatory] To imperfectly transform information.
2. A comprehensive rewrite of a routine, data structure or the whole program.
3. To modify data in some way the speaker doesn't need to go into right now or cannot describe succinctly (compare mumble). This term is often confused with mung, which probably was derived from it. However, it also appears the word `munge' was in common use in Scotland in the 1940s, and in Yorkshire in the 1950s, as a verb, meaning to munch up into a masticated mess, and as a noun, meaning the result of munging something up (the parallel with the kluge/kludge pair is amusing).

*-Murphy's Law

prov.

The correct, *original* Murphy's Law reads "If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it. " This is a principle of defensive design, cited here because it is usually given in mutant forms less descriptive of the challenges of design for lusers. For example, you don't make a two-pin plug symmetrical and then label it `THIS WAY UP'; if it matters which way it is plugged in, then you make the design asymmetrical (see also the anecdote under magic smoke). Edward A. Murphy, Jr. was one of the engineers on the rocket-sled experiments that were done by the U. S. Air Force in 1949 to test human acceleration tolerances (USAF project MX981). One experiment involved a set of 16 accelerometers mounted to different parts of the subject's body. There were two ways each sensor could be glued to its mount, and somebody methodically installed all 16 the wrong way around. Murphy then made the original form of his pronouncement, which the test subject (Major John Paul Stapp) quoted at a news conference a few days later. Within months `Murphy's Law' had spread to various technical cultures connected to aerospace engineering. Before too many years had gone by vari-

ants had passed into the popular imagination, changing as they went. Most of these are variants on “Anything that can go wrong, will”; this is sometimes referred to as Finagle's Law. The memetic drift apparent in these mutants clearly demonstrates Murphy's Law acting on itself!

*-Music

n. A common extracurricular interest of hackers (compare science-fiction fandom, oriental food; see also filk). Hackish folklore has long claimed that musical and programming abilities are closely related, and there has been at least one large-scale statistical study that supports this. Hackers, as a rule, like music and often develop musical appreciation in unusual and interesting directions. Folk music is very big in hacker circles; so is electronic music, and the sort of elaborate instrumental jazz/rock that used to be called `progressive' and isn't recorded much any more. The hacker's musical range tends to be wide; many can listen with equal appreciation to (say) Talking Heads, Yes, Gentle Giant, Pat Metheny, Scott Joplin, Tangerine Dream, Dream Theater, King Sunny Ade, The Pretenders, Screaming Trees, or the Brandenburg Concerti. It is also apparently true that hackerdom includes a much higher concentration of talented amateur musicians than one would expect from a similar-sized control group of mundane types.

*-Mutter

vt. To quietly enter a command not meant for the ears, eyes, or fingers of ordinary mortals. Often used in `mutter an incantation'. See also wizard.

Mutual Suspicion

Condition in which two entities need to rely upon each other to perform a service, yet neither entity trusts the other to properly protect shared data.

Mutual Synchronization

A timing subsystem not employing directed control, by which the frequency of the clock at a particular node is controlled by some weighted average of the timing on all signals received from neighboring nodes. See also democratically synchronized network, hierarchically synchronized network, master-slave timing, mutually synchronized network, oligarchically synchronized network, synchronization.

Mutually Suspicious

1. The state that exists between interacting processes (subsystems or programs) in which neither process can expect the other process to function securely with respect to some property. (*NCSC-WA*-001-85;)
2. Pertaining to the state that exists between interacting processes (subsystems or programs) each of which contains sensitive data and is assumed to be designed so as to extract data from the other and to protect its own data. (*FIPS PUB* 39;; *AR* 380-380;)

Mutually Synchronized Network

A network-synchronizing arrangement in which each clock in the network exerts a degree of control on all others. See also democratically synchronized network, hierarchically synchronized network, master-slave timing, mutual synchronization, oligarchically synchronized network, synchronization.

MUX

See multiplex, multiplexer. See multiplexing.

Mw

N

*-N

/N/ quant.

1. A large and indeterminate number of objects “There were N bugs in that crock!” Also used in its original sense of a variable name “This crock has N bugs, as N goes to infinity. ” (The true number of bugs is always at least N + 1; see Lubarsky's Law of Cybernetic Entomology.)
2. A variable whose value is inherited from the current context. For example, when a meal is being ordered at a restaurant, N may be understood to mean however many people there are at the table. From the remark “We'd like to order N wonton soups and a family dinner for N - 1” you can deduce that one person at the table wants to eat only soup, even though you don't know how many people there are (see great-wall).
3. `Nth' adj. The ordinal counterpart of N, senses 1 and 2. “Now for the Nth and last time. ” In the specific context “Nth-year grad student”, N is generally assumed to be at least 4, and is usually 5 or more (see tenured graduate student). See also random numbers, two-to-the-N.

N-Entity

An active element in the n-th layer of the Open Systems Interconnection--Reference Model that interacts directly with elements (entities) of the layer immediately above or below the n-th layer. It is defined by a unique set of rules (syntax) and information formats (data/control), and it performs a defined set of functions. See also Open Systems Interconnection--Reference Model, protocol.

N-Function

A defined action performed by an N-entity. It may be either a single action (primitive function) or a set of

actions. See also Open Systems Interconnection--Reference Model.

N-Tuple

An ordered set of n elements. (ET;, MA;)

*-Nadger

/nad'jr/ v. [UK] Of software or hardware (not people), to twiddle some object in a hidden manner, generally so that it conforms better to some format. For instance, string printing routines on 8-bit processors often take the string text from the instruction stream, thus a print call looks like `jsr print:"Hello world"'. The print routine has to `nadger' the saved instruction pointer so that the processor doesn't try to execute the text as instructions when the subroutine returns. Apparently this word originated on a now-legendary 1950s radio comedy program called "The Goon Show". The Goon Show usage of "nadger" was definitely in the sense of "jinxed" "clobbered" "fouled up". The American mutation adger seems to have preserved more of the original flavor.

*-Nagware

/nag'weir/ n. [Usenet] The variety of shareware that displays a large screen at the beginning or end reminding you to register, typically requiring some sort of keystroke to continue so that you can't use the software in batch mode. Compare crippleware.

*-Nailed To The Wall adj.

[like a trophy] Said of a bug finally eliminated after protracted, and even heroic, effort.

*-Nailing Jelly vi.

See like nailing jelly to a tree.

*-Naïve adj.

Untutored in the perversities of some particular program or system; one who still tries to do things in an intuitive way, rather than the right way (in really good designs these coincide, but most designs aren't `really good' in the appropriate sense). This trait is completely unrelated to general maturity or competence, or even competence at any other specific program. It is a sad commentary on the primitive state of computing that the natural opposite of this term is often claimed to be `experienced user' but is really more like `cynical user'.

*-Naive User

n. A luser. Tends to imply someone who is ignorant mainly owing to inexperience. When this is applied to someone who *has* experience, there is a definite implication of stupidity.

NAK

/nak/ interj. [from the ASCII mnemonic for 0010101] negative-acknowledge character

1. On-line joke answer to ACK? "I'm not here. "
2. On-line answer to a request for chat "I'm not available. "
3. Used to politely interrupt someone to tell them you don't understand their point or that they have suddenly stopped making sense.

Nak Attack

A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus, leaves the system in an unprotected state during such interrupts. (*FIPS PUB* 39;)

*-Nano

[CMU from `nanosecond'] A brief period of time. "Be with you in a nano" means you really will be free shortly, i. e. , implies what mainstream people mean by "in a jiffy" (whereas the hackish use of `jiffy' is quite different -- see jiffy).

*-Nano- pref.

[SI the next quantifier below micro-; meaning * 10^(-9)] Smaller than micro-, and used in the same rather loose and connotative way. Thus, one has nanotechnology (coined by hacker K. Eric Drexler) by analogy with `microtechnology'; and a few machine architectures have a `nanocode' level below `microcode'. Tom Duff at Bell Labs has also pointed out that "Pi seconds is a nanocentury". See also quantifiers, pico-, nanoacre, nanobot, nanocomputer, nanofortnight.

*-Nanoacre

/nan'oh-ay`kr/ n. A unit (about 2 mm square) of real estate on a VLSI chip. The term gets its giggle value from the fact that VLSI nanoacres have costs in the same range as real acres once one figures in design and fabrication-setup costs.

*-Nanobot

/nan'oh-bot/ n. A robot of microscopic proportions, presumably built by means of nanotechnology. As yet, only used informally (and speculatively!). Also called a `nanoagent'.

*-Nanocomputer

/nan'oh-k*m-pyoo'tr/ n. A computer with molecular-sized switching elements. Designs for mechanical nanocomputers which use single-molecule sliding rods for their logic have been proposed. The controller for a nanobot would be a nanocomputer.

*-Nanofortnight n.

[Adelaide University] 1 fortnight * 10^-9, or about 1. 2 msec. This unit was used largely by students doing undergraduate practicals. See microfortnight, attoparsec, and micro-.

*-Nanotechnology

/nan'-oh-tek-no`l*-jee/ n. A hypothetical fabrication technology in which objects are designed and built

with the individual specification and placement of each separate atom. The first unequivocal nanofabrication experiments took place in 1990, for example with the deposition of individual xenon atoms on a nickel substrate to spell the logo of a certain very large computer company. Nanotechnology has been a hot topic in the hacker subculture ever since the term was coined by K. Eric Drexler in his book "Engines of Creation", where he predicted that nanotechnology could give rise to replicating assemblers, permitting an exponential growth of productivity and personal wealth. See also blue goo, gray goo, nanobot.

Narrative Traffic

Messages normally prepared in accordance with standardized procedures for transmission via optical character recognition equipment or teletypewriter. (~) Note: In contrast to data pattern traffic, narrative messages contain additional message format lines. See also record traffic.

Narrowband Modem

A modem whose modulated output signal has an essential frequency spectrum that is limited to that which can be wholly contained within, and faithfully transmitted through, a voice channel with a nominal 4-kHz bandwidth. (~) Note: High frequency (HF) modems are limited to operation over a voice channel with a nominal 3 kHz bandwidth. See also channel, modem, narrowband radio voice frequency, wideband modem.

*-Nasal Demons

n. Recognized shorthand on the Usenet group comp. std. c for any unexpected behavior of a C compiler on encountering an undefined construct. During a discussion on that group in early 1992, a regular remarked "When the compiler encounters [a given undefined construct] it is legal for it to make demons fly out of your nose" (the implication is that the compiler may choose any arbitrarily bizarre way to interpret the code without violating the ANSI C standard). Someone else followed up with a reference to "nasal demons", which quickly became established.

*-Nastygram

1. /nas'tee-gram/ n. A protocol packet or item of email (the latter is also called a letterbomb) that takes advantage of misfeatures or security holes on the target system to do untoward things.
2. Disapproving mail, esp. from a net. god, pursuant to a violation of netiquette or a complaint about failure to correct some mail- or news-transmission problem. Compare mailbomb.
3. A status report from an unhappy, and probably picky, customer. "What'd Corporate say in today's nastygram?"
4. [deprecated] An error reply by mail from a daemon; in particular, a bounce message.

*-Nathan Hale

An asterisk (see also splat, ASCII). Oh, you want an etymology? Notionally, from "I regret that I have only one asterisk for my country!", a misquote of the famous remark uttered by Nathan Hale just before he was hanged. Hale was a (failed) spy for the rebels in the American War of Independence.

National Communications System

1. The organization established by Section 1(a) of Executive Order No. 12472 to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget, in the discharge of their national security emergency preparedness telecommunications functions. The NCS consists of both the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals, and the Manager.
2. The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. (JCS1-DoD) (FS1037S1. TXT) (NCS)
3. The organization established by Section 1(a) of Executive Order No. 12472 to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget, in the discharge of their national security emergency preparedness telecommunications functions. The NCS consists of both the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals, and the Manager.
4. The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. (JCS1-DoD)

National Computer Security Assessment Program

(CSTVRP) A program designed to evaluate the interrelationship of empirical data of computer security infractions and that of critical systems profiles while comprehensively incorporating information from the Computer Security Technical Vulnerability Reporting Program. The assessment will build threat and vulnerability scenarios that are based on a collection of facts from relevant reported cases. Such scenarious are a powerful, dramatic, and consice form of repre-

senting the value of loss experience analysis. (*NCSC-WA*-001-85;)

National Computer Security Center

1. Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. (AF9K_JBC. TXT)
2. (NCSC) Originally named the DoD Computer Security Center. With the signing of NSDD-145;, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. (*NCSC-WA*-001-85;)

National Coordinating Center (NCC)

The joint telecommunications industry-Federal Government operation established by the National Communications System to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunication services or facilities. (FS1037S1. TXT)

National Electric Code®

A standard governing the use of electrical wire, cable, and fixtures installed in buildings; developed by the NEC Committee of the American National Standards Institute (ANSI), sponsored by the National Fire Protection Association (NFPA), identified by the description ANSI/NFPA 70-1990. (~)

#-National Information Infrastructure

This KSA has no definition.

National Security

The national defense or foreign relations of the United States. (EO 12356; NACSIM 4004)

National Security /or Emergency Preparedness Telecommunications

See NS/EP telecommunications.

National Security And Emergency Telecommunications

National Security Decision Directive

National Security Decision Directive 145

Signed by President Reagan on 17 September, 1984, this directive is entitled, "National Policy on Telecommunications and Automated Information Systems Security". It provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding systems which process, store, or communicate sensitive information, establishes a mechanism for policy development and assigns implementation responsibilities. (*NCSC-WA*-001-85;)

National Security Decision Directive 145 (NSDD 145)

Signed by President Reagan on 17 September 1984, this directive is entitled 'National Policy on Telecommunications and Automated Information Systems Security. " It provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding systems that process, store, or communicate sensitive information; establishes a mechanism for policy development; and assigns implementation responsibilities.

National Security Information

1. Information that has been determined, pursuant to Executive Order 12356 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.
2. Classified information related to the national defense or foreign relations of the United States (NSA, *National INFOSEC Glossary*, 10/88)

National Security Systems

Telecommunications and automated information systems operated by the U. S. Government, its contractors, or agents, that contain classified information or, as set forth in 10 U. S. C. Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

National Telecommunications And Information System Security Advisory/Information

NTISS Advisory/Information Memoranda provide advice, assistance, or information of general interest on telecommunications and automated information systems security to all applicable federal departments and agencies. NTISSAMs are promulgated by the National Manager for Automated Information Systems Security and are recommendatory. (*NCSC-WA*-001-85;)

NATO

See North Atlantic Treaty Organization.

*-Nature

See has the X nature.

*-Neat Hack

1. A clever technique.
2. A brilliant practical joke, where neatness is correlated with cleverness, harmlessness, and surprise value.

*-Neats Vs. Scruffies

The label used to refer to one of the continuing holy wars in AI research. This conflict tangles together two separate issues. One is the relationship between human reasoning and AI; `neats' tend to try to build systems that `reason' in some way identifiably similar to the way humans report themselves as doing, while `scruffies' profess not to care whether an algorithm resembles human reasoning in the least as long as it works. More importantly, neats tend to believe that logic is king, while scruffies favor looser, more ad-hoc methods driven by empirical knowledge. To a neat, scruffy methods appear promiscuous, successful only by accident, and not productive of insights about how intelligence actually works; to a scruffy, neat methods appear to be hung up on formalism and irrelevant to the hard-to-capture `common sense' of living intelligences.

Necessary Bandwidth

For a given class of emission, the width of the frequency band which is just sufficient to ensure the transmission of information at the rate and with the quality required under specified conditions. (RR) (~) Note: Emissions useful for the adequate functioning of the receiving equipment, e. g. , the emission corresponding to the carrier of reduced carrier systems, must be included in the necessary bandwidth. (~) (See Annex J of NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management for formulas used to calculate necessary bandwidth.) See also bandwidth, bandwidth compression, carrier (cxr), frequency, nominal bandwidth, occupied bandwidth, spurious emission, spurious response, suppressed carrier transmission.

Need To Know

1. A criterion used in security procedures that requires the custodians of classified information to establish, before disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 1-02)
2. A determination made by the processor of sensitive information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the sensitive information in order to perform official tasks or services. (CSC-STD-004-85)
3. The necessity for access to, knowledge of, or possession of certain information required to carry out official duties. Responsibility for determining whether a person's duties require that possession of or access to such information and whether the individual is authorized to receive it rests upon the individual having current possession, knowledge, or control of the information involved and not upon the prospective recipient(s). (*OPNAVINST* 5239. 1 A; *AR* 380-380)
4. The determination made in the interest of U. S. national security by the custodian of classified or sensitive unclassified information, which a prospective recipient has the requirement for access to, knowledge of, or possession of the information to perform official tasks or services. (DODD 5200. 28; DO E 563 5. 1 A)

#-Need-To-Know Controls

Administrative procedures for access to, or knowledge or possession of, specific information required to carry out official duties. (Source: NSTISSI 4009).

Need-To-Know Violation

The disclosure of classified or other sensitive defence information to a person who is cleared but has no requirement for such information to carry out assigned official duties. (*AR* 380-380;)

*-Neep-Neep

/neep neep/ n. [onomatopoeic, from New York SF fandom] One who is fascinated by computers. Less specific than hacker, as it need not imply more skill than is required to boot games on a PC. The derived noun `neeping' applies specifically to the long conversations about computers that tend to develop in the corners at most SF-convention parties (the term `neepery' is also in wide use). Fandom has a related proverb to the effect that “Hacking is a conversational black hole!”.

Negative-Acknowledge Character

A transmission control character sent by a station as a negative response to the station with which the connection has been set up. (FP) (~)

Note 1: In binary synchronous communication protocol, used to indicate that an error was detected in the previously received block and that the receiver is ready to accept retransmission of the erroneous block.

Note 2: In multipoint systems, used as the not-ready reply to a poll.

See also acknowledge character, character, compelled signaling, control character. (FS1037S1. TXT)

(NAK) A transmission control character sent by a station as a negative response to the station with which the connection has been set up. (FP) (~) Note 1: In binary synchronous communication protocol, used to indicate that an error was detected in the previously received block and that the receiver is ready to accept retransmission of the erroneous block. Note 2: In multipoint systems, used as the not-ready reply to a poll. See also acknowledge character, character, compelled signaling, control character.

*-Neophilia

/nee`oh-fil'-ee-*/ n. The trait of being excited and pleased by novelty. Common among most hackers,

SF fans, and members of several other connected leading-edge subcultures, including the pro-technology `Whole Earth' wing of the ecology movement, space activists, many members of Mensa, and the Discordian/neo-pagan underground. All these groups overlap heavily and (where evidence is available) seem to share characteristic hacker tropisms for science fiction, music, and oriental food. The opposite tendency is `neophobia'.

Net

See communications net, communications network.

Net Control Station

(NCS) Terminal in a secure telecommunications net responsible for distributing key in electronic form to the members of the net. (F:\NEWDEFS. TXT) Terminal in a secure telecommunications net responsible for distributing key in electronic form to the members of the net.

Net Operation

The operation of an organization of stations capable of direct communication on a common channel or frequency. Note: Nets (netted operations) are ordered conferences whose participants have common information needs or similar functions to perform. Nets are characterized by adherence to standard formats. They are responsive to a common supervisor, called the “net controller” or “net control station,” whose functions include permitting access to the net and maintaining circuit discipline. See also communications net, polling.

*-Net

. - /net dot/ pref. [Usenet] Prefix used to describe people and events related to Usenet. From the time before the Great Renaming, when most non-local newsgroups had names beginning `net. '. Includes net. gods, `net. goddesses' (various charismatic net. women with circles of on-line admirers), `net. lurkers' (see lurker), `net. person', `net. parties' (a synonym for, sense
2. , and many similar constructs. See also net. police.

*-Net. God

/net god/ n. Accolade referring to anyone who satisfies some combination of the following conditionshas been visible on Usenet for more than 5 years, ran one of the original backbone sites, moderated an important newsgroup, wrote news software, or knows Gene, Mark, Rick, Mel, Henry, Chuq, and Greg personally. See demigod. Net. goddesses such as Rissa or the Slime Sisters have (so far) been distinguished more by personality than by authority.

*-Net. Personality

/net per`sn-al'-*-tee/ n. Someone who has made a name for him or herself on Usenet, through either longevity or attention-getting posts, but doesn't meet the other requirements of net. godhood.

*-Net. Police

/net-p*-lees'/ n. (var. `net. cops')
Those Usenet readers who feel it is their responsibility to pounce on and flame any posting which they regard as offensive or in violation of their understanding of netiquette. Generally used sarcastically or pejoratively. Also spelled `net police'. See also net. -, code police.

*-NetBOLLIX

[from bollix to bungle] IBM's NetBIOS, an extremely brain-damaged network protocol that, like Blue Glue, is used at commercial shops that don't know any better.

*-Netburp

[IRC] When netlag gets really bad, and delays between servers exceed a certain threshhold, the IRC network effectively becomes partitioned for a period of time, and large numbers of people seem to be signing off at the same time and then signing back on again when things get better. An instance of this is called a `netburp' (or, sometimes, netsplit). netdeadn. [IRC] The state of someone who signs off IRC, perhaps during a netburp, and doesn't sign back on until later. In the interim, he is “dead to the net”.

*-Nethack

/net'hak/ n.
[UNIX] A dungeon game similar to rogue but more elaborate, distributed in C source over Usenet and very popular at UNIX sites and on PC-class machines (nethack is probably the most widely distributed of the freeware dungeon games). The earliest versions, written by Jay Fenlason and later considerably enhanced by Andries Brouwer, were simply called `hack'. The name changed when maintenance was taken over by a group of hackers originally organized by Mike Stephenson; the current contact address (as of mid-1993) is nethack-bugs@linc. cis. upenn. edu.

*-Netiquette

/net'ee-ket/ or /net'i-ket/ n.
[portmanteau from “network etiquette”] The conventions of politeness recognized on Usenet, such as avoidance of cross-posting to inappropriate groups and refraining from commercial pluggery outside the biz groups.

*-Netlag n.

[IRC, MUD] A condition that occurs when the delays in the IRC network or on a MUD become severe enough that servers briefly lose and then reestablish contact, causing messages to be delivered in bursts, often with delays of up to a minute. (Note that this term has nothing to do with mainstream “jet lag”, a condition which hackers tend not to be much bothered by.)

*-Netnews

/net'n[y]ooz/ n.

1. The software that makes Usenet run.
2. The content of Usenet. “I read netnews right after my mail most mornings. ”

*-Netrock

/net'rok/ n. [IBM]

A flame; used esp. on VNET, IBM's internal corporate network.

*-Netsplit

n. Syn. netburp.

*-Netter

1. Loosely, anyone with a network address.
2. More specifically, a Usenet regular. Most often found in the plural. “If you post *that* in a technical group, you're going to be flamed by angry netters for the rest of time!”:network address n. (also `net address') As used by hackers, means an address on `the' network (see network, the; this is almost always a bang path or Internet address). Such an address is essential if one wants to be to be taken seriously by hackers; in particular, persons or organizations that claim to understand, work with, sell to, or recruit from among hackers but *don't* display net addresses are quietly presumed to be clueless poseurs and mentally flushed (see flush, sense 4). Hackers often put their net addresses on their business cards and wear them prominently in contexts where they expect to meet other hackers face-to-face (see also science-fiction fandom). This is mostly functional, but is also a signal that one identifies with hackerdom (like lodge pins among Masons or tie-dyed T-shirts among Grateful Dead fans). Net addresses are often used in email text as a more concise substitute for personal names; indeed, hackers may come to know each other quite well by network names without ever learning each others' `legal' monikers.
3. See also sitename, domainist.

Network

1. Two or more systems connected by a communications medium. (*AFR* 205-16)
2. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. (DODD 5200. 28)
3. A communications medium and all components the transfer of information. Such components may include ADP systems, packet switches, telecommunications controllers, key distribution centers, technical control devices, and other networks. (DOE 5637. 1)
4. This is the interconnection of two or more ADP central computer facilities that provides for the transfer or sharing of ADP resources. The ADP network consists of the central computer facilities, the remote terminals, the interconnecting communication links, the front-end processors, and the telecommunications systems. (*OPNAVINST* 5239. lA)
5. See COMPUTER NETWORK.

Network Architecture

1. The design principles, physical configuration, functional organization, operational procedures, and data formats used as the basis for the design, construction, modification, and operation of a communications network. (~) See also Open Systems Interconnection--Reference Model.
2. The structure of an existing communication network including the facilities, operational structure and procedures, and the data formats. (~) See also centralized operation, distributed control, distributed network, distributed switching, network connectivity.

Network Busy Hour

See busy hour. (FS1037S1. TXT) (NBH) See busy hour.

#-Network Communications Protocols

A set of rules and formats for the exchange of information, particularly over a communications network. (Source: “*Computer Security Basics*” Deborah Russell and G. T. Gangemi Sr. Pub. O'Reilly and Associates, Inc. , July 1992).

Network Connectivity

The topological description of a network, which specifies the interconnection of the transmission nodes in terms of circuit termination locations and quantities. (~) See also distributed network, network, network architecture, node.

Network Control System

The computer system that provides the means of collecting and processing information concerning the status of a telecommunications network. (GAO;)

#-Network Firewalls

This KSA has no definition.

Network Front End

A device that implements the necessary network protocols, including security related protocols, to allow a computer system to be attached to a network. (2) Device that implements the needed security-related protocols to allow a computer system to be attached to a network. (*NCSC-WA*-001-85;)

Network Interface

1. The point of interconnection between a user terminal and a private or public network.
2. The point of interconnection between the public switched network and a privately owned terminal. (~) Note: Code of Federal Regulations, Title 47, part 68, stipulates the interface parameters.
3. The point of interconnection between one network and another network (or portion thereof). (~) See also divestiture, entrance facility, gateway, interface, network, network terminating interface, registered jack, service termination point.

Network Interface Device

1. A device that performs functions such as code and protocol conversion, and buffering required for communications to and from a network.
2. A device used primarily within a local area network to allow a number of independent devices, with varying protocols, to communicate with each other. This communication is accomplished by converting each device protocol into a common transmission protocol. Note: The transmission protocol may be chosen to accommodate, directly without interface conversion, some of the devices used within the network. Synonym network interface unit. See also local area network, medium interface point, network. (FS1037S1. TXT) (NID)

3; A device that performs functions such as code and protocol conversion, and buffering required for communications to and from a network.

4. A device used primarily within a local area network to allow a number of independent devices, with varying protocols, to communicate with each other. This communication is accomplished by converting each device protocol into a common transmission protocol. Note: The transmission protocol may be chosen to accommodate, directly without interface conversion, some of the devices used within the network. See network interface unit. See also local area network, medium interface point, network.

Network Interface Unit (NIU)

Synonym network interface device. (FS1037S1. TXT) See network interface device.

Network Layer

See Open Systems Interconnection--Reference Model.

Network Manager

Individual responsible for the operation of a network; usually authorizes network membership. (*AR* 380-380)

*-Network Meltdown

n.

A state of complete network overload; the network equivalent of thrashing. This may be induced by a Chernobyl packet. See also broadcast storm, kamikaze packet. Network meltdown is often a result of network designs that are optimized for a steady state of moderate load and don't cope well with the very jagged, bursty usage patterns of the real world. One amusing instance of this is triggered by the the popular and very bloody shoot-'em-up game Doom on the PC. When used in multiplayer mode over a network, the game uses broadcast packets to inform other machines when bullets are fired. This causes problems with weapons like the chain gun which fire rapidly -- it can blast the network into a meltdown state just as easily as it shreds opposing monsters.

#-Network Monitoring

A combination of hardware and software attached directly to the network to analyze the status of the network. Such devices can have the effect of turning a host computer into a network analyzer. Such devices are used to supervise, maintain, and troubleshoot networks and are capable of monitoring all communication and to gain access to the contents of a user communications, but are not typically used in this way. Such devices provide a mans for responsible personnel to discover problems with the network and to initiate corrections. Where used to gain access to the contents of user communications, such devices constitute keystroke monitoring. (Source panel of experts).

Network Reference

Access control concept that refers to monitor an abstract machine that mediates all access to objects within a network by subjects within the network.

Network Reference Monitor

Access control concept that refers to an abstract machine that mediates all access to objects within a network by subjects within the network. See Reference Monitor.

Network Security

1. Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. NOTE: Network security includes providing for data integrity.
2. Individual formally appointed by a officer designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network.

Network Security Manager (NSM)

Term no longer used, see Network Security Officer (NSO). (AF9K_JBC. TXT)

Network Security Officer

Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network. See Information System Security Officer (ISSO). (AF9K_JBC. TXT) (NSO) Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network. See Information System Security Officer (ISSO).

#-Network Security Software

This KSA has no definition.

#-Network Switching

This KSA has no definition.

Network System

System that is implemented with a collection of interconnected network components. NOTE: A network system is based on a coherent security architecture and design.

Network Terminal Number

In the CCITT International X. 121 format, the sets of digits that comprise the complete address of the data terminal end point.

Note: For an NTN that is not part of a national integrated numbering format, the NTN is the 10 digits of the CCITT X. 25 14-digit address that follow the Data Network Identification Code (DNIC). When part of a national integrated numbering format, the NTN is the 11 digits of the CCITT X. 25 14-digit address that follow the DNIC. (FS1037S1. TXT) (NTN) In the CCITT International X. 121 format, the sets of digits that comprise the complete address of the data terminal end point.

Note: For an NTN that is not part of a national integrated numbering format, the NTN is the 10 digits of the CCITT X. 25 14-digit address that follow the Data Network Identification Code (DNIC). When part of a national integrated numbering format, the NTN is the 11 digits of the CCITT X. 25 14-digit address that follow the DNIC.

#-Network Topology

1. The geometric arrangement of nodes and cable links in a local area network. Network topologies fall into two categories: centralized and decentralized. In a centralized topology such as a star network, a central computer controls access to the network. This design ensures data security and central management control over the network's contents and activities. In a decentralized topology such as a bus network or fine network, no central computer controls the network's activities. Rather, each workstation can access the network independently and establish it's own connections with other workstations. (QCUD+Pf-90.
2. The specific physical (real) or logical (virtual) arrangement of the elements of a network. Note: Two networks have the same topology if the connecting configuration is the same, although the networks may differ in physical interconnections, distance between nodes, transmission rates, and signal types. See topology. See also bus topology, logical topology, physical topology, ring network, star topology, tree topology.

Network Trusted

Totality of protection mechanisms computing base within a network system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy.

Network Trusted Computing Base (NTCB)

Totality of protection mechanisms within a network system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. See Trusted Computing Base.

Network Utility

An internetwork administrative signaling mechanism in the call control procedure between packet switching public data networks.

Network Weaving

Network weaving is a technique using different communication networks to gain access to an organization's system. For example, a perpetrator [.] makes a call through AT&T, jumps over to Sprint, then to MCI, and then to Tymnet. The purpose is to avoid detection and trace-backs to the source of the call. (TC;)

*-Network, The

1. The union of all the major noncommercial, academic, and hacker-oriented networks, such as Internet, the old ARPANET, NSFnet, BITNET, and the virtual UUCP and Usenet `networks', plus the corporate in-house networks and commercial time-sharing services (such as CompuServe) that gateway to them. A site is generally considered `on the network' if it can be reached through some combination of Internet-style (@-sign) and UUCP (bang-path) addresses. See bang path, Internet address, network address.
2. A fictional conspiracy of libertarian hacker-subversives and anti-authoritarian monkeywrenchers described in Robert Anton Wilson's novel “Schr”odinger's Cat”, to which many hackers have subsequently decided they belong (this is an example of ha ha only serious). In sense 1, `network' is often abbreviated to `net'. “Are you on the net?” is a frequent question when hackers first meet face

to face, and “See you on the net!” is a frequent goodbye.

*-New Testament

n. [C programmers] The second edition of K&R's “The C Programming Language” (Prentice-Hall, 1988; ISBN 0-13-110362-8), describing ANSI Standard C. See K&R.

*-Newbie

/n[y]oo'bee/ n. [orig. from British public-school and military slang variant of `new boy'] A Usenet neophyte. This term surfaced in the newsgroup talk. bizarre but is now in wide use. Criteria for being considered a newbie vary wildly; a person can be called a newbie in one newsgroup while remaining a respected regular in another. The label `newbie' is sometimes applied as a serious insult to a person who has been around Usenet for a long time but who carefully hides all evidence of having a clue. See B1FF.

*-Newgroup Wars

/n[y]oo'groop worz/ n. [Usenet] The salvos of dueling `newgroup' and `rmgroup' messages sometimes exchanged by persons on opposite sides of a dispute over whether a newsgroup should be created netwide, or (even more frequently) whether an obsolete one should be removed. These usually settle out within a week or two as it becomes clear whether the group has a natural constituency (usually, it doesn't). At times, especially in the completely anarchic alt hierarchy, the names of newsgroups themselves become a form of comment or humor; e. g. , the spinoff of alt. swedish. chef. bork. bork. bork from alt. tv. muppets in early 1990, or any number of specialized abuse groups named after particularly notorious flamers, e. g. , alt. weemba.

*-Newline

1. /n[y]oo'li:n/ n. [techspeak, primarily UNIX] The ASCII LF character (0001010), used under UNIX as a text line terminator. A Bell-Labs-ism rather than a Berkeleyism; interestingly (and unusually for UNIX jargon), it is said to have originally been an IBM usage. (Though the term `newline' appears in ASCII standards, it never caught on in the general computing world before UNIX).
2. More generally, any magic character, character sequence, or operation (like Pascal's writeln procedure) required to terminate a text record or separate lines.

See crlf, terpri.

*-News

/nee'wis/, /n[y]oo'is/ or /n[y]ooz/ n. [acronym; the `Network Window System'] The road not taken in window systems, an elegant PostScript-based environment that would almost certainly have won the standards war with X if it hadn't been proprietary to Sun Microsystems. There is a lesson here that too many software vendors haven't yet heeded. Many hackers insist on the two-syllable pronunciations above as a way of distinguishing NeWS from news (the netnews software).

*-Newsfroup

[Usenet] Silly synonym for newsgroup, originally a typo but now in regular use on Usenet's talk. bizarre and other lunatic-fringe groups. Compare hing, grilf, and filk.

*-Newsgroup

[Usenet] One of Usenet's huge collection of topic groups or fora. Usenet groups can be `unmoderated' (anyone can post) or `moderated' (submissions are automatically directed to a moderator, who edits or filters and then posts the results). Some newsgroups have parallel mailing lists for Internet people with no netnews access, with postings to the group automatically propagated to the list and vice versa. Some moderated groups (especially those which are actually gatewayed Internet mailing lists) are distributed as `digests', with groups of postings periodically collected into a single large posting with an index. Among the best-known are comp. lang. c (the C-language forum), comp. arch (on computer architectures), comp. unix. wizards (for UNIX wizards), rec. arts. sf. written and siblings (for science-fiction fans), and talk. politics. misc (miscellaneous political discussions and flamage).

Nibble

Half a byte. See also byte.

*-Nick

n. [IRC] Short for nickname. On IRC, every user must pick a nick, which is sometimes the same as the user's real name or login name, but is often more fanciful. Compare handle. nickle/ni'kl/ n. [from `nickel', common name for the U. S. 5-cent coin] A nybble + 1; 5 bits. Reported among developers for Mattel's GI 1600 (the Intellivision games processor), a chip with 16-bit-wide RAM but 10-bit-wide ROM. See also deckle, and nybble for names of other bit units.

*-Night Mode

n. See phase (of people).

*-Nightmare File System

n.

Pejorative hackerism for Sun's Network File System (NFS). In any nontrivial network of Suns where there is a lot of NFS cross-mounting, when one Sun goes down, the others often freeze up. Some machine tries to access the down one, and (getting no response) repeats indefinitely. This causes it to appear dead to some messages (what is actually happening is that it is locked up in what should have been a brief excursion

to a higher spl level). Then another machine tries to reach either the down machine or the pseudo-down machine, and itself becomes pseudo-down. The first machine to discover the down one is now trying both to access the down one and to respond to the pseudo-down one, so it is even harder to reach. This situation snowballs very quickly, and soon the entire network of machines is frozen -- worst of all, the user can't even abort the file access that started the problem! Many of NFS's problems are excused by partisans as being an inevitable result of its statelessness, which is held to be a great feature (critics, of course, call it a great misfeature). (ITS partisans are apt to cite this as proof of UNIX's alleged bogosity; ITS had a working NFS-like shared file system with none of these problems in the early 1970s.) See also broadcast storm.

*-NIL

/nil/

No. Used in reply to a question, particularly one asked using the `-P' convention. Most hackers assume this derives simply from LISP terminology for `false' (see also T), but NIL as a negative reply was well-established among radio hams decades before the advent of LISP. The historical connection between early hackerdom and the ham radio world was strong enough that this may have been an influence.

*-Ninety-Ninety Rule

n. “The first 90% of the code accounts for the first 90% of the development time. The remaining 10% of the code accounts for the other 90% of the development time. ” Attributed to Tom Cargill of Bell Labs, and popularized by Jon Bentley's September 1985 “Bumper-Sticker Computer Science” column in “Communications of the ACM”. It was there called the “Rule of Credibility”, a name which seems not to have stuck.

*Non-Maskable Interrupt

-NMI /N-M-I/ n. An IRQ 7 on the PDP-11 or 680[01234]0; the NMI line on an 80[1234]86. In contrast with a priority interrupt (which might be ignored, although that is unlikely), an NMI is *never* ignored. Except, that is, on clone boxes, where NMI is often ignored on the motherboard because flaky hardware can generate many spurious ones.

No Addtional Requirements

No Contract

No contractor dissemination. This term indicates that the information contained in the document must not be released to contractors/consultants. (DOE 5635. 1A;)

No-Lone Zone

Area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other.

*-No-Op

NOP /nop/ [no operation]

1. A machine instruction that does nothing (sometimes used in assembler-level programming as filler for data or patch areas, or to overwrite code to be removed in binaries). See also JFCL.
2. A person who contributes nothing to a project, or has nothing going on upstairs, or both. As in “He's a no-op. ”
3. Any operation or sequence of operations with no effect, such as circling the block without finding a parking space, or putting money into a vending machine and having it fall immediately into the coin-return box, or asking someone for help and being told to go away. “Oh, well, that was a no-op. ” Hot-and-sour soup (see great-wall) that is insufficiently either is `no-op soup'; so is wonton soup if everybody else is having hot-and-sour.

*-Noddy

/nod'ee/ adj. [UK from the children's books]

1. Small and un-useful, but demonstrating a point. Noddy programs are often written by people learning a new language or system. The archetypal noddy program is hello, world. Noddy code may be used to demonstrate a feature or bug of a compiler. May be used of real hardware or software to imply that it isn't worth using. “This editor's a bit noddy. ”
2. A program that is more or less instant to produce. In this use, the term does not necessarily connote uselessness, but describes a hack sufficiently trivial that it can be written and debugged while carrying on (and during the space of) a normal conversation. “I'll just throw together a noddy awk script to dump all the first fields. ” In North America this might be called a mickey mouse program. See toy program.

Node

1. In network topology, a terminal of any branch of a network or an interconnection common to two or more branches of a network. (~) See s junction point, nodal point. See also branch (def. #3), communications, extension facility, extension terminal, interface message processor, network.
2. In a switched network, one of the switches forming the network backbone.
3. A technical control facility (TCF). (~)
4. A point in a standing or stationary wave at which the amplitude is a minimum. (~) In this sense, See null (def. #2). See also anti-node, standing wave ratio.

NOFORN

No foreign dissemination. This term indicates that the information contained in the document must not be released to foreign nations. (DOE 5635. 1A;)

Noise

Disturbances superimposed upon a signal that tend to obscure its information content.

*-NOMEX Underwear

/noh'meks uhn'-der-weir/ n.

[Usenet] Syn. asbestos longjohns, used mostly in auto-related mailing lists and newsgroups. NOMEX underwear is an actual product available on the racing equipment market, used as a fire resistance measure and required in some racing series.

Nominal Bit Stuffing Rate

The rate at which stuffing bits are inserted (or deleted) when both the input and output bit rates are at their nominal values. (~) See also binary digit, bit stuffing, de-stuffing, maximum stuffing rate.

*-Nominal Semidestructor

n.

Soundalike slang for `National Semiconductor', found among other places in the Networking/2 networking sources. During the late 1970s to mid-1980s this company marketed a series of microprocessors including the NS16000 and NS32000 and several variants. At one point early in the great microprocessor race, the specs on these chips made them look like serious competition for the rising Intel 80x86 and Motorola 680x0 series. Unfortunately, the actual parts were notoriously flaky and never implemented the full instruction set promised in their literature, apparently because the company couldn't get any of the mask steppings to work as designed. They eventually sank without trace, joining the Zilog Z8000 and a few even more obscure also-rans in the graveyard of forgotten microprocessors. Compare HP-SUX, AIDX, buglix, Macintrash, Telerat, Open DeathTrap, ScumOS, sunstools.

Non-Discretionary Security

The aspect of *DOD* security policy which restricts access on the basis of security levels. A security level is composed of a read level and a category set restriction. For read-access to an item of information, a user must have a clearance level greater than or equal to the classification of the information and also have a category clearance which includes all of the access categories specified for the information. (MTR-8201;)

#-Non-Inference Model

A computer systems model which gives the impression to a user that they own the entire resources of the machine. All responses to a users request for resources are as if no other users are on the machine.

Non-Kernel Security-Related Software (NKSR)

1. Security-relevant software which is executed in the environment provided by a security kernel rather than as a part of the kernel. Processes executing NKSR software may or may not require special privilege to override kernel-enforced security rules. (MTR-8201;)
2. Software that is part of the Trusted Computing Base but not part of the security kernel. (*NCSC-WA*-001-85;) (AF9K_JBC. TXT) (NKSR) Security-relevant software which is executed in the environment provided by a security kernel, rather than as a part of the kernel itself.

*-Non-Optimal Solution

n.

(also `sub-optimal solution') An astoundingly stupid way to do something. This term is generally used in deadpan sarcasm, as its impact is greatest when the person speaking looks completely serious. Compare stunning. See also Bad Thing.

Non-Processing Input And Output Devices

A device used to enter information and commands into a host computer and receive information from the host, but performs no processing itself (e. g. , simple, memoryless terminals). (JCS PUB 6-03. 7)

Non-Removable Storage Media

Storage media such as a hard disk, that is internal to the system. Sometimes called “fixed” disk storage. Generally, this type of media is removed only when neccessary for maintenance purposes. See Removable Storage Media.

Non-Repudiation

Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Non-Return-To-Zero Code

A code form having two states, termed “zero” and “one,” and no neutral or rest condition. (~) Note 1: Contrast with Manchester encoding and return-to-zero code. Note 2: For a given data transmission (bit) rate, the non-return-to-zero code requires only one-half the bandwidth required by the Manchester code. See also bipolar signal, code, duobinary signal, Manchester encoding, non-return-to-zero change-on-ones, return-to-zero code.

Non-Return-To-Zero, Change-On-Ones

A method of encoding, i. e. , data representation, in which “ones” are represented by a change in condition and “zeros” are represented by no change. (~) See also code, return-to-zero code. (FS1037S1. TXT) (NRZ1) A method of encoding, i. e. , data representa-

tion, in which “ones” are represented by a change in condition and “zeros” are represented by no change. (~) See also code, return-to-zero code.

Non-Secret Encryption

See Public Key Cryptography.

Non-Volatile Memory

Memory (such as semiconductor memory) that does not lose its memory retention capability when electric power is removed. (JCS PUB 6-03. 7)

Noncentralized Operation

A control discipline for multipoint data communication links in which transmission may be between tributary stations or between the control station and tributary station(s). See also communications, link.

Noncooperative

Noncooperative Remote Rekeying

See Automatic Remote Rekeying.

Nonferrous Shielding

An RF shielding material which does not contain iron, and therefore provides less magnetic field attentuation than ferrous shielding. Nonferrous shields, such as aluminum and copper, do provide a high degree of electrostatic shielding. (NACSEM 5203)

*-Nonlinear

adj.

1. [scientific computation] Behaving in an erratic and unpredictable fashion; unstable. When used to describe the behavior of a machine or program, it suggests that said machine or program is being forced to run far outside of design specifications. This behavior may be induced by unreasonable inputs, or may be triggered when a more mundane bug sends the computation far off from its expected course.
2. When describing the behavior of a person, suggests a tantrum or a flame. “When you talk to Bob, don't mention the drug problem or he'll go nonlinear for hours. ” In this context, `go nonlinear' connotes `blow up out of proportion' (proportion connotes linearity).

Nonprocedural Language

A formal high-level language for the specification of program modules. Such languages express relations which hold between “input” and “output” values of program variables without constraining the particular algorithms which implement the change. (MTR-8201;)

Nonsynchronous Network

A network in which the clocks do not need to be synchronous or mesochronous. (~) See asynchronous network. See also clock, network.

Nonsynchronous System

See asynchronous transmission.

*-Nontrivial

adj. Requiring real thought or significant computing power. Often used as an understated way of saying that a problem is quite difficult or impractical, or even entirely unsolvable (“Proving P=NP is nontrivial”). The preferred emphatic form is `decidedly nontrivial'. See trivial, uninteresting, interesting.

Nontunable

A term used to describe a test, or test instrumentation, in which frequency coverage is selected in one or more discrete increments; i. e. , not continuously variable. Nontunable detection systems do not contain a demodulator.

Nonvolatile Memory

Media which retains information in the absence of power and makes the information available when power is restored. See Memory and Volatile Memory.

*-Not Ready For Prime Time

adj.

Usable, but only just so; not very robust; for internal use only. Said of a program or device. Often connotes that the thing will be made more solid Real Soon Now. This term comes from the ensemble name of the original cast of “Saturday Night Live”, the “Not Ready for Prime Time Players”. It has extra flavor for hackers because of the special (though now semi-obsolescent) meaning of prime time. Compare beta.

Notarization

The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery. (SS;)

Notebook Computer

Small hand-carried computer, typically weighing seven pounds or less. See Laptop Computer.

Notices

*-Notwork

/not'werk/ n.

A network, when it is acting flaky or is down. Compare nyetwork. Said at IBM to have originally referred to a particular period of flakiness on IBM's VNET corporate network ca. 1988; but there are independent reports of the term from elsewhere.

*-NP

- /N-P/ pref.

Extremely. Used to modify adjectives describing a level or quality of difficulty; the connotation is often

`more so than it should be' (NP-complete problems all seem to be very hard, but so far no one has found a good a priori reason that they should be. ) “Coding a BitBlt implementation to perform correctly in every case is NP-annoying. ” This is generalized from the computer-science terms `NP-hard' and `NP-complete'. NP is the set of Nondeterministic-Polynomial algorithms, those that can be completed by a nondeterministic Turing machine in an amount of time that is a polynomial function of the size of the input; a solution for one NP-complete problem would solve all the others. Note, however, that the NP- prefix is, from a complexity theorist's point of view, the wrong part of `NP-complete' to connote extreme difficulty; it is the completeness, not the NP-ness, that puts any problem it describes in the `hard' category.

*-Nroff

/N'rof/ n.
[UNIX, from “new roff” (see troff)] A companion program to the UNIX typesetter troff, accepting identical input but preparing output for terminals and line printers.

*-NSA Line Eater n.

The National Security Agency trawling program sometimes assumed to be reading the net for the U. S. Government's spooks. Most hackers describe it as a mythical beast, but some believe it actually exists, more aren't sure, and many believe in acting as though it exists just in case. Some netters put loaded phrases like `KGB', `Uzi', `nuclear materials', `Palestine', `cocaine', and `assassination' in their sig blocks in a (probably futile) attempt to confuse and overload the creature. The GNU version of EMACS actually has a command that randomly inserts a bunch of insidious anarcho-verbiage into your edited text. There is a mainstream variant of this myth involving a `Trunk Line Monitor', which supposedly used speech recognition to extract words from telephone trunks. This one was making the rounds in the late 1970s, spread by people who had no idea of then-current technology or the storage, signal-processing, or speech recognition needs of such a project. On the basis of mass-storage costs alone it would have been cheaper to hire 50 high-school students and just let them listen in. Speech-recognition technology can't do this job even now (1993), and almost certainly won't in this millennium, either. The peak of silliness came with a letter to an alternative paper in New Haven, Connecticut, laying out the factoids of this Big Brotherly affair. The letter writer then revealed his actual agenda by offering -- at an amazing low price, just this once, we take VISA and MasterCard -- a scrambler guaranteed to daunt the Trunk Trawler and presumably allowing the would-be Baader-Meinhof gangs of the world to get on with their business.

NSA's Ratings Maintenance Phase

NTISSD

NTISS Directives National Telecommunications and Information Systems Security Directives establish national-level decisions relating to NTISS policies, plans, programs, systems, or organizational delegations of authority. NTISSDs are promulgated by the Executive Agent of the Government for Telecommunications and Information Systems Security, or by the Chairman of the NTISSC when so delegated by the Executive Agent. NTISSDs are binding upon all federal departments and agencies.

NTISSI

National Telecommunications and Information Systems Security Advisory Memoranda/ Instructions NTISS Advisory Memoranda and Instructions provide advice, assistance, or information of general interest on telecommunications and systems security to all applicable federal departments and agencies. NTISSAMs/NTISSIs are promulgated by the National Manager for Telecommunications and Automated Information Systems Security and are recommendatory.

NTISSP

See National Telecommunications and Information Systems Security Policy.

NTSC Standard

See National Television Standards Committee standard. The North American standard for the generation, transmission, and reception of television communication wherein the 525-line picture is the standard.
Note 1: The picture information is transmitted in AM and the sound information is transmitted in FM. Compatible with CCIR Standard M. Note 2: This standard is used also in Central America, a number of South American countries, and some Asian countries, including Japan. See also PAL, PAL-M, SECAM, teleconference, television.
Note 2: Never Twice the Same Color

*-Nude

adj. Said of machines delivered without an operating system (compare bare metal). “We ordered 50 systems, but they all arrived nude, so we had to spend a an extra weekend with the installation tapes. ” This usage is a recent innovation reflecting the fact that most PC clones are now delivered with DOS or Microsoft Windows pre-installed at the factory. Other kinds of hardware are still normally delivered without OS, so this term is particular to PC support groups.

*-Nuke

/n[y]ook/ vt.
1. To intentionally delete the entire contents of a given directory or storage volume. “On UNIX, `rm

-r /usr' will nuke everything in the usr filesystem. ” Never used for accidental deletion. Oppose blow away.
2. Syn. for dike, applied to smaller things such as files, features, or code sections. Often used to express a final verdict. “What do you want me to do with that 80-meg wallpaper file?” “Nuke it. ”
3. Used of processes as well as files; nuke is a frequent verbal alias for `kill -9' on UNIX.
4. On IBM PCs, a bug that results in fandango on core can trash the operating system, including the FAT (the in-core copy of the disk block chaining information). This can utterly scramble attached disks, which are then said to have been `nuked'. This term is also used of analogous lossages on Macintoshes and other micros without memory protection.

Null

1. A dummy letter, letter symbol, or code group inserted in an encrypted message to delay or prevent its solution, or to complete encrypted groups for transmission or transmission security purposes.
2. See node (def. #4).
3. Of an antenna radiation pattern, a specific direction in which the radiated power of a transmitting antenna (or response sensitivity of a receiving antenna) approaches zero in relation to the radiated power in the main beam (or desired direction). Note: Often the null has a narrow directivity (angle) compared to that of the main beam, and this can be used for desirable purposes such as radio navigation or prevention of interfering signals in a given direction.

*-Number-Crunching

n. Computations of a numerical nature, esp. those that make extensive use of floating-point numbers. The only thing Fortrash is good for. This term is in widespread informal use outside hackerdom and even in mainstream slang, but has additional hackish connotations namely, that the computations are mindless and involve massive use of brute force. This is not always evil, esp. if it involves ray tracing or fractals or some other use that makes pretty pictures, esp. if such pictures can be used as wallpaper. See also crunch.

*-Numbers

n. [scientific computation] Output of a computation that may not be significant results but at least indicate that the program is running. May be used to placate management, grant sponsors, etc. `Making numbers' means running a program because output -- any output, not necessarily meaningful output -- is needed as a demonstration of progress. See pretty pictures, math-out, social science number.

*-NUXI Problem

/nuk'see pro'bl*m/ n. Refers to the problem of transferring data between machines with differing byte-order. The string `UNIX' might look like `NUXI' on a machine with a different `byte sex' (e. g. , when transferring data from a little-endian to a big-endian, or vice-versa). See also middle-endian, swab, and byte-sexual.

NXX

*-Nybble

/nib'l/ (alt. `nibble') n. [from v. `nibble' by analogy with `bite' => `byte'] Four bits; one hex digit; a half-byte. Though `byte' is now techspeak, this useful relative is still jargon. Compare byte; see also bit, Apparently this spelling is uncommon in Commonwealth Hackish, as British orthography suggests the pronunciation /ni:'bl/. Following `bit', `byte' and `nybble' there have been quite a few analogical attempts to construct unambiguous terms for bit blocks of other sizes. All of these are strictly jargon, not techspeak, and not very common jargon at that (most hackers would recognize them in context but not use them spontaneously). We collect them here for reference together with the ambiguous techspeak terms `word', `half-word' and `quadwords'; some (indicated) have substantial information separate entries. 2 bits ocrumb, quad quarter, tayste 4 bits nybble 5 bits nickle 10 bits deckle 16 bits playte, chawmp (on a 32-bit machine), word (on a 16-bit machine), half-word (on a 32-bit machine). 18 bits chawmp (on a 36-bit machine), half-word (on a 36-bit machine) 32 bits dynner, gawble (on a 32-bit machine), word (on a 32-bit machine), longword (on a 16-bit machine). 36 word (on a 36-bit machine) 48 bits gawble (under circumstances that remain obscure) The fundamental motivation for most of these jargon terms (aside from the normal hackerly enjoyment of punning wordplay) is the extreme ambiguity of the term `word' and its derivatives.

*-Nyetwork

/nyet'werk/ n. [from Russian `nyet' = no] A network, when it is acting flaky or is down. Compare notwork.

O

*-Ob

/ob/ pref. Obligatory. A piece of netiquette acknowledging that the author has been straying from the newsgroup's charter topic. It is considered a sign of great winnitude when one's Obs are more interesting than other people's whole postings.

*-Obfuscated C Contest

n. (in full, the `International Obfuscated C Code Contest', or IOCCC) An annual contest run since 1984 over Usenet by Landon Curt Noll and friends. The overall winner is whoever produces the most unread-

able, creative, and bizarre (but working) C program; various other prizes are awarded at the judges' whim. C's terse syntax and macro-preprocessor facilities give contestants a lot of maneuvering room. The winning programs often manage to be simultaneously (a) funny, (b) breathtaking works of art, and (c) horrible examples of how *not* to code in C. This relatively short and sweet entry might help convey the flavor of obfuscated C /* * HELLO WORLD program * by Jack Applin and Robert Heckendorn, 1985 */ main(v,c)char**c;for(v[c++]=“Hello, world!\n)”;(!!c)[*c]&&(v--||--c&&execlp(*c,*c,c[!!c]+!!c,!c)); **c=!c)write(!!*c,*c,!!**c); Here's another good one /* * Program to compute an approximation of pi * by Brian Westley, 1988 */ #define _ -F<00||--F-OO--; int F=00,OO=00; main()F_OO();printf(“%1. 3f\n”,4. *-F/OO/OO);F_OO() _-_-_-_ _-_-_-_-_-_-_-_-_ _-_-_-
_-_-_-_-_-_-_-_-_ _-_-_-_-_-_-_-_-_-_-_-_-_ _-_-_-
_-_-_-_-_-_-_-_-_-_-_ _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-
_ _-_-_-_-_-_-_-_-_-_-_-_-_-_-_ _-_-_-_-_-_-_-_-_-_-
_-_-_-_-_-_ _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_ _-_-_-
_-_-_-_-_-_-_-_-_-_-_-_ _-_-_-_-_-_-_-_-_-_-_-_-_-_-
_-_ _-_-_-_-_-_-_-_-_-_-_-_-_-_ _-_-_-_-_-_-_-_-_-_-
_-_-_-_ _-_-_-_-_-_-_-_-_-_-_-_-_-_ _-_-_-_-_-_-_-_ _-
_-_-_ Note that this program works by computing its own area. For more digits, write a bigger program. See also hello, world.

*-Obi-Wan Error

/oh'bee-won` er'*r/ n. [RPI, from `off-by-one' and the Obi-Wan Kenobi character in “Star Wars”] A loop of some sort in which the index is off by 1. Common when the index should have started from 0 but instead started from 1. A kind of off-by-one error. See also zeroth.

Object

A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc. (CSC-STD-001-83;; *AFR* 205-16;; *NCSC-WA*-001-85;; *DCID* 1/16-1, Sup. ;)

#-Object Labeling

See Labeling.

Object Reuse

The reassignment to some subject of a medium (e. g. , page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media must contain no residual data from the previously contained object(s). (CSC-STD-001-83;; *NCSC-WA*-001-85;)

Object Sharing

*-Objectionable-C

n. Hackish take on “Objective-C”, the name of an object-oriented dialect of C in competition with the better-known C++ (it is used to write native applications on the NeXT machine). Objectionable-C uses a Smalltalk-like syntax, but lacks the flexibility of Smalltalk method calls, and (like many such efforts) comes frustratingly close to attaining the Right Thing without actually doing so.

*-Obscure

adj. Used in an exaggeration of its normal meaning, to imply total incomprehensibility. “The reason for that last crash is obscure. ” “The `find(1)' command's syntax is obscure!” The phrase `moderately obscure' implies that something could be figured out but probably isn't worth the trouble. The construction `obscure in the extreme' is the preferred emphatic form.

Observables

Actions that reveal indicators exploitable by adversaries, but that must be carried out regardless, to plan, prepare for, and execute activities.

*-Octal Forty

/ok'tl for'tee/ n. Hackish way of saying “I'm drawing a blank. ” Octal 40 is the ASCII space character, 0100000; by an odd coincidence, hex 40 (01000000) is the EBCDIC space character. See wall.

Octet

A byte of eight binary digits usually operated upon as an entity. (~) See also binary digit, byte.

Odd Parity

See parity, parity check.

Odd-Even Check

See parity check.

Oersted

A unit of measure of the magnetizing force necessary to produce a desired magnetic flux across a surface. (CSC-STD-005-85;)

*-Off The Trolley

adj. Describes the behavior of a program that malfunctions and goes catatonic, but doesn't actually crash or abort. See glitch, bug, deep space.

*-Off-By-One Error

n. Exceedingly common error induced in many ways, such as by starting at 0 when you should have started at 1 or vice-versa, or by writing `< N' instead of `<= N' or vice-versa. Also applied to giving something to the person next to the one who should have gotten it.

Often confounded with fencepost error, which is properly a particular subtype of it.

Off-Line Crypto-Operation

1. Encryption or decryption performed separately and at a different time from the transmission or decryption, as by manual or machine crypto-equipments not electrically connected to a signal line. (NCSC-9)
2. See CRYPTO-OPERATION.

Off-Line Cryptosystem

Cryptosystem in which encryption and decryption are performed independently of the transmission and reception functions.

#-Off-Site Security (Information, Processing)

This KSA has no definition.

Off-The-Shelf Item

An item that has been developed and produced to military or commercial standards and specifications, is readily available for delivery from an industrial source, and may be procured without change to satisfy a military requirement. (JCS1-DoD) Note: The same definition applies to civil-sector procurement.

Office Of Information And Regulatory Affairs

Office Of Personnel Management

See OPM

Official Use Only (OUO)

1. A designation identifying unclassified information that may be exempt from mandatory disclosure under the FOIA. (DOE 5635. lA)
2. Synonymous with FOR OFFICIAL USE ONLY.

*-Offline

adv. Not now or not here. “Let's take this discussion offline. ” Specifically used on Usenet to suggest that a discussion be moved off a public newsgroup to email.

Offline Crypto-Operation

-Oid*

1. suff. [from `android'] Used as in mainstream English to indicate a poor imitation, a counterfeit, or some otherwise slightly bogus resemblance. Hackers will happily use it with all sorts of non-Greco/Latin stem words that wouldn't keep company with it in mainstream English. For example, “He's a nerdoid” means that he superficially resembles a nerd but can't make the grade; a `modemoid' might be a 300-baud box (Real Modems run at 9600 or up); a `computeroid' might be any bitty box. The word `keyboid' could be used to describe a chiclet keyboard, but would have to be written; spoken, it would confuse the listener as to the speaker's city of origin.
2. More specifically, an indicator for `resembling an android' which in the past has been confined to science-fiction fans and hackers. It too has recently (in 1991) started to go mainstream (most notably in the term `trendoid' for victims of terminal hipness). This is probably traceable to the popularization of the term droid in “Star Wars” and its sequels. Coinages in both forms have been common in science fiction for at least fifty years, and hackers (who are often SF fans) have probably been making `-oid' jargon for almost that long [though GLS and I can personally confirm only that they were already common in the mid-1970s -- ESR].

*-Ogg /og/ v. [CMU]

1. In the multi-player space combat game Netrek, to execute kamikaze attacks against enemy ships which are carrying armies or occupying strategic positions. Named during a game in which one of the players repeatedly used the tactic while playing Orion ship G, showing up in the player list as “Og”. This trick has been roundly denounced by those who would return to the good old days when the tactic of dogfighting was dominant, but as Sun Tzu wrote, “What is of supreme importance in war is to attack the enemy's strategy. ” However, the traditional answer to the newbie question “What does ogg mean?” is just “Pick up some armies and I'll show you. ”
2. In other games, to forcefully attack an opponent with the expectation that the resources expended will be renewed faster than the opponent will be able to regain his previous advantage. Taken more seriously as a tactic since it has gained a simple name.
3. To do anything forcefully, possibly without consideration of the drain on future resources. “I guess I'd better go ogg the problem set that's due tomorrow. ” “Whoops! I looked down at the map for a sec and almost ogged that oncoming car. ”

*-Old Fart n.

Tribal elder. A title self-assumed with remarkable frequency by (esp.) Usenetters who have been programming for more than about 25 years; often appears in sig blocks attached to Jargon File contributions of great archeological significance. This is a term of insult in the second or third person but one of pride in first person.

*-Old Testament n.

[C programmers] The first edition of K&R, the sacred text describing Classic C.

On-Line Crypto-Operation

1. The use of crypto-equipment that is directly connected to a signal line, so that encryption and transmission are accomplished simultaneously. (NCSC-9)
2. See CRYPTO-OPERATION.

On-Line Cryptosystem

Cryptosystem in which encryption and decryption are performed in association with the transmitting and receiving functions.

*-One-Banana Problem n.

At mainframe shops, where the computers have operators for routine administrivia, the programmers and hardware people tend to look down on the operators and claim that a trained monkey could do their job. It is frequently observed that the incentives that would be offered said monkeys can be used as a scale to describe the difficulty of a task. A one-banana problem is simple; hence, “It's only a one-banana job at the most; what's taking them so long?” At IBM, folklore divides the world into one-, two-, and three-banana problems. Other cultures have different hierarchies and may divide them more finely; at ICL, for example, five grapes (a bunch) equals a banana. Their upper limit for the in-house sysapes is said to be two bananas and three grapes (another source claims it's three bananas and one grape, but observes “However, this is subject to local variations, cosmic rays and ISO”). At a complication level any higher than that, one asks the manufacturers to send someone around to check things. See also Infinite-Monkey Theorem.

*-One-Line Fix n.

Used (often sarcastically) of a change to a program that is thought to be trivial or insignificant right up to the moment it crashes the system. Usually `cured' by another one-line fix. See also I didn't change anything!

*-One-Liner Wars

n. A game popular among hackers who code in the language APL (see write-only language and line noise). The objective is to see who can code the most interesting and/or useful routine in one line of operators chosen from APL's exceedingly hairy primitive set. A similar amusement was practiced among TECO hackers and is now popular among Perl aficionados. Ken Iverson, the inventor of APL, has been credited with a one-liner that, given a number N, produces a list of the prime numbers from 1 to N inclusive. It looks like this (2 = 0 +. = T o. | T) / T <- iN where `o' is the APL null character, the assignment arrow is a single character, and `i' represents the APL iota.

One-Part Code

Code in which plain text elements and their accompanying code groups are arranged in alphabetical, numerical, or other systematic order, so that one listing serves for both encoding and decoding. NOTE: One-part codes are normally small codes that are used to pass small volumes of low-sensitivity information.

One-Time

Cryptosystem employing key which is cryptosystem used only once.

One-Time Cryptosystem

Cryptosystem employing keys which are used only once.

One-Time Pad (OTP)

Manual one-time cryptosystem produced in pad form. (F:\NEWDEFS. TXT)

#-One-Time Passwords

1. One-time passwords [are] those that are changed after each use [and] are useful when the password is not adequately protected from compromise during login (e. g. , the communication line is suspected of being tapped). (*FIPS PUB* 112;)
2. A private character string that is used only once to authenticate an identity. After each use, a new character string is generated.

One-Time Tape (OTT)

Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems. (F:\NEWDEFS. TXT) Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems.

One-Way Function

A mathematical process that involves the transformation of data, usually with encryption-related routines, into a quantity that cannot then be used to recover the original data. (WB;)

Online Crypto-Operation

*-Ooblick

/oo'blik/ n. [from the Dr. Seuss title “Bartholomew and the Oobleck”] A bizarre semi-liquid sludge made from cornstarch and water. Enjoyed among hackers who make batches during playtime at parties for its amusing and extremely non-Newtonian behavior; it pours and splatters, but resists rapid motion like a solid and will even crack when hit by a hammer. Often found near lasers. Here is a field-tested ooblick recipe contributed by GLS 1 cup cornstarch 1 cup baking soda 3/4 cup water N drops of food coloring This recipe isn't quite as non-Newtonian as a pure cornstarch ooblick, but has an appropriately slimy feel. Some, however, insist that the notion of an ooblick *recipe* is far too mechanical, and that it is best to add the water in small increments so that the various mixed states the cornstarch goes through as it *becomes* ooblick can be grokked in fullness by many hands. For optional ingredients of this experi-

ence, see the “Ceremonial Chemicals” section of Appendix B.

*-Op /op/ n.

1. In England and Ireland, common verbal abbreviation for `operator', as in system operator. Less common in the U. S. , where sysop seems to be preferred.
2. [IRC] Someone who is endowed with privileges on IRC, not limited to a particular channel. These are generally people who are in charge of the IRC server at their particular site. Sometimes used interchangeably with CHOP. Compare sysop.

*-Open n.

Abbreviation for `open (or left) parenthesis' --- used when necessary to eliminate oral ambiguity. To read aloud the LISP form (DEFUN FOO (X) (PLUS X 1)) one might say “Open defun foo, open eks close, open, plus eks one, close close. ”

*-Open DeathTrap n.

Abusive hackerism for the Santa Cruz Operation's `Open DeskTop' product, a Motif-based graphical interface over their UNIX. The funniest part is that this was coined by SCO's own developers. Compare AIDX, Macintrash Nominal Semidestructor, ScumOS, sun-stools, HP-SUX.

Open Security

Environment that does not provide environment sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.

Open Security Environment

An enviornment that includes those systems in which one of the following conditions holds true:

a. Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic.
b. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications. (CSC-STD-004-85;; CSC-STD-003-85;; *NCSC-WA*-001-85;)

Open Source Information

Material available in the public domain. *Information of potential intelligence value (i. e. , intelligence information) available to the general public such as papers, books, periodicals, and other printed information It also includes information derived from radio and television transmissions, press agencies, maps, and photography (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89) *Information of potential intelligence value (i. e. , intelligence information) which is available to the general public(JCS PUB 1-02, 12/89)

Open Sources

Overt contacts between people or oral, documentary, pictorial, and physical materials accessible by the public (JCS MOP 199, 12/89)

Open Storage

The storage of classified information on shelves, in metal containers, locked or unlocked, but not in GSA-approved secure containers, within an accredited facility when such facility is not occupied by authorized personnel. (JCS PUB 6-03. 7)

*-Open Switch

n. [IBM prob. from railroading] An unresolved question, issue, or problem.

Open System

A system whose characteristics comply with specified, publicly maintained, readily available standards and that therefore can be connected to other systems that comply with these same standards. (After FP) (After ISO)

#-Open Systems Interconnect Model OSI

1. Pertaining to an ISO reference model intended to coordinate the development of standards and all levels of communications. The objective is to allow purchasers of communications equipment much greater freedom in mixing and matching equipment as well as a greater degree of protection against obsolescence. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992)
2. An international standard for the organization of local area networks (LANs) established by the International Standards Organization (ISO) and the Institute of Electrical and Electronic Engineers (IEEE). The OSI reference model is an important contribution to the conceptual design of local area networks because this model establishes hardware independence. The model separates the communications process into distinct layers: The physical hardware (such as cabling), the transport layer (the method by which data is communicated via the physical hardware), the presentation layer (the layer by which the transmitted data interacts with application programs in each computer), and the application layer (the programs available to all users of the network). (*QCUS+Pf-90*)

Open Systems Interconnection

(OSI) A logical structure for network operations standardized within the ISO; a seven-layer network architecture being used for the definition of network protocol standards to enable any OSI-compliant com-

puter or device to communicate with any other OSI-compliant computer or device for a meaningful exchange of information.

Open Systems Interconnection - Protocol Specifications

(OSI) The lowest level of abstraction within the OSI standards scheme. Each OSI-Protocol Specification operates at a single layer. Each defines the primitive operations and permissible responses required to exchange information between peer processes in communicating systems to carry out all or a subset of the services defined within the OSI-Service Definitions for that layer.

Open Systems Interconnection - Service Definitions

The next lower level of abstraction below that of the OSI--Reference Model. The OSI--Service Definitions for each layer define the layer's abstract interface and the facilities provided to the user of the service independent of the mechanism used to accomplish the service.

Open Systems Interconnection - Systems Management

Functions in the Application Layer related to the management of various OSI resources and their status across all layers of the OSI architecture.

Open Systems Interconnection Architecture

Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Architecture. (FS1037S1. TXT) (OSI) Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Architecture.

Open Systems Interconnection Protocol Specifications

The lowest level of abstraction within the OSI standards scheme. Each OSI-Protocol Specification operates at a single layer. Each defines the primitive operations and permissible responses required to exchange information between peer processes in communicating systems to carry out all or a subset of the services defined within the OSI-Service Definitions for that layer.

Open Systems Interconnection Service Definitions

The next lower level of abstraction below that of the OSI--Reference Model. The OSI--Service Definitions for each layer define the layer's abstract interface and the facilities provided to the user of the service independent of the mechanism used to accomplish the service.

Open Systems Interconnection Systems Management

Functions in the Application Layer related to the management of various OSI resources and their status across all layers of the OSI architecture.

Open Systems Interconnection--Reference Model (OSI-RM)

An abstract description of the digital communications between application processes running in distinct systems. The model employs a hierarchical structure of seven layers. Each layer performs value-added service at the request of the adjacent higher layer and, in turn, requests more basic services from the adjacent lower layer:

(a) Physical Layer: Layer 1, the lowest of seven hierarchical layers. The Physical layer performs services requested by the Data Link Layer. The major functions and services performed by the physical layer are: (a) establishment and termination of a connection to a communications medium; (b) participation in the process whereby the communication resources are effectively shared among multiple users, e. g. , contention resolution and flow control; and, (c) conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel.

(b) Data Link Layer: Layer 2. This layer responds to service requests from the Network Layer and issues service requests to the Physical Layer. The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. Note: Examples of data link protocols are HDLC and ADCCP for point-to-point or packet-switched networks and LLC for local area networks.

(c) Network Layer: Layer 3. This layer responds to service requests from the Transport Layer and issues service requests to the Data Link Layer. The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the Transport Layer. The Network Layer performs network routing, flow control, segmentation/desegmentation, and error control functions.

(d) Transport Layer: Layer 4. This layer responds to service requests from the Session Layer and issues service requests to the Network Layer. The purpose of the Transport Layer is to provide transparent transfer of data between end users, thus relieving the upper layers from any concern with providing reliable and cost-effective data transfer.

(e) Session Layer: Layer 5. This layer responds to service requests from the Presentation Layer and

issues service requests to the Transport Layer. The Session Layer provides the mechanism for managing the dialogue between end-user application processes. It provides for either duplex or half-duplex operation and establishes checkpointing, adjournment, termination, and restart procedures.

(f) Presentation Layer: Layer 6. This layer responds to service requests from the Application Layer and issues service requests to the Session Layer. The Presentation Layer relieves the Application Layer of concern regarding syntactical differences in data representation within the end-user systems. Note: An example of a presentation service would be the conversion of an EBCDIC-coded text file to an ASCII-coded file.

(g) Application Layer: Layer 7. The highest layer. This layer interfaces directly to and performs common application services for the application processes; it also issues requests to the Presentation Layer. The common application services provide semantic conversion between associated application processes. Note: Examples of common application services of general interest include the virtual file, virtual terminal, and job transfer and manipulation protocols.

#-Open Systems Security

Provision of tools for the secure internetworking of open systems. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Operand

An entity on which an operation is performed. (FP) (ISO) See also operation.

Operating System

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in operating a computer system. Operating systems may perform input or output, accounting, resource allocation, storage assignment tasks, and other system related functions. Synonymous with Monitor, Executive Control Program and Supervisor. (DODD 5200. 28M;)

#-Operating System Integrity

This KSA has no definition.

#-Operating System Security Features

This KSA has no definition.

#-Operating Systems

An integrated collection of routines that service the sequencing and processing of programs by a computer. (Source: NSAM 130-1).

Operation

1. The method, act, process, or effect of using a device or system. (~)
2. A well-defined action that, when applied to any permissible combination of known entities, produces a new entity, e. g. , the process of addition in arithmetic--in adding 5 and 3 to obtain 8, the numbers 5 and 3 are the operands, the number 8 is the result, and the plus sign is the operator indicating that the operation performed is addition. (FP) (ISO)
3. A program step, usually specified by the operation part of an instruction, that is undertaken or executed by a computer, e. g. , addition, multiplication, extraction, comparison, shift, transfer. (FP) See also instruction, operand.

Operational Data

Protection of data from security accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, or output operations.

Operational Data Security

The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations. (*AR* 380-380; *NCSC-WA*-001-85;)

Operational Key

Key intended for use on-the-air for protection of operational information or for the production or secure electrical transmission of key streams.

#-Operational Procedures Review

Determine if operational procedures have been established and are being followed by all appropriate users to minimize deficiencies and to validate correctness. (SOURCE: DACUM IV).

Operational Security Indicators

Actions or classified or unclassified information, obtainable by an (OPSEC) adversary, that would result in adversary appreciations, plans, and actions harmful to achieving friendly intentions and preserving friendly military capabilities. (*AFR* 700-10;)

Operational Site Security Manual

The manual documents the operational requirements, anualsecurity environment, hardware and software configurations and interfaces; all security procedures, measures, and features; and, for computer facilities, the contingency plans for continued support in case of a local disaster. (*AFR* 205-16;)

Operational Waiver

Authority for continued use of unmodified COMSEC end-items, pending the completion of a mandatory modification.

Operations Code (OPCODE)

Code composed largely of words and phrases which are suitable for general communications use.

Operations Security (OPSEC)

1. The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. (NCSC-9)
2. An analytical process by which the U. S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations. (*NCSC-TG*-004-88)

Operations Security Appraisal

The initial data collection and evaluation effort that validates the need for and provides the focus for the activities of the OPSEC survey (NASA, Operations Security Program Plan, 4/86)

Operations Security Assessment

A process of analyzing information and indicator sources associated with operations and other activities to evaluate and improve the effectiveness of an organization in protecting its critical information from adversaries. Note: Operations security techniques include: (a) identifying critical information that must be protected. (b) identifying indicators of information that can be observed or obtained by adversaries that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and (c) selecting and recommending measures that eliminate or reduce the vulnerabilities of friendly actions or information to adversary exploitation. See also operations security, operations security survey.

