Consolidated Security Glossary

This consolidated glossary of security terminology has been compiled as a working paper for the IEEE POSIX P1003.6 Security Working Group as part of the exercise of producing P1003.22 A Security Framework.

It is a source document for security terminology and does not represent endorsement of any of the definitions contained herein.

It should be noted that many of the source documents are in draft form and therefore subject to change, additionally the latest draft may not be that available when composing this document.

The source documents for the current version are:

ECMA TR/46 1988
ECMA-138 1989
TCSEC 1985
ITSEC Ver 1.2 1991
Federal Criteria Ver 1.0 Dec 1992
CESG memorandum No1 Issue 1.2 Oct 1992
POSIX.0 Draft 15 Jun 1992
POSIX.6 Draft 13 Nov 1992
ISO 7498-2 1989
ISO/IEC CD 10181-1 Dec 1992
ISO/IEC DIS 10181-2 1991
ISO/IEC CD 10181-3 Oct 1991
ISO/IEC CD 10181-7 Aug 1992
ISO/IEC DIS 10745 May 1992

A comparison with ISO/IEC JTC 1/SC 27/WG 1/SD 6 Draft 3 has found terms included from:

ISO/IEC 9798-1
ISO/IEC 9594-8 and CCITT X509
ISO 8372
ISO/IEC 10116
ISO 10202-1

Most, if not all, the missing terms are related to cryptography.

It is intended that in producing the POSIX Security Framework terminology will be based upon ISO terminology as far as possible.

abstract security service

[ECMA-138 Dec 1989]

A set of security functions that together provide one or more of the security facilities defined in ECMA TR/46.

acceptance procedure

[ITSEC Ver 1.2 1991]

A procedure which takes objects produced during the development, production and maintenance processes for a Target of Evaluation and, as a positive act, places them under the controls of a Configuration Control system.

acceptance testing

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Formal testing conducted to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept it.

access

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

1. Condition where the potential exists for information to flow between entities.

2. A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

access

[FC Ver 1.0 Dec 1992]

Ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or object in an Information Technology (IT) Product. Frequently used as a verb, contrary to the rules of grammar.

Note: An individual does not have "access" if the proper authority or a physical, technical, or procedural measure prevents them from obtaining knowledge or having an opportunity to alter information, material, resources, or components.

access

[POSIX.6/D13 Nov 1992]

A specific type of interaction between a subject and an object that results in the flow of information from one to the other. Possible information flows include the transfer of attributes pertaining to that object, the transfer of data pertaining to that object, or the fact of existence of that object.

access

[TCSEC Dec 1985]

A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

access ACL

[POSIX.6/D13 Nov 1992]

An ACL which is used in making access control decisions for an object.

access context

[ECMA TR/46 Jul 1988]

The context, in terms of such variables as location, time of day, level of security of the underlying associations, etc., in which an access to a security object is made.

access control

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

1. Control over the flow of information between entities.

2. The prevention of access without access rights.

access control

[ECMA TR/46 Jul 1988]

The prevention of use of a resource by unidentified and/or authorized entities in any other than an authorized manner.

access control

[FC Ver 1.0 Dec 1992]

Process of limiting access to the resources of an IT product only to authorized users, programs, processes, systems, or other IT products.

access control

[ISO 7498-2:1989]

The prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner.

access control

[POSIX.6/D13 Nov 1992]

The prevention of unauthorized access of subjects to objects.

access control certificate

[ISO/IEC CD 10181-3 Oct 1991]

ADI in the form of a security certificate

access control decision function (ADF)

[ISO/IEC CD 10181-3 Oct 1991]

A specialized function that makes access control decisions by applying access control policy rules to a requested action, ACI (of initiators, targets, actions, or that retained from prior actions), and the context in which the request is made.

access control decision information (ADI)

[ISO/IEC CD 10181-3 Oct 1991]

The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.

access control enforcement function (AEF)

[ISO/IEC CD 10181-3 Oct 1991]

A specialized function that is part of the access path between an initiator and a target on each access and enforces the decisions made by the ADF.