Operations Security Indicators

Actions or classified or unclassified information, obtainable by an (OPSEC) adversary, that would result in adversary appreciations, plans, and actions harmful to achieving friendly intentions and preserving friendly military capabilities. (*AFR* 700-10)

Operations Security Measures

Methods and means to delay or prevent the exploitation of sensitive/critical information. *Methods and means to gain and maintain essential secrecy about critical information. The following categories apply:

1. Action Control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake, decide whether or not to execute actions; and determine the “who, when, where, and how” for actions necessary to accomplish tasks.
2. Countermeasures. The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed Use of diversions, camouflage, concealment, jamming, threats, law enforcement powers, and force against adversary information gathering and processing capabilities.
3. Counteranalysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers (JCS PUB 3-54, 9/89)

Operations Security Monitoring

A review of an organization's operations and activities to ensure that OPSEC measures remain effective.

Operations Security Planning Guidance

Guidance that serves as the blueprint for OPSEC planning by all functional elements throughout an organization. It defines the critical information that requires protection from adversary appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence system threats. It also should outline provisional OPSEC measures to ensure the requisite essential secrecy. (JCS PUB 3-54, 9/89)

Operations Security Process

A systems analysis methodology as outlined in NSDD-298 involving identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Operations Security Survey

A thorough on-site examination of an operation or activity to determine if there are vulnerabilities that would permit adversaries' exploitation of critical information during the planning, preparation, execution, and post-execution phases of any operation or activity. See also operations security, operations security assessment.

Operations Security Vulnerability

A condition in which critical or sensitive information is subject to adversary exploitation. *A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making (JCS PUB 3-54, 9/89)

Operations Security Working Group

A formally designated body representing a broad range of administrative and programmatic activities which provides review, support, and participation with management in the implementation and furtherance of their OPSEC program.

Operator

Operator Of A Federal Computer System

A federal agency, contractor of a federal agency, or other organization that processes information using a

computer system on behalf of the federal government to accomplish a federal function. (PL 100-235)

Optical Character Reader

A device employed for optical character recognition.

Optical Character Recognition

The machine identification of printed characters through use of light-sensitive devices. (~) See also character.

*-Optical Diff

n. See vdiff.

*-Optical Grep

n. See vgrep.

Optical Intelligence

(OPTINT) That portion of electro-optical intelligence that deals with visible light. *That portion of electro-optical intelligence that deals with visible light. (*IC Staff, Glossary of Intelligence Terms and Definitions,* 6/89)

#-Optical/Imaging Systems Security

This KSA has no definition.

*-Optimism

n. What a programmer is full of after fixing the last bug and before discovering the *next* last bug. Fred Brooks's book "The Mythical Man-Month" (See "Brooks's Law") contains the following paragraph that describes this extremely well All programmers are optimists. Perhaps this modern sorcery especially attracts those who believe in happy endings and fairy godmothers. Perhaps the hundreds of nitty frustrations drive away all but those who habitually focus on the end goal. Perhaps it is merely that computers are young, programmers are younger, and the young are always optimists. But however the selection process works, the result is indisputable"This time it will surely run," or "I just found the last bug. ". See also Lubarsky's Law of Cybernetic Entomology.

Optional Modification

National Security Agency approved modification that is not required for universal implementation by all holders of a COMSEC end-item. NOTE: This class of modification requires all of the engineering/ doctrinal control of mandatory modification, but is usually not related to security, safety, TEMPEST, or reliability.

Orange Book

Alternate name for DoD Trusted Computer Security Evaluation Criteria. (*NCSC-TG*-004-88)

Orange Book Terminology

The *DOD* 5200. 28-STD (*Orange Book*) classifies AISs into four broad hierarchical divisions of security protection. Within divisions C and B there are further subdivisions called classes. These classes are also ordered in a hierarchical manner characterized by a set of computer security features they possess. (DODD 5200. 28;)

ORCON

Originator Controlled. This is an indication that documents bearing the marking are controlled by the originator. Reproduction or redistribution require the permission of the originator. (DOE 5635. 1A;)

Organization C4 Systems Security Office

Office charged with the responsibility for managing and executing the C4 systems security program for a unit.

Organizational

Limited maintenance performed by a maintenance user organization.

#-Organizational Culture

This KSA has no definition.

Organizational Maintenance

Limited maintenance performed by a user organization.

#-Organizational Placement Of The IS/IT Security Function

This KSA has no definition.

*-Oriental Food n.

Hackers display an intense tropism towards oriental cuisine, especially Chinese, and especially of the spicier varieties such as Szechuan and Hunan. This phenomenon (which has also been observed in subcultures that overlap heavily with hackerdom, most notably science-fiction fandom) has never been satisfactorily explained, but is sufficiently intense that one can assume the target of a hackish dinner expedition to be the best local Chinese place and be right at least three times out of four. See also ravs, great-wall, stir-fried random, laser chicken, Yu-Shiang Whole Fish. Thai, Indian, Korean, and Vietnamese cuisines are also quite popular.

Orientation

The formal and informal presentations and discussions with the authority responsible for the ADO system which supplements the information in the initial security testing and evaluation (ST&E) request and provides the system evaluators an introduction to the operating environment, the techniques used to provide system security, the identity and location of documentation describing the implementation of system security measures (e. g. , O/S modifications, etc.), and the techniques available to demonstrate the effectiveness of such measures in meeting requirements of DoD Directive 5200. 28. (DODD 5200. 28M;)

Originating User

*-Orphan

n. [UNIX] A process whose parent has died; one inherited by `init(1)'. Compare zombie.

*-Orphaned I-Node

/or'f*nd i:'nohd/ n. [UNIX]

1. [techspeak] A file that retains storage but no longer appears in the directories of a filesystem.
2. By extension, a pejorative for any person no longer serving a useful function within some organization, esp. lion food without subordinates.

*-Orthogonal adj. [from mathematics]

Mutually independent; well separated; sometimes, irrelevant to. Used in a generalization of its mathematical meaning to describe sets of primitives or capabilities that, like a vector basis in geometry, span the entire `capability space' of the system and are in some sense non-overlapping or mutually independent. For example, in architectures such as the PDP-11 or VAX where all or nearly all registers can be used interchangeably in any role with respect to any instruction, the register set is said to be orthogonal. Or, in logic, the set of operators `not' and `or' is orthogonal, but the set `nand', `or', and `not' is not (because any one of these can be expressed in terms of the others). Also used in comments on human discourse “This may be orthogonal to the discussion, but. ”

OS

1. Open Skies (Treaty)
2. /O-S/ [Operating System] n. An abbreviation heavily used in email, occasionally in speech.

*-OS/2

/O S too/ n. The anointed successor to MS-DOS for Intel 286- and 386-based micros; proof that IBM/Microsoft couldn't get it right the second time, either. Often called `Half-an-OS'. Mentioning it is usually good for a cheap laugh among hackers --- the design was so baroque, and the implementation of 1. x so bad, that 3 years after introduction you could still count the major apps shipping for it on the fingers of two hands -- in unary. The 2. x versions are said to have improved somewhat, and informed hackers now rate them superior to Microsoft Windows (an endorsement which, however, could easily be construed as damning with faint praise). See monstrosity, cretinous, second-system effect.

*-OSU

/O-S-U/ n. ,obs. [TMRC] Acronym for Officially Sanctioned User; a user who is recognized as such by the computer authorities and allowed to use the computer above the objections of the security monitor.

*-Out-Of-Band

1. adj. [from telecommunications and network theory] In software, describes values of a function which are not in its `natural' range of return values, but are rather signals that some kind of exception has occurred. Many C functions, for example, return a nonnegative integral value, but indicate failure with an out-of-band return value of -1. Compare hidden flag, green bytes, fence.
2. Also sometimes used to describe what communications people call `shift characters', such as the ESC that leads control sequences for many terminals, or the level shift indicators in the old 5-bit Baudot codes.
3. In personal communication, using methods other than email, such as telephones or snail-mail.

Out-Of-Band Emission

Emission on a frequency or frequencies immediately outside the necessary bandwidth, which results from the modulation process, but excluding spurious emission. (RR) See also emission.

Out-Of-Band Signaling

1. The transmission of signaling via a different channel (either FDM or TDM) from that used for the primary information transfer. (~)
2. Signals using a portion of the channel bandwidth provided by the medium such as the carrier channel, but denied to the speech or intelligence path by filters.

Note: This results in a reduction of the effective available bandwidth. See also bandwidth, channel, channel-associated signaling, common-channel signaling, frequency, in-band signaling, retrieval, signal.

Outage

A telecommunication service condition wherein a user is completely deprived of service due to any cause within the communication system. (~) Note: For a particular system, “outage” may be defined in terms of minimum acceptable performance. See also continuous operation, degraded service state, failure, operational service state, performance measurement period, performance parameter.

Outage Duration

That period of time between the onset of an outage and the restoration of service. (~) See also downtime, mean time to service restoral, operational service period.

Outage Probability

The probability that the outage state will occur within a specified time period. See also outage ratio, performance measurement period.

Output

1. Information retrieved from a functional unit or from a network, usually after some processing. (FP)
2. An output state, or sequence of states. (FP) (ISO)

3. Pertaining to a device, process, or channel involved in the production of data by a computer or by any of its components. (FP) (ISO)
3. Information that has been exported by a TCB (CSC-STD-001-83)

Output-Only Devices

Devices such as printers, connected to a host (directly or via communications devices) that perform no input functions to the host. (JCS PUB 6-03. 7)

Outside Plant

Over-The-Air Key

Providing electronic key via distribution over-the-air rekeying, over-the-air key transfer, or cooperative key generation.

Over-The-Air Key Distribution

(OTAD) Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.

Over-The-Air Key Transfer (OTAT)

Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished. (F:\NEWDEFS. TXT)

Over-The-Air Rekeying (OTAR)

Changing traffic encryption key or transmission security key in remote crypto-equipment by sending new key directly to the remote crypto-equipment over the communications path it secures. (F:\NEWDEFS. TXT)

Overall Security

A property of a system involving consideration of all assets and threats. (RM;)

Overflow

1. Generally, the generation of potential traffic beyond the capacity of a system or subsystem. (~)
2. A count of telephone call attempts made on busy groups of trunks or access lines. See also high-usage trunk group, traffic overflow.
3. Traffic handled by overflow equipment.
4. Traffic that exceeds the capacity of the switching equipment and is therefore lost. (~)
5. Excess traffic on a particular route, which is offered to another (alternate) route. (~)
6. A condition existing within a digital computer resulting from an attempt to calculate a value that exceeds the numbering capacity of the machine. (~) See arithmetic overflow. See also underflow.

*-Overflow Bit n.

1. [techspeak] A flag on some processors indicating an attempt to calculate a result too large for a register to hold.
2. More generally, an indication of any kind of capacity overload condition. “Well, the Ada description was baroque all right, but I could hack it OK until they got to the exception handling . that set my overflow bit. ”
3. The hypothetical bit that will be set if a hacker doesn't get to make a trip to the Room of Porcelain Fixtures “I'd better process an internal interrupt before the overflow bit gets set”.

*-Overflow Pdl

n. [MIT] The place where you put things when your pdl is full. If you don't have one and too many things get pushed, you forget something. The overflow pdl for a person's memory might be a memo pad. This usage inspired the following doggere l Hey, diddle, diddle The overflow pdl To get a little more stack; If that's not enough Then you lose it all, And have to pop all the way back. --The Great Quux The term pdl seems to be primarily an MITism; outside MIT this term is replaced by `overflow stack'.

Overhead Bit

Any bit other than a user information bit. (~) See also binary digit, front-end processing, maximum stuffing rate, overhead information, service bit, and user information bit.

Overhead Communications

See overhead bit.

*-Overrun n.

1. [techspeak] Term for a frequent consequence of data arriving faster than it can be consumed, esp. in serial line communications. For example, at 9600 baud there is almost exactly one character per millisecond, so if a silo can hold only two characters and the machine takes longer than 2 msec to get to service the interrupt, at least one character will be lost.
2. Also applied to non-serial-I/O communications. “I forgot to pay my electric bill due to mail overrun. ” “Sorry, I got four phone calls in 3 minutes last night and lost your message to overrun. ” When thrashing at tasks, the next person to make a request might be told “Overrun!” Compare firehose syndrome.
3. More loosely, may refer to a buffer overflow not necessarily related to processing time.

#-Oversight

This KSA has no definition.

Overt Channel

A path within a computer system or network that is designed for the authorized transfer of data. (*NCSC-WA*-001-85;) See Covert Channel.

Overt Collection

The acquisition of intelligence information in the public domain. *The acquisition of intelligence information from public media, observation, government-to-government dialogue, elicitation, and from the sharing of data openly acquired; the process may be classified or unclassified; the target and host governments as well as the sources involved normally are aware of the general collection activity, although the specific acquisition, sites, and processes may be successfully concealed. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Overwrite

A procedure to remove or destroy data recorded on magnetic storage media by writing patterns of data over or on top of the data stored on the media. (*NCSC-WA*-001-85;)

Overwrite Procedure

1. A stimulation to change the state of a bit followed by a known pattern.
2. Process which removes or destroys data recorded on an AIS storage medium by writing patterns of data over, or on top of, the data stored on the medium.
3. A procedure to remove or destroy data recorded on ADP magnetic storage media by recording patterns of unclassified data over or on top of the data stored on the media. (CSC-STD-005-85;) See Magnetic Remanence.

Overwriting

1. The obliteration of material by writing over the record. (*AR* 380-380;)
2. The obliteration of recorded data by recording different data on the same surface. (*FIPS PUB* 39;)

Owner Access Mode

Owner Of Data

The individual or group that has responsibility for specific data types and that is charged with the communication of the need for certain security-related handling procedures to both the users and custodians of this data. (WB;)

P

*-P-Mail

n. Physical mail, as opposed to email. Synonymous with snail-mail.
A Shareware e-mail package

*-P. O. D.

/P-O-D/ Acronym for `Piece Of Data' (as opposed to a code section). Usagepedantic and rare. See also pod.

PABX

See private automatic branch exchange. Note: Use of the term “PBX” is more common than “PABX,” regardless of automation.

Packet

In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and possibly error control information, are arranged in a specific format. (FP) (ISO) (~) See also binary digit, burst switching, format, packet switching, protocol, protocol data unit.

Packet Assembler/disassembler

(PAD) A functional unit that enables data terminal equipment not equipped for packet switching to access a packet-switched network. (FP) (ISO)

#-Packet Filtering

A feature incorporated into routers to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network.

Packet Format

The structure of data and control of information in a packet. (~) Note: The size and content of the various fields are defined by a set of rules that are used to make up a packet. See also format (def. #1), protocol.

#-Packet Switched Networks

1. A network of devices that communicate between each other by transmitting packets addressed to particular destinations. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992)
2. A system that partitions a unit of information or messages into smaller standardized units and then sends these units into the network with routing information so that they can reach their final destination.

Packet Switching

The process of routing and transferring data by means of addressed packets so that a channel is occupied during the transmission of the packet only, and upon completion of the transmission the channel is made available for the transfer of other traffic. (FP) (ISO) (~) See also channel, circuit switching, compelled signaling, connectionless mode transmission, data, interface message processor, message switching, packet, packet mode terminal, packet-switching network, public switched network, switching system.

Packet Transfer Mode

A method of information transfer, by means of packet transmission and packet switching, that permits dy-

namic sharing of network resources among many connections. See also connection.

Packet-Mode Terminal

Data terminal equipment that can control, format, transmit, and receive packets. (FP) (ISO) (~) See also mode (def. #3), packet switching, terminal.

Packet-Switched Data Transmission Service

A service that provides the transmission of data in the form of packets. (~) Note: This service may or may not provide for the assembly and disassembly of data packets. See also data, data transmission.

Packet-Switching Network

A network designed to carry data in the form of packets. Note: The packet format, internal to the network, may require conversion at a gateway. (~) See also burst switching, data, packet, packet switching.

PAD

See packet assembler/ disassembler.

*-Padded Cell

n. Where you put lusers so they can't hurt anything. A program that limits a luser to a carefully restricted subset of the capabilities of the host system (for example, the `rsh(1)' utility on USG UNIX). Note that this is different from an iron box because it is overt and not aimed at enforcing security so much as protecting others (and the luser) from the consequences of the luser's boundless naivete (see naive). Also `padded cell environment'.

*-Page In

1. v. [MIT] To become aware of one's surroundings again after having paged out (see page out). Usually confined to the sarcastic comment “Eric pages in, film at 11!”
2. Syn. `swap in'; see swap.

*-Page Out

1. vi. [MIT] To become unaware of one's surroundings temporarily, due to daydreaming or preoccupation. “Can you repeat that? I paged out for a minute. ” See page in. Compare glitch, thinko.
2. Syn. `swap out'; see swap.

*-Pain In The Net

n. A flamer.

Paired Disparity Code

A code in which some or all of the characters are represented by two sets of digits of opposite disparity that are used in sequence so as to minimize the total disparity of a longer sequence, e. g. , an alternate mark inversion signal. (~) See also alternate mark inversion signal.

*-Paper-Net

n. Hackish way of referring to the postal service, analogizing it to a very slow, low-reliability network. Usenet sig blocks sometimes include a “Paper-Net:” header just before the sender's postal address; common variants of this are “Papernet” and “P-Net”. Note that the standard netiquette guidelines discourage this practice as a waste of bandwidth, since netters are quite unlikely to casually use postal addresses. Compare voice-net, snail-mail, P-mail.

Paperwork Reduction Act

Parallel Computer

A computer that has multiple arithmetic units or logic units that are used to accomplish parallel operations or parallel processing. (FP) (ISO)

Parallel Information Unit

Two or more bits arranged in a deterministic order which are transferred when a clock or trigger pulse causes the entire unit to be simultaneously gated out of a register or other storage device. Two or more units can form a larger unit.

Parallel Processing

Pertaining to the concurrent or simultaneous execution of two or more processes in a single unit. (FP) (ISO)

Parallel Transmission

The simultaneous transmission of the signal elements of a group representing a character or other data item. (FP) (~) See also serial transmission.

Parallel-To-Serial Converter

A digital device that converts a group of simultaneous inputs, often constituting a byte or other defined block of data, into corresponding time-sequenced signal elements. See s dynamicizer, serializer. See also serial-to-parallel converter.

*-Param

/p*-ram'/ n. Shorthand for `parameter'. See also parm; compare arg, var.

Parameters

Values associated with assets used in costing functions. (RM;)

*-Parent Message

n. What a followup follows up.

Parity

In binary-coded systems, the oddness or evenness of the number of ones in a finite binary stream. (~) Note: By the addition of one extra bit, a bit stream can be forced to a specified parity state. This is often used as a simple error-detection check, and will detect (but not correct) the occurrences of any single bit error in the field. See also block parity.

Parity Check

A check that tests whether the number of ones or zeros in an array of binary digits is odd or even. (~) Note: Odd parity is standard for synchronous transmission and even parity for asynchronous transmission. See odd-even check. See also block parity, check bit, check digit, code, error control.

*-Parity Errors

pl. n. Little lapses of attention or (in more severe cases) consciousness, usually brought on by having spent all night and most of the next day hacking. “I need to go home and crash; I'm starting to get a lot of parity errors. ” Derives from a relatively common but nearly always correctable transient error in RAM hardware. Parity errors can also afflict mass storage and serial communication lines; this is more serious because not always correctable.

*-Parkinson's Law Of Data

prov. “Data expands to fill the space available for storage”; buying more memory encourages the use of more memory-intensive techniques. It has been observed over the last 10 years that the memory usage of evolving systems tends to double roughly once every 18 months. Fortunately, memory density available for constant dollars also tends to double about once every 12 months (see Moore's Law); unfortunately, the laws of physics guarantee that the latter cannot continue indefinitely.

*-Parm

/parm/ n. Further-compressed form of param. This term is an IBMism, and written use is almost unknown outside IBM shops; spoken /parm/ is more widely distributed, but the synonym arg is favored among hackers. Compare arg, var.

*-Parse

[from linguistic terminology] vt.

1. To determine the syntactic structure of a sentence or other utterance (close to the standard English meaning). “That was the one I saw you. ” “I can't parse that. ”
2. More generally, to understand or comprehend. “It's very simple; you just kretch the glims and then aos the zotz. ” “I can't parse that. ”
3. Of fish, to have to remove the bones yourself. “I object to parsing fish”, means “I don't want to get a whole fish, but a sliced one is okay”. A `parsed fish' has been deboned. There is some controversy over whether `unparsed' should mean `bony', or also mean `deboned'.

Partial Ordering

Partitioned Security Code

1. A mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information handled by the AIS. This encompasses the compartmented mode defined in *DCID* 1/1 6. (DODD 5200. 28)
2. A mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information contained in the system. (*NCSC-TG*-004-88)

Partitioned Security Mode

A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval, for all information handled by the AIS. This security mode encompasses the compartmented mode defined in *DCID* 1/16. (DODD 5200. 28;; *NCSC-WA*-001-85;) NOTE: This security mode encompasses the compartmented mode and applies to non-intelligence DoD organizations and DoD contractors.

*-Pascal

n. An Algol-descended language designed by Niklaus Wirth on the CDC 6600 around 1967--68 as an instructional tool for elementary programming. This language, designed primarily to keep students from shooting themselves in the foot and thus extremely restrictive from a general-purpose-programming point of view, was later promoted as a general-purpose tool and, in fact, became the ancestor of a large family of languages including Modula-2 and Ada (see also bondage-and-discipline language). The hackish point of view on Pascal was probably best summed up by a devastating (and, in its deadpan way, screamingly funny) 1981 paper by Brian Kernighan (of K&R fame) entitled “Why Pascal is Not My Favorite Programming Language”, which was turned down by the technical journals but circulated widely via photocopies. It was eventually published in “Comparing and Assessing Programming Languages”, edited by Alan Feuer and Narain Gehani (Prentice-Hall, 1984). Part of his discussion is worth repeating here, because its criticisms are still apposite to Pascal itself after ten years of improvement and could also stand as an indictment of many other bondage-and-discipline languages. At the end of a summary of the case against Pascal, Kernighan wrote 9. There is no escape This last point is perhaps the most important. The language is inadequate but circumscribed, because there is no way to escape its limitations. There are no casts to disable the type-checking when necessary. There is no way to replace the defective run-time environment with a sensible one, unless one controls the compiler that defines the “standard procedures”. The language is closed. People who use Pascal for serious programming fall into a fatal trap. Because the language is impotent, it must be extended. But each group extends Pascal in its own direction, to make it look like whatever language they really want. Extensions for

separate compilation, FORTRAN-like COMMON, string data types, internal static variables, initialization, octal numbers, bit operators, etc. , all add to the utility of the language for one group but destroy its portability to others. I feel that it is a mistake to use Pascal for anything much beyond its original target. In its pure form, Pascal is a toy language, suitable for teaching but not for real programming. Pascal has since been almost entirely displaced (by C) from the niches it had acquired in serious applications and systems programming, but retains some popularity as a hobbyist language in the MS-DOS and Macintosh worlds.

Pass Key

Passive Attack

Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data. See Active Attack.

Passive Station

On a multipoint connection or a point-to-point connection using basic mode link control, any tributary station waiting to be polled or selected. (FP) (ISO) See also node, terminal.

Passive Threat

The threat of unauthorized disclosure of information without changing the state of the system. (SS;)

Passive Wiretapping

The monitoring and/or recording of data while the data is being transmitted over a communications link. (*FIPS PUB* 39;)

Passphrase

A sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length. (*FIPS PUB* 112;) See Password.

Password

1. A protected word or string of characters that identifies or authenticates a user for access to a specific resource such as a system, data set, file, record, and so forth. (*AFR* 205-16;; *AR* 380-380;; *OPNAVINST* 5239. 1A;)
2. A private character string that is used to authenticate an identity. (CSC-STD-001-83;)
3. A protected word, phrase or string of symbols that is used to authenticate the identity of a user. (DOE 5636. 2A;)
4. A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type. Synonymous with Keyword. (*FIPS PUB* 39;)
5. A protected/private character string used to authenticate an identity. Knowledge of a valid user ID and its associated password is considered proof of authorization to access a system. (*NCSC-WA*-001-85;; CSC-STD-002-85;)
6. Confidential authentication information, usually composed of a string of characters. (SS;)

Password Dialogue

Interactive communications between user and computer to enter and verify a password. See Handshaking Procedure.

Password Length Equation

An equation that determines an appropriate password length, M, which provides an acceptable probability, P, that a password will be guessed in its lifetime. Note: The password length is given by M = (log S)/(log N) where S is the size of the password space and N is the number of characters available. The password space is given by S = LR/P, where L is the maximum lifetime of a password and R is the number of guesses per unit of time. See also password length parameter.

Password Length Parameter

A basic parameter affecting the password length needed to provide a given degree of security. Note 1: Password length parameters are related by the expression P = LR/S, where P is the probability that a password can be guessed in its lifetime, L is the maximum lifetime a password can be used to log into a system, R is the number of guesses per unit of time, and S is the number of unique algorithm-generated passwords (the password space). Note 2: The degree of password security is determined by the probability that a password can be guessed in its lifetime.

#-Password Management

This KSA has no definition.

Password Management Guideline

Password Space

The total number of possible passwords that can be created by a given password generation scheme. (DOE 5637-1)

Password System

1. A part of an ADP system that is used to authenticate a user's identity. Assurance of unequivocal identification is based on the user's ability to enter a private password that noone else should know. (CSC-STD-002-85;)
2. A system that uses a password or passphrase to authenticate a person's identity or to authorize a person's access to data and which consists of a means for performing one or more of the following password operations: generation, distribution, entry, storage, authentication, replacement, encryption and/or decryption of passwords. (*FIPS PUB* 112;)

*-Pastie

/pay'stee/ n. An adhesive-backed label designed to be attached to a key on a keyboard to indicate some non-standard character which can be accessed through that key. Pasties are likely to be used in APL environments, where almost every key is associated with a special character. A pastie on the R key, for example, might remind the user that it is used to generate the rho character. The term properly refers to nipple-concealing devices formerly worn by strippers in concession to indecent-exposure laws; compare tits on a keyboard.

*-Patch

1. n. A temporary addition to a piece of code, usually as a quick-and-dirty remedy to an existing bug or misfeature. A patch may or may not work, and may or may not eventually be incorporated permanently into the program. Distinguished from a diff or mod by the fact that a patch is generated by more primitive means than the rest of the program; the classical examples are instructions modified by using the front panel switches, and changes made directly to the binary executable of a program originally written in an HLL. Compare one-line fix.
2. vt. To insert a patch into a piece of code. [in the UNIX world] n. A diff (sense 2) A set of modifications to binaries to be applied by a patching program. IBM operating systems often receive updates to the operating system in the form of absolute hexadecimal patches. If you have modified your OS, you have to disassemble these back to the source. The patches might later be corrected by other patches on top of them (patches were said to “grow scar tissue”). The result was often a convoluted patch space and headaches galore. [UNIX] the `patch(1)' program, written by Larry Wall, which automatically applies a patch to a set of source code. There is a classic story of a tiger team penetrating a secure military computer that illustrates the danger inherent in binary patches (or, indeed, any patches that you can't -- or don't -- inspect and examine before installing). They couldn't find any trap doors or any way to penetrate security of IBM's OS, so they made a site visit to an IBM office (remember, these were official military types who were purportedly on official business), swiped some IBM stationery, and created a fake patch. The patch was actually the trapdoor they needed. The patch was distributed at about the right time for an IBM patch, had official stationery and all accompanying documentation, and was dutifully installed. The installation manager very shortly thereafter learned something about proper procedures.

*-Patch Space

n. An unused block of bits left in a binary so that it can later be modified by insertion of machine-language instructions there (typically, the patch space is modified to contain new code, and the superseded code is patched to contain a jump or call to the patch space). The widening use of HLLs has made this term rare; it is now primarily historical outside IBM shops. See patch (sense 4), zap (sense 4), hook.

*-Path

1. n. A bang path or explicitly routed Internet address; a node-by-node specification of a link between two machines.
2. [UNIX] A filename, fully specified relative to the root directory (as opposed to relative to the current directory; the latter is sometimes called a `relative path'). This is also called a `pathname'.
3. [UNIX and MS-DOS] The `search path', an environment variable specifying the directories in which the shell (COMMAND. COM, under MS-DOS) should look for commands. Other, similar constructs abound under UNIX (for example, the C preprocessor has a `search path' it uses in looking for `#include' files).

*-Pathological

1. adj. [scientific computation] Used of a data set that is grossly atypical of normal expected input, esp. one that exposes a weakness or bug in whatever algorithm one is using. An algorithm that can be broken by pathological inputs may still be useful if such inputs are very unlikely to occur in practice.
2. When used of test input, implies that it was purposefully engineered as a worst case. The implication in both senses is that the data is spectacularly ill-conditioned or that someone had to explicitly set out to break the algorithm in order to come up with such a crazy example.
3. Also said of an unlikely collection of circumstances. “If the network is down and comes up halfway through the execution of that command by root, the system may just crash. ” “Yes, but that's a pathological case. ” Often used to dismiss the case from discussion, with the implication that the consequences are acceptable, since they will happen so infrequently (if at all) that it doesn't seem worth going to the extra trouble to handle that case (see sense 1).

Patterns

Stereotyped operations, procedures, or processes that reveal protected informationSee Signature.

PAX

*-Payware

/pay'weir/ n. Commercial software. Oppose shareware or freeware.

***-PBD**

/P-B-D/ n. [abbrev. of `Programmer Brain Damage'] Applied to bug reports revealing places where the program was obviously broken by an incompetent or short-sighted programmer. Compare UBD; see also brain-damaged.

***-PC-Ism**

/P-C-izm/ n. A piece of code or coding technique that takes advantage of the unprotected single-tasking environment in IBM PCs and the like, e. g. , by busy-waiting on a hardware register, direct diddling of screen memory, or using hard timing loops. Compare ill-behaved, vaxism, unixism. Also, `PC-ware' n. , a program full of PC-isms on a machine with a more capable operating system. Pejorative.

***-PD**

/P-D/ adj. Common abbreviation for `public domain', applied to software distributed over Usenet and from Internet archive sites. Much of this software is not in fact public domain in the legal sense but travels under various copyrights granting reproduction and use rights to anyone who can snarf a copy. See copyleft.

Pdl

/P-D-L/, /pid'l/, /p*d'l/ or /puhd'l/
n. `Program Design Language'. Any of a large class of formal and profoundly useless pseudo-languages in which management forces one to design programs. Too often, management expects PDL descriptions to be maintained in parallel with the code, imposing massive overhead to little or no benefit.

***-PDP-10**

n. [Programmed Data Processor model 10] The machine that made timesharing real. It looms large in hacker folklore because of its adoption in the mid-1970s by many university computing facilities and research labs, including the MIT AI Lab, Stanford, and CMU. Some aspects of the instruction set (most notably the bit-field instructions) are still considered unsurpassed. The 10 was eventually eclipsed by the VAX machines (descendants of the PDP-11) when DEC recognized that the 10 and VAX product lines were competing with each other and decided to concentrate its software development effort on the more profitable VAX. The machine was finally dropped from DEC's line in 1983, following the failure of the Jupiter Project at DEC to build a viable new model. (Some attempts by other companies to market clones came to nothing; see Foonly and Mars.) This event spelled the doom of ITS and the technical cultures that had spawned the original Jargon File, but by mid-1991 it had become something of a badge of honorable old-timerhood among hackers to have cut one's teeth on a PDP-10. See TOPS-10, ITS, AOS, BLT, DDT, DPB, EXCH, HAKMEM, JFCL, LDB, pop, push.

***-PDP-20**

n. The most famous computer that never was. PDP-10 computers running the TOPS-10 operating system were labeled `DECsystem-10' as a way of differentiating them from the PDP-11. Later on, those systems running TOPS-20 were labeled `DECSYSTEM-20' (the block capitals being the result of a lawsuit brought against DEC by Singer, which once made a computer called `system-10'), but contrary to popular lore there was never a `PDP-20'; the only difference between a 10 and a 20 was the operating system and the color of the paint. Most (but not all) machines sold to run TOPS-10 were painted `Basil Blue', whereas most TOPS-20 machines were painted `Chinese Red' (often mistakenly called orange).

***-Peek**

n. ,vt. (and poke) The commands in most microcomputer BASICs for directly accessing memory contents at an absolute address; often extended to mean the corresponding constructs in any HLL (peek reads memory, poke modifies it). Much hacking on small, non-MMU micros consists of `peek'ing around memory, more or less at random, to find the location where the system keeps interesting stuff. Long (and variably accurate) lists of such addresses for various computers circulate (see interrupt list, the). The results of `poke's at these addresses may be highly useful, mildly amusing, useless but neat, or (most likely) total lossage (see killer poke). Since a real operating system provides useful, higher-level services for the tasks commonly performed with peeks and pokes on micros, and real languages tend not to encourage low-level memory groveling, a question like “How do I do a peek in C?” is diagnostic of the newbie. (Of course, OS kernels often have to do exactly this; a real C hacker would unhesitatingly, if unportably, assign an absolute address to a pointer variable and indirect through it.)

Peer-Entity Authentication

The corroboration that a peer entity in an association is the one claimed. (SS;)

#-Peer-To-Peer Security

pertaining to the action of communicating parties seeking to verify each others' identities (Source -: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

***-Pencil And Paper**

n. An archaic information storage and transmission device that works by depositing smears of graphite on bleached wood pulp. More recent developments in paper-based technology include improved `write-once' update devices which use tiny rolling heads similar to mouse balls to deposit colored pigment. All these devices require an operator skilled at so-called

`handwriting' technique. These technologies are ubiquitous outside hackerdom, but nearly forgotten inside it. Most hackers had terrible handwriting to begin with, and years of keyboarding tend to have encouraged it to degrade further. Perhaps for this reason, hackers deprecate pencil-and-paper technology and often resist using it in any but the most trivial contexts.

Penetration

1. The successful unauthorized access to an automated system. (*AR* 380-380;; *FIPS PUB* 39;)
2. The successful act of bypassing the security mechanisms of a system. (*NCSC-WA*-001-85;)
3. The successful and repeatable extraction and identification of recognizable information from a protected data file or data set without any attendant arrests. (*OPNAVINST* 5239. 1; DODD 5200. 28M;)
4. The act of overcoming one or more measures designed to protect an organization's operation, activity, facilities, information, or personnel. *The recruitment of agents within or the infiltration of agents or introduction of technical monitoring devices into an organization or group or physical facility for the purpose of acquiring information or influencing its activities. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)
5. The successful act of bypassing the security mechanisms of a cryptographic or automated information system. (NSA, *National INFOSEC Glossary*, 10/88)

Penetration Paths

Penetration Profile

A delineation of activities required to effect a penetration. (*FIPS PUB* 39;; *AR* 380-380;)

Penetration Signature

1. The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress. (*AR* 380-380;; *FIPS PUB* 39;)
2. The characteristics or identifying marks that may be produced of an unsuccessful or successful penetration. (*NCSC-WA*-001-85;)

Penetration Study

A study to determine the feasibility and methods for defeating controls of an Automated Information System. (*NCSC-WA*-001-85;)

Penetration Testing

1. The use of teams consisting of data processing, communications, and security specialists to attempt to penetrate a system for the purpose of identifying any security weaknesses. (*AR* 380-380;)
2. The use of special programmer analyst teams to attempt to penetrate a system for the purpose of identifying any security weaknesses. (*FIPS PUB* 39;)
3. The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users. (*NCSC-WA*-001-85;; CSC-STD-001-83;)
4. The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users. (*NCSC-TG*-004-88)

*-Peon

n. A person with no special (root or wheel) privileges on a computer system. “I can't create an account on *foovax* for you; I'm only a peon there. ”

Per-Call Key

Unique traffic encryption key generated automatically by certain secure telecommunications systems to secure single voice or data transmissions. See Cooperative Key Generation.

Perceived Threat

Estimate of possible present and future resource allocation and capabilities of an adversary to gain information Synonymous with Potential Threat.

*-Percent-S

/per-sent' es'/ n. [From the code in C's `printf(3)' library function used to insert an arbitrary string argument] An unspecified person or object. “I was just talking to some percent-s in administration. ” Compare random.

*-Perf

/perf/ n. Syn. chad (sense 1). The term `perfory' /per'f*-ree/ is also heard. The term perf may also refer to the perforations themselves, rather than the chad they produce when torn.

*-Perfect Programmer Syndrome

n. Arrogance; the egotistical conviction that one is above normal human error. Most frequently found among programmers of some native ability but relatively little experience (especially new graduates; their perceptions may be distorted by a history of excellent performance at solving toy problems). “Of course my program is correct, there is no need to test

it. ” “Yes, I can see there may be a problem here, but *I'll* never type `rm -r /' while in root mode. ”

Performance Parameter

Peril

1. A generic form of misadventure to which certain classes of entities of the internal environment may be prone; for example, destruction, theft. (ET;)
2. A number of different problems that assets of various types might experience. for computer systems, these are frequently taken to be theft, destruction, disclosures, contamina-, tion, and interruption. (RM;)
3. A type of impact (such as theft, destruction and contamination). (MK;)

Periods Processing

1. Intervals of time when security environments are temporarily established for processing information. For example, an automated system could process Top Secret in the dedicated security mode during one period, both Confidential and Secret in the controlled security mode in a second period, and only unclassified material in a third period. The system is purged of all information and brought to a secure state when transitioning from one period to the next. There will be users during the new period who do not have clearance and need-to-know for information processed during the previous period. (*AFR* 205-16;)
2. The processing of various levels of classified information at distinctly different times with the system being properly cleared or declassified between periods of processing. (*AR* 380-380;)
3. The processing of various levels of sensitive information at distinctly different times. The Automated Information System must be purged of all information before transitioning from one period to the next whenever there will be new users who do not have clearances and the need-to-know for data processed during the previous period. (*NCSC-WA*-001-85;)
4. Processing data of a given classification level during a period of time and data of a different classification during a different period of time. Also applies to changing security mode of operation. (*OPNAVINST* 5239. 1A;)

Peripheral Device

See peripheral equipment.

Peripheral Devices

Input/output devices and auxiliary storage units of a computer system.

Peripheral Equipment

In a data processing system, any equipment, distinct from the central processing unit, that may provide the system with additional capabilities. Note: Such equipment is often off-line until needed for a specific purpose and may, in some cases, be shared among several users. See also keyboard, modem, terminal.

*-Perl

/perl/ n. [Practical Extraction and Report Language, a. k. a Pathologically Eclectic Rubbish Lister] An interpreted language developed by Larry Wall <lwall@jpl. nasa. gov>, author of `patch(1)' and `rn(1)') and distributed over Usenet. Superficially resembles awk, but is much hairier, including many facilities reminiscent of `sed(1)' and shell and a comprehensive UNIX system-call interface. UNIX sysadmins, who are almost always incorrigible hackers, increasingly consider it one of the languages of choice. Perl has been described, in a parody of a famous remark about `lex(1)', as the “Swiss-Army chainsaw” of UNIX programming.

Permissions

A description of the type of authorized interactions a subject can have with an object. Permissions include: read, write, execute, add, modify, and delete. (*AFR* 205-16;; *NCSC-WA*-001-85;) See Read Down, Write Down, and Write Up.

Permuter

Device used in a crypto-equipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits.

Perpetrator

1. The entity from the external environment that is taken to be the cause of a risk. An agent or Nature. Note that an agent may also be in the internal environment. (ET;)
2. An entity (individual or class) in the external environment that performs an attack. (MK;)

*-Person Of No Account

n. [University of California at Santa Cruz] Used when referring to a person with no network address, frequently to forestall confusion. Most often as part of an introduction “This is Bill, a person of no account, but he used to be bill@random. com”. Compare return from the dead.

Personal Data

1. Any unique data used in the system of records to locate or retrieve an individual's record. Information subject to the Privacy Act of 1974. (*AFR* 205-16;)
2. Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbols, or other identifying particular assigned to the indi-

vidual, such as a finger or voice print or a photograph. (*OPNAVINST* 5239. 1A;)

Personal Identification Number

Personal Identifier

A data item associated with a specific individual which represents the identity of that individual and may be known by other individuals. (*FIPS PUB* 112;)

Personal Password

A password that is known by only one person and is used to authenticate that person's identity. (*FIPS PUB* 112;)

Personnel

An asset category consisting of all people in the organization. (RM;)

Personnel Screening

A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual. (Guidelines on screening non-federal employees are available from the Off ice of ADP Management.) (*DOE 1360. 2A*)

Personnel Security

1. The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances. (DOE 5636. 2A;)
2. The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)
3. The procedures established to ensure that each individual has a background which indicated a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access. (*OPNAVINST* 5239. 1A;)
4. The means or procedures designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy. *The means or procedures such as selective investigations, record checks, personal interviews, and supervisory controls designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89) *The procedures established to ensure that all personnel who have access to sensitive or classified information have the required authority as well as appropriate clearances. (NSA, *National INFOSEC Glossary*, 10/88)

#-Personnel Security Policies And Guidance

This KSA has no definition.

PES

See Positive Enable System.

*-Pessimal

/pes'im-l/ adj. [Latin-based antonym for `optimal'] Maximally bad. “This is a pessimal situation. ” Also `pessimize' vt. To make as bad as possible. These words are the obvious Latin-based antonyms for `optimal' and `optimize', but for some reason they do not appear in most English dictionaries, although `pessimize' is listed in the OED.

*-Pessimizing Compiler

/pes'*-mi:z`ing k*m-pi:l'r/ n. A compiler that produces object [antonym of `optimizing compiler'] code that is worse than the straightforward or obvious hand translation. The implication is that the compiler is actually trying to optimize the program, but through excessive cleverness is doing the opposite. A few pessimizing compilers have been written on purpose, however, as pranks or burlesques.

*-Peta

/pe't*/ pref [SI] See quantifiers.

*-PETSCII

/pet'skee/ n. [abbreviation of PET ASCII] The variation (many would say perversion) of the ASCII character set used by the Commodore Business Machines PET series of personal computers and the later Commodore C64, C16, and C128 machines. The PETSCII set used left-arrow and up-arrow (as in old-style ASCII) instead of underscore and caret, placed the unshifted alphabet at positions 65--90, put the shifted alphabet at positions 193--218, and added graphics characters.

*-Phage

n. A program that modifies other programs or databases in unauthorized ways; esp. one that propagates a virus or Trojan horse. See also worm, mockingbird. The analogy, of course, is with phage viruses in biology.

*-Phase

1. n. The offset of one's waking-sleeping schedule with respect to the standard 24-hour cycle; a useful concept among people who often work at night and/or according to no fixed schedule. It is not un-

common to change one's phase by as much as 6 hours per day on a regular basis. “What's your phase?” “I've been getting in about 8 P. M. lately, but I'm going to wrap around to the day schedule by Friday. ” A person who is roughly 12 hours out of phase is sometimes said to be in `night mode'. (The term `day mode' is also (but less frequently) used, meaning you're working 9 to 5 (or, more likely, 10 to 6).) The act of altering one's cycle is called `changing phase'; `phase shifting' has also been recently reported from Caltech.

2. `change phase the hard way' To stay awake for a very long time in order to get into a different phase.
3. `change phase the easy way' To stay asleep, etc. However, some claim that either staying awake longer or sleeping longer is easy, and that it is *shortening* your day or night that is really hard (see wrap around). The `jet lag' that afflicts travelers who cross many time-zone boundaries may be attributed to two distinct causes the strain of travel per se, and the strain of changing phase. Hackers who suddenly find that they must change phase drastically in a short period of time, particularly the hard way, experience something very like jet lag without traveling.

*-Phase Of The Moon

n. Used humorously as a random parameter on which something is said to depend. Sometimes implies unreliability of whatever is dependent, or that reliability seems to be dependent on conditions nobody has been able to determine. “This feature depends on having the channel open in mumble mode, having the foo switch set, and on the phase of the moon. ” See also heisenbug. True story Once upon a time there was a bug that really did depend on the phase of the moon. There was a little subroutine that had traditionally been used in various programs at MIT to calculate an approximation to the moon's true phase. GLS incorporated this routine into a LISP program that, when it wrote out a file, would print a timestamp line almost 80 characters long. Very occasionally the first line of the message would be too long and would overflow onto the next line, and when the file was later read back in the program would barf. The length of the first line depended on both the precise date and time and the length of the phase specification when the timestamp was printed, and so the bug literally depended on the phase of the moon! The first paper edition of the Jargon File (Steele-1983) included an example of one of the timestamp lines that exhibited this bug, but the typesetter `corrected' it. This has since been described as the phase-of-the-moon-bug bug.

Phase-Locked Loop

*-Phase-Wrapping

n. [MIT] Syn. wrap around, sense 2.

Phonetic Alphabet

A list of standard words used to identify letters in a message transmitted by radio or telephone. The following are the authorized words, listed in order, for each letter in the alphabet: Alpha, Bravo, Charlie, Delta, Echo, Foxtrot, Golf, Hotel, India, Juliet, Kilo, Lima, Mike, November, Oscar, Papa, Quebec, Romeo, Sierra, Tango, Uniform, Victor, Whiskey, X-ray, Yankee, Zulu. (JCS1-DoD) See also alphabet.

Photosensitive Recording

Facsimile recording by the exposure of a photosensitive surface to a signal-controlled light beam or spot. (~) See also dark current, facsimile, recording.

Phracker

Individual who combines phone “PHReaking” with computer “hACKing”. (BBD;)

Phreak

Individual fascinated by the telephone system (a PHone fREAK). Commonly, an individual who uses his knowledge of the telephone system to make calls at the expense of another. (BBD;)

*-Phreaker

n. One who engages in phreaking.

*-Phreaking

/freek'ing/ n. [from `phone phreak']

1. The art and science of cracking the phone network (so as, forexample, to make free long-distance calls).
2. By extension, security-cracking in any other context (especially, but not exclusively, on communications networks) (see cracking). At one time phreaking was a semi-respectable activity among hackers; there was a gentleman's agreement that phreaking as an intellectual game and a form of exploration was OK, but serious theft of services was taboo. There was significant crossover between the hacker community and the hard-core phone phreaks who ran semi-underground networks of their own through such media as the legendary “TAP Newsletter”. This ethos began to break down in the mid-1980s as wider dissemination of the techniques put them in the hands of less responsible phreaks. Around the same time, changes in the phone network made old-style technical ingenuity less effective as a way of hacking it, so phreaking came to depend more on overtly criminal acts such as stealing phone-card numbers. The crimes and punishments of gangs like the `414 group' turned that game very ugly. A few old-time hackers still phreak casually just to keep their hand in, but most these days have hardly even heard of `blue boxes' or any of the other paraphernalia of the great phreaks of yore.

Physical Compromise

The compromise of information through loss, theft, capture, recovery by salvage, defection of individuals, unauthorized viewing or photography, or by any other physical means. (NACSIM 5203)

Physical Control Space

(PCS) Spherical space surrounding electronic equipment used to process information under sufficient physical control to stop hostile intercept of compromising emanations. It is usually expressed in meters and can be controlled by fences, guards, patrols, walls, and so forth.

Physical Control Space/physically Controlled Space (PCs)

1. The spherical space surrounding electronic equipment used to process information under sufficient physical control to stop intercept of compromising emanations. It is usually expressed in meters and can be controlled by fences, guards, patrols, walls, and so forth. The exact method of securing the PCs may vary depending upon resources available. (*AFR* 205-16; *OPNAVINST* 5239. l A)
2. The space surrounding equipment processing classified information which is under sufficient physical and technical control to preclude a successful hostile intercept attack. (*AR* 380-380)

Physical Layer

See Open Systems Interconnection--Reference Model.

Physical Memory Location Of The Instruction

Physical Seals

Physical Security

1. The use of locks, guards, badges, alarms, and similar measures (alone or in combination) to control access to the classified ADP system and related equipment. b) The measures required for the protection of the structures housing the classified ADP system, related equipment, and their contents from espionage, theft, misuse, abuse, or damage by accident, fire, and environmental hazards. (DOE 5636. 2A;)
   a) The use of locks, guards, badges, and similar administrative measures to control access to the computer and related equipment.
   b) The measures required for the protection of the structures housing the computer, related equipment and their contents from damage by accident, fire, and environmental hazards. (*FIPS PUB* 39;)
2. The application of physical barriers and control procedures as preventative measures or countermeasures against threats to resources and sensitive information. (*NCSC-WA*-001-85;)
3. Physical security is the protection of a material entity (property) from disruption of its safe and secure state and is concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. a) The use of locks, badges, and similar measures to control access to the central computer facility. b) The measures required for the protection of the structures housing the central computer facility from damage by accident, fire, environmental hazards, loss of utilities, and unauthorized access. (*OPNAVINST* 5239. 1A;)

   The measures used to provide physical protection of resources against deliberate and accidental threats. (SS;)

*-Pico

pref. [SI a quantifier meaning * 10^-12] Smaller than nano-; used in the same rather loose connotative way as nano- and micro-. This usage is not yet common in the way nano- and micro- are, but should be instantly recognizable to any hacker. See also quantifiers, micro-.

*-Pig, Run Like A

v. To run very slowly on given hardware, said of software. Distinct from hog.

Piggy Back

The gaining of unauthorized access to a system via another user's legitimate connection. (*NCSC-WA*-001-85;)

Piggy Back Entry

Unauthorized access that is gained to an ADP system through another user's legitimate connection. (*FIPS PUB* 39;; *AR* 380-380;)

Piggyback

1. Method of gaining unauthorized access to a system via another user's legitimate connection.
2. See BETWEEN-THE-LINES ENTRY and PIGGY BACK ENTRY.

*-Pilot Error

n. [Sun from aviation] A user's misconfiguration or misuse of a piece of software, producing apparently buglike results (compare UBD). “Joe Luser reported a bug in sendmail that causes it to generate bogus headers. ” “That's not a bug, that's pilot error. His `sendmail. cf' is hosed. ”

*-Ping

1. [from the submariners' term for a sonar pulse] n. Slang term for a small network message (ICMP ECHO) sent by a computer to check for the presence and alertness of another. The UNIX command `ping' can be used to do this manually (note that `ping''s author denies the widespread folk etymology that the name was ever intended as acronym `Packet INternet Groper'). Occasionally used as a phone greeting. See ACK, also ENQ.
2. vt. To verify the presence of.
3. vt. To get the attention of.
4. vt. To send a message to all members of a mailing list requesting an ACK (in order to verify that everybody's addresses are reachable). “We haven't heard much of anything from Geoff, but he did respond with an ACK both times I pinged jargon-friends. ”
5. n. A quantum packet of happiness. People who are very happy tend to exude pings; furthermore, one can intentionally create pings and aim them at a needy party (e. g. , a depressed person). This sense of ping may appear as an exclamation; “Ping!” (I'm happy; I am emitting a quantum of happiness; I have been struck by a quantum of happiness). The form “pingfulness”, which is used to describe people who exude pings, also occurs. (In the standard abuse of language, “pingfulness” can also be used as an exclamation, in which case it's a much stronger exclamation than just “ping”!). Oppose blargh. The funniest use of `ping' to date was described in January 1991 by Steve Hayman on the Usenet group comp. sys. next. He was trying to isolate a faulty cable segment on a TCP/IP Ethernet hooked up to a NeXT machine, and got tired of having to run back to his console after each cabling tweak to see if the ping packets were getting through. So he used the sound-recording feature on the NeXT, then wrote a script that repeatedly invoked `ping', listened for an echo, and played back the recording on each returned packet. Result? A program that caused the machine to repeat, over and over, “Ping . ping . ping . ” as long as the network was up. He turned the volume to maximum, ferreted through the building with one ear cocked, and found a faulty tee connector in no time.

*-Pink-Shirt Book

“The Peter Norton Programmer's Guide to the IBM PC”. The original cover featured a picture of Peter Norton with a silly smirk on his face, wearing a pink shirt. Perhaps in recognition of this usage, the current edition has a different picture of Norton wearing a pink shirt. See also book titles.

*-PIP

/pip/ vt. ,obs. [Peripheral Interchange Program] To copy; from the program PIP on CP/M, RSX-11, RSTS/E, TOPS-10, and OS/8 (derived from a utility on the PDP-6) that was used for file copying (and in OS/8 and RT-11 for just about every other file operation you might want to do). It is said that when the program was originated, during the development of the PDP-6 in 1963, it was called ATLATL (`Anything, Lord, to Anything, Lord'; this played on the Nahuatl word `atlatl' for a spear-thrower, with connotations of utility and primitivity that were no doubt quite intentional). See also BLT, dd, cat.

Piracy

*-Pistol

n. [IBM] A tool that makes it all too easy for you to shoot yourself in the foot. “UNIX `rm *' makes such a nice pistol!”

*-Pixel Sort

n. [Commodore users] Any compression routine which irretrievably loses valuable data in the process of crunching it. Disparagingly used for `lossy' methods such as JPEG. The theory, of course, is that these methods are only used on photographic images in which minor loss-of-data is not visible to the human eye. The term `pixel sort' implies distrust of this theory. Compare bogo-sort.

*-Pizza Box

n. [Sun] The largish thin box housing the electronics in (especially Sun) desktop workstations, so named because of its size and shape and the dimpled pattern that looks like air holes. Two meg single-platter removable disk packs used to be called pizzas, and the huge drive they were stuck into was referred to as a pizza oven. It's an index of progress that in the old days just the disk was pizza-sized, while now the entire computer is.

*-Pizza, ANSI Standard

/an'see stan'd*rd peet'z*/ [CMU] Pepperoni and mushroom pizza. Coined allegedly because most pizzas ordered by CMU hackers during some period leading up to mid-1990 were of that flavor. See also rotary debugger; compare tea, ISO standard cup of.

PL/1

A programming language that is designed for use in a wide range of commercial and scientific computer applications. (FP)

*-Plaid Screen

n. [XEROX PARC] A `special effect' that occurs when certain kinds of memory smashes overwrite the control blocks or image memory of a bit-mapped display. The term “salt and pepper” may refer to a different pattern of similar origin. Though the term as coined at PARC refers to the result of an error, some

of the X demos induce plaid-screen effects deliberately as a display hack.

Plain Text

1. Unencrypted information. ;
2. Intelligible text or signals that have meaning and which can be read or acted upon without the application of any decryption. (*FIPS PUB* 39;; *AR* 380-380;)

See clear text. See also cipher text, cryptology.

Plain Text/plain-Text

Intelligible text or signals-that have meaning and which can be read or acted upon without the application of any decryption. (*FIPS PUB* 39; *AR* 380-380; NACSEM 5103; NACSEM 5201; NACSIM 5203)

*-Plain-ASCII

/playn-as'kee/ Syn. flat-ASCII.

Plaintext

Intelligence-bearing signals which can be interpreted without recourse to any decryption or deciphering process. (NACSEM 5106)

*-Plan File

n. [UNIX] On systems that support finger, the `. plan' file in a user's home directory is displayed when the user is fingered. This feature was originally intended to be used to keep potential fingerers apprised of one's location and near-future plans, but has been turned almost universally to humorous and self-expressive purposes (like a sig block). See also Hacking X for Y. A recent innovation in plan files has been the introduction of “scrolling plan files” which are one-dimensional animations made using only the printable ASCII character set, carriage return and line feed, avoiding terminal specific escape sequences, since the finger command will (for security reasons; see letterbomb) not pass the escape character. Scrolling . plan files have become art forms in miniature, and some sites have started competitions to find who can create the longest running, funniest, and most original animations. Various animation characters include Centipede mmmmme Lorry/Truck oo-oP Andalusian Video Snail _@/ and a compiler (ASP) is available on Usenet for producing them. See also twirling baton.

Planning

#-Platform-Specific Security

This KSA has no definition.

*-Platinum-Iridium

adj. Standard, against which all others of the same category are measured. Usage silly. The notion is that one of whatever it is has actually been cast in platinum-iridium alloy and placed in the vault beside the Standard Kilogram at the International Bureau of Weights and Measures near Paris. (From ~9 to 1960, the meter was defined to be the distance between two scratches in a platinum-iridium bar kept in that same vault --- this replaced an earlier definition as 10^(-7) times the distance between the North Pole and the Equator along a meridian through Paris; unfortunately, this had been based on an inexact value of the circumference of the Earth. From 1960 to 1984 it was defined to be 1650763. 73 wavelengths of the orange-red line of krypton-86 propagating in a vacuum. It is now defined as the length of the path traveled by light in a vacuum in the time interval of 1/299,792,458 of a second. The kilogram is now the only unit of measure officially defined in terms of a unique artifact.) “This garbage-collection algorithm has been tested against the platinum-iridium cons cell in Paris. ” Compare golden.

*-Playpen

n. [IBM] A room where programmers work. Compare salt mines.

*-Playte

/playt/ 16 bits, by analogy with nybble and byte. Usage rare and extremely silly. See also dynner and crumb. General discussion of such terms is under nybble.

*-Plingnet

/pling'net/ n. Syn. UUCPNET. Also see Commonwealth Hackish, which uses `pling' for bang (as in bang path).

*-Plokta

/plok't*/ v. [acronym Press Lots Of Keys To Abort] To press random keys in an attempt to get some response from the system. One might plokta when the abort procedure for a program is not known, or when trying to figure out if the system is just sluggish or really hung. Plokta can also be used while trying to figure out any unknown key sequence for a particular operation. Someone going into `plokta mode' usually places both hands flat on the keyboard and mashes them down, hoping for some useful response. A slightly more directed form of plokta can often be seen in mail messages or Usenet articles from new users -- the text might end with ^X^C q quit q ^C end x exit ZZ ^D ? help as the user vainly tries to find the right exit sequence, with the incorrect tries piling up at the end of the message.

*-Plonk

excl. [Usenet possibly influenced by British slang `plonk' for cheap booze, or `plonker' for someone behaving stupidly (latter is lit. equivalent to Yiddish `schmuck')] The sound a newbie makes as he falls to the bottom of a kill file. While it originated in the newsgroup talk. bizarre, this term (usually written

"*plonk*") now (1994) widespread on Usenet as a term of public ridicule.

Plotter

An output unit that presents data in the form of a two-dimensional graphic representation. (FP) (ISO)

*-Plugh

/ploogh/ v. [from the ADVENT game] See xyzzy.

*-Plumbing

n. [UNIX] Term used for shell code, so called because of the prevalence of `pipelines' that feed the output of one program to the input of another. Under UNIX, user utilities can often be implemented or at least prototyped by a suitable collection of pipelines and temp-file grinding encapsulated in a shell script; this is much less effort than writing C every time, and the capability is considered one of UNIX's major winning features. A few other OSs such as IBM's VM/CMS support similar facilities. Esp. used in the construction `hairy plumbing' (see hairy). "You can kluge together a basic spell-checker out of `sort(1)', `comm(1)', and `tr(1)' with a little plumbing. " See also tee.

*-Pnambic

/p*-nam'bik/ [Acronym from the scene in the film version of "The Wizard of Oz" in which the true nature of the wizard is first discovered "Pay no attention to the man behind the curtain. "]

1. A stage of development of a process or function that, owing to incomplete implementation or to the complexity of the system, requires human interaction to simulate or replace some or all of the actions, inputs, or outputs of the process or function.
2. Of or pertaining to a process or function whose apparent operations are wholly or partially falsified.
3. Requiring prestidigitization. The ultimate pnambic product was "Dan Bricklin's Demo", a program which supported flashy user-interface design prototyping. There is a related maxim among hackers

"Any sufficiently advanced technology is indistinguishable from a rigged demo. " See magic, sense 1, for illumination of this point.

*-Pod

n. [allegedly from abbreviation POD for `Prince Of Darkness'] A Diablo 630 (or, latterly, any letter-quality impact printer). From the DEC-10 PODTYPE program used to feed formatted text to it. Not to be confused with P. O. D.

Point Of Presence

*-Point-And-Drool Interface

n. Parody of the techspeak term `point-and-shoot interface', describing a windows, icons, and mouse-based interface such as is found on the Macintosh. The implication, of course, is that such an interface is only suitable for idiots. See for the rest of us, WIMP environment, Macintrash, drool-proof paper. Also `point-and-grunt interface'.

*-Pointer Bug

n. Synonym for aliasing bug used esp. among microcomputer hackers.

Poisson Function

A probability distribution assumed to approximate the distribution of event severity. (RM;)

*-Poke

n. ,vt. See peek.

Policy

Administrative decisions which determine how certain security-related concepts will be interpreted as system requirements. All such policy decisions must eventually be interpreted formally and implemented. (MTR-8201;)

#-Policy Development

This KSA has no definition.

#-Policy Enforcement

This KSA has no definition.

*-Poll

1. v. ,n. [techspeak] The action of checking the status of an input line, sensor, or memory location to see if a particular external event has been registered.
2. To repeatedly call or check with someone "I keep polling him, but he's not answering his phone; he must be swapped out. "
3. To ask. "Lunch? I poll for a takeout order daily. "

*-Polygon Pusher

n. A chip designer who spends most of his or her time at the physical layout level (which requires drawing *lots* of multi-colored polygons). Also `rectangle slinger'.

Polygraphic Processing

Processing where the data (bits) are parallel processed, and the characters are processed more than one at a time.

*-Pop

/pop/ [from the operation that removes the top of a stack, and the fact that procedure return addresses are usually saved on the stack] (also capitalized `POP')

1. vt. To remove something from a stack or pdl. If a person says he/she has popped something from his stack, that means he/she has finally finished work-

ing on it and can now remove it from the list of things hanging overhead.

2. When a discussion gets to a level of detail so deep that the main point of the discussion is being lost, someone will shout “Pop!”, meaning “Get back up to a higher level!” The shout is frequently accompanied by an upthrust arm with a finger pointing to the ceiling.

*-POPJ

/pop'J/ n. ,v. [from a PDP-10 return-from-subroutine instruction] To return from a digression. By verb doubling, “Popj, popj” means roughly “Now let's see, where were we?” See RTI.

*-Poser

n. A wannabee; not hacker slang, but used among crackers, phreaks and warez d00dz. Not as negative as lamer por leech. Probably derives from a similar usage among punk-rockers and metalheads, putting down those who “talk the talk but don't walk the walk”.

#-Position Sensitivity

This KSA has no definition.

Positive Control

Generic term referring to a sealed material authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material or devices.

Positive Control Material

Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or neuclear command and control documents, material or devices.

*-Post

v. To send a message to a mailing list or newsgroup. Distinguished in context from `mail'; one might ask, for example “Are you going to post the patch or mail it to known users?” (2) n. Power On Self Test

Post-Selection

*-Postcardware

n. A kind of shareware that borders on freeware, in that the author requests only that satisfied users send a postcard of their home town or something. (This practice, silly as it might seem, serves to remind users that they are otherwise getting something for nothing, and may also be psychologically related to real estate `sales' in which $1 changes hands just to keep the transaction from being a gift.)

*-Posting

n. Noun corresp. to v. post (but note that post can be nouned). Distinguished from a `letter' or ordinary email message by the fact that it is broadcast rather than point-to-point. It is not clear whether messages sent to a small mailing list are postings or email; perhaps the best dividing line is that if you don't know the names of all the potential recipients, it is a posting.

*-Postmaster

n. The email contact and maintenance person at a site connected to the Internet or UUCPNET. Often, but not always, the same as the admin. The Internet standard for electronic mail (RFC-822) requires each machine to have a `postmaster' address; usually it is aliased to this person.

*-PostScript

n. A Page Description Language (PDL), based on work originally done by John Gaffney at Evans and Sutherland in 1976, evolving through `JaM' (`John and Martin', Martin Newell) at XEROX PARC, and finally implemented in its current form by John Warnock et al. after he and Chuck Geschke founded Adobe Systems Incorporated in 1982. PostScript gets its leverage by using a full programming language, rather than a series of low-level escape sequences, to describe an image to be printed on a laser printer or other output device (in this it parallels EMACS, which exploited a similar insight about editing tasks). It is also noteworthy for implementing on-the fly rasterization, from Bezier curve descriptions, of high-quality fonts at low (e. g. 300 dpi) resolution (it was formerly believed that hand-tuned bitmap fonts were required for this task). Hackers consider PostScript to be among the most elegant hacks of all time, and the combination of technical merits and widespread availability has made PostScript the language of choice for graphical output.

Potential Threat

See Perceived Threat.

*-Pound On

vt. Syn. bang on.

#-Power Controls (e. G. , UPS, Emergency Power)

This KSA has no definition.

*-Power Cycle

vt. (also, `cycle power' or just `cycle') To power off a machine and then power it on immediately, with the intention of clearing some kind of hung or gronked state. Syn. 120 reset; see also Big Red Switch. Compare Vulcan nerve pinch, bounce (sense 4), and boot, and see the “AI Koans” (in Appendix A) about Tom Knight and the novice.

*-Power Hit

n. A spike or drop-out in the electricity supplying your machine; a power glitch. These can cause

crashes and even permanent damage to your machine(s).

Power Line Conduction

Plaintext emanations which are propagated or transmitted over power lines. (NACSEM 5106)

Power Line Modulation

Phase or amplitude variations of the input power current which may be related to the information being processed on a power line. (NACSEM 5106)

Powerline Conduction

See Line Conduction.

*-PPN

/P-P-N/, /pip'n/ n. [from `Project-Programmer Number'] A user-ID under TOPS-10 and its various mutant progeny at SAIL, BBN, CompuServe, and elsewhere. Old-time hackers from the PDP-10 era sometimes use this to refer to user IDs on other systems as well.

Practice Dangerous To Security

(PDS) A procedure that has the potential to jeopardize the security of COMSEC material if allowed to continue.

#-Practices

This KSA has no definition.

Pre-Selection

*-Precedence Lossage

/pre's*-dens los'*j/ n. [C programmers] Coding error in an expression due to unexpected grouping of arithmetic or logical operators by the compiler. Used esp. of certain common coding errors in C due to the nonintuitively low precedence levels of `&', `|', `^', `<<', and `>>' (for this reason, experienced C programmers deliberately forget the language's baroque precedence hierarchy and parenthesize defensively). Can always be avoided by suitable use of parentheses. LISP fans enjoy pointing out that this can't happen in *their* favorite language, which eschews precedence entirely, requiring one to use explicit parentheses everywhere. See aliasing bug, memory leak, memory smash, smash the stack, fandango on core.

Precision

Predicated Event

An Event which, to be realized, requires the occurrence of one or more prior Events. The prior Events may or may not be required to occur in sequence or simultaneously. (MK;)

Preferred Products List (PPL)

1. A list of commercially produced equipments which meet TEMPEST and other requirements prescribed by NSA. (*NCSC-WA*-001-85;)
2. List of commercially-produced equipments that meet TEMPEST and other requirements prescribed by the National Security Agency (NSA). This list is included in the NSA Information Systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office.

Preferred Products List (PPL)

A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by the National Security Agency. This list is included in the NSA Information Systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office. (*NCSC-TG*-004-88)

Preliminary Technical Report

See (PTR)

*-Prepend

/pree`pend'/ vt. [by analogy with `append'] To prefix. As with `append' (but not `prefix' or `suffix' as a verb), the direct object is always the thing being added and not the original word (or character string, or whatever). “If you prepend a semicolon to the line, the translation routine will pass it through unaltered. ”

Preproduction Model

(P Model) Version of a crypto-equipment that employs standard parts and is in final mechanical and electrical form suitable for complete evaluation of form, design, and performance. NOTE: Preproduction models are often referred to as E-model equipment.

President's Council On Integrity And Efficiency

*-Prestidigitization

/pres`t*-di`j*-ti:-zay'sh*n/ n.

1. The act of putting something into digital notation via sleight of hand.
2. Data entry through legerdemain.

*-Pretty Pictures

n. [scientific computation] The next step up from numbers. Interesting graphical output from a program that may not have any sensible relationship to the system the program is intended to model. Good for showing to management.

*-Prettyprint

/prit'ee-print/ v. (alt. `pretty-print')

1. To generate `pretty' human-readable output from a hairy internal representation; esp. used for the process of grinding (sense 1) program code, and most esp. for LISP code.
2. To format in some particularly slick and nontrivial way.

***-Pretzel Key**
n. [Mac users] See feature key.

#-Preventative Controls
This KSA has no definition.

Prevention
The process of inhibiting agents from performing events " the purpose of some protective mechanisms. (RM;)

Preventive Maintenance
1. The care and servicing by personnel for the purpose of maintaining equipment and facilities in satisfactory operating condition by providing for systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects. (JCS1-DoD)
2. Systematic and/or prescribed maintenance intended to reduce the probability of failure. (JCS1-NATO)
3. Maintenance, including tests, measurements, adjustments, and parts replacement, performed specifically to prevent faults from occurring. (~) See also corrective maintenance, fault, maintenance.

Price

***-Priesthood**
n. ,obs. [TMRC] The select group of system managers responsible for the operation and maintenance of a batch operated computer system. On these computers, a user never had direct access to a computer, but had to submit his/her data and programs to a priest for execution. Results were returned days or even weeks later. See acolyte.

Primary Distribution
The initial targeted distribution of, or access to, technical documents authorized by the controlling *DOD* office. (DODD 5230. 24;)

Primary RED Conductor
Any conductor intended to carry national security information and terminating in RED equipment or in the RED side of crypto-equipment or isolation devices.

Primary Station
In a data communication network, the station responsible for unbalanced control of a data link. Note: The primary station generates commands and interprets responses, and is responsible for initialization of data and control information interchange, organization and control of data flow, retransmission control, and all recovery functions at the link level. See also control station, data communication, link, master station, network, secondary station, slave station, tributary station.

Primary Substation
Equipment that switches or modifies voltage, frequency, or other characteristics of primary power. (~) See also primary power.

***-Prime Time**
n. [from TV programming] Normal high-usage hours on a timesharing system; the day shift. Avoidance of prime time was traditionally given as a major reason for night mode hacking. The rise of the personal workstation has rendered this term, along with timesharing itself, almost obsolete. The hackish tendency to late-night hacking runs has changed not a bit.

Primitive

Principle Of Least Privilege
The granting of the minimum access authorization necessary for the performance of required tasks. (*FIPS PUB* 39;; *AR* 380-380;)

#-Principles Of Control
This KSA has no definition.

Print Suppression
Eliminating the displaying of characters in order to preserve their secrecy; e. g. , not displaying the characters of a password as it is keyed at the input terminal.

Print Suppression/print Suppress
To eliminate the printing of characters in order to preserve their secrecy; for example, the characters of a password as it is keyed at the input terminal. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

***-Printing Discussion**
n. [XEROX PARC] A protracted, low-level, time-consuming, generally pointless discussion of something only peripherally interesting to all.

***-Priority Interrupt**
n. [from the hardware term] Describes any stimulus compelling enough to yank one right out of hack mode. Classically used to describe being dragged away by an SO, but may also refer to more mundane interruptions such as a fire alarm going off in the near vicinity. Also called an NMI (non-maskable interrupt), especially in PC-land.

Priority Message
A category or precedence reserved for messages that require expeditious action by the addressee(s) and/or furnish essential information for the conduct of operations in progress when routine precedence will not suffice. (JCS1-DoD) See also precedence, seizing.

#-Privacy

1. The right of an individual to self-determination as to the degree to which personal information will be shared among other individuals or organizations. This includes the right of individuals and organizations to control the collection, storage, and dissemination of personal or organizational information. (*AR* 380-380;)
   a) The right of an individual to self-determination as to the degree to which the individual is willing to share with others information about himself that may be compromised by unauthorized exchange of such information among other individuals or organizations.
   b) The right of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves. (*FIPS PUB* 39;)
2. The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note: Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security. (SS;)
3. Is the right to be left alone, the right to be free from unwarranted publicity, and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned. It is inherent in the concept of ordered liberty, and prevents governmental interference in intimate personal relationships or activities, freedoms of an individual to make fundamental choices involving himself, his family, and his relationships with others. It also includes the right of an individual (or corporation) to withhold himself and his property from public scrutiny, if he so chooses. (Source Blacks);
4. A security principle that protects individuals from the collection, storage, and dissemination of information about themselves and the possible compromises resulting from unauthorized release of that information. (CSB+RG-92.) See also authenticate, communications.

Privacy Protection

The establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records and to protect both security and confidentiality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained. (*FIPS PUB* 39;)

Privacy System

Commercial encryption system that affords telecommunications limited protection to deter a casual listener, but cannot withstand a technically competent cryptanalytic attack.

Privacy Transformation

Synonymous with ENCRYPTION ALGORITHM

Private Automatic Branch Exchange

(PABX) An automatic PBX. (~) Note: Use of the term “PBX” is more common than “PABX,” regardless of automation.

Private Automatic Exchange

(PAX) See private automatic branch exchange.

Private Branch Exchange

See PBX.

#-Private Branch Exchange Security

This KSA has no definition.

Private Communication

A communication in which the parties thereto, in the absence of their consent to be monitored for COMSEC purposes, have a-reasonable expectation of privacy. (NACSI 4000A)

Private Exchange

A private telecommunication switch that usually includes access to the public switched network. See also PBX, private automatic branch exchange. (FS1037S1. TXT) (PX) A private telecommunication switch that usually includes access to the public switched network. See also PBX, private automatic branch exchange.

#-Private Key Cryptology

An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group.

Private Line

See leased circuit.

#-Private Networks

This KSA has no definition.

Privilege

System environment functions controlled by the operating system and administered by the system manager.

Privilege Levels

Privilege Profile

A computer resident record that indicates the resources that a specific user, process, or computer has been explicitly authorized to access. (WB;)

Privileged Data

Data not subject to usual rules because of confidentiality imposed by law, such as chaplain, legal, and medical files. (*AFR* 205-16)

Privileged Instructions

1. A set of instructions generally executable only when the automated system is operating in the executive state (such as, interrupt handling); special computer instructions designed to control the protection features of an ADP system (such as storage protection features. (*AR* 380-380; *FIPS PUB* 39)
2. A set of instructions (e. g. , interrupt handling or special computer instructions) to control features (such as storage protection features) generally executable only when the automated system is operating in the executive state. (*NCSC-TG*-004-88)

Privileged Process

A process that is afforded (by the kernel) some privileges not afforded normal user processes. A typical privilege is the ability to override the security *-property. Privileged processes are trusted. (MTR-8201;)

#-Privileges (Class, Nodes)

1. Pertaining to a program or user and characterized the type of operation that can be performed. Privileged users or programs can perform operations normally considered to be the domain of the operating system and which can affect the system performance. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992)
2. A right granted to a user, a program, or a process. For example: certain users may have privileges that allow them to access certain files in a system. Only the system administrator may have the privileges necessary to export data from a trusted system. (Source: "*Computer Security Basics*" Deborah Russell and G. T. Gangemi Sr. Pub. O'Reilly and Associates, Inc. , July 1992.)

Privity

A privileged mode of operation wherein all instructions are operative giving complete and unrestricted control of the system. (*AR* 380-380;)

Procedural Security

1. The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide protection for sensitive defense information. (*AR* 380-380)
2. Synonymous with ADMINISTRATIVE SECURITY.
3. See ADMINISTRATIVE SECURITY. (*NCSC-TG*-004-88)

Procedure-Oriented Language

A problem-oriented language that facilitates the expression of a procedure as explicit algorithms; for example, FORTRAN, ALGOL, COBOL, PL/1. (FP)

Procedures

See BACKUP PROCEDURES, HANDSHAKING PROCEDURES, RECOVERY PROCEDURES, and SYSTEM INTEGRITY PROCEDURES.

Process

1. A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space. (*DOD* 5200. 28-STD)
2. The active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. A process consists of a unique address space containing its accessible program code and data, a program location for the currently executing instruction, and periodic access to the processor in order to continue. (MTR-8201)
3. A program in execution. See domain and subject. (*NCSC-TG*-004-88)

Process Computer System

A computer system, with a process interface system, that monitors or controls a technical process. (FP) See also process interface system.

Process Control

Automatic control of a process, in which a computer system is used to regulate the usually continuous operations or processes. (FP) (ISO)

Process Control Equipment

Equipment that measures the variables of a technical process, directs the process according to control signals from the process computer system, and provides appropriate signal transformation, for example, equipment such as actuators, sensors, and transducers. (FP) (ISO) See also process computer system.

Process Control System

A computer system, process control equipment, and possibly a process interface system. The process interface system may be part of a special-purpose computer. (FP) (ISO) See also process interface system.

Process Interface System

A functional unit that adapts process control equipment to the computer system in a process computer system. (FP) (ISO)

Process Isolation

Process Manager

Process Signaling

Processing
See automatic data processing, batch processing, data processing, multiprocessing, remote batch processing.

Processing Unit
A functional unit that consists of one or more processors and their internal storage. (FP) (ISO)

Processor
In a computer, a functional unit that interprets and executes instructions. Note: A processor consists of at least an instruction control unit and an arithmetic unit. (FP) (ISO) See also central processing unit.

Procurement
The process of obtaining personnel, services, supplies, and equipment. (JCS1-DoD)

Procurement Lead Time
The interval in months between the initiation of procurement action and receipt into the supply system of the production model (excludes prototypes) purchased as the result of such actions, and is composed of two elements, production lead time and administrative lead time. (JCS1-DoD)

Product Questionnaire

Production Model
Crypto-equipment in its final mechanical and electrical form of production design made by use of production tools, jigs, fixtures, and methods using standard parts.

#-Professional Interfaces
This KSA has no definition.

Profile
(1) Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an AIS. (2) n. A control file for a program, esp. a text file automatically read from each user's home directory and intended to be easily modified by the user in order to customize the program's behavior. Used to avoid hardcoded choices (see also dot file, rc file). (3) A report on the amounts of time spent in each routine of a program, used to find and tune away the hot spots in it. This sense is often verbed. Some profiling modes report units other than time (such as call counts) and/or report at granularities other than per-routine, but the idea is similar. See graded-index profile, index profile, parabolic profile, power-law index profile.

Profiles
A detailed security description of the physical structure, equipment components, equipment locations and relationships, and general operating environment of the automated system. (*AR* 380-380;)

***-Proglet**
/prog'let/ n. [UK] A short extempore program written to meet an immediate, transient need. Often written in BASIC, rarely more than a dozen lines long, and containing no subroutines. The largest amount of code that can be written off the top of one's head, that does not need any editing, and that runs correctly the first time (this amount varies significantly according to one's skill and the language one is using). Compare toy program, noddy, one-liner wars.

Program
1. A plan or routine for solving a problem on a computer.
2. A sequence of instructions used by a computer to do a particular job or solve a given problem.
3. To design, write, and test programs. (FP) (ISO) See also computer.

Program Origin
See computer program origin.

Programmable
Pertaining to a device that can accept instructions that alter its basic functions. (FP)

Programmable Logic Array
(PLA) An array of gates whose interconnections can be programmed to perform a specific logical function. (FP)

Programmable Read-Only Memory
(PROM) A storage device that, after being written once, becomes a read-only memory. (FP) (ISO) See also read-only memory.

Programmer
1. That part of digital apparatus having the function of controlling the timing and sequencing of operations. (~)
2. A person who prepares sequences of instructions for a computer. (~) See also compile, computer, computer language.

***-Programmer's Cheer**
“Shift to the left! Shift to the right! Pop up, push down! Byte! Byte! Byte!” A joke so old it has hair on it.

***-Programming**
1. n. The art of debugging a blank sheet of paper (or, in these days of on-line editing, the art of debugging an empty file).
2. A pastime similar to banging one's head against a wall, but with fewer opportunities for reward.
3. The most fun you can have with your clothes on (although clothes are not mandatory).

***-Programming Fluid**

1. n. Coffee.
2. Cola.
3. Any caffeinacious stimulant. Many hackers consider these essential for those all-night hacking runs. See wirewater.

Programming Language

An artificial language that is used to generate or to express programs.

Programming System

One or more programming languages and the software necessary for using these languages with particular automatic data processing equipment. (FP)

PROM

See Programmable Read-Only Memory.

Propagation

The directed motion of waves. See also anomalous propagation, backscattering, diffraction, direct ray, forward scatter, ionospheric scatter, line-of-sight propagation, multipath, refraction, scatter, sporadic E propagation, tropospheric scatter.

Propagation Of Risk

Spreading of risk in a network when a system with an accepted level of risk is connected to that network.

***-Propeller Head**

n. Used by hackers, this is syn. with computer geek. Non-hackers sometimes use it to describe all techies. Prob. derives from SF fandom's tradition (originally invented by old-time fan Ray Faraday Nelson) of propeller beanies as fannish insignia (though nobody actually wears them except as a joke).

***-Propeller Key**

n. [Mac users] See feature key.

Property

Property Protection Area

An area set aside for the protection of property as required by this Order. See DOE 5632. 4 for further information. (DOE 5637. 1)

PROPIN

See PROPrietary INformation.

***-Proprietary**

1. adj. In marketroid-speak, superior; implies a product imbued with exclusive magic by the unmatched brilliance of the company's own hardware or software designers.
2. In the language of hackers and users, inferior; implies a product not conforming to open-systems standards, and thus one that puts the customer at the mercy of a vendor able to gouge freely on service and upgrade charges after the initial sale has locked the customer in.

Proprietary Data

Data that is created, used, and marketed by individuals or organizations having exclusive legal rights (NSA, *National INFOSEC Glossary*, 10/88) (*AFR* 205-16;)

Proprietary Information

Material and information relating to or associated with a company's products, business or activities, including but not limited to: financial information; data or statements; trade secrets; product research and developement; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked as proprietary information, trade secrets or company confidential information.

NOTE: Trade secrets constitute the whole or any portion or phase of any technical information, design process, procedure, formula or improvement that is not generally available to the public, that a company considers company confidential and that could give or gives an advantage over competitors who do not know or use the trade secret.

PROSECUTION

Protect As Restricted Data

(PARD) A handling method for computer-generated numerical data, or related information, which is not readily recognized as classified or unclassified because of the high volume of output and low density of potentially classified data. The above information is designated as PARD because it has not had a sensitivity (classification) review and must be protected under a different set of security rules. (DOE 5637. 1; DOE 5635. lA)

Protected

Telecommunications deriving their communications protection through use of type 2 products or data encryption standard equipment.

Protected Communications

Telecommunications deriving their protection through use of type 2 products or data encryption standard equipment. See Secure Communications.

#-Protected Distributed System

Wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the uninterrupted transmission of classified information. (Source: NSTISSI 4009).

Protected Distribution System (PDS)

1. An approved telecommunications systems to which electromagnetic and physical safeguards have been applied to permit safe electric transmission of unencrypted sensitive information. (*AR* 380-380)
2. A telecommunications system to which acoustical, electrical, electromagnetic and physical safeguards have been applied to permit its use for secure electrical or optical transmission of unencrypted classified information or sensitive unclassified information. (DOE 5637. 1; JCS PUB 6-03. 7)
3. An approved wire line and/or fiber optics system to which adequate acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit its use for the transmission of unencrypted classified information. The associated facilities include all equipment and wire lines so safeguarded. Major components are wire lines, and/or fiber optics, subscriber sets, and terminal equipment. Also known as an "approved circuit. " The major components are defined as follows: a. Distribution System. --The metallic wirepaths or fiber optic transmission paths providing interconnection between components of the protected system. b. Subscriber Sets and End Terminal Equipments. --The complete assembly of equipment, exclusive of interconnecting wire lines, located on the end-user's or customer's premises. This includes such items as telephones, teletypewriters, facsimile data sets, input-output devices, switchboards, patchboards, and consoles. (NACSIM 5203)
4. A wireline or fiber-optics system which includes adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information. NOTE: A complete PDS includes the subscriber and terminal equipment, as well as the interconnecting lines. (NCSC-9)
5. A telecommunications system to which electromagnetic and physical safeguards have been applied to permit secure transmission of unencrypted classified information, and which has been approved by the department or agency. The associated facilities include all equipment and lines so safeguarded. Major components are lines (wire or fiber optic), subscriber sets, and terminal equipment. Also known as approved circuit. (NACSIM 5203)

Protected Information

Includes sensitive, critical, and/or classified information.

#-Protected Services

This KSA has no definition.

Protected Wireline Distribution System

1. A telecommunications system which has been approved by a legally designated authority and to which electromagnetic and physical safeguards have been applied to permit safe electrical transmission of unencrypted sensitive information. Synonymous with approved circuit. (*FIPS PUB* 39)
2. See PROTECTED DISTRIBUTION SYSTEM.

Protection

1. The act of applying safeguards in order to reduce the amount of impact expected from risks. (ET;)
2. A hardware mechanism that enforces limitations on access to storage by processes. See DATA-DEPENDENT PROTECTION, FETCH PROTECTION, FILE PROTECTION, LOCK-AND-KEY PROTECTION SYSTEM, and PRIVACY PROTECTION.

Protection Bits

Protection Critical

Portion of the Trusted Computing Base (TCB) whose normal function is to deal with the control of access between subjects and objects, and whose correct operation is essential to the protection of data in the system.

Protection Equipment

Type 2 product or data encryption standard equipment that the National Security Agency has endorsed to meet applicable standards for the protection of telecommunications or automated information systems containing national security information.

#-Protection From Malicious Code

This KSA has no definition.

Protection Index

A measure of perceived risk determined from the combination of the clearance level of users and the classification of the data on the classified ADP system. The determination of this index is described on page 111-14, paragraph 5. (DOE 5637. 1)

Protection Mechanisms

See Security Features.

Protection Philosophy

An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination (appropriate to the evaluation class) of formal and informal techniques is used to show that the mechanisms are adequate to enforce the security policy. (CSC-STD-001-83;; *NCSC-WA*-001-85;)

Protection Ring

1. One of a hierarchy of privileged modes of an ADP system that gives certain access rights to user programs and processes authorized to operate in a given mode. (*FIPS PUB* 39; *AR* 380-380)
2. one of hierarchy of privileged modes of a system that gives certain access rights to user programs and processes authorized to operate in a given mode. (*NCSC-TG*-004-88)

Protection-Critical Portions Of The TCB

Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. Their correct operation is essential to the protection of the data on the system.

Protection-Critical Portions Of Trusted Computing Base

1. Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. (*DOD* 5200. 28-STD)
2. Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. Their correct operation is essential to the protection of the data on the system. (*NCSC-TG*-004-88)

Protective

Any penetration of information system technology/package security protective technology or incident packaging, such as a crack, cut, or tear.

Protective Features

Protective Measures

Physical, administrative, personnel, and technical security measures which, when applied separately or in combination, are designed to reduce the probability of harm, loss or damage to, or compromise of an unclassified computer system or sensitive and/or mission-essential information. (*DOE 1360. 2A*)

Protective Mechanism

A physical or procedural device used to reduce exposures (may involve the prevention of, detection of, or recovery from events.) (RM;)

Protective Packaging

Packaging techniques for COMSEC material which discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

Protective Technologies

Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

#-Protective Technology

This KSA has no definition.

Protective Technology/Package Incident

Any penetration of information system security protective technology or packaging, such as a crack, cut, or tear.

Protocol

1. [In general,] A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (~) (FP) (ISO) Note: Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communication over a data link is performed in terms of the particular transmission mode, control procedures, and recovery procedures. See also communications, handshaking, link (def. #1), link protocol, N-entity, network, packet, packet format.
2. In layered communication system architecture, a formal set of procedures that are adopted to facilitate functional interoperation within the layered hierarchy. See also Open Systems Interconnection--Protocol Specifications, Open Systems Interconnection--Reference Model.

Protocol Data Unit

Information that is delivered as a unit between peer entities of a network and may contain control information, address information, or data. See also Open Systems Interconnection--Reference Model.

Protocols

A set of rules and formats (semantic and syntactic) which determines the common behaviour of entities (*NCSC-WA*-001-85;)

Prototype

1. A pre-production, functioning specimen(s) that is the first of its type, typically used for the evaluation of design, performance, and/or production potential.
2. A model suitable for evaluation of design, performance, and production potential. (JCS1-DoD)

Provably Secure Operating System

(PSOS) A capability-based operating system structured as a hierarchy of nested abstract machines. PSOS was designed at SRI and the system design utilizes SPECIAL and MLS. (MTR-8201)

Provisioning

The act of supplying telecommunications service to a user, including all associated transmission, wiring, and equipment. In NS/EP telecommunication services, “provisioning” and “initiation” are See ous and include altering the state of an existing priority ser-

vice or capability. See also NS/EP telecommunications.

*-Provocative Maintenance

[common ironic mutation of `preventive maintenance'] Actions performed upon a machine at regularly scheduled intervals to ensure that the system remains in a usable state. So called because it is all too often performed by a field servoid who doesn't know what he is doing; such `maintenance' often *induces* problems, or otherwise results in the machine's remaining in an *un*usable state for an indeterminate amount of time. See also scratch monkey.

*-Prowler

n. [UNIX] A daemon that is run periodically (typically once a week) to seek out and erase core files, truncate administrative logfiles, nuke `lost+found' directories, and otherwise clean up the cruft that tends to pile up in the corners of a file system. See also GFR, reaper, skulker.

*-Pseudo

/soo'doh/ n. [Usenet truncation of `pseudonym']

1. An electronic-mail or Usenet persona adopted by a human for amusement value or as a means of avoiding negative repercussions of one's net. behavior; a `nom de Usenet', often associated with forged postings designed to conceal message origins. Perhaps the best-known and funniest hoax of this type is B1FF. See also tentacle.
2. Notionally, a flamage-generating AI program simulating a Usenet user. Many flamers have been accused of actually being such entities, despite the fact that no AI program of the required sophistication yet exists. However, in 1989 there was a famous series of forged postings that used a phrase-frequency-based travesty generator to simulate the styles of several well-known flamers; it was based on large samples of their back postings (compare Dissociated Press). A significant number of people were fooled by the forgeries, and the debate over their authenticity was settled only when the perpetrator came forward to publicly admit the hoax.

Pseudo-Flaw

An apparent loophole deliberately implanted in an operating system program as a trap for intruders. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

*-Pseudoprime

n. A backgammon prime (six consecutive occupied points) with one point missing. This term is an esoteric pun derived from a mathematical method that, rather than determining precisely whether a number is prime (has no divisors), uses a statistical technique to decide whether the number is `probably' prime. A number that passes this test was, before about 1985, called a `pseudoprime' (the terminology used by number theorists has since changed slightly; pre-1985 pseudoprimes are now `probable primes' and `pseudoprime' has a more restricted meaning in modular arithmetic). The hacker backgammon usage stemmed from the idea that a pseudoprime is almost as good as a prime it does the job of a prime until proven otherwise, and that probably won't happen.

Pseudorandom Noise

Noise that satisfies one or more of the standard tests for statistical randomness. (~) Note: Although it seems to lack any definite pattern, the pseudorandom sequence of pulses will repeat after a very long time interval. See also noise, white noise.

Pseudorandom Number Sequence

An ordered set of numbers that has been determined by some defined arithmetic process but is effectively a random number sequence for the purpose for which it is required. (FP) (ISO) Note: Although it seems to lack any definite pattern, this sequence of numbers will repeat after a very long time interval. See also random number, spread spectrum.

*-Pseudosuit

n. /soo'doh-s[y]oot`/ A suit wannabee; a hacker who has decided that he wants to be in management or administration and begins wearing ties, sport coats, and (shudder!) suits voluntarily. It's his funeral. See also lobotomy.

PSOS

Provably Secure Operating System. A capability based operating system structured as a hierarchy of nested abstract machines. PSOS was designed at SRI and the system design utilizes SPECIAL and MLS. (MTR-8201;)

*-Psychedelicware

/si:`k*-del'-ik-weir/ n. [UK] Syn. display hack. See also smoking clover.

*-Psyton

/si:'ton/ n. [TMRC] The elementary particle carrying the sinister force. The probability of a process losing is proportional to the number of psytons falling on it. Psytons are generated by observers, which is why demos are more likely to fail when lots of people are watching. [This term appears to have been largely superseded by bogon; see also quantum bogodynamics. -- ESR]

Public Cryptography

Body of cryptographic and related knowledge, study, techniques, and applications that is, or intended to be, in the public domain.

Public Data Network

A network established and operated by a telecommunication administration, or a recognized private operating agency, for the specific purpose of providing data transmission services for the public. (~) See also

communications, data transmission, public data transmission service, public switched network, public switched telephone network.

Public Data Transmission Service

A data transmission service that is established and operated by a telecommunication administration, or a recognized private operating agency, and uses a public data network. Note: The service may include circuit-switched, packet-switched, and leased-circuit data transmission. See also data transmission, public data network.

Public Domain

1. In open view; before the public-at-large and not in private or employng secrecy or other protective measures.
2. Software acquired from government or non-government sources, often at no charge, when the source takes no responsibility for the integrity or maintenance of the software. (JCS PUB 6-03. 7; *AFR* 205-16)

Public Domain Software

Software distributed without charge. Such software commonly does not have security protection features and is more susceptible to viruses. See Freeware and Shareware.

Public Key

Type of cryptography in which the cryptography encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. NOTE: Commonly called non-secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography.

Public Key Cryptography (PKC)

Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. NOTE: Commonly called non-secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography. (F:\NEWDEFS. TXT)

#-Public Key Encryption

Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decrypting key is protected so that only party with knowledge of both parts of the decrypting process can decrypt the cipher text. (Source: NSTISSI 4009).

Public Law 100-235

Also known as the Computer Security Act of 1987, this law creates a means for establishing minimum acceptable security practices for improving the security and privacy of sensitive information in federal computer systems. This law assigns to the National Institute of Standards and Technology responsibility for developing standards and guidelines for federal computer systems processing unclassified data. The law also requires establishment of security plans by all operators of federal computer systems that contain sensitive information. (*NCSC-TG*-004-88)

Public Policy

Public Switched Network (PSN)

Any common carrier network that provides circuit switching among public users. (~) Note: The term is usually applied to the public switched telephone network, but it could be applied more generally to other switched networks, e. g. , public data networks and packet-switched public data networks. See also circuit, communications, packet switching, public data network, public switched telephone network. (FS1037S1. TXT)

Public Switched NS/EP Telecommunications Services

Those NS/EP telecommunications services utilizing public switched networks. Such services may include both interexchange and intraexchange network facilities (e. g. , switching systems, interoffice trunks, and subscriber loops). See also private NS/EP telecommunications services.

Public Switched Telephone Network

The domestic telecommunications network commonly accessed by ordinary telephones, key telephone systems, private branch exchange trunks, and data arrangements. Note: Completion of the circuit between the calling and called parties in this network requires network signaling in the form of dial pulses or multifrequency signals. See also circuit, communications, public data network, public switched network, telephony.

Public Utility Commission

A generic term for any state regulatory body charged with regulating intrastate utilities, including telecommunications. Note: In some states this function is performed by public service commissions or state corporation commissions. (FS1037S1. TXT) (PUC) A generic term for any state regulatory body charged with regulating intrastate utilities, including telecommunications. Note: In some states this function is performed by public service commissions or state corporation commissions.

*-Puff

vt. To decompress data that has been crunched by Huffman coding. At least one widely distributed Huffman decoder program was actually *named* `PUFF', but these days it is usually packaged with the encoder. Oppose huff.

*-Punched Card

n. obs. [techspeak] (alt. `punch card') The signature medium of computing's Stone Age, now obsolescent outside of some IBM shops. The punched card actually predated computers considerably, originating in 1801 as a control device for mechanical looms. The version patented by Hollerith and used with mechanical tabulating machines in the 1890 U. S. Census was a piece of cardboard about 90 mm by 215 mm. There is a widespread myth that it was designed to fit in the currency trays used for that era's larger dollar bills, but recent investigations have falsified this. IBM (which originated as a tabulating-machine manufacturer) married the punched card to computers, encoding binary information as patterns of small rectangular holes; one character per column, 80 columns per card. Other coding schemes, sizes of card, and hole shapes were tried at various times. The 80-column width of most character terminals is a legacy of the IBM punched card; so is the size of the quick-reference cards distributed with many varieties of computers even today. See chad, chad box, eighty-column mind, green card, dusty deck, lace card, card walloper.

*-Punt

v. [from the punch line of an old joke referring to American football “Drop back 15 yards and punt!”]

1. To give up, typically without any intention of retrying. “Let's punt the movie tonight. ” “I was going to hack all night to get this feature in, but I decided to punt” may mean that you've decided not to stay up all night, and may also mean you're not ever even going to put in the feature.
2. More specifically, to give up on figuring out what the Right Thing is and resort to an inefficient hack.
3. A design decision to defer solving a problem, typically because one cannot define what is desirable sufficiently well to frame an algorithmic solution. “No way to know what the right form to dump the graph in is -- we'll punt that for now. ”
4. To hand a tricky implementation problem off to some other section of the design. “It's too hard to get the compiler to do that; let's punt to the run-time system. ”

Purge

1. Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is ensurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. (DODD 5200. 28)
2. The removal of sensitive data from an AIS, AIS storage device, or peripheral device with storage capacity, at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. After a purge, the medium can be declassified by observing the review procedures of the respective agency. Replaces the term clear. (*NCSC-TG*-004-88)

Purging

The orderly review of storage and removal of inactive or obsolete data files and the removal of obsolete data by erasure, overwriting of storage, or resetting of registers. (*AR* 380-380;; *NCSC-WA*-001-85;; *FIPS PUB* 39;)

Purging Magnetic Media

Removing information from a medium so that data scavenging using any known technique or analysis is prevented. This medium can be subsequently declassified upon observing the review and verify procedures of the respective agency. (NCSC-td-004-88)

*-Purple Book

1. n. The “System V Interface Definition”. The covers of the first editions were an amazingly nauseating shade of off-lavender.
2. Syn. Wizard Book. Donald Lewine's “POSIX Programmer's Guide” (O'Reilly, 1991, ISBN 0-937175-73-0). See also book titles.

*-Purple Wire

n. [IBM] Wire installed by Field Engineers to work around problems discovered during testing or debugging. These are called `purple wires' even when (as is frequently the case) their actual physical color is yellow. Compare blue wire, yellow wire, and red wire.

Purpose And Scope

*-Push

[from the operation that puts the current information on a stack, and the fact that procedure return addresses are saved on a stack] (Also PUSH /push/ or PUSHJ /push'J/, the latter based on the PDP-10 procedure call instruction.)

1. To put something onto a stack or pdl. If one says that something has been pushed onto one's stack, it means that the Damoclean list of things hanging over ones's head has grown longer and heavier yet. This may also imply that one will deal with it

before other pending items; otherwise one might say that the thing was `added to my queue'.
2. vi. To enter upon a digression, to save the current discussion for later. Antonym of pop; see also stack, pdl.

Q

*-Quad

1. n. Two bits; syn. for quarter, crumb, tayste.
2. A four-pack of anything (compare hex, sense 2.
3. The rectangle or box glyph used in the APL language for various arcane purposes mostly related to I/O. Former Ivy-Leaguers and Oxford types are said to associate it with nostalgic memories of dear old University.

QUADRANT

Short name referring to technology which provides tamper-resistant protection to crypto-equipment.

*-Quadruple Bucky

1. n. ,obs. On an MIT space-cadet keyboard, use of all four of the shifting keys (control, meta, hyper, and super) while typing a character key.
2. On a Stanford or MIT keyboard in raw mode, use of four shift keys while typing a fifth character, where the four shift keys are the control and meta keys on *both* sides of the keyboard. This was very difficult to do! One accepted technique was to press the left-control and left-meta keys with your left hand, the right-control and right-meta keys with your right hand, and the fifth key with your nose. Quadruple-bucky combinations were very seldom used in practice, because when one invented a new command one usually assigned it to some character that was easier to type. If you want to imply that a program has ridiculously many commands or features, you can say something like “Oh, the command that makes it spin the tapes while whistling Beethoven's Fifth Symphony is quadruple-bucky-cokebottle. ” See double bucky, bucky bits, cokebottle.

#-Quality Assurance

Measuring or estimating the quality of delivered products and services. Software quality assurance focuses more on process than on product. (Source Marciniak, vol II).

Quality Control

(QC) A management function whereby control of the quality of raw materials, assemblies, produced materiel, and services is exercised for the purpose of preventing production of defective materiel or providing faulty services. (~) See also grade of service.

Quality Of Service

1. The quality specification of a communication channel or system. (~) Note: It may be stated in terms of signal-to-noise ratio, bit error ratio, message throughput rate, or call blocking probability.
2. A subjective rating of telephone communication quality, in which listeners judge a transmission as excellent, good, fair, poor, or unsatisfactory. See also call, grade of service.

*-Quantifiers

In techspeak and jargon, the standard metric prefixes used in the SI (Syst`eme International) conventions for scientific measurement have dual uses. With units of time or things that come in powers of 10, such as money, they retain their usual meanings of multiplication by powers of 1000 = 10^3. But when used with bytes or other things that naturally come in powers of 2, they usually denote multiplication by powers of 1024 = 2^(10). Here are the SI magnifying prefixes, along with the corresponding binary interpretations in common use prefix decimal binary kilo- 1000^1 1024^1 = 2^10 = 1,024 mega- 1000^2 1024^2 = 2^20 = 1,048,576 giga- 1000^3 1024^3 = 2^30 = 1,073,741,824 tera- 1000^4 1024^4 = 2^40 = 1,099,511,627,776 peta- 1000^5 1024^5 = 2^50 = 1,125,899,906,842,624 exa- 1000^6 1024^6 = 2^60 = 1,152,921,504,606,846,976 zetta- 1000^7 1024^7 = 2^70 = 1,180,591,620,717,411,303,424 yotta- 1000^8 1024^8 = 2^80 = 1,208,925,819,614,629,174,706,176 Here are the SI fractional prefixes *prefix decimal jargon usage* milli- 1000^-1 (seldom used in jargon) micro- 1000^-2 small or human-scale (see micro-) nano- 1000^-3 even smaller (see nano-) pico- 1000^-4 even smaller yet (see pico-) femto- 1000^-5 (not used in jargon--yet) atto- 1000^-6 (not used in jargon--yet) zepto- 1000^-7 (not used in jargon--yet) yocto- 1000^-8 (not used in jargon--yet) The prefixes zetta-, yotta-, zepto-, and yocto- have been included in these tables purely for completeness and giggle value; they were adopted in 1990 by the `19th Conference Generale des Poids et Mesures'. The binary peta- and exa- loadings, though well established, are not in jargon use either -- yet. The prefix milli-, denoting multiplication by 1000^(-1), has always been rare in jargon (there is, however, a standard joke about the `millihelen' -- notionally, the amount of beauty required to launch one ship). See the entries on micro-, pico-, and nano- for more information on connotative jargon use of these terms. `Femto' and `atto' (which, interestingly, derive not from Greek but from Danish) have not yet acquired jargon loadings, though it is easy to predict what those will be once computing technology enters the required realms of magnitude (however, see attoparsec). There are, of course, some standard unit prefixes for powers of 10. In the following table, the `prefix' column is the international standard suffix for the appropriate power of ten; the `binary' column lists jargon abbreviations and words for the corresponding power of 2. The B-suffixed forms are commonly used

for byte quantities; the words `meg' and `gig' are nouns that may (but do not always) pluralize with `s'. prefix decimal binary pronunciation kilo- k K, KB, /kay/ mega- M M, MB, meg /meg/ giga- G G, GB, gig /gig/,/jig/ Confusingly, hackers often use K or M as though they were suffix or numeric multipliers rather than a prefix; thus “2K dollars”, “2M of disk space”. This is also true (though less commonly) of G. Note that the formal SI metric prefix for 1000 is `k'; some use this strictly, reserving `K' for multiplication by 1024 (KB is thus `kilobytes'). K, M, and G used alone refer to quantities of bytes; thus, 64G is 64 gigabytes and `a K' is a kilobyte (compare mainstream use of `a G' as short for `a grand', that is, $1000). Whether one pronounces `gig' with hard or soft `g' depends on what one thinks the proper pronunciation of `giga-' is. Confusing 1000 and 1024 (or other powers of 2 and 10 close in magnitude) -- for example, describing a memory in units of 500K or 524K instead of 512K -- is a sure sign of the marketroid. One example of this it is common to refer to the capacity of 3. 5” microfloppies as `1. 44 MB' In fact, this is a completely bogus number. The correct size is 1440 KB, that is, 1440 * 1024 = 1474560 bytes. So the `mega' in `1. 44 MB' is compounded of two `kilos', one of which is 1024 and the other of which is 1000. The correct number of megabytes would of course be 1440 / 1024 = 1. 40625. Alas, this fine point is probably lost on the world forever. [1993 update hacker Morgan Burke has proposed, to general approval on Usenet, the following additional prefixes:groucho 10^(-30)harpo 10^(-27)harpi 10^(27)grouchi 10^(30) We observe that this would leave the prefixes zeppo-, gummo-, and chico- available for future expansion. Sadly, there is little immediate prospect that Mr. Burke's eminently sensible proposal will be ratified.]

Quantization

A process in which the continuous range of values of a signal is divided into nonoverlapping (but not necessarily equal) subranges, a discrete value being uniquely assigned to each subrange. Note: When sampling, e. g. , to achieve pulse-code modulation, if the sampled signal value falls within a given subrange, the sample is assigned the corresponding discrete value. (~) See also a-law, quantization level, signal, uniform encoding.

Quantization Level

In the quantization process, the discrete value assigned to a particular subrange. (~) See also a-law, level, quantization, uniform encoding.

*-Quantum Bogodynamics

/kwon'tm boh`goh-di:-nam'iks/ n. A theory that characterizes the universe in terms of bogon sources (such as politicians, used-car salesmen, TV evangelists, and suits in general), bogon sinks (such as taxpayers and computers), and bogosity potential fields. Bogon absorption, of course, causes human beings to behave mindlessly and machines to fail (and may also cause both to emit secondary bogons); however, the precise mechanics of the bogon-computron interaction are not yet understood and remain to be elucidated. Quantum bogodynamics is most often invoked to explain the sharp increase in hardware and software failures in the presence of suits; the latter emit bogons, which the former absorb. See bogon, computron, suit, psyton.

*-Quarter

n. Two bits. This in turn comes from the `pieces of eight' famed in pirate movies -- Spanish silver crowns that could be broken into eight pie-slice-shaped `bits' to make change. Early in American history the Spanish coin was considered equal to a dollar, so each of these `bits' was considered worth 12. 5 cents. Syn. tayste, crumb, quad. Usage rare. General discussion of such terms is under nybble.

Quartz Clock

A clock containing a quartz oscillator that determines the accuracy and precision of the clock.

*-Ques

1. /kwes/ n. The question mark character (`?', ASCII 0111111).
2. interj. What? Also frequently verb-doubled as “Ques ques?” See wall.

Queue

A collection of items, such as telephone calls, that is arranged in sequence. (~) Note: Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive. See also buffer, queue traffic.

Queue Traffic

1. In a store-and-forward switching center, the outgoing messages awaiting transmission at the outgoing line position. (~)
2. A series of calls waiting for service. (~) See also buffer, called-party camp-on, calling-party camp-on, first-in first-out, message switching, queueing, selective calling.

Queueing

The process of entering elements into or removing elements from a queue. (~) See also buffer, queue traffic.

Queueing Delay

1. In an automatically switched telephone network, the time period that occurs between the completion of the calling party signaling and the arrival of a ringing signal at the called instrument. (~) Note: It may be due to delays (queues) at the originating

switch, any intermediate switches, or the called-party servicing switch.
2. In a data network, the sum of all the delays introduced by the network between the originator's request for service and the establishment of a circuit to the called data terminal equipment.
3. In a packet-switched network, the sum of all of the delays encountered by a packet between the time of introduction into the network and the time of delivery to the addressee. (~) See also buffer.

*-Quick-And-Dirty

adj. Describes a crock put together under time or user pressure. Used esp. when you want to convey that you think the fast way might lead to trouble further down the road. “I can have a quick-and-dirty fix in place tonight, but I'll have to rewrite the whole module to solve the underlying design problem. ” See also kluge.

*-Quine

/kwi:n/ n. [from the name of the logician Willard van Orman Quine, via Douglas Hofstadter] A program that generates a copy of its own source text as its complete output. Devising the shortest possible quine in some given programming language is a common hackish amusement. Here is one classic quine ((lambda (x) (list x (list (quote quote) x))) (quote (lambda (x) (list x (list (quote quote) x))))) This one works in LISP or Scheme. It's relatively easy to write quines in other languages such as Postscript which readily handle programs as data; much harder (and thus more challenging!) in languages like C which do not. Here is a classic C quine for ASCII machines char*f=“char*f=%c%s%c;main() printf(f,34,f,34,10);%c”; main()printf(f,34,f,34,10); For excruciatingly exact quinishness, remove the interior line breaks. Some infamous Obfuscated C Contest entries have been quines that reproduced in exotic ways.

*-Quote Chapter And Verse

v. [by analogy with the mainstream phrase] To cite a relevant excerpt from an appropriate bible. “I don't care if `rn' gets it wrong; `Followup-To poster' is explicitly permitted by RFC-1036. I'll quote chapter and verse if you don't believe me. ” See also legalese, language lawyer, RTFS (sense 2). .

*-Quotient

n. See coefficient of X.

*-QWERTY

/kwer'tee/ adj. [from the keycaps at the upper left] Pertaining to a standard English-language typewriter keyboard (sometimes called the Sholes keyboard after its inventor), as opposed to Dvorak or foreign-language layouts or a space-cadet keyboard or APL keyboard. Historical note The QWERTY layout is a fine example of a fossil. It is sometimes said that it was designed to slow down the typist, but this is wrong; it was designed to allow *faster* typing -- under a constraint now long obsolete. In early typewriters, fast typing using nearby type-bars jammed the mechanism. So Sholes fiddled the layout to separate the letters of many common digraphs (he did a far from perfect job, though; `th', `tr', `ed', and `er', for example, each use two nearby keys). Also, putting the letters of `typewriter' on one line allowed it to be typed with particular speed and accuracy for demos. The jamming problem was essentially solved soon afterward by a suitable use of springs, but the keyboard layout lives on.

R

Radar Intelligence

Intelligence information derived from data collected by radar. (JCS1-DoD)

Radiant Energy

Energy that is transferred via electromagnetic waves; i. e. , the time integral of radiant power, usually expressed in joules. (~) See also radiance.

Radiant Power

The time rate of flow of radiant energy, expressed in watts. Note: The prefix is often dropped, and the term “power” is used. Colloquial synonyms flux, optical power, power, radiant flux. See also radiance, radiometry.

Radiated Signal

Electromagnetic or acoustic emissions of undesired signal data which are propagated through space. (NACSEM 5106)

Radiation

1. In radio communication, the emission of energy in the form of electromagnetic waves. (~)
2. The outward flow of energy from any source in the form of radio waves. (RR)
3. See also antenna, hazards of electromagnetic radiation to fuel, hazards of electromagnetic radiation to ordnance, hazards of electromagnetic radiation to personnel, radiation pattern, radiation scattering, spurious radiation, thermal radiation.

Radio

1. A general term applied to the use of radio waves. (RR)
2. A method of communicating over a distance by modulating electromagnetic waves and radiating these waves. (~)

3. See also combat-net radio, radio waves or Hertzian waves.

Radio Fingerprinting

The process of recording and studying the characteristics of the emissions of a radio transmitter in order to identify the transmitting station. (NSA, *National INFOSEC Glossary*, 10/88)

*-Rain Dance

1. n. Any ceremonial action taken to correct a hardware problem, with the expectation that nothing will be accomplished. This especially applies to reseating printed circuit boards, reconnecting cables, etc. “I can't boot up the machine. We'll have to wait for Greg to do his rain dance. ”
2. Any arcane sequence of actions performed with computers or software in order to achieve some goal; the term is usually restricted to rituals that include both an incantation or two and physical activity or motion. Compare magic, voodoo programming, black art, cargo cult programming, wave a dead chicken.

#-Rainbow Series

1. A set of publications issued by the Nation Computer Security Center (NCSC) under the authority of *DOD* DIR 5215. 1. These publications provide insight into the *Orange Book* requirements and guidance for meeting each requirement. (source - Panel of experts);
2. A series of books produced by the NCSC relating to special topics about AIS security.

Ramp

*-Random

1. adj. Unpredictable (closest to mathematical definition); weird. “The system's been behaving pretty randomly. ”
2. Assorted; undistinguished. “Who was at the conference?” “Just a bunch of random business types. ”
3. (pejorative) Frivolous; unproductive; undirected. “He's just a random loser. ”
4. Incoherent or inelegant; poorly chosen; not well organized. “The program has a random set of misfeatures. ” “That's a random name for that function. ” “Well, all the names were chosen pretty randomly. ”
5. In no particular order, though deterministic. “The I/O channels are in a pool, and when a file is opened one is chosen randomly. ”
6. Arbitrary. “It generates a random name for the scratch file. ”
7. Gratuitously wrong, i. e. , poorly done and for no good apparent reason. For example, a program that handles file name defaulting in a particularly useless way, or an assembler routine that could easily have been coded using only three registers, but redundantly uses seven for values with non-overlapping lifetimes, so that no one else can invoke it without first saving four extra registers. What randomness!
8. n. A random hacker; used particularly of high-school students who soak up computer time and generally get in the way.
9. n. Anyone who is not a hacker (or, sometimes, anyone not known to the hacker speaking); the noun form of sense 2. “I went to the talk, but the audience was full of randoms asking bogus questions”.
10. n. (occasional MIT usage) One who lives at Random Hall. See also J. Random, some random X.

Random Access Memory

(RAM) High-speed read/write memory with an access time that is essentially the same for all storage locations. (FP) See also read-only memory, volatile storage.

Random Noise

Noise consisting of a large number of transient disturbances with a statistically random time distribution. (~) Note: Thermal noise is an example of random noise. See also impulse noise, noise.

Random Number

1. A number selected from a known set of numbers in such a way that each number in the set has the same probability of occurrence. (FP) (ISO)
2. A number obtained by chance. (FP)
3. One of a sequence of numbers considered appropriate for satisfying certain statistical tests or believed to be free from conditions that might bias the result of a calculation. (FP) See also pseudo-random number sequence.

*-Random Numbers

n. When one wishes to specify a large but random number of things, and the context is inappropriate for N, certain numbers are preferred by hacker tradition (that is, easily recognized as placeholders). These include the following 17 Long described at MIT as `the least random number'; see 23. 23 Sacred number of Eris, Goddess of Discord (along with 17 and 5). 42 The Answer to the Ultimate Question of Life, the Universe, and Everything. (Note that this answer is completely fortuitous. `:-)') 69 From the sexual act. This one was favored in MIT's ITS culture. 105 69 hex = 105 decimal, and 69 decimal = 105 octal. 666 The Number of the Beast. For further enlightenment, study the “Principia Discordia”, “The Hitchhiker's Guide to the Galaxy”, “The Joy of Sex”, and the Christian Bible (Revelation 13:18). See also Discor-

dianism or consult your pineal gland. See also for values of.

Randomizer

1. A device used to invert the sense of pseudorandomly selected bits of a bit stream to avoid long sequences of bits of the same sense. (~) Note: The same selection pattern must be used on the receive terminal in order to restore the original bit stream.
2. An analog or digital source of unpredictable, unbiased, and usually independent bits. Note: Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator. See also binary digit, data scrambler, descrambler, limited protection voice equipment, scrambler.

*-Randomness

1. n. An inexplicable misfeature; gratuitous inelegance.
2. A hack or crock that depends on a complex combination of coincidences (or, possibly, the combination upon which the crock depends for its accidental failure to malfunction). “This hack can output characters 40--57 by putting the character in the four-bit accumulator field of an XCT and then extracting six bits -- the low 2 bits of the XCT opcode are the right thing. ” “What randomness!”
3. Of people, synonymous with `flakiness'. The connotation is that the person so described is behaving weirdly, incompetently, or inappropriately for reasons which are (a) too tiresome to bother inquiring into, (b) are probably as inscrutable as quantum phenomena anyway, and (c) are likely to pass with time. “Maybe he has a real complaint, or maybe it's just randomness. See if he calls back. ”

*-Rare Mode

adj. [UNIX] CBREAK mode (character-by-character with interrupts enabled). Distinguished from raw mode and cooked mode; the phrase “a sort of half-cooked (rare?) mode” is used in the V7/BSD manuals to describe the mode. Usagerare.

*-Raster Blaster

n. [Cambridge] Specialized hardware for bitblt operations (a blitter). Allegedly inspired by `Rasta Blasta', British slang for the sort of portable stereo Americans call a `boom box' or `ghetto blaster'.

*-Raster Burn

n. Eyestrain brought on by too many hours of looking at low-res, poorly tuned, or glare-ridden monitors, esp. graphics monitors. See terminal illness.

*-Rat Belt

n. A cable tie, esp. the sawtoothed, self-locking plastic kind that you can remove only by cutting (as opposed to a random twist of wire or a twist tie or one of those humongous metal clip frobs). Small cable ties are `mouse belts'.

Rating

Rating Maintenance Phase

Rating Maintenance Plan (RM-Plan, RM Plan).

Rating Maintenance Report (RMR)

See RMR

Ratings Maintenance Phase (ramp)

Ratings Maintenance Plan

*-Rave

1. vi. [WPI] To persist in discussing a specific subject.
2. To speak authoritatively on a subject about which one knows very little.
3. To complain to a person who is not in a position to correct the difficulty.
4. To purposely annoy another person verbally.
5. To evangelize. See flame. 6. Also used to describe a less negative form of blather, such as friendly BS. `Rave' differs slightly from flame in that `rave' implies that it is the persistence or obliviousness of the person speaking that is annoying, while flame implies somewhat more strongly that the tone or content is offensive as well.

*-Rave On!

imp. Sarcastic invitation to continue a rave, often by someone who wishes the raver would get a clue but realizes this is unlikely.

*-Raw Mode

n. A mode that allows a program to transfer bits directly to or from an I/O device (or, under bogus systems that make a distinction, a disk file) without any processing, abstraction, or interpretation by the operating system. Compare rare mode, cooked mode. This is techspeak under UNIX, jargon elsewhere.

*-Rc File

/R-C fi:l/ n. [UNIXfrom `runcom files' on the CTSS system ca. 1955, via the startup script `/etc/rc'] Script file containing startup instructions for an application program (or an entire operating system), usually a text file containing commands of the sort that might have been invoked manually once the system was running but are to be executed automatically each time the system starts up. See also dot file, profile (sense 1).

Read

A fundamental operation that results only in the flow of information from an object to a subject. (CSC-STD-001-83;; CSC-WA-001-85;) See Access Type and Write.

Read Access

Permission to read information. (CSC-STD-001-83; *NCSC-WA*-001-85;) See Write Access.

Read Down

Ability of a subject to read objects classified at the subject's security level and below. Permission is provided through the security functions on a system and administered by the system manager. See Read Up, Write Down, and Write Up.

Read Head

A magnetic head capable of reading only. (FP) (ISO)

Read Up

Ability of a subject to read objects classified above the subject's security level. This should never happen. See Read Down, Write Down, and Write Up.

Read-Only Memory

(ROM) A storage area in which the contents can be read but not altered during normal computer processing. (*DOD* 5200. 28-STD)

Read-Only Storage

A storage device whose contents cannot be modified, except by a particular user, or when operating under particular conditions, for example, a storage device in which writing is prevented by a lockout. (~) (FP) See fixed storage. See also erase, firmware, permanent storage, reading, storage.

*-Read-Only User

n. Describes a luser who uses computers almost exclusively for reading Usenet, bulletin boards, and/or email, rather than writing code or purveying useful information. See twink, terminal junkie, lurker.

Read/write Opening

See read/write slot.

Read/write Slot

An opening in the jacket of a diskette to allow access to the read/write heads. See read/write opening.

Reading

The acquisition or interpretation of data from a storage device, from a data medium, or from another source. (FP) (ISO)

*-README File

n. Hacker's-eye introduction traditionally included in the top-level directory of a UNIX source distribution, containing a pointer to more detailed documentation, credits, miscellaneous revision history, notes, etc. (The file may be named README, or READ. ME, or rarely ReadMe or readme. txt or some other variant.) In the Mac and PC worlds, software is not usually distributed in source form, and the README is more likely to contain user-oriented material like last-minute documentation changes, error workarounds, and restrictions. When asked, hackers invariably relate the README convention to the famous scene in Lewis Carroll's “Alice's Adventures In Wonderland” in which Alice confronts magic munchies labeled “Eat Me” and “Drink Me”.

*-Real

adj. Not simulated. Often used as a specific antonym to virtual in any of its jargon senses.

*-Real Estate

n. May be used for any critical resource measured in units of area. Most frequently used of `chip real estate', the area available for logic on the surface of an integrated circuit (see also nanoacre). May also be used of floor space in a dinosaur pen, or even space on a crowded desktop (whether physical or electronic).

*-Real Hack

n. A crock. This is sometimes used affectionately; see hack.

*-Real Operating System

n. The sort the speaker is used to. People from the BSDophilic academic community are likely to issue comments like “System V? Why don't you use a *real* operating system?”, people from the commercial/industrial UNIX sector are known to complain “BSD? Why don't you use a *real* operating system?”, and people from IBM object “UNIX? Why don't you use a *real* operating system?” Only MS-DOS is universally considered unreal. See holy wars, religious issues, proprietary, Get a real computer!

*-Real Programmer

n. [indirectly, from the book “Real Men Don't Eat Quiche”] A particular sub-variety of hacker one possessed of a flippant attitude toward complexity that is arrogant even when justified by experience. The archetypal `Real Programmer' likes to program on the bare metal and is very good at same, remembers the binary opcodes for every machine he has ever programmed, thinks that HLLs are sissy, and uses a debugger to edit his code because full-screen editors are for wimps. Real Programmers aren't satisfied with code that hasn't been bummed into a state of tenseness just short of rupture. Real Programmers never use comments or write documentation “If it was hard to write”, says the Real Programmer, “it should be hard to understand. ” Real Programmers can make machines do things that were never in their spec sheets; in fact, they are seldom really happy unless doing so. A Real Programmer's code can awe with its fiendish brilliance, even as its crockishness appalls.

Real Programmers live on junk food and coffee, hang line-printer art on their walls, and terrify other programmers -- because someday, somebody else might have to try to understand their code in order to change it. Their successors generally consider it a Good Thing that there aren't many Real Programmers around any more. For a famous (and somewhat more positive) portrait of a Real Programmer, see “The Story of Mel, a Real Programmer” in Appendix A. The term itself was popularized by a 1983 Datamation article “Real Programmers Don't Use Pascal” by Ed Post, still circulating on Usenet and Internet in online form.

*-Real Soon Now

adv. [orig. from SF's fanzine community, popularized by Jerry Pournelle's column in “BYTE”]

1. Supposed to be available (or fixed, or cheap, or whatever) real soon now according to somebody, but the speaker is quite skeptical.
2. When one's gods, fates, or other time commitments permit one to get to it (in other words, don't hold your breath). Often abbreviated RSN. Compare copious free time.

Real Time

1. The actual time during which a physical process occurs. (~)
2. Pertaining to the performance of a computation during the actual time that the related physical process occurs, in order that results of the computation can be used in guiding the physical process.
3. The absence of delay, except for the time required for the transmission by electromagnetic energy, between the occurrence of an event or the transmission of data, and the knowledge of the event, or reception of the data at some other location. (JCS1-DoD). See also absolute delay, near real time, transmission.

*-Real User

1. n. A commercial user. One who is paying *real* money for his computer usage.
2. A non-hacker. Someone using the system for an explicit purpose (a research project, a course, etc.) other than pure exploration. See user. Hackers who are also students may also be real users. “I need this fixed so I can do a problem set. I'm not complaining out of randomness, but as a real user. ” See also luser.

*-Real World

1. n. Those institutions at which `programming' may be used in the same sentence as `FORTRAN', `COBOL', `RPG', `IBM', `DBASE', etc. Places where programs do such commercially necessary but intellectually uninspiring things as generating payroll checks and invoices.
2. The location of non-programmers and activities not related to programming.
3. A bizarre dimension in which the standard dress is shirt and tie and in which a person's working hours are defined as 9 to 5 (see code grinder).
4. Anywhere outside a university. “Poor fellow, he's left MIT and gone into the Real World. ” Used pejoratively by those not in residence there. In conversation, talking of someone who has entered the Real World is not unlike speaking of a deceased person. It is also noteworthy that on the campus of Cambridge University in England, there is a gaily-painted lamp-post which bears the label `REALITY CHECKPOINT'. It marks the boundary between university and the Real World; check your notions of reality before passing. This joke is funnier because the Cambridge `campus' is actually coextensive with the center of Cambridge. See also fear and loathing, mundane, and uninteresting.

Real-Time Reaction

Immediate response to a penetration attempt which is detected and diagnosed in time to prevent the actual penetration. (*FIPS PUB* 39;; *AR* 380-380;)

*-Reality Check

1. n. The simplest kind of test of software or hardware; doing the equivalent of asking it what 2 + 2 is and seeing if you get
4. The software equivalent of a smoke test.
2. The act of letting a real user try out prototype software. Compare sanity check.

Realization

A single successful occurrence of a threat. (RM;)

Realization Cost

The expected cost to the agent resulting from his attempts to perpetrate an event. (RM;)

*-Reaper

n. A prowler that GFRs files. A file removed in this way is said to have been `reaped'.

Reasonability Checks

Rules describing unacceptable combinations of results. For example, a program predicting weather should not forecast snow with high temperatures. (*AFR* 205-16)

REASSURE

Risk Evaluation and Assessment Support System, Using Relevant Environments.

Receive Only

(RO) Pertaining to a device or a mode of operation capable of receiving messages, but not of transmitting messages. (~)

Recertification

An ongoing reassurance that a previously certified unclassified computer application processing sensitive information has been periodically reviewed, that compliance with established protection policies-and procedures remains in effect, and that security risks remain at an acceptable level. (*DOE 1360. 2A*)

*-RechRef

/tek'ref/ n. [MS-DOS] The original “IBM PC Technical Reference Manual”, including the BIOS listing and complete schematics for the PC. The only PC documentation in the issue package that's considered serious by real hackers.

Recognition

1. The determination by any means of the individuality of persons, or of objects, such as aircraft, ships, or tanks, or of phenomena such as communications-electronics patterns. (JCS1-DoD) (~)
2. In ground combat operations, the determination that an object is similar within a category of something already known; e. g. , tank, truck, man. (JCS1-DoD)
3. The determination of the nature of a detected person, object, or phenomenon, and possibly its class or type. This may include the determination of an individual within a particular class or type. (JCS1-NATO) See also authenticate, identification friend or foe, identification friend or foe personal identifier, intelligibility.

#-Reconciliation

In auditing, pertaining to the identification and analysis of detected differences between values contained in two substantially similar files or between a detail file and a control total. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

Record

A set of related data elements treated as a unit. (~) See also file.

Record Communication

A telecommunication process that produces a hard copy record of the transmission, such as teletypewriter and facsimile. (~) See also communications, facsimile, hard copy, teletypewriter.

Record Information

All forms (e. g. , narrative, graphic, data, computer memory) of information registered in either temporary or permanent form so that it can be retrieved, reproduced, or preserved. (JCS1-DoD) See also hard copy.

Record Medium

1. The physical medium on which information is stored in recoverable form. (~)
2. In facsimile transmission, the physical medium on which the recorder forms an image of the subject copy. (~) Note: The record medium and the record sheet may be identical. See record sheet. See also facsimile, hard copy.

Record Sheet

See record medium.

Record Traffic

1. Traffic that is recorded, in permanent or quasipermanent form, by the originator, the addressee, or both. (~)
2. Traffic that is permanently or semipermanently recorded in response to administrative procedures or public law. See also hard copy, narrative traffic.

Recorded Copy

In facsimile, a visible image of the original in record form. (~) See also facsimile, hard copy.

Recording

1. The process of converting electrical signals to a recoverable form on a preservable medium. (~)
2. In facsimile systems, the process of converting the electrical signals to an image on a preservable medium. (~)

Recording Density

See bit density (def. #1).

Recoverable Zone

The three-dimensional space surrounding an equipment or system processing national security information within which it is theoretically possible to recover the information processed. For radiated signals, this term may be used interchangeably with Equipment Radiation TEMPEST Zone (ERTZ).

Recovery

1. The process of restoring an organization to operate as before an event. (RM;)
2. The restoration of an Asset or Assets to a specified prior state. (MK;)
3. In a database management system, the procedures and capabilities available for reconstruction of the contents of a database to a state that prevailed before the detection of processing errors and before the occurrence of a hardware or software failure that resulted in the destruction of some or all of the stored data.
4. The breaking back of intelligence from a TEMPEST signal. (NACSEM 5106)

Recovery Procedure

1. The actions necessary to restore an automated information system's data files and computational capability after a system failure.
2. In data communications, a process whereby a data station attempts to resolve conflicting or erroneous

conditions arising during the transfer of data. See also clear collision, error.

Recovery Procedures

1. The actions necessary to restore a system's computational capability and data files after a system failure or penetration. (*FIPS PUB* 39; *AR* 380-380)
2. The actions necessary to restore a system's computational capability and data files after a system failure. (*NCSC-TG*-004-88)

*-Rectangle Slinger

n. See polygon pusher.

*-Recursion

n. See recursion. See also tail recursion.

*-Recursive Acronym

n. A hackish (and especially MIT) tradition is to choose acronyms/abbreviations that refer humorously to themselves or to other acronyms/abbreviations. The classic examples were two MIT editors called EINE ("EINE Is Not EMACS") and ZWEI ("ZWEI Was EINE Initially"). More recently, there is a Scheme compiler called LIAR (Liar Imitates Apply Recursively), and GNU (q. v. , sense 1) stands for "GNU's Not UNIX!" -- and a company with the name CYGNUS, which expands to "Cygnus, Your GNU Support". See also mung, EMACS.

RED

1. Refers to equipment and wire lines handling non-encrypted, classified information. (*AFR* 205-16;);
2. Designation applied to telecommuni-cations and automated information systems, plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.
3. See RED DESIGNATION.

*-Red Book

1. n. Informal name for one of the three standard references on PostScript ("PostScript Language Reference Manual", Adobe Systems (Addison-Wesley, 1985; QA76. 73. P67P67; ISBN 0-201-10174-2, or the 1990 second edition ISBN 0-201-18127-4); the others are known as the Green Book, the Blue Book, and the White Book (sense 2) .
2. Informal name for one of the 3 standard references on Smalltalk ("Smalltalk-80 The Interactive Programming Environment" by Adele Goldberg (Addison-Wesley, 1984; QA76. 8. S635G638; ISBN 0-201-11372-4); this too is associated with blue and green books).
3. Any of the 1984 standards issued by the CCITT eighth plenary assembly. These include, among other things, the X. 400 email spec and the Group 1 through 4 fax standards.
4. The new version of the Green Book (sense 4) -- IEEE 1003. 1-1990, a. k. a ISO 9945-1 -- is (because of the color and the fact that it is printed on A4 paper) known in the U. S. A. as "the Ugly Red Book That Won't Fit On The Shelf" and in Europe as "the Ugly Red Book That's A Sensible Size".
5. The NSA "Trusted Network Interpretation" companion to the *Orange Book*. See also book titles.

RED Conductor

Any conductor, which may or may not be intended to carry RED signals, connected to RED equipment. The RED side of crypto-equipment or the RED side of isolation devices. (NACSEM 5201)

RED Designation

A designation applied to: (1) all wire lines within the terminal or switching facility carrying classified plain language; (2) all wire lines between the unencrypted side of the on-line crypto-equipment and individual subscriber sets or terminal equipment; (3) equipment and sets originating or terminating classified plain language processing equipment; and (4) areas containing these wire lines, equipment, and their interconnecting and auxiliary facilities.

RED Equipment

Electrical or electronic equipment used to process classified information.

RED Equipment Area

(REA) The space within an LEA which is designated for installation of RED information processing equipment, power, signal control, groups feeder, and distribution facilities. (NACSIM 5203)

Red Key

Unencrypted key. See Black Key.

RED Line

A primary or secondary RED conductor.

RED Signal

1. Telecommunications or automated information systems signal that would divulge classified information if recovered and analyzed. NOTE: RED signals may be plain text, key, subkey, initial fill, control, or traffic flow related information.
2. Any classified signal (e. g. , plain text, key, subkey, initial fill, control signal or traffic-flow-related signal) which would divulge classified information if recovered and analyzed. See also BLACK, BLACK signal.

RED Signal Line

A line which intentionally carries RED signals externally to or from the Equipment Under Test (EUT).

*-Red Wire

n. [IBM] Patch wires installed by programmers who have no business mucking with the hardware. It is said that the only thing more dangerous than a hardware guy with a code patch is a softy with a soldering iron. Compare blue wire, yellow wire, purple wire.

RED/BLACK Concept

1. The concept that electrical and electronic circuits, components, equipment, systems, and so forth, which handle classified plain language information in electric signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to and differentiate between such circuits, components, equipment, systems, and so forth, and the areas in which they are contained. (*AR* 380-380; JCS PUB 6-03. 7)
2. The concept that telecommunications circuits components, equipment, and systems which handle classified plain-language information in electrical signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). (NCSC-9)

#-Redundancy

1. In the transmission of data, the excess of transmitted message symbols over that required to convey the essential information in a noise-free circuit. Note: Redundancy may be introduced intentionally (as in the case of error detection/correction codes) or inadvertently (such as by oversampling a band-limited signal, inefficient formats, etc.).
2. In a communication system, surplus capability usually provided to improve the reliability and quality of service. (~) See also continuous operation, data, data compression, frequency diversity, space diversity.

Redundancy Check

1. A method of verifying that any redundant hardware or software in a communication system is in an operational condition. (~)
2. A check that uses one or more extra binary digits or characters attached to data for the detection of errors. (FP) (ISO) (~) See also operational service state, performance parameter.

Redundant Code

A code using more signal elements than necessary to represent the intrinsic information. (~) Note: The redundancy may be used for error-control purposes. See also error control, redundancy.

Reference Monitor

A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base. (MTR-8201;)

Reference Monitor Concept

An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. (*NCSC-WA*-001-85;, CSC-STD-001-83;)

#-Reference Monitors

Access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. (Source: NSTISSI 4009).

Reference Validation

Portion of a trusted computing base, the mechanism normal function of which is to control access between subjects and objects, and the correct operation of which is essential to the protection of data in the system. NOTE: This is the implementation of reference monitor.

Reference Validation Mechanism

1. An implementation of the reference monitor concept. A security kernel is a particular (but not the only) type of a reference validation mechanism. (*NCSC-WA*-001-85;)
2. Portion of a trusted computing base, the normal function of which is to control access between subjects and objects, and the correct operation of which is essential to the protection of data in the system. NOTE: This is the implementation of reference monitor. See Trusted Computing Base (TCB).

Refresh

The process of repeatedly producing a display image on a display surface so that the image remains visible. (FP) (ISO)

Regeneration

1. The gain that results from coupling the output of an amplifier to its input. (~) Synonym positive feedback.
2. The action of a regenerative repeater in which digital signals are amplified, reshaped, retimed, and retransmitted. (~)
3. In a storage device whose information storing state may deteriorate, the process of restoring the device to its latest undeteriorated state. (~) See also closed loop transfer function, dejitterizer, feedback, signal regeneration.

*-Regexp

/reg'eksp/ n. [UNIX] (alt. `regex' or `reg-ex')

1. Common written and spoken abbreviation for `regular expression', one of the wildcard patterns used, e. g. , by UNIX utilities such as `grep(1)', `sed(1)', and `awk(1)'. These use conventions simi-

lar to but more elaborate than those described under glob. For purposes of this lexicon, it is sufficient to note that regexps also allow complemented character sets using `^'; thus, one can specify `any non-alphabetic character' with `[^A-Za-z]'.

2. Name of a well-known PD regexp-handling package in portable C, written by revered Usenetter Henry Spencer <henry@zoo. toronto. edu>.

Register

A temporary-memory device used to receive, hold, and transfer data (usually a computer word) to be operated upon by a processing unit. (~) Note: Computers typically contain a variety of registers. General-purpose registers perform such functions as accumulating arithmetic results. Other registers hold the instruction being executed, the address of a storage location, or data being retrieved from or sent to storage. See also buffer, fetch protection, M-sequence, read-only storage, permanent storage, random-access memory, shift register, storage.

*-Register Dancing

n. Many older processor architectures suffer from a serious shortage of general-purpose registers. This is especially a problem for compiler-writers, because their generated code needs places to store temporaries for things like intermediate values in expression evaluation. Some designs with this problem, like the Intel 80x86, do have a handful of special-purpose registers that can be pressed into service, providing suitable care is taken to avoid unpleasant side effects on the state of the processor while the special-purpose register is being used to hold an intermediate value, a delicate minuet is required in which the previous value of the register is saved and then restored just before the official function (and value) of the special-purpose register is again needed.

Regrade

A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection. An “upgrade” results in a higher classification; a “downgrade” results in a lower classification. (MTR-8201;)

Reimbursement

*-Reincarnation, Cycle Of

n. See cycle of reincarnation.

*-Reinvent The Wheel

v. To design or implement a tool equivalent to an existing one or part of one, with the implication that doing so is silly or a waste of time. This is often a valid criticism. On the other hand, automobiles don't use wooden rollers, and some kinds of wheel have to be reinvented many times before you get them right. On the third hand, people reinventing the wheel do tend to come up with the moral equivalent of a trapezoid with an offset axle.

Release Prefix

Prefix appended to the short title of United States produced keying material to indicate its foreign releasability. NOTE: “A” designates material that is releasable to specific allied nations and “US” designates material intended exclusively for United States use.

Reliability

1. The probability of a given automatic system performing its mission adequately for a period of time under the expected operating conditions. (*AR* 380-380)
2. The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions. (*NCSC-TG*-004-88)

#-Reliability Testing

Validate that the system meets the required reliability. (Source: DACUM IV).

*-Religion Of CHI

/ki:/ n. [Case Western Reserve University] Yet another hackish parody religion (see also Church of the SubGenius, Discordianism). In the mid-70s, the canonical “Introduction to Programming” courses at CWRU were taught in Algol, and student exercises were punched on cards and run on a Univac 1108 system using a homebrew operating system named CHI. The religion had no doctrines and but one ritual whenever the worshipper noted that a digital clock read 11:08, he or she would recite the phrase “It is 11:08; ABS, ALPHABETIC, ARCSIN, ARCCOS, ARCTAN. ” The last five words were the first five functions in the appropriate chapter of the Algol manual; note the special pronunciations /obz/ and /ark'sin/ rather than the more common /ahbz/ and /ark'si:n/. Using an alarm clock to warn of 11:08's arrival was considered harmful.

*-Religious Issues

n. Questions which seemingly cannot be raised without touching off holy wars, such as “What is the best operating system (or editor, language, architecture, shell, mail reader, news reader)?”, “What about that Heinlein guy, eh?”, “What should we add to the new Jargon File?” See holy wars; see also theology, bigot. This term is a prime example of ha ha only serious. People actually develop the most amazing and religiously intense attachments to their tools, even when the tools are intangible. The most constructive thing one can do when one stumbles into the crossfire is

mumble Get a life! and leave -- unless, of course, one's *own* unassailably rational and obviously correct choices are being slammed.

#-Remanance

1. A measure of the magnetic flux density remaining after removal of an applied magnetic force. Can also mean any data remaining on an ADP storage media after removal of power. (Source: NCSC TG 005);
2. Information that is unintentionally left behind in an AIS magnetic or semi-conductor memory.
3. The residual magnetism that remains on magnetic storage media after degaussing. (*FIPS PUB* 39;; *AR* 380-380;)
4. A measure of the magnetic flux density remaining after removal of an applied magnetic force. Can also mean any data remaining on ADP storage media after removal of the power. (CSC-STD-005-85;) See Magnetic Remanence.

Remote Access

1. Pertaining to communication with a data processing facility through a data link. (FP)
2. A PABX service feature that allows a user at a remote location to access PABX features by telephone; e. g. , WATS lines. Note: Individual authorization codes are usually required. See also access, PABX, remote control equipment, service feature, Wide Area Telephone Service.

Remote Access Data Processing

Data processing in which some input/output functions are performed by devices that are connected to a computer system by means of data communication. (FP) (ISO)

Remote Batch Entry

Submission of batches of data through an input unit that has access to a computer through a data link. (FP) (ISO)

Remote Batch Processing

Batch processing in which input-output units have access to a computer through a data link. (FP) (ISO)

Remote Call Forwarding

A service feature that allows calls coming to a remote call-forwarding number to be automatically forwarded to any answering location that the called customer wishes. Note: Customers may have a remote-forwarding telephone number in a central switching office without having any other local telephone service in that office.

Remote Control Equipment

Devices used to perform monitoring, controlling, and/or supervisory functions, at a distance. (~) See also access point, remote access.

Remote Job Entry

(RJE) In computer operations, that mode of operation that allows input of a job to a computer from a remote site and receipt of the output at a remote site via a communications link. See also remote access.

Remote Rekeying

Procedure by which a distant crypto-equipment is rekeyed electrically. See Automatic Remote Rekeying and Manual Remote Rekeying.

Remote Terminal Area

Remote computer facilities, peripheral devices, or terminals which are located outside the central computer facility. (*AR* 380-380; JCS PUB 6-03. 7)

#-Remote Terminal Protection Devices

This KSA has no definition.

Remotely Accessed Resource-Sharing Computer System

A computer system which includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more users, and which can be entered from terminals located outside the central computer facility. (DODD 5200. 28M;)

Removable Disk Media

Removable Storage Media

Storage media, such as a Bernoulli disk, that can be removed easily and transferred to a compatible system or secured.

Repair

The restoration of an item to serviceable condition through correction of a specific failure or unserviceable condition. (JCS1-DoD)

Repair Action

National Security Agency approved change to a COMSEC end item that does not affect the original characteristics of the end item and is provided for optional application by holders. NOTE: Repair actions are limited to minor electrical and/or mechanical improvements to enhance operation, maintenance, or reliability. They do not require an identification label, marking, or control, but must be fully documented by changes to the maintenance manual.

Repertory Dialer

Replacement Cost

A parameter indicating the amount required to replace the asset. (RM;)

*-Replicator

n. Any construct that acts to produce copies of itself; this could be a living organism, an idea (see meme), a program (see quine, worm, wabbit, fork bomb, and virus), a pattern in a cellular automaton (see life, sense 1), or (speculatively) a robot or nanobot. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator; see UNIX conspiracy.

Report

Represented Asset Value

A Parameter indicating the value of an Asset within the organisation as opposed to the Replacement Cost of the Data which represents the Asset. (MK;)

Reproducibility

See precision.

Repudiation

Denial by one of the entities involved in a communication of having participated in all or part of the communication. (SS;)

Request

See access request, ARQ, data transfer request signal, disengagement request, request data transfer.

Request Data Transfer

A signal sent by the DTE to the DCE to request the establishment of a data connection. See also call control signal, data, data circuit-terminating equipment, data terminal equipment, signal.

#-Requirements Traceability

Determine that the test plans and procedures cover all the security requirements of the security policy and system specifications. (Source: DACUM IV).

Resale Parameter

A parameter indicating the proportion of the replacement cost obtainable at the present time if the asset were sold. (RM;)

Rescind

Reserve Keying

Key held to satisfy unplanned material needs.

Reserve Keying Material

Key held to satisfy unplanned needs. See Contingency Key.

Reserved Word

In programming languages, a keyword whose definition is fixed by the programming language and which cannot be changed by the user. Note: In Ada® and COBOL all keywords are reserved words, while FORTRAN has no reserved words. (FP) (ISO)

Resident Memory

Section of the central processing unit that, during processing, holds program instructions, input data, calculation results, and data to be output. Also called internal storage, main memory, or primary memory.

Residual Risk

The portion of risk that remains after security measures have been applied. (*AFR* 205-16;; *NCSC-WA*-001-85;)

Residue

Data left in storage after processing operations and before degaussing or rewriting has taken place. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

Resource

1. Anything used or consumed while performing a function. The categories of resources are time, information, objects (information containers), or processors (the ability to use information). Specific examples are CPU time; terminal connect time; amount of directly addressable memory; disk space; number of I/O requests per minute, etc. (CSC-STD-001-83;)
2. In an ADP system, any function, device, or data collection that may be allocated to users or programs. (*FIPS PUB* 39;)

Resource Encapsulation

A resource must not be directly accessible by a subject but must be protected so that the reference monitor can properly mediate accesses to the resource. A requirement for accurate auditing of resource usage. (*NCSC-WA*-001-85;) NOTE: Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.

Resource Sharing

In an ADP system, the concurrent use of a resource by more than one user, job or program. (*FIPS PUB* 39;)

Resource-Sharing Computer System

A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and process co-resident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multiprogramming, multi-accessing, multi-processing, or concurrent processing. (DODD 5200. 28M;)

Response

1. A reply to a query. (~)
2. In data transmission, the content of the control field of a response frame advising the primary sta-

tion concerning the processing by the secondary station of one or more command frames.
3. The effect of an active or passive device upon an input signal. See also polling, response time.

Response Frame

In data transmission, all frames that may be transmitted by a secondary station. See also frame, secondary station.

Response Time

1. The time a system takes to react to a given input. (~) Note: If a message is keyed into a terminal by an operator and the reply from the computer, when it comes, is typed at the same terminal, response time may be defined as the time interval between the operator pressing the last key and the terminal typing the first letter of the reply.
2. In a data system, the elapsed time between the end of transmission of an enquiry message and the beginning of the receipt of a response message, measured at the enquiry originating station.
3; The time a functional unit takes to react to a given input. (~) See also overshoot, turnaround time.

Responsibilities

Responsibility

Restart

The resumption of the execution of a computer program using the data recorded at a checkpoint. (FP) (ISO) See also checkpoint.

Restitution

A series of significant conditions determined by the decisions taken according to the products of the demodulation process. (~) See also demodulation, detection.

Restricted Access

A class of service in which users may be denied access to one or more of the system features or operating levels. (~) See also access control, classmark, code restriction, controlled access, service feature.

Restricted Area

1. Those areas that contain Air Force resources designated a security priority and equates to the term “limited area” as specified in DODD 5210. 41 for areas containing nuclear weapons. (*AFR* 207-1)
2. Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property or material. (*AR* 380-380;; *NCSC-WA*-001-85;)
3. An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. For areas containing nuclear weapons, the term is synonymous with the Department of Defense term, “limited area “ as defined in *DOD* Directive 5210. 41. (*AFR* 205-16)
4. Controlled space is less than eight meters (25 feet), or does not meet controlled space attenuation requirements.

Restricted Data

All data concerning design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the restricted data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended. (DOE 5635. lA)

Restricted Service

See restricted access.

Restriction

1. See restricted access.
2. n. A bug or design error that limits a program's capabilities, and which is sufficiently egregious that nobody can quite work up enough nerve to describe it as a. Often used (esp. by types) to make it sound as though some crippling bogosity had been intended by the designers all along, or was forced upon them by arcane technical constraints of a nature no mere user could possibly comprehend (these claims are almost invariably false). Old-time hacker Joseph M. Newcomer advises that whenever choosing a quantifiable but arbitrary restriction, you should make it either a power of 2 or a power of 2 minus 1. If you impose a limit of 17 items in a list, everyone will know it is a random number -- on the other hand, a limit of 15 or 16 suggests some deep reason (involving 0- or 1-based indexing in binary) and you will get less for it. Limits which are round numbers in base 10 are always especially suspect.

*-Retcon

/ret'kon/ [short for `retroactive continuity', from the Usenet newsgroup rec. arts. comics]

1. n. The common situation in pulp fiction (esp. comics or soap operas) where a new story `reveals' things about events in previous stories, usually leaving the `facts' the same (thus preserving continuity) while completely changing their interpretation. For example, revealing that a whole season of “Dallas” was a dream was a retcon.
2. vt. To write such a story about a character or fictitious object. “Byrne has retconned Superman's cape so that it is no longer unbreakable. ” “Marvelman's old adventures were retconned into synthetic dreams. ” “Swamp Thing was retconned from a transformed person into a sentient vegetable. ” “Darth Vader was retconned into Luke Skywalker's father in “The Empire Strikes Back”. [This term is included because it is a good exam-

ple of hackish linguistic innovation in a field completely unrelated to computers. The word `retcon' will probably spread through comics fandom and lose its association with hackerdom within a couple of years; for the record, it started here. -- ESR] [1993 update some comics fans on the net now claim that retcon was independently in use in comics fandom before rec. arts. comics. In lexicography, nothing is ever simple. -- ESR]

*-RETI

v. Syn. RTI

Retrieval

1. In common-channel signaling, the procedure for guarding against the loss of signaling information when a signaling link fails and changeover is initiated. Note: Retrieval involves the retransmission of lost or mutilated messages.
2. In information processing, the act or process of recovering data or information from storage. (FP) See also common-channel signaling, link, out-of-band signaling.

Retrieval Function

In a data manipulation language, a capability to select and to locate stored records with specified characteristics and to transfer these records to a work area for any required further processing by an application program. (FP)

Retrieval Service

In ISDN applications, an interactive telecommunications service allowing access to and retrieval of stored information (a database).

Retro-Virus

A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state. (IC;)

*-Retrocomputing

/ret'-roh-k*m-pyoo'ting/ n. Refers to emulations of way-behind-the-state-of-the-art hardware or software, or implementations of never-was-state-of-the-art; esp. if such implementations are elaborate practical jokes and/or parodies, written mostly for hack value, of more `serious' designs. Perhaps the most widely distributed retrocomputing utility was the `pnch(6)' or `bcd(6)' program on V7 and other early UNIX versions, which would accept up to 80 characters of text argument and display the corresponding pattern in punched card code. Other well-known retrocomputing hacks have included the programming language INTERCAL, a JCL-emulating shell for UNIX, the card-punch-emulating editor named 029, and various elaborate PDP-11 hardware emulators and RT-11 OS emulators written just to keep an old, sourceless Zork binary running.

*-Return From The Dead

v. To regain access to the net after a long absence. Compare person of no account.

Revenue

Review And Approval

The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network. (*OPNAVINST* 5239. 1A;)

*-RFC

/R-F-C/ n. [Request For Comment] One of a long-established series of numbered Internet informational documents and standards widely followed by commercial software and freeware in the Internet and UNIX communities. Perhaps the single most influential one has been RFC-822 (the Internet mail-format standard). The RFCs are unusual in that they are floated by technical experts acting on their own initiative and reviewed by the Internet at large, rather than formally promulgated through an institution such as ANSI. For this reason, they remain known as RFCs even once adopted as standards. The RFC tradition of pragmatic, experience-driven, after-the-fact standard writing done by individuals or small working groups has important advantages over the more formal, committee-driven process typical of ANSI or ISO. Emblematic of some of these advantages is the existence of a flourishing tradition of `joke' RFCs; usually at least one a year is published, usually on April 1st. Well-known joke RFCs have included 527 ("ARPAWOCKY", R. Merryman, UCSD; 22 June 1973), 748 ("Telnet Randomly-Lose Option", Mark R. Crispin; 1 April 1978), and 1149 ("A Standard for the Transmission of IP Datagrams on Avian Carriers", D. Waitzman, BBN STC; 1 April 1990). The first was a Lewis Carroll pastiche; the second a parody of the TCP-IP documentation style, and the third a deadpan skewering of standards-document legalese, describing protocols for transmitting Internet data packets by carrier pigeon. The RFCs are most remarkable for how well they work -- they manage to have neither the ambiguities that are usually rife in informal specifications, nor the committee-perpetrated misfeatures that often haunt formal standards, and they define a network that has grown to truly worldwide proportions.

*-RFE

1. /R-F-E/ n. [techspeak] Request For Enhancement (compare RFC).
2. [from `Radio Free Europe', Bellcore and Sun] Radio Free Ethernet, a system (originated by Peter Langston) for broadcasting audio among Sun SPARCstations over the ethernet.

*-Rib Site

n. [by analogy with backbone site] A machine that has an on-demand high-speed link to a backbone site and serves as a regional distribution point for lots of third-party traffic in email and Usenet news. Compare leaf site, backbone site.