access control information (ACI)

[ISO/IEC CD 10181-3 Oct 1991]

Any information used for access control purposes, including contextual information.

access control list

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A list associated with an object specifying the access rights of subjects to that object.

access control list

[ECMA TR/46 Jul 1988]

A set of control attributes. It is a list, associated with a security object or group of security objects. The list contains the names of security subjects and the type of access that may be granted.

access control list

[FC Ver 1.0 Dec 1992]

A list of subjects that are authorized to have access to some object(s). Usually, this list contains entries consisting of identifiers of users and groups of users and access rights.

access control list

[ISO 7498-2:1989]

A list of entities, together with their access rights which are authorized to have access to a resource.

access control list

[POSIX.6/D13 Nov 1992]

Discretionary access control mechanism associated with an object, consisting of a list of entries, where each entry is a subject identifier coupled with a set of access permissions.

access control mechanism

[FC Ver 1.0 Dec 1992]

Security safeguards designed to detect and prevent unauthorized access, and to permit authorized access in an IT product.

access control policy

[ECMA TR/46 Jul 1988]

A set of rules, part of a security policy, by which human users, or their representatives, are authenticated and by which access by these users to applications and other services and security objects is granted or denied.

access control policy

[ISO/IEC CD 10181-3 Oct 1991]

The set of rules that define the conditions under which an access may take place.

access control policy

[POSIX.6/D13 Nov 1992]

A set of rules, part of a security policy, by which subjects are authorized and by which access by these subjects to objects is granted or denied.

access control system (ACS)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A component of a system which enforces access control.

access matrix

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A notional table of permitted operations, indexed by subject and object, constituting the access rights to be enforced by a system.

Consolidated Security Glossary

access mediation

[FC Ver 1.0 Dec 1992]

Process of monitoring and controlling access to the resources of an IT product, including but not limited to the monitoring and updating of policy attributes during accesses as well as the protection of unauthorized or inappropriate accesses (see Access Control).

access permission

[POSIX.6/D13 Nov 1992]

See file access permissions.

access right

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Authorization of access.

Notes: [1] Access rights may be more or less explicit, both in the granularity of definition of subjects and objects used in implementing the security policy and in authorization of different types of access (eg read, write, execute).

[2] Within a given context (for example within an Electronic Security Environment or a database) access rights exist insofar as they are not denied.

See also: Need-to-Know, Least Privilege.

accountability

[FC Ver 1.0 Dec 1992]

Means of linking individuals to their interactions with an IT product, thereby supporting identification of and recovery from unexpected or unavoidable failures of the control objectives.

accountability

[ISO 7498-2:1989]

The property that ensures that the actions of an entity may be traced to that entity.

accounting

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Recording of the exercise of access rights to types of information specified in the System Security policy.

Note: The term "security accounting" may be used to avoid ambiguity.

See also: Audit Trail.

accreditation

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A statement by a Departmental Security Officer to a System Manager confirming that the use of a system to process, store and/or forward classified information under conditions specified in the System Security Policy meets his Security Requirement, does not present an unacceptable risk to national security and may, therefore, be brought into operation.

Note: Where the System Security policy calls for security measures to be enforced by hardware and software, accreditation may be dependent on evaluation and certification.

accreditation

[FC Ver 1.0 Dec 1992]

Formal declaration by a designated approving authority that an Automated Information System (AIS) is approved to operate in a particular security configuration using a prescribed set of safeguards.

accreditation (1)

[ITSEC Ver 1.2 1991]

The procedure for accepting an ITSEC Ver 1.2 1991 system for use within a particular environment.

accreditation (2)

[ITSEC Ver 1.2 1991]

The procedure for recognising both the technical competence and the impartiality of a test laboratory to carry out its associated tasks.

accreditation panel

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Group of people brought together by the Departmental Security Officer to satisfy him that a system has an adequate and acceptable System Security policy and that it will be compliant with it when in operation.