*-Rice Box

n. [from ham radio slang] Any Asian-made commodity computer, esp. an 80x86-based machine built to IBM PC-compatible ISA or EISA-bus standards.

*-Right Thing

n. That which is *compellingly* the correct or appropriate thing to use, do, say, etc. Often capitalized, always emphasized in speech as though capitalized. Use of this term often implies that in fact reasonable people may disagree. “What's the right thing for LISP to do when it sees `(mod a 0)'? Should it return `a', or give a divide-by-0 error?” Oppose Wrong Thing.

Ring Back

Procedure where connection to the computer requires two calls. The first, which usually is only one ring, alerts the modem, which will not answer unless the ringing stops for some period of time (typically 30 seconds). This allows the phone to be answered by the computer when appropriate and still be used for normal voice communications. (BBD;)

Risk

1. The loss potential that exists as the result of threat-vulnerability pairs. Reducing either the threat or the vulnerability reduces the risk. (*AFR* 205-16;; *AFR* 700-10;)
2. The uncertainty of loss expressed in terms of probability of such loss. (*AR* 380-380;)
3. The probability that a hostile entity will successfully exploit a particular telecommunications or COMSEC system for intelligence purposes; its factors are threat and vulnerability. (NCSC-9)
4. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact. (*AFR* 205-16)
5. the probability that a particular threat will exploit a particular vulnerability of the system. (NCSC-Td-004-88)

#-Risk Acceptance Process

Synonymous with Risk Management.

Risk Analysis

1. A part of risk management that is used to minimize risk by effectively applying security measures commensurate with the relative threats, vulnerabilities, and values of the resources to be protected. The value of the resources includes impact on the organization the automated system supports and the impact of the loss or unauthorized modification of data. Risk analysis consists of four modules: sensitivity assessment, risk assessment, economic assessment, and security test and evaluation. (*AFR* 205-16;; *AFR* 700-10;)
2. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. (*AR* 380-380;; *FIPS PUB* 39;)
3. The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. (*NCSC-WA*-001-85;; DODD 5200. 28;) See Risk Assessment.
4. A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios to determine the likelihood of compromise of protected information. See Risk Assessment. *An analysis of system assets and vulnerabilities to establish expected loss from certain events based on estimated probabilities of the occurrence of those events. (DOE, Glossary of Safeguards and Security, 8/87)
5. Synonymous with RISK ASSESSMENT.

Risk And Magnitude Of The Harm

Risk Assessment

1. A study of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. Managers use the results of a risk assessment to develop security requirements and specifications. (*AFR* 205-16)
2. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. (*AR* 380-380)
3. An identification of a specific ADP facility's assets, the threats to these assets, and the ADP facility's vulnerability to those threats. (DOE 5637. 1)
4. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level. (*OPNAVINST* 5239. 1 A)
5. A management tool which provides a systematic approach for determining the relative value and sensitivity of computer installation assets, assessing vulnerabilities, assessing loss expectancy or perceived risk exposure levels, assessing existing protection features and additional protection alternatives or acceptance of risks and documenting management decisions. Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and sensitiv-

ity/value of the assets to be protected. Risk assessments may vary from an informal review of a small scale microcomputer installation to a more formal and fully documented analysis (i. e. , risk analysis) of a large scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches. (*DOE 1360. 2A*)

Risk Index

1. The difference between the minimum clearance or authorization of AIS users and the maximum sensitivity (e. g. , classification and categories) of data processed by the AIS. (DODD 5200. 28; CSC-STD-004-85; CSC-STD-004-85)
2. The difference between the minimum clearance or authorization of system users and the maximum sensitivity (e. g. , classification and categories of data processed by a system. (*NCSC-TG*-004-88)

Risk Management

1. The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA approval. The process facilitates the management of security risks by each level of management throughout the system life cycle. The approval process consists of three elements: risk analysis, certification, and approval. (*AFR* 205-16; *AFR* 700-10)
2. An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases: a. Risk assessment, as derived from an evaluation of threats and vulnerabilities. b. Management decision. c. Control implementation. d. Effectiveness review. (*AR* 380-380)
3. The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review. (DODD 5200. 28)
4. The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. lt indudes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (*NCSC-TG*-0004-88)

*-Roach

vt. [Bell Labs] To destroy, esp. of a data structure. Hardware gets toasted or fried, software gets roached.

*-Robot

n. [IRC, MUD] An IRC or MUD user who is actually a program. On IRC, typically the robot provides some useful service. Examples are NickServ, which tries to prevent random users from adopting nicks already claimed by others, and MsgServ, which allows one to send asynchronous messages to be delivered when the recipient signs on. Also common are `annoybots', such as KissServ, which perform no useful function except to send cute messages to other people. Service robots are less common on MUDs; but some others, such as the `Julia' robot active in 1990--91, have been remarkably impressive Turing-test experiments, able to pass as human for as long as ten or fifteen minutes of conversation.

*-Robust

adj. Said of a system that has demonstrated an ability to recover gracefully from the whole range of exceptional inputs and situations in a given environment. One step below bulletproof. Carries the additional connotation of elegance in addition to just careful attention to detail. Compare smart, oppose brittle.

*-Rococo

adj. Terminally baroque. Used to imply that a program has become so encrusted with the software equivalent of gold leaf and curlicues that they have completely swamped the underlying design. Called after the later and more extreme forms of Baroque architecture and decoration prevalent during the mid-1700s in Europe. Alan Perlis said “Every program eventually becomes rococo, and then rubble. ” Compare critical mass.

*-Rogue

n. [UNIX] A Dungeons-and-Dragons-like game using character graphics, written under BSD UNIX and subsequently ported to other UNIX systems. The original BSD `curses(3)' screen-handling package was hacked together by Ken Arnold to support `rogue(6)' and has since become one of UNIX's most important and heavily used application libraries. Nethack, Omega, Larn, and an entire subgenre of computer dungeon games all took off from the inspiration provided by `rogue(6)'. See also nethack. room-temperature IQ quant. [IBM] 80 or below (nominal room temperature is 72 degrees Fahrenheit, 22 degrees Celsius). Used in describing the expected intelligence range of the luser. “Well, but how's this interface going to play with the room-temperature IQ crowd?” See drool-proof paper. This is a much more insulting phrase in countries that use Celsius thermometers.

#-Role-Based Access Controls

Synonymous with Discretionary access control (DAC).

#-Roles And Responsibilities

This KSA has no definition.

ROM

See Read-Only Memory. ()

*-Root

n. [UNIX]

1. The superuser account (with user name `root') that ignores permission bits, user number 0 on a UNIX system. The term avatar is also used.
2. The top node of the system directory structure (home directory of the root user).
3. By extension, the privileged system-maintenance login on any OS. See root mode, go root, see also wheel.

*-Root Mode

n. Syn. with wizard mode or `wheel mode'. Like these, it is often generalized to describe privileged states in systems other than OSes.

*-Rot13

/rot ther'teen/ n. ,v. [Usenet from `rotate alphabet 13 places'] The simple Caesar-cypher encryption that replaces each English letter with the one 13 places forward or back along the alphabet, so that “The butler did it!” becomes “Gur ohgyre qvq vg!” Most Usenet news reading and posting programs include a rot13 feature. It is used to enclose the text in a sealed wrapper that the reader must choose to open -- e. g. , for posting things that might offend some readers, or spoilers. A major advantage of rot13 over rot(N) for other N is that it is self-inverse, so the same code can be used for encoding and decoding.

*-Rotary Debugger

n. [Commodore] Essential equipment for those late-night or early-morning debugging sessions. Mainly used as sustenance for the hacker. Comes in many decorator colors, such as Sausage, Pepperoni, and Garbage. See pizza, ANSI standard.

*-Round Tape

n. Industry-standard 1/2-inch magnetic tape (7- or 9-track) on traditional circular reels. See macrotape, oppose square tape.

Routine

1. An APL function, a STAPLE function, or a STAPLE procedure. (ET;)
2. An APL function, a STAPLE function, or else a STAPLE procedure. (MA;)

Routing Control

The application of rules during the process of routing so as to chose or avoid specific networks, links or relays. (SS;)

*-RTBM

/R-T-B-M/ imp. [UNIX] Commonwealth Hackish variant of RTFM; expands to `Read The Bloody Manual'. RTBM is often the entire text of the first reply to a question from a newbie; the *second* would escalate to “RTFM”.

*-RTFAQ

/R-T-F-A-Q/ imp. [Usenet primarily written, by analogy with RTFM] Abbrev. for `Read the FAQ!', an exhortation that the person addressed ought to read the newsgroup's FAQ list before posting questions.

*-RTFB

/R-T-F-B/ imp. [UNIX] Acronym for `Read The Binary'. Used when neither documentation nor source for the problem at hand exists, and the only thing to do is use some debugger or monitor and directly analyze the assembler or even the machine code. “No source for the buggy port driver? Aaargh! I *hate* proprietary operating systems. Time to RTFB. ” Of the various RTF? forms, `RTFB' is the least pejorative against anyone asking a question for which RTFB is the answer; the anger here is directed at the absence of both source *and* adequate documentation.

*-RTFM

1. /R-T-F-M/ imp. [UNIX] Acronym for `Read The Manual'. Used by gurus to brush off questions they consider trivial or annoying. Compare Don't do that, then!.
2. Used when reporting a problem to indicate that you aren't just asking out of randomness. “No, I can't figure out how to interface UNIX to my toaster, and yes, I have RTFM. ” Unlike sense 1, this use is considered polite. See also FM, RTFAQ, RTFB, RTFS, RTM, all of which mutated from RTFM, and compare UTSL.

*-RTFS

1. /R-T-F-S/ [UNIX] imp. Acronym for `Read The Source'. Variant form of RTFM, used when the problem at hand is not necessarily obvious and not answerable from the manuals -- or the manuals are not yet written and maybe never will be. For even trickier situations, see RTFB. Unlike RTFM, the anger inherent in RTFS is not usually directed at the person asking the question, but rather at the people who failed to provide adequate documentation.
2. imp. `Read The Standard'; this oath can only be used when the problem area (e. g. , a language or operating system interface) has actually been codified in a ratified standards document. The existence of these standards documents (and the technically inappropriate but politically mandated compromises that they inevitably contain, and the impenetrable legalese in which they are invariably written, and the unbelievably tedious bureaucratic process by which they are produced) can be unnerving to hackers, who are used to a certain amount of ambiguity in the specifications of the

systems they use. (Hackers feel that such ambiguities are acceptable as long as the Right Thing to do is obvious to any thinking observer; sadly, this casual attitude towards specifications becomes unworkable when a system becomes popular in the Real World.) Since a hacker is likely to feel that a standards document is both unnecessary and technically deficient, the deprecation inherent in this term may be directed as much against the standard as against the person who ought to read it.

*-RTI

/R-T-I/ interj. The mnemonic for the `return from interrupt' instruction on many computers including the 6502 and 6800. The variant `RETI' is found among former Z80 hackers (almost nobody programs these things in assembler anymore). Equivalent to “Now, where was I?” or used to end a conversational digression. See pop; see also POPJ.

*-RTM

/R-T-M/ [Usenet abbreviation for `Read The Manual']

1. A more polite variant of RTFM.
2. Robert T. Morris Jr. , perpetrator of the great Internet worm of 1988 (see Great Worm, the); villain to many, naive hacker gone wrong to a few. Morris claimed that the worm that brought the Internet to its knees was a benign experiment that got out of control as the result of a coding error. After the storm of negative publicity that followed this blunder, Morris's username on ITS was hacked from RTM to RTFM.

*-RTS

/R-T-S/ imp. Acronym for `Read The Screen'. Mainly used by hackers in the microcomputer world. Refers to what one would like to tell the suit one is forced to explain an extremely simple application to. Particularly appropriate when the suit failed to notice the `Press any key to continue' prompt, and wishes to know `why won't it do anything'. Also seen as `RTFS' in especially deserving cases.

*-Rude

1. [WPI] adj. (of a program) Badly written.
2. Functionally poor, e. g. , a program that is very difficult to use because of gratuitously poor (random?) design decisions. Oppose cuspy.
3. Anything that manipulates a shared resource without regard for its other users in such a way as to cause a (non-fatal) problem. Examplesprograms that change tty modes without resetting them on exit, or windowing programs that keep forcing themselves to the top of the window stack. Compare all-elbows.

Rule

1. A heuristic which specifies a conclusion to assert and/or an action (operation on the knowledge base) to perform, when a specific condition is satisfied. (ET;)
2. A heuristic that specifies specifies a conclusion to assert or an action (an operation on the KB) to perform when a specific condition is satisfied. (MA;)

#-Rule Of Least Privilege

1. The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. (Source NCSC TG 004);
2. A program or process running in a computer should have the fewest capabilities (privileges) needed to execute.

Rule-Based Access Controls

Rule-Based Security Policy

A security policy based on global rules imposed for all users. these rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. (SS;)

#-Rules-Based Access Controls

Synonymous with Mandatory Access Control (MAC)

Run

1. The execution of one or more [computer] jobs or programs.
2. A performance of one or more [computer] programs. (FP) (ISO)

Run-Length Encoding

A redundancy-reduction technique for facsimile in which a run of consecutive picture elements having the same state (gray scale or color) is encoded into a single codeword. (~) See also code, facsimile.

*-Runes

1. pl. n. Anything that requires heavy wizardry or black art to parse core dumps, JCL commands, APL, or code in a language you haven't a clue how to read. Not quite as bad as line noise, but close. Compare casting the runes, Great Runes.
2. Special display characters (for example, the high-half graphics on an IBM PC).

*-Runic

adj. Syn. obscure. VMS fans sometimes refer to UNIX as `Runix'; UNIX fans return the compliment by expanding VMS to `Very Messy Syntax' or `Vachement Mauvais Syst`eme' (French idiom, “Hugely Bad System”).

*-Rusty Iron

n. Syn. tired iron. It has been claimed that this is the inevitable fate of water MIPS.

*-Rusty Memory

n. Mass-storage that uses iron-oxide-based magnetic media (esp. tape and the pre-Winchester removable disk packs used in washing machines). Compare donuts.

*-Rusty Wire

n. [Amateur Packet Radio] Any very noisy network medium, in which the packets are subject to frequent corruption. Most prevalent in reference to wireless links subject to all the vagaries of RF noise and marginal propagation conditions. “Yes, but how good is your whizbang new protocol on really rusty wire?”.

S

S

See second.

S Interface

For basic rate access in an ISDN environment, the S interface denotes a user-to-network interface reference point characterized by a four-wire, 144-kbps (2B+D) user rate. Note 1: As a universal interface between ISDN terminals or terminal adapters and the network channel termination, the S interface allows a variety of terminal types and subscriber networks (e. g. , PBXs, LANs, and controllers) to be connected to this type of network. Note 2: At the S interface, there are 4000 frames of 48 bits each, per second, for 192 kbps. The user's portion is 36 bits per frame, or 144 kbps. See also Integrated Services Digital Network, R interface, T interface, U interface.

*-Sacred

adj. Reserved for the exclusive use of something (an extension of the standard meaning). Often means that anyone may look at the sacred object, but clobbering it will mess up whatever it is sacred to. The comment “Register 7 is sacred to the interrupt handler” appearing in a program would be interpreted by a hacker to mean that if any *other* part of the program changes the contents of register 7, dire consequences are likely to ensue.

Safeguard

An entity (possibly a physical object, a procedure, or software) used to prevent, lessen the impact of, assist in the detection of or in the recovery from risks. (ET;)

Safeguarding

Statement affixed to a computer statement output or printout that states the highest classification being processed at the time the product was produced, and requires control of the product, at that level, until determination of the true classification by an authorized person.

Safeguarding Statement

1. A statement affixed to computer outputs which states the highest classification being processed in an automated system at the time product was produced and requiring its control at that level until a responsible person can determine its true classification. (*AR* 380-380; JCS PUB 6-03. 7)
2. See CAUTION STATEMENT.

Safeguards

See Security Safeguards.

#-Safety

This KSA has no definition.

*-Sagan

/say'gn/ n. [from Carl Sagan's TV series “Cosmos”; think “billions and billions”] A large quantity of anything. “There's a sagan different ways to tweak EMACS. ” “The U. S. Government spends sagans on bombs and welfare -- hard to say which is more destructive. ”

*-SAIL

1. /sayl/, not /S-A-I-L/ n. The Stanford Artificial Intelligence Lab. An important site in the early development of LISP; with the MIT AI Lab, BBN, CMU, XEROX PARC, and the UNIX community, one of the major wellsprings of technical innovation and hacker-culture traditions (see the WAITS entry for details). The SAIL machines were shut down in late May 1990, scant weeks after the MIT AI Lab's ITS cluster was officially decommissioned.
2. The Stanford Artificial Intelligence Language used at SAIL (sense 1). It was an Algol-60 derivative with a coroutining facility and some new data types intended for building search trees and association lists.

Salami Technique

In data security, pertains to a fraud spread over a large number of individual transactions, e. g. , a program which does not correctly round off figures but diverts the leftovers to a personal account. (MS;)

*-Salescritter

/sayls'kri`tr/ n. Pejorative hackerism for a computer salesperson. Hackers tell the following joke Q. What's the difference between a used-car dealer and a computer salesman? A. The used-car dealer knows he's lying. [Some versions add . and probably knows how to drive.] This reflects the widespread hacker belief that salescritters are self-selected for stupidity (after all, if they had brains and the inclination to use them, they'd

be in programming). The terms `salesthing' and `salesdroid' are also common. Compare marketroid, suit, droid.

Salt

(1) Strategic Arms Limitation Talks (Treaty) (2) n. A tiny bit of near-random data inserted where too much regularity would be undesirable; a data frob (sense 1). For example, the Unix crypt(3) man page mentions that "the salt string is used to perturb the DES algorithm in one of 4096 different ways. "

*-Salt Mines

n. Dense quarters housing large numbers of programmers working long hours on grungy projects, with some hope of seeing the end of the tunnel in N years. Noted for their absence of sunshine. Compare playpen, sandbox.

*-Salt Substrate

n. [MIT] Collective noun used to refer to potato chips, pretzels, saltines, or any other form of snack food designed primarily as a carrier for sodium chloride. From the technical term `chip substrate', used to refer to the silicon on the top of which the active parts of integrated circuits are deposited.

*-Same-Day Service

n. Ironic term used to describe long response time, particularly with respect to MS-DOS system calls (which ought to require only a tiny fraction of a second to execute). Such response time is a major incentive for programmers to write programs that are not well-behaved. See also PC-ism.

*-Samizdat

n. [Russian, literally "self publishing"] The process of disseminating documentation via underground channels. Originally referred to photocopy duplication and distribution of banned books in the former Soviet Union; now refers by obvious extension to any less-than-official promulgation of textual material, esp. rare, obsolete, or never-formally-published computer documentation. Samizdat is obviously much easier when one has access to high-bandwidth networks and high-quality laser printers. Note that samizdat is properly used only with respect to documents which contain needed information (see also hacker ethic, the) but which are for some reason otherwise unavailable, but *not* in the context of documents which are available through normal channels, for which unauthorized duplication would be unethical copyright violation. See Lions Book for a historical example.

Sample Key

Key intended for off-the-air demonstration use only.

*-Samurai

n. A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith. In 1991, mainstream media reported the existence of a loose-knit culture of samurai that meets electronically on BBS systems, mostly bright teenagers with personal micros; they have modeled themselves explicitly on the historical samurai of Japan and on the "net cowboys" of William Gibson's cyberpunk novels. Those interviewed claim to adhere to a rigid ethic of loyalty to their employers and to disdain the vandalism and theft practiced by criminal crackers as beneath them and contrary to the hacker ethic; some quote Miyamoto Musashi's "Book of Five Rings", a classic of historical samurai doctrine, in support of these principles. See also Stupids, social engineering, cracker, hacker ethic, the, and dark-side hacker.

*-Sandbender

n. [IBM] A person involved with silicon lithography and the physical design of chips. Compare ironmonger, polygon pusher.

*-Sandbox

1. n. (also `sandbox, the') Common term for the R&D department at many software and computer companies (where hackers in commercial environments are likely to be found). Half-derisive, but reflects the truth that research is a form of creative play. Compare playpen.
2. Syn. link farm.
3. A portion of memory set aside for Java programs

Sanitization

The elimination of classified information from magnetic media to permit the reuse of the media at a lower classification level or to permit the release to uncleared personnel or personnel without the proper information access authorizations. (DOE 5636. 2A;)

Sanitize

1. To erase or overwrite classified data stored on magnetic media for the purpose of declassifying the media. (CSC-STD-005-85;)
2. To remove sensitive data so that the remaining data is of a lower sensitivity than the original aggregate. (*NCSC-WA*-001-85;)

Sanitizing

The degaussing or overwriting of sensitive information in magnetic or other storage media. (*FIPS PUB* 39; *AR* 380-380)

Synonymous with SCRUBBING.

*-Sanity Check

1. n. The act of checking a piece of code (or anything else, e. g. , a Usenet posting) for completely stupid mistakes. Implies that the check is to make sure

the author was sane when it was written; e. g. , if a piece of scientific software relied on a particular formula and was giving unexpected results, one might first look at the nesting of parentheses or the coding of the formula, as a `sanity check', before looking at the more complex I/O or data structure manipulation routines, much less the algorithm itself. Compare reality check.

2. A run-time test, either validating input or ensuring that the program hasn't screwed up internally (producing an inconsistent value or state).

#-Satellite Communications Security

This KSA has no definition.

*-Saturday-Night Special

n. [from police slang for a cheap handgun] A quick-and-dirty program or feature kluged together during off hours, under a deadline, and in response to pressure from a salescritter. Such hacks are dangerously unreliable, but all too often sneak into a production release after insufficient review.

*-Say

1. vt. To type to a terminal. “To list a directory verbosely, you have to say `ls -l'. ” Tends to imply a newline-terminated command (a `sentence').
2. A computer may also be said to `say' things to you, even if it doesn't have a speech synthesizer, by displaying them on a terminal in response to your commands. Hackers find it odd that this usage confuses mundanes.

*-Scag

vt. To destroy the data on a disk, either by corrupting the filesystem or by causing media damage. “That last power hit scagged the system disk. ” Compare scrog, roach.

Scanner

A device that examines a spatial pattern, one part after another, and generates analog or digital signals corresponding to the pattern. Note: Scanners are often used in mark sensing, pattern recognition, or character recognition. (FP) (ISO) (~) See also facsimile, scanning, simple scanning.

Scanning

1. In telecommunication systems, periodic examination of the traffic activity to determine whether further processing is required.
2. In television, facsimile, and picture transmission, the process of analyzing successively the colors and densities of the subject copy according to the elements of a predetermined pattern. (~)
3. The process of tuning a device through a predetermined range of frequencies in prescribed increments and times (regular or random). (~)
4. Scanning is accomplished by sequentially going through combinations of numbers and letters to look for access to telephone numbers and secret passwords. (TC)
5. See EXHAUSTIVE ATTACK

Scanning Line

The path traversed by a scanning spot during a single line sweep.

Scanning Line Frequency

In facsimile, the frequency at which a fixed line perpendicular to the direction of scanning is crossed by a scanning spot. (~) Note: This is equivalent to drum speed in some mechanical systems. See also facsimile, frequency, scanning, stroke speed.

Scanning Line Length

In facsimile systems, the total length of a scanning line, equal to the spot speed divided by the scanning line frequency. (~) Note: This is generally greater than the length of the available line. See also dead sector, facsimile, scanning, spot speed.

Scanning Pitch

The distance between the centers of consecutive scanning lines. See also facsimile, scanning.

Scanning Rate

In facsimile and television systems, the rate of displacement of the scanning spot along the scanning line. (~) See also facsimile, scanning.

Scanning Spot

In facsimile systems, the area on the subject copy covered instantaneously by the pickup system of the scanner. (~) See also elemental area, facsimile, raster scanning, scanning.

*-Scanno

/skan'oh/ n. An error in a document caused by a scanner glitch, analogous to a typo or thinko.

Scavenging

1. Searching through residue for the purpose of unauthorized data acquisition. (*FIPS PUB* 39;; *AR* 380-380;)
2. Searching through object residue to acquire unauthorized data. (*NCSC-WA*-001-85;)

Scenario

1. A description of an event indicating how the event is envisaged as occurring. (RM;)
2. A natural language description of an event. (MK;)

Scenario Analysis

An information systems vulnerability assessment technique in which various possible attack methods are identified and the existing controls are examined in light of their ability to counter such attack methods. (WB;)

Schematic

A diagram that details the electrical elements of a circuit or system. See also circuit, system.

*-Schroedinbug

/shroh'din-buhg/ n. [MIT from the Schroedinger's Cat thought-experiment in quantum physics] A design or implementation bug in a program that doesn't manifest until someone reading source or using the program in an unusual way notices that it never should have worked, at which point the program promptly stops working for everybody until fixed. Though (like bit rot) this sounds impossible, it happens; some programs have harbored latent schroedinbugs for years. Compare heisenbug, Bohr bug, mandelbug.

*-Science-Fiction Fandom

n. Another voluntary subculture having a very heavy overlap with hackerdom; most hackers read SF and/or fantasy fiction avidly, and many go to `cons' (SF conventions) or are involved in fandom-connected activities such as the Society for Creative Anachronism. Some hacker jargon originated in SF fandom; see defenestration, great-wall, cyberpunk, h, ha ha only serious, IMHO, mundane, neep-neep, Real Soon Now. Additionally, the jargon terms cowboy, cyberspace, de-rezz, go flatline, ice, phage, virus, wetware, wirehead, and worm originated in SF stories.

Scientific And Technical Information

(STI) Communicable knowledge or information resulting from or pertaining to the conduct and management of R&E efforts. STI is used by administrators, managers, scientists, and engineers engaged in scientific and technological efforts and is the basic intellectual resource for the result of such effort. (*DODD 3200. 12*;; DODD 5230. 24;) (Unknown)

Scientific And Technical Intelligence

Intelligence concerning developments in basic and applied scientific and technical research and development, including engineering and production techniques, new technology, and weapon systems and their capabilities and characteristics. *Intelligence concerning foreign developments in basic and applied scientific and technical research and development, including engineering and production techniques, new technology, and weapon systems and their capabilities and characteristics; it also includes intelligence which requires scientific or technical expertise on the part of the analyst, such as medicine, physical health studies, and behavioral analyses. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

SCOMP

Secure Communications Processor. The name given to the Honeywell Level 6 Minicomputer modified to increase its protection capability. Four protection rings were added along with user-initiated input/output to direct-memory access devices. (MTR-8201;) See Secure Communications Processor.

*-Scram Switch

n. [from the nuclear power industry] An emergency-power-off switch (see Big Red Switch), esp. one positioned to be easily hit by evacuating personnel. In general, this is *not* something you frob lightly; these often initiate expensive events (such as Halon dumps) and are installed in a dinosaur pen for use in case of electrical fire or in case some luckless field servoid should put 120 volts across himself while Easter egging. (See also molly-guard, TMRC.)

*-Scratch

1. [from `scratchpad'] adj. Describes a data structure or recording medium attached to a machine for testing or temporary-use purposes; one that can be scribbled on without loss. Usually in the combining forms `scratch memory', `scratch register', `scratch disk', `scratch tape', `scratch volume'. See also scratch monkey.
2. [primarily IBM] vt. To delete (as in a file).

*-Scratch Monkey

n. As in “Before testing or reconfiguring, always mount a scratch monkey”, a proverb used to advise caution when dealing with irreplaceable data or devices. Used to refer to any scratch volume hooked to a computer during any risky operation as a replacement for some precious resource or data that might otherwise get trashed. This term preserves the memory of Mabel, the Swimming Wonder Monkey, star of a biological research program at the University of Toronto. Mabel was not (so the legend goes) your ordinary monkey; the university had spent years teaching her how to swim, breathing through a regulator, in order to study the effects of different gas mixtures on her physiology. Mabel suffered an untimely demise one day when a DEC engineer troubleshooting a crash on the program's VAX inadvertently interfered with some custom hardware that was wired to Mabel. It is reported that, after calming down an understandably irate customer sufficiently to ascertain the facts of the matter, a DEC troubleshooter called up the field circus manager responsible and asked him sweetly, “Can you swim?” Not all the consequences to humans were so amusing; the sysop of the machine in question was nearly thrown in jail at the behest of certain clueless droids at the local `humane' society. The moral is clear When in doubt, always mount a scratch monkey. [The actual incident occured in 1979 or 1980. There is a version of this story, complete with reported dialogue between one of the project people and DEC field service, that has been circulating on Internet since 1986. It is hilarious and mythic, but gets some facts wrong. For example, it reports the machine as a PDP-11 and alleges that Mabel's demise

occurred when DEC PMed the machine. Earlier versions of this entry were based on that story; this one has been corrected from an interview with the hapless sysop. -- ESR]

Scratch Pad Store

(SPS) Momentary key storage in crypto-equipment.

*-Scream And Die

v. Syn. cough and die, but connotes that an error message was printed or displayed before the program crashed.

*-Screaming Tty

n. [UNIX] A terminal line which spews an infinite number of random characters at the operating system. This can happen if the terminal is either disconnected or connected to a powered-off terminal but still enabled for login; misconfiguration, misimplementation, or simple bad luck can start such a terminal screaming. A screaming tty or two can seriously degrade the performance of a vanilla UNIX system; the arriving "characters" are treated as userid/password pairs and tested as such. The UNIX password encryption algorithm is designed to be computationally intensive in order to foil brute-force crack attacks, so although none of the logins succeeds; the overhead of rejecting them all can be substantial.

*-Scribble

n. To modify a data structure in a random and unintentionally destructive way. "Bletch! Somebody's disk-compactor program went berserk and scribbled on the i-node table. " "It was working fine until one of the allocation routines scribbled on low core. " Synonymous with trash; compare mung, which conveys a bit more intention, and mangle, which is more violent and final.

*-Scrog

/skrog/ vt. [Bell Labs] To damage, trash, or corrupt a data structure. "The list header got scrogged. " Also reported as `skrog', and ascribed to the comic strip "The Wizard of Id". Compare scag; possibly the two are related. Equivalent to scribble or mangle.

*-Scrool

/skrool/ n. [from the pioneering Roundtable chat system in Houston ca. 1984; prob. originated as a typo for `scroll'] The log of old messages, available for later perusal or to help one get back in synch with the conversation. It was originally called the `scrool monster', because an early version of the roundtable software had a bug where it would dump all 8K of scrool on a user's terminal.

*-Scrozzle

/skroz'l/ vt. Used when a self-modifying code segment runs incorrectly and corrupts the running program or vital data. "The compiler scrozzled itself again!"

Scrubbing

Synonymous with SANITIZING.

*-Scruffies

n. See neats vs. scruffies.

*-SCSI

n. [Small Computer System Interface] A bus-independent standard for system-level interfacing between a computer and intelligent devices. Typically annotated in literature with `sexy' (/sek'see/), `sissy' (/sis'ee/), and `scuzzy' (/skuh'zee/) as pronunciation guides -- the last being the overwhelmingly predominant form, much to the dismay of the designers and their marketing people. One can usually assume that a person who pronounces it /S-C-S-I/ is clueless.

*-ScumOS

/skuhm'os/ or /skuhm'O-S/ n. Unflattering hackerism for SunOS, the UNIX variant supported on Sun Microsystems's UNIX workstations (see also sun-stools), and compare AIDX, Macintrash, Nominal Semidestructor, Open DeathTrap, HP-SUX. Despite what this term might suggest, Sun was founded by hackers and still enjoys excellent relations with hackerdom; usage is more often in exasperation than outright loathing.

*-Search-And-Destroy Mode

n. Hackerism for a noninteractive search-and-replace facility in an editor, so called because an incautiously chosen match pattern can cause infinite damage.

Second

In the International System of Units (SI), the time interval equal to 9,192,631,770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the atom of cesium-133. (~) See also cesium clock, cesium standard, Coordinated Universal Time, DoD master clock, International Atomic Time.

*-Second-System Effect

n. (sometimes, more euphoniously, `second-system syndrome') When one is designing the successor to a relatively small, elegant, and successful system, there is a tendency to become grandiose in one's success and design an elephantine feature-laden monstrosity. The term was first used by Fred Brooks in his classic " The Mythical Man-Month Essays on Software Engineering" (Addison-Wesley, 1975; ISBN 0-201-00650-2). It described the jump from a set of nice, simple operating systems on the IBM 70xx series to OS/360 on the 360 series. A similar effect can also happen in an evolving system; see Brooks's Law, creeping elegance, creeping featurism. See also Multics, OS/2, X, software bloat. This version of the jar-

gon lexicon has been described (with altogether too much truth for comfort) as an example of second-system effect run amok on jargon-1.

Secondary Channel

A data transmission channel having a lower signaling rate capacity than the primary channel in a system in which two channels share a common interface. See also channel, primary channel.

*-Secondary Damage

n. When a fatal error occurs (esp. a segfault) the immediate cause may be that a pointer has been trashed due to a previous fandango on core. However, this fandango may have been due to an *earlier* fandango, so no amount of analysis will reveal (directly) how the damage occurred. “The data structure was clobbered, but it was secondary damage. ” By extension, the corruption resulting from N cascaded fandangoes on core is `Nth-level damage'. There is at least one case on record in which 17 hours of grovelling with `adb' actually dug up the underlying bug behind an instance of seventh-level damage! The hacker who accomplished this near-superhuman feat was presented with an award by his fellows.

Secondary Distribution

Release of technical documents provided after primary distribution. It includes loaning, allowing the reading of, or releasing a document outright, in whole or in part. (DODD 5230. 24;)

Secondary RED Conductor

Any conductor, other than primary RED, which connects to RED equipment, the RED side of crypto-equipment, or the RED of isolation devices, which does not intentionally carry national security information; but because the coupling mechanism with the RED equipment might carry compromising information, is designated secondary RED (e. g. , indicator lines, control lines, timing lines, etc.). Power distribution panels and grounding systems serving RED wire lines and equipments may also be so designated.

Secondary Station

Secretary Of Commerce

Secretary Of Defense

Secretary Of State

Sector

A predetermined, addressable angular part of a track or a band on a magnetic drum or magnetic disk.

Secure Communications

1. Telecommunications which are effectively secured against hostile exploitation by COMSEC equipment and/or protected distribution systems.
2. Telecommunications deriving security through use of type 1 products and/or protected distribution systems. See Protected Communications.

Secure Communications Processor

(SCOMP) The name given to the Honeywell I Level 6 Minicomputer modified to increase its protection capability. Four protection rings were added along with user-initiated input/output to direct memory access devices. (MTR-8201)

Secure Configuration Management

1. The set of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that such changes will not lead to decreased data security. (*AR* 380-380; *FIPS PUB* 39)
2. The set of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy. (*NCSC-TG*-004-88)

Secure Operating System

1. An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system. (*FIPS PUB* 39;; *AR* 380-380;)
2. Resident software that controls hardware and other software functions in an AIS to provide a level of protection or security appropriate to the classification, sensitivity, and, or criticality of the data and resources it manages. (AF MAN 33-270)

Secure Path

See TRUSTED PATH.

Secure State

1. A known, intended condition through the use of protected or trusted software. In periods processing, the secure state may be reached by booting the controlled copy of the operating system at the beginning of each session. (*AFR* 205-16;)
2. A condition where no subject can access any object in an unauthorized manner. (*NCSC-WA*-001-85;)

Secure Subsystem

A subsystem that contains its own implementation of the reference monitor concept for those resources it controls. However, the secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects. (*NCSC-WA*-001-85;)

#-Secure System Operations

Resident software that controls hardware and other software functions in an AIS to provide a level of protection or security appropriate to the classification, sensitivity, and/or criticality of the data and resources it manages. (Source: NSTISSI 4009).

Secure Telecommunications And Information Handling Equipment

Equipment designed to secure telecommunications and information handling media by converting information to a form unintelligible to an unauthorized interceptor and by reconverting the information to its original form for authorized recipients. Such equipments, employing a classified cryptographic logic, may be stand-alone crypto-equipments, as well as telecommunications and information handling equipments with integrated or embedded cryptography. (NTISSI 400 1)

Secure Telephone Unit

(STU) A U. S. Government-approved telecommunication terminal designed to protect the transmission of sensitive or classified information in the voice, data, and facsimile modes.

Secure Working Area

An accredited facility which is used for handling, discussing, or processing sensitive defence information. (*AR* 380-380;; *NCSC-WA*-001-85;)

Security

1. The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure. The term is also applied to those measures necessary to achieve this condition and to the organizations responsible for those measures. (JCS1-NATO)
2. Measures taken by a military unit, an activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JCS1-DoD)
3. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JCS1-DoD)
4. With respect to classified matter, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (JCS1-DoD)
5. Precautions taken to establish and maintain an acceptable level of protection. *Establishment and maintenance of protective measures that are intended to ensure a state of inviolability from hostile acts or influences. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)
5. See also ADD-ON SECURITY, ADMINISTRATIVE SECURITY, COMMUNICATIONS SECURITY, DATA SECURITY, EMANATION SECURITY, PERSONNEL SECURITY, PHYSICAL SECURITY, PROCEDURAL SECURITY, TELEPROCESSING SECURITY, and TRAFFIC FLOW SECURITY.

Security Administrator

The AIS administrative personnel shall only be able to perform Security Administrator functions after taking a distinct auditable action to assume the Security Administrator role on the AIS. Nonsecurity functions that can be performed in the Security Administrator role shall be limited strictly to those essential to performing the security role effectively. ”

Security Advisory/information Memorandum

Security And Privacy Advisory Board

#-Security Architecture

A detailed description of all aspects of the system that relate to security. along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements. (NOTE: a security architecture is basically an architectural overlay that addresses security. It is increasingly important in distributed systems, since there are many ways in which security functions can be distributed and care is needed to ensure that they work together.) (Source: *NCSC-TG*- 029).

Security Area

A physically defined space containing classified matter (documents or material) subject to physical protection and personnel access controls. (DOE 5636. 2A;)

Security Audit

1. An examination of data security procedures and measures for the purpose of evaluating their adequacy and compliance with established policy. (*FIPS PUB* 39;)
2. An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. (SS;)

Security Audit Trail

Data collected and potentially used to facilitate a security audit. (SS;)

#-Security Awareness

This KSA has no definition.

Security Awareness And Training

Security Breach

A violation of controls of a particular information system such that information assets or system components are unduly exposed. (WB;)

Security Classification Guide

SCG

Security Cost Benefit Analysis

A detailed study of security measures, their technical and operational feasibility, and their associated costs and benefits.

Security Countermeasures

Countermeasures that are aimed at specific threats and vulnerabilities (operations security procedures; camouflage, concealment, and other denial techniques) or involve more active techniques (counter-imagery programs, counter-SIGINT operations, and telecommunications and computer security) as well as activities traditionally perceived as security.

Security Criteria

The set of requirements that should be met to provide a maximum degree of effective protection at the lowest possible cost based on a risk assessment. *The set of requirements that should be met so the security system can provide a maximum degree of effective deterrence at the lowest cost which satisfies the system specifications. (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

Security Critical

Security mechanisms which require correct operation to make sure security policy is enforced. The mechanisms may or may not be part of the trusted computing base. (*AFR* 205-16)

Security Critical Mechanisms

Those security mechanisms whose correct operation necessary to ensure the security policy is enforced. The mechanisms may or may not be part of the Trusted Computing Base. (*NCSC-WA*-001-85;; *AFR* 205-16;)

Security Design Review

A review process where the objective is to ascertain that implemented protective measures meet the original overall system design and approved computer application security requirements. The security design review may be a separate activity or an integral function of the overall application system design review activity. (*DOE 1360. 2A*)

Security Directives

NTISS Directives establish national level decisions relating to NTISS policies, plans, programs, systems, or organizational delegations of authority. NTISSDs are promulgated by the Executive Agent of the Government for Telecommunications and Information Systems Security, or by the Chairman of the NTISSC when so delegated by the Executive Agent. NTISSDs are binding upon all federal departments and agencies. (*NCSC-WA*-001-85;)

#-Security Domains

1. The sets of objects that a subject has the ability to access. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).
2. (Class B3) Advanced Trusted Computing Base (TCB) which provides highly effective Discretionary Access Controls (DAC) and Mandatory Access Controls (MAC). Significant security and software engineering must be accomplished during the design, implementation, and testing phases to achieve the required level of confidence, or trust. Operational support features extend auditing capabilities as well as other functions needed for a trusted system recovery. (F:\NEWDEFS. TXT) (Class B3) Advanced Trusted Computing Base (TCB) which provides highly effective Discretionary Access Controls (DAC) and Mandatory Access Controls (MAC). Significant security and software engineering must be accomplished during the design, implementation, and testing phases to achieve the required level of confidence, or trust. Operational support features extend auditing capabilities as well as other functions needed for a trusted system recovery.

#-Security Education

This KSA has no definition.

Security Engineering

See Data Protection Engineering.

Security Environment

Environmental security factors, in a specific location, which keep a system from being exploited or deactivated.

Security Evaluation

1. One of two types of evaluations done to assess the degree of trust that can be placed in Automated Information Systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing an Automated Information System's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process. (*NCSC-WA*-001-85;)
2. A product, system, or procedural evaluation performed to assess the degree of confidence that can

be placed in the protective measures in place. *A product evaluation or a system evaluation performed to assess the degree of trust that can be placed in an automated information system for the secure handling of sensitive information. (NSA, *National INFOSEC Glossary*, 10/88)

Security Fault Analysis

(SFA) A security analysis, usually performed on hardware at the gate level, to determine the security properties of a device when a hardware fault is encountered. (*NCSC-WA*-001-85;)

Security Features

1. The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e. g. , identification, authentication, audit trail, access control). (DODD 5200. 28)
2. The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards. (*NCSC-TG*-004-88)

Security Features Users' Guide

(SFUG).

Security Filter

1. A set of software routines and techniques employed in ADP systems to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons. (*FIPS PUB* 39;)
2. A secure subsystem that enforces security policy on the data that passes through it. (*NCSC-WA*-001-85;)

Security Flaw

An error of commission or omission in a system that may allow protection mechanisms to be bypassed. See Flaw.

Security Flow Analysis

1. A type of security analysis performed on a non-procedural formal system specification which locates potential flows of information between system variables. By assigning security levels to system variables, many indirect information channels can be identified. Security flow analysis defines a security model similar to the access control model (Bell La Padula) but with a finer protection granularity. (MTR-8201)
2. A security analysis performed on a formal system specification that locates potential flows of information within the system. (*NCSC-TG*-004-88)

#-Security Functional Testing

Validate that the system provides the required security features. If the system connects to a network or another system, security of both. (Source: DACUM IV).

Security Incident

1. Any act or circumstance that involves classified informationthat deviates from the requirements of governing security publications, for example, compromise, possible compromise, inadvertent disclosure, and deviation. (*AR* 380-380;; *AFR* 205-16;)
2. An event involving protected information or a facility in which there is a deviation from the requirements of the governing security regulations. *An incident involving classified information in which there is a deviation from the requirements of the governing security regulations. NOTE: Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents. (NSA, *National INFOSEC Glossary*, 10/88)

Security Inspection

An examination of an ADP system to determine compliance with ADP security policy, procedures, and practices. (*OPNAVINST* 5239. 1A;; *NCSC-WA*-001-85;)

#-Security Inspections

1. Examination of an AIS to determine compliance with security policy, procedures, and practices. (NSTISSI 4009);
2. The ISSO must perform periodic inspections of the systems in order to assess and report the status to the DAA. (DACUM IV).

Security Interest

Consists of any of the following which requires special protection: classified matter, special nuclear material, security shipments, secure communications center, sensitive compartmented information facilities, automatic data processing centers, or other systems including classified information, or departmental property. (DOE 563 5. 1 A)

Security Kernel

1. The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct. (CSC-STD-001-85; *NCSC-WA*-001-85;)
2. The central part of a computer system (software and hardware) that implements the fundamental security procedures for controlling access to system resources. (*FIPS PUB* 39;)
3. A localized mechanism, composed of hardware and software, that controls the access of users (and processes executing on their behalf) to repositories of information resident in or connected to the system. The correct operation of the kernel along with any associated trusted processes should be

sufficient to guarantee enforcement of the constraints on access. TCBs have been implemented using security kernels along with trusted processes. (MTR-8201;)

Security Label

Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable non-hierarchical security categories (e. g. , sensitive compartmented information, critical nuclear weapon design information).

Security Level

The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information. (CSC-STD-001-83;; *NCSC-WA*-001-85;) See Access Level and Category.

Security Measures

1. Elements of software, firmware, hardware, or procedures included in the system to satisfy security specifications. (*AFR* 205-16)
2. Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications. (*NCSC-TG*-004-88)

Security Mechanisms

Security Mode

1. A mode of operation in which the DAA accredits an AIS to operate. inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the system. (DODD 5200. 28)
2. A secure mode of operation in which the approving authority accredits a system to operate. Inherent within each of the security modes are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, environmental restrictions, and the range of sensitive information permitted on the system. (*NCSC-TG*-004-88)

Security Module

A shielded and self-contained microcomputer-based device that securely stores security parameters, and that automatically erases such parameters if the device is tampered with. (WB;)

Security Officer

The ADP official, described in OMB Circular A-71, Transmittal Memorandum Number 1 (July 27, 1978), having the designated responsibility for the security of an ADP system. (*FIPS PUB* 112;)

Security Officers

See Network Security Officer (NSO).

Security Parameters

The variable secret components that control security processes. Examples include passwords, encryption keys, encryption initialization vectors, pseudo-random number generator seeds, and biometric identity parameters. (WB;)

Security Perimeter

1. The boundary where security controls are in effect to protect assets. (*NCSC-WA*-001-85;)
2. Synonymous with Control Zone.

Security Policy

1. The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (*DOD* 5200. 28-STD)
2. The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (*NCSC-TG*-004-88) Note: a complete security policy will necessarily address many concerns which are outside of the scope of OSI. (SS;)

Security Policy Model

1. An informal presentation of a formal security policy model. (*DOD* 5200. 28-STD)
2. A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information. See Bell-LaPadula model and formal security policy model (*NCSC-TG*-004-88)
3. See BELL LAPADULA MODEL, FORMAL SECURITY POLICY MODEL, POLICY and SECURITY POLICY.

#-Security Product Integration

This KSA has no definition.

#-Security Product Testing/Evaluation

An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system. (Source: *NCSC-TG*-0004).

#-Security Products

Hardware, firmware, software or procedures that may be included in a system to meet security specifications. (Source panel of experts).

Security Range

The highest and lowest security levels that are permitted in/on an Automated Information System or network. (*NCSC-WA*-001-85;)

Security Relevant Event

Any event that attempts to change the security state of the system (e. g. , change discretionary access controls, change the security level of the subject, change user password, etc.). Also, any event that attempts to violate the security policy of the system (e. g. , too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.). (DODD 5200. 28-STD;)

Security Relevant Portion

Security Requirements

1. Types and levels of protection necessary for equipment, data, information, applications, and facilities. (*AFR* 205-16)
2. The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (*NCSC-TG*-004-88)

Security Requirements Baseline

1. A description of minimum requirements provided for a system to maintain an acceptable level of security. The baseline does not necessarily constitute one document but may be an accumulation of the security requirements stated in several documents such as SONs, SOWs, ISRDs, and others. (*AFR* 205-16;)
2. A description of minimum requirements necessary for a system to maintain an acceptable level of security. (*NCSC-WA*-001-85;)

Security Requirements For Automatic Information Systems (AISs)

#-Security Reviews

Aperiodic reviews of the rules and practices that regulate how a system manages, protects and distributes information. (Source Panel of experts).

Security Safeguards

1. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. (DODD 5200-28)
2. The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas and devices. Also called safeguards. (*NCSC-TG*-004-88)

Security Service

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers. (SS;)

Security Specification

Detailed description of the safeguards required to protect an AIS.

Security Specifications

1. A detailed description of the safeguards required to protect a sensitive application. (A-130;)
2. Detailed descriptions of the measures required for protection according to security requirements. Applicable requirements for Air Force policies, publications, and standards are addressed. (*AFR* 205-16;)
3. A detailed description of the safeguards required to protect an Automated Information System. (*NCSC-WA*-001-85;)
4. A detailed description of the countermeasures required to protect an ADP activity or network from unauthorized (accidental or unintentional) disclosure, modification, and destruction of data, or denial of service. (*OPNAVINST* 5239. 1A;)

#-Security Staffing Requirements

This KSA has no definition.

Security Test And

Examination and analysis of the evaluation safeguards required to protect an AIS, as they have been applied in an operational environment, to determine the security posture of that system.

Security Test And Evaluation

1. (ST&E) The process to determine that the system administrative, technical, and physical security measures are adequate; to document and report test findings to appropriate authorities; and to make recommendations based on test results. ST&E may be an integral part of other tests and evaluations. Managers must ensure changes made to correct one problem do not adversely affect other previously tested security measures. (*AFR* 205-16; *OPNAVINST* 5239. l A)
2. An examination and analysis of the security features of an operational automated system to develop evidence upon which an accreditation can be based. (*AR* 380-380; JCS PUB 6-03. 7)
3. An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system. (*NCSC-TG*-004-88)

Security Testing

A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification. (CSC-STD-001-83;; *NCSC-WA*-001-85;)

Security Threat

The technical and operational capability of an adversary to detect and exploit vulnerabilities.

*-Security Through Obscurity

(alt. `security by obscurity') A term applied by hackers to most OS vendors' favorite way of coping with security holes -- namely, ignoring them, documenting neither any known holes nor the underlying security algorithms, trusting that nobody will find out about them and that people who do find out about them won't exploit them. This “strategy” never works for long and occasionally sets the world up for debacles like the RTM worm of 1988 (see Great Worm, the), but once the brief moments of panic created by such events subside most vendors are all too willing to turn over and go back to sleep. After all, actually fixing the bugs would siphon off the resources needed to implement the next user-interface frill on marketing's wish list -- and besides, if they started fixing security bugs customers might begin to *expect* it and imagine that their warranties of merchantability gave them some sort of *right* to a system with fewer holes in it than a shotgunned Swiss cheese, and *then* where would we be? Historical note There are conflicting stories about the origin of this term. It has been claimed that it was first used in the Usenet newsgroup in comp. sys. apollo during a campaign to get HP/Apollo to fix security problems in its UNIX-clone Aegis/DomainOS (they didn't change a thing). ITS fans, on the other hand, say it was coined years earlier in opposition to the incredibly paranoid Multics people down the hall, for whom security was everything. In the ITS culture it referred to (1) the fact that by the time a tourist figured out how to make trouble he'd generally gotten over the urge to make it, because he felt part of the community; and (2) (self-mockingly) the poor coverage of the documentation and obscurity of many commands. One instance of *deliberate* security through obscurity is recorded; the command to allow patching the running ITS system (altmode altmode control-R) echoed as $$^D. If you actually typed alt alt ^D, that set a flag that would prevent patching the system even if you later got it right.

#-Security Training

This KSA has no definition.

Security Violation

An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. (WB;)

#-Security Violations Reporting Process

This KSA has no definition.

Security-Relevant Event

Security-Relevant Functions

*-SED

n. [TMRC, from `Light-Emitting Diode'] /S-E-D/ Smoke-emitting diode. A friode that lost the war. See also LER.

Seed Key

Initial key used to start an updating or key generation process.

Seek

To position selectively the access mechanism of a direct access [storage] device. (FP)

Seek Time

The time required for the access arm of a direct-access storage device to be positioned on the appropriate track. (FP) (ISO) See positioning time.

Seepage

The accidental flow to unauthorized individuals of data or information, access to which is presumed to be controlled by computer security safeguards. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

*-Segfault

n. ,vi. Syn. segment, segmentation fault.

*-Seggie

/seg'ee/ n. [UNIX] Shorthand for segmentation fault reported from Britain.

*-Segment

/seg'ment/ vi. To experience a segmentation fault. Confusingly, this is often pronounced more like the noun `segment' than like mainstream v. segment; this is because it is actually a noun shorthand that has been verbed.

*-Segmentation Fault

1. n. [UNIX] An error in which a running program attempts to access memory not allocated to it and core dumps with a segmentation violation error.
2. To lose a train of thought or a line of reasoning. Also uttered as an exclamation at the point of befuddlement.

Segmented Encoding Law

An encoding law in which an approximation to a smooth law is obtained by a number of linear seg-

ments. See piece-wise linear encoding. See also code, encoding law.

Segments

Segregation

See privacy (def. #1).

*-Segv

/seg'vee/ n. ,vi. Yet another synonym for segmentation fault (actually, in this case, `segmentation violation').

Selective Field Protection

The protection of specific fields within a message which is to be transmitted. (SS;)

Self-Authentication

Implicit authentication, to a predetermined level, of all transmissions on a secure communications system.

Self-Certification

*-Self-Reference

n. See self-reference.

*-Selvage

/sel'v*j/ n. [from sewing and weaving] See chad (sense 1).

*-Semi

1. /se'mee/ or /se'mi:/ n. Abbreviation for `semicolon', when speaking. “Commands to grind are prefixed by semi-semi-star” means that the prefix is `;;*', not 1/4 of a star.
2. A prefix used with words such as `immediately' as a qualifier. “When is the system coming up?” “Semi-immediately. ” (That is, maybe not for an hour.) “We did consider that possibility semi-seriously. ” See also infinite.

*-Semi-Infinite

n. See infinite.

Sender

A device that accepts address information from a register or routing information from a translator, and then transmits the proper routing digits to a trunk or to local equipment. Note: Sender and register functions are often combined in a single unit. (~) See also address.

*-Sendmail

n. The standard UNIX mail agent; written by Eric Allman. It is very flexible, but has very hairy configuration syntax and has had numerous security bugs, because it's a large, monolithic program which needs to run with suid root privileges. See also bug-of-the-month club and Great Worm, The.

*-Senior Bit

n. [IBM] Syn. meta bit.

Sensitive

Information contained in the Military Critical Technologies List, information which could be useful to a hostile agent in the development of countermeasures, information which could involve new or high technology, information which could involve key indicators of operational capabilities which could be used by hostile agents to determine operational capabilities, weaknesses, and wartime missions. (*AFR* 700-10;)

Sensitive Application

An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application. (A-130;)

Sensitive Business Data

Data which requires protection under Title 18, USC 1905, and other data which, by its nature, requires controlled distribution or access for reasons other than that it is classified or personal data. Sensitive business data is recognized in the following categories. 9) For Official Use Only “ Requiring confidentiality of information derived from Inspector General, authority, or other investigative activity. b) Financial “ Requiring protection to ensure the integrity of funds or other fiscal assets. c) Sensitive Management “ Requiring protection to defend against the loss of property, material, or supplies or to defend against the disruption of operations or normal management practices, etc. d) Proprietary “ Requiring protection to protect data or information in conformance with a limited rights agreement or which is the exclusive property of a civilian corporation or individual and which is on loan to the Government for evaluation or for its proper use in adjudicating contracts. e) Privileged “ Requiring protection for conformance with business standards or as required by law. (Example: Government developed information involving the award of a contract.) (*OPNAVINST* 5239. 1A;)

Sensitive But Unclassified

Sensitive Compartmented Information

1. (SCI) Classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence. (DODD 5200. 28)
2. All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These

special Community controls are formal systems of restricted access established to protect the sensitive aspects of intelligence sources and methods and analytical procedures of foreign intelligence programs. The term does not include restricted data as defined in Section 11, Public Law 585, Atomic Energy Act of 1954, as amended. (*DCID* 1/1 6; *DCID* 1/1 6, Sup. ; NACSI M 5203; DOE 5635. lA)

Sensitive Compartmented Information Facility

(SCIF) An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed, and/or processed. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Sensitive Compartmented Intelligence

(SCI) Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is established. (*AR* 380-380)

Sensitive Data

1. Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability to accomplish a mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (A-130)
2. Data designated by a knowledgeable authority to require protection because its unauthorized disclosure, alteration, loss, or destruction could cause damage. It includes both classified and sensitive unclassified data. (*AFR* 205-16)

Sensitive Defence Information

Any information which requires a degree of protection and which should not be made generally available. This type of information includes, but is not limited to that information which must be safeguarded so as to: 9) Prevent damage to national defence and which usually bears a security classification. b) Assure the individual privacy of U. S. citizens as provided by the Privacy Act of 1974. c) Maintain the confidentiality of FOUO information derived from the Inspector General, an audit, or other investigative activities such as medical or other jurisprudence or disciplinary information derived from records of doctor/patient or lawyer/client relationships. d) Protect funds, supplies, and material from theft, fraud, misappropriation, or misuse. This includes asset or resource accounting or systems or operations which are involved in the control and distribution of funds or the processing of information which offers the opportunity to divert economically valuable resources. e) Protect proprietary information which is the exclusive property of an individual or corporation. This proprietary information may be on loan, leased, or purchased by the Government or made available to the Government for its proper use, to include evaluating or adjudicating contracts. f) Protect Government developed privileged information involving the award of contracts. g) Protect information which the commander considers essential for mission accomplishment. (*AR* 380-380;)

Sensitive Defense Information

Any information which requires a degree of protection and which should not be made generally available. This type of information includes, but is not limited to, that information which must be safeguarded as to: a. Prevent damage to national defense and which usually bears a security classification. b. Assure the individual privacy of U. S. citizens as provided by the Privacy Act of 1974. c. Maintain the confidentiality for FOUO information derived from the Inspector General, an audit, or other investigative activities such as medical or other jurisprudence or disciplinary information derived from records of doctor/patient or lawyer/client relationships. d. Protect funds, supplies, and material from theft, fraud, misappropriation, or misuse. This includes asset or resource accounting or systems or operations which are involved in the control and distribution of funds or the processing of information which offers the opportunity to divert economically valuable resources. e. Protect proprietary information which is the exclusive property of an individual or corporation. This proprietary information may be on loan, leased, or purchased by the government or made available to the government for its proper use, to include evaluating or adjudicating contracts. f. Protect government-developed privileged information involving the award of contracts. g. Protect information which the commander considers essential for mission accomplishment. (*AR* 380-380)

Sensitive Information

1. Any information which requires a degree of protection and which should not be made generally available. (*FIPS PUB* 39)
2. Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. (*DOD* 5200. 28-STD; CSC-STD-003-85; CSC-STD-004-85)
3. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a Of title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria estab-

lished by an executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (PL 100-235)

4. Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U. S. Code, but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy. (*NCSC-TG*-004-88)
5. See SENSITIVE UNCLASSIFIED INFORMATION.

Sensitive Nuclear Material Production Information

a. Classified production rate or stockpile quantity information relating to plutonium, tritium, enriched lithium-6 and uranium-235 and 233. b. Laser separation technology. (DOE 563 5. 1 A)

Sensitive Software

Any data processing software that could bypass, penetrate, or damage data processing security controls. (*AR* 380-380;)

#-Sensitive System

An AIS which processes, stores or transmits sensitive data. (Source panel of experts).

Sensitive Unclassified Information

1. Plain text or machine-encoded data that, as determined by competent authority (e. g. , information owners), has relative sensitivity and requires mandatory protection because of statutory or regulatory restrictions (e. g. , unclassified controlled nuclear information, Official Use Only Information, Privacy Act information) or requires a degree of discretionary protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect national or other DOE interests (e. g. , program critical information, or controlled scientific and technical information which may include computer codes (computer programs) used to process such information). (*DOE 1360. 2A*)
2. Any information, the loss, misuse, or unauthorized access to, or modification of which, adversely might affect U. S. national interest, the conduct of *DOD* programs, or the privacy of *DOD* personnel (e. g. , FOIA exempt information and information whose distribution is limited by DODD 5230. 24). (DODD 5200. 28)
3. Information that requires protection due to the risk and magnitude of harm or loss that could result from unauthorized disclosure, alteration, loss, or destruction. The term includes records about individuals requiring protection under the Privacy Act, proprietary data, information not releasable under the Freedom of Information Act, and *DOD* and Air Force data that affects the mission. (*AFR* 205. 16)

Sensitivity

The characteristic of a resource which implies its value or importance, and may include its vulnerability. (SS;)

Sensitivity And Criticality

A method developed to describe the value of an information system by taking into account the cost, capability, and jeopardy to mission accomplishments or human life associated with the system. (*AFR* 700-10;)

Sensitivity And Criticality Assessment

Study to determine the value of a computer system by taking into account the cost, capability, and jeopardy to mission accomplishment or human life associated with the system.

Sensitivity Assessment

A study of the data to determine level of protection required. (*AFR* 205-16;)

Sensitivity Label

A piece of information that represents the security level of an object and that describes the sensitivity (e. g. , classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions. (CSC-STD-001-83;; *DCID* 1/16-1, Sup. ;; *NCSC-WA*-001-85;)

Sensitivity Level

Sensor

1. A device that responds to a physical stimulus (such as heat, light, sound, pressure, magnetism, or a particular motion) and produces a resulting signal.
2. An equipment which detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected, or modified by objects. (JCS1-DoD) (JCS1-NATO) See also active sensor, passive sensor.

Sentinel

See flag.

#-Separation Of Duties

Separation Of Privilege

The separation of functions, namely between the commands, programs, and interfaces implementing those functions, such that malicious or erroneous code in one function is prevented from affecting the code or data of another function.

Sequence
An arrangement of items according to a specified set of rules, for example, items arranged alphabetically, numerically, or chronologically. (FP) See also automatic sequential connection, bit-sequence independence, flag sequence.

Sequential Access
See serial access.

Sequential Logic Element
A device that has at least one output channel and one or more input channels, all characterized by discrete states, such that the state of each output channel is determined by the previous states of the input channels. (FP)

Serial
1. Pertaining to a process in which all events occur one after the other; for example, the serial transmission of the bits of a character according to the CCITT V. 25 protocol. (FP) (ISO)
2. Pertaining to the sequential or consecutive occurrence of two or more related activities in a single device or channel. (FP)
3. Pertaining to the sequential processing of the individual parts of a whole, such as the bits of a character or the characters of a word, using the same facilities for successive parts. (FP) See also parallel processing.
4. An element or a group of elements within a series which is given a numerical or alphabetical designation for convenience in planning, scheduling, and control. (JCS1-DoD) (JCS1-NATO)

Serial Access
1. Pertaining to the sequential or consecutive transmission of data to or from storage. (~)
2. That process wherein data are obtained from a storage device or are entered into a storage device in such a way that the process depends on the location of those data and on a reference to data previously accessed. Synonym sequential access. See also access, data communication control procedure.

Serial Digital Computer
A digital computer in which the digits are handled serially. Note: The bits that comprise a digit may be handled either serially or in parallel.

Serial Transmission
The sequential transmission of the signal elements of a group representing a character or other entity of data. (FP) (ISO) See sequential transmission. See also data communication control procedure, data stream, parallel transmission.

Serial-To-Parallel Converter
A digital device that accepts a single time sequence of signal elements and distributes them among multiple parallel outputs. (~) See staticizer. See also parallel-to-serial converter.

Serializer
See parallel-to-serial converter.

*-Server
n. A kind of daemon that performs a service for the requester and which often runs on a computer other than the one on which the server runs. A particularly common term on the Internet, which is rife with `name servers', `domain servers', `news servers', `finger servers', and the like.

Service
An asset category consisting of the coordinated interaction of all other assets (may involve a synergistic element - the amount by which the value of the service exceeds the sum of the values of the individual assets). (RM;)

Service Feature

Service Interruption Hazard
Probability that an action may occur which would have a detrimental effect on the operational integrity of a system.

Services
Includes any service, test, inspection, repair, training, publication, technical or other assistance, or defence information used to furnish military assistance, including military education and training activities. (DODD 2040. 2;)

Session
An activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of loggoff). (*DCID* 1/16-1, Sup. ;)

Session Layer
See Open Systems Interconnection--Reference Model.

Session Security Level
The security level of a session is the low water mark of the security levels of the user, the terminal, a level specified by the user, and the system from which the session originates. (*DCID* 1/16-1, Sup. ;)

Set
1. A finite or infinite number of objects, entities, or concepts, that have a given property or properties in common. (FP) (ISO)
2. To put all or part of a device into a specified state.

Seven-Bit Byte
See septet.

Severity

A measure of the degree of damage suffered as the result of an event; may be expressed as a percentage of the impacted assets or as a time interval. (RM;)

*-SEX

/seks/ [Sun Users' Group & elsewhere] n.

1. Software EXchange. A technique invented by the blue-green algae hundreds of millions of years ago to speed up their evolution, which had been terribly slow up until then. Today, SEX parties are popular among hackers and others (of course, these are no longer limited to exchanges of genetic software). In general, SEX parties are a Good Thing, but unprotected SEX can propagate a virus.
2. The rather Freudian mnemonic often used for Sign EXtend, a machine instruction found in the PDP-11 and many other architectures. The RCA 1802 chip used in the early Elf and SuperElf personal computers had a `SEt X register' SEX instruction, but this seems to have had little folkloric impact. DEC's engineers nearly got a PDP-11 assembler that used the `SEX' mnemonic out the door at one time, but (for once) marketing wasn't asleep and forced a change. That wasn't the last time this happened, either. The author of “The Intel 8086 Primer”, who was one of the original designers of the 8086, noted that there was originally a `SEX' instruction on that processor, too. He says that Intel management got cold feet and decreed that it be changed, and thus the instruction was renamed `CBW' and `CWD' (depending on what was being extended). Amusingly, the Intel 8048 (the microcontroller used in IBM PC keyboards) is also missing straight `SEX' but has logical-or and logical-and instructions `ORL' and `ANL'. The Motorola 6809, used in the U. K. 's `Dragon 32' personal computer, actually had an official `SEX' instruction; the 6502 in the Apple II with which it competed did not.

*-Sex Changer

n. Syn. gender mender.

Sexadecimal

See hexadecimal.

Sextet

A byte composed of six binary elements. (FP) (ISO) See six-bit byte.

*-Shambolic Link

/sham-bol'ik link/ n. A UNIX symbolic link, particularly when it confuses you, points to nothing at all, or results in your ending up in some completely unexpected part of the filesystem.

*-Shar File

n. Syn. sharchive.

*-Sharchive

/shar'ki:v/ n. [UNIX and Usenet; from /bin/sh archive] A flattened representation of a set of one or more files, with the unique property that it can be unflattened (the original files restored) by feeding it through a standard UNIX shell; thus, a sharchive can be distributed to anyone running UNIX, and no special unpacking software is required. Sharchives are also intriguing in that they are typically created by shell scripts; the script that produces sharchives is thus a script which produces self-unpacking scripts, which may themselves contain scripts. (The downsides of sharchives are that they are an ideal venue for Trojan horse attacks and that, for recipients not running UNIX, no simple un-sharchiving program is possible; sharchives can and do make use of arbitrarily-powerful shell features.) Sharchives are also commonly referred to as `shar files' after the name of the most common program for generating them.

*-Share And Enjoy!

1. imp. Commonly found at the end of software release announcements and README files, this phrase indicates allegiance to the hacker ethic of free information sharing (see hacker ethic, the, sense 1).
2. The motto of the Sirius Cybernetics Corporation (the ultimate gaggle of incompetent suits) in Douglas Adams's “Hitch Hiker's Guide to the Galaxy”. The irony of using this as a cultural recognition signal appeals to freeware hackers.

Shareware

Software freely distributed with the understanding that users will voluntarily pay for it if they continue to use it after a short (typically 30 days) trial period. Shareware is not synonymous with freeware. See Freeware and Public Domain Software.

Sharing

Sharing Of Software

*-Shelfware

/shelfweir/ n. Software purchased on a whim (by an individual user) or in accordance with policy (by a corporation or government agency), but not actually required for any particular use. Therefore, it often ends up on some shelf.

Shell

In a computer environment, an operating system's command interpreter; the part of the operating system that reads an input and performs the appropriate operation.

*-Shell Out

n. [UNIX] To spawn an interactive subshell from within a program (e. g. , a mailer or editor). “Bang

foo runs foo in a subshell, while bang alone shells out. ”

Shielded Enclosure

An area (room or box) specifically designed to attenuate electromagnetic radiation and/or acoustic emanation, which may originate either inside or outside the area. (NACSEM 5201; NACSIM 5203)

#-Shielded Enclosures

Room or container designed to attenuate electromagnetic radiation. (Source: NSTISSI 4009).

*-Shift Left (or Right) Logical

[from any of various machines' instruction sets]

1. vi. To move oneself to the left (right). To move out of the way.
2. imper. “Get out of that (my) seat! You can shift to that empty one to the left (right). ” Often used without the `logical', or as `left shift' instead of `shift left'. Sometimes heard as LSH /lish/, from the PDP-10 instruction set. See Programmer's Cheer.

Shift Register

1. A register in which shifts are performed. (FP) (ISO)
2. A storage device in which a serially ordered set of data may be moved, as a unit, into a discrete number of storage locations. (~) Note 1: Shift registers may be configured so that the stored data may be moved in more than one direction. Note 2: Shift registers may be configured so that data may be entered (stored) from multiple inputs. Note 3: Shift registers may be grouped into arrays of two or more dimensions in order to perform more complex data operations. See also data, M-sequence, register, shift.

*-Shim

n. A small piece of data inserted in order to achieve a desired memory alignment or other addressing property. For example, the PDP-11 UNIX linker, in split I&D (instructions and data) mode, inserts a two-byte shim at location 0 in data space so that no data object will have an address of 0 (and be confused with the C null pointer). See also loose bytes.

*-Short Card

n. A half-length IBM XT expansion card or adapter that will fit in one of the two short slots located towards the right rear of a standard chassis (tucked behind the floppy disk drives). See also tall card.

Short Range Plan

A documented, tactical (1 year) plan describing the implementation of the Classified Computer Security Program. (DOE 5637. 1)

Short Title

Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and control. NOTE: NAG-16C/TSEC is an example of a short title.

*-Shotgun Debugging

n. The software equivalent of Easter egging; the making of relatively undirected changes to software in the hope that a bug will be perturbed out of existence. This almost never works, and usually introduces more bugs.

Shoulder Surfing

The stealing of passwords by watching users sign on to systems at their terminals [.]. (TC;)

*-Shovelware

/shuh'v*l-weir`/ n. Extra software dumped onto a CD-ROM or tape to fill up the remaining space on the medium after the software distribution it's intended to carry, but not integrated with the distribution.

*-Showstopper

n. A hardware or (especially) software bug that makes an implementation effectively unusable; one that absolutely has to be fixed before development can go on. Opposite in connotation from its original theatrical use, which refers to something stunningly *good*.

*-Shriek

n. See excl. Occasional CMU usage, also in common use among APL fans and mathematicians, especially category theorists.

*-Shub-Internet

/shuhb in't*r-net/ n. [MUD from H. P. Lovecraft's evil fictional deity `Shub-Niggurath', the Black Goat with a Thousand Young] The harsh personification of the Internet, Beast of a Thousand Processes, Eater of Characters, Avatar of Line Noise, and Imp of Call Waiting; the hideous multi-tendriled entity formed of all the manifold connections of the net. A sect of MUDders worships Shub-Internet, sacrificing objects and praying for good connections. To no avail -- its purpose is malign and evil, and is the cause of all network slowdown. Often heard as in “Freela casts a tac nuke at Shub-Internet for slowing her down. ” (A forged response often follows along the lines of “Shub-Internet gulps down the tac nuke and burps happily. ”) Also cursed by users of FTP and TELNET when the system slows down. The dread name of Shub-Internet is seldom spoken aloud, as it is said that repeating it three times will cause the being to wake, deep within its lair beneath the Pentagon.

*-Sidecar

1. n. Syn. slap on the side. Esp. used of add-ons for the late and unlamented IBM PCjr.

2. The IBM PC compatibility box that could be bolted onto the side of an Amiga. Designed and produced by Commodore, it broke all of the company's own design rules. If it worked with any other peripherals, it was by magic.
3. More generally, any of various devices designed to be connected to the expansion slot on the left side of the Amiga 500 (and later, 600 & 1200), which included a hard drive controller, a hard drive, and additional memory.

*-SIG

/sig/ n. (also common as a prefix in combining forms) A Special Interest Group, in one of several technical areas, sponsored by the Association for Computing Machinery; well-known ones include SIGPLAN (the Special Interest Group on Programming Languages), SIGARCH (the Special Interest Group for Computer Architecture) and SIGGRAPH (the Special Interest Group for Computer Graphics). Hackers, not surprisingly, like to overextend this naming convention to less formal associations like SIGBEER (at ACM conferences) and SIGFOOD (at University of Illinois).

*-Sig Block

/sig blok/ n. [UNIX; often written `. sig' there] Short for `signature', used specifically to refer to the electronic signature block that most UNIX mail- and news-posting software will automagically append to outgoing mail and news. The composition of one's sig can be quite an art form, including an ASCII logo or one's choice of witty sayings (see sig quote, fool file, the); but many consider large sigs a waste of bandwidth, and it has been observed that the size of one's sig block is usually inversely proportional to one's longevity and level of prestige on the net. See also doubled sig.

*-Sig Quote

/sig kwoht/ n. [Usenet] A maxim, quote, proverb, joke, or slogan embedded in one's sig block and intended to convey something of one's philosophical stance, pet peeves, or sense of humor. “Calm down, it's only ones and zeroes. ”

*-Sig Virus

n. A parasitic meme embedded in a sig block. There was a meme plague or fad for these on Usenet in late 1991. Most were equivalents of “I am a . sig virus. Please reproduce me in your . sig block. ”. Of course, the . sig virus's memetic hook is the giggle value of going along with the gag; this, however, was a self-limiting phenomenon as more and more people picked up on the idea. There were creative variants on it; some people stuck `sig virus antibody' texts in their sigs, and there was at least one instance of a sig virus eater.

Signal

1. Detectable transmitted energy that can be used to carry information. (~)
2. A time-dependent variation of a characteristic of a physical phenomenon, used to convey information.
3. As applied to electronics, any transmitted electrical impulse. (JCS1-DoD) (JCS1-NATO)
4. Operationally, a type of message, the text of which consists of one or more letters, words, characters, signal flags, visual displays, or special sounds, with prearranged meanings and which is conveyed or transmitted by visual, acoustical, or electrical means. (JCS1-DoD) (JCS1-NATO)
5. A fluctuating quantity, such as voltage, current, electrical field strength, sound pressure level, etc. , the variations of which convey information.

Signal Intelligence

See signals intelligence.

Signal Security

A generic term that includes both communications security and electronic security. (JCS1-DoD) See also electronic warfare, TEMPEST.

*-Signal-To-Noise Ratio

[from analog electronics] n. Used by hackers in a generalization of its technical meaning. `Signal' refers to useful information conveyed by some communications medium, and `noise' to anything else on that medium. Hence a low ratio implies that it is not worth paying attention to the medium in question. Figures for such metaphorical ratios are never given. The term is most often applied to Usenet newsgroups during flame wars. Compare bandwidth. See also coefficient of X, lost in the noise.

Signals Intelligence

1. (SIGINT) A category of intelligence information comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. (JCS1-DoD) See also electronics intelligence, electronic warfare.
2. (SIGINT) Intelligence information derived from signals interception. *Intelligence information derived from signals intercept comprising, either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Signals Security

Generic term encompassing communications security and electronic security. (NSA, *National INFOSEC Glossary*, 10/88)

Signature

See Pattern.

Significant Change

A change in an unclassified computer installation which could impact overall processing requirements and conditions or installation security requirements (e. g. , adding a local area network; changing from batch to online processing; adding dial-up capability; carrying out major hardware configuration upgrades; operating system changes; making change to the physical installation; or changing installation location). (*DOE 1360. 2A*)

Significant Computer Security Incident

1. The occurrence of an event which would be of concern to senior DOE management due to potential for public interest or embarrassment to the organization, or potential for occurring at other DOE sites; these events would include such things as unauthorized access, theft, an interruption to computer service or protective controls, an incident involving damage, a disaster, or discovery of a vulnerability. (*DOE 1360. 2A*)
2. See COMPUTER SECURITY INCIDENT

Significant Condition

See significant instant.

Significant Digit

In a numeral, a digit that is needed for a given purpose; in particular, a digit that must be kept to preserve a given accuracy or a given precision. (FP) (ISO)

Significant Instant

In a time-plot of a signal, such as a time-plot of a pulsed electromagnetic wave, an instant at which a particular type of a usually repetitive event occurs, such as a transition to another significant condition, such as a different electric field strength, power level, polarization, frequency, or phase in a modulated wave. (~) Note: The significant conditions are those recognized by an appropriate device. Each of the significant instants is determined at the moment the appropriate device assumes a condition or state usable for performing a specific function, such as recording, processing, or gating. See also decision instant, significant interval, start-stop distortion.

Significant Modification

Any modification to the facility or system that impacts the operation or affects the security measures of the system. Determination of impact is a subjective evaluation and depends on the environment where the system operates. (*AFR* 205-16;)

Significant Risk Of Telecommunications Exploitation

Exists (a) when information of high value to an adversary may be handled by the telecommunication system and (b) when there is a high potential threat to or a readily exploitable vulnerability in the system. (NCSC-1 1)

SIGNIN

See LOGON.

SIGNON

See LOGON.

SIGSEC Signals Analysis

Analysis of the external signal parameters of U. S. official electronic emissions. *Analysis of the external signal parameters of U. S. official electronic emissions. NOTE: This analysis includes the identification of signals anomalies that might be exploited by an adversary SIGINT effort. (NSA, *National INFOSEC Glossary*, 10/88)

*-Silicon

n. Hardware, esp. ICs or microprocessor-based computer systems (compare iron). Contrasted with software. See also sandbender.

*-Silly Walk

vi. [from Monty Python's Flying Circus]

1. A ridiculous procedure required to accomplish a task. Like grovel, but more random and humorous. “I had to silly-walk through half the /usr directories to find the maps file. ”
2. Syn. fandango on core.

*-Silo

n. The FIFO input-character buffer in an RS-232 line card. So called from DEC terminology used on DH and DZ line cards for the VAX and PDP-11, presumably because it was a storage space for fungible stuff that went in at the top and came out at the bottom.

*-Silver Book

n. Jensen and Wirth's infamous “Pascal User Manual and Report”, so called because of the silver cover of the widely distributed Springer-Verlag second edition of 1978 (ISBN 0-387-90144-2). See book titles, Pascal.

Simple Buffering

A technique for assigning buffer storage for the duration of the execution of a computer program. (FP) (ISO) See also buffer (def. #1).

Simple Scanning

In facsimile transmission, scanning using only one spot at a time. (~) See also facsimile, scanner, scanning (def. #2).

Simple Security

Bell-La Padula security model rule property allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

Simple Security Condition

1. A Bell LaPadula-security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object. (*DOD* 5200. 28-STD)
2. Synonymous with SIMPLE SECURITY PROPERTY.
3. See SIMPLE SECURITY PROPERTY. (*NCSC-TG*-004-88)

Simple Security Property

A Bell-LaPadula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object. Also called simple security condition. (*NCSC-TG*-004-88)

Simplex Operation

1. Operating method in which transmission occurs in only one preassigned direction. See one-way operation. (~)
2. Deprecated definition: A mode of operation in which communications between two terminals takes place in either direction, but only one direction at a time. Note: This type of operation may occur only on simplex circuits as defined in simplex circuit (def. #2) above.
3. . Operating method in which transmission is made possible alternately in each direction of a telecommunication channel, for example by means of manual control. Note: In general, duplex operation and semiduplex operation require two frequencies in radiocommunication; simplex operation may use either one or two. (RR) CAUTION: These three definitions are contradictory; however, all are in common use--the first two are used in telephony; the last one, in radio. The user is cautioned to verify the nature of the service specified by this term. See also duplex circuit, duplex operation, half-duplex circuit, half-duplex operation, one-way communication, one-way-only channel, phantom circuit, simplex circuit, simplex signaling.

Simulate

To represent certain features of the behavior of a physical or abstract system by the behavior of another system, for example, to use delay lines to represent the propagation delay and phase shift of an actual transmission path. (After FP) Note: The simulator imitates one or more of the operations and functions of the unit it simulates. It is not, however, a complete functional equivalent. For example, a cockpit simulator imitates flight parameters, but does not fly. Contrast with emulate.

*-Since Time T Equals Minus Infinity

adv. A long time ago; for as long as anyone can remember; at the time that some particular frob was first designed. Usually the word `time' is omitted. See also time T; contrast epoch.

Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI)

A *DOD* special access program. (DODD 5200. 28)

Single Point Keying

(SPK) Means of distributing key to multiple, local crypto-equipment or devices from a single fill point.

#-Single Sign-On

A method by which a user must identify him/herself and present their credentials only once to a system. Information needed by future system to grant access to resources will be forwarded by the initial system signed on by the user.

Single-Level Device

A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, sensitivity labels do not have to be stored with the data being processed. (CSC-STD-001-83;; *NCSC-WA*-001-85;)

Single-User Hosts

Host computers (e. g. , intelligent terminals) that perform processing for only one user at a time (this does not preclude multiple users overtime). (JCS PUB 6-03. 7)

#-Site

(1) DODIIS SITE: An administrative grouping of a combination of DoD intelligence information systems accredited and managed collectively on the basis of geographical or organizational boundaries. Therefore, each DoDIIS Site contains multiple DoD intelligence information systems which support the sites intelligence mission. A DoDIIS Site must have the following characteristics: (1) One or more Sensitive Compartmented Information Facilities (SCIFs); (2) An established AIS security management structure, including the appointment of a Site ISSO; (3) An established AIS management process, with the appropriate CM procedures; (4) A DoDIIS Core Product or Key Project installed; and (5) Recognition as a DoDIIS Site by the appropriate DoD component authorities. (Source: DIAM 50-4).

*-Sitename

/si:t'naym/ n. [UNIX/Internet] The unique electronic name of a computer system, used to identify it in UUCP mail, Usenet, or other forms of electronic information interchange. The folklore interest of sitenames stems from the creativity and humor they often display. Interpreting a sitename is not unlike interpreting a vanity license plate; one has to mentally unpack it, allowing for mono-case and length restrictions and the lack of whitespace. Hacker tradition deprecates dull, institutional-sounding names in favor

of punchy, humorous, and clever coinages (except that it is considered appropriate for the official public gateway machine of an organization to bear the organization's name or acronym). Mythological references, cartoon characters, animal names, and allusions to SF or fantasy literature are probably the most popular sources for sitenames (in roughly descending order). The obligatory comment when discussing these is Harris's Lament “All the good ones are taken!” See also network address.

Six-Bit Byte

See sextet.

*-Skrog

v. Syn. scrog.

*-Skulker

n. Syn. prowler.

*-Slab

1. [Apple] n. A continuous horizontal line of pixels, all with the same color.
2. vi. To paint a slab on an output device. Apple's QuickDraw, like most other professional-level graphics systems, renders polygons and lines not with Bresenham's algorithm, but by calculating `slab points' for each scan line on the screen in succession, and then slabbing in the actual image pixels.

*-Slack

1. n. Space allocated to a disk file but not actually used to store useful information. The techspeak equivalent is `internal fragmentation'. Antonym hole.
2. In the theology of the Church of the SubGenius, a mystical substance or quality that is the prerequisite of all human happiness. Since UNIX files are stored compactly, except for the unavoidable wastage in the last block or fragment, it might be said that “Unix has no slack”. See ha ha only serious.

*-Slap On The Side

n. (also called a sidecar, or abbreviated `SOTS'. ) A type of external expansion hardware marketed by computer manufacturers (e. g. , Commodore for the Amiga 500/1000 series and IBM for the hideous failure called `PCjr'). Various SOTS boxes provided necessities such as memory, hard drive controllers, and conventional expansion slots.

*-Slash

n. Common name for the slant (`/', ASCII 0101111) character. See ASCII for other synonyms.

*-Sleep

1. vi. [techspeak] To relinquish a claim (of a process on a multitasking system) for service; to indicate to the scheduler that a process may be deactivated until some given event occurs or a specified time delay elapses.
2. In jargon, used very similarly to v. block; also in `sleep on', syn. with `block on'. Often used to indicate that the speaker has relinquished a demand for resources until some (possibly unspecified) external event “They can't get the fix I've been asking for into the next release, so I'm going to sleep on it until the release, then start hassling them again. ”

*-Slim

n. A small, derivative change (e. g. , to code).

*-Slop

1. n. A one-sided fudge factor, that is, an allowance for error but in only one of two directions. For example, if you need a piece of wire 10 feet long and have to guess when you cut it, you make very sure to cut it too long, by a large amount if necessary, rather than too short by even a little bit, because you can always cut off the slop but you can't paste it back on again. When discrete quantities are involved, slop is often introduced to avoid the possibility of being on the losing side of a fencepost error.
2. The percentage of `extra' code generated by a compiler over the size of equivalent assembler code produced by hand-hacking; i. e. , the space (or maybe time) you lose because you didn't do it yourself. This number is often used as a measure of the goodness of a compiler; slop below 5% is very good, and 10% is usually acceptable. With modern compiler technology, esp. on RISC machines, the compiler's slop may actually be *negative*; that is, humans may be unable to generate code as good. This is one of the reasons assembler programming is no longer common.

*-Slopsucker

/slop'suhk-r/ n. A lowest-priority task that waits around until everything else has `had its fill' of machine resources. Only when the machine would otherwise be idle is the task allowed to `suck up the slop'. Also called a `hungry puppy' or `bottom feeder'. One common variety of slopsucker hunts for large prime numbers. Compare background.

Slot

A data structure that represents an attribute of an entity (q. v.). (ET;, MA;)

*-Slurp

vt. To read a large data file entirely into core before working on it. This may be contrasted with the strategy of reading a small piece at a time, processing it, and then reading the next piece. “This program slurps in a 1K-by-1K matrix and does an FFT. ” See also sponge.

*-Smart

adj. Said of a program that does the Right Thing in a wide variety of complicated circumstances. There is a difference between calling a program smart and calling it intelligent; in particular, there do not exist any intelligent programs (yet -- see AI-complete). Compare robust (smart programs can be brittle).

Smart Card

Smart Terminal

A terminal (or communications software) which provides features beyond simply transferring data to and from the system. Typical features are: upload and download, graphics displays, formatted screen displays, etc. (BBD)

#-Smartcards/Token Authentication

This KSA has no definition.

*-Smash Case

vi. To lose or obliterate the uppercase/lowercase distinction in text input. “MS-DOS will automatically smash case in the names of all the files you create. ” Compare fold case.

*-Smash The Stack

n. [C programming] To corrupt the execution stack by writing past the end of a local array or other data structure. Code that smashes the stack can cause a return from the routine to jump to a random address, resulting in some of the most insidious data-dependent bugs known to mankind. Variants include `trash' the stack, scribble the stack, mangle the stack; the term **mung the stack is not used, as this is never done intentionally. See spam; see also aliasing bug, fandango on core, memory leak, memory smash, precedence lossage.

*-Smiley

n. See emoticon.

*-Smoke

1. vi. To crash or blow up, usually spectacularly. “The new version smoked, just like the last one. ” Used for both hardware (where it often describes an actual physical event), and software (where it's merely colorful).
2. [from automotive slang] To be conspicuously fast. “That processor really smokes. ” Compare magic smoke.

*-Smoke And Mirrors

n. Marketing deceptions. The term is mainstream in this general sense. Among hackers it's strongly associated with bogus demos and crocked benchmarks (see also MIPS, machoflops). “They claim their new box cranks 50 MIPS for under $5000, but didn't specify the instruction mix --- sounds like smoke and mirrors to me. ” The phrase, popularized by newspaper columnist Jimmy Breslin c. 1975, has been said to derive from carnie slang for magic acts and `freak show' displays that depend on `trompe l'oeil' effects, but also calls to mind the fierce Aztec god Tezcatlipoca (lit. “Smoking Mirror”) for whom the hearts of huge numbers of human sacrificial victims were regularly cut out. Upon hearing about a rigged demo or yet another round of fantasy-based marketing promises, hackers often feel analogously disheartened.

*-Smoke Test

1. n. A rudimentary form of testing applied to electronic equipment following repair or reconfiguration, in which power is applied and the tester checks for sparks, smoke, or other dramatic signs of fundamental failure. See magic smoke.
2. By extension, the first run of a piece of software after construction or a critical change. See and compare reality check. There is an interesting semi-parallel to this term among typographers and printers When new typefaces are being punch-cut by hand, a `smoke test' (hold the letter in candle smoke, then press it onto paper) is used to check out new dies.

*-Smoking Clover

n. [ITS] A display hack originally due to Bill Gosper. Many convergent lines are drawn on a color monitor in AOS mode (so that every pixel struck has its color incremented). The lines all have one endpoint in the middle of the screen; the other endpoints are spaced one pixel apart around the perimeter of a large square. The color map is then repeatedly rotated. This results in a striking, rainbow-hued, shimmering four-leaf clover. Gosper joked about keeping it hidden from the FDA (the U. S. 's Food and Drug Administration) lest its hallucinogenic properties cause it to be banned.

*-SMOP

/S-M-O-P/ n. [Simple (or Small) Matter of Programming]

1. A piece of code, not yet written, whose anticipated length is significantly greater than its complexity. Used to refer to a program that could obviously be written, but is not worth the trouble. Also used ironically to imply that a difficult problem can be easily solved because a program can be written to do it; the irony is that it is very clear that writing such a program will be a great deal of work. “It's easy to enhance a FORTRAN compiler to compile COBOL as well; it's just an SMOP. ”
2. Often used ironically by the intended victim when a suggestion for a program is made which seems easy to the suggester, but is obviously (to the victim) a lot of work.

*-Smurf

/smerf/ n. [from the soc. motss newsgroup on Usenet, after some obnoxiously gooey cartoon characters] A newsgroup regular with a habitual style that is irreverent, silly, and cute. Like many other hackish terms for people, this one may be praise or insult depending on who uses it. In general, being referred to as a smurf is probably not going to make your day unless you've previously adopted the label yourself in a spirit of irony. Compare old fart.

*-SNAFU Principle

/sna'foo prin'si-pl/ n. “True communication is Situation Normak, All Fargled Up” possible only between equals, because inferiors are more consistently rewarded for telling their superiors pleasant lies than for telling the truth. ” -- a central tenet of Discordianism, often invoked by hackers to explain why authoritarian hierarchies screw up so reliably and systematically. The effect of the SNAFU principle is a progressive disconnection of decision-makers from reality. This lightly adapted version of a fable dating back to the early 1960s illustrates the phenomenon perfectly: In the beginning was the plan, and then the specification; And the plan was without form, and the specification was void. And darkness was on the faces of the implementors thereof; And they spake unto their leader, saying “It is a crock , and smells as of a sewer. ” And the leader took pity on them, and spoke to the project leader “It is a crock of excrement, and none may abide the odor thereof. ” And the project leader spake unto his section head, saying “It is a container of excrement, and it is very strong, such that none may abide it. ” The section head then hurried to his department manager, and informed him thus “It is a vessel of fertilizer, and none may abide its strength. ” The department manager carried these words to his general manager, and spoke unto him saying “It containeth that which aideth the growth of plants, and it is very strong. ” And so it was that the general manager rejoiced and delivered the good news unto the Vice President. “It promoteth growth, and it is very powerful. ” The Vice President rushed to the President's side, and joyously exclaimed “This powerful new software product will promote the growth of the company!” And the President looked upon the product, and saw that it was very good. After the subsequent disaster, the suits protect themselves by saying “I was misinformed!”, and the implementors are demoted or fired.

*-Snail

vt. To snail-mail something. “Snail me a copy of those graphics, will you?”

*-Snail-Mail

n. Paper mail, as opposed to electronic. Sometimes written as the single word `SnailMail'. One's postal address is, correspondingly, a `snail address'. Derives from earlier coinage `USnail' (from `U. S. Mail'), for which there have even been parody posters and stamps made. Oppose email.

*-Snap

v. To replace a pointer to a pointer with a direct pointer; to replace an old address with the forwarding address found there. If you telephone the main number for an institution and ask for a particular person by name, the operator may tell you that person's extension before connecting you, in the hopes that you will `snap your pointer' and dial direct next time. The underlying metaphor may be that of a rubber band stretched through a number of intermediate points; if you remove all the thumbtacks in the middle, it snaps into a straight line from first to last. See chase pointers. Often, the behavior of a trampoline is to perform an error check once and then snap the pointer that invoked it so as henceforth to bypass the trampoline (and its one-shot error check). In this context one also speaks of `snapping links'. For example, in a LISP implementation, a function interface trampoline might check to make sure that the caller is passing the correct number of arguments; if it is, and if the caller and the callee are both compiled, then snapping the link allows that particular path to use a direct procedure-call instruction with no further overhead.

*-Snarf

/snarf/ vt.

1. To grab, esp. to grab a large document or file for the purpose of using it with or without the author's permission. See also BLT.
2. [in the UNIX community] To fetch a file or set of files across a network. See also blast. This term was mainstream in the late 1960s, meaning `to eat piggishly'. It may still have this connotation in context. “He's in the snarfing phase of hacking -- FTPing megs of stuff a day. ”
3. . To acquire, with little concern for legal forms or politesse (but not quite by stealing). “They were giving away samples, so I snarfed a bunch of them. ”
4. Syn. for slurp. “This program starts by snarfing the entire database into core, then. ” 5. [GEnie] To spray food or programming fluids due to laughing at the wrong moment. “I was drinking coffee, and when I read your post I snarfed all over my desk. ” “If I keep reading this topic, I think I'll have to snarf-proof my computer with a keyboard condom. ” [This sense appears to be widespread among mundane teenagers -- ESR]

*-Snarf & Barf

/snarf'n-barf`/ n. Under a WIMP environment, the act of grabbing a region of text and then stuffing the contents of that region into another region (or the same one) to avoid retyping a command line. In the late

1960s, this was a mainstream expression for an `eat now, regret it later' cheap-restaurant expedition.

*-Snarf Down

v. To snarf, with the connotation of absorbing, processing, or understanding. “I'll snarf down the latest version of the nethack user's guide -- it's been a while since I played last and I don't know what's changed recently. ”

*-Snark

n. [Lewis Carroll, via the Michigan Terminal System]

1. A system failure. When a user's process bombed, the operator would get the message “Help, Help, Snark in MTS!”
2. More generally, any kind of unexplained or threatening event on a computer (especially if it might be a boojum). Often used to refer to an event or a log file entry that might indicate an attempted security violation. See snivitz.

*-Sneaker

n. An individual hired to break into places in order to test their security; analogous to tiger team.

*-Sneakernet

/snee'ker-net/ n. Term used (generally with ironic intent) for transfer of electronic information by physically carrying tape, disks, or some other media from one machine to another. “Never underestimate the bandwidth of a station wagon filled with magtape, or a 747 filled with CD-ROMs. ” Also called `Tennis-Net', `Armpit-Net', `Floppy-Net' or `Shoenet'.

*-Sniff

v. ,n. Synonym for poll.

*-Snivitz

/sniv'itz/ n. A hiccup in hardware or software; a small, transient problem of unknown origin (less serious than a snark). Compare glitch.

*-SO

/S-O/ n.

1. (also `S. O. ') Abbrev. for Significant Other, almost invariably written abbreviated and pronounced /S-O/ by hackers. Used to refer to one's primary relationship, esp. a live-in to whom one is not married. See MOTAS, MOTOS, MOTSS.
2. The Shift Out control character in ASCII (Control-N, 0001110).

#-Social Engineering

(1) This KSA has no definition. (2) n. Term used among crackers and for cracking techniques that rely on weaknesses in rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

*-Social Science Number

n. [IBM] A statistic that is content-free, or nearly so. A measure derived via methods of questionable validity from data of a dubious and vague nature. Predictively, having a social science number in hand is seldom much better than nothing, and can be considerably worse. As a rule, management loves them. See also numbers, math-out, pretty pictures.

*-Soft Boot

n. See boot.

Soft Copy

A nonpermanent display image, for example, a cathode ray tube display. (FP) (ISO) See also hard copy.

Soft Sectoring

The identification of sector boundaries on a magnetic disk by using recorded information. (FP) (ISO) See also hard sectoring.

*-Softcopy

/soft'kop-ee/ n. [by analogy with `hardcopy'] A machine-readable form of corresponding hardcopy. See bits, machinable.

Softlifting

Illegal copying of licensed software for personal use. (PC/PCIE;)

Software

A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system; e. g. , compilers, library routines, manuals, circuit diagrams. (JCS1-DoD) See also computer, firmware, hardware.

#-Software Architecture Study

Map the security requirements, security policy, and security CONOPS to the system design. (Source: DACUM IV).

#-Software Asset Management

This KSA has no definition.

*-Software Bloat

n. The results of second-system effect or creeping featuritis. Commonly cited examples include `ls(1)', X, BSD, Missed'em-five, and OS/2.

Software Development Methodologies

Methodologies for specifying and verifying design programs for system development. Each methodology is written for a specific computer language. See Enhanced Hierarchical Development Methodology, Formal Development Methodology, Gypsy Verifica-

tion Environment, and Hierarchical Development Methodology.

#-Software Engineering

1. The application of a systematic, disciplined, quantifiable approach to the development, operation and maintenance of software; that is, the application of engineering to software. (IEEE Standard Glossary of Software)
2. An applied science devoted to improving and optimizing the production of computer software. (*QCUS+Pf-90*)

Software Interface Functions

TCB operations that can be invoked by software. (MTR-8201)

*-Software Laser

n. An optical laser works by bouncing photons back and forth between two mirrors, one totally reflective and one partially reflective. If the lasing material (usually a crystal) has the right properties, photons scattering off the atoms in the crystal will excite cascades of more photons, all in lockstep. Eventually the beam will escape through the partially-reflective mirror. One kind of sorcerer's apprentice mode involving bounce messages can produce closely analogous results, with a cascade of messages escaping to flood nearby systems. By mid-1993 there had been at least two publicized incidents of this kind.

#-Software Licensing

A legal agreement included with commercial programs. The software license specifies the rights and obligations of the user who purchased the program and limits the liability of the software publisher. (*QCUS+Pf-90*)

#-Software Piracy

1. The unauthorized copying, distribution or use of computer software. (Source panel of experts)
2. The unauthorized and illegal duplication of copyrighted software without the permission of the software publisher. ref: 3.

*-Software Rot

n. Term used to describe the tendency of software that has not been used in a while to lose; such failure may be semi-humorously ascribed to bit rot. More commonly, `software rot' strikes when a program's assumptions become out of date. If the design was insufficiently robust, this may cause it to fail in mysterious ways. For example, owing to endemic shortsightedness in the design of COBOL programs, most will succumb to software rot when their 2-digit year counters wrap around at the beginning of the year 2000. Actually, related lossages often afflict centenarians who have to deal with computer software designed by unimaginative clods. One such incident became the focus of a minor public flap in 1990, when a gentleman born in ~9 applied for a driver's license renewal in Raleigh, North Carolina. The new system refused to issue the card, probably because with 2-digit years the ages 101 and 1 cannot be distinguished. Historical note Software rot in an even funnier sense than the mythical one was a real problem on early research computers (e. g. , the R1; see grind crank). If a program that depended on a peculiar instruction hadn't been run in quite a while, the user might discover that the opcodes no longer did the same things they once did. (“Hey, so-and-so needs an instruction to do such-and-such. We can snarf this opcode, right? No one uses it. ”) Another classic example of this sprang from the time an MIT hacker found a simple way to double the speed of the unconditional jump instruction on a PDP-6, so he patched the hardware. Unfortunately, this broke some fragile timing software in a music-playing program, throwing its output out of tune. This was fixed by adding a defensive initialization routine to compare the speed of a timing loop with the real-time clock; in other words, it figured out how fast the PDP-6 was that day, and corrected appropriately. Compare bit rot.

Software Security

1. Those general purpose (executive, utility, or software development tools) and applications programs, and routines which protect data handled by an ADP system and its resources. (*AR* 380-380)
2. General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system. (*NCSC-TG*-004-88)

Software System Test

Process that plans, develops, and evaluation process documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

Software System Test And Evaluation Process

A process that plans, develops and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational and interface requirements.

*-Softwarily

/soft-weir'i-lee/ adv. In a way pertaining to software. “The system is softwarily unreliable. ” The adjective **`softwary' is *not* used. See hardwarily.

*-Softy

n. [IBM] Hardware hackers' term for a software expert who is largely ignorant of the mysteries of hardware.

Solid-State Scanning

In facsimile, scanning in which all or a part of the scanning process is performed by electronic commutation of a solid-state array of photosensitive elements. (~) See also facsimile, scanning.

*-Some Random X

adj. Used to indicate a member of class X, with the implication that Xs are interchangeable. “I think some random cracker tripped over the guest timeout last night. ” See also J. Random.

*-Sorcerer's Apprentice Mode

n. [from Goethe's “Der Zauberlehrling” via the film “Fantasia”] A bug in a protocol where, under some circumstances, the receipt of a message causes multiple messages to be sent, each of which, when received, triggers the same bug. Used esp. of such behavior caused by bounce message loops in email software. Compare broadcast storm, network meltdown, software laser, ARMM.

Sort

A meta-attribute of a slot: there are four sorts in MAPLESS: Qualitative, Predicate, Valued, and Method (q. v.). (MA;)

*-SOS

1. n. ,obs. /S-O-S/ An infamously losing text editor. Once, back in the 1960s, when a text editor was needed for the PDP-6, a hacker crufted together a quick-and-dirty `stopgap editor' to be used until a better one was written. Unfortunately, the old one was never really discarded when new ones (in particular, TECO) came along. SOS is a descendant (`Son of Stopgap') of that editor, and many PDP-10 users gained the dubious pleasure of its acquaintance. Since then other programs similar in style to SOS have been written, notably the early font editor BILOS /bye'lohs/, the Brother-In-Law Of Stopgap.
2. /sos/ vt. To decrease; inverse of AOS, from the PDP-10 instruction set.

Source

In communications, that part of a system from which messages are considered to originate. (~) See also data terminal equipment, destination user, optical source, sink, source user.

Source Code

*-Source Of All Good Bits

n. A person from whom (or a place from which) useful information may be obtained. If you need to know about a program, a guru might be the source of all good bits. The title is often applied to a particularly competent secretary.

Source User

The user providing the information to be transferred to a destination user during a particular information transfer transaction. See information source. See also access originator, call originator, communications source, destination user, sink, source.

Space

An asset category consisting of the physical premises occupied by the installation and its immediate environment. (RM;)

#-Space Systems Security

This KSA has no definition.

*-Space-Cadet Keyboard

n. A now-legendary device used on MIT LISP machines, which inspired several still-current jargon terms and influenced the design of EMACS. It was equipped with no fewer than *seven* shift keys four keys for bucky bits (`control', `meta', `hyper', and `super') and three like regular shift keys, called `shift', `top', and `front'. Many keys had three symbols on them a letter and a symbol on the top, and a Greek letter on the front. For example, the `L' key had an `L' and a two-way arrow on the top, and the Greek letter lambda on the front. By pressing this key with the right hand while playing an appropriate `chord' with the left hand on the shift keys, you could get the following results: L lowercase l shift-L uppercase L front-L lowercase lambda front-shift-L uppercase lambda top-L two-way arrow (front and shift are ignored) And of course each of these might also be typed with any combination of the control, meta, hyper, and super keys. On this keyboard, you could type over 8000 different characters! This allowed the user to type very complicated mathematical text, and also to have thousands of single-character commands at his disposal. Many hackers were actually willing to memorize the command meanings of that many characters if it reduced typing time (this attitude obviously shaped the interface of EMACS). Other hackers, however, thought having that many bucky bits was overkill, and objected that such a keyboard can require three or four hands to operate. See bucky bits, cokebottle, double bucky, meta bit, quadruple bucky. Note early versions of this entry incorrectly identified the space-cadet keyboard with the `Knight keyboard'. Though both were designed by Tom Knight, the latter term was properly applied only to a keyboard used for ITS on the PDP-10 and modeled on the Stanford keyboard (as described under bucky bits). The true space-cadet keyboard evolved from the first Knight keyboard.

*-SPACEWAR

n. A space-combat simulation game, inspired by E. E. “Doc” Smith's “Lensman” books, in which two spaceships duel around a central sun, shooting torpedoes at

each other and jumping through hyperspace. This game was first implemented on the PDP-1 at MIT in 1960--61. SPACEWAR aficionados formed the core of the early hacker culture at MIT. Nine years later, a descendant of the game motivated Ken Thompson to build, in his spare time on a scavenged PDP-7, the operating system that became UNIX. Less than nine years after that, SPACEWAR was commercialized as one of the first video games; descendants are still feeping in video arcades everywhere.

*-Spaghetti Code

n. Code with a complex and tangled control structure, esp. one using many GOTOs, exceptions, or other `unstructured' branching constructs. Pejorative. The synonym `kangaroo code' has been reported, doubtless because such code has so many jumps in it.

*-Spaghetti Inheritance

n. [encountered among users of object-oriented languages that use inheritance, such as Smalltalk] A convoluted class-subclass graph, often resulting from carelessly deriving subclasses from other classes just for the sake of reusing their code. Coined in a (successful) attempt to discourage such practice, through guilt-by-association with spaghetti code.

*-Spam

1. vt. [from “Monty Python's Flying Circus”] To crash a program by overrunning a fixed-size buffer with excessively large input data. See also buffer overflow, smash the stack.
2. To cause a newsgroup to be flooded with irrelevant or inappropriate messages. You can spam a newsgroup with as little as one well- (or ill-) planned message (e. g. asking “What do you think of abortion?” on soc. women). This is often done with cross-posting (e. g. any message which is crossposted to alt. rush-limbaugh and alt. politics. homosexuality will almost inevitably spam both groups). The second definition has become much more prevalent as the Internet has opened up to non-techies, and to many Usenetters it is probably now (1995) primary.

Spare

An individual part, subassembly, or assembly supplied for the maintenance or repair of systems or equipment. (JCS1-NATO)

Special Access Program(s) (SAP)

1. Any programs imposing need-to-know or related security requirements or constraints which are beyond those normally provided for the protection of information classified in one of the three security classification designations; i. e. , Confidential, Secret, or Top Secret. Such a program includes but is not limited to, special clearance, adjudicative, or investigative requirements, special designation of officials authorized to determine need-to-know, or special lists or briefings of personnel determined to have a need-to-know. SIOP-ESI is an example of a *DOD* Special Access Program. Other sources of additional access control or other pertinent security requirements, not generally applicable to the same security classification category within *DOD* include: (a) the Atomic Energy Act of 1954; (b) procedures based on International Treaty requirements; and (c) programs for the collection of foreign intelligence or under the jurisdiction of the National Foreign Intelligence Board or the U. S. Communications Security Board. (*OPNAVINST* 5239. l A) (*OPNAVINST* 5239. 1A;, DODD 5200. 28;)

2) Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know. (*AFR* 205-16; DOE 5635. lA)

3. (SAP) Any program created under the authority of Executive Order that imposes additional controls governing access to classified information. *Any program established under Executive Order 12356 that imposes additional controls governing access to classified information involved with such programs beyond those required by normal management and safeguarding practices. These programs may include, but are not limited to, access approval, adjudication or investigative requirements, special designation of officials authorized to determine a need-to-know, or special lists of persons determined to have a need-to-know. (*IC Staff, Glossary of Intelligence Terms and Definitions,* 6/89)

Special Markings

1. Special Markings are not classification levels [but rather] are used on certain classified documents to indicate that the document has special access or handling requirements. (DOE 5635. 1A;)
2. Synonymous with Handling Caveats; Dissemination Controls; Dissemination Control Markings; Handling Restrictions.

Special Mission

Modification that applies only modification to a specific mission, purpose, operational, or environmental need. NOTE: Special mission modifications may be either optional or mandatory.

Special Mission Modification

Modification that applies only to a specific mission, purpose, operational, or environmental need. NOTE: Special mission modifications may be either optional or mandatory.

Special Purpose Computer

A computer that is designed to operate upon a restricted class of problems. (FP)

*-Special-Case

vt. To write unique code to handle input to or situations arising in a program that are somehow distinguished from normal processing. This would be used for processing of mode switches or interrupt characters in an interactive interface (as opposed, say, to text entry or normal commands), or for processing of hidden flags in the input of a batch program or filter.

Specification

A document intended primarily for use in procurement, which clearly and accurately describes the essential technical requirements for items, materials, or services, including the procedures by which it will be determined that the requirements have been met. Specifications for items and materials may also contain preservation, packaging, packing, and marking requirements. (~) See also design objective.

Speech Privacy

Techniques that use fixed sequence permutations or voice/speech inversion to render speech unintelligible to the casual listener.

Speed Calling

A service feature that enables a switch or station to store certain telephone numbers and dial them automatically when a short (1-, 2-, or 3-digit) code is entered. (~) See also abbreviated dialing, card dialer, repertory dialer, service feature.

Speed Dialing

Dialing at a speed greater than the normal ten pulses per second. (~) See also abbreviated dialing, pulse, pulsing.

*-Speedometer

n. A pattern of lights displayed on a linear set of LEDs (today) or nixie tubes (yesterday, on ancient mainframes). The pattern is shifted left every N times the operating system goes through its main loop. A swiftly moving pattern indicates that the system is mostly idle; the speedometer slows down as the system becomes overloaded. The speedometer on Sun Microsystems hardware bounces back and forth like the eyes on one of the Cylons from the wretched "Battlestar Galactica" TV series. Historical note One computer, the GE 600 (later Honeywell 6000) actually had an *analog* speedometer on the front panel, calibrated in instructions executed per second.

*-Spell

n. Syn. incantation.

*-Spelling Flame

n. [Usenet] A posting ostentatiously correcting a previous article's spelling as a way of casting scorn on the point the article was trying to make, instead of actually responding to that point (compare dictionary flame). Of course, people who are more than usually slovenly spellers are prone to think *any* correction is a spelling flame. It's an amusing comment on human nature that spelling flames themselves often contain spelling errors.

Spelling Table

See Syllabary.

*-Spiffy

1. /spi'fee/ adj. Said of programs having a pretty, clever, or exceptionally well-designed interface. "Have you seen the spiffy X version of empire yet?"
2. Said sarcastically of a program that is perceived to have little more than a flashy interface going for it. Which meaning should be drawn depends delicately on tone of voice and context. This word was common mainstream slang during the 1940s, in a sense close to 1.

*-Spike

v. To defeat a selection mechanism by introducing a (sometimes temporary) device that forces a specific result. The word is used in several industries; telephone engineers refer to spiking a relay by inserting a pin to hold the relay in either the closed or open state, and railroaders refer to spiking a track switch so that it cannot be moved. In programming environments it normally refers to a temporary change, usually for testing purposes (as opposed to a permanent change, which would be called hardwired).

Spill Forward

*-Spin

vi. Equivalent to buzz. More common among C and UNIX programmers.

*-Spl

/S-P-L/ [abbrev, from Set Priority Level] The way traditional UNIX kernels implement mutual exclusion by running code at high interrupt levels. Used in jargon to describe the act of tuning in or tuning out ordinary communication. Classically, spl levels run from 1 to 7; "Fred's at spl 6 today" would mean that he is very hard to interrupt. "Wait till I finish this; I'll spl down then. " See also interrupts locked out.

*-Splash Screen

n. [Mac users] Syn. banner, sense 3.

*-Splat

1. n. Name used in many places (DEC, IBM, and others) for the asterisk (`*') character (ASCII 0101010). This may derive from the `squashed-

bug' appearance of the asterisk on many early line printers.
2. [MIT] Name used by some people for the `#' character (ASCII 0100011).
3. . [Rochester Institute of Technology] The feature key on a Mac (same as alt, sense 2).
4. obs. Name used by some people for the Stanford/ITS extended ASCII circle-x character. This character is also called `blobby' and `frob', among other names; it is sometimes used by mathematicians as a notation for `tensor product'. 5. obs. Name for the semi-mythical Stanford extended ASCII circle-plus character. See also ASCII.

Split Knowledge

1. The condition under which two or more parties separately have part of the data, that when combined, will yield a security parameter or that will allow them to perform some sensitive function. (WB)
2. The separation of data into two or more parts, each part constantly kept under control of separate authorized individuals or teams, so that no one individual will be knowledgeable of the total data involved. (NCSC-9)

*-Spod

n. [UK] A lower form of life found on talker systems and MUDs. The spod has few friends in RL and uses talkers instead, finding communication easier and preferable over the net. He has all the negative traits of the computer geek without having any interest in computers per se. Lacking any knowledge of or interest in how networks work, and considering his access a God-given right, he is a major irritant to sysadmins, clogging up lines in order to reach new MUDs, following passed-on instructions on how to sneak his way onto Internet (“Wow! It's in America!”) and complaining when he is not allowed to use busy routes. A true spod will start any conversation with “Are you male or female?” (and follow it up with “Got any good numbers/IDs/passwords?”) and will not talk to someone physically present in the same terminal room until they log onto the same machine that he is using and enter talk mode. Compare newbie, tourist, weenie, twink, terminal junkie.

*-Spoiler

1. n. [Usenet] A remark which reveals important plot elements from books or movies, thus denying the reader (of the article) the proper suspense when reading the book or watching the movie.
2. Any remark which telegraphs the solution of a problem or puzzle, thus denying the reader the pleasure of working out the correct answer (see also interesting). Either sense readily forms compounds like `total spoiler', `quasi-spoiler' and even `pseudo-spoiler'. By convention, articles which are spoilers in either sense should contain the word `spoiler' in the Subject line, or guarantee via various tricks that the answer appears only after several screens-full of warning, or conceal the sensitive information via rot13, or some combination of these techniques.

*-Sponge

n. [UNIX] A special case of a filter that reads its entire input before writing any output; the canonical example is a sort utility. Unlike most filters, a sponge can conveniently overwrite the input file with the output data stream. If a file system has versioning (as ITS did and VMS does now) the sponge/filter distinction loses its usefulness, because directing filter output would just write a new version. See also slurp.

Sponsor Of Data

Synonymous with OWNER OF DATA.

Spoofing

1. The deliberate inducement of a user or a resource to take an incorrect action. (*AR* 380-380; *FIPS PUB* 39)
2. See MASQUERADING. (*NCSC-TG*-004-88)

*-Spool

vi. [from early IBM `Simultaneous Peripheral Operation On-Line', but this acronym is widely thought to have been contrived for effect] To send files to some device or program (a `spooler') that queues them up and does something useful with them later. Without qualification, the spooler is the `print spooler' controlling output of jobs to a printer; but the term has been used in connection with other peripherals (especially plotters and graphics devices) and occasionally even for input devices. See also demon.

*-Spool File

n. Any file to which data is spooled to await the next stage of processing. Especially used in circumstances where spooling the data copes with a mismatch between speeds in two devices or pieces of software. For example, when you send mail under UNIX, it's typically copied to a spool file to await a transport demon's attentions. This is borderline

Spooling

The use of auxiliary storage as buffer storage to reduce processing delays when transferring data between peripheral equipment and the processors of a computer. Note: The term is derived from the expression simultaneous peripheral operation on line. (FP) (ISO)

Spread Spectrum

1. A telecommunications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. (~) (After INFOSEC)

2. A signal structuring technique that employs direct sequence, frequency hopping or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy and increasing the immunity of spread spectrum receivers to noise and interference. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wide band of frequencies. The receiver correlates the signals to retrieve the original information signal. (NTIA) (~) See also anti-jam, frequency hopping, pseudorandom number sequence.

#-Spread Spectrum Analysis

Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. (Source: NSTISSI 4009).

*-Squirrelcide

n. [common on Usenet's comp. risks newsgroup] (alt `squirrelicide') What all too frequently happens when a squirrel decides to exercise its species's unfortunate penchant for shorting out power lines with their little furry bodies. Result; one dead squirrel, one down computer installation. In this situation, the computer system is said to have been

*-Squirrelcided. Stack

n. The set of things a person has to do in the future. One speaks of the next project to be attacked as having risen to the top of the stack. “I'm afraid I've got real work to do, so this'll have to be pushed way down on my stack. ” “I haven't done it yet because every time I pop my stack something new gets pushed. ” If you are interrupted several times in the middle of a conversation, “My stack overflowed” means “I forget what we were talking about. ” The implication is that more items were pushed onto the stack than could be remembered, so the least recent items were lost. The usual physical example of a stack is to be found in a cafeteria a pile of plates or trays sitting on a spring in a well, so that when you put one on the top they all sink down, and when you take one off the top the rest spring up a bit. See also push and pop. At MIT, pdl used to be a more common synonym for stack in all these contexts, and this may still be true. Everywhere else stack seems to be the preferred term. Knuth (“The Art of Computer Programming”, second edition, vol. 1, p. 236) says Many people who realized the importance of stacks and queues independently have given other names to these structures: stacks have been called push-down lists, reversion storages, cellars, nesting stores, piles, last-in-first-out (“LIFO”) lists, and even yo-yo lists!

ST&E Tools And Equipment

Specialized techniques, procedures, criteria, standards, programs, or equipment accepted by qualified ST&E personnel for uniform or standard use in testing and evaluating the secure features of ADP systems or networks. (*OPNAVINST* 5239. 1A;; DODD 5200. 28M;)

*-Stack Puke

n. Some processor architectures are said to `puke their guts onto the stack' to save their internal state during exception processing. The Motorola 68020, for example, regurgitates up to 92 bytes on a bus fault. On a pipelined machine, this can take a while. stale

Stand Alone Security Mode

A mode of operation in which a microcomputer is not networked with another. May process information of any sensitivity level It applies only to microcomputers without nonremoveable media. (*AFR* 205-16)

Stand Alone Security Mode Of Operation

This mode of operation is meant for microcomputers that are used by only one user at a time. It does NOT apply to microcomputers processing classified, microcomputers with fixed storage if need-to-know does not apply to all users, and microcomputers with active communications or resource sharing. (*AFR* 205-16;)

Stand Alone, Shared Automated Information System

An Automated Information System that is physically and electrically isolated from all other Automated Information Systems, and is intended to be used by more than one person, either simultaneously (e. g. , an Automated Information System with multiple terminals) or serially, with data belonging to one user remaining available to the Automated Information System while another user is using the Automated Information System (e. g. , a PC with non-removable storage media such as a hard disk). (*NCSC-WA*-001-85;)

Stand Alone, Single-User Automated Information System

An Automated Information System that is physically and electrically isolated from all other Automated Information Systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the Automated Information System (e. g. , a PC with removable storage media such as a floppy disk). (*NCSC-WA*-001-85;)

#-Stand-Alone Systems And Remote Terminals

A system that is normally isolated from other systems and is intended to be used by only one person at a time. Under operator control, this system may be connected to another system or network and used for remote access to that system. (Source panel of experts).

Stand-Alone, Shared System

A system that is physically and electrically isolated from all other systems, and is intended to be used by more than one person, either simultaneously (e. g. , a system with multiple terminals) or serially, with data belonging to one user remaining available to the system while another user is using the system (e. g. , a personal computer with nonremovable storage media such as a hard disk).

Stand-Alone, Single-User System

A system that is physically and electrically isolated from all other systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e. g. , a personal computer with removable storage media such as a floppy disk).

Standard

1. Guideline documentation that reflects agreements on products, practices, or operations by nationally or internationally recognized industrial, professional, trade associations or governmental bodies. Note: This concept applies to formal, approved standards, as contrasted to de facto standards and proprietary standards, which are exceptions to this concept. See also de facto standards, proprietary standard.
2. A document that establishes engineering and technical requirements for processes, procedures, practices, and methods that have been adopted as standard.
3. An exact value, a physical entity, or an abstract concept, established and defined by authority, custom, or common consent to serve as a reference, model, or rule in measuring quantities or qualities, establishing practices or procedures, or evaluating results. A fixed quantity or quality. (JCS1-DoD) (JCS1-NATO)

Standard Measurement Point

The point where the compromising emanation performance requirement (CEPR) applies. For an electric or magnetic field emanation, the standard measurement point is one meter from the equipment under test. For a conducted emanation, the standard measurement point is at the design radius.

#-Standards

Common methods and protocols for data protection which enable the secure exchange of data between parties which may not belong to the same organizations. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

#-Standards Of Conduct

Ensure public do not violate public trust. Each employee has a responsibility to the USG and its citizens to place loyalty to the Constitution, laws and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in the DoD Joint Ethic Regulation (JER), as well as implementing standards contained within the JER and in supplemental agency regulations. (Source DoD JER).

STAPLE

Structured turing APL Environment. The newly defined language in which MAPLESS procedures are to be written.

STAR

See System Threat Assessment Report.

Star (*) Property

Bell-La Padula security model rule allowing a subject write access to an object only if the security level of the object dominates the security level of the subject.

Star Network

A radial (starlike) configuration of communication-network nodes such that there is a direct path between each node and a central node that serves as a central distribution node. (~) See also bus topology, node (def. #1), ring network, tree topology.

*-Star Out

v, [University of York, England] To replace a user's encrypted password in /etc/passwd with a single asterisk. Under Unix this is not a legal encryption of any password; hence the user is not permitted to log in. In general, accounts like adm, news, and daemon are permanently “starred out”; occasionally a real user might have the this inflicted upon him/her as a punishment, e. g. “Graham was starred out for playing Omega in working hours”. Also occasionally known as The Order Of The Gold Star in this context. “Don't do that, or you'll be awarded the Order of the Gold Star. ” Compare disusered.

Star Property

Bell-La Padula security model rule allowing a subject write access to an object only if the security level of the object dominates the security level of the subject.

Star Property (* Property)

1. A Bell LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. (*DOD* 5200. 28-STD)
2. Synonymous with CONFINEMENT PROPERTY.

Star Topology

1. A communication network topology in which peripheral nodes are connected to a central node, which rebroadcasts all transmissions, received from any peripheral node, to all peripheral nodes on the network, including the originating node. Note 1: All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. Note 2: The failure of a transmission line (channel) linking any peripheral node to the central node will result in the isolation of that peripheral node from all others. Note 3: If the star's central node is passive, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way transmission time (i. e. , to and from the central node, plus any delay generated in the central node). An active star (star network having an active central node) may have means to prevent echo-related problems. (~) See also bus topology, local area network, node (def. #1), ring network, star network, tree topology.

START

Strategic Arms Reduction Treaty

Start-Stop Character

A character including one start signal at the beginning and one or two stop signals at the end. (FP) (ISO)

Start-Stop Modulation

A method of modulation in which the time of occurrence of the bits within each character, or block of characters, relates to a fixed time frame, but the start of each character, or block of characters, is not related to this fixed time frame. (~) See also asynchronous communication system, binary digit, modulation.

Start-Stop System

See asynchronous communication system.

Start-Stop Transmission

1. A form of asynchronous operation used in digital communications, which employs a start pulse and a stop pulse for each symbol. (~)
2. Signaling in which each group of code elements corresponding to an alphanumeric signal is preceded by a start signal that serves to prepare the receiving mechanism for the reception and registration of a character, and is followed by a stop signal that serves to bring the receiving mechanism to rest in preparation for the reception of the next character. (~) See also asynchronous operation, asynchronous transmission, code, pulse.

Start-Stop TTY Distortion

See teletypewriter signal distortion.

Start-Up KEK

Key encryption key held in common by a group of potential communicating entities and used to establish ad hoc tactical nets.

*-State

1. n. Condition, situation. “What's the state of your latest hack?” “It's winning away. ” “The system tried to read and write the disk simultaneously and got into a totally wedged state. ” The standard question “What's your state?” means “What are you doing?” or “What are you about to do?” Typical answers are “about to gronk out”, or “hungry”. Another standard question is “What's the state of the world?”, meaning “What's new?” or “What's going on?”. The more terse and humorous way of asking these questions would be “State-p?”. Another way of phrasing the first question under sense 1 would be “state-p latest hack?”.
2. Information being maintained in non-permanent memory (electronic or human).

State Delta Verification System

A system designed to give high confidence regarding microcode performance by utilizing formula that represent isolated states of a computation to check proofs concerning the course of that computation. (*NCSC-WA*-001-85;)

State Variable

A variable that represents either the state of the system or the state of the system resource. (*NCSC-WA*-001-85;)

Statement

1. In [computer] programming languages, a language construct that represents a set of declarations or a step in a sequence of actions. (FP)
2. In computer programming, a symbol string or other arrangement of symbols. (FP)
3. In computer programming, a meaningful expression or generalized instruction represented in a source language.
4. Deprecated See instruction.

Statement Of Need

Statement of Need

Statement Of Work

Statement of Work

Station

1. One or more transmitters or receivers or a combination of transmitters and receivers, including the accessory equipment necessary at one location, for carrying on radio communication service. Each station will be classified by the service in which it operates permanently or temporarily. (JCS1-DoD)
2. One or more transmitters or receivers or a combination of transmitters and receivers, including the

accessory equipment, necessary at one location for carrying on a radiocommunication service, or the radio astronomy service. Each station shall be classified by the service in which it operates permanently or temporarily. (RR) Note: The use of the term is not limited to radio applications.

*-Steam-Powered

adj. Old-fashioned or underpowered; archaic. This term does not have a strong negative loading and may even be used semi-affectionately for something that clanks and wheezes a lot but hangs in there doing the job.

*-Stiffy

n. [University of Lowell, Massachusetts.] 3. 5-inch microfloppies, so called because their jackets are more rigid than those of the 5. 25-inch and the (now totally obsolete) 8-inch floppy. Elsewhere this might be called a `firmy'.

*-Stir-Fried Random

n. (alt. `stir-fried mumble') Term used for the best dish of many of those hackers who can cook. Consists of random fresh veggies and meat wokked with random spices. Tasty and economical. See random, great-wall, ravs, laser chicken, oriental food; see also mumble

*-Stomp On

vt. To inadvertently overwrite something important, usually automatically. “All the work I did this weekend got stomped on last night by the nightly server script. ” Compare scribble, mangle, trash, scrog, roach

*-Stone Age

1. n. ,adj. In computer folklore, an ill-defined period from ENIAC (ca. 1943) to the mid-1950s; the great age of electromechanical dinosaurs. Sometimes used for the entire period up to 1960--61 (see Iron Age); however, it is funnier and more descriptive to characterize the latter period in terms of a `Bronze Age' era of transistor-logic, pre-ferrite-core machines with drum or CRT mass storage (as opposed to just mercury delay lines and/or relays). See also Iron Age.
2. More generally, a pejorative for any crufty, ancient piece of hardware or software technology. Note that this is used even by people who were there for the Stone Age (sense 1).

*-Stone Knives And Bearskins

n. [from the Star Trek Classic episode “The City on the Edge of Forever”] A term traditionally used to describe (and deprecate) computing environments that are grotesquely primitive in light of what is known about good ways to design things. As in “Don't get too used to the facilities here. Once you leave SAIL it's stone knives and bearskins as far as the eye can see”. Compare steam-powered

Stop Element

See stop signal.

Stop Signal

1. In start-stop transmission, a signal at the end of a character that prepares the receiving device for the reception of a subsequent character. A stop signal is usually limited to one signal element having any duration equal to or greater than a specified minimum value. (FP) (ISO) (~)
2. A signal to a receiving mechanism to wait for the next signal. (FP) See also control character, overhead bit, start signal.

Stop-Record Signal

In facsimile systems, a signal used for stopping the process of converting the electrical signal to an image on the record sheet. (~) See also facsimile, signal.

*-Stoppage

/sto'p*j/ n. Extreme lossage that renders something (usually something vital) completely unusable. “The recent system stoppage was caused by a fried transformer. ”

Storage

1. The retention of data in any form, usually for the purpose of orderly retrieval and documentation. (JCS1-DoD)
2. A device consisting of electronic, electrostatic, electrical, hardware or other elements into which data may be entered, and from which data may be obtained, as desired. (JCS1-DoD) See also erase, fetch protection, read-only storage, register.

#-Storage Area Controls

This KSA has no definition.

Storage Cell

1. [In information processing,] An addressable storage unit. (FP)
2. [In information processing,] The smallest subdivision of storage into which a unit of data has been or can be entered, in which it is or can be stored, and from which it can be retrieved. (FP) See storage element.

Storage Element

See storage cell.

#-Storage Media Protection And Control

This KSA has no definition.

Storage Object

An object that supports both read and write accesses. (CSC-STD-001-83;; *DCID* 1/16-1, Sup. ;; *NCSC-WA*-001-85;)

Storage Register

See register.

*-Store

n. [prob. from techspeak `main store'] In some varieties of Commonwealth hackish, the preferred synonym for core. Thus, `bringing a program into store' means not that one is returning shrink-wrapped software but that a program is being swapped in

Store-And-Forward

(S-F) Applied to communication systems in which messages are received at intermediate routing points and recorded (stored). They are then transmitted (forwarded) to a further routing point or to the ultimate recipient. (~) See also electronic mail, message switching.

Stored-Program Computer

A computer controlled by internally stored instructions, that can synthesize and store instructions, and that can subsequently execute those instructions. (FP)

Streamer

See streaming tape drive.

Streaming Tape Drive

A magnetic tape unit especially designed to make a nonstop dump or restore magnetic disks without stopping at interblock gaps. (FP) (ISO) See streamer.

Streaming Tape Recording

A method of recording on magnetic tape that maintains continuous tape motion without the requirement to start and stop within the interrecord gap. (FP)

*-Strided

/str:'d*d/ adj. [scientific computing] Said of a sequence of memory reads and writes to addresses, each of which is separated from the last by a constant interval called the `stride length'. These can be a worst-case access pattern for the standard memory-caching schemes when the stride length is a multiple of the cache line size. Strided references are often generated by loops through an array, and (if youre data is large enough that access-time is significant) it can be worthwhile to tune for better locality by inverting double loops or by partially unrolling the outer loop of a loop nest. This usage is borderline techspeak; the related term `memory stride' is definitely techspeak.

String

A sequence of elements of the same type, such as characters, considered as a whole. (FP) (ISO)

*-Stroke

n. Common name for the slant (`/', ASCII 0101111) character. See ASCII for other synonyms.

Structured Programming

A technique for organizing and coding [computer] programs in which a hierarchy of modules is used, each having a single entry and a single exit point, and in which control is passed downward through the structure without unconditional branches to higher levels of the structure. Three types of control flow are used: sequential, test, and iteration. (FP)

Structured Protection

(Class B2) Enhanced-level Trusted Computing Base (TCB) which provides intermediate-level Mandatory Access Control (MAC) protection features, as well as enhanced Discretionary Access Control (DAC) features. Sensitivity labels are used to enforce access control decisions and are based on a formally specified security policy model that documents rules for how each and every subject (users, programs) may access each and every object (files, records). Operational support features are provided, such as a Trusted Facility Manual, System Security Officer, and Administrator functions, and stringent configuration management practices.

*-Strudel

n. Common (spoken) name for the at-sign (`@', ASCII 1000000) character. See ASCII for other synonyms.

*-Stubroutine

/stuhb'roo-teen/ n. [contraction of `stub subroutine'] Tiny, often vacuous placeholder for a subroutine that is to be written or fleshed out later.

*-Studly

adj. Impressive; powerful. Said of code and designs which exhibit both complexity and a virtuoso flair. Has connotations similar to hairy but is more positive in tone. Often in the emphatic `most studly' or as noun-form `studliness'. “Smail 3. 0's configuration parser is most studly. ”

*-Studlycaps

/stuhd'lee-kaps/ n. A hackish form of silliness similar to BiCapitalization for trademarks, but applied randomly and to arbitrary text rather than to trademarks. ThE oRigiN and SigNificaNce of thIs pRacTicE iS oBscuRe.

Stuffing

See bit stuffing, de-stuffing.

*-Stunning

adj. Mind-bogglingly stupid. Usually used in sarcasm. “You want to code *what* in ADA? That's a . stunning idea!”

Stunt Box

A device that controls the nonprinting functions of a printer at a terminal.

*-Stupid-Sort

n. Syn. bogo-sort.

*-Stupids

n. Term used by samurai for the suits who employ them; succinctly expresses an attitude at least as common, though usually better disguised, among other subcultures of hackers. There may be intended reference here to an SF story originally published in 1952 but much anthologized since, Mark Clifton's “Star, Bright”. In it, a super-genius child classifies humans into a very few `Brights' like herself, a huge majority of `Stupids', and a minority of `Tweens', the merely ordinary geniuses.

*-Sturgeon's Law

prov. “Ninety percent of everything is worthless”. Derived from a quote by science fiction author Theodore Sturgeon, who once said, “Sure, 90% of science fiction is crud. That's because 90% of everything is crud. ” Oddly, when Sturgeon's Law is cited, the final word is almost invariably changed to 'crud'. Compare Hanlon's Razor, Ninety-Ninety Rule. Though this maxim originated in SF fandom, most hackers recognize it and are all too aware of its truth

Subassembly

Major subdivision of a cryptographic assembly which consists of a package of parts, elements, and circuits that performs a specific function.

Subcommittee On Automated Information Systems Security (SAISS)

NSDD-145 authorizes and directs the establishment, under the NTISSC, of a permanent Subcommittee on Automated Information Systems Security. The SAISS is composed of one voting member from each organization represented on the NTISSC.

Subcommittee On Automated Information Sytemse Security (SAISS)

The NDSS-145 authorizes and directs the establishment, under the NTISSC, of a permanent Subcommittee on Automated Information Systems Security. The SAISS is chaired by the Director, National Computer Security Center and composed of one voting member from each organization represented on the NTISSC. (*NCSC-WA*-001-85;)

Subcommittee On Compromising Emanations

(SCOCE) This subcommittee, composed of representatives rom various government organizations, is charged with specific responsibilities designed to implement Government-wide programs for the control and suppression of compromising emanations. In carrying out these responsibilities it is an instrument for exchanging technical TEMPEST information, techniques, and criteria among Government organizations and their contractors.

Subcommittee On Telecommunications Security

The NSDD-145; authorizes and directs the establishment, under the NTISSC, of a permanent Subcommittee on Telecommunications Security. The STS is composed of one voting member from each organization represented on the NTISSC. (*NCSC-WA*-001-85;)

Subject

An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair. (CSC-STD-001-83;; *AFR* 205-16;; *NCSC-WA*-001-85;; *DCID* 1/16-1, Sup. ;)

Subject Security Level

A subjects security level is equal to the security level of the objects to which it has both read and write access. A subjects security level must always be dominated by the clearance of the user with which the subject is associated.

Subject Sensitivity Level

Subject's Security Level

1. A subject's security level is equal to the security level of the objects to which it has either read only or both read and write access. A subject's security level must always be dominated by the session security level. (*DCID* 1/16-1, Sup. ;)
2. The security level of the objects to which the subject has both read and write access. A subject's security level must always be greater than or equal to the clearance of the user the subject is associated with. (*NCSC-WA*-001-85;; CSC-STD-001-83;)

Subroutine

A set of computer instructions to carry out a predefined function or computation. Note: “Open” subroutines are integrated into the main program. “Closed” subroutines are arranged so that program control is shifted to them for execution of their task(s) and then returned to the main program.

Subscriber Sets And End Terminal Equipments

The complete assembly of equipment, exclusive of interconnecting wire lines, located on the enduser's or customer's premises. This includes such items as telephones, teletypewriters, facsimile data sets, input-output devices, switchboards, patchboards, and consoles. (NACSIM 5203)

Subset-Domain

Subsystem
Component of an AIS, which may be software or hardware, that performs a specific function or functions.

Successful Block Delivery
The transfer of a nonduplicate user information block between the source user and intended destination user. Note: Successfully delivered blocks include incorrect blocks in addition to successfully transferred (correct) blocks. See also block, block transfer failure.

Successful Block Transfer
The transfer of a correct, nonduplicate, user information block between the source user and intended destination user. Note: Successful block transfer occurs at the moment when the last bit of the transferred block crosses the functional interface between the telecommunication system and the intended destination user. Successful block transfer can only occur within a defined maximum block transfer time after initiation of a block transfer attempt. See also block, block transfer attempt, block transfer failure, block transfer time, maximum block transfer time.

Successful Disengagement
The termination of user information transfer between a source user and a destination user in response to a disengagement request. Note: Successful disengagement occurs at the earliest moment at which either user is able to initiate a new information transfer transaction. See also access phase, disconnect, disengagement attempt, disengagement failure, disengagement phase, disengagement request, information-transfer phase.

*-Sucking Mud
[Applied Data Research] adj. (also `pumping mud') Crashed or wedged. Usually said of a machine that provides some service to a network, such as a file server. This Dallas regionalism derives from the East Texas oilfield lament, “Shut 'er down, Ma, she's a-suckin' mud”. Often used as a query. “We are going to reconfigure the network, are you ready to suck mud?”:sufficiently smalladj. Syn. suitably small.

*-Suit
1. n. Ugly and uncomfortable `business clothing' often worn by non-hackers. Invariably worn with a `tie', a strangulation device that partially cuts off the blood supply to the brain. It is thought that this explains much about the behavior of suit-wearers. Compare droid.
2. A person who habitually wears suits, as distinct from a techie or hacker. See loser, burble, management, Stupids, SNAFU principle, and brain-damaged. English, by the way, is relatively kind; our Moscow correspondent informs us that the corresponding idiom in Russian hacker jargon is `sovok', lit. a tool for grabbing garbage. suitable win. See win.

*-Suitably Small
adj. [perverted from mathematical jargon] An expression used ironically to characterize unquantifiable behavior that differs from expected or required behavior. For example, suppose a newly created program came up with a correct full-screen display, and one publicly exclaimed It works!” Then, if the program dumped core on the first mouse click, one might add Well, for suitably small values of `works'. ” Compare the characterization of pi under random numbers. sun loungen. [UK] The room where all the Sun workstations live. The humor in this term comes from the fact that it's also in mainstream use to describe a solarium, and all those Sun workstations clustered together give off an amazing amount of heat.

Sum Check
See summation check.

Summation Check
A check based on the formation of the sum of the digits of a numeral. The sum of the individual digits is usually compared with a previously computed value. (FP) (ISO) See sum check.

*-Sun-Stools
n. Unflattering hackerism for SunTools, a pre-X windowing environment notorious in its day for size, slowness, and misfeatures. X, however, is larger and slower; see second-system effect.

*-Sunspots
1. n. Notional cause of an odd error. “Why did the program suddenly turn the screen blue?” “Sunspots, I guess. ”
2. Also the cause of bit rot -- from the myth that sunspots will increase cosmic rays, which can flip single bits in memory. See also phase of the moon.

*-Super Source Quench
n. A special packet designed to shut up an Internet host. The Internet Protocol (IP) has a control message called Source Quench that asks a host to transmit more slowly on a particular connection to avoid congestion. It also has a Redirect control message intended to instruct a host to send certain packets to a different local router. A “super source quench” is actually a redirect control packet, forged to look like it came from a local router, that instructs a host to send all packets to its own local loopback address. This will effectively tie many Internet hosts up in knots. Compare Godzillagram, breath-of-life packet

Superencryption

The process of encrypting encrypted information. Note: This process occurs when a message encrypted off-line is transmitted over a secured circuit or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.

Supergroup

See group, multiplex hierarchy.

*-Superprogrammer

n. A prolific programmer; one who can code exceedingly well and quickly. Not all hackers are superprogrammers, but many are. (Productivity can vary from one programmer to another by three orders of magnitude. For example, one programmer might be able to write an average of 3 lines of working code in one day, while another, with the proper tools, might be able to write 3,000. This range is astonishing; it is matched in very few other areas of human endeavor.) The term `superprogrammer' is more commonly used within such places as IBM than in the hacker community. It tends to stress naive measures of productivity and to underweight creativity, ingenuity, and getting the job *done* -- and to sidestep the question of whether the 3,000 lines of code do more or less useful work than three lines that do the Right Thing. Hackers tend to prefer the terms hacker and wizard

Supersession

Scheduled or unscheduled replacement of a COMSEC aid with a different edition.

Supershell

A partially instantiated expert system, but without any data. Only the structure and application-specific parts that are common to all the expert systems to be created from it are included. (ET;, MA;)

*-Superuser

n. [UNIX] Syn. root, avatar. This usage has spread to non-UNIX environments; the superuser is any account with all wheel bits on. A more specific term than wheel.

Supervisor

See supervisory program.

Supervisor State

See Executive State.

Supervisory Control

The use of characters or signals to automatically actuate equipment or indicators. See also character, signal, supervisory signals.

Supervisory Program

1. A program, usually part of an operating system, that controls the execution of other routines and regulates work scheduling, input-output operations, error actions, and similar functions. (~) See also control station.
2. A computer program that allocates computer component space and schedules computer events by task queueing and system interrupts. Note: Control of the system is returned to the supervisory program frequently enough to ensure that demands on the system are met.
3. . A computer program, usually part of an operating system, that controls the execution of other computer programs and regulates the flow of work in a data processing system. (FP) (ISO) See s executive program, supervisor.

Supervisory Routine

A routine that allocates computer component space and schedules computer events by task queueing and system interrupts. Note: Control of the system is returned to the supervisory program frequently enough to ensure that demands on the system are met.

Supervisory Signals

Signals used to indicate (or, in modern usage, to indicate and to control) the various operating states of the circuits or circuit combinations involved in a particular connection. (~) See also forward busying, orderwire circuit, signal, supervisory control.

Supplies

An asset category consisting of consumable items in the installation. (RM;)

*-Support

n. After-sale handholding; something many software vendors promise but few deliver. To hackers, most support people are useless -- because by the time a hacker calls support he or she will usually know the software and the relevant manuals better than the support people (sadly, this is *not* a joke or exaggeration). A hacker's idea of `support' is a t^ete-`a-t^ete with the software's designer.

Suppression

The reduction of the levels of compromising emanations.

Suppression Measure

Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in a telecommunications or automated information system.

*-Surf

v. To traverse the Internet in search of interesting stuff, used esp. if one is doing so with a World-Wide-Web browser. It is also common to speak of `surfing in' to a particular resource.

Surveillance

The systematic observation or monitoring of places, persons, or things by visual, aural, electronic, photographic, or other means. *The systematic observation or monitoring of places, persons, or things by visual, aural, electronic, photographic, or other means. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Survivability

A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; e. g. , nuclear attack. (~) Note: This term must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration. See also communications system, continuous operation, electromagnetic survivability, endurability.

Survivable Operation

See survivability.

Susceptibility

1. The state or quality of being more exploitable due to a higher level of sensitivity of operations. (*AR* 380-380;)
2. Inability of a system to prevent: a. An electronic compromise of National Security Information or, b. Detrimental affects on its operational integrity.

*-Suzie COBOL

1. /soo'zee koh'bol/ [IBM prob. from Frank Zappa's `Suzy Creamcheese'] n. A coder straight out of training school who knows everything except the value of comments in plain English. Also (fashionable among personkind wishing to avoid accusations of sexism) `Sammy Cobol' or (in some non-IBM circles) `Cobol Charlie'.
2. [proposed] Meta-name for any code grinder, analogous to J. Random Hacker.

*-Swab

/swob/ [From the mnemonic for the PDP-11 `SWAp Byte' instruction, as immortalized in the `dd(1)' option `conv=swab' (see dd)]

1. vt. To solve the NUXI problem by swapping bytes in a file.
2. n. The program in V7 UNIX used to perform this action, or anything functionally equivalent to it. See also big-endian, little-endian, middle-endian,.

*-Swap

1. vt. [techspeak] To move information from a fast-access memory to a slow-access memory (`swap out'), or vice versa (`swap in'). Often refers specifically to the use of disks as `virtual memory'. As pieces of data or program are needed, they are swapped into core for processing; when they are no longer needed they may be swapped out again.
2. The jargon use of these terms analogizes people's short-term memories with core. Cramming for an exam might be spoken of as swapping in. If you temporarily forget someone's name, but then remember it, your excuse is that it was swapped out. To `keep something swapped in' means to keep it fresh in your memory “I reread the TECO manual every few months to keep it swapped in. ” If someone interrupts you just as you got a good idea, you might say “Wait a moment while I swap this out”, implying that a piece of paper is your extra-somatic memory and that if you don't swap the idea out by writing it down it will get overwritten and lost as you talk. Compare page in, page out.

*-Swap Space

n. Storage space, especially temporary storage space used during a move or reconfiguration. “I'm just using that corner of the machine room for swap space. ”

*-Swapped In

n. See swap. See also page in.

*-Swapped Out

n. See swap. See also page out.

Switchboard

Equipment with which switching operations are performed manually. (~) See also cord circuit, PBX.

*-Swizzle

v. To convert external names, array indices, or references within a data structure into address pointers when the data structure is brought into main memory from external storage (also called `pointer swizzling'); this may be done for speed in chasing references or to simplify code (e. g. , by turning lots of name lookups into pointer dereferences). The converse operation is sometimes termed `unswizzling'. See also snap.

Syllabary

List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. NOTE: A syllabary may also be known as a spelling table.

Syllable

A character string or a bit string in a word. (FP)

Symbolic Language

A computer programming language used to express addresses and instructions with symbols convenient to humans rather than to machines.

Symbolic Logic

The discipline in which valid arguments and operations are dealt with using an artificial language designed to avoid the ambiguities and logical inadequacies of natural languages. (FP) (ISO)

*-Sync

1. /sink/ n. , vi. (var. `synch') To synchronize, to bring into synchronization.
2. [techspeak] To force all pending I/O to the disk; see flush, sense 2.
3. More generally, to force a number of competing processes or agents to a state that would be `safe' if the system were to crash; thus, to checkpoint (in the database-theory sense).

Synchronism

The state of being synchronous. See also synchronous network.

Synchronization

The process of attaining synchronism. (~) See also acquisition time, analog synchronization, bilateral synchronization, bit-synchronous operation, carrier synchronization, double-ended synchronization, frame synchronization, linear analog synchronization, mutually synchronized network, single-ended synchronization, synchronization code, synchronous data link control, synchronous data network, unilateral synchronization system.

Synchronization Bit

A binary digit used to achieve or maintain synchronism. (~)

Note: The term “synchronization bit” is usually applied to digital data streams, whereas the term “synchronization pulse” is usually applied to analog signals. See also binary digit, bit synchronization, character, digit, timing signal.

Synchronization Code

In digital systems, a sequence of digital symbols introduced into a transmission signal to achieve or maintain synchronism. See also frame synchronization, synchronization, synchronous data network.

Synchronization Flags

Synchronized Network

See democratically synchronized network, hierarchically synchronized network, master-slave timing, mutually synchronized network, oligarchically synchronized network.

Synchronous

Pertaining to two or more processes that depend upon the simultaneous occurrence of specific events such as a common timing signal. (~) Note: “Isochronous” and “anisochronous” are characteristics, while “synchronous” and “asynchronous” are relationships. See also asynchronous transmission, bit-by-bit asynchronous operation, frame-alignment time slot, frame duration, framing.

#-Synchronous Communication

pronounced “sink' -roh-nuss. ” The transmission of data at very high speeds using parallel circuits in which the transfer of data is synchronized by electronic clock signals. Synchronous communication is used within the computer and in high-speed mainframe computer networks. (Source: “Que's Computer User's Dictionary, “Bryan Pfaffenberger, Ph. D. 1990).

Synchronous Crypto-Operation

Method of on-line crypto-operation in which crypto-equipment and associated terminals have timing systems to keep them in step.

Synchronous Data Link Control

A bit-oriented protocol for the control of synchronous transmission over data links in a data network. See also Advanced Data Communication Control Procedure, binary synchronous communication, data, data transmission, link, network, synchronization.

Synchronous Data Network

A data network in which synchronism is achieved and maintained between data circuit-terminating equipment (DCE) and the data switching exchange (DSE), and between DSEs. (~) Note: The data signaling rates are controlled by timing equipment within the network. See also data circuit-terminating equipment, data switching exchange, link (def. #1), synchronization, synchronization code.

Synchronous Idle Character

A transmission control character used in synchronous transmission systems to provide a signal from which synchronism or synchronous correction may be achieved between data terminal equipment, particularly when no other character is being transmitted. (FP) (ISO)

Synchronous Network

A network in which clocks are controlled so as to run, ideally, at identical rates, or at the same mean rate with limited but constant relative phase displacement. (~) Note: Ideally, the clocks are synchronous, but they may be mesochronous in practice. By common usage, such mesochronous networks are frequently described as synchronous. See also clock, data transmission, synchronism.

Synchronous TDM

A multiplexing scheme in which timing is obtained from a clock that in turn controls both the multiplexer and the channel source. (~) See also asynchronous

time-division multiplexing, time-division multiplexing.

Synchronous Transfer Mode

A proposed transport level, a time-division multiplex-and-switching technique to be used across the user's network interface for a broadband ISDN. See also Integrated Services Digital Network.

Synchronous Transmission

Data transmission in which the time of occurrence of each signal representing a bit is related to a fixed time base. (FP) (ISO) (~) Note: “Isochronous” and “anisochronous” are characteristics, while “synchronous” and “asynchronous” are relationships. See also asynchronous transmission, bit-by-bit asynchronous operation, frame-alignment time slot, frame duration, framing.

*-Syntactic Salt

n. The opposite of syntactic sugar, a feature designed to make it harder to write bad code. Specifically, syntactic salt is a hoop the programmer must jump through just to prove that he knows what's going on, rather than to express a program action. Some programmers consider required type declarations to be syntactic salt. A requirement to write `end if', `end while', `end do', etc. to terminate the last block controlled by a control construct (as opposed to just `end') would definitely be syntactic salt. Syntactic salt is like the real thing in that it tends to raise hackers' blood pressures in an unhealthy way. Compare candygrammar.

*-Syntactic Sugar

n. [coined by Peter Landin] Features added to a language or other formalism to make it `sweeter' for humans, features which do not affect the expressiveness of the formalism (compare chrome). Used esp. when there is an obvious and trivial translation of the `sugar' feature into other constructs already present in the notation. C's `a[i]' notation is syntactic sugar for `*(a + i)'. “Syntactic sugar causes cancer of the semicolon. ” -- Alan Perlis. The variants `syntactic saccharin' and `syntactic syrup' are also recorded. These denote something even more gratuitous, in that syntactic sugar serves a purpose (making something more acceptable to humans), but syntactic saccharin or syrup serve no purpose at all. Compare candygrammar, syntactic salt.

Syntax

1. The relationships among characters or groups of characters, independent of their meanings or the manner of their interpretation and use. (FP)
2. The structure of expressions in a language. (FP)
3. The rules governing the structure of a language. (FP)
4. The relationship among symbols. (FP)

*-Sys-Frog

/sis'frog/ n. [the PLATO system] Playful variant of `sysprog', which is in turn short for `systems programmer'.

*-Sysadmin

/sis'ad-min/ n. Common contraction of `system admin'; see admin.

*-Sysape

/sys'ayp/ n. A rather derogatory term for a computer operator; a play on sysop common at sites that use the banana hierarchy of problem complexity (see one-banana problem).

Sysop

(1) The SYStem OPerator. (BBD;) (2) /sis'op/ n. [esp. in the BBS world] The operator (and usually the owner) of a bulletin-board system. A common neophyte mistake on FidoNet is to address a message to `sysop' in an international echo, thus sending it to hundreds of sysops around the world.

System

1. An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, controlling or receiving data with a minimum of human intervention. (CSC-STD-003-85;; *AFR* 205-16;; CSC-STD-004-85;) See Automated Information System (AIS).
2. A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement. *A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement. (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)
3. See ADP SYSTEM, AUTOMATED INFORMATION SYSTEM, CIPHER SYSTEM, CODE SYSTEM, CONCEALMENT SYSTEM, CRYPTOGRAPHIC SYSTEM, LOCK-AND-KEY PROTECTION SYSTEM, PROTECTED WIRELINE DISTRIBUTION SYSTEM, and SECURE OPERATING SYSTEM.

System Administration

System Administrator

System Analysis

A systematic investigation of a real or planned system to determine the functions of the system and how they relate to each other and to any other system. (FP) (ISO) See systems analysis.

System Architecture

System Design

System Development

Methodologies developed through software methodologies engineering to manage the complexity of system development. NOTE: Development methodologies include software engineering aids and high-level design analysis tools.