Note: An Accreditation Panel should normally be chaired by the Departmental Security officer or his representative and should include the ITSO, the Project Manager, the System Manager, the Certifier and representatives of other security authorities having a legitimate interest in the security of the system (eg data providers or accreditors of interconnected systems).

See also: Configuration Management Board.

accreditor

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The person responsible for accreditation of a system.

Note: This is normally the Departmental Security officer or the ITSO of the System Manager's Department.

action

[ISO/IEC CD 10181-3 Oct 1991]

The operations and operands that form part of an attempted access.

action access control decision information (action ADI)

[ISO/IEC CD 10181-3 Oct 1991]

Action decision information associated with the action.

active threat

[ISO 7498-2:1989]

The threat of a deliberate unauthorized change to the state of the system.

Note: Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity and denial of service.

administration documentation

[ITSEC Ver 1.2 1991]

The information about a Target of Evaluation supplied by the developer for use by an administrator.

administrator

[ITSEC Ver 1.2 1991]

A person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.

alarm collector function

[ISO/IEC CD 10181-7 Aug 1992]

A function that collects the security alarm messages, translates them into security alarm records, and writes them to the security alarm log.

alarm examiner function

[ISO/IEC CD 10181-7 Aug 1992]

A function that interfaces with a security alarm administrator.

application

[ECMA-138 Dec 1989]

Where the word "application" is used in this text it refers to a generic concept and should not be confused with the terms "application process" and "application entity".

application

[POSIX.0/D15 Jun 1992]

The use of capabilities (services/facilities) provided by an information system specific to the satisfaction of a set of user requirements.

Note: These capabilities include hardware, software, and data.

application area profile

[POSIX.0/D15 Jun 1992]

A profile created from multiple standards that specify multiple, divers types of functionality for a particular application are (e.g., database, networking, graphics, operating system).

application environment profile (AEP)

[POSIX.0/D15 Jun 1992]

A profile, specifying a completed and coherent specification of the OSE, in which the standards, options, and parameters chosen are necessary to support a class of applications.

application platform

[POSIX.0/D15 Jun 1992]

A set of resources that support the services on which application software will run.

The application platform provides services at its interfaces that, as much as possible, make the specific characteristics of the platform irrelevant to the application software.

application program interface

[FC Ver 1.0 Dec 1992]

System access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well defined functionality.

application program interface

[POSIX.0/D15 Jun 1992]

The interface between the application software and the application platform, across which all services are provided.

The application program interface is primarily in support of application portability, but system and application interoperability are also supported by a communication API.

application software

[POSIX.0/D15 Jun 1992]

Software that is specific to an application and is composed of programs, data and documentation.

approval/accreditation

[TCSEC Dec 1985]

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.

architectural design

[ITSEC Ver 1.2 1991]

A phase of the Development Process wherein the top level definition and design of a Target of Evaluation is specified.

architecture

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A description of a system and its structure. In each structural component the various elements (or entities), their properties, and their interrelationships are explicitly defined.

See also: Security Architecture.

assertion

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Explicit statement in a System Security policy that security measures in one security domain constitute an adequate basis for security measures (or lack of them) in another.

assignment

[FC Ver 1.0 Dec 1992]

Requirement in a protection profile taken directly as stated, without change, from the list of components or derived by placing a bound on a threshold definition.

> Note: The assignment of environment-specific requirements to generic component requirements is performed when a component requirement corresponds to an environment-specific requirement.

association-security-state

[ISO/IEC DIS 10745 May 1992]

The collection of information which is relevant to the control of communications security for a particular application-association.

assurance

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A more general term than "confidence" indicating the particular measures that can be taken to establish confidence.

assurance

[FC Ver 1.0 Dec 1992]

(See Profile Assurance and IT Product Assurance).

assurance

[ITSEC Ver 1.2 1991]

The confidence that may be held in the security provided by a Target of Evaluation.

assurance profile

[ITSEC Ver 1.2 1991]

An assurance requirement for a TOE whereby different levels of confidence are required in different security enforcing functions.

asymmetric authentication method

[ISO/IEC DIS 10181-2 Jul 1991]

Method for demonstrating knowledge of a secret, in which not all authentication information is shared by both entities.

attribute authority

[ECMA-138 Dec 1989]

An authority recognised in a security domain as a trusted source of attributes for entities within the domain. (See also Subject Authority).

audit

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

1. An independent review and examination of system records and activities in order to test for the adequacy of system security measures, to identify the degree of conformance with established security policy and operational procedures and to recommend any indicated changes in measures, policy and/or procedures.

2. Monitoring to detect and warn of events which might threaten security.

Note: The term "security audit" may be used to avoid ambiguity.

audit

[FC Ver 1.0 Dec 1992]

Independent review and examination of records and activities to determine compliance with established usage policies and to detect possible inadequacies in product technical security policies of their enforcement.

audit

[ISO 7498-2:1989]

See Security Audit

audit

[POSIX.6/D13 Nov 1992]

To generate the audit trail, read and interpret its contents, manage its storage, and control its generation.

audit authority

[ISO/IEC CD 10181-7 Aug 1992]

The manager responsible for defining those aspects of a security policy applicable to maintaining a security audit.

audit event

[POSIX.6/D13 Nov 1992]

An activity which may cause an audit record to be reported in an audit trail. The POSIX.6/D13.1 option specifies the audit events corresponding to POSIX.1 interfaces.

audit event type

[POSIX.6/D13 Nov 1992]

A field within an audit record that identifies the activity reported by the record, and defines the required content of the record.

audit ID

[POSIX.6/D13 Nov 1992]

An identifier for the individual user accountable for an audit event.

audit information

[ECMA-138 Dec 1989]

Information recording security events in the system.

audit record

[POSIX.6/D13 Nov 1992]

The discrete unit of data reportable in an audit trail on the occurrence of an audit event.

audit recorder function

[ISO/IEC CD 10181-7 Aug 1992]

A function that records the security-relevant messages in a security audit trail.

audit trail

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The set of records generated by a system in response to accounting operations, providing the basis for audit.

audit trail

[FC Ver 1.0 Dec 1992]

Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. [NSTISSI 4009]

audit trail

[ISO 7498-2:1989]

See Security Audit Trail

audit trail

[POSIX.6/D13 Nov 1992]

The destination of audit records that are recorded, and the source of records read by an audit post-processing application.

audit trail

[TCSEC Dec 1985]

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.

audit trail analyzer function

[ISO/IEC CD 10181-7 Aug 1992]

A function that checks a security audit trail in order to produce, if appropriate, security alarm messages.

audit trail archiver function

[ISO/IEC CD 10181-7 Aug 1992]

A function that archives a part of the security audit trail.

audit trail collector function

[ISO/IEC CD 10181-7 Aug 1992]

A function that collects individual audit trail records into a security audit trail.

audit trail examiner function

[ISO/IEC CD 10181-7 Aug 1992]

A function that builds security reports out of one or more security audit trails.

audit trail provider function

[ISO/IEC CD 10181-7 Aug 1992]

A function that provides security audit trails according to some criteria.

authenticate

[FC Ver 1.0 Dec 1992]

Verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT product.

authenticate

[POSIX.6/D13 Nov 1992]

To establish the validity of a claimed identity.

authenticate

[TCSEC Dec 1985]

To establish the validity of a claimed identity.

authenticated identity

[ISO/IEC DIS 10181-2 Jul 1991]

An identity of a principal that has been assured through authentication.

authentication

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The verification of a claimed identity.

Example: By the use of a password.

authentication

[ECMA-138 Dec 1989]

The process by which the identity of an entity is established.

authentication

[FC Ver 1.0 Dec 1992]

Means of verifying an entity's (e.g., individual user, machine, software component) eligibility to receive specific categories of information.

authentication

[ISO 7498-2:1989]

See data origin authentication, and peer entity authentication.