System Development Methodologies

Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

System Documentation

The collection of documents that describes the requirements, capabilities, limitations, design, operation, and maintenance of an information processing system. (FP) (ISO)

System Environment

Configuration of an AIS.

Physical conditions of temperature, humidity, and so forth.

System Generation

The process of selecting optional parts of an operating system and of creating a particular operating system tailored to the requirements of a data processing installation. (FP) (ISO)

System High

Highest security level supported by an AIS. See System Low.

System High Mode

AIS security mode of operation wherein each user, with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:(a)Valid security clearance for all information within an AIS. (b)Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs). (c)Valid need-to-know for some of the information contained within the AIS.

System High Mode Or System High Security Mode

AIS security mode of operation wherein each user, with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:

1. Valid security clearance for all information within an AIS.
2. Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, and/or special access programs).
3. . Valid need-to-know for some of the information contained within the AIS. NOTE: See Modes of Operation.

System High Security Mode

1. A mode of operation where all personnel with access to the automated system have a security clearance but not a need-to-know for all material then contained in the system. A system operates in the system high security mode when the central computer facility and all of its connected peripheral devices and remote terminals are protected according to the requirement for the highest classifica- tion of material contained in the system. In this mode, the system design and operation must provide for some internal control of concurrently available classified material in the system on the basis of need-to-know. (*AFR* 205-16;; *AFR* 700-10;; *OPNAVINST* 5239. 1A;)
2. The mode of operation in which system hardware/software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/orstored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed. (CSC-STD-003-85;)
3. A mode of operation wherein all users having access to the AIS possess a security clearance and formal access approval but not necessarily a need-to-know for all data handled by the AIS. (DODD 5200. 28;)
4. The mode of operation in which the computer system and all of its connected peripheral devices and

remote terminals are protected in accordance with the requirements for the highest security level of material contained in the system at that time. All personnel having access to the Automated Information System have a security clearance but not a need-to-know for all material then contained in the system. (*NCSC-WA*-001-85;)

System Indicator

Symbol or group of symbols in an off-line encrypted message that identifies the specific cryptosystem or key used in the encryption.

System Integration

The progressive linking and testing of system components to merge their functional and technical characteristics into a comprehensive, interoperable system. Note: Integration of data systems allows data existing on disparate systems to be shared or accessed across functional or system boundaries.

System Integrity

1. The state that exists when there is complete assurance that under all conditions an automated system is based on the logical correctness and reliability of the operating hardware and software that implement the protection mechanisms, and data soundness. (*AR* 380-380)
2. The state that exists when there is complete assurance that under all conditions an ADP system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity. (*FIPS PUB* 39)
3. The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (*NCSC-TG*-004-88)

System Integrity Procedures

1. The procedure established for assuring that the hardware, software and data in an automated system maintain their state of original integrity. (*AR* 380-380;)
2. The procedure established for assuring that the hardware, software and data in an ADP system maintain their state of original integrity and are not tampered with by program changes. (*FIPS PUB* 39;)

System Life Cycle

The course of developmental changes through which a system passes from its conception to the termination of its use; for example, the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system. (FP)

System Loading

In an FDM transmission system, the absolute power level, referred to a zero transmission level point, of the composite signal (speech, data, and signaling) transmitted in one direction. (~) See also level (def. #1), loading, transmission level point.

System Low

The lowest security level supported by a system at a particular time or in a particular environment. (*NCSC-WA*-001-85;)

System Manager

The ADP official who is responsible for the operation of an ADP system. (*FIPS PUB* 112;)

*-System Mangler

n. Humorous synonym for `system manager', poss. from the fact that one major IBM OS had a root account called SYSMANGR. Refers specifically to a systems programmer in charge of administration, software maintenance, and updates at some site. Unlike admin, this term emphasizes the technical end of the skills involved.

System Of Records

System Operational Threshold

A defined value, for a supported performance parameter, which value establishes the minimum operational service performance level for the parameter. (~) Note: A measured parameter value worse than the associated outage threshold indicates that the telecommunication service is in an outage state. See also performance parameter.

System Operator

System Overhead Information

See overhead information.

System Programmer

System Report

System Security

1. Measure of security provided by a system, as determined by evaluation of the totality of all system elements and COMSEC measures that support telecommunications and AIS protection.
2. The efforts that help achieve maximum engineering security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort.

3. Determination of the risk associated evaluation with the use of a given system, considering its vulnerabilities and perceived security threat.
4. A formal document that fully describes management plan the planned security tasks required to meet system security requirements.

#-System Security Architecture Study

Ensure the system architecture supports and security CONOPS to the system. (Source: DACUM IV).

#-System Security Engineering

(SSE) The efforts that help achieve maximum security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort. *An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats. (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

System Security Evaluation

Determination of the risk associated with the use of a given system, considering its vulnerabilities and perceived security threat. *Determination of the risk associated with the use of a given system, considering the vulnerabilities in the system and the threat against it. (NSA, *National INFOSEC Glossary*, 10/88)

System Security Management Plan

(SSMP) A formal document that fully describes the planned security tasks required to meet system security requirements. *A formal document that fully describes the planned security tasks required to meet system security requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering, design, and management activities, and related systems. (DoD, System Security Engineering Program Management Requirements, MIL-STD 1785, 9/89)

System Security Map

System Security Officer

1. The person responsible for the security of an ADP system. The SSO is authorized to act in the "security administrator" role as defined in CSC-STD-001-83;. Functions that the SSO is expected to perform include auditing and changing security characteristics of a user. (CSC-STD-002-85;; CSC-STD-005-85;)
2. The person(s) responsible for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal. (DODD 5200. 28;)
3. The person responsible for the security of an Automated Information System and having the authority to enforce the security safeguards on all others who have access to the Automated Information System. (*NCSC-WA*-001-85;)
4. Synonymous with Computer System Security Officer (CSSO).

System Software

Routines and programs designed to extend or facilitate the use of particular automated equipment. System software is usually provided by the vendor and is essential for system operation. Some examples are operating systems, compilers, and assemblers.

#-System Software Controls

This KSA has no definition.

System Support

The continued provision of services and material necessary for the use and improvement of a system after the system has been adopted. (FP) (ISO)

System Test Time

That part of operating time during which the functional unit is tested for proper operation. Since a functional unit may consist of a computer and its operating system, system test time in some cases includes the time for testing computer programs belonging to the operating system. (FP) (ISO)

#-System Testing And Evaluation Process

This KSA has no definition.

System Tests

System Users

Users with direct connections to the system and also those individuals without direct connections who receive output or generate input that is not reliably reviewed for classification by a responsible individual. The clearance of system users is used in the calculation of the risk index. (CSC-STD-003-85;, CSC-STD-004-85;, *NCSC-WA*-001-85;)

#-System-High Mode

Security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: a. Valid security clearance for all information within the system; b. Formal access approval and signed non-disclosure agreements for all of the information stored and/or processed (including all compartments, subcompartments and/or special access programs) (Source: *NCSC-TG*-029).

Systems Analysis

See system analysis.

Systems Design

1. A process of defining the hardware and software architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. (FP) (ISO)
2. The preparation of an assembly of methods, procedures, or techniques united by regulated interaction to form an organized whole. (JCS1-DoD) (JCS1-NATO)

Systems Of Records

Systems Security Steering Group

The NSDD-145; establishes a Steering Group to oversee the NSDD-145; and to ensure its implementation. This group is chaired by the Assistant to the President for National Security Affairs and consists of the Secretary of State, Secretary of Treasury, the Secretary of Defence, the Attorney General, the Director of Office of Management and Budget, and the Director of Central Intelligence. (*NCSC-WA*-001-85;)

*-SysVile

/sis-vi:l'/ n. See Missed'em-five.

T

Tactical Communication System

A system configured by various types of fixed-size, self-contained assemblages, such as radio terminals and repeaters; switching, transmission, and terminal equipment; and interconnect and control facilities, that are used within or in support of tactical forces and are designed to meet the requirements of changing tactical situations. (~) Note: The system provides securable voice and data communications among mobile users to facilitate command and control within, and in support of, tactical forces. Based on different requirements of the multichannel trunking networks, a distinction is made between: (a) tactical systems requiring extremely short facility-installation times (on the order of hours), necessitated by relocation requirements that are sometimes frequent, and (b) other tactical telecommunication systems. See also communications system, TRI-TAC equipment.

*-Tail Recursion

n. If you aren't sick of it already, see tail recursion.

Tailing

In facsimile systems, the excessive prolongation of the decay of the signal. (~) See hangover. See also facsimile, underlap.

*-Talk Mode

n. A feature supported by UNIX, ITS, and some other OSes that allows two or more logged-in users to set up a real-time on-line conversation. It combines the immediacy of talking with all the precision (and verbosity) that written language entails. It is difficult to communicate inflection, though conventions have arisen for some of these (see the section on writing style in the Prependices for details). Talk mode has a special set of jargon words, used to save typing, which are not used orally. Some of these are identical to (and probably derived from) Morse-code jargon used by ham-radio amateurs since the 1920s. AFAIK as far as I know BCNU be seeing you BTW by the way BYE? are you ready to unlink? (this is the standard way to end a talk-mode conversation; the other person types `BYE' to confirm, or else continues the conversation) CUL see you later ENQ? are you busy? (expects `ACK' or `NAK' in return) FOO? are you there? (often used on unexpected links, meaning also “Sorry if I butted in . ” (linker) or “What's up?” (linkee)) FWIW for what it's worth FYI for your information FYA for your amusement GA go ahead (used when two people have tried to type simultaneously; this cedes the right to type to the other) GRMBL grumble (expresses disquiet or disagreement) HELLOP hello? (an instance of the `-P' convention) JAM just a minute (equivalent to `SEC. ') MIN same as `JAM' NIL no (see NIL) O over to you OO over and out / another form of “over to you” (from x/y as “x over y”) \ lambda (used in discussing LISPy things) OBTW oh, by the way OTOH on the other hand R U THERE? are you there? SEC wait a second (sometimes written `SEC. ') T yes (see the main entry for T) TNX thanks TNX 1. 0E6 thanks a million (humorous) TNXE6 another form of “thanks a million” WRT with regard to, or with respect to. WTF the universal interrogative particle; WTF knows what it means? WTH what the hell? <double newline> When the typing party has finished, he/she types two newlines to signal that he/she is done; this leaves a blank line between `speeches' in the conversation, making it easier to reread the preceding text. <name>: When three or more terminals are linked, it is conventional for each typist to prepend his/her login name or handle and a colon (or a hyphen) to each line to indicate who is typing (some conferencing facilities do this automatically). The login name is often shortened to a unique prefix (possibly a single letter) during a very long conversation. /\/\/\ A giggle or chuckle. On a MUD, this usually means `earthquake fault'. Most of the above sub-jargon is used at both Stanford and MIT. Several of these expressions are also common in email, esp. FYI, FYA, BTW, BCNU, WTF, and CUL. A few other abbreviations have been reported from commercial networks, such as GEnie and CompuServe, where on-line `live' chat including more than two people is common and usually involves a more `social' context, notably the following <g> grin <gr&d> grinning, running, and ducking BBL be back later BRB be right back HHOJ ha

ha only joking HHOK ha ha only kidding HHOS ha ha only serious IMHO in my humble opinion (see IMHO) LOL laughing out loud NHOH Never Heard of Him/Her (often used in initgame) ROTF rolling on the floor ROTFL rolling on the floor laughing AFK away from keyboard b4 before CU l8tr see you later MORF male or female? TTFN ta-ta for now TTYL talk to you later OIC oh, I see rehi hello again Most of these are not used at universities or in the UNIX world, though ROTF and TTFN have gained some currency there and IMHO is common; conversely, most of the people who know these are unfamiliar with FOO?, BCNU, HELLOP, NIL, and T. The MUD community uses a mixture of Usenet/Internet emoticons, a few of the more natural of the old-style talk-mode abbrevs, and some of the `social' list above; specifically, MUD respondents report use of BBL, BRB, LOL, b4, BTW, WTF, TTFN, and WTH. The use of `rehi' is also common; in fact, mudders are fond of re- compounds and will frequently `rehug' or `rebonk' (see bonk/oif) people. The word `re' by itself is taken as `regreet'. In general, though, MUDders express a preference for typing things out in full rather than using abbreviations; this may be due to the relative youth of the MUD cultures, which tend to include many touch typists and to assume high-speed links. The following uses specific to MUDs are reported CU l8er see you later (mutant of `CU l8tr') FOAD F**** off and die (use of this is generally OTT) OTT over the top (excessive, uncalled for) ppl abbrev for "people" THX thanks (mutant of `TNX'; clearly this comes in batches of 1138 (the Lucasian K)). UOK? are you OK? Some B1FFisms (notably the variant spelling `d00d') appear to be passing into wider use among some subgroups of MUDders. One final note on talk mode style eophytes, when in talk mode, often seem to think they must produce letter-perfect prose because they are typing rather than speaking. This is not the best approach. It can be very frustrating to wait while your partner pauses to think of a word, or repeatedly makes the same spelling error and backs up to fix it. It is usually best just to leave typographical errors behind and plunge forward, unless severe confusion may result; in that case it is often fastest just to type "xxx" and start over from before the mistake. See also hakspek, emoticon. t

*-Talker System

n. British hackerism for software that enables real-time chat or talk mode. tall card. A PC/AT-size expansion card (these can be larger than IBM PC or XT cards because the AT case is bigger). See also short card. When IBM introduced the PS/2 model 30 (its last gasp at supporting the ISA) they made the case lower and many industry-standard tall cards wouldn't fit; this was felt to be a reincarnation of the connector conspiracy, done with less style.

Tamper-Indicative Seal

A special seal, approved by NSA, that can be used to seal physical objects, such as ADP terminal workstations. The unauthorized removal of such a seal is clearly recognizable. (JCS PUB 6-03. 7)

Tampering

An unauthorized modification which alters the proper functioning of a system or piece of equipment in a manner which degrades the security it provides. (*NCSC-WA*-001-85;)

*-Tanked

adj. Same as down, used primarily by UNIX hackers. See also hosed. Popularized as a synonym for `drunk' by Steve Dallas in the late lamented "Bloom County" comic strip.

*-TANSTAAFL

/tan'stah-fl/ [acronym, from Robert Heinlein's classic "The Moon is a Harsh Mistress".] "There Ain't No Such Thing As A Free Lunch", often invoked when someone is balking at the prospect of using an unpleasantly heavyweight technique, or at the poor quality of some piece of free software, or at the signal-to-noise ratio of unmoderated Usenet newsgroups. "What? Don't tell me I have to implement a database back end to get my address book program to work!" "Well, TANSTAAFL you know. " This phrase owes some of its popularity to the high concentration of science-fiction fans and political libertarians in hackerdom (see A Portrait of J. Random Hacker in Appendix B).

Tap

In fiber optics, a device for extracting a portion of the optical signal from an optical fiber.

Tape Mixer

Teletypewriter security equipment that encrypts plain text and decrypts cipher text by combining them with a key stream from a one-time tape.

Tapes

*-Tar And Feather

vi. [from UNIX `tar(1)'] To create a transportable archive from a group of files by first sticking them together with `tar(1)' (the Tape ARchiver) and then compressing the result (see compress). The latter action is dubbed `feathering' partly for euphony and (if only for contrived effect) by analogy to what you do with an airplane propeller to decrease wind resistance, or with an oar to reduce water resistance; smaller files, after all, slip through comm links more easily.

Target

An individual, operation, or activity which an adversary has determined possesses protected information.

*In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. (Definition #2, JCS PUB 1-02, 12/89)

Tasking

See multitasking.

*-Taste

1. [primarily MIT] n. The quality in a program that tends to be inversely proportional to the number of features, hacks, and kluges programmed into it. Also `tasty', `tasteful', `tastefulness'. “This feature comes in N tasty flavors. ” Although `tasty' and `flavorful' are essentially synonyms, `taste' and flavor are not. Taste refers to sound judgment on the part of the creator; a program or feature can *exhibit* taste but cannot *have* taste. On the other hand, a feature can have flavor. Also, flavor has the additional meaning of `kind' or `variety' not shared by `taste'. The marked sense of flavor is more popular than `taste', though both are widely used. See also elegant.
2. Alt. sp. of tayste.

*-Tayste

/tayst/ n. Two bits; also as taste. Syn. crumb, quarter. See nybble.

TCSEC

DoD Trusted Computer System Evaluation Criteriaacceptance inspection. The final inspection to determine whether or not a facility or system meets the specified technical and performance standards. Note: This inspection is held immediately after facility and software testing and is the basis for commissioning or accepting the information system. See DoD Trusted Computer System Evaluation Criteria.

#-TCSEC/ITSEC/Common Criteria

This KSA has no definition.

*-Tea, ISO Standard Cup Of

n. [South Africa] A cup of tea with milk and one teaspoon of sugar, where the milk is poured into the cup before the tea. Variations are ISO 0, with no sugar; ISO 2, with two spoons of sugar; and so on. Like many ISO standards, this one has a faintly alien ring in North America, where hackers generally shun the decadent British practice of adulterating perfectly good tea with dairy products and prefer instead to add a wedge of lemon, if anything. If one were feeling extremely silly, one might hypothesize an analogous `ANSI standard cup of tea' and wind up with a political situation distressingly similar to several that arise in much more serious technical contexts. Milk and lemon don't mix very well.

Technical Attack

An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

Technical Data

1. Classified or unclassified information of any kind that can be used, or adapted for use in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation maintenance, or reconstruction of goods or munitions; or any technology that advances the state-of-the-art or establishes a new art in an area of significant military applicability in the United States. The data may be tangible, such as a model, prototype, blueprint, or an operating manual, or may be intangible, such as a technical service or oral or visual interactions. (DODD 2040. 2;)
2. Recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications standards, process sheets, manuals, technical reports, catalog item identifications, and related information and computer software documentation. (DODD 5230. 24;)

Technical Document

Any recorded information that conveys scientific and technical information or technical data. (DODD 5230. 24;)

Technical Information

Information, including scientific information, that relates to research, development, engineering, test, evaluation, production operation, use, and maintenance of munitions and other military supplies and equipment. (DODD 5230. 24;)

Technical Penetration

Deliberate penetration of a security area by technical means to gain unauthorized interception of information-bearing energy.

Technical Point Of Contact

See (TPOC)

Technical Rationale Behind Csc-Std-003-85: Computer Security Requirements

Technical Review

Technical Review Board

Technical Security

1. The set of hardware, firmware, software and supporting controls that implement security policy, accountability, assurance, and documentation as defined in CSC-STD-001-83;. (GAO;)
2. Equipment, components, devices and associated documentation or other media which pertain to cryptography or to the securing of telecommunications and automated information systems. (NSDD-145;)

#-Technical Security Guidance

Provide advice to DAA on proposed changes to systems. (DACUM IV).

Technical Security Hazard

Condition that could permit the technical penetration of an area through equipment that by reason of its normal design, installation, operation, maintenance, or damaged condition, allows the unauthorized transmission of classified information.

Technical Security Material

Equipment, components, devices, and associated documentation or other media that pertains to cryptography or the securing of telecommunications and automated information systems.

#-Technical Surveillance Countermeasures

(TSCM) Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to protected information. *Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employ of optical, electro-optical, electromagnetic, fludic, and acoustic means, as the sensor and transmission medium, or the use of various types of stimulation of or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Technical Vulnerability

1. A hardware, firmware or software weakness or design deficiency that leaves an automated information system open to potential exploitation either externally or internally, thereby resulting in risk or compromise of information, alteration of information, or denial of service. Technical vulnerability information, if made available to unauthorized persons, may allow an AIS to be exploited resulting in potentially serious damage to national security. (DODI 5215. 2;)
2. A hardware, firmware, communication, or software flaw which leaves a computer processing system open for potential exploitation either externally or internally, thereby resulting in risk for the owner, user, or manager of the system. (*NCSC-WA*-001-85;)

Technological Attack

An attack which can be perpetrated by circumventing or nullifying hardware and software access control mechanisms rather than by subverting system personnel or other users. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

#-Technological Threats

Any hardware, software, firmware, communication flaw or other circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data and or denial of service. (Source Panel of Experts).

Technology

The technical information and know how that can be used to design, produce, manufacture, use or reconstruct goods including technical data and computer software. The term does not include the goods themselves. (DODD 2040. 2;)

Technology Trade-Offs

Trade-offs, among risks; that is, the effect of technology on the development of new hardware, software, or procedures. (DoD, System Security Engineering Program management Requirements, MIL-STD 1785, 9/89)

#-Technology Trends

This KSA has no definition.

*-Techspeak. Square Tape

n. Mainframe magnetic tape cartridges for use with IBM 3480 or compatible tape drives; or QIC tapes used on workstations and micros. The term comes from the square (actually rectangular) shape of the cartridges; contrast round tape.

*-TECO

1. /tee'koh/ n. ,v. ,obs. [originally an acronym for `[paper] Tape Editor and COrrector'; later, `Text Editor and COrrector'] n. A text editor developed at MIT and modified by just about everybody. With all the dialects included, TECO may have been the most prolific editor in use before EMACS, to which it was directly ancestral. Noted for its powerful programming-language-like features and its unspeakably hairy syntax. It is literally the case that every string of characters is a valid TECO program (though probably not a useful one); one common game used to be mentally working out what the TECO commands corresponding to human names did.

2. vt. Originally, to edit using the TECO editor in one of its infinite variations (see below).
3. vt. ,obs. To edit even when TECO is *not* the editor being used! This usage is rare and now primarily historical. As an example of TECO's obscurity, here is a TECO program that takes a list of names such as Loser, J. Random Quux, The Great Dick, Moby sorts them alphabetically according to surname, and then puts the surname last, removing the comma, to produce the following Moby Dick J. Random Loser The Great Quux The program is [1 J^P$L$$ J <. -Z; . ,(S,$ -D .)FX1 @F^B $K I $ G1 L>$$ (where ^B means `Control-B' (ASCII 0000010) and $ is actually an alt or escape (ASCII 0011011) character). In fact, this very program was used to produce the second, sorted list from the first list. The first hack at it had a bugGLS (the author) had accidentally omitted the `@' in front of `F^B', which as anyone can see is clearly the Wrong Thing. It worked fine the second time. There is no space to describe all the features of TECO, but it may be of interest that `^P' means `sort' and `J<. -Z; . L>' is an idiomatic series of commands for `do once for every line'. In mid-1991, TECO is pretty much one with the dust of history, having been replaced in the affections of hackerdom by EMACS. Descendants of an early (and somewhat lobotomized) version adopted by DEC can still be found lurking on VMS and a couple of crufty PDP-11 operating systems, however, and ports of the more advanced MIT versions remain the focus of some antiquarian interest. See also retrocomputing, write-only language.

*-Tee

n. ,vt. [Purdue] A carbon copy of an electronic transmission. “Oh, you're sending him the bits to that? Slap on a tee for me. ” From the UNIX command `tee(1)', itself named after a pipe fitting (see plumbing). Can also mean `save one for me', as in “Tee a slice for me!” Also spelled

Telecommunication

1. Any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. (RR)
2. Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. (JCS1-DoD) (JCS1-NATO) See also automatic data processing, communications.

Telecommunication Architecture

Within a telecommunication system, the overall plan governing the capabilities of functional elements and their interaction, including configuration, integration, standardization, life-cycle management, and definition of protocol specifications, among these elements.

Telecommunication Facilities

The aggregate of equipment, such as telephones, teletypewriters, facsimile equipment, cables, and switches, used for various modes of transmission, such as digital data, audio signals, and video signals.

Telecommunication Service

1. Any service provided by a telecommunication provider.
2. A specified set of user-information transfer capabilities provided to a group of users by a telecommunication system. (~) Note: The telecommunication service user is responsible for the information content of the message. The telecommunication service provider has the responsibility for the acceptance, transmission, and delivery of the message. See also telecommunication system operator.

Telecommunication System

See communications system.

Telecommunication System Operator

The organization responsible for providing telecommunication service to users.

Telecommunications

1. A general term expressing data transmission between a computing system and remotely located devices via a unit that performs the necessary format conversion and controls the rate of transmission. (DODD 5200. 28;; *NCSC-WA*-001-85;)
2. Any transmission, emission, or reception of signs, signals, writing, images, sounds or other information by wire, radio, visual or any electromagnetic systems. (*FIPS PUB* 39;)
3. The preparation, transmission, communication, or related processing of information by electrical, electromagnetic, electro- mechanical, or electro-optical means. (NSDD-145;) (Note: This definition includes the processing of information by noncommunicating equipment.)
4. The preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electromagnetic, electromechanical, electro-optical, or electronic means. *The preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electromagnetic, electromechanical, electro-optical, or electronic means (NSA, *National INFOSEC Glossary*, 9/88)

Telecommunications And Automated Information Systems Security

(TAISS) Protection afforded to telecommunications and automated information systems in order to prevent exploitation through interception, unauthorized

electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information. (NSDD-145;; *NCSC-WA*-001-85;)

Telecommunications Security

See Communications Security (COMSEC).

Telecommunications System

The devices used to transmit and/or receive communications or process telecommunications, including the [)reparation of information, therefore; the devices may be electrical, electromagnetic, electromechanical, or electro-optical. (NACSI 4000A)

Teleconference

A conference between persons remote from one another but linked by a telecommunications system. (JCS1-DoD) (JCS1-NATO) Note: The conference is supported by audio and/or video communication equipment that enables the live exchange of information among remotely located persons and machines.

Telegram

Written matter intended to be transmitted by telegraphy for delivery to the addressee. This term also includes radio telegrams unless otherwise specified. In this definition the term “telegraphy” has the same general meaning as defined in the [1979 General Worldwide Administrative Radio Conference] Convention. (RR)

Telegraph

A system of telecommunication using coded signals. (~) See also code, polar direct-current telegraph transmission, radio telegraphy, voice-frequency telegraph.

Telegraphy

A form of telecommunication which is concerned in any process providing transmission and reproduction at a distance of documentary matter, such as written or printed matter or fixed images, or the reproduction at a distance of any kind of information in such a form. For the purposes of the Radio Regulations, unless otherwise specified therein, telegraphy shall mean a form of telecommunication for the transmission of written matter by the use of a signal code. (RR)

Telemetry

The use of telecommunication for automatically indicating or recording measurements at a distance from the measuring instrument. (RR) See also space telemetry.

Telemetry Intelligence

(TELINT) Technical and intelligence information derived from intercept, processing, and analysis of telemetry. *Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry; a subcategory of foreign instrumentation signals intelligence. (*IC Staff, Glossary of Intelligence Terms and Definitions*, 6/89)

Telephone Exchange

See exchange, switching center.

Telephony

A form of telecommunication set up for the transmission of speech or, in some cases, other sounds. (RR) See also message, public switched telephone network.

Teleprinter

See teletypewriter.

Teleprocessing

1. A form of information processing in which remote terminals access a computer via some type of communications line. (*AR* 380-380)
2. Pertaining to an information transmission system that combines telecommunications, ADP systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole. (*FIPS PUB* 39)
3. The overall function of an information transmission system which combines telecommunications, automatic data processing, and man-machine interface equipment and their interaction as an integrated whole. (NCSC-9)

Teleprocessing Security

The protection that results from measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system. (*FIPS PUB* 39;; *AR* 380-380;)

*-Telerat

/tel'*-rat/ n. Unflattering hackerism for `Teleray', a line of extremely losing terminals. Compare AIDX, Macintrash Nominal Semidestructor, Open Death-Trap, ScumOS, sun-stools, HP-SUX.

Teleservice

See telecommunication service.

Teletex

An international store-and-forward, error-free communication service defined by the CCITT with a recommended user data rate of 2400 bits per second over the general switched telephone network. Note: Teletex is expected to replace international Telex®.

The communications protocol used for teletex is being enhanced as the basis for the CCITT group 4 facsimile service.

Teletext

A type of communications service in which a user can access a remote database and receive the requested data on the user's video display. Note: The database information is returned to the user's video display over a common carrier channel. See also viewdata.

Teletypewriter (TTY)

A printing telegraph instrument having a signal-actuated mechanism for automatically printing received messages. Note 1: It may have a keyboard similar to that of a typewriter for sending messages. (~) Note 2: The term “teleprinter” may be applied to a receive-only unit having no keyboard. Radio circuits carrying TTY traffic are sometimes referred to as “RTTY” or “RATT. ” See also radio teletypewriter, sending-end crossfire. (FS1037S1. TXT)

Teletypewriter Control Unit

A device that serves as the control and coordination unit between teletypewriter devices and a message switching center when employing controlled teletypewriter operations. (~)

Teletypewriter Exchange Service

A switched teletypewriter service in which suitably arranged teletypewriter stations are provided with lines to a central office for access to other such stations. Note: TWX® and Telex® are commercial teletypewriter exchange services.

Television

A form of telecommunication for the transmission of transient images of fixed or moving objects. (RR) Note: The picture signal is generally accompanied by the sound signal, and follows the NTSC standard in North America. See also NTSC standard.

*-TELNET

/tel'net/ vt. (also commonly lowercased as `telnet') To communicate with another Internet host using the TELNET (RFC 854) protocol (usually using a program of the same name). TOPS-10 people used the word IMPCOM, since that was the program name for them. Sometimes abbreviated to TN /T-N/. “I usually TN over to SAIL just to read the AP News. ”:ten-finger interface. The interface between two networks that cannot be directly connected for security reasons; refers to the practice of placing two terminals side by side and having an operator read from one and type into the other.

TEMPEST

1. A short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term “compromising emanations” for example TEMPEST tests, TEMPEST inspections. (AFR700-10; DOE 5637. 1; NCSC-9; JCS PUB 6-03. 7)
2. TEMPEST is the unclassified name for the studies and investigations of compromising emanations. (*AR* 380-380)
3. The study and control of spurious electronic signals emitted from ADP equipment. (*DOD* 5200. 28-STD; *AFR* 205-16)
4. The study and control of spurious electronic signals emitted by electrical equipment. (*NCSC-TG*-004-88)

TEMPEST Channel

An unintentional communications channel which conveys information about the information processed through the intentional communications channel.

TEMPEST Encoding

An unintentional process which results in the altering of information before it is emitted into the TEMPEST channel.

TEMPEST Test

A laboratory or on-site (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising informationA test normally includes detection and measurement of these signals, and analysis to determine correlation between received signals and potentially compromising transmitted signals.

TEMPEST Zone

Defined area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated without emanating electromagnetic radiation beyond the controlled space boundary of the facility. NOTE: Facility TEMPEST zones are determined by measuring electromagnetic attenuation provided by a building's properties and the free space loss to the controlled space boundary. Equipment TEMPEST zone assignments are based on the level of compromising emanations produced by the equipment.

*-Tense

adj. Of programs, very clever and efficient. A tense piece of code often got that way because it was highly bummed, but sometimes it was just based on a great idea. A comment in a clever routine by Mike Kazar, once a grad-student hacker at CMU: “This routine is so tense it will bring tears to your eyes. ” A tense programmer is one who produces tense code.

*-Tentacle

n. A covert pseudo, sense 1. An artificial identity created in cyberspace for nefarious and deceptive purposes. The implication is that single person may have

multiple tentacles. This term was originally floated in some paranoid ravings on the cypherpunks list (see cypherpunk, and adopted in a spirit of irony by other members. It has since shown up, used seriously, in the documentation for some remailer software, and is now (1994) widely recognized on the net.

*-Tenured Graduate Student

n. One who has been in graduate school for 10 years (the usual maximum is 5 or 6) a `ten-yeared' student (get it?). Actually, this term may be used of any grad student beginning in his seventh year. Students don't really get tenure, of course, the way professors do, but a tenth-year graduate student has probably been around the university longer than any untenured professor. See Herb and Nathan

*-Tera

/te'r*/ pref. [SI] See quantifiers.

*-Teraflop Club

/te'r*-flop kluhb/ n. [FLOP = Floating Point Operation] A mythical association of people who consume outrageous amounts of computer time in order to produce a few simple pictures of glass balls with intricate ray-tracing techniques. Caltech professor James Kajiya is said to have been the founder. Compare Knights of the Lambda Calculus.

*-Terminak

/ter'mi-nak`/ n. [Caltech, ca. 1979] Any malfunctioning computer terminal. A common failure mode of Lear-Siegler ADM 3a terminals caused the `L' key to produce the `K' code instead; complaints about this tended to look like “Terminak #3 has a bad keyboard. Pkease fix. ” See AIDX, Nominal Semidestructor, Open DeathTrap, ScumOS, sun-stools, Telerat, HP-SUX.

Terminal

Any device capable of sending, receiving, or sending and receiving information over a communication channel. (~) See also bit synchronous operation, called-line identification facility, call release time, data circuit-terminating equipment, data terminal equipment, end instrument, input/output device, main station, packet mode terminal, passive station, peripheral equipment, port.

Terminal Adapter

An interfacing device employed at the “R” reference point in an ISDN environment that allows connection of a non-ISDN terminal at the physical layer to communicate with an ISDN network. Typically, this adapter will support standard RJ-11 telephone connection plugs for voice and RS-232C, V. 35 and RS-449 interfaces for data. See also Integrated Services Digital Network.

Terminal Area Security Officer

(TASO) Individual responsible for security-related issues for terminals at a remote terminal area. The TASO receives guidance from the Computer Security Officer (CSO) or Network Security Officer (NSO), and provides status and other reports to the CSO/NSO.

*-Terminal Brain Death

n. The extreme form of terminal illness (sense 1). What someone who has obviously been hacking continuously for far too long is said to be suffering from.

Terminal ID

Terminal Identification

1. The means used to establish the unique identification of a terminal by an automated system. (*AR* 380-380; *FIPS PUB* 39)
2. The means used to uniquely identify a terminal to a system. (*NCSC-TG*-004-88)

*-Terminal Illness

1. n. Syn. raster burn.
2. The `burn-in' condition your CRT tends to get if you don't have a screen saver.

*-Terminal Junkie

n. [UK] A wannabee or early larval stage hacker who spends most of his or her time wandering the directory tree and writing noddy programs just to get a fix of computer time. Variants include `terminal jockey', `console junkie', and console jockey. The term `console jockey' seems to imply more expertise than the other three (possibly because of the exalted status of the console relative to an ordinary terminal). See also twink, read-only user.

Terminals

Terminology

*-Terpri

/ter'pree/ vi. [from LISP 1. 5 (and later, MacLISP)] To output a newline. Now rare as jargon, though still used as techspeak in Common LISP. It is a contraction of `TERminate PRInt line', named for the fact that, on some early OSes and hardware, no characters would be printed until a complete line was formed, so this operation terminated the line and emitted the output.

Terrorism

The use of violence and intimidation to achieve an end, usually political. *The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any

segment thereof, in furtherance of political or social objectives. (FBI Definition)

*-Test

1. n. Real users bashing on a prototype long enough to get thoroughly acquainted with it, with careful monitoring and followup of the results.
2. Some bored random user trying a couple of the simpler features with a developer looking over his or her shoulder, ready to pounce on mistakes. Judging by the quality of most software, the second definition is far more prevalent. See also demo.

Test And Validation

Physical measurements taken to verify conclusions obtained from mathematical modeling and analysis or taken for the purpose of developing mathematical models. (~) See also acceptance test, quality assurance.

Test Condition

Test Data

An asset category consisting of information used to determine the applicability, efficiency, or accuracy of systems. (MK;, RM;)

Test Detection System

The instrumentation used in performing a TEMPEST test including the transducer, detector, display devices, recording devices, filters, coaxial switches, etc.

Test Documentation

Test Key

Key intended for on-the-air testing of COMSEC equipment or systems.

Test Message

A series of characters or signals chosen to be processed by the equipment under test during TEMPEST testing.

Test Plan

Test Point

That point within an equipment or equipment string that provides electrical access to signals for the purpose of fault isolation. (~) See also fault.

Test Procedure

Test Program

*-TeX:

/tekh/ n. X An extremely powerful macro-based text formatterwritten by Donald E. Knuth, very popular in the computer-science community (it is good enough to have displaced UNIX troff, the other favored formatter, even at many UNIX installations). TeX fans insist on the correct (guttural) pronunciation, and the correct spelling (all caps, squished together, with the E depressed below the baseline; the mixed-case `TeX' is considered an acceptable kluge on ASCII-only devices). Fans like to proliferate names from the word `TeX' -- such as TeXnician (TeX user), TeXhacker (TeX programmer), TeXmaster (competent TeX programmer), TeXhax, and TeXnique. See also CrAp-TeX. Knuth began TeX because he had become annoyed at the declining quality of the typesetting in volumes I--III of his monumental “Art of Computer Programming” (see Knuth, also bible). In a manifestation of the typical hackish urge to solve the problem at hand once and for all, he began to design his own typesetting language. He thought he would finish it on his sabbatical in 1978; he was wrong by only about 8 years. The language was finally frozen around 1985, but volume IV of “The Art of Computer Programming” has yet to appear as of mid-1993. The impact and influence of TeX's design has been such that nobody minds this very much. Many grand hackish projects have started as a bit of toolsmithing on the way to something else; Knuth's diversion was simply on a grander scale than most. TeX has also been a noteworthy example of free, shared, but high-quality software. Knuth used to offer monetary awards to people who found and reported bugs in it; as the years wore on and the few remaining bugs were fixed (and new ones even harder to find), the bribe went up. Though well-written, TeX is so large (and so full of cutting edge technique) that it is said to have unearthed at least one bug in every Pascal system it has been compiled with.

*-Text

1. n. [techspeak] Executable code, esp. a `pure code' portion shared between multiple instances of a program running in a multitasking OS. Compare English.
2. Textual material in the mainstream sense; data in ordinary ASCII or EBCDIC representation (see flat-ASCII). “Those are text files; you can review them using the editor. ” These two contradictory senses confuse hackers, too. thanks in advance [Usenet] Conventional net. politeness ending a posted request for information or assistance. Sometimes written `advTHANKSance' or `aTdHvAaNnKcSe' or abbreviated `TIA'. See net. -, netiquette. That's not a bug, that's a feature! The canonical first parry in a debate about a purported bug. The complainant, if unconvinced, is likely to retort that the bug is then at best a misfeature. See also feature. the X that can be Y is not the true X Yet another instance of hackerdom's peculiar at-

traction to mystical references -- a common humorous way of making exclusive statements about a class of things. The template is from the “Tao te Ching” “The Tao which can be spoken of is not the true Tao. ” The implication is often that the X is a mystery accessible only to the enlightened. See the trampoline entry for an example, and compare has the X nature.

Text Editor

Theft

A peril involving removal of an asset for subsequent use by an agent. (RM;)

Theft Of Data

*-Theology

1. n. Ironically or humorously used to refer to religious issues.
2. Technical fine points of an abstruse nature, esp. those where the resolution is of theoretical interest but is relatively marginal with respect to actual use of a design or system. Used esp. around software issues with a heavy AI or language-design component, such as the smart-data vs. smart-programs dispute in AI.

*-Theory

n. The consensus, idea, plan, story, or set of rules that is currently being used to inform a behavior. This usage is a generalization and (deliberate) abuse of the technical meaning. “What's the theory on fixing this TECO loss?” “What's the theory on dinner tonight?” (“Chinatown, I guess. ”) “What's the current theory on letting lusers on during the day?” “The theory behind this change is to fix the following well-known screw. ”

*-Thinko

/thing'koh/ n. [by analogy with `typo'] A momentary, correctable glitch in mental processing, especially one involving recall of information learned by rote; a bubble in the stream of consciousness. Syn. braino; see also brain fart. Compare mouso. This can't happen Less clipped variant of can't happen. This time, for sure!excl. Ritual affirmation frequently uttered during protracted debugging sessions involving numerous small obstacles (e. g. , attempts to bring up a UUCP connection). For the proper effect, this must be uttered in a fruity imitation of Bullwinkle J. Moose. Also heard “Hey, Rocky! Watch me pull a rabbit out of my hat!” The canonical response is, of course, “But that trick *never* works!” See Humor, Hacker.

#-Third-Party Evaluation

This KSA has no definition.

*-Thrash

vi. To move wildly or violently, without accomplishing anything useful. Paging or swapping systems that are overloaded waste most of their time moving data into and out of core (rather than performing useful computation) and are therefore said to thrash. Someone who keeps changing his mind (esp. about what to work on next) is said to be thrashing. A person frantically trying to execute too many tasks at once (and not spending enough time on any single task) may also be described as thrashing. Compare multitask.

*-Thread

1. n. [Usenet, GEnie, CompuServe] Common abbreviation of `topic thread', a more or less continuous chain of postings on a single topic. To `follow a thread' is to read a series of Usenet postings sharing a common subject or (more correctly) which are connected by Reference headers. The better newsreaders can present news in thread order automatically. Interestingly, this is far from a neologism.
2. The OED says: “That which connects the successive points in anything, esp. a narrative, train of thought, or the like; the sequence of events or ideas continuing throughout the whole course of anything;” Citations are given going back to 1642!

Threat

1. The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. Categorize and classify threats as follows:Categories ClassesHuman Intentional Unintentional Environmental Natural Fabricated(*AFR* 205-16;; *AFR* 700-10;)
2. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification or data, and/or denial of service. (*NCSC-WA*-001-85;)
3. Any circumstance or event with the potential to cause harm to the ADP system or activity in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities regardless of the amount of fire protection available. (*OPNAVINST* 5239. 1A;; *AR* 380-380;)
4. Types of computer systems related adverse events (i. e. , perils) that may result in losses. Examples are flooding, sabotage and fraud. (WB;)
5. An assertion primarily concerning entities of the external environment (agents); we say that an agent (or class of agents) poses a threat to one or more assets; we write: T(e;i) where: e is an exter-

nal entity; i is an internal entity or an empty set. (ET;)

6. An undesirable occurrence that might be anticipated but is not the result of a conscious act or decision. In threat analysis, a threat is defined as an ordered pair, <peril; asset category>, suggesting the nature of these occurrences but not the details (details are specific to events). (RM;)
7. A potential violation of security. (SS;)
8. A set of properties of a specific external entity (which may be either an individual or class of entities) that, in union with a set of properties of a specific internal entity, implies a risk (according to some body of knowledge). (MK;)

Threat Agent

1. Methods and things used to exploit a vulnerability in an information system, operation, or facility, i. e. , fire, natural disaster and so forth. (*AFR* 700-10;; *AFR* 206-16; *AR* 380-380;)
2. A method used to exploit a vulnerability in a system,operation or facility. (*NCSC-WA*-001-85;)

Threat Analysis

1. The examination of all actions and events that might adversely effect an Automated Information System or operation. (*NCSC-WA*-001-85;)
2. A methodology for determining the areas of vulnerability within a system and the result of emplacing countermeasures to counteract perceived threats to assets. (RM;)
3. Process of studying information to identify the nature of and elements comprising a threat.

Threat Assessment

Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Threat Event

A specific type of threat event as often specified in a risk analysis procedure. Examples are the neighbouring river overflows its banks and submerges the adjacent data processing center under ten feet of water, and an ex-employee throws a molotov cocktail into the organization's off-site data storage facility. (WB;)

Threat Monitoring

1. The analysis, assessment and review of audit trails and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data security. (*AR* 380-380;)
2. The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data privacy matters. (*FIPS PUB* 39;)
3. The analysis, assessment and review of audit trails and other data collected for the purpose of searching out system events which may constitute violations or attempted violations of system security. (*NCSC-WA*-001-85;)

Threat Realization Cost

The cost to a perpetrator of performing an attack. This could be financial, punitive, embarassment, etc. (MK;)

Threat Viability Threshold

The perpetrator's cost/benefit ratio which makes an attack viable (feasible?). Also could be called the Threat Activation Threshold. (MK;)

Threat, Postulated

The means through which the hypothesized ability or intent, inferred from related conditions or evidence, threaten to adversely affect an automated system, facility or operation. (*AR* 380-380;)

Three-Bit Byte

See triplet.

*-Three-Finger Salute

n. Syn. Vulcan nerve pinch.

Threshold

1. The minimum value of a signal that can be detected by the system or sensor under consideration. (~)
2. A value used to denote predetermined levels, such as those pertaining to volume of message storage, i. e. , in-transit storage or queue storage, used in a message switching center. (~)
3. The minimum value of the parameter used to activate a device. (~)
4. The minimum value a stimulus may have to create a desired effect. See also FM improvement threshold, outage, system operational threshold.

Throughput

1. The number of bits, characters, or blocks that can pass through a data communication system (or portion of that system) when the system (or portion of the system measured) is working at saturation. The throughput will vary greatly from its theoretical maximum. (~) Note: The throughput is expressed in data units per period of time; e. g. , in AUTODIN, as blocks per second.
2. A measure of the amount of work performed by a system over a period of time, e. g. , the number of jobs per day. See also binary digit, block, block transfer efficiency, block transfer rate, data communication, data transfer rate, effective data transfer rate, effective speed of transmission, efficiency factor, maximum user signaling rate, Nyquist rate, Shannon's law, speed of service.

*-Thumb

n. The slider on a window-system scrollbar. So called because moving it allows you to browse through the contents of a text window in a way analogous to thumbing through a book.

*-Thunk

1. /thuhnk/ n. “A piece of coding which provides an address”, according to P. Z. Ingerman, who invented thunks in 1961 as a way of binding actual parameters to their formal definitions in Algol-60 procedure calls. If a procedure is called with an expression in the place of a formal parameter, the compiler generates a thunk which computes the expression and leaves the address of the result in some standard location.
2. Later generalized into an expression, frozen together with its environment, for later evaluation if and when needed (similar to what in techspeak is called a `closure'). The process of unfreezing these thunks is called `forcing'.
3. . A stubroutine, in an overlay programming environment, that loads and jumps to the correct overlay. Compare trampoline.
4. People and activities scheduled in a thunklike manner. “It occurred to me the other day that I am rather accurately modeled by a thunk -- I frequently need to be forced to completion. ” --- paraphrased from a plan file. Historical note There are a couple of onomatopoeic myths circulating about the origin of this term. The most common is that it is the sound made by data hitting the stack; another holds that the sound is that of the data hitting an accumulator. Yet another suggests that it is the sound of the expression being unfrozen at argument-evaluation time. In fact, according to the inventors, it was coined after they realized (in the wee hours after hours of discussion) that the type of an argument in Algol-60 could be figured out in advance with a little compile-time thought, simplifying the evaluation machinery. In other words, it had `already been thought of'; thus it was christened a `thunk', which is “the past tense of `think' at two in the morning”.

*-Tick

1. n. A jiffy (sense 1).
2. In simulations, the discrete unit of time that passes between iterations of the simulation mechanism. In AI applications, this amount of time is often left unspecified, since the only constraint of interest is the ordering of events. This sort of AI simulation is often pejoratively referred to as `tick-tick-tick' simulation, especially when the issue of simultaneity of events with long, independent chains of causes is handwaved.
3. . In the FORTH language, a single quote character.

*-Tick-List Features

n. [Acorn Computers] Features in software or hardware that customers insist on but never use (calculators in desktop TSRs and that sort of thing). The American equivalent would be `checklist features', but this jargon sense of the phrase has not been reported.

Ticket-Oriented

A computer protection system in which each subject maintains a list of unforgeable bit patterns, called tickets, one for each object the subject is authorized to access. May be contrasted with a list-oriented protection system in which each protected object has a list of all subjects authorized to access it. (*NCSC-WA-*001-85;)

*-Tickle A Bug

vt. To cause a normally hidden bug to manifest itself through some known series of inputs or operations. “You can tickle the bug in the Paradise VGA card's highlight handling by trying to set bright yellow reverse video. ”

*-Tiger Team

1. n. [U. S. military jargon] Originally, a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. These people are paid professionals who do hacker-type tricks, e. g. , leave cardboard signs saying “bomb” in critical defense installations, hand-lettered notes saying “Your codebooks have been stolen” (they usually haven't been) inside safes, etc. After a successful penetration, some high-ranking security type shows up the next morning for a `security review' and finds the sign, note, etc. , and all hell breaks loose. Serious successes of tiger teams sometimes lead to early retirement for base commanders and security officers (see the patch entry for an example).
2. Recently, and more generally, any official inspection team or special firefighting group called in to look at a problem. A subset of tiger teams are professional crackers, testing the security of military computer installations by attempting remote attacks via networks or supposedly `secure' comm channels. Some of their escapades, if declassified, would probably rank among the greatest hacks of all times. The term has been adopted in commercial computer-security circles in this more specific sense.

Time

1. An epoch, i. e. , the designation of an instant on a selected time scale, astronomical or atomic. It is used in the sense of time of day. (JCS1-DoD) (~)

2. See time scale. (~) See also coordinated time scale, Coordinated Universal Time, International Atomic Time, precise time, primary time standard, real time, standard time and frequency signal service.

Time Bomb

n. A subspecies of logic bomb that is triggered by reaching some preset time, either once or periodically. There are numerous legends about time bombs set up by programmers in their employers' machines, to go off if the programmer is fired or laid off and is not present to perform the appropriate suppressing action periodically. Interestingly, the only such incident for which we have been pointed to documentary evidence took place in the Soviet Union in 1986! A disgruntled programmer at the Volga Automobile Plant (where the Fiat clones called Ladas were manufactured) planted a time bomb which, a week after he'd left on vacation, stopped the entire main assembly line for a day. The case attracted lots of attention in the Soviet Union because it was the first cracking case to make it to court there. The perpetrator got a suspended sentence of 3 years in jail and was barred from future work as a programmer.

Time Bomb/time-Bomb

In computer security, a variant of the Trojan horse in which malicious code is inserted to be triggered later. (MS; JCS PUB 6-03. 7)

Time Compliance Date

(TCD) Date by which a manditory modification to a COMSEC end item must be incorporated if the item is to remain approved for operational use.

Time Marker

A reference signal, often repeated periodically, enabling the correlation of specific events with a time scale. Note: Time markers are used in some systems for establishing synchronization.

Time Of Occurrence

The date (instant) of an event, with reference to a particular time scale. (~) See also Coordinated Universal Time, time scale.

*-Time Sink

n. [poss. by analogy with `heat sink' or `current sink'] A project that consumes unbounded amounts of time.

Time Slot

1. Period of time during which certain activities are governed by specific regulations. (JCS1-DoD) (JCS1-NATO)
2. Any time interval that can be recognized and defined uniquely. (~) See also digit time slot.

Time Standard

A stable device that emits signals at equal intervals such that their count may be used as a clock. See also clock, Coordinated Universal Time, DoD master clock, master-slave timing, primary time standard.

*-Time T

/ti:m T/ n. An unspecified but usually well-understood time, often used in conjunction with a later time T+1. “We'll meet on campus at time T or at Louie's at time T+1” means, in the context of going out for dinner: “We can meet on campus and go to Louie's, or we can meet at Louie's itself a bit later. ” (Louie's was a Chinese restaurant in Palo Alto that was a favorite with hackers.) Had the number 30 been used instead of the number 1, it would have implied that the travel time from campus to Louie's is 30 minutes; whatever time T is (and that hasn't been decided on yet), you can meet half an hour later at Louie's than you could on campus and end up eating at the same time. See also since time T equals minus infinity.

Time Tick

A time mark output of a clock system.

Time-Bomb

Time-Dependent Password

A password which is valid only at a certain time of day or during a specified interval of time. (*FIPS PUB* 39;; *AR* 380-380;; *NCSC-WA*-001-85;)

Time-Division Multiple Access

A communication technique that uses a common channel (multipoint or broadcast) for communication among multiple users by allocating unique time slots to the different users. (~) Note: Used extensively in satellite systems, local area networks, physical security systems, and combat-net radio systems. See also channel time slot, frequency-division multiple access, multiplexing.

Time-Division Multiplexing

A method of deriving two or more apparently simultaneous channels from a given frequency spectrum of a transmission medium connecting two or more points by assigning discrete time intervals in sequence to each of the individual channels. During a given time interval the entire available frequency spectrum can be used by the channel to which it is assigned. (~) Note: In general, time-division multiplexing systems use pulse transmission. The multiplex pulse train may be considered to be the interleaved pulse trains of the individual channels. The individual channel pulses may be modulated either in an analog or a digital manner. See also asynchronous time-division multiplexing, channelization, concentrator, digit time slot, frequency-derived channel, frequency-division multiplexing, highway, multiplex aggregate bit rate, multiplex hierarchy, multiplexing, synchronous TDM, time-sharing.

Time-Division Switching

A switching method for TDM channels. It requires the shifting of data from one time slot to another in the TDM frame. (~) See also digital switching, switching system, time-division multiplexing.

Time-Out

1. A network parameter related to an enforced event designed to occur at the conclusion of a predetermined elapsed time. (~)
2. An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. The time out can be prevented by an appropriate signal. (FP) (ISO) (~) See also call control signal.

Time-Sharing

1. A mode of operation that provides for the interleaving of two or more independent processes on one functional unit. (~)
2. Pertaining to the interleaved use of time on a computing system that enables two or more users to execute computer programs concurrently. See also multiprocessing, multiprogramming, on-line computer system.

*-Times-Or-Divided-By

quant. [by analogy with `plus-or-minus'] Term occasionally used when describing the uncertainty associated with a scheduling estimate, for either humorous or brutally honest effect. For a software project, the scheduling uncertainty factor is usually at least 2.

*-Tinkerbell Program

n. A monitoring program used to scan incoming network calls and generate alerts when calls are received from particular sites, or when logins are attempted using certain IDs. Named after `Project Tinkerbell', an experimental phone-tapping program developed by British Telecom in the early 1980s.

*-Tip Of The Ice-Cube

n. [IBM] The visible part of something small and insignificant. Used as an ironic comment in situations where `tip of the iceberg' might be appropriate if the subject were at all important.

*-Tired Iron

n. [IBM] Hardware that is perfectly functional but far enough behind the state of the art to have been superseded by new products, presumably with sufficient improvement in bang-per-buck that the old stuff is starting to look a bit like a dinosaur.

*-Tits On A Keyboard

n. Small bumps on certain keycaps to keep touch-typists registered (usually on the `5' of a numeric keypad, and on the `F' and `J' of a QWERTY keyboard; but the Mac, perverse as usual, has them on the `D' and `K' keys).

*-TLA

/T-L-A/ n. [Three-Letter Acronym]

1. Self-describing abbreviation for a species with which computing terminology is infested.
2. Any confusing acronym. Examples include MCA, FTP, SNA, CPU, MMU, SCCS, DMU, FPU, NNTP, TLA. People who like this looser usage argue that not all TLAs have three letters, just as not all four-letter words have four letters. One also hears of `ETLA' (Extended Three-Letter Acronym, pronounced /ee tee el ay/) being used to describe four-letter acronyms. The term `SFLA' (Stupid Four-Letter Acronym) has also been reported. See also YABA. The self-effacing phrase “TDM TLA” (Too Many.) is often used to bemoan the plethora of TLAs in use. In 1989, a random of the journalistic persuasion asked hacker Paul Boutin “What do you think will be the biggest problem in computing in the 90s?” Paul's straight-faced response “There are only 17,000 three-letter acronyms. ” (To be exact, there are 26^3 = 17,576.)

*-TMRC

/tmerk'/ n. The Tech Model Railroad Club at MIT, one of the wellsprings of hacker culture. The 1959 “Dictionary of the TMRC Language” compiled by Peter Samson included several terms that became basics of the hackish vocabulary (see esp. foo, mung, and frob). By 1962, TMRC's legendary layout was already a marvel of complexity (and has grown in the thirty years since; all the features described here are still present). The control system alone featured about 1200 relays. There were scram switches located at numerous places around the room that could be thwacked if something undesirable was about to occur, such as a train going full-bore at an obstruction. Another feature of the system was a digital clock on the dispatch board, which was itself something of a wonder in those bygone days before cheap LEDS and seven-segment displays. When someone hit a scram switch the clock stopped and the display was replaced with the word `FOO'; at TMRC the scram switches are therefore called `foo switches'. Steven Levy, in his book “Hackers” (see the Bibliography in Appendix C), gives a stimulating account of those early years. TMRC's Power and Signals group included most of the early PDP-1 hackers and the people who later became the core of the MIT AI Lab staff. Thirty years later that connection is still very much alive, and this lexicon accordingly includes a number of entries from a recent revision of the TMRC dictionary.

*-TMRCie

/tmerk'ee/, n. [MIT] A denizen of TMRC. to a first approximation

1. [techspeak] When one is doing certain numerical computations, an approximate solution may be computed by any of several heuristic methods,

then refined to a final value. By using the starting point of a first approximation of the answer, one can write an algorithm that converges more quickly to the correct result.

2. In jargon, a preface to any comment that indicates that the comment is only approximately true. The remark “To a first approximation, I feel good” might indicate that deeper questioning would reveal that not all is perfect (e. g. , a nagging cough still remains after an illness). to a zeroth approximation [from `to a first approximation'] A *really* sloppy approximation; a wild guess. Compare social science number.

*-Toad

1. vt. [MUD] Notionally, to change a MUD player into a toad.
2. To permanently and totally exile a player from the MUD. A very serious action, which can only be done by a MUD wizard; often involves a lot of debate among the other characters first. See also frog, FOD.

*-Toast

1. n. Any completely inoperable system or component, esp. one that has just crashed and burned”Uh, oh . I think the serial board is toast. ”
2. vt. To cause a system to crash accidentally, especially in a manner that requires manual rebooting. “Rick just toasted the firewall machine again. ” Compare fried.

*-Toaster

1. n. The archetypal really stupid application for an embedded microprocessor controller; often used in comments that imply that a scheme is inappropriate technology (but see elevator controller). “DWIM for an assembler? That'd be as silly as running UNIX on your toaster!”
2. A very, very dumb computer. “You could run this program on any dumb toaster. ” See bitty box, Get a real computer!, toy, beige toaster.
3. . A Macintosh, esp. the Classic Mac. Some hold that this is implied by sense 2.
4. A peripheral device. “I bought my box without toasters, but since then I've added two boards and a second disk drive. ”:

*-Toeprint

n. A footprint of especially small size.

*-Toggle

vt. To change a bit from whatever state it is in to the other state; to change from 1 to 0 or from 0 to 1. This comes from `toggle switches', such as standard light switches, though the word `toggle' actually refers to the mechanism that keeps the switch in the position to which it is flipped rather than to the fact that the switch has two positions. There are four things you can do to a bit set it (force it to be 1), clear (or zero) it, leave it alone, or toggle it. (Mathematically, one would say that there are four distinct boolean-valued functions of one boolean argument, but saying that is much less fun than talking about toggling bits.):

Token

In certain local-area-network protocols, a group of bits that serves as a symbol of authority, is passed among data stations, and is used to indicate the station that is temporarily in control of the transmission medium. See also token-ring network.

Token Passing

A network access procedure in which a token passes from station to station and the only station allowed to transmit information is the station with the token. See also local area network, ring network, token.

Token-Bus Network

A bus network in which a token passing procedure is used. (FP) (ISO) See also bus topology, local area network, token.

Token-Ring Network

A ring network that allows unidirectional data transmission between data stations by a token-passing procedure over one transmission medium such that the transmitted data return to the transmitting station. (FP)

Tolerance

The permissible range of variation of some characteristic from its nominal value.

Tool

1. n. A program used primarily to create, manipulate, modify, or analyze other programs, such as a compiler or an editor or a cross-referencing program.

2. [UNIX] An application program with a simple, `transparent' (typically text-stream) interface designed specifically to be used in programmed combination with other tools (see filter, plumbing).
3. . vi. To work; to study (connotes tedium). The TMRC Dictionary defined this as “to set one's brain to the grindstone”. (4) In some computer languages, a small program executed as a shell command. Note: In other computer languages, such as BASIC, it is called a “utility. ”

*-Toolsmith

n. The software equivalent of a tool-and-die specialist; one who specializes in making the tools with which other programmers create applications. Many hackers consider this more fun than applications per se; to understand why, see uninteresting. Jon Bentley, in the “Bumper-Sticker Computer Science” chapter of

his book “More Programming Pearls”, quotes Dick Sites from DEC as saying “I'd rather write programs to write programs than write programs”.

Top-Level Specification

(TLS) A non-procedural description of system behavior at the most abstract level. Typically functional specification that omits all implementation details. (*DOD* 5200. 28-STD)

*-Topic Drift

n. Term used on GEnie, Usenet and other electronic fora to describe the tendency of a thread to drift away from the original subject of discussion (and thus, from the Subject header of the originating message), or the results of that tendency. Often used in gentle reminders that the discussion has strayed off any useful track. “I think we started with a question about Niven's last book, but we've ended up discussing the sexual habits of the common marmoset. Now *that's* topic drift!”:

*-Topic Group

n. Syn. forum.

Topology

See network topology.

*-TOPS-10:

/tops-ten/ n. DEC's proprietary OS for the fabled PDP-10 machines, long a favorite of hackers but now effectively extinct. A fountain of hacker folklore; see Appendix A. See also ITS, TOPS-20, TWENEX, VMS, operating system. TOPS-10 was sometimes called BOTS-10 (from `bottoms-ten') as a comment on the inappropriateness of describing it as the top of anything.

*-TOPS-20:

/tops-twen'tee/ n. See TWENEX.

Torn-Tape Relay

An antiquated tape relay system in which the perforated tape is manually transferred by an operator to the appropriate outgoing transmitter. (~) See also reperforator, tape relay.

Touch-Sensitive

Pertaining to a device that allows a user to interact with a computer system by touching an area on the surface of the device with a finger, pencil, or other object; for example, a touch-sensitive keypad or screen. (FP)

*-Tourist

n. [ITS] A guest on the system, especially one who generally logs in over a network from a remote location for comm mode, email, games, and other trivial purposes. One step below luser. Hackers often spell this turist, perhaps by some sort of tenuous analogy with luser (this also expresses the ITS culture's penchant for six-letterisms). Compare twink, read-only user.

*-Tourist Information

n. Information in an on-line display that is not immediately useful, but contributes to a viewer's gestalt of what's going on with the software or hardware behind it. Whether a given piece of info falls in this category depends partly on what the user is looking for at any given time. The `bytes free' information at the bottom of an MS-DOS `dir' display is tourist information; so (most of the time) is the TIME information in a UNIX `ps(1)' display.

*-Touristic

adj. Having the quality of a tourist. Often used as a pejorative, as in `losing touristic scum'. Often spelled `turistic' or `turistik', so that phrase might be more properly rendered `lusing turistic scum'.

*-Toy

n. A computer system; always used with qualifiers.

1. `nice toy' One that supports the speaker's hacking style adequately.
2. `just a toy' A machine that yields insufficient computrons for the speaker's preferred uses. This is not condemnatory, as is bitty box; toys can at least be fun. It is also strongly conditioned by one's expectations; Cray XMP users sometimes consider the Cray-1 a `toy', and certainly all RISC boxes and mainframes are toys by their standards. See also Get a real computer!.

*-Toy Language

n. A language useful for instructional purposes or as a proof-of-concept for some aspect of computer-science theory, but inadequate for general-purpose programming. Bad Things can result when a toy language is promoted as a general purpose solution for programming (see bondage-and-discipline language); the classic example is Pascal. Several moderately well-known formalisms for conceptual tasks such as programming Turing machines also qualify as toy languages in a less negative sense. See also MFTL.

*-Toy Problem

n. [AI] A deliberately oversimplified case of a challenging problem used to investigate, prototype, or test algorithms for a real problem. Sometimes used pejoratively. See also gedanken, toy program.

*-Toy Program

1. n. One that can be readily comprehended; hence, a trivial program (compare noddy).
2. One for which the effort of initial coding dominates the costs through its life cycle. See also noddy.

Trace Packet

In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control center from each visited system element. See also audit trail.

Trace Program

A computer program that performs a check on another computer program by exhibiting the sequence in which the instructions are executed and usually the results of executing the instructions. (FP)

Track

On a data medium, a path associated with a single read/write head as data move past the head. (FP) (ISO)

Track Density

The number of tracks per unit length, measured in a direction perpendicular to the tracks. (FP) (ISO) See also track.

Tracking Error

The deviation of a dependent variable with respect to a reference function.

Tracking Mode

An operational mode during which a system is operating within specified movement limits relative to a reference. (~) See also coasting mode, frequency tolerance.

Tracking Phase

See tracking mode.

Trade Secret

A secret formula, method or device that gives a manufacturer an advantage over competitors.

Traditional COMSEC Program

COMSEC program in which the National Security Agency acts as the central procurement agency for the development and, in some cases, the production of COMSEC items. NOTE: This includes the Authorized Vendor Program and user partnerships. Modifications to the COMSEC end items used in products developed and/or produced under these programs must be approved by the National Security Agency.

Traffic

1. The information moved over a communication channel. (~)
2. A quantitative measurement of the total messages and their length, expressed in CCS or other units, during a specified period of time. (~) See also busy hour, call-second, communications, erlang, narrative traffic, record traffic.

#-Traffic Analysis

1. (TA) The process of monitoring lines, not intercepting the information being transmitted but determiniming the rate of transmission. (*AFR* 205-16;)
2. The process of deducing information from the nature of the traffic on a network (message frequency, message length, etc.) rather than having knowledge of the actual data being transmitted. (WB;)
3. The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency). (SS;)
4. The study of communications characteristics which are external to the encrypted texts. (NCSC-9)
5. The process of deducing information from the nature of the traffic on a network (message frequency, message length, etc.) rather than having knowledge of the actual data being transmitted. (WB)

Traffic Capacity

The maximum traffic per unit of time that a given telecommunication system, subsystem, or device can carry under specified conditions. (~) See also busy hour, call-second, communications, erlang, traffic load.

Traffic Encryption Key

(TEK) Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

Traffic F Low Security

1. The protection that results from those features in some crypto-equipment that conceal the presence of valid messages on a communications circuit. This is usually done by causing the circuit to appear busy at all times, or by encrypting the source and destination addresses of valid messages. (*FIPS PUB* 39; *AR* 380-380)
2. The capability of certain on-line, machine cryptosystems to conceal the presence of valid traffic. (NCSC-9)

Traffic Flow Confidentiality

A confidentiality service to protect against traffic analysis. (SS;)

Traffic Flow Information

Any information which reveals the presence or absence of a legitimate message within a given time period. (NACSEM 5201)

Traffic Flow Security

(TFS) The protection that results from those features in some crypto-equipment that conceal the presence of valid messages on a communications circuit. This is usually done by causing the circuit to appear busy

at all times, or by encrypting the source and destination addresses of valid messages. (*FIPS PUB* 39;; *AR* 380-380;)

Traffic Padding

The generation of spurious instances of communication, spurious data units and/or spurious data within data units. (SS;)

Traffic-Flow Security

1. Measures used to conceal the presence of valid messages in an on-line cryptosystem or secure communication system. Note: Encryption of sending and receiving addresses and causing the circuit to appear busy at all times by sending dummy traffic are two methods of traffic-flow security. A more common method is to send a continuous encrypted signal, irrespective of whether traffic is being transmitted.
2. The protection resulting from features, inherent in some cryptoequipment, which conceal the presence of valid messages on a communications circuit; normally achieved by causing the circuit to appear busy at all times. (JCS1-DoD) See also cryptology, electronic warfare.

Training

An effective countermeasure

Training Key

Cryptographic key intended for on-the-air or off-the-air training.

*-Trampoline

n. An incredibly hairy technique, found in some HLL and program-overlay implementations (e. g. , on the Macintosh), that involves on-the-fly generation of small executable (and, likely as not, self-modifying) code objects to do indirection between code sections. These pieces of live data are called `trampolines'. Trampolines are notoriously difficult to understand in action; in fact, it is said by those who use this term that the trampoline that doesn't bend your brain is not the true trampoline. See also snap.

Tranquility

A security model rule stating that the security level of an active object cannot change during the period of activity. (*NCSC-WA*-001-85;; MTR-8201;)

Tranquillity

1. A security model rule stating that the security level of an active object cannot change during the period of activity. (MTR-8201)
2. A security model rule stating that the security level of an object cannot change while the object is being processed by an AlS. (*NCSC-TG*-004-88)

Transceiver

A device that performs, within one chassis, both telecommunication transmitting and receiving functions. (~)

Transducer

A device for converting energy from one form to another. (FP) See also interface, optoelectronic.

Transfer

To send information from one location and to receive it at another.

Transfer Characteristics

Those intrinsic parameters of a system, subsystem, or equipment which, when applied to the input of the system, subsystem, or equipment, will fully describe its output.

Transfer Function

1. [of a device] A mathematical statement expressing the transfer characteristics of a system, subsystem, or equipment.
2. The relationship between the input and the output in terms of the transfer characteristics. See also insertion-loss-vs-frequency characteristic, transfer characteristics.

Transfer Mode

A method of transmission, multiplexing, and switching used in an ISDN.

Transfer Rate

See data transfer rate.

Translating Program

See translator (def. #2).

Translator

1. A device that converts information from one system of representation into equivalent information in another system of representation. (~) Note: In telephone equipment, it is the device that converts dialed digits into call-routing information. See also transponder.
2. A computer program that translates from one language into another language and in particular from one programming language into another programming language. (FP) (ISO) See translating program. See also address translator.
3. In FM and TV broadcasting, a repeater station that receives a primary station's signal, amplifies it, shifts it in frequency, and rebroadcasts it.

Transliterate

To convert the characters of one alphabet to the corresponding characters of another alphabet. (FP)

Transmission

1. The dispatching, for reception elsewhere, of a signal, message, or other form of information, e. g. , telegraphy, telephony, or facsimile, by means of wire, optical fiber, or radio. (~)

2. The transfer of electrical power from one location to another over conductors. (~)

Transmission Block

A group of bits or characters transmitted as a unit, usually with an encoding procedure for error control purposes. (FP) (ISO) See also binary digit, character.

Transmission Frame

A data structure, beginning and ending with delimiters, that consists of fields predetermined by a protocol for the transmission of user data and control data. (FP) (ISO)

Transmission Security

(TRANSEC) The component of COMSEC which consists of all measures designed to protect radio transmission from interception and exploitation by means other than cryptanalysis. *The component of COMSEC which consists of all measures designed to protect radio transmission from interception and exploitation by means other than cryptanalysis. (NSA, *National INFOSEC Glossary*, 10/88)

Transmission Security Key

(TSK) A key that is used in the control of transmission security processes such as frequency hopping and spread spectrum. See also key. (AF9K_JBC. TXT) (TSK) Key that is used in the control of transmission security processes, such as frequency hopping and spread spectrum.

Transparent Interface

An interface that facilitates the capability to connect and operate a system, subsystem, or equipment with another system, subsystem, or equipment, without modification of their characteristics or operational procedures on either side of the interface. (~) See also commonality, interface, interoperability, mechanically intermateable connectors.

Transponder

1. An automatic device that receives, amplifies, and retransmits a signal on a different frequency. (~)
2. An automatic device that transmits a predetermined message in response to a predefined received signal. (~) Note: Used in identification-friend-or-foe systems and air-traffic-control systems. See also identification friend or foe.
3. A receiver-transmitter that will generate a reply signal upon proper interrogation. (JCS1-DoD) (JCS1-NATO)

Transport Layer

See Open System Interconnection--Reference Model.

Transportability

1. The quality of equipment, devices, systems, and associated hardware that permits its being moved from one location to another to interconnect with locally available equivalents. Note: The quality involves elements such as standardized plugs and transmission media. See also compatibility, interoperability.
2. The capability of material to be moved by towing, self-propulsion, or carrier via any means, such as railways, highways, waterways, pipelines, oceans, and airways. (JCS1-DoD) See also mobile service, mobile station, portability.

Transportable Station

A station that is transferred to various fixed locations but is not intended to be used while in motion. (NTIA)

#-Transportation Of Media

This KSA has no definition.

Transposition

1. In data transmission, a transmission defect in which, during one character period, one or more signal elements are changed from one significant condition to the other, and an equal number of elements are changed in the opposite sense. (~) See also code, translator.
2. In outside plant construction, an interchange of positions of the several conductors of a circuit between successive lengths; this interchange is normally used to reduce inductive interference on communication circuits. (~)

*-Trap

1. n. A program interrupt, usually an interrupt caused by some exceptional situation in the user program. In most cases, the OS performs some action, then returns control to the program.
2. vi. To cause a trap. “These instructions trap to the monitor. ” Also used transitively to indicate the cause of the trap. “The monitor traps all input/output instructions. ” This term is associated with assembler programming (`interrupt' or `exception' is more common among HLL programmers) and appears to be fading into history among programmers as the role of assembler continues to shrink. However, it is still important to computer architects and systems hackers (see system, sense 1), who use it to distinguish deterministically repeatable exceptions from timing-dependent ones (such as I/O interrupts).

Trap Door

1. A hidden software or hardware mechanism used to circumvent security controls. (*AFR* 205-16;)
2. A condition existing in the system software or hardware which can be triggered to subvert the software or hardware security features. Basically, the condition is prompted internally (such as by a computer, a date or time value, or any specific set of pre-established circumstances) or externally

(such as by a remote terminal or application program input message). (*AR* 380-380;)

3. A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e. g. , special “random” key sequence at a terminal). (CSC-STD-001-83;)
4. A breach created intentionally in an ADP system for the purpose of collecting, altering or destroying data. (*FIPS PUB* 39;)
5. A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some innocent appearing manner, e. g. , special “random” key sequence at a terminal. Software developers often introduce trap doors in their code that enable them to re-enter the system and perform certain functions. (*NCSC-WA*-001-85;)
6. A trap door (also known as a back door) is a hidden software or hardware mechanism included by the author of the software that permits system protection mechanisms to be bypassed. It is activated in some obscure manner, such as a universal password that gives unhindered access to all files on a system. (IC;)

*-Trash

vt. To destroy the contents of (said of a data structure). The most common of the family of near-synonyms including mung, mangle, and scribble.

*-Trawl

v. To sift through large volumes of data (e. g. , Usenet postings, FTP archives, or the Jargon File) looking for something of interest.

Tree Search

In a tree structure, a search in which it is possible to decide, at each step, which part of the tree may be rejected without a further search. (FP) (ISO)

Tree Structure

A hierarchical organization in which each node is considered to be an ancestor of all lower level nodes to which it is connected; the root, or base node, is an ancestor of all other nodes. (FP)

Tree Topology

A communication network topology which, from a purely topologic viewpoint, resembles a star network in that individual peripheral nodes are required to transmit to and receive from one other node only, toward a central node, and are not required to act as repeaters or regenerators. The function of the central node, however, may be distributed. (~) Note 1: As in the conventional star network, individual nodes may thus still be isolated from the network by a single-point failure of a transmission path to the node. Note 2: A single-point failure of a transmission path within the distributed node will result in partitioning two or more stations from the rest of the network. See also bus topology, local area network, network topology, node (def. #1), ring network, star network, star topology.

*-Tree-Killer

1. n. [Sun] A printer.
2. A person who wastes paper. This epithet should be interpreted in a broad sense; `wasting paper' includes the production of spiffy but content-free documents. Thus, most suits are tree-killers. The negative loading of this term may reflect the epithet `tree-killer' applied by Treebeard the Ent to the Orcs in J. R. R. Tolkien's “Lord of the Rings” (see also elvish, elder days).

*-Treeware

/tree'weir/ n. Printouts, books, and other information media made from pulped dead trees. Compare tree-killer, see documentation.

TRI-TAC Equipment

Equipment designed to accommodate the transition from the manual and analog systems currently being used to fully automated digital systems, and to provide message switching, circuit switching for voice communications, secure voice terminals, digital facsimile systems, and a user's digital voice terminal.

Triplet

A byte composed of three bits. See three-bit byte.

*-Trit

/trit/ n. [by analogy with `bit'] One base-3 digit; the amount of information conveyed by a selection among one of three equally likely outcomes (see also bit). Trits arise, for example, in the context of a flag that should actually be able to assume *three* values -- such as yes, no, or unknown. Trits are sometimes jokingly called `3-state bits'. A trit may be semi-seriously referred to as `a bit and a half', although it is linearly equivalent to 1. 5849625 bits (that is, log2(3) bits).