Note: In this part of 7498 the term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead.

authentication authority

[ECMA-138 Dec 1989]

An authority recognised in a security domain as a source of certified identities. (See also Subject Authority).

authentication certificate

[ISO/IEC DIS 10181-2 Jul 1991]

Authentication information in the form of a security certificate which may be used to assure the identity of an entity guaranteed by an authentication authority.

authentication exchange

[ISO 7498-2:1989]

A mechanism intended to ensure the identity of an entity by means of information exchange.

authentication exchange

[ISO/IEC DIS 10181-2 Jul 1991]

A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.

authentication information

[ISO 7498-2:1989]

Information used to establish the validity of a claimed identity.

authentication initiator

[ISO/IEC DIS 10181-2 Jul 1991]

The entity which starts an authentication exchange.

authentication policy

[ECMA TR/46 Jul 1988]

A set of rules, part of an access control policy, by which credentials are matched against claims of identity.

authentication responder

[ISO/IEC DIS 10181-2 Jul 1991]

The entity which receives the first transfer of exchange AI in an authentication exchange.

authority

[ECMA-138 Dec 1989]

An entity recognised by some set of secure systems as a trusted source of security information.

authorization

[ECMA TR/46 Jul 1988]

The granting of access to a security object.

authorization

[ECMA-138 Dec 1989]

The process by which an access control decision is made and enforced.

authorization

[FC Ver 1.0 Dec 1992]

Access rights granted to a user, program, or process. [NSTISSI 4009]

authorization

[ISO 7498-2:1989]

The granting of rights, which includes the granting of access based on access rights.

authorization policy

[ECMA TR/46 Jul 1988]

A set of rules, part of an access control policy, by which access by security subjects to security objects is granted or denied. An authorization policy may be defined in terms of access control lists, capabilities or attributes assigned to security subjects, security objects or both.

authorized

[FC Ver 1.0 Dec 1992]

Entitled to a specific mode of access.

automated information system (AIS)

[FC Ver 1.0 Dec 1992]

Any equipment or interconnected systems 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 computer software, firmware, and hardware. [NSTISSI 4009]

automatic data processing (ADP) system

[TCSEC Dec 1985]

An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

availability

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The prevention of denial of service.

availability

[FC Ver 1.0 Dec 1992]

Ability to access a specific resource within a specific time frame as defined within the IT product specification.

availability

[ISO 7498-2:1989]

The property of being accessible and useable upon demand by an authorized entity.

availability

[ITSEC Ver 1.2 1991]

The prevention of the unauthorised withholding of information or resources.

availability

[POSIX.6/D13 Nov 1992]

The property of an object being accessible and usable upon demand by an authorized subject.

bandwidth

[FC Ver 1.0 Dec 1992]

Rate at which information is transmitted through a channel. (See channel capacity)

Note: Bandwidth is originally a term used in analog communication, measured in Hertz, and related to information rate by the "sampling theorem" (generally attributed to H. Nyquist although the theorem was in fact known before Nyquist used it in communication theory). Nyquist's sampling theorem says that the information rate in bits (samples) per second is at most twice the bandwidth in Hertz of an analog signal created from a square wave. In a covert-channel context "bandwidth" is given in bits/second rather than Hertz and is commonly used, in an abuse of terminology, as a synonym for information rate.

bandwidth

[TCSEC Dec 1985]

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.

base standard

[POSIX.0/D15 Jun 1992]

A standard or specification that is recognized as appropriate for normative reference in a profile by the body adopting that profile, but is not a profile itself.

basic component

[ITSEC Ver 1.2 1991]

A component that is identifiable at the lowest hierarchical level of specification produced during Detailed Design.

Bell-La Padula security model

[FC Ver 1.0 Dec 1992]

Any formal state-transition model of a technical security policy for an AIS that presents (a) Access Constraints (including initial-state constraints and variants or the simple security and star properties), (b) allowed state transitions (called "rules of operation"), and (c) a proof that the allowed state transitions guarantee satisfaction of the constraints.