*-Trivial

1. adj. Too simple to bother detailing.
2. Not worth the speaker's time.
3. . Complex, but solvable by methods so well known that anyone not utterly cretinous would have thought of them already.
4. Any problem one has already solved (some claim that hackish `trivial' usually evaluates to `I've seen it before'). Hackers' notions of triviality may be quite at variance with those of non-hackers. See nontrivial, uninteresting.

*-Troff:

/T'rof/ or /trof/ n. [UNIX] The gray eminence of UNIX text processing; a formatting and phototypesetting program, written originally in PDP-11 assembler and then in barely-structured early C by the late Jo-

seph Ossanna, modeled after the earlier ROFF which was in turn modeled after Multics' RUNOFF by Jerome Saltzer (*that* name came from the expression “to run off a copy”). A companion program, nroff, formats output for terminals and line printers. In 1979, Brian Kernighan modified `troff' so that it could drive phototypesetters other than the Graphic Systems CAT. His paper describing that work (“A Typesetter-independent troff,” AT&T CSTR #97) explains troff's durability. After discussing the program's “obvious deficiencies -- a rebarbative input syntax, mysterious and undocumented properties in some areas, and a voracious appetite for computer resources” and noting the ugliness and extreme hairiness of the code and internals, Kernighan concludes None of these remarks should be taken as denigrating Ossanna's accomplishment with TROFF. It has proven a remarkably robust tool, taking unbelievable abuse from a variety of preprocessors and being forced into uses that were never conceived of in the original design, all with considerable grace under fire. The success of TeX and desktop publishing systems have reduced `troff''s relative importance, but this tribute perfectly captures the strengths that secured `troff' a place in hacker folklore; indeed, it could be taken more generally as an indication of those qualities of good programs that, in the long run, hackers most admire.

*-Troglodyte

1. n. [Commodore] A hacker who never leaves his cubicle. The term `Gnoll' (from Dungeons & Dragons) is also reported.
2. A curmudgeon attached to an obsolescent computing environment. The combination `ITS troglodyte' was flung around some during the Usenet and email wringle-wrangle attending the 2. x. x revision of the Jargon File; at least one of the people it was intended to describe adopted it with pride.

*-Troglodyte Mode

n. [Rice University] Programming with the lights turned off, sunglasses on, and the terminal inverted (black on white) because you've been up for so many days straight that your eyes hurt (see raster burn). Loud music blaring from a stereo stacked in the corner is optional but recommended. See larval stage, hack mode.

Trojan Horse

1. An apparently useful program containing hidden code which allows the unauthorized collection, falsification, or destruction of data. (*AFR* 205-16;)
2. A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a “blind copy” of a sensitive file for the creator of the Trojan Horse. (CSC-STD-001-83;)
3. A computer program that is apparently or actually useful and that contains a trap door. (*FIPS PUB* 39;)
4. A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity. For example, making a “blind copy” of a sensitive file for the creator of the Trojan horse. (*NCSC-WA*-001-85;)
5. A trojan horse is a computer program that appears to perform a useful and innocent function, but it contains additional hidden functions that exploit the legitimate authorizations of the user who invokes the trojan horse. For example, it may make an unauthorized copy of a sensitive file for the creator of the Trojan Horse. (IC;)

*-Troll

v. ,n. To utter a posting on Usenet designed to attract stupid responses or flames. May derive from the phrase “trolling for newbies” or some similar construction. The well-constructed troll is a post that induces lots of newbies and flamers to make themselves look even more like idiots than they already do, while subtly conveying to the more savvy and experienced that it is in fact a deliberate troll. If you don't fall for the joke, you get to be in on it. Some people claim that the troll is properly a narrower category than flame bait, that a troll is categorized by containing some assertion that is wrong but not overtly controversial.

*-Tron

v. [NRL, CMU; prob. fr. the movie “Tron”] To become inaccessible except via email or `talk(1)', especially when one is normally available via telephone or in person. Frequently used in the past tense, as in “Ran seems to have tronned on us this week” or “Gee, Ran, glad you were able to un-tron yourself”. One may also speak of `tron mode'; compare spod.

*-True-Hacker

n. [analogy with `trufan' from SF fandom] One who exemplifies the primary values of hacker culture, esp. competence and helpfulness to other hackers. A high compliment. “He spent 6 hours helping me bring up UUCP and netnews on my FOOBAR 4000 last week -- manifestly the act of a true-hacker. ” Compare demigod, oppose munchkin.

Truncation

[In data processing,] The deletion or omission of a leading or a trailing portion of a string in accordance with specified criteria. (FP)

Truncation Error

In the representation of a number, the error introduced when one or more digits are dropped.

Trunk

1. A single transmission channel between two points that are switching centers or nodes, or both. (~)
2. [A] circuit between switchboards or other switching equipment, as distinguished from circuits which extend between central office switching equipment and information origination/termination equipment. (CFR 47) See also central office trunk, channel (defs. #1, #3, #5), circuit (def. #2), common trunk, cross-office trunk, interposition trunk, interswitch trunk, intraoffice trunk, one-way trunk, tandem center, tandem tie trunk network, transmission channel.

Trunk Encryption Device (TED)

A bulk encryption device used to provide secure communication over a wideband digital transmission link. (~) Note: It is usually located between the output of a trunk group multiplexer and a wideband radio or cable facility. See also bulk encryption, link encryption. (FS1037S1. TXT)

Trunk Group

Two or more trunks of the same type between the same two points. (~) See also group.

#-Trust

Confidence that an entity , to which trust is applied, will perform in a way that will not prejudice the security of the user of the system of which that entity is a part. NOTE: Trust is always restricted to specific functions or ways of behavior (e. g. , “trusted to connect A to B properly). Trust is meaningful only in the context of a security policy; an entity may be trusted in the context of one policy, but untrusted in the context of another policy. (Source: *NCSC-TG*-029).

Trusted Computer System

1. A system that employs sufficient hardware and software integrity measures to allow its use for simultaneous processing of multiple levels of classified and/or sensitive information. (*AR* 380-380;; CSC-STD-001-83;; DODD 5215. 1;)
2. A system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of sensitive or classified information. (*NCSC-WA*-001-85;)
3. (TCS) An automated information system, including all of the hardware, firmware, and software that, by virtue of having undergone sufficient benchmark validation and testing, as well as acceptance and user testing, can be expected to meet the user's requirements for reliability, security, and operational effectiveness with specified performance characteristics. Note: Such a system is primarily intended for simultaneously processing various levels of sensitive and classified information without danger of compromise. (~) See also automated information systems security, computer, data security. (F:\NEWDEFS. TXT)

Trusted Computer System Evaluation Criteria

#-Trusted Computer System Evaluation Criteria (*Orange Book*)

A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information. (Source: *NCSC-TG*-0004).

Trusted Computing Base

(TCB) The totality of protection mechanisms within a computer system “ including hardware, firmware, and software “ the combination of which are responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e. g. , a user's clearance) related to the security policy. (CSC-STD-001-83;; *AFR* 205-16;; *NCSC-WA*-001-85;; DODD 5200. 28-STD;) See also automated information systems security, computer, data security.

Trusted Computing Base (TCB)

1. The totality of protection mechanisms within a computer system including hardware, firmware, and software -the combination of which are responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e. g. , a user's clearance) related to the security policy. (*DOD* 5200,28-STD; *AFR* 205-16)
2. The totality of protection mechanisms within a computer system, including hardware firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e. g. , a user's clearance level) related to the security policy. (*NCSC-TG*-004-88)

Trusted Courier

Trusted Database Interpretation

Trusted Database Management System Interpretation Of The Tcsec

Trusted Distribution
A trusted method for distributing the TCB hardware, software, and firmware components, both originals and updates, that provides methods for protecting the TCB from modification during distribution and for detection of any changes to the TCB that may occur.

Trusted Element
An element of the system which is relied upon to perform its function correctly and reliably. There may be limited evidence to substantiate the trust and, as a result, there is only limited confidence in the element. (MK;)

Trusted Facility Management
Trusted facility management is one of the areas of operational assurance. As such, the trusted facility management is an aspect of the objective, "assurance. "

Trusted Facility Manual
(TFM) Manual which documents the operational requirements; security environment; hardware and software configurations and interfaces; all security procedures, measures, and features; and the contingency plans for continued operations in case of a local disaster.

Trusted Functionality
That which is perceived to be correct with respect to some criteria, e. g. as established by a security policy. (SS;)

Trusted Identification Forwarding
An identification method used in networks where the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user. (CSC-STD-002-85;; *NCSC-WA*-001-85;)

Trusted Network
Network that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Network Interface
A special-purpose device placed between the network and other devices using the network. (*AFR* 205-16)

Trusted Network Interpreation

#-Trusted Network Interpretation (Red Book)
This document in the Rainbow Series provides interpretations of the *Orange Book* for trusted computer/communications network systems. The specific security features, the assurance requirements and the rating structure of the *Orange Book* are extended to networks of computers ranging from isolated LANs to WANs. (Source panel of experts).

Trusted Network Interpretation Environments Guideline

Trusted Path
A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software. (CSC-STD-001-83;; *NCSC-WA*-001-85;)

Trusted Process
1. A process which can affect system security. It is sometimes, but not always endowed with privileges to override kernel-enforced rules. The protection capabilities or characteristics of a trusted process must be reliably demonstrated to comply with stated requirements through formal verification when possible. Trusted processes are sometimes used to execute NKSR software. (MTR-8201;)
2. A process whose incorrect or malicious execution is capable of violating system security policy. (*NCSC-TG*-004-88)

Trusted Product Evaluation Program

Trusted Product Evaluation Questionnaire
See *NCSC-TG*-019

Trusted Product Evaluations

Trusted Products
Products certified by Director, NCSC for inclusion on the Evaluated Products List (EPL). (DODD 5200. 28;)

Trusted Software

1. The software portion of a TCB that can be relied upon to enforce security policy. (*AFR* 205-16)
2. Software, usually affecting system security, that has been certified to perform as specified. Certification may be performed by any organization the accreditor deems appropriate, depending on the situation. (JCS PUB 6-03. 7)
3. The software portion of a trusted computing base. (*DOD* 5200. 28-STD)
4. See TRUSTED PROCESS.

Trusted Subject

Trusted System

Employing sufficient integrity measures to allow its use for processing intelligence information involving sensitive intelligence sources and methods (*DCID* 1/16, Sup.)

Trusted Unix Working Group

(trusix)

Trusted Users

Trustworthy Element

An element of the system which is relied upon to perform its function correctly and reliably. The element has been evaluated and there exists a body of evidence which provides justification for the trust. (MK;)

Truth Table

1. An operation table for a logic operation. (FP) (ISO)
2. A table that describes a logic function by listing all possible combinations of input values and indicating, for each combination, the output value. (FP)

TSEC Nomenclature

System for identifying the type and purpose of certain items of COMSEC material. NOTE: TSEC is derived from telecommunications security.

*-Tube

1. n. A CRT terminal. Never used in the mainstream sense of TV; real hackers don't watch TV, except for Loony Toons, Rocky & Bullwinkle, Trek Classic, the Simpsons, and the occasional cheesy old swashbuckler movie.
2. IBM] To send a copy of something to someone else's terminal. “Tube me that note?”

*-Tube Time

n. Time spent at a terminal or console. More inclusive than hacking time; commonly used in discussions of what parts of one's environment one uses most heavily. “I find I'm spending too much of my tube time reading mail since I started this revision. ”

Tunable

A term used to describe a test, or test instrumentation designed to cover a fixed frequency range in continuous or stepped contiguous (within the specified bandwidth) increments. Tunable detection systems may contain a demodulator.

*-Tunafish

n. In hackish lore, refers to the mutated punchline of an age-old joke to be found at the bottom of the manual pages of `tunefs(8)' in the original BSD 4. 2 distribution. The joke was removed in later releases once commercial sites started using 4. 2. Tunefs relates to the `tuning' of file-system parameters for optimum performance, and at the bottom of a few pages of wizardly inscriptions was a `BUGS' section consisting of the line “You can tune a file system, but you can't tunafish”. Variants of this can be seen in other BSD versions, though it has been excised from some versions by humorless management droids. The [nt]roff source for SunOS 4. 1. 1 contains a comment apparently designed to prevent this: “Take this out and a Unix Demon will dog your steps from now until the `time_t"s wrap around. ”

*-Tune

vt. [from automotive or musical usage] To optimize a program or system for a particular environment, esp. by adjusting numerical parameters designed as hooks for tuning, e. g. , by changing `#define' lines in C. One may `tune for time' (fastest execution), `tune for space' (least memory use), or `tune for configuration' (most efficient use of hardware). See bum, hot spot, hand-hacking.

*-Turbo Nerd

n. See computer geek.

Turing Machine

A mathematical model of a device that changes its internal state and reads from, writes on, and moves a potentially infinite tape, all in accordance with its present state, thereby constituting a model for computer-like behavior. (FP)

*-Turing Tar-Pit

1. n. A place where anything is possible but nothing of interest is practical. Alan Turing helped lay the foundations of computer science by showing that all machines and languages capable of expressing a certain very primitive set of operations are logically equivalent in the kinds of computations they can carry out, and in principle have capabilities that differ only in speed from those of the most powerful and elegantly designed computers. However, no machine or language exactly matching Turing's primitive set has ever been built (other than possibly as a classroom exercise), because it would be horribly slow and far too painful to use.

A `Turing tar-pit' is any computer language or other tool that shares this property. That is, it's theoretically universal -- but in practice, the harder you struggle to get any real work done, the deeper its inadequacies suck you in. Compare bondage-and-discipline language.

2. The perennial holy wars over whether language A or B is the “most powerful”.

*-Turist

/too'rist/ n. Var. sp. of tourist, q. v. Also in adjectival form, `turistic'. Poss. influenced by luser and `Turing'.

Turnaround Time

In a half-duplex circuit, the actual time required to reverse the direction of transmission from send to receive or vice versa. (~) See also half-duplex circuit, response time, round-trip delay time.

Turnkey

Pertaining to a procurement process involving contractual action through, at least, the system, subsystem, or equipment installation phase. Follow-on contractual actions for test, training, logistics support, and operation may be included in any combination. (~) Note: For precise definition of the types of allowable contractual features, the Federal Acquisition Regulations apply.

TV

See television.

*-Tweak

1. vt. To change slightly, usually in reference to a value. Also used synonymously with twiddle. If a program is almost correct, rather than figure out the precise problem you might just keep tweaking it until it works. See frobnicate and fudge factor; also see shotgun debugging.
2. To tune or bum a program; preferred usage in the U. K.

*-Tweeter

n. [University of Waterloo] Syn. perf, chad (sense 1). This term (like woofer) has been in use at Waterloo since 1972 but is elsewhere unknown. In audio jargon, the word refers to the treble speaker(s) on a hi-fi.

*-TWENEX:

n. /twe'neks/ The TOPS-20 operating system by DEC -- the second proprietary OS for the PDP-10 -- preferred by most PDP-10 hackers over TOPS-10 (that is, by those who were not ITS or WAITS partisans). TOPS-20 began in 1969 as Bolt, Beranek & Newman's TENEX operating system using special paging hardware. By the early 1970s, almost all of the systems on the ARPANET ran TENEX. DEC purchased the rights to TENEX from BBN and began work to make it their own. The first in-house code name for the operating system was VIROS (VIRtual memory Operating System); when customers started asking questions, the name was changed to SNARK so DEC could truthfully deny that there was any project called VIROS. When the name SNARK became known, the name was briefly reversed to become KRANS; this was quickly abandoned when someone objected that `krans' meant `funeral wreath' in Swedish (though some Swedish speakers have since said it means simply `wreath'; this part of the story may be apocryphal). Ultimately DEC picked TOPS-20 as the name of the operating system, and it was as TOPS-20 that it was marketed. The hacker community, mindful of its origins, quickly dubbed it TWENEX (a contraction of `twenty TENEX'), even though by this point very little of the original TENEX code remained (analogously to the differences between AT&T V6 UNIX and BSD). DEC people cringed when they heard “TWENEX”, but the term caught on nevertheless (the written abbreviation `20x' was also used). TWENEX was successful and very popular; in fact, there was a period in the early 1980s when it commanded as fervent a culture of partisans as UNIX or ITS -- but DEC's decision to scrap all the internal rivals to the VAX architecture and its relatively stodgy VMS OS killed the DEC-20 and put a sad end to TWENEX's brief day in the sun. DEC attempted to convince TOPS-20 users to convert to VMS, but instead, by the late 1980s, most of the TOPS-20 hackers had migrated to UNIX.

*-Twiddle

1. n. Tilde (ASCII 1111110, `~'). Also called `squiggle', `sqiggle' (sic -- pronounced /skig'l/), and `twaddle', but twiddle is the most common term.
2. A small and insignificant change to a program. Usually fixes one bug and generates several new ones (see also shotgun debugging).
3. . vt. To change something in a small way. Bits, for example, are often twiddled. Twiddling a switch or knob implies much less sense of purpose than toggling or tweaking it; see frobnicate. To speak of twiddling a bit connotes aimlessness, and at best doesn't specify what you're doing to the bit; `toggling a bit' has a more specific meaning (see bit twiddling, toggle).

*-Twilight Zone

n. [IRC] Notionally, the area of cyberspace where IRC operators live. An op is said to have a “connection to the twilight zone”.

*-Twink

/twink/ n. [UCSC] Equivalent to read-only user. Also reported on the Usenet group soc. motss; may derive from gay slang for a cute young thing with nothing upstairs (compare mainstream `chick').

*-Twirling Baton

n. [PLATO] The overstrike sequence -/|\-/|\- which produces an animated twirling baton. If you output it with a single backspace between characters, the baton spins in place. If you output the sequence BS SP between characters, the baton spins from left to right. If you output BS SP BS BS between characters, the baton spins from right to left. The twirling baton was a popular component of animated signature files on the pioneering PLATO educational timesharing system. The `archie' Internet service is perhaps the best-known baton program today; it uses the twirling baton as an idler indicating that the program is working on a query.

Twit

User who can not, or will not use the system properly. Reactions to this type of user are usually severe, including denial of access and notification to other SYSOPs in the area. (BBD;)

Two Person Integrity

(TPI) A system of storage and handling designed to prohibit access to certain COMSEC keying material, by requiring the presence of at least two formally authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. (NTISSI 3004)

*-Two Pi

quant. The number of years it takes to finish one's thesis. Occurs in stories in the following form “He started on his thesis; 2 pi years later. ”:two-to-the-N quant. An amount much larger than N but smaller than infinity. “I have 2-to-the-N things to do before I can go out for lunch” means you probably won't show up.

Two-Out-Of-Five Code

A binary-coded decimal notation in which each decimal digit is represented by a binary numeral consisting of five binary digits of which two are of one kind, conventionally “ones,” and three are of the other kind, conventionally “zeros. ” The usual weights are 0-1-2-3-6, except for the representation of “zero,” which is then 01100. (FP) (ISO)

Two-Part Code

Code consisting of an encoding section, in which the vocabulary items (with their associated code groups) are arranged in alphabetical or other systematic order, and a decoding section, in which the code groups (with their associated meanings) are arranged in a separate alphabetical or numeric order.

Two-Person Control

(TPC) Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

Two-Person Integrity

(TPI) System of storage and handling designed to prohibit individual access to certain COMSEC keying material, by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. NOTE: Two-person integrity procedures differ from COMSEC no-lone zone procedures in that, under two-person integrity controls, two authorized persons must directly participate in the handling and safeguarding of the keying material (as in accessing storage containers, transportation, keying/rekeying operations, and destruction). COMSEC no-lone zone controls are less restrictive in that the two authorized persons need only to be physically present in the common area where the material is located. Two-person control refers to nuclear command and control COMSEC material while two-person integrity refers only to COMSEC keying material.

Two-Way Encryption

*-Twonkie

/twon'kee/ n. The software equivalent of a Twinkie (a variety of sugar-loaded junk food); a useless `feature' added to look sexy and placate a marketroid (compare Saturday-night special). The term may also be related to “The Twonky”, title menace of a classic SF short story by Lewis Padgett (Henry Kuttner and C. L. Moore), first published in the September 1942 “Astounding Science Fiction” and subsequently much anthologized.

Type 1 Magnetic Media

Magnetic media with coercivity factors not exceeding 325 oersteds. (CSC-STD-005-85;) See Magnetic Media.

Type 1 Product

Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U. S. Government information, when appropriately keyed. NOTE: The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified National Security Agency algorithms. They are available to U. S. Government users, their contractors, and federally sponsored non-U. S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

Type 2 Magnetic Media

Magnetic media with coercivity factors exceeding 325 oersteds, possibly as high as 750 oersteds (also known as high energy media). (CSC-STD-005-85;) See Magnetic Media.

Type 2 Product

Unclassified cryptographic equipment, assembly, or component, endorsed by the National Security Agency, for use in telecommunications and automated information systems for the protection of national security information. NOTE: The term refers only to products, not to information, key, services, or controls. Type 2 products may not be used for classified information, but contain classified National Security Agency algorithms that distinguish them from products containing the unclassified data encryption standard algorithm. Type 2 products are available to U. S. Government departments and agencies and sponsored elements of state and local governments, sponsored U. S. Government contractors, and sponsored private sector entities. Type 2 products are subject to export restrictions in accordance with International Traffic in Arms Regulation.

Type 3 Algorithm

Cryptographic algorithm that has been registered by the National Institute of Standards and Technology and has been published as a Federal Information Processing Standard for use in protecting unclassified sensitive information or commercial information.

Type 4 Algorithm

Unclassified cryptographic algorithm that has been registered by the National Institute of Standards and Technology, but is not a Federal Information Processing Standard.

Type Accreditation

Official authorization by the DAA to employ a system in a specified environment. This authorization includes a statement of residual risk, delineates operating environment, and specific use. It is performed when multiple copies of a system are to be fielded. (*AFR* 205-16;)

Type Of Event

U

*-U

pref. Written shorthand for micro-. Derived from the Greek letter “mu”, the first letter of “micro” (and which letter looks a lot like the English letter “u”).

U. S. Controlled Facility

Base or building, access to which is physically controlled by U. S. persons who are authorized U. S. Government or U. S. Government contractor employees.

U. S. Controlled Space

Room or floor within a facility that is not a U. S. -controlled facility, access to which is physically controlled by U. S. persons who are authorized U. S. Government or U. S. Government contractor employees. NOTE: Keys or combinations to locks controlling entrance to U. S. -controlled spaces must be under the exclusive control of U. S. persons who are U. S. Government or U. S. Government contractor employees.

U. S. Nongovernmental Source

An individual citizen of the United States or a U. S. corporation, association or other organization substantially composed of United States citizens, which is not directly a part of the government (for example, a self-employed individual, consulting firm, licensee, or contractor, excluding active or reserve military personnel, Civil Service employees, and other individuals employed directly by the government); specifically excluded are corporations or associations under foreign ownership, control, and influence. (NCSC-2)

U. S. Person

United States citizen or resident alien.

U. S. -Controlled Facility

Base or building, access to which is physically controlled by U. S. persons who are authorized U. S. Government or U. S. Government contractor employees.

U. S. -Controlled Space

Room or floor within a facility that is not a U. S. -controlled facility, access to which is physically controlled by U. S. persons who are authorized U. S. Government or U. S. Government contractor employees. NOTE: Keys or combinations to locks controlling entrance to U. S. -controlled spaces must be under the exclusive control of U. S. persons who are U. S. Government or U. S. Government contractor employees.

*-UBD

/U-B-D/ n. [abbreviation for `User Brain Damage'] An abbreviation used to close out trouble reports obviously due to utter cluelessness on the user's part. Compare pilot error; oppose PBD; see also brain-damaged.

*-UN*X

n. Used to refer to the UNIX operating system (a trademark of AT&T) in writing, but avoiding the need for the ugly (TM) typography. Also used to refer to any or all varieties of Unixoid operating systems.

Ironically, lawyers now say that the requirement for the TM-postfix has no legal force, but the asterisk usage is entrenched anyhow. It has been suggested that there may be a psychological connection to practice in certain religions (especially Judaism) in which the name of the deity is never written out in full, e. g. , `YHWH' or `G--d' is used. See also glob.

Unapproved Software

All software that has not been formally identified, evaluated, and examined by competent personnel to ensure that the software performs to exact specifications. (*AR* 380-380;)

Unauthorized Disclosure

The revelation of information to individuals not authorized to receive it.

#-Unauthorized Disclosure Of Information

The revelation of information to individuals not authorized to receive it. (Source: NSTISSI 4009).

Unauthorized Modification

Unauthorized User

Unavailability

A measure of the degree to which a system, subsystem, or equipment is not operable and not in a committable state at the start of a mission, when the mission is called for at an unknown (random) point in time. Expressed mathematically, 1 minus the availability. (~) Note: The conditions determining operability and committability must be specified. See also availability.

Unbundling

In the context of the FCC's Computer III Inquiry, the process of separating individual tariffed offerings and services that are associated with a specific element in the CEI or ONA tariff from other tariffed basic service offerings. (After para. 158, FCC Report and Order, 6/16/86) See also basic service element, basic serving arrangement.

Uncertainty Calculus

1. A set of certainty measures and operations for combining them. (MA;)
2. A set of uncertainty measures and operations for amalgamating uncertainty measures. (ET;)

Unclassified

Information that has not been determined, pursuant to E. O. 12356 or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.

Unclassified Controlled Nuclear Information

(UCNI) Unclassified information whose unauthorized dissemination is prohibited under section 148 of the Atomic Energy Act. (DOE 5635. 1a)

Unclassified Information

Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse. (DODD 5200. 28)

Unclassified Telecommunications Security

That domain of unclassified computer security that is concerned with protecting the point-to-point communication (e. g. , input device to computer, computer to computer) of sensitive unclassified information with appropriate cost effective measures (e. g. , data encryption and protected distribution systems). Such communications generally occur via data communication systems, links, and devices such as networks, local area networks, telephone/wire lines, fiber optics, radio waves/microwaves, and integrated circuits. (*DOE 1360. 2A*)

Uncontrolled Access Area

(UAA) The area external or internal to a facility over which no personnel access controls can be or are exercised. (NACSIM 5203)

*-Undefined External Reference

excl. [UNIX] A message from UNIX's linker. Used in speech to flag loose ends or dangling references in an argument or discussion.

*-Under The Hood

1. [hot-rodder talk] Used to introduce the underlying implementation of a product (hardware, software, or idea). Implies that the implementation is not intuitively obvious from the appearance, but the speaker is about to enable the listener to grok it. “Let's now look under the hood to see how . ”
2. Can also imply that the implementation is much simpler than the appearance would indicate “Under the hood, we are just fork/execing the shell. ”
3. . Inside a chassis, as in “Under the hood, this baby has a 40MHz 68030!”

Underlap

In facsimile, a defect that occurs when the width of the scanning line is less than the scanning pitch. See also facsimile, tailing.

Undesired Signal Data Emanations

(USDE) Compromising emanations or a primary RED line amplitude density spectrum which exceeds limits specified in the applicable TEMPEST standard.

*-Undocumented Feature

n. See feature.

Uniform Encoding

An analog-to-digital conversion process in which, except for the highest and lowest quantization steps, all of the quantization subrange values are equal. See uniform quantizing. See also analog encoding, code, quantization, quantization level, signal.

*-Uninteresting

1. adj. Said of a problem that, although nontrivial, can be solved simply by throwing sufficient resources at it.
2. Also said of problems for which a solution would neither advance the state of the art nor be fun to design and code. Hackers regard uninteresting problems as intolerable wastes of time, to be solved (if at all) by lesser mortals. *Real* hackers (see toolsmith) generalize uninteresting problems enough to make them interesting and solve them -- thus solving the original problem as a special case (and, it must be admitted, occasionally turning a molehill into a mountain, or a mountain into a tectonic plate). See WOMBAT, SMOP; compare toy problem, oppose interesting.

Unit Element

In the representation of a character, a signal element that has a duration (length) equal to the unit interval. (~) See also character, code.

Unit Interval

In a system using isochronous transmission, that interval of time such that the theoretical durations of the significant intervals of a signal are all whole multiples of this interval. (~) Note: The unit interval is the shortest time interval between two consecutive significant instants. See also character interval.

UNIX

A computer operating system. See also operating system.

*-UNIX Brain Damage

n. Something that has to be done to break a network program (typically a mailer) on a non-UNIX system so that it will interoperate with UNIX systems. The hack may qualify as `UNIX brain damage' if the program conforms to published standards and the UNIX program in question does not. UNIX brain damage happens because it is much easier for other (minority) systems to change their ways to match non-conforming behavior than it is to change all the hundreds of thousands of UNIX systems out there. An example of UNIX brain damage is a kluge in a mail server to recognize bare line feed (the UNIX newline) as an equivalent form to the Internet standard newline, which is a carriage return followed by a line feed. Such things can make even a hardened jock weep.

*-UNIX Conspiracy

n. [ITS] According to a conspiracy theory long popular among ITS and TOPS-20 fans, UNIX's growth is the result of a plot, hatched during the 1970s at Bell Labs, whose intent was to hobble AT&T's competitors by making them dependent upon a system whose future evolution was to be under AT&T's control. This would be accomplished by disseminating an operating system that is apparently inexpensive and easily portable, but also relatively unreliable and insecure (so as to require continuing upgrades from AT&T). This theory was lent a substantial impetus in 1984 by the paper referenced in the back door entry. In this view, UNIX was designed to be one of the first computer viruses (see virus) -- but a virus spread to computers indirectly by people and market forces, rather than directly through disks and networks. Adherents of this `UNIX virus' theory like to cite the fact that the well-known quotation “UNIX is snake oil” was uttered by DEC president Kenneth Olsen shortly before DEC began actively promoting its own family of UNIX workstations. (Olsen now claims to have been misquoted.)

*-UNIX Weenie

1. n. [ITS] A derogatory play on `UNIX wizard', common among hackers who use UNIX by necessity but would prefer alternatives. The implication is that although the person in question may consider mastery of UNIX arcana to be a wizardly skill, the only real skill involved is the ability to tolerate (and the bad taste to wallow in) the incoherence and needless complexity that is alleged to infest many UNIX programs. “This shell script tries to parse its arguments in 69 bletcherous ways. It must have been written by a real UNIX weenie. ”
2. A derogatory term for anyone who engages in uncritical praise of UNIX. Often appearing in the context “stupid UNIX weenie”. See Weenix, UNIX conspiracy. See also weenie.

*-UNIX:

/yoo'niks/ n. [In the authors' words, “A weak pun on Multics”] (also `Unix') An interactive time-sharing system invented in 1969 by Ken Thompson after Bell Labs left the Multics project, originally so he could play games on his scavenged PDP-7. Dennis Ritchie, the inventor of C, is considered a co-author of the system. The turning point in UNIX's history came when it was reimplemented almost entirely in C during 1972--1974, making it the first source-portable OS. UNIX subsequently underwent mutations and expansions at the hands of many different people, resulting in a uniquely flexible and developer-friendly environment. By 1991, UNIX had become the most widely used multiuser general-purpose operating system in the world. Many people consider this the most important victory yet of hackerdom over industry opposition (but see UNIX weenie and UNIX conspiracy

for an opposing point of view). See Version 7, BSD, USG UNIX. Some people are confused over whether this word is appropriately `UNIX' or `Unix'; both forms are common, and used interchangeably. Dennis Ritchie says that the `UNIX' spelling originally happened in CACM's 1973 paper because “we had a new typesetter and troff had just been invented and we were intoxicated by being able to produce small caps. ” Later, dmr tried to get the spelling changed to `Unix' in a couple of Bell Labs papers, on the grounds that the word is not acronymic. He failed, and eventually (his words) “wimped out” on the issue. So both capitalizations are grounded in ancient usage.

*-Unixism

n. A piece of code or a coding technique that depends on the protected multi-tasking environment with relatively low process-spawn overhead that exists on virtual-memory UNIX systems. Common unixisms include gratuitous use of `fork(2)'; the assumption that certain undocumented but well-known features of UNIX libraries such as `stdio(3)' are supported elsewhere; reliance on obscure side-effects of system calls (use of `sleep(2)' with a 0 argument to clue the scheduler that you're willing to give up your timeslice, for example); the assumption that freshly allocated memory is zeroed; and the assumption that fragmentation problems won't arise from never `free()'ing memory. Compare vaxocentrism; see also New Jersey.

Unnumbered Command

In a data transmission, a command that does not contain sequence numbers in the control field. See also control character.

Unnumbered Response

In a data transmission, a response that does not contain sequence numbers in the control field. See also response.

Unprivileged User

Unprotect

1. A software program which copies copy protected software. Usually these programs are available before the “protected” product. (BBD)
2. See COPY PROTECTED.

Unprotected

Unsuccessful Call

A call attempt that does not result in the establishment of a connection. See also lost call.

*-Unswizzle

v. See swizzle.

Untrusted Applications

Untrusted Element

An element of the system which can not be relied upon to perform its function correctly or reliably. (MK;)

Untrusted Process

1. A process whose incorrect or malicious execution cannot affect system security. Verification is usually not applied to untrusted processes. (MTR-8201)
2. A process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms. (*NCSC-TG*-004-88)

*-Unwind The Stack

1. vi. [techspeak] During the execution of a procedural language, one is said to `unwind the stack' from a called procedure up to a caller when one discards the stack frame and any number of frames above it, popping back up to the level of the given caller. In C this is done with `longjmp'/`setjmp', in LISP with `throw/catch'. See also smash the stack.
2. People can unwind the stack as well, by quickly dealing with a bunch of problems “Oh heck, let's do lunch. Just a second while I unwind my stack. ”

*-Unwind-Protect

N. [MIT
from the name of a LISP operator] A task you must remember to perform before you leave a place or finish a project. “I have an unwind-protect to call my advisor. ”

*-Up

adj. Working, in order. “The down escalator is up. ” Oppose down.

Up-Converter

A device for performing frequency translation in such a manner that the output frequencies are higher than the input frequencies. (~) See also down-converter, erect position, frequency, frequency translation, inverted position.

Updating

Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system.

Upgrade Parameter

A parameter indicating a policy of replacing an impacted asset with an item of higher quality. (RM;)

Uplink

1. That portion of a communication link used for transmission of signals from an Earth terminal to a satellite or airborne platform. It is the converse of “downlink. ” (~)

2. Pertaining to data transmission from a data station to the head-end. (FP) (ISO) (~) See also downlink, link, satellite.

*-Upload

1. /uhp'lohd/ v. [techspeak] To transfer programs or data over a digital communications link from a smaller or peripheral `client' system to a larger or central `host' one. A transfer in the other direction is, of course, called a download (but see the note about ground-to-space comm under that entry).
2. [speculatively] To move the essential patterns and algorithms that make up one's mind from one's brain into a computer. Those who are convinced that such patterns and algorithms capture the complete essence of the self view this prospect with pleasant anticipation.

*-Upthread

adv. Earlier in the discussion (see thread), i. e. , `above'. “As Joe pointed out upthread, . ” See also followup.

Uptime

The time during which a functional unit is fully operational. (~) See also downtime.

*-Urchin

n. See munchkin.

*-URL

/erl/ n. Universal Resource Locator, an address widget that identifies a document or resource on the World-Wide Web. This entry is here primarily to record the fact that the term is commonly pronounced /erl/, not /U-R-L/ (except perhaps in the most formal contexts).

Usable Line Length

See available line.

Usage

See occupancy.

Useful Line

See available line.

*-Usenet

/yoos'net/ or /yooz'net/ n. [from `Users' Network'; the original spelling was USENET, but the mixed-case form is now widely preferred] A distributed bboard (bulletin board) system supported mainly by UNIX machines. Originally implemented in 1979--1980 by Steve Bellovin, Jim Ellis, Tom Truscott, and Steve Daniel at Duke University, it has swiftly grown to become international in scope and is now probably the largest decentralized information utility in existence. As of early 1993, it hosts well over 1200 newsgroups and an average of 40 megabytes (the equivalent of several thousand paper pages) of new technical articles, news, discussion, chatter, and flamage every day.

User

1. A person, organization, or other entity (including a computer or computer system), that employs the services provided by a telecommunication system, or by an information processing system, for transfer of information to others. (~) Note: A user functions as a source or final destination of user information, or both.
2. In automated information systems, a person or process accessing an automated information system by direct connections (e. g. , via terminals), or indirect connections (i. e. , prepare input data or receive output that is not reviewed for content or classification by a responsible individual).
3. In COMSEC, an individual who is required to use COMSEC material in the performance of his/her duties, and who is responsible for safeguarding that COMSEC material. See also access originator, automated information system, communications sink, communications source, destination user, originating user, terminal. (Combined Glossary
4. An organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to the manager or director of the facility or to the same immediate supervisor. (A-130)
5. An individual (person or organization) with direct access to the system or an individual without access who receives output or generates input not reviewed by another. (*AFR* 205-16; *AFR* 700-10)
6. Any authorized person, office, or staff agency who may use or receive services or products from a computer system. Synonymous with customer. (*AR* 380-380)
7. Any person who interacts directly with a computer system. (*DOD* 5200. 28-STD)
8. A user is an individual and/or processes operating on his/her/its behalf. (*DCID* 1/1 6, Sup.)
9. People or processes accessing an AIS either by direct connections (i. e. , via terminals) or indirect connections (i. e. , prepare input data or software or receive output that is not reviewed for content and classification by a responsible individual). (DODD 5200. 28)
10. Any individual who is able to operate any equipment that can access the ADP system or input commands to the ADP system or receive output from the ADP system without intervention of an authorized reviewing official. Note that a user may not necessarily be an authorized user of the ADP system. (DOE 5637. 1)
11. A person or organization receiving products or services produced by an ADP system either by ac-

cess to the system or by other means. (*OPNAVINST* 5239. 1 A)

User ID

A unique symbol or character string that is used by a system to identify a specific user. (*NCSC-TG*-004-88)

User Identification

Unique symbol or character string that is used by an AIS to uniquely identify a specific user. See User ID

User Information

Information transferred across the functional interface between a source user and a telecommunication system for the purpose of ultimate delivery to a destination user. Note: In data telecommunication systems, “user information” includes user overhead information. See also delivered overhead bit, delivered overhead block, destination user, interface (def. #2), overhead bit, overhead information, source user.

User Information Bit

A bit transferred from a source user to a telecommunication system for the purpose of ultimate delivery to a destination user. (~) Note: User information bits do not include those overhead bits originated by, or having their primary functional effect within, the telecommunication system. See also binary digit, overhead bit.

User Information Block

A block that contains at least one user information bit. (~) See also block.

User Partnership Program

(UPP) Partnership between the National Security Agency and a U. S. Government department or agency to facilitate the development of secure information processing and communications equipment incorporating National Security Agency approved cryptographic security.

User Profile

Patterns of a user's activity which can detect changes in normal routines. (*NCSC-WA*-001-85;)

*-User-Obsequious

adj. Emphatic form of user-friendly. Connotes a system so verbose, inflexible, and determinedly simple-minded that it is nearly unusable. “Design a system any fool can use and only a fool will want to use it. ” See WIMP environment, Macintrash.

User/process Interface

*-USG UNIX

/U-S-G yoo'niks/ n. Refers to AT&T UNIX commercial versions after Version 7, especially System III and System V releases 1, 2, and 3. So called because during most of the lifespan of those versions AT&T's support crew was called the `UNIX Support Group'. See BSD, UNIX.

Utility Program

A computer program in general support of the processes of a computer; for example, a diagnostic program, a trace program. See service program.

Utility Routine

A routine in general support of the processes of a computer; for example, an input routine. (FP) (ISO) See service routine. See also tool.

*-UTSL

// n. [UNIX] On-line acronym for `Use the Source, Luke' (a pun on Obi-Wan Kenobi's “Use the Force, Luke!” in “Star Wars”) -- analogous to RTFS (sense 1), but more polite. This is a common way of suggesting that someone would be better off reading the source code that supports whatever feature is causing confusion, rather than making yet another futile pass through the manuals, or broadcasting questions on Usenet that haven't attracted wizards to answer them. Once upon a time in elder days, everyone running UNIX had source. After 1978, AT&T's policy tightened up, so this objurgation was in theory appropriately directed only at associates of some outfit with a UNIX source license. In practice, bootlegs of UNIX source code (made precisely for reference purposes) were so ubiquitous that one could utter it at almost anyone on the network without concern. Nowadays, free UNIX clones are becoming common enough that almost anyone can read source legally. The most widely distributed is probably Linux, with variants of the NET/2 and 4. 4BSD distributions running second. Cheap commercial UNIXes with source such as BSD/386 are accelerating this trend.

*-UUCPNET

n. The store-and-forward network consisting of all the world's connected UNIX machines (and others running some clone of the UUCP (UNIX-to-UNIX CoPy) software). Any machine reachable only via a bang path is on UUCPNET. See network address

V

V Model

See adVanced development model.

*-V7

n. See Version 7.

Vaccines

Program that “injects” itself into an executable program to perform a signature check and warns if there have been any changes. See Anti-Virus Program.

*-Vadding

/vad'ing/ n. [from VAD, a permutation of ADV (i. e. , ADVENT), used to avoid a particular admin's continual search-and-destroy sweeps for the game]

A leisure-time activity of certain hackers involving the covert exploration of the `secret' parts of large buildings -- basements, roofs, freight elevators, maintenance crawlways, steam tunnels, and the like. A few go so far as to learn locksmithing in order to synthesize vadding keys. The verb is `to vad' (compare phreaking; see also hack, sense 9). This term dates from the late 1970s, before which such activity was simply called `hacking'; the older usage is still prevalent at MIT. The most extreme and dangerous form of vadding is `elevator rodeo', a. k. a. `elevator surfing', a sport played by wrasslin' down a thousand-pound elevator car with a 3-foot piece of string, and then exploiting this mastery in various stimulating ways (such as elevator hopping, shaft exploration, rat-racing, and the ever-popular drop experiments). Kids, don't try this at home! See also hobbit (sense 2. .

Valid Password

A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system. (*FIPS PUB* 112;)

Validation

1. The performance of tests and evaluations in order to determine compliance with security specifications and requirements. (*FIPS PUB* 39;)
2. That portion of the development of specialized ST&E, procedures, tools, and equipment needed to establish acceptance for joint usage by one or more *DOD* components or their contractors. Such action will include, as necessary, final development, evaluation, testing, leading to acceptance by senior ST&E staff specialists of the three Military Departments or a Defence Agency, and approval for joint usage by the Deputy Under Secretary of Defence for Policy Review. (*OPNAVINST* 5239. 1A;; *AR* 380-380;; DODD 5200. 28M;) See also automated information system, trusted computer system.

#-Validation (Testing)

Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an AIS by one or more departments or agencies and their contractors. (Source: NSTISSI 4009).

Value Of The Represented

A parameter indicating the value of an asset within the organization as opposed to the replacement cost of the data which represents the asset. (RM;)

#-Value-Added Networks

A communications service using the communications networks of a common carrier for transmission and providing added data services with separate additional equipment (or software). Added services may include store and forward message switching, terminal and host interfacing. (Source -: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

*-Vanilla

adj. [from the default flavor of ice cream in the U. S.] Ordinary flavor, standard. When used of food, very often does not mean that the food is flavored with vanilla extract! For example, `vanilla wonton soup' means ordinary wonton soup, as opposed to hot-and-sour wonton soup. Applied to hardware and software, as in “Vanilla Version 7 UNIX can't run on a vanilla 11/34. ” Also used to orthogonalize chip nomenclature; for instance, a 74V00 means what TI calls a 7400, as distinct from a 74LS00, etc. This word differs from canonical in that the latter means `default', whereas vanilla simply means `ordinary'. For example, when hackers go on a great-wall, hot-and-sour soup is the canonical soup to get (because that is what most of them usually order) even though it isn't the vanilla (wonton) soup.

*-Vannevar

/van'*-var/ n. A bogus technological prediction or a foredoomed engineering concept, esp. one that fails by implicitly assuming that technologies develop linearly, incrementally, and in isolation from one another when in fact the learning curve tends to be highly nonlinear, revolutions are common, and competition is the rule. The prototype was Vannevar Bush's prediction of `electronic brains' the size of the Empire State Building with a Niagara-Falls-equivalent cooling system for their tubes and relays, a prediction made at a time when the semiconductor effect had already been demonstrated. Other famous vannevars have included magnetic-bubble memory, LISP machines, videotex, and a paper from the late 1970s that computed a purported ultimate limit on areal density for ICs that was in fact less than the routine densities of 5 years later.

*-Vaporware

/vay'pr-weir/ n. Products announced far in advance of any release (which may or may not actually take place). See also brochureware.

*-Var

/veir/ or /var/ n. Short for `variable'. Compare arg, param.

Variable Length Buffer

A buffer into which data may be entered at one rate and removed at another, without changing the data sequence. (~) Note: Most first-in first-out (FIFO) storage devices serve this purpose in that the input rate may be variable while the output rate is constant or the output rate may be variable while the input rate

is fixed. Various clocking and control systems are used to allow control of underflow or overflow conditions. See also buffer, data, elastic buffer.

Variant

1. One of two or more cipher or code symbols which have the same plain text equivalent. (JCS1-DoD)
2. One of several plain text meanings that are represented by a single code group. See alternative. (JCS1-DoD) See also code, cryptology, encode.

*-VAX

1. /vaks/ n. [from Virtual Address eXtension] The most successful minicomputer design in industry history, possibly excepting its immediate ancestor, the PDP-11. Between its release in 1978 and its eclipse by killer micros after about 1986, the VAX was probably the hacker's favorite machine of them all, esp. after the 1982 release of 4. 2 BSD UNIX (see BSD). Esp. noted for its large, assembler-programmer-friendly instruction set -- an asset that became a liability after the RISC revolution.
2. A major brand of vacuum cleaner in Britain. Cited here because its alleged sales pitch, “Nothing sucks like a VAX!” became a sort of battle-cry of RISC partisans. It is even sometimes claimed that DEC actually entered a cross-licensing deal with the vacuum-Vax people that allowed them to market VAX computers in the U. K. in return for not challenging the vacuum cleaner trademark in the U. S. It is sometimes claimed that this slogan was *not* actually used by the Vax vacuum-cleaner people, but was actually that of a rival brand called Electrolux (as in “Nothing sucks like. ”). It has been reliably confirmed that Electrolux (a Swedish company) actually did use this slogan in the late 1960s; it has apparently become a classic example (used in textbooks) of the perils of not knowing the local idiom. It appears, however, that the Vax people thought the slogan a sufficiently good idea to copy it. Several British hackers report that their promotions used it in 1986--1987, and we have one report from a New Zealander that the infamous slogan surfaced there in TV ads for the product as recently as 1992!

*-VAXectomy

/vak-sek't*-mee/ n. [by analogy with `vasectomy'] A VAX removal. DEC's Microvaxen, especially, are much slower than newer RISC-based workstations such as the SPARC. Thus, if one knows one has a replacement coming, VAX removal can be cause for celebration.

*-VAXen

/vak'sn/ n. [from `oxen', perhaps influenced by `vixen'] (alt. `vaxen') The plural canonically used among hackers for the DEC VAX computers. “Our installation has four PDP-10s and twenty vaxen. ” See boxen.

*-Vaxherd

n. /vaks'herd/ [from `oxherd'] A VAX operator.

*-Vaxism

/vak'sizm/ n. A piece of code that exhibits vaxocentrism in critical areas. Compare PC-ism, unixism.

*-Vaxocentrism

/vak`soh-sen'trizm/ n. [analogy with `ethnocentrism'] A notional disease said to afflict C programmers who persist in coding according to certain assumptions that are valid (esp. under UNIX) on VAXen but false elsewhere. Among these are

1. The assumption that dereferencing a null pointer is safe because it is all bits 0, and location 0 is readable and 0. Problem: this may instead cause an illegal-address trap on non-VAXen, and even on VAXen under OSes other than BSD UNIX. Usually this is an implicit assumption of sloppy code (forgetting to check the pointer before using it), rather than deliberate exploitation of a misfeature.
2. The assumption that characters are signed.
3. The assumption that a pointer to any one type can freely be cast into a pointer to any other type. A stronger form of this is the assumption that all pointers are the same size and format, which means you don't have to worry about getting the casts or types correct in calls. Problem this fails on word-oriented machines or others with multiple pointer formats.
4. The assumption that the parameters of a routine are stored in memory, on a stack, contiguously, and in strictly ascending or descending order. Problem this fails on many RISC architectures.
5. The assumption that pointer and integer types are the same size, and that pointers can be stuffed into integer variables (and vice-versa) and drawn back out without being truncated or mangled. Problem this fails on segmented architectures or word-oriented machines with funny pointer formats.
6. The assumption that a data type of any size may begin at any byte address in memory (for example, that you can freely construct and dereference a pointer to a word- or greater-sized object at an odd char address). Problem this fails on many (esp. RISC) architectures better optimized for HLL execution speed, and can cause an illegal address fault or bus error.
7. The (related) assumption that there is no padding at the end of types and that in an array you can thus step right from the last byte of a previous component to the first byte of the next one. This is not only machine- but compiler-dependent.
8. The assumption that memory address space is globally flat and that the array reference `foo[-1]' is necessarily valid. Problem this fails at 0, or

other places on segment-addressed machines like Intel chips (yes, segmentation is universally considered a brain-damaged way to design machines (see moby), but that is a separate issue).

9. The assumption that objects can be arbitrarily large with no special considerations. Problem this fails on segmented architectures and under non-virtual-addressing environments.
10. The assumption that the stack can be as large as memory. Problem this fails on segmented architectures or almost anything else without virtual addressing and a paged stack.
11. The assumption that bits and addressable units within an object are ordered in the same way and that this order is a constant of nature. Problem this fails on big-endian machines.
12. The assumption that it is meaningful to compare pointers to different objects not located within the same array, or to objects of different types. Problem the former fails on segmented architectures, the latter on word-oriented machines or others with multiple pointer formats.
13. The assumption that an `int' is 32 bits, or (nearly equivalently) the assumption that `sizeof(int) == sizeof(long)'. Problem this fails on PDP-11s, 286-based systems and even on 386 and 68000 systems under some compilers.
14. The assumption that `argv[]' is writable. Problem this fails in many embedded-systems C environments and even under a few flavors of UNIX. Note that a programmer can validly be accused of vaxocentrism even if he or she has never seen a VAX. Some of these assumptions (esp. 2--5) were valid on the PDP-11, the original C machine, and became endemic years before the VAX. The terms `vaxocentricity' and `all-the-world's-a-VAX syndrome' have been used synonymously.

*-Vdiff

/vee'dif/ v. ,n. Visual diff. The operation of finding differences between two files by eyeball search. The term `optical diff' has also been reported, and is sometimes more specifically used for the act of superimposing two nearly identical printouts on one another and holding them up to a light to spot differences. Though this method is poor for detecting omissions in the `rear' file, it can also be used with printouts of graphics, a claim few if any diff programs can make. See diff.

VDT

See Video Display Terminal.

*-Veeblefester

/vee'b*l-fes`tr/ n. [from the “Born Loser” comix via Commodore; prob. originally from “Mad” Magazine's `Veeblefeetzer' parodies ca. 1960] Any obnoxious person engaged in the (alleged) professions of marketing or management. Antonym of hacker. Compare suit, marketroid.

Vendor Security Analyst

Unknown

*-Ventilator Card

n. Syn. lace card.

*-Venus Flytrap

n. [after the insect-eating plant] See firewall machine.

*-Verbage

/ver'b*j/ n. A deliberate misspelling and mispronunciation of verbiage that assimilates it to the word `garbage'. Compare content-free. More pejorative than `verbiage'.

*-Verbiage

n. When the context involves a software or hardware system, this refers to documentation. This term borrows the connotations of mainstream `verbiage' to suggest that the documentation is of marginal utility and that the motives behind its production have little to do with the ostensible subject.

Verifiable Identification Forwarding

1. An identification method used in networks where the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user. (DOE 5637. 1)
2. See TRUSTED IDENTIFICATION FORWARDING.

Verification

1. The documentation of penetration or attempts to penetrate an actual on-line system in support or in contradiction of assumptions developed during system review and analysis. (*AR* 380-380;)
2. The successful testing and documentation of actual on-line system penetration or attempts to penetrate the system in support or in contradiction or assumptions developed during system review and analysis which are to be included in the evaluation report. (DODD 5200. 28M;)
3. The process of comparing two levels of system specification for proper correspondence (e. g. , security policy model with top-level specifications, top-level specification with source code, or source code with object code). This process may or may not be automated. (*NCSC-WA*-001-85;; CSC-STD-001-83;)

#-Verification And Validation Process

The process of comparing two levels of a system specification for proper correspondence or of proving that some property of a specification is correctly im-

plemented by the system (e. g. , security policy model with top- level specification, top-level specification with source code with object).
NOTE: Verification may be formal or informal, or automated or not automated. Formal verification is the process of using formal proofs (complete mathematical argument) to demonstrate the consistency between formal specification of a system and formal security policy model (design verification) or between formal specification and its high-level program implementation (implementation verification). Formal implies using a formal mathematical language.

Verified Design

Computer protection class in which formal security verification methods are used to assure that the AIS mandatory and discretionary security controls can effectively protect classified and sensitive information stored in, or processed by, the system. NOTE: Class A1 system is verified design.

*-Version 7

alt. V7 /vee' se'vn/ n. The first widely distributed version of UNIX, released unsupported by Bell Labs in 1978. The term is used adjectivally to describe UNIX features and programs that date from that release, and are thus guaranteed to be present and portable in all UNIX versions (this was the standard gauge of portability before the POSIX and IEEE 1003 standards). Note that this usage does *not* derive from the release being the “seventh version of UNIX”; research UNIX at Bell Labs has traditionally been numbered according to the edition of the associated documentation. Indeed, only the widely-distributed Sixth and Seventh Editions are widely known as V[67]; the OS that might today be known as `V10' is instead known in full as “Tenth Edition Research Unix” or just “Tenth Edition” for short. For this reason, “V7” is often read by cognoscenti as “Seventh Edition”. See BSD, USG UNIX, UNIX. Some old-timers impatient with commercialization and kernel bloat still maintain that V7 was the Last True UNIX.

*-Vgrep

/vee'grep/ v. ,n. Visual grep. The operation of finding patterns in a file optically rather than digitally (also called an `optical grep'). See grep; compare vdiff.

*-Vi

/V-I/, *not* /vi:/ and *never* /siks/ n. [from `Visual Interface'] A screen editor crufted together by Bill Joy for an early BSD release. Became the de facto standard UNIX editor and a nearly undisputed hacker favorite outside of MIT until the rise of EMACS after about 1984. Tends to frustrate new users no end, as it will neither take commands while expecting input text nor vice versa, and the default setup provides no indication of which mode the editor is in (one correspondent accordingly reports that he has often heard the editor's name pronounced /vi:l/). Nevertheless it is still widely used (about half the respondents in a 1991 Usenet poll preferred it), and even EMACS fans often resort to it as a mail editor and for small editing jobs (mainly because it starts up faster than the bulkier versions of EMACS). See holy wars.

Video Display Terminal

See visual display unit.

Video Display Unit

See visual display unit.

Video Signal

A signal normally used to transmit changing pictorial information in real time. Note 1: The video signal bandwidth depends upon the mode of transmission, e. g. , slow-scan TV, full-scan, or digitized full-scan. Note 2: This definition describes the generic signal between a transmitter and receiver. See also signal, television.

*-Videotex

n. ,obs. An electronic service offering people the privilege of paying to read the weather on their television screens instead of having somebody read it to them for free while they brush their teeth. The idea bombed everywhere it wasn't government-subsidized, because by the time videotex was practical the installed base of personal computers could hook up to timesharing services and do the things for which videotex might have been worthwhile better and cheaper. Videotex planners badly overestimated both the appeal of getting information from a computer and the cost of local intelligence at the user's end. Like the gorilla arm effect, this has been a cautionary tale to hackers ever since. See also vannevar.

Videotext

Pertaining to a type of communication service in which a user can access a remote database and receive the requested data on the user's video display. Note: The database information is transmitted to the user's video display over a separate channel that may be a commercial carrier channel.

View

In satellite communications, the ability of a satellite Earth terminal to “see” a satellite, having it sufficiently above the horizon and clear of other obstructions so that it is within a free line of sight from the satellite Earth terminal. (~) Note: A pair of satellite Earth terminals has a satellite in “mutual” view when both have unobstructed line-of-sight contact with the satellite simultaneously. See also footprint, horizon angle, line-of-sight propagation, satellite.

Viewdata
An information retrieval system that uses a remote database accessible through the public telephone network. Video display of the data is on a monitor or television receiver. See also teletext.

Violation
See AMI violation.

Violations

*-Virgin
adj. Unused; pristine; in a known initial state. “Let's bring up a virgin system and see if it crashes again. ” (Esp. useful after contracting a virus through SEX.) Also, by extension, buffers and the like within a program that have not yet been used.

*-Virtual
adj. [via the technical term `virtual memory', prob. from the term `virtual image' in optics]
1. Common alternative to logical; often used to refer to the artificial objects (like addressable virtual memory larger than physical memory) created by a computer system to help the system control access to shared resources.
2. Simulated; performing the functions of something that isn't really there. An imaginative child's doll may be a virtual playmate. Oppose real.

Virtual Call
A call, established over a network, that uses the capabilities of either a real or virtual circuit by sharing all or any part of the resources of the circuit for the duration of the call.

Virtual Call Capability
A user service feature in which a call set-up procedure and a call-clearing procedure will determine a period of communication between two DTEs in which user's data will be transferred by the network in the packet mode of operation. Note 1: This service requires end-to-end transfer control of packets within a network. Note 2: Data may be delivered to the network before the call setup has been completed but it will not be delivered to the destination address if the call setup attempt is unsuccessful. Note 3: All the user's data are delivered from the network in the same order in which they are received by the network. Multi-access DTEs may have several virtual calls in operation at the same time. See virtual call facility. See also call, data terminal equipment, network, permanent virtual circuit, virtual circuit.

Virtual Call Facility
See virtual call capability.

Virtual Carrier Frequency
The location in the frequency spectrum that carrier energy would occupy if carrier energy were present. (~) See also carrier (cxr), frequency.

Virtual Circuit
(VC) A communications arrangement in which data from a source user may be passed to a destination user over various real circuit configurations during a single period of communication. (~) Note: Virtual circuits are generally set up on a per-call basis and are disconnected when the call is terminated; however, a permanent virtual circuit can be established as an option to provide a dedicated link between two facilities. See logical circuit. See also circuit, data, data circuit, network, permanent virtual circuit, virtual call capability.

Virtual Circuit Capability
A network service feature providing a user with a virtual circuit. Note: This feature is not necessarily limited to packet mode transmission, e. g. , an analog signal may be converted at its network node to a digital form, which may then be routed over the network via any available route.

Virtual Connection
A logical connection that is made to a virtual circuit.

*-Virtual Friday
n. (also `logical Friday') The last day before an extended weekend, if that day is not a `real' Friday. For example, the U. S. holiday Thanksgiving is always on a Thursday. The next day is often also a holiday or taken as an extra day off, in which case Wednesday of that week is a virtual Friday (and Thursday is a virtual Saturday, as is Friday). There are also `virtual Mondays' that are actually Tuesdays, after the three-day weekends associated with many national holidays in the U. S.

Virtual Memory
In computer systems, the memory as it appears to the operating programs running in the CPU; this memory may appear smaller, equal to, or larger than the real memory present in the system. See also central processing unit.

Virtual Network
A network providing virtual circuits and established from the facilities of a real network. See also virtual circuit.

Virtual Password
A password computed from a passphrase that meets the requirements of password storage (e. g. , 64 bits for DES). (*FIPS PUB* 112;)

*-Virtual Reality
1. n. Computer simulations that use 3-D graphics and devices such as the Dataglove to allow the user to interact with the simulation. See cyberspace.
2. A form of network interaction incorporating aspects of role-playing games, interactive theater,

improvisational comedy, and `true confessions' magazines. In a virtual reality forum (such as Usenet's alt. callahans newsgroup or the MUD experiments on Internet), interaction between the participants is written like a shared novel complete with scenery, `foreground characters' that may be personae utterly unlike the people who write them, and common `background characters' manipulable by all parties. The one iron law is that you may not write irreversible changes to a character without the consent of the person who `owns' it. Otherwise anything goes. See bamf, cyberspace, teledildonics.

*-Virtual Shredder

n. The jargonic equivalent of the bit bucket at shops using IBM's VM/CMS operating system. VM/CMS officially supports a whole bestiary of virtual card readers, virtual printers, and other phantom devices; these are used to supply some of the same capabilities UNIX gets from pipes and I/O redirection.

Virtual Storage

The storage space that may be regarded as addressable main storage by the user of a computer system in which virtual addresses are mapped into real addresses. Note: The size of virtual storage is limited by the addressing scheme of the computer system and by the amount of auxiliary storage available, and not by the actual number of main storage locations. (FP) (ISO)

Virus

1. A variation of Trojan Horse. It is propagating (attaching itself to files, programs) with a triggering mechanism (event, time) with a mission (delete files, send data). Protection from a virus is beyond the Criteria. (*AFR* 205-16;)
2. A self-propagating trojan horse, composed of three parts: a mission component, a trigger component and a self-propagating component. (*NCSC-WA*-001-85;)
3. A program that can “infect” other programs by modifying them to include a, possibly evolved, copy of itself. (Cohen;)
4. A virus is a program which “infects” other programs by modifying them to include a copy of itself. It cannot activiate itself independently, but only when its host program is explicitly invoked. The virus may contain a logic bomb or trojan horse. (IC;)

*-Visionary

1. n. One who hacks vision, in the sense of an Artificial Intelligence researcher working on the problem of getting computers to `see' things using TV cameras. (There isn't any problem in sending information from a TV camera to a computer. The problem is, how can the computer be programmed to make use of the camera information? See SMOP, AI-complete.)
2. [IBM] One who reads the outside literature. At IBM, apparently, such a penchant is viewed with awe and wonder.

*-VMS

/V-M-S/ n. DEC's proprietary operating system for its VAX minicomputer; one of the seven or so environments that loom largest in hacker folklore. Many UNIX fans generously concede that VMS would probably be the hacker's favorite commercial OS if UNIX didn't exist; though true, this makes VMS fans furious. One major hacker gripe with VMS concerns its slowness -- thus the following limerick There once was a system called VMS Of cycles by no means abstemious. It's chock-full of hacks And runs on a VAX And makes my poor stomach all squeamious. -- The Great Quux See also VAX, TOPS-10, TOPS-20, UNIX, runic.

Vocoder

See voice-coder. A type of voice coder, usually consisting of a speech analyzer and a speech synthesizer. (~) Note 1: The analyzer circuitry converts analog speech waveforms into digital signals. The synthesizer converts the digital signals into artificial speech sounds. Note 2: For COMSEC purposes, a vocoder may be used in conjunction with a key generator and a modulator-demodulator device to transmit digitally encrypted speech signals over normal narrowband voice communication channels. These devices are used to reduce the bandwidth requirements for transmitting digitized speech signals. Note 3. There are analog vocoders that move incoming signals from one portion of the spectrum to another portion. See also code, communications security.

*-Voice

vt. To phone someone, as opposed to emailing them or connecting in talk mode. “I'm busy now; I'll voice you later. ”

#-Voice Communications Security

This KSA has no definition.

#-Voice Mail Security

This KSA has no definition.

*-Voice-Net

n. Hackish way of referring to the telephone system, analogizing it to a digital network. Usenet sig blocks not uncommonly include the sender's phone next to a “Voice:” or “Voice-Net:” header; common variants of this are “Voicenet” and “V-Net”. Compare paper-net, snail-mail.

Volatile Memory

Memory (such as semiconductor memory) that loses memory retention capability when electric power is removed. (JCS PUB 6-03. 7)

Volatility

See data volatility.

Volume

A portion of data, together with its data carrier, that can be handled conveniently as a unit; for example, a reel of magnetic tape, a disk pack. (FP)

*-Voodoo Programming

n. [from George Bush's "voodoo economics"] The use by guess or cookbook of an obscure or hairy system, feature, or algorithm that one does not truly understand. The implication is that the technique may not work, and if it doesn't, one will never know why. Almost synonymous with black magic, except that black magic typically isn't documented and *nobody* understands it. Compare magic, deep magic, heavy wizardry, rain dance, cargo cult programming, wave a dead chicken.

*-VR

// [MUD] n. On-line abbrev for virtual reality, as opposed to RL.

*-Vulcan Nerve Pinch

n. [from the old "Star Trek" TV series via Commodore Amiga hackers] The keyboard combination that forces a soft-boot or jump to ROM monitor (on machines that support such a feature). On many micros this is Ctrl-Alt-Del; on Suns, L1-A; on some Macintoshes, it is <Cmd>-<Power switch>! Also called three-finger salute. Compare quadruple bucky.

Vulnerability

1. A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing. (*AFR* 700-10;; *AFR* 205-16;; *AR* 380-380;)
2. A weakness in system security procedures, hardware design, internal controls, etc. , which could be exploited to gain unauthorized access to classified or sensitive information. (*NCSC-WA*-001-85;)
3. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack. (*OPNAVINST* 5239. 1A;)
4. An assertion primarily concerning entities of the internal environment (assets); we say that an asset (or class of assets) is vulnerable (in some way, possibly involving an agent or collection of agents); we write: V(i,e) where: e may be an empty set. (ET;)
5. Susceptibility to various threats. (RM;)
6. A set of properties of a specific internal entity that, in union with a set of properties of a specific external entity, implies a risk. (MK;)
7. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02) (AF MAN 33-270)

Vulnerability Analysis

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Assessment

1. A review of the susceptibility to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and/or adverse or unfavorable public opinion. (A-123)
2. A measurement of vulnerability which would include: a. The susceptibility of a particular system to a specific attack. b. The opportunity available to a threat agent (methods or things which may be used to exploit a vulnerability(such as fire)) to mount that attack. A vulnerability is always demonstrable but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control. (*AR* 380-380)
3. A review of the susceptibility to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and adverse or unfavorable public opinion. Vulnerability assessments do not identify weaknesses or result in improvements. They are the mechanism with which an organization can determine quickly the potential for losses in its different programs or functions. The schedule of internal control reviews should be based on the results of the vulnerability assessments. (DODD 7040. 6)
4. The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation. (NCSC-9)
5. A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack. (*NCSC-TG*-004-88)

*-Vulture Capitalist

n. Pejorative hackerism for `venture capitalist', deriving from the common practice of pushing contracts that deprive inventors of control over their own innovations and most of the money they ought to have made from them.

W

*-Wabbit

/wab'it/ n. [almost certainly from Elmer Fudd's immortal line “You wascawwy wabbit!”]

1. A legendary early hack reported on a System/360 at RPI and elsewhere around 1978; this may have descended (if only by inspiration) from hack called RABBITS reported from 1969 on a Burroughs 55000 at the University of Washington Computer Center. The program would make two copies of itself every time it was run, eventually crashing the system.
2. By extension, any hack that includes infinite self-replication but is not a virus or worm. See fork bomb and rabbit job, see also cookie monster.

*-WAITS

/wayts/ n. The mutant cousin of TOPS-10 used on a handful of systems at SAIL up to 1990. There was never an `official' expansion of WAITS (the name itself having been arrived at by a rather sideways process), but it was frequently glossed as `West-coast Alternative to ITS'. Though WAITS was less visible than ITS, there was frequent exchange of people and ideas between the two communities, and innovations pioneered at WAITS exerted enormous indirect influence. The early screen modes of EMACS, for example, were directly inspired by WAITS's `E' editor -- one of a family of editors that were the first to do `real-time editing', in which the editing commands were invisible and where one typed text at the point of insertion/overwriting. The modern style of multi-region windowing is said to have originated there, and WAITS alumni at XEROX PARC and elsewhere played major roles in the developments that led to the XEROX Star, the Macintosh, and the Sun workstations. Also invented there were bucky bits -- thus, the ALT key on every IBM PC is a WAITS legacy. One notable WAITS feature seldom duplicated elsewhere was a news-wire interface that allowed WAITS hackers to read, store, and filter AP and UPI dispatches from their terminals; the system also featured a still-unusual level of support for what is now called `multimedia' computing, allowing analog audio and video signals to be switched to programming terminals.

Waiver

Permission to operate while not in compliance

*-Walk

n. ,vt. Traversal of a data structure, especially an array or linked-list data structure in core. See also code-walker, silly walk, clobber.

*-Walk Off The End Of

vt. To run past the end of an array, list, or medium after stepping through it -- a good way to land in trouble. Often the result of an off-by-one error. Compare clobber, roach, smash the stack.

*-Walking Drives

n. An occasional failure mode of magnetic-disk drives back in the days when they were huge, clunky washing machines. Those old dinosaur parts carried terrific angular momentum; the combination of a misaligned spindle or worn bearings and stick-slip interactions with the floor could cause them to `walk' across a room, lurching alternate corners forward a couple of millimeters at a time. There is a legend about a drive that walked over to the only door to the computer room and jammed it shut; the staff had to cut a hole in the wall in order to get at it! Walking could also be induced by certain patterns of drive access (a fast seek across the whole width of the disk, followed by a slow seek in the other direction). Some bands of old-time hackers figured out how to induce disk-accessing patterns that would do this to particular drive models and held disk-drive races.

*-Wall

1. interj. [WPI] An indication of confusion, usually spoken with a quizzical tone “Wall??”
2. A request for further explication. Compare octal forty.
3. . [UNIX, from `write all'] v. To send a message to everyone currently logged in, esp. with the wall (8) utility. It is said that sense 1 came from the idiom `like talking to a blank wall'. It was originally used in situations where, after you had carefully answered a question, the questioner stared at you blankly, clearly having understood nothing that was explained. You would then throw out a “Hello, wall?” to elicit some sort of response from the questioner. Later, confused questioners began voicing “Wall?” themselves.

*-Wall Follower

n. A person or algorithm that compensates for lack of sophistication or native stupidity by efficiently following some simple procedure shown to have been effective in the past. Used of an algorithm, this is not necessarily pejorative; it recalls `Harvey Wallbanger', the winning robot in an early AI contest (named, of course, after the cocktail). Harvey successfully solved mazes by keeping a `finger' on one wall and running till it came out the other end. This was inelegant, but it was mathematically guaranteed to work on simply-connected mazes --- and, in fact, Harvey outperformed more sophisticated robots that tried to `learn' each maze by building an internal representation of it.

Used of humans, the term *is* pejorative and implies an uncreative, bureaucratic, by-the-book mentality. See also code grinder; compare droid.

*-Wall Time

n. (also `wall clock time')

1. `Real world' time (what the clock on the wall shows), as opposed to the system clock's idea of time.
2. The real running time of a program, as opposed to the number of ticks required to execute it (on a timesharing system these always differ, as no one program gets all the ticks, and on multiprocessor systems with good thread support one may get more processor time than real time).

*-Wallpaper

1. n. A file containing a listing (e. g. , assembly listing) or a transcript, esp. a file containing a transcript of all or part of a login session. (The idea was that the paper for such listings was essentially good only for wallpaper, as evidenced at Stanford, where it was used to cover windows.) Now rare, esp. since other systems have developed other terms for it (e. g. , PHOTO on TWENEX). However, the UNIX world doesn't have an equivalent term, so perhaps wallpaper will take hold there. The term probably originated on ITS, where the commands to begin and end transcript files were `:WALBEG' and `:WALEND', with default file `WALL PAPER' (the space was a path delimiter).
2. The background pattern used on graphical workstations (this is techspeak under the `Windows' graphical user interface to MS-DOS).
3. `wallpaper file' n. The file that contains the wallpaper information before it is actually printed on paper. (Even if you don't intend ever to produce a real paper copy of the file, it is still called a wallpaper file.)

WAN

See wide area network.

*-Wango

/wang'goh/ n. Random bit-level grovelling going on in a system during some unspecified operation. Often used in combination with mumble. For example “You start with the `. o' file, run it through this postprocessor that does mumble-wango -- and it comes out a snazzy object-oriented executable. ”

*-Wannabee

/won'*-bee/ n, (also, more plausibly, spelled `wannabe') [from a term recently used to describe Madonna fans who dress, talk, and act like their idol; prob. originally from biker slang] A would-be hacker. The connotations of this term differ sharply depending on the age and exposure of the subject. Used of a person who is in or might be entering larval stage, it is semi-approving; such wannabees can be annoying but most hackers remember that they, too, were once such creatures. When used of any professional programmer, CS academic, writer, or suit, it is derogatory, implying that said person is trying to cuddle up to the hacker mystique but doesn't, fundamentally, have a prayer of understanding what it is all about. Overuse of terms from this lexicon is often an indication of the wannabee nature. Compare newbie. Historical note The wannabee phenomenon has a slightly different flavor now (1993) than it did ten or fifteen years ago. When the people who are now hackerdom's tribal elders were in larval stage, the process of becoming a hacker was largely unconscious and unaffected by models known in popular culture -- communities formed spontaneously around people who, *as individuals*, felt irresistibly drawn to do hackerly things, and what wannabees experienced was a fairly pure, skill-focused desire to become similarly wizardly. Those days of innocence are gone forever; society's adaptation to the advent of the microcomputer after 1980 included the elevation of the hacker as a new kind of folk hero, and the result is that some people semi-consciously set out to *be hackers* and borrow hackish prestige by fitting the popular image of hackers. Fortunately, to do this really well, one has to actually become a wizard. Nevertheless, old-time hackers tend to share a poorly articulated disquiet about the change; among other things, it gives them mixed feelings about the effects of public compendia of lore like this one.

*-War Dialer

A cracking tool, a program that calls a given list or range of numbers and records those which answer with handshake tones (and so might be entry points to computer or telecommunications systems). Some of these programs have becomequite sophisticated, and can now detect modem, fax or pbx tones and log each one separately. The war dialer is one of the most important tools in the phreaker's kit. These programs evolved from early demon dialers.

-Ware*

suff. [from `software'] Commonly used to form jargon terms for classes of software. For examples, see careware, crippleware, crudware, freeware, fritterware, guiltware, liveware, meatware, payware, psychedelicware, shareware, shelfware, vaporware, wetware.

*-Warez

/weirz/ n. Widely used in cracker subcultures to denote cracked version of commercial software, that is versions from which copy-protection has been stripped. Hackers recognize this term but don't use it themselves. See warez d00dz.

*-Warlording

v. [from the Usenet group alt. fan. warlord] The act of excoriating a bloated, ugly, or derivative sig block. Common grounds for warlording include the presence of a signature rendered in a BUAF, over-used or cliched sig quotes, ugly ASCII art, or simply excessive size. The original `Warlord' was a B1FF-like newbie c. 1991 who featured in his sig a particularly large and obnoxious ASCII graphic resembling the sword of Conan the Barbarian in the 1981 John Milius movie; the group name alt. fan. warlord was sarcasm, and the characteristic mode of warlording is devastatingly sarcastic praise.

*-Warm Boot

n. See boot.

#-Warranties

Are promises that a proposition of fact is true. They are an assurance by one party to an agreement of the existence of fact upon which the other party may rely. It is intended to relieve the promises of any duty to ascertain fact for himself, and amounts to a promise to indemnify the promisee for any loss if the fact warranted proves untrue. (Source - Blacks).

*-Wart

n. A small, crocky feature that sticks out of an otherwise clean design. Something conspicuous for localized ugliness, especially a special-case exception to a general rule. For example, in some versions of `csh(1)', single quotes literalize every character inside them except `!'. In ANSI C, the `??' syntax used for obtaining ASCII characters in a foreign environment is a wart. See also miswart.

*-Wash Software

v. The process of recompiling a software collection (used more often when the recompilation is occuring from scratch) to pick up and merge together all of the various changesthat have been made to the source.

*-Washing Machine

1. n. Old-style 14-inch hard disks in floor-standing cabinets. So called because of the size of the cabinet and the `top-loading' access to the media packs -- and, of course, they were always set on `spin cycle'. The washing-machine idiom transcends language barriers; it is even used in Russian hacker jargon. See also walking drives. The thick channel cables connecting these were called `bit hoses' (see hose, sense 3).
2. [CMU] A machine used exclusively to wash software. CMU has clusters of these.