Bell-LaPadula model

[TCSEC Dec 1985]

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 to be "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. The clearance/classification scheme is expressed in terms of a lattice. See also: Lattice, Simple Security Property, *-Property.

binding of functionality

[ITSEC Ver 1.2 1991]

An aspect of the assessment of the effectiveness of a Target of Evaluation, namely the ability of its security enforcing functions and mechanisms to work together in a way which is mutually supportive and provides an integrated and effective whole.

capability

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A token allowing its holder an access right.

Note: Capability-based systems (eg PIDs) provide added value in authentication but, since they are not cryptographically secure, cannot replace the password system.

capability

[ECMA TR/46 Jul 1988]

As used in the context of security, a form of privilege attribute. It is a token (recognized by a process managing access to security objects) possession of which grants access to the security objects to which the token applies.

capability

[ECMA-138 Dec 1989]

A privilege attribute used as an identifier for a resource such that possession of the privilege attribute confers access rights for the resource.

capability

[ISO 7498-2:1989]

A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

category

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A component of a security clearance and/or security class used for computing access rights and controlling information flow by restricting access to the information to a specific group of subjects.

Note: [1] When more than one category is combined within a security class, access rights are granted only when all categories are present in the security clearance.

[2] Adding a category to a security class restricts the group of subjects who may have access.

[3] Codewords and Privacy and Restrictive markings may be represented by categories or caveats.

See also: Caveat, Classification, Dominance.

category

[FC Ver 1.0 Dec 1992]

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. [NSTISSI 4009]

Note: Examples include sensitive compartmented information and proprietary information. Individuals are granted access to special category information only after being granted formal access authorization.

caveat

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A component of a security clearance and/or security class used for computing access rights and controlling information flow by authorising a specific group of subjects to have access to the information.

Note: [1] When one or more caveats (of a given set) occurs within a security class, access rights are granted when:

a. at least one of the caveats is present in the security clearance and

b. the security clearance contains no caveat that is not also present in the security class.

(i.e., the caveats in the clearance are a non-empty subset of those in the security class).

[2] Adding a caveat to a group of caveats (of the same set) in a security class extends the group of subjects who may have access.

See also: Category, Classification, Dominance.

certificate

[ECMA-138 Dec 1989]

Security data sealed by an Authority. The certificate contains the security data and the seal.

certification

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The issue by the UK Certification Body of a formal statement, based on a review of the conduct and results of an evaluation, of the extent to which;

a. technical security measures meet the Security Requirement for a system, or

b. security claims are upheld by a product.

Note: A System Electronic Information Security policy is required as the basis for certification of a system.

See also: Accreditation, Confidence, Information Technology Security Evaluation and Certification Scheme.

certification

[FC Ver 1.0 Dec 1992]

Comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NSTISSI 4009]

certification

[ITSEC Ver 1.2 1991]

The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used were correctly applied.

certification

[TCSEC Dec 1985]

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 implementations meet a set of specified security requirements.

certification body

[ITSEC Ver 1.2 1991]

An independent and impartial national organisation that performs certification.

certification body (CB)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The Certification Body for the UK Evaluation and Certification Scheme is a joint CESG/DTI operation under a Scheme Management Board. Its principal role is to carry out the certification of the results of all evaluations of systems and products carried out under the auspices of the UK Scheme and to deal with other nations on the mutual recognition of such certificates.

certified identity

[ECMA-138 Dec 1989]

An identity in the form of an attribute in a certificate. The issuing authority will have authenticated the owner of the certificate.

certifier

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Person responsible for certification of a system and/or product.

channel

[ISO 7498-2:1989]

An information transfer path.

channel

[POSIX.6/D13 Nov 1992]

An information transfer path within a system. May also refer to the mechanism by which the path is effected.

channel

[TCSEC Dec 1985]

An information transfer path within a system. May also refer to the mechanism by which the path is effected.

channel capacity

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The rate at which information may be transmitted through a channel.

Note: Usually measured in bits per second.

channel capacity

[FC Ver 1.0 Dec 1992]

Maximum possible error-free rate, measured in bits per second, at which information can be sent along a communications path.

ciphertext

[ISO 7498-2:1989]

Data produced through the use of encipherment. The semantic content of the resulting data is not available.