*-Water MIPS

n. (see MIPS, sense 2) Large, water-cooled machines of either today's ECL-supercomputer flavor or yesterday's traditional mainframe type.

*-Wave A Dead Chicken

v. To perform a ritual in the direction of crashed software or hardware that one believes to be futile but is nevertheless necessary so that others are satisfied that an appropriate degree of effort has been expended. “I'll wave a dead chicken over the source code, but I really think we've run into an OS bug. ” Compare voodoo programming, rain dance.

Weapon Data

Restricted data or formerly restricted data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices. (DOE 5635. 1 A)

*-Weasel

n. [Cambridge] A naive user, one who deliberately or accidentally does things that are stupid or ill-advised. Roughly synonymous with loser.

*-Wedged

1. adj. To be stuck, incapable of proceeding without help. This is different from having crashed. If the system has crashed, it has become totally nonfunctioning. If the system is wedged, it is trying to do something but cannot make progress; it may be capable of doing a few things, but not be fully operational. For example, a process may become wedged if it deadlocks with another (but not all instances of wedging are deadlocks). See also gronk, locked up, hosed.
2. Often refers to humans suffering misconceptions. “He's totally wedged -- he's convinced that he can levitate through meditation. ”
3. [UNIX] Specifically used to describe the state of a TTY left in a losing state by abort of a screen-oriented program or one that has messed with the line discipline in some obscure way. There is some dispute over the origin of this term. It is usually thought to derive from a common description of recto-cranial inversion; however, it may actually have originated with older `hot-press' printing technology in which physical type elements were locked into type frames with wedges driven in by mallets. Once this had been done, no changes in the typesetting for that page could be made.

*-Wedgie

n. [Fairchild] A bug. Prob. related to wedged.

*-Wedgitude

/wedj'i-t[y]ood/ n. The quality or state of being wedged.

*-Weeble

/weeb'l/ interj. [Cambridge] Used to denote frustration, usually at amazing stupidity. “I stuck the disk in upside down. ” “Weeble. ” Compare gurfle.

*-Weeds

1. n. Refers to development projects or algorithms that have no possible relevance or practical application. Comes from `off in the weeds'. Used in phrases like “lexical analysis for microcode is serious weeds. ”
2. At CDC/ETA before its demise, the phrase `go off in the weeds' was equivalent to IBM's branch to Fishkill and mainstream hackerdom's jump off into never-never land.

*-Weenie

1. n. [on BBSes] Any of a species of luser resembling a less amusing version of B1FF that infests many BBS systems. The typical weenie is a teenage boy with poor social skills travelling under a grandiose handle derived from fantasy or heavy-metal rock lyrics. Among sysops, `the weenie problem' refers to the marginally literate and profanity-laden flamage weenies tend to spew all over a newly-discovered BBS. Compare spod, computer geek, terminal junkie.
2. [Among hackers] When used with a qualifier (for example, as in UNIX weenie, VMS weenie, IBM weenie) this can be either an insult or a term of praise, depending on context, tone of voice, and whether or not it is applied by a person who considers him or herself to be the same sort of weenie. Implies that the weenie has put a major investment of time, effort, and concentration into the area indicated; whether this is good or bad depends on the hearer's judgment of how the speaker feels about that area. See also bigot.
3. The semicolon character, `;' (ASCII 0111011).

*-Weenix

/wee'niks/ n. [ITS] A derogatory term for UNIX, derived from UNIX weenie. According to one noted ex-ITSer, it is “the operating system preferred by Unix Weenies: typified by poor modularity, poor reliability, hard file deletion, no file version numbers, case sensitivity everywhere, and users who believe that these are all advantages”. Some ITS fans behave as though they believe UNIX stole a future that rightfully belonged to them. See ITS, sense 2.

*-Well-Behaved

1. adj. [primarily MS-DOS] Said of software conforming to system interface guidelines and standards. Well-behaved software uses the operating system to do chores such as keyboard input, allocating memory and drawing graphics. Oppose ill-behaved.
2. Software that does its job quietly and without counterintuitive effects. Esp. said of software having an interface spec sufficiently simple and well-defined that it can be used as a tool by other software. See cat.

*-Well-Connected

adj. Said of a computer installation, asserts that it has reliable email links with the network and/or that it relays a large fraction of available Usenet newsgroups. `Well-known' can be almost synonymous, but also implies that the site's name is familiar to many (due perhaps to an archive service or active Usenet users).

Wet Line

An interface line of the equipment under test, where the signal normally transmitted over the line is present.

*-Wetware

/wet'weir/ n. [prob. from the novels of Rudy Rucker]

1. The human nervous system, as opposed to computer hardware or software. “Wetware has 7 plus or minus 2 temporary registers. ”
2. Human beings (programmers, operators, administrators) attached to a computer system, as opposed to the system's hardware or software. See liveware, meatware.

*-Whack

v. According to arch-hacker James Gosling, to “. modify a program with no idea whatsoever how it works. ” (See whacker.) It is actually possible to do this in nontrivial circumstances if the change is small and well-defined and you are very good at glarking things from context. As a trivial example, it is relatively easy to change all `stderr' writes to `stdout' writes in a piece of C filter code which remains otherwise mysterious.

*-Whacker

1. n. [University of Maryland from hacker] A person, similar to a hacker, who enjoys exploring the details of programmable systems and how to stretch their capabilities. Whereas a hacker tends to produce great hacks, a whacker only ends up whacking the system or program in question. Whackers are often quite egotistical and eager to claim wizard status, regardless of the views of their peers.
2. A person who is good at programming quickly, though rather poorly and ineptly.

*-Whales

n. See like kicking dead whales down the beach.

*-Whalesong

n. The peculiar clicking and whooshing sounds made by a PEP modem such as the Telebit Trailblazer as it tries to synchronize with another PEP modem for their special high-speed mode. This sound isn't anything like the normal two-tone handshake between

conventional modems and is instantly recognizable to anyone who has heard it more than once. It sounds, in fact, very much like whale songs. This noise is also called “the moose call” or “moose tones”.

*-What's A Spline?

[XEROX PARC] This phrase expands to “You have just used a term that I've heard for a year and a half, and I feel I should know, but don't. My curiosity has finally overcome my guilt. ” The PARC lexicon adds “Moral don't hesitate to ask questions, even if they seem obvious. ”

*-Wheel

n. [from slang `big wheel' for a powerful person] A person who has an active wheel bit. “We need to find a wheel to unwedge the hung tape drives. ” (See wedged, sense 1. ) The traditional name of security group zero in BSD (to which the major system-internal users like root belong) is `wheel'. Some vendors have expanded on this usage, modifying UNIX so that only members of group `wheel' can go root

*-Wheel Bit

n. A privilege bit that allows the possessor to perform some restricted operation on a timesharing system, such as read or write any file on the system regardless of protections, change or look at any address in the running monitor, crash or reload the system, and kill or create jobs and user accounts. The term was invented on the TENEX operating system, and carried over to TOPS-20, XEROX-IFS, and others. The state of being in a privileged logon is sometimes called `wheel mode'. This term entered the UNIX culture from TWENEX in the mid-1980s and has been gaining popularity there (esp. at university sites). See also root.

*-Wheel Wars

n. [Stanford University] A period in larval stage during which student hackers hassle each other by attempting to log each other out of the system, delete each other's files, and otherwise wreak havoc, usually at the expense of the lesser users.

*-White Book

1. n. Syn. K&R.
2. Adobe's fourth book in the PostScript series, describing the previously-secret format of Type 1 fonts; “Adobe Type 1 Font Format, version 1. 1”, (Addison-Wesley, 1990, ISBN 0-201-57044-0). See also Red Book, Green Book, Blue Book.

White Noise

Noise whose frequency spectrum is continuous and uniform over a wide frequency range. (~) Note: White noise has equal power per hertz over the frequency band of interest. See also frequency, in-band noise power ratio, pink noise, pseudorandom noise.

*-WIBNI

// n. [Wouldn't It Be Nice If] What most requirements documents and specifications consist entirely of. Compare IWBNI.

Wide Area Network

(WAN) A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

Note 1: A user may describe a collection of physical networks, e. g. , ISDN, X. 25, T1, as the user's logical WAN environment.

Note 2: A MAN is a special case of a WAN in which the area covered is a metropolitan area. WANs may be country-wide or world-wide. See also local access and transport area, local area network, metropolitan area network, network.

#-Wide Area Network Security

This KSA has no definition.

#-Wide Area Networks

1. A comprehensive multimode network connecting large numbers of computer and terminals spread over a large geographical area. (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992)
2. (a) A network which ranges from a few kilometers to thousands of kilometers and handles transmission speeds from a few kilobits/second to megabits/second. ref: 2. (b) A computer network that uses high-speed, long distance communications networks or satellites to connect computers over distances greater than (one or two miles) traversed by local area networks. (*QCUS+Pf-90*)

Wide Area Telephone Service

(WATS) A toll service offering for customer dial-type telecommunications between a given customer [user] station and stations within specified geographic rate areas employing a single access line between the customer [user] location and the serving central office. Each access line may be arranged for either outward (OUT-WATS) or inward (IN-WATS) service, or both. (CFR 47) Note: The offering is for fixed-rate inter- and intra-LATA services measured by zones and hours. See also local access and transport area.

*-Widget n.

1. A meta-thing. Used to stand for a real object in didactic examples (especially database tutorials). Legend has it that the original widgets were hold-

ers for buggy whips. “But suppose the parts list for a widget has 52 entries. ”

2. [poss. evoking `window gadget'] A user interface object in X graphical user interfaces.

***-Wiggles n.**

[scientific computation] In solving partial differential equations by finite difference and similar methods, wiggles are sawtooth (up-down-up-down) oscillations at the shortest wavelength representable on the grid. If an algorithm is unstable, this is often the most unstable waveform, so it grows to dominate the solution. Alternatively, stable (though inaccurate) wiggles can be generated near a discontinuity by a Gibbs phenomenon.

***-WIMP Environment n. [acronym `**

Window, Icon, Menu, Pointing device (or Pull-down menu)'] A graphical-user-interface environment such as X or the Macintosh interface, esp. as described by a hacker who prefers command-line interfaces for their superior flexibility and extensibility. However, it is also used without negative connotations; one must pay attention to voice tone and other signals to interpret correctly. See menuitis, user-obsequious.

***-Win**

1. vi. To succeed. A program wins if no unexpected conditions arise, or (especially) if it sufficiently robust to take exceptions in stride.
2. n. Success, or a specific instance thereof. A pleasing outcome. “So it turned out I could use a lexer generator instead of hand-coding my own pattern recognizer. What a win!” Emphatic forms `moby win', `super win', `hyper-win' (often used interjectively as a reply). For some reason `suitable win' is also common at MIT, usually in reference to a satisfactory solution to a problem. Oppose lose; see also big win, which isn't quite just an intensification of `win'.

***-Win Big vi.**

To experience serendipity. “I went shopping and won big; there was a 2-for-1 sale. ” See big win.

***-Win Win**

excl. Expresses pleasure at a win.

***-Winchester: n.**

Informal generic term for sealed-enclosure magnetic-disk drives in which the read-write head planes over the disk surface on an air cushion. There is a legend that name arose because the original 1973 engineering prototype for what later became the IBM 3340 featured two 30-megabyte volumes; 30--30 became `Winchester' when somebody noticed the similarity to the common term for a famous Winchester rifle (in the latter, the first 30 referred to caliber and the second to the grain weight of the charge). Others claim, however, that Winchester was simply the laboratory in which the technology was developed.

Window

1. A band of wavelengths at which an optical fiber is sufficiently transparent for practical use in communications applications. See also spectral window.
2. A portion of a display surface in which display images pertaining to a particular application can be presented. Note: Different applications can be displayed simultaneously in different windows. (FP)

***-Window Shopping n.**

[US Geological Survey] Among users of WIMP environments like X or the Macintosh, extended experimentation with new window colors, fonts, and icon shapes. This activity can take up hours of what might otherwise have been productive working time. “I spent the afternoon window shopping until I found the coolest shade of green for my active window borders -- now they perfectly match my medium slate blue background. ” Serious window shoppers will spend their days with bitmap editors, creating new and different icons and background patterns for all to see. Also `window dressing', the act of applying new fonts, colors, etc. See fritterware, compare macdink.

***-Window SysIWYG n.**

A bit was named aften /bee't*/ prefer to use the other guy's re, especially in every cast a chuckle on neithout getting into useful informash speech makes removing a featuring a move or usage actual abstractionsidered interj. Indeed spectace logic or problem! A hackish idle pastime is to apply letter-based Dissociated Press to a random body of text and vgrep the output in hopes of finding an interesting new word. (In the preceding example, `window sysIWYG' and `informash' show some promise.) Iterated applications of Dissociated Press usually yield better results. Similar techniques called `travesty generators' have been employed with considerable satirical effect to the utterances of Usenet flamers; see pseudo.

***-Windoze /win'dohz/ n.**

See Microsloth Windows.

***-Winged Comments n.**

Comments set on the same line as code, as opposed to boxed comments. In C, for example d = sqrt(x*x + y*y); /* distance from origin */ Generally these refer only to the action(s) taken on that line.

***-Winkey n.**

(alt. `winkey face') See emoticon.

***-Winner**

1. n. An unexpectedly good situation, program, programmer, or person.
2. `real winner'Often sarcastic, but also used as high praise (see also the note under user). “He's a real

winner -- never reports a bug till he can duplicate it and send in an example. ”

2. The quality of winning (as opposed to winnage, which is the result of winning). “Guess what? They tweaked the microcode and now the LISP interpreter runs twice as fast as it used to. ” “That's really great! Boy, what winnitude!” “Yup. I'll probably get a half-hour's winnage on the next run of my program. ” Perhaps curiously, the obvious antonym `lossitude' is rare.

***-Wired**

n. See hardwired.

***-Wirehead /wi:r'hed/ n.**

[prob. from SF slang for an electrical-brain-stimulation addict]

1. A hardware hacker, especially one who concentrates on communications hardware.
2. An expert in local-area networks. A wirehead can be a network software wizard too, but will always have the ability to deal with network hardware, down to the smallest component. Wireheads are known for their ability to lash up an Ethernet terminator from spare resistors, for example.

Wiretapping

1. Cutting in on a communications line to get information. a. Active. The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users. b. Passive. The monitoring and/or recording of data which is being transmitted over a communication link. (*AR* 380-380)
2. See ACTIVE WIRETAPPING and PASSIVE WIRETAPPING.

***-Wirewater n.**

Syn. programming fluid. This melds the mainstream slang adjective `wired' (stimulated, up, hyperactive) with `firewater'; however, it refers to caffeinacious rather than alcoholic beverages.

***-Wish List n.**

A list of desired features or bug fixes that probably won't get done for a long time, usually because the person responsible for the code is too busy or can't think of a clean way to do it. “OK, I'll add automatic filename completion to the wish list for the new interface. ” Compare tick-list features.

***-Within Delta Of**

adj. See delta.

***-Within Epsilon Of**

adj. See epsilon.

#-Witness Interviewing/Interrogation

In criminal law, is the process of questions propounded by police to a person arrested or suspected to seek solution of a crime. Such person is entitled to be advised of his Miranda Rights. (Source Blacks).

***-Wizard n.**

1. A person who knows how a complex piece of software or hardware works (that is, who groks it); esp. someone who can find and fix bugs quickly in an emergency. Someone is a hacker if he or she has general hacking ability, but is a wizard with respect to something only if he or she has specific detailed knowledge of that thing. A good hacker could become a wizard for something given the time to study it.
2. A person who is permitted to do things forbidden to ordinary people; one who has wheel privileges on a system.
3. . A UNIX expert, esp. a UNIX systems programmer. This usage is well enough established that `UNIX Wizard' is a recognized job title at some corporations and to most headhunters. See guru, lord high fixer. See also deep magic, heavy wizardry, incantation, magic, mutter, rain dance, voodoo programming, wave a dead chicken.

***-Wizard Book n.**

“Structure and Interpretation of Computer Programs” (Hal Abelson, Jerry Sussman and Julie Sussman; MIT Press, 1984; ISBN 0-262-01077-1), an excellent computer science text used in introductory courses at MIT. So called because of the wizard on the jacket. One of the bibles of the LISP/Scheme world. Also, less commonly, known as the Purple Book.

***-Wizard Mode n.**

[from rogue] A special access mode of a program or system, usually passworded, that permits some users godlike privileges. Generally not used for operating systems themselves (`root mode' or `wheel mode' would be used instead). This term is often used with respect to games that have editable state.

***-Wizardly adj.**

Pertaining to wizards. A wizardly feature is one that only a wizard could understand or use properly.

WNINTEL

See Warning Notice”Intelligence Sources or Methods Involved

***-Wok-On-The-Wall n.**

A small microwave dish antenna used for cross-campus private network circuits, from the obvious resemblance between a microwave dish and the Chinese culinary utensil.

Word

A character string or a bit string considered to be an entity for some purpose. (FP) (ISO) (~) Note: In telegraph communications, six character intervals are defined as a word when computing traffic capacity in words per minute, which is computed by multiplying the data signaling rate in baud by 10 and dividing the resulting product by the number of unit intervals per character. See also baud, binary digit, bit string, block, byte, character, code word, computer word.

Word Length

The number of characters or bits in a word. (FP) See also binary digit, character.

Word Processing

The use of a system to manipulate text by performing functions such as entering, editing, rearranging, sorting, storing, retrieving, displaying, and printing. See text processing.

Work Factor

1. An estimate of the effort or time needed to overcome a protective measure by a potential penetrator with specified expertise and resources. (*AR* 380-380)
2. An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and resources. (*FIPS PUB* 39)
3. An estimate of the effort or time needed by a potential penetrator with specified expertise and resources to overcome a protective measure. (*NCSC-TG*-004-88)

Work Space

That portion of main storage that is used by a computer program for temporary storage of data. (FP) (ISO)

Work Station

1. For automated systems, a configuration of input, output, display and processing equipment that provides an operator interface to a system, such as a central computer, communication, or control system.
2. A configuration of input, output, display, and processing equipment that constitutes a stand-alone system not requiring external access.

*-Workaround n.

1. A temporary kluge used to bypass, mask, or otherwise avoid a bug or misfeature in some system. Theoretically, workarounds are always replaced by fixes; in practice, customers often find themselves living with workarounds for long periods of time. “The code died on NUL characters in the input, so I fixed it to interpret them as spaces. ” “That's not a fix, that's a workaround!”
2. A procedure to be employed by the user in order to do what some currently non-working feature should do. Hypothetical example: “Using META-F7 crashes the 4. 43 build of Weemax, but as a workaround you can type CTRL-R, then SHIFT-F5, and delete the remaining cruft by hand. ”

*-Working As Designed

1. adj. [IBM] In conformance to a wrong or inappropriate specification; useful, but misdesigned.
2. requently used as a sardonic comment on a program's utility.
3. Unfortunately also used as a bogus reason for not accepting a criticism or suggestion. At IBM, this sense is used in official documents! See BAD.

#-Workstations Security

Provision of access and integrity controls for an intelligent terminal designed for specific tasks, eg, word processing, computer aided design, etc. (Source -: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992).

World

A collection of conceptual entities which, if taken with a set of descriptors, constitutes a universe of discourse. (MA;)

Worm

1. A program or executable code module which resides in distributed systems or networks. It will replicate itself, if necessary, in order to exercise as much of the system's resources as possible for its own processing. Such resources may take the form of CPU time, I/O channels, or system memory. (*NCSC-WA*-001-85;)
2. A worm is a program that can run on its own and can propagate itself to other machines on a network. A worm can be a useful tool for distributing information such as mail, or it can be used to spread a time bomb or trojan horse - if it can gain access to the host. (IC;)

*-Wormhole

/werm'hohl/ n. [from the `wormhole' singularities hypothesized in some versions of General Relativity theory]

1. obs. A location in a monitor which contains the address of a routine, with the specific intent of making it easy to substitute a different routine. This term is now obsolescent; modern operating systems use clusters of wormholes extensively (for modularization of I/O handling in particular, as in the UNIX device-driver organization) but the preferred techspeak for these clusters is `device tables', `jump tables' or `capability tables'.
2. [Amateur Packet Radio] A network path using a commercial satellite link to join two or more amateur VHF networks. So called because traffic routed through a wormhole leaves and re-enters

the amateur network over great distances with usually little clue in the message routing header as to how it got from one relay to the other. Compare gopher hole (sense2. .

*-Wound Around The Axle

adj. In an infinite loop. Often used by older computer types.

*-Wrap Around

vi. (also n. `wraparound' and v. shorthand `wrap')

1. [techspeak] The action of a counter that starts over at zero or at `minus infinity' (see infinity) after its maximum value has been reached, and continues incrementing, either because it is programmed to do so or because of an overflow (as when a car's odometer starts over at 0).
2. To change phase gradually and continuously by maintaining a steady wake-sleep cycle somewhat longer than 24 hours, e. g. , living six long (28-hour) days in a week (or, equivalently, sleeping at the rate of 10 microhertz). This sense is also called phase-wrapping.

Write

1. A fundamental operation that results only in the flow of information from a subject to an object. (CSC-STD-001-83;; *NCSC-WA*-001-85;)
2. To make a permanent or transient recording of data in a storage device or on a data medium. (FP)

Write Access

Permission to write an object. (CSC-STD-001-83;; *NCSC-WA*-001-85;) See Read Access.

Write Cycle Time

The minimum time interval between the starts of successive write cycles of a storage device that has separate reading and writing cycles. (FP) (ISO)

Write Down

Ability of a subject to write data to an object that is classified at a lower level than the subject's security level. This is normally not allowed. See Read Down, Read Up, and Write Up.

Write Head

A magnetic head capable of writing only. (FP) (ISO)

Write Protection Label

A removable label, the presence or absence of which on a diskette prevents writing on the diskette. (FP) (ISO) See write-protect tab.

Write Up

Ability of a subject to write data to an object that is classified at a higher level than the subject's security level. Permission is provided through the security functions of a system and administered by the system manager. See Read Down, Read Up, and Write Down.

*-Write-Only Code

n. [a play on `read-only memory'] Code so arcane, complex, or ill-structured that it cannot be modified or even comprehended by anyone but its author, and possibly not even by him/her. A Bad Thing.

*-Write-Only Language

n. A language with syntax (or semantics) sufficiently dense and bizarre that any routine of significant size is automatically write-only code. A sobriquet applied occasionally to C and often to APL, though INTERCAL and TECO certainly deserve it more.

*-Write-Only Memory

n. The obvious antonym to `read-only memory'. Out of frustration with the long and seemingly useless chain of approvals required of component specifications, during which no actual checking seemed to occur, an engineer at Signetics once created a specification for a write-only memory and included it with a bunch of other specifications to be approved. This inclusion came to the attention of Signetics management only when regular customers started calling and asking for pricing information. Signetics published a corrected edition of the data book and requested the return of the `erroneous' ones. Later, around 1974, Signetics bought a double-page spread in “Electronics” magazine's April issue and used the spec as an April Fools' Day joke. Instead of the more conventional characteristic curves, the 25120 “fully encoded, 9046 x N, Random Access, write-only-memory” data sheet included diagrams of “bit capacity vs. Temp. ”, “Iff vs. Vff”, “Number of pins remaining vs. number of socket insertions”, and “AQL vs. selling price”. The 25120 required a 6. 3 VAC VFF supply, a +10V VCC, and VDD of 0V, +/- 2%.

Write-Protect Tab

See write protection label.

*-Wrong Thing

n. A design, action, or decision that is clearly incorrect or inappropriate. Often capitalized; always emphasized in speech as if capitalized. The opposite of the Right Thing; more generally, anything that is not the Right Thing. In cases where `the good is the enemy of the best', the merely good -- although good -- is nevertheless the Wrong Thing. “In C, the default is for module-level declarations to be visible everywhere, rather than just within the module. This is clearly the Wrong Thing. ”

*-Wugga Wugga

/wuh'g* wuh'g*/ n. Imaginary sound that a computer program makes as it labors with a tedious or difficult task. Compare cruncha cruncha cruncha, grind (sense 4).

*-Wumpus

/wuhm'p*s/ n. The central monster (and, in many versions, the name) of a famous family of very early computer games called “Hunt The Wumpus”, dating back at least to 1972 (several years before ADVENT) on the Dartmouth Time-Sharing System. The wumpus lived somewhere in a cave with the topology of an dodecahedron's edge/vertex graph (later versions supported other topologies, including an icosahedron and M”obius strip). The player started somewhere at random in the cave with five `crooked arrows'; these could be shot through up to three connected rooms, and would kill the wumpus on a hit (later versions introduced the wounded wumpus, which got very angry). Unfortunately for players, the movement necessary to map the maze was made hazardous not merely by the wumpus (which would eat you if you stepped on him) but also by bottomless pits and colonies of super bats that would pick you up and drop you at a random location (later versions added `anaerobic termites' that ate arrows, bat migrations, and earthquakes that randomly changed pit locations). This game appears to have been the first to use a non-random graph-structured map (as opposed to a rectangular grid like the even older Star Trek games). In this respect, as in the dungeon-like setting and its terse, amusing messages, it prefigured ADVENT and Zork and was directly ancestral to the latter (Zork acknowledged this heritage by including a super-bat colony). Today, a port is distributed with SunOS and as freeware for the Mac. A C emulation of the original Basic game is in circulation as freeware on the net.

WWMCCS

See Worldwide Military Command and Control System.

*-WYSIAYG

/wiz'ee-ayg/ adj. Describes a user interface under which “What You See Is *All* You Get”; an unhappy variant of WYSIWYG. Visual, `point-and-shoot'-style interfaces tend to have easy initial learning curves, but also to lack depth; they often frustrate advanced users who would be better served by a command-style interface. When this happens, the frustrated user has a WYSIAYG problem. This term is most often used of editors, word processors, and document formatting programs. WYSIWYG `desktop publishing' programs, for example, are a clear win for creating small documents with lots of fonts and graphics in them, especially things like newsletters and presentation slides. When typesetting book-length manuscripts, on the other hand, scale changes the nature of the task; one quickly runs into WYSIAYG limitations, and the increased power and flexibility of a command-driven formatter like TeX or UNIX's troff becomes not just desirable but a necessity. Compare YAFIYGI.

*-WYSIWYG

/wiz'ee-wig/ adj. Describes a user interface under which “What You See Is What You Get”, as opposed to one that uses more-or-less obscure commands that do not result in immediate visual feedback. True WYSIWYG in environments supporting multiple fonts or graphics is a a rarely-attained ideal; there are variants of this term to express real-world manifestations including WYSIAWYG (What You See Is *Almost* What You Get) and WYSIMOLWYG (What You See Is More or Less What You Get). All these can be mildly derogatory, as they are often used to refer to dumbed-down user-friendly interfaces targeted at non-programmers; a hacker has no fear of obscure commands (compare WYSIAYG). On the other hand, EMACS was one of the very first WYSIWYG editors, replacing (actually, at first overlaying) the extremely obscure, command-based TECO. See also WIMP environment. [Oddly enough, WYSIWYG has already made it into the OED, in lower case yet. -- ESR]

X

*-X

1. /X/ n. Used in various speech and writing contexts (also in lowercase) in roughly its algebraic sense of `unknown within a set defined by context' (compare N). Thus, the abbreviation 680x0 stands for 68000, 68010, 68020, 68030, or 68040, and 80x86 stands for 80186, 80286 80386 or 80486 (note that a UNIX hacker might write these as 680[0-4]0 and 80[1-4]86 or 680?0 and 80?86 respectively; see glob).
2. [after the name of an earlier window system called `W'] An over-sized, over-featured, over-engineered and incredibly over-complicated window system developed at MIT and widely used on UNIX systems.

X-Dimension Of Recorded Spot

In facsimile, the center-to-center distance between two recorded spots measured in the direction of the recorded line. (~) Note: This term applies to facsimile equipment that responds to a constant density in the subject copy by yielding a succession of discrete recorded spots. See also facsimile, maximum keying frequency, recording.

X-Dimension Of Scanning Spot

In facsimile, the center-to-center distance between two scanning spots measured in the direction of the scanning line on the subject copy. (~) Note: The numerical value of this term will depend upon the type of system used. See also facsimile, scanning.

XDM

See Exploratory Development Model

XDM/X Model

See eXperimental Development Model eXploratory development Model.

Xerographic Recording

Recording by action of a light spot on an electrically charged photoconductive insulating surface where the latent image is developed with a resinous powder. See also recording.

*-XEROX PARC

/zee'roks park'/ n. The famed Palo Alto Research Center. For more than a decade, from the early 1970s into the mid-1980s, PARC yielded an astonishing volume of groundbreaking hardware and software innovations. The modern mice, windows, and icons style of software interface was invented there. So was the laser printer and the local-area network; and PARC's series of D machines anticipated the powerful personal computers of the 1980s by a decade. Sadly, the prophets at PARC were without honor in their own company, so much so that it became a standard joke to describe PARC as a place that specialized in developing brilliant ideas for everyone else. The stunning shortsightedness and obtusity of XEROX's top-level suits has been well anatomized in “Fumbling The Future: How XEROX Invented, Then Ignored, the First Personal Computer” by Douglas K. Smith and Robert C. Alexander (William Morrow & Co. , 1988, ISBN 0-688-09511-9).

*-XOFF

/X-of/ n. Syn. control-S.

*-XON

/X-on/ n. Syn. control-Q.

*-Xor

/X'or/, /kzor/ conj. Exclusive or. `A xor B' means `A or B, but not both'. “I want to get cherry pie xor a banana split. ” This derives from the technical use of the term as a function on truth-values that is true if exactly one of its two arguments is true.

*-Xref

/X'ref/ vt. ,n. Hackish standard abbreviation for `cross-reference'.

*-XXX

/X-X-X/ n. A marker that attention is needed. Commonly used in program comments to indicate areas that are kluged up or need to be. Some hackers liken `XXX' to the notional heavy-porn movie rating. Compare FIXME.

*-Xyzzy

/X-Y-Z-Z-Y/, /X-Y-ziz'ee/, /ziz'ee/, or /ik-ziz'ee/ adj. [from the ADVENT game] The canonical `magic word'. This comes from ADVENT, in which the idea is to explore an underground cave with many rooms and to collect the treasures you find there. If you type `xyzzy' at the appropriate time, you can move instantly between two otherwise distant points. If, therefore, you encounter some bit of magic, you might remark on this quite succinctly by saying simply “Xyzzy!” “Ordinarily you can't look at someone else's screen if he has protected it, but if you type quadruple-bucky-clear the system will let you do it anyway. ” “Xyzzy!” Xyzzy has actually been implemented as an undocumented no-op command on several OSes; in Data General's AOS/VS, for example, it would typically respond “Nothing happens”, just as ADVENT did if the magic was invoked at the wrong spot or before a player had performed the action that enabled the word. In more recent 32-bit versions, by the way, AOS/VS responds “Twice as much happens”. The popular `minesweeper' game under Microsoft Windows has a cheat mode triggered by the command `xyzzy<enter><right-shift>' that turns the top-left pixel of the screen different colors depending on whether or not the cursor is over a bomb.

Y

*-Y

A-abbrev. [Yet Another] In hackish acronyms this almost invariably expands to Yet Another, following the precedent set by UNIX `yacc(1)' (Yet Another Compiler-Compiler). See YABA.

Y-Dimension Of Recorded Spot

In facsimile, the center-to-center distance between two recorded spots measured perpendicular to the recorded line. (~) See also facsimile, recording, scanning.

Y-Dimension Of Scanning Spot

In facsimile, the center-to-center distance between two scanning spots measured perpendicular to the scanning line on the subject copy. (~) Note: The numerical value of this term will depend upon the type of system used. See also facsimile, scanning.

*-YABA

/ya'b*/ n. [Cambridge] Yet Another Bloody Acronym. Whenever some program is being named, someone invariably suggests that it be given a name that is acronymic. The response from those with a trace of originality is to remark ironically that the proposed name would then be `YABA-compatible'. Also used in response to questions like “What is WYSIWYG?” See also TLA.

*-YAFIYGI

/yaf'ee-y*-gee/ adj. [coined in response to WYSIWYG] Describes the command-oriented ed/vi/nroff/TeX style of word processing or other user interface, the opposite of WYSIWYG. Stands for “You asked for it, you got it”, because what you actu-

ally asked for is often not apparent until long after it is too late to do anything about it. Used to denote perversity (“Real Programmers use YAFIYGI tools. and *like* it!”) or, less often, a necessary tradeoff (“Only a YAFIYGI tool can have full programmable flexibility in its interface. ”). This precise sense of “You asked for it, you got it” seems to have first appeared in Ed Post's classic parody “Real Programmers don't use Pascal”; the acronym is a more recent (as of 1993) invention.

*-YAUN

/yawn/ n. [Acronym for `Yet Another UNIX Nerd'] Reported from the San Diego Computer Society (predominantly a microcomputer users' group) as a good-natured punning insult aimed at UNIX zealots.

*-Yellow Book

n. [proposed] The print version of this Jargon File; “The New Hacker's Dictionary”, MIT Press, 1991 (ISBN 0-262-68069-6). Includes all the material in the 2. 9. 6 version of the File, plus a Foreword by Guy L. Steele Jr. and a Preface by Eric S. Raymond. Most importantly, the book version is nicely typeset and includes almost all of the infamous Crunchly cartoons by the Great Quux, each attached to an appropriate entry. The second edition corresponds to the Jargon File 3. 0. 0.

*-Yellow Wire

n. [IBM] Repair wires used when connectors (especially ribbon connectors) got broken due to some schlemiel pinching them, or to reconnect cut traces after the FE mistakenly cut one. Compare blue wire, purple wire, red wire.

*-Yet Another

adj. [From UNIX's `yacc(1)', `Yet Another Compiler-Compiler', a LALR parser generator]

1. Of your own work A humorous allusion often used in titles to acknowledge that the topic is not original, though the content is. As in `Yet Another AI Group' or `Yet Another Simulated Annealing Algorithm'.
2. Of others' work Describes something of which there are already far too many.

See also YA-, YABA, YAUN.

*-YKYBHTLW

abbrev. // Abbreviation of `You know you've been hacking too long when. ', which became established on the Usenet group alt. folklore. computers during extended discussion of the indicated entry in the Jargon File.

*-YMMV

cav. Written-only abbreviation for Your mileage may vary. You are not expected to understand this [UNIX] cav. The canonical comment describing something magic or too complicated to bother explaining properly. From an infamous comment in the context-switching code of the V6 UNIX kernel. You know you've been hacking too long when. The set-up line for a genre of one-liners told by hackers about themselves. These include the following * not only do you check your email more often than your paper mail, but you remember your network address faster than your postal one. * your SO kisses you on the neck and the first thing you think is “Uh, oh, priority interrupt. ” * you go to balance your checkbook and discover that you're doing it in octal. * your computers have a higher street value than your car. * in your universe, `round numbers' are powers of 2, not 10. * more than once, you have woken up recalling a dream in some programming language. * you realize you have never seen half of your best friends. [An early version of this entry said “All but one of these have been reliably reported as hacker traits (some of them quite often). Even hackers may have trouble spotting the ringer. ” The ringer was balancing one's checkbook in octal, which I made up out of whole cloth. Although more respondents picked that one out as fiction than any of the others, I also received multiple independent reports of its actually happening, most famously to Grace Hopper while she was working with BINAC in 1949. -- ESR]

*-Your Mileage May Vary

cav. [from the standard disclaimer attached to EPA mileage ratings by American car manufacturers]

1. A ritual warning often found in UNIX freeware distributions. Translates roughly as “Hey, I tried to write this portably, but who *knows* what'll happen on your system?”
2. More generally, a qualifier attached to advice. “I find that sending flowers works well, but your mileage may vary. ”:Yow!/yow/ interj. [from “Zippy the Pinhead” comix] A favored hacker expression of humorous surprise or emphasis. “Yow! Check out what happens when you twiddle the foo option on this display hack!”

*-Yu-Shiang Whole Fish

/yoo-shyang hohl fish/ n. ,obs. The character gamma (extended SAIL ASCII 0001001), which with a loop in its tail looks like a little fish swimming down the page. The term is actually the name of a Chinese dish in which a fish is cooked whole (not parsed) and covered with Yu-Shiang (or Yu-Hsiang) sauce. Usage primarily by people on the MIT LISP Machine, which could display this character on the screen. Tends to elicit incredulity from people who hear about it second-hand.

Z

Z

See Zulu time. See Coordinated Universal Time (UTC).

Z Time

See Coordinated Universal Time.

*-Zap

1. n. Spiciness.
2. vt. To make food spicy.
3. vt. To make someone `suffer' by making his food spicy. (Most hackers love spicy food. Hot-and-sour soup is considered wimpy unless it makes you wipe your nose for the rest of the meal.) See zapped.
4. vt. To modify, usually to correct; esp. used when the action is performed with a debugger or binary patching tool. Also implies surgical precision. “Zap the debug level to 6 and run it again. ” In the IBM mainframe world, binary patches are applied to programs or to the OS with a program called `superzap', whose file name is `IMASPZAP' (possibly contrived from I M A SuPerZAP).
5. vt. To erase or reset.
6. To fry a chip with static electricity. “Uh oh -- I think that lightning strike may have zapped the disk controller. ”

*-Zapped

adj. Spicy. This term is used to distinguish between food that is hot (in temperature) and food that is *spicy*-hot. For example, the Chinese appetizer Bon Bon Chicken is a kind of chicken salad that is cold but zapped; by contrast, vanilla wonton soup is hot but not zapped. See also oriental food, laser chicken. See zap, senses 1 and 2.

*-Zen

vt. To figure out something by meditation or by a sudden flash of enlightenment. Originally applied to bugs, but occasionally applied to problems of life in general. “How'd you figure out the buffer allocation problem?” “Oh, I zenned it. ” Contrast grok, which connotes a time-extended version of zenning a system. Compare hack mode. See also guru.

*-Zero

1. vt. To set to 0. Usually said of small pieces of data, such as bits or words (esp. in the construction `zero out').
2. To erase; to discard all data from. Said of disks and directories, where `zeroing' need not involve actually writing zeroes throughout the area being zeroed. One may speak of something being `logically zeroed' rather than being `physically zeroed'. See scribble.

Zero Suppression

The elimination of nonsignificant zeros from a numeral. (FP) (ISO)

Zero-Bit Insertion

A bit-stuffing technique used with bit-oriented protocols to ensure that six consecutive “one” bits never appear between the two flags that define the beginning and the ending of a transmission frame. Note: When five consecutive “one” bits occur in any part of the frame other than the beginning and ending flag, the sending station inserts an extra “zero” bit. When the receiving station detects five “one” bits followed by a “zero” bit, it removes the extra “zero” bit, thereby restoring the bit stream to its original value.

*-Zero-Content

adj. Syn. content-free.

Zerofill

To fill unused storage locations with the representation of the character denoting “0”. (FP) (ISO)

Zeroize

Remove or eliminate the key from a crypto-equipment or fill device.

*-Zeroth

/zee'rohth/ adj. First. Among software designers, comes from C's and LISP's 0-based indexing of arrays. Hardware people also tend to start counting at 0 instead of 1; this is natural since, e. g. , the 256 states of 8 bits correspond to the binary numbers 0, 1, . , 255 and the digital devices known as `counters' count in this way. Hackers and computer scientists often like to call the first chapter of a publication `chapter 0', especially if it is of an introductory nature (one of the classic instances was in the First Edition of K&R). In recent years this trait has also been observed among many pure mathematicians (who have an independent tradition of numbering from 0). Zero-based numbering tends to reduce fencepost errors, though it cannot eliminate them entirely.

*-Zigamorph

1. /zig'*-morf/ n. Hex FF (11111111) when used as a delimiter or fence character. Usageprimarily at IBM shops.
2. [proposed] n. The Unicode non-character +UFFFF (1111111111111111), a character code which is not assigned to any character, and so is usable as end-of-string. (Unicode (a subset of ISO 10646) is a 16-bit character code intended to cover all of the world's writing systems, including Roman, Greek, Cyrillic, Chinese, hiragana, katakana, Devanagari, Easter Island `rongo-rongo', and even elvish.)

*-Zip

[primarily MS-DOS] vt. To create a compressed archive from a group of files using PKWare's PKZIP or a compatible archiver. Its use is spreading now that portable implementations of the algorithm have been written. Commonly used as follows: “I'll zip it up and send it to you. ” See tar and feather.

*-Zipperhead

n. [IBM] A person with a closed mind.

*-Zombie

n. [UNIX] A process that has died but has not yet relinquished its process table slot (because the parent process hasn't executed a `wait(2)' for it yet). These can be seen in `ps(1)' listings occasionally. Compare orphan.

#-Zone Of Control/Zoning

1. Zone of control is the three dimensional space surrounding equipment that process national security information within which unauthorized personnel (1) are denied unrestricted access and (2) are either escorted by authorized personnel or are under continuous physical or electronic surveillance. Zoning is a concept in which a defined area within a facility has been approved for the operation of equipment with appropriate TEMPEST Characteristics without emanating classified electromagnetic radiation beyond the controlled space boundary of the facility. The zones are determined by measuring electromagnetic attenuation provided by a building's physical properties and the free space loss to the controlled space boundary. Equipment zone ratings are based on the level of compromising emanations produced by the equipment. (Source -panel of experts)
2. A technique in which a protected building is divided into area: any alarm initiating device can be programmed to signal an identifying code and or indicate on an annunciator the type of problem (fire, flooding, physical penetration, etc). (Source: *Information Security: Dictionary of Concepts, Standards and Terms*; Longley, Shain, Caelli; Macmillan, 1992)

*-Zorch

1. /zorch/ [TMRC] v. To attack with an inverse heat sink.
2. [TMRC] v. To travel, with v approaching c [that is, with velocity approaching lightspeed -- ESR].
3. [MIT] v. To propel something very quickly. “The new comm software is very fast; it really zorches files through the network. ”
4. [MIT] n. Influence. Brownie points. Good karma. The intangible and fuzzy currency in which favors are measured. “I'd rather not ask him for that just yet; I think I've used up my quota of zorch with him for the week. ”
5. [MIT] n. Energy, drive, or ability. “I think I'll punt that change for now; I've been up for 30 hours and I've run out of zorch. ”
6. [MIT] v. To flunk an exam or course.

*-Zork

/zork/ n. The second of the great early experiments in computer fantasy gaming; see ADVENT. Originally written on MIT-DM during 1977-1979, later distributed with BSD UNIX (as a patched, sourceless RT-11 FORTRAN binary; see retrocomputing) and commercialized as `The Zork Trilogy' by Infocom. The FORTRAN source was later rewritten for portability and released to Usenet under the name “Dungeon”. Both FORTRAN “Dungeon” and translated C versions are available at many FTP sites.

*-Zorkmid

/zork'mid/ n. The canonical unit of currency in hacker-written games. This originated in Zork but has spread to nethack and is referred to in several other games.

Zulu Time

(Z) See Coordinated Universal Time. Formerly a synonym for Greenwich Mean Time.

1TBS*

31 U. S. C. 11
31 U. S. C. 1108
31 U. S. C. 3511
31 U. S. C. 3512
40 Federal Register 28949-28978
40 U. S. C. 759 And 487
44 U. S. C. 3501
44 U. S. C. 3506 44 U. S. C. 3507
47 Federal Register 21656-21658
5 CFR 1320
5 CFR 1320. 7
5 U. S. C. 552
5 U. S. C. 552a

Abbreivations

ACD
Abbreviation for automatic call distributor.

ACL
see Access Control List.

ACU
Abbreviation for automatic calling unit.

ADC
See analog-to-digital converter.

ADCCP
Abbreviation for Advanced Data Communication Control Procedure.

ADH
Abbreviation for automatic data handling.

ADM
see Advanced Development Model.

ADP
See Automatic Data Processing,

ADPCM
Abbreviation for adaptive differential pulse-code modulation.

ADPE
See Automated Data Processing Equipment

AE
See Application Entity.

****-AFAIK***
n. [Usenet] Abbrev. for "As Far As I Know".

AFDTC
Air Force Development Test Center

AFR
Air Force Regulation

AFSSI
See Air Force Systems Security Instruction.

AFSSM
See Air Force Systems Security Memorandum.

AIG
See Address Indicator Group.

AIN
Abbreviation for advanced intelligent network.

AIOD
Abbreviation for automatic identified outward dialing.

AIRK
See Area Interswitch Rekeying Key.

AIS
See Automated Information System.

AISS
See Automated Information System Security.

AJ
See Anti-Jamming.

AK
See Automatic remote reKeying.

AKD/RCU
See Automatic Key Distribution/Rekeying Control Unit.

AKDC
See Automatic Key Distribution Center.

AKM
See Automated Key Management center.

ALC
See Accounting Legend Code.

ALC-3
See Accounting Legend Code.

ALC-4
See Accounting Legend Code.

ALE
See Accounting Legend Code.

ALU
Abbreviation for arithmetic and logic unit.

AMA
Abbreviation for automatic message accounting.

AMI
Abbreviation for alternate mark inversion. See alternate mark inversion signal.

AMS
See Auto-Manual System, Autonomous Message Switch.

ANDVT
See Advanced Narrowband Digital Voice Terminal.

ANI
Abbreviation for automatic number identification.

AOSS
See Automated Office Support Systems.

AP
Abbreviation for anomalous propagation.

APC
See Adaptive Predictive Coding.

APD
Abbreviation for avalanche photodiode. Note: apd and a. p. d. are also used.

APL
See Assessed Products List.

APU
See Auxiliary Power Unit.

AR
Army Regulation

AR 380-380
Army Regulation

ARES
See Automated Risk Evaluation System.

ARCH:D1
Army Regulation

ARCH:D2
Army Regulation

ARQ

ARS

ASPJ
See Advanced Self-Protection Jammer.

ASU
See Approval for Service Use.

ATAM
See Automated Threat Assessment Methodology.

AUD (audit)

AUD/D1

AUD/D2

AUD/D3

AUTOSEVOCOM
See AUTOmatic SEcure VOice COMmunications (Network).

AUTOVON
See AUTOmatic VOice Network.

Auxiliary Operation
An off-line operation performed by equipment not under control of the processing unit. (FP)

AV
See Auxiliary Vector.

AVP
See Authorized Vendor Program.

B-ISDN
Abbreviation for broadband ISDN.

BCC
Abbreviation for block check character.

BCD
Abbreviation for binary coded decimal.

BCI
Abbreviation for bit-count integrity. See character-count and bit-count integrity.

BCSSO
See Base Computer System Security Officer.

Bd
Abbreviation for baud.

BER

BERT

BIU
Abbreviation for bus interface unit. See network interface device.

BPI
Abbreviation for bits per inch.

BPOC

BPS
See Bits Per Second.

****-BQS****
/B-Q-S/ adj. Syn. Berkeley Quality Software.

BR
Abbreviation for bit rate.

****-BRS****
/B-R-S/ n. Syn. Big Red Switch. This abbreviation is fairly common on-line.

BSA
Abbreviation for basic serving arrangement.

BSE
Abbreviation for basic service element.

Business Point Of Contact
(BPOC)

BW
Abbreviation For Bandwidth.

****-BWQ****
/B-W-Q/ n. [IBM abbreviation, `Buzz Word Quotient'] The percentage of buzzwords in a speech or documents. Usually roughly proportional to bogosity. See TLA.

C1

C2

C3
See Command, Control, and Communications.

C3I
See Command, Control, Communications and Intelligence.

C4
See Command, Control, Communications and Computers.

CA
See Controlling Authority, Crypto-Analysis, COMSEC Account, Command Authority.

CBA

CCB
See Configuration Control Board.

CCEP
See Commercial COMSEC Endorsement Program.

CCI
See Controlled Cryptographic Item, Controlled COMSEC Item

CCIS
Abbreviation for common-channel interoffice signaling.

CCITT
Abbreviation for International Telegraph and Telephone Consultative Committee.

CCO
See Circuit Control Officer, Configuration Control Officer.

CDRL
See Contract Data Requirements List.

CDS
See Cryptographic Device Services.

CELP

CEOI
See Communications Electronics Operating Instruction.

CEPR
See Compromising Emanation Performance Requirement.

CERT
See Computer Emergency Response Team.

CF
See Code Freeze

CFD
See Common Fill Device.

CFE
Convential Armed Forces in Europe (Treaty)

CF
See Code Freeze

CFD
See Common Fill Device.

CFE
Convential Armed Forces in Europe (Treaty)

****-CHANOP****
/chan'-op/ n. [IRC] See channel op.

CI
See Configuration Item.

CIAC
See Computer Incident Assessment Capability.

CIK
See Crypto-Ignition Key.

CIP
See Crypto-Ignition Plug.

CIRCULAR No. A-127
See Financial Management Systems

Circular No. A-130
See Management of federal Information Resources

CIRK
See Common Interswitch Rekeying Key.

CK
See Compartment Key.

CKG
See Cooperative Key Generation.

CKL
See Compromised Key List.

CLMD
See COMSEC Local Management Device.

CM
See Configuration Management.

CMCS
See COMSEC Material Control System.

CMP
See Configuration Management Plan.

CMS
See C4 Systems Security Management System.

CN
Counternarcotics

CNCS
See CryptoNet Control Station.

CNK
See Cryptonet Key.

CNLZ
See COMSEC No-Lone Zone.

COMPUSEC
See COMPUter SECurity.

COMSEC
See COMmunications SECurity.

COOP
See Continuity Of Operations Plan.

COR
See Central Office of Record.

COTS
See Commercial Off The Shelf.

CPC
See Computer Program Component.

CPCI
See Computer Program Configuration Item.

Cpi
Abbreviation for characters per inch. The number of characters recorded on an inch of recording medium. (~)

CPS
See COMSEC Parent Switch.

CPU
See Central Processing Unit.

CRB

CRC
See Cyclic Redundancy Check.

CRIB
See Card Reader Insert Board.

CRLCMP
See Computer Resources Life Cycle Management Plan.

CRO
See COMSEC Responsible Officer.

CRP
See COMSEC Resources Program (Budget).

CRWG
See Computer Resources Working Group.

CSA
See Cognizant Security Authority.

CSC
See Computer Software Component.

CSC Bulletin

CSC-STD-001-83

CSC-STD-002-85

CSC-STD-0030-85

CSC-STD-004-85

CSCI
See Computer Software Configuration Item.

CSE
See Communications Security Element.

CSETWG
See Computer Security Education and Training Working Group.

CSM
See Computer System Manager.

CSO
See Computer Security Officer, C4 Systems Officer

CSPP
See Communications-Computer Systems Program Plan.

CSRD
See Communications-Computer Systems Requirements Document.

CSS
See COMSEC Subordinate Switch, Constant Surveillance Service (Courier), Continuous Signature Service (Courier).

CSSO
See Contractor Special Security Officer, Computer System Security Officer. ()

CSSP
See Computer Security Support Program.

CSTVRP
See Computer Security Technical Vulnerability Reporting Program.

CSWG
See Computer Security Working Group.

CTAK
See Cipher Text Auto-Key.

CTTA
See Certified TEMPEST Technical Authority.

CUP
See COMSEC Utility Program.

CVA
See Clandestine Vulnerability Analysis.

CVRP
See C4 System Security Vulnerability Reporting Program.

CWC
Chemical Weapons Convention (Treaty)

D&V
See Demonstration and Validation.

DAA
See Designated Approving Authority.

DAC
See Discretionary Access Control.

DAC/D1

DAC/D2

DAC/D3

DAMA
See Demand Assigned Multiple Access.

DBMS
See Data Base Management System.

DC
Direct Current

DCA
Defense Communications Agency

DCID
Director Central Intelligence Directive

DCP
See Decision Coordinating Paper.

DCS
See Defense Communications System, Defense Courier Service.

DCSP
See Design Controlled Spare Part(s).

DD:D1

DD:D2

DDD
Abbreviation for direct distance dialing.

DDN
See Defense Data Network.

DDS
See Dual Driver Service (courier).

DES
See Data Encryption Standard.

DF
Direction Finding

DIB
See Directory Information Base.

DID
See Data Item Description.

DLE

DLED
See Dedicated Loop Encryption Device.

DMA
Direct Memory Access.

DO

DOD
See Deparment of Defense

DoD 5200. 28-M
Automated Data Processing Security Manual.

DoD 5200. 28-STD

DoD 5200. 28-STD, 1985.

DoD 5200. 28-STD.
Trusted Computer System Evaluation Criteria (*Orange Book*.

DoD Directive 5200. 28

DoD Directive 5215. 1
Department of Defense (DoD) Computer Security Center.

DODD
Department of Defence Directive

DOE
Department of Energy

DON
Department of the Navy

DS
Abbreviation for digital signal.

DSN
See Defense Switched Network.

DSU
Abbreviation for data service unit.

DSVT
See Digital Subscriber Voice Terminal.

DT&E
See Development Testing and Evaluation.

DTD
See Data Transfer Device.

DTE
Abbreviation for data terminal equipment.

DTIRP
Defense Treaty Inspection Readiness Program

DTLS
See Descriptive Top-Level Specification.

DTS
See Diplomatic Telecommunications Service.

DUA
See Directory User Agent.

EAM
See Emergency Action Message.

ECM
See Electronic CounterMeasures.

ECPL
See Endorsed Cryptographic Products List (a section in the Information Systems Security Products and Services Catalogue).

EDAC
See Error Detection And Correction.

EDESPL
See Endorsed Data Encryption Standard Products List.

EDM
See Engineering Development Model.

EEFI
Essential Elements of Friendly Information

EEI
Essential Elements of Information

EEPROM
See Electrically Erasable Programmable Read Only Memory.

EFD
See Electronic Fill Device.

Efficiency

EFT

EFTO
See Encrypt For Transmission Only.

EGADS
See Electronic Generation, Accounting, and Distribution System.

EIF
Entry Into Force

EKMS
See Electronic Key Management System.

ELECTRO-OPTINT
Electro-Optical Intelligence

ELINT
See ELectronic INTelligence.

ELSEC
See ELectronics SECurity.

EMS

EMSEC
See EMissions SECurity.

EOT
Abbreviation for end of transmission character.

EPL
See Evaluated Products List (a section in the Information Systems Security Products and Services Catalogue).

ERTZ
See Equipment Radiation TEMPEST Zone.

ES

ESS

ETAP
See Education, Training, and Awareness Program.

ETB

ETL
See Endorsed Tools List.

ETPL
See Endorsed TEMPEST Products List.

ETX

EUCI
See Endorsed for Unclassified Cryptographic Information.

EV
See Enforcement Vector.

****-FAQL***
/fa'kl/ n. Syn. FAQ list.

FCA
See Functional Configuration Audit, Formal Cryptographic Access.

FDDI
Abbreviation for fiber distributed data interface.

FDDI-2
See fiber distributed data interface.

FDIU
See Fill Device Interface Unit.

FDM
See Formal Development Methodology.

Federal Information Processing Standards

Federal Managers Financial Integrity Act

Federal Property And Administrative Service Act

Federal Property And Administrative Services Act Of 1949

Federal Records Act

Federal Register

Federal Telecommunications Fund

FIPS
See Federal Information Processing Standards.

FIPS PUB
See Federal Information Processing Standard Publication.

FIPS PUB *39*
See A Glossary For Computer Systems Security

FOCI
See Foreign Owned, Controlled or Influenced.

FOI
Freedom of Information. Information or activities related to the Freedom of Information Act. (ed. ;)

FOIA
See Freedom of Information Act

FOT&E
See Follow-on Operational Test and Evaluation.

FOUO
See For Official Use Only.

FQR
See Formal Qualification Review.

FQT
See Formal Qualification Testing.

FRD
Formerly Restricted Data

FSD
See Full Scale Development.

FSRS
See Functional Security Requirements Specification.

FSTS
See Federal Secure Telephone Service.

FTAM
See File Transfer Access Management.

FTLS
See Formal Top-Level Specification.

FTS
See Federal Telecommunications System.

GAO;
General Accounting Office

****-GPL***
/G-P-L/ n. Abbreviation for `General Public License' in widespread use; see copyleft, General Public Virus.

GPS
See Global Positioning System.

****-GPV***
/G-P-V/ n. Abbrev. for General Public Virus in widespread use.

GSA
See General Services Administration

GTS
See Global Telecommunications Service.

Guidance For Applying The DoD TCSEC In Specific Environments

Guidance For Conducting Matching Programs

Guide To Writing The Security Features Users Guide For Trusted Systems

Guidelines For Formal Verification Systems
See *NCSC-TG*-014

Guidelines For Trusted Facility Management

Guidelines For Writing Trusted Facility Manuals
See *NCSC-TG*-016

HD
Abbreviation For Half Duplex. ()

HDLC
Abbreviation for high-level data link control.

HDM
See Hierarchical Development Methodology.

HF
Abbreviation for high frequency.

****-HHOK***
See ha ha only serious.

****-HHOS***
See ha ha only serious.

HOIST
HOIS

HOL
See High Order Language.

HSM
See Human Safety Mandatory modification.

HUMINT
Human Intelligence

HUS
See Hardened Unique Storage.

HUSK
See Hardened Unique Storage Key.

Hz
See hertz

I&A

I&A/D1

I&A/D2

I/0 Devices

I/0 Handlers

I/0 Manager

I/O
See Input/Output.

I/O Controller
See input-output controller.

IAC
Information Analysis Center

IBAC
See Identity Based Access Control.

ICU
See Interface Control Unit.

IDN
Abbreviation for integrated digital network.

IDS
See Intrusion Detection System.

IEMATS
See Improved Emergency Message Automatic Transmission System.

IFF
See Identification, Friend or Foe.

IFFN
See Identification, Friend, Foe, or Neutral.

II
Imagery Interpretation

IIRK
See Interarea Interswitch Rekeying Key.

ILS
See Integrated Logistics Support.

IMINT
Imagery Intelligence

IMP
Abbreviation for interface message processor.

IN
Abbreviation for intelligent network.

INF
Intermediate-Range Nuclear Forces (Treaty)

INFOSEC
See INFOrmation systems SECurity.

INTSEC
A balancing of the INFOSEC and SIGINT missions

IOC
See Initial Operational Capability

IOSS
Interagency OPSEC Support Staff

IOT&E
See Initial Operational Test and Evaluation.

IP
See Internet Protocol.

IPAR

IPC
Interprocess Communication

IPC Files

IPM
See InterPersonal Messaging.

IPSO
See Internet Protocol Security Option.

IRK
See Interswitch Rekeying Key.

IRM
Information Resource Management

IS
See Information System.

ISDN
See Integrated Services Digital Network.

ISINT
Instrumentation Signals Security

ISM
(Information Systems Management)

ISO
See International Standards Organization.

ISRD
Information System Requirements Document

ISS
See Information Systems Security.

ISSO
See Information Systems Security Officer.

IT
(Information Technology)
See Information Technology

ITAR
See International Traffic in Arms Regulation.

ITF
(Information Technology Facility)
See Information Technology Facility

ITM
(Information Technology Management)
See Information Technology Management

IV&V
See Independent Verification and Validation.

IVDT

****-IWBNI***
// Abbreviation for `It Would Be Nice If'. Compare WIBNI.

JTIDS
See Joint Tactical Information Distribution System.

JTRB
Abbreviation For Joint Telecommunications Resources Board. (FS1037S1. TXT) See Joint Telecommunications Resources Board.

KAK
See Key-Auto-Key.

KB
Shorthand for Knowledge Base (q. v.).

KBAF
Shorthand for Knowledge Base Access Functions (part of MAPLESS)

KBE
Shorthand for Knowledge Base Editor (part of MAPLESS).

KDC
Key Distribution Center

KE
Shorthand for Knowledge " the user of MAPLESS.

KEK
See Key Encryption Key.

KG
See Key Generator.

KMASE
See Key Management Application Service Element.

KMC
See Key Management Center.

KMID
See Key Management IDentification number.

KMODC
See Key Material Ordering and Distribution Center.

KMP
See Key Management Protocol.

KMPDU
See Key Management Protocol Data Unit.

KMS
See Key Management System.

KMSA
See Key Management System Agent.

KMUA
See Key Management User Agent.

KP
See Key Processor.

KPK
See Key Production Key.

KSOS
See Kernelized Secure Operating System.

KVG
See Key Variable Generator.

LAN
See Local Area Network.

LASINT
See laser intelligence.

LATA
See local access and transport area.

LEAD
See Low-cost Encryption/Authentication Device.

LIFO
See last in, first out.

LIMDIS
Limited Distribution. A HANDLING CAVEAT or SPECIAL MARKING indicating limited distribution of the associated information. (ed. ;)

LIMFACS
Limiting Factors

LKG
See Loop Key Generator.

LLC

LLNL
Lawrence Livermore National Laboratory

LMD
See Local Management Device.

LME
See Layer Management Entry.

LMI
See Layer Management Interface.

LOS
See line of sight. See line-of-sight propagation.

LP
See linear programming.

LPC
See linear predictive coding.

LPD
See Low Probability of Detection.

LPI
See Low Probability of Intercept.

LRIP
See Limited Rate Initial Preproduction.

LSI
See Large Scale Integration.

MAC
See Mandatory Access Control, Message Authentication Code, medium access control sublayer.

MAN
See MANditory modification, metropolitan area network.

MCCB
See Modification/Configuration Control Board.

MCCR
See Mission Critical Computer Resources.

MCSSM
See MAJCOM Computer System Security Manager.

MCTL
See Military Critical Technologies List.

MDC
See Manipulation Detection Code, Message Distribution Center.

MEP
See Management Engineering Plan.

MER
See Minimum Essential Requirements.

Mgt
(management)
See Management

MHS
See Message Handling System.

MHz
See megahertz

MI
See Message Indicator.

MIB
See Management Information Base.

MIJI
See Meaconing, Intrusion, Jamming and Interference.

MIL-STD
See MILitary STandarD.

MINTERM
See MINiature TERMinal.

MIPR
See Military Interdepartmental Purchase Request.

MLS
The multilevel security formula generator, a flow analysis tool developed at SRI for use with HDM. (MTR-8201)

MOA
See Memorandum Of Agreement.

MOE
See Measure Of Effectiveness.

MOP
See Measure Of Performance.

MOU
See Memorandum Of Understanding.

MRK
See Manual Remote reKeying.

MRT
See Miniature Receiver Terminal.

MSE
See Mobile Subscriber Equipment.

MTBF
See mean time between failures.

MTR
Mitre Corporation

MTT
See Methodologies, Tools, and Techniques.

NACAM
See NAtional COMSEC Advisory Memorandum.

NACSEM
NAtional COMSEC Emanations Memorandum. (AF9K_JBC. TXT) See NAtional COMSEC Emanations Memorandum.

NACSI
See NAtional COMSEC Instruction.

NACSIM
See NAtional COMSEC Information Memorandum.

NAR

NARA
National Archives And Records Act National Archives And Records Administration

NBH

NCA
See National Command Authority.

NCC
See National Coordinating Center.

NCCD
See National Command and Control Document.

NCS
See National Communications System.

NCSC
See National Computer Security Center.

NCSC Bulletin

NCSC-TG-001
See A Guide to Understanding Audit in Trusted Systems Version 2

NCSC-TG-*002*
See Trusted Product Evaluations - A Guide for Vendors Version 1

NCSC-TG-*003*
See A Guide to Understanding Discretionary Access Control in Trusted Systems Version 1

NCSC-TG-*004*
See Glossary of Computer Security Terms Version 1

NCSC-TG-*006*
See A Guide to Understanding Configuration Management in Trusted Systems Version 1

NCSC-TG-*007*
See A Guide to Understanding Design Documentation in Trusted Systems Version 1

NCSC-TG-*008*
See A Guide to Understanding Trusted Distribution in Trusted Systems Version 1

NCSC-TG-*009*
See Computer Security Subsystem Interpretation (CSSI) of the Trusted Computer System Evaluation Criteria (TCSEC) Version 1

NCSC-TG-*010*
See A Guide to Understanding Security Modeling in trusted Systems Version 1

NCSC-TG-*011*
See Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation Version 1

NCSC-TG-*013*
See Rating Maintenance Phase Program Document Version 1

NCSC-TG-*014*
See Guidelines for Formal Verification Systems Version 1

NCSC-TG-*015*
See A Guide to Understanding Trusted Facility Management Version 1

NCSC-TG-*016*
See Guidelines for Writing Trusted Facility Manuals Version 1

NCSC-TG-*017*
See A Guide to Understanding Identification and Authentication in Trusted Systems Version 1

NCSC-TG-*018*
See A Guide to Understanding Object Reuse in Trusted Systems Version 1

NCSC-TG-*019*
See Trusted Product Evaluation Questionnaire Version 2

NCSC-TG-*021*
See Trusted Database Management System Interpretation (TDI) of the Trusted Computer System Evaluation Criteria (TCSEC) Version 1

NCSC-TG-*022*
See A Guide to understanding Trusted Recovery in Trusted Systems Version 1

NCSC-TG-*023*

NCSC-TG-024
See A Guide to Procurement of Trusted Systems

NCSC-TG-*025*

NCSC-TG-026
See A Guide to Writing the Security Feautures User's Guide for Trusted Systems Version 1

NCSC-TG-*027*
See A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems Version 1

NCSC-TG-*028*
See Assessing Controlled Access Protection Version 1

NCSC-TG-*029*
See Introduction to Certification and Accreditation

NCSC-TG-*030*

NEC
See National Electric Code.

NETS
See Nationwide Emergency Telecommunications Service.

NID
See network interface device, network inward-dialing.

NII
National Information Infrastructure

NISAC
See National INFOSEC Assessment Center, National Industrial Security Advisory Committee.

NIST
See National Institute of Standards and Technology.

NIU
See network interface unit. See network interface device.

NKSR
See Non-Kernel Security-Related software.

NM

NRZ
See non-return-to-zero. See non-return-to-zero code.

NRZ1
See non-return-to-zero, change-on-ones.

NSA
See National Security Agency.

NSAD
See Network Security Architecture and Design.

NSD
See National Security Directive.

NSDD
See National Security Decision Directive.

NSDD 145

NSEP
See National Security Emergency Preparedness.

NSI
National Security Information

NSM
See Network Security Manager.

NSO
See Network Security Officer.

NSP
See Network Security Plan.

NSRP
Non-technical Support Real Property

NSTAC
See National Security Telecommunications Advisory Committee.

NSTISSAM
See National Security Telecommunications and Information Systems Security Advisory/information Memorandum.

NSTISSC
See National Security Telecommunications and Information Systems Security Committee.

NSTISSD
See National Security Telecommunications and Information Systems Security Directive.

NSTISSI
See National Security Telecommunications and Information Systems Security Instruction.

NSTISSP
See National Security Telecommunications and Information Systems Security Policy.

NTCB
See Network Trusted Computing Base.

NTI
See network terminating interface.

NTIA
See National Telecommunications and Information Administration.

NTIS
National Technical Information Service

NTISS
National Telecommunications and Information System Security

NTISSAM
See National Telecommunications and Information Systems Security Advisory/information Memorandum.

NTISSC
See National Telecommunications and Information Systems Security Committee.

NTM
National Technical Means

NTN
See network terminal number.

O&M
See Operations and Maintenance.

OADR
See Originating Agency's Determination Required.

OCR
See optical character reader, optical character recognition.

OEM
Original Equipment Manufacturer

OMB
See Office of Management and Budget

OMB A-130

OMB CIR
See Office of Management and Budget CIRcular.

OMB CIRC
Office of Management and Budget Circular

OMB Circular A-127
See Financial Management Systems

ONA
See open network architecture.

OPCODE
See OPerations CODE.

OPI
Office of Primary Interest

OPM
See Office of Personnel Management

OPNAVINST
Office of Navy Operations Instruction

OPNAVINST 5239. 1A
See Automatic Data Processing Security Program

OPSEC
See OPerations SECurity.

OPT
See OPTional modification.

OPTINT
Optical Intelligence

OR
Object Reuse

OR/D2

ORD
Operational Requirements Document

OSI

OSINT
Open Source Intelligence (Unknown) an acronym for Open Source Intelligence.

OT&E
See Operational Test and Evaluation.

OTAD
See Over-The-Air key Distribution.

OTAR
See Over-The-Air Rekeying.

OTAT
See Over-The-Air key Transfer.

****-OTOH***
[USENET] On The Other Hand.

OTP
See One-Time Pad.

OTT
See One-Time Tape.

OUSDR&E
Office of the Under Secretary of Defence for Research and Engineering

P Model
See Preproduction Model.

P&D
See Production and Deployment.

PA
See Privacy Act.

PAA
See Peer Access Approval.

PAE
See Peer Access Enforcement.

PAL
See Permissive Action Link.

****-PARC***
n. See XEROX PARC.

PBX

PC
See Personal Computer.

PCA
See Physical Configuration Audit.

PCS
See Physical Control Space.

PCZ
See Protected Communications Zone, Physical Control Zone.

PDN

PDR
See Preliminary Design Review.

PDS
See protected distribution system. (F:\NEWDEFS. TXT) See Practice Dangerous to Security, Protected Distribution System.

PDU
See Protocol Data Unit.

PERC
See Product Evaluation Resource Center.

PKA
See Public Key Algorithm.

PKC
See Public Key Cryptography.

PKSD
See Programmable Key Storage Device.

PL
See Public Law.

PLA
See programmable logic array.

PLSDU
See Physical Layer Service Data Unit.

PM
See Program Manager, Preventative Maintenance.

PMD
See Program Management Directive.

PMO
See Program Management Office.

PMP
See Program Management Plan.

PNEK
See Post-Nuclear Event Key.

PNET
Peacetime Nuclear Elimination Treaty

POM
See Program Objective Memorandum.

PPL
See Preferred Products List (A section in the Information Systems Security Products and Services Catalogue).

PRBAC
See Partition Rule Base Access Control.

Privacy Act

Privacy Act Guidelines

Privacy Act Of 1974

PSDU
See Physical layer Service Data Unit.

PSL
See Protected Services List.

PSN

PSTN

PTR
See Preliminary Technical Report

PTT
See Push-To-Talk.

PUC
See public utility commission.

PVC
See permanent virtual circuit.

PWA
See Printed Wiring Assembly.

PWDS
See Protected Wireline Distribution System.

PX
See private exchange, peak envelope power [of a radio transmitter].

QA
See quality assurance.

QC
See quality control.

QOS

QOT&E
See Qualification Operational Test and Evaluation.

QT&E
See Qualification Test and Evaluation.

R&D
See Research and Development.

RAC
See Repair ACtion.

RACE
See Rapid Automatic Cryptographic Equipment.

RADINT
See radar intelligence.

RAM
See Random Access Memory.

RCCI
See Regional Computer Crime Investigator.

RD
Restricted Data

REL
Releasable Only to Those Mentioned

RF
Radio Frequency

RFP
See Request For Proposal.

RKV
Rekeying variable

****-RL***
// n. [MUD community] Real Life. “Firiss laughs in RL” means that Firiss's player is laughing. Oppose VR.

RM Plan

RM-Plan

RMR
See Rating Maintenance Report

RO
See receive only.

RQT
See Reliability Qualification Tests.

****-RSN***
/R-S-N/ adj. See Real Soon Now.

S&T
Scientific and Technical

S-F
See store-and-forward.

****-S/N Ratio***
// n. (also `s/n ratio', `s:n ratio'). Syn. signal-to-noise ratio. Often abbreviated `SNR'.

SAISS
See Subcommittee on Automated Information Systems Security of the NTISSC.

SAMS
See Semi-Automatic Message Switch.

SAO
See Special Access Office.

SAP
See System Acquisition Plan, Special Access Program.

SARK
See SAVILLE Advanced Remote Keying.

SAV
Special Right of Access Visits

SCG

SCI
See Sensitive Compartmented Information.

SCIF
See Sensitive Compartmented Information Facility.

SCP
See System Concept Paper.

SDLC
Systems Development Life Cycle

SDNRIU
See Secure Digital Net Radio Interface Unit.

SDNS
See Secure Data Network System.

SDR
See System Design Review.

SecDef
Seecretary of Defense

SFA
See Security Fault Analysis.

SFUG

SFUG:D1

SFUG:D2

SI
See Special Intelligence.

SIGINT
See signals intelligence.

SIGSEC
See SIGnals SECurity.

SIOP-ESI
An acronym for Single Integrated Operational Plan - Extremely Sensitive Information; a *DOD* special access program. (DODD 5200. 28;)

SISS
See Subcommittee on Information Systems Security of the NSTISSC.

SMM
See Special Mission Manditory modification.

SMO
See Special Mission Optional modification.

SMU
See Secure Mobile Unit.

SOH
See start-of-heading character.

SOIC
Senior Official of the Intelligence Community

SON
See Statement of Operational Need.

SORD
See Systems Operational Requirements Document.

SOW
See Statement Of Work.

SPK
See Single Point Key(ing).

SPO
See System Program Office.

SPS
See Scratch Pad Store.

SRI
SRI International

SRP

SRR
See System Requirements Review.

SSE
System Security Engineering

SSMP
System Security Management Plan

SSO
See Special Security Officer.

SSR
See Software Specification Review.

ST&E
See Security Test and Evaluation.

STD
See STandarD.

STI

STS
See Subcommittee on Telecommunications Security of the NTISSC.

STU
See secure telephone unit.

STX
See start-of-text character.

SUB
See substitute character.

SVRR
Russian Foreign Intelligence Service

SYN
See synchronous idle character.

SYSADM
System Administrator

SYSGEN
See system generation.

T&E
See Test and Evaluation.

TA
See Traffic Analysis.

TACTED
See TACtical Trunk Encryption Device.

TACTERM
See TACtical TERMinal.

TAG
See TEMPEST Advisory Group, flag, label.

TAISS
See Telecommunications and Automated Information Systems Security.

TASO
See Terminal Area Security Officer.

TCB
See Trusted Computing Base.

TCB Subset

TCD
See Time Compliance Data.

TCS
See trusted computer system.

TCU
See teletypewriter control unit.

TD
See Transfer Device.

TD:D1

TD:D2

TDBI
See Trusted Data Base Interpretation of the TCSEC.

TDM
See time-division multiplexing.

TDMA
See time-division multiple access.

TED
See trunk encryption device.

TEI
See Trusted Evaluated Interpretation of the TCSEC.

TEK
See traffic encryption key.

TELINT
Telemetry Intelligence

TEMP
See Test and Evaluation Master Plan.

TEP
See TEMPEST Endorsement Program.

TEST:D1

TEST:D2

TFM
See Trusted Facility Manual.

TFM:D1

TFM:D2

TFS
See Traffic Flow Security.

TIOCC
Treaty Inspections OPSEC Coordinating Committee

TLS
See Top-Level Specification. ()

TMC
See Two-Man Control.

TNI
See Trusted Network Interpretation of the TCSEC.

TNIEG
See Trusted Network Interpretation Environment Guideline.

TPC
See Two-Person Control.

TPI
See Two-Person Integrity.

TPOC
Technical Point Of Contact

TPWG
See Test Planning Working Group.

TRANSEC
See TRANsmission SECurity.

TRB
See Technical Review Board. ()

TRI-TAC
See TRI-service TACtical communications system, tactical communication.

TRR
See Test Readiness Review.

TSCM
See Technical Surveillance Counter-Measures.

TSEC
See Telecommunications SECurity.

TSK
See Transmission Security Key.

TTBT
Threshold Test Ban Treaty

Tty
See teletypewriter.

TTY/TDD
A unique telecommunication device for the deaf, using TTY principles.

TWX
See teletypewriter exchange service

UA
See User Agent.

UIRK
See Unique Interswitch Rekeying Key.

UIS
See User Interface System.

UK
See Unique Key.

UPP
See User Partnership Program.

UV
Unique variable

VSA

VST
See VINSON Subscriber Terminal.

VTT
See VINSON Trunk Terminal.

WATS
See Wide Area Telephone Service. See also local access and transport area.

- The Jargon File v3. 2. 0 3/21/1995
- KSA from The Unified Taxonomy