Note: Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.

claim authentication information (claim AI)

[ISO/IEC DIS 10181-2 Jul 1991]

Information used by a claimant to generate exchange AI needed to authenticate a principal.

claimant

[ISO/IEC DIS 10181-2 Jul 1991]

An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

class

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

See: Security Class

classification

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

[1] A marking applied to information, indicating the estimated damage to the national interest that would be caused by its unauthorised disclosure, and used to determine the minimum standards of protection that should be applied.

[2] A component of a security clearance and/or security class used for computing access rights and controlling information flow.

Note: Access rights are granted when the classification element of the security clearance is greater than or equal to that of the security class.

See also: Category, Caveat, Dominance.

clear-text

[FC Ver 1.0 Dec 1992]

Intelligible data, the semantic content of which is available. [ISO]

clearance

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

See: Security Clearance.

cleartext

[ISO 7498-2:1989]

Intelligible data, the semantic content of which is available.

commercial licensed evaluation facility

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Evaluations conducted under UK Information Technology Evaluation and Certification Scheme may only take place in approved evaluation facilities. Commercial companies wishing to offer evaluation services may be licensed by the Certification Body of the Scheme as Commercial Licensed Evaluation Facilities.

communication interface

[POSIX.0/D15 Jun 1992]

That part of the API devoted to communications with other application software, external data transport facilities, and devices.

The services provided are those whose protocol state, syntax, and format all must be standardized for interoperability.

communications security

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Measures to ensure the confidentiality and integrity of information in telecommunications systems and channels.

See also: Electronic Information Systems Security.

community security policy

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The definition of the basic security principles and policy for a community of interconnected systems thereby allowing a series of bilateral SISPs to be produced while preserving the security of the whole.

See also: System Interconnection Security policy.

compartmented security mode

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A system operating in this mode is one whose users are all cleared for all the data stored on and/or processed by it, but who only need to have, and are only given, access to some of that data. This mode of operation is used mainly in the US.

component

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A self-contained part of a system that implements a set of functions.

component

[ITSEC Ver 1.2 1991]

An identifiable and self-contained portion of a Target of Evaluation.

component profile

[POSIX.0/D15 Jun 1992]

A profile that is made up of a defined subset of a single standard.

confidence

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A measure of the security of a trusted function, or a set of trusted functions, as calculated by a competent authority.

Note: For HMG purposes, the Head of the Certification Body of the UK Scheme is the "competent authority".

See also: Assurance, Confidence Level.

confidence level

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A measure of confidence as described in CESG Computer Security Memorandum No. 3 - "UK Systems Security Confidence Levels".

Note: ITSEC uses the term "assurance" rather than "confidence".

confidentiality

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The prevention of the unauthorized disclosure of information.

confidentiality

[ECMA TR/46 Jul 1988]

A security property of an object that prevents:

- its existence being known and/or

- its content being known.

This property is relative to some subject population and to some agreed degree of security.

confidentiality

[FC Ver 1.0 Dec 1992]

Assurance that information is not disclosed to inappropriate entities or processes.

confidentiality

[ISO 7498-2:1989]

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

confidentiality

[ITSEC Ver 1.2 1991]

The prevention of the unauthorised disclosure of information.

confidentiality

[POSIX.6/D13 Nov 1992]

The property that the existence of an object and/or its contents is not made available or disclosed to unauthorized subjects.

configuration

[FC Ver 1.0 Dec 1992]

Selection of one of the sets of possible combinations of features of a system. [ITSEC]

configuration

[ITSEC Ver 1.2 1991]

The selection of one of the sets of possible combinations of features of a Target of Evaluation.

configuration baseline

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Documentation that formally defines the configuration items of a system.

configuration control

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The process of evaluating, approving or disapproving, coordinating and recording changes to configuration items.

configuration control

[ITSEC Ver 1.2 1991]

A system of controls imposed on changing controlled objects produced during the development, production, and maintenance processes for a Target of Evaluation.

configuration item

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A collection of hardware and software elements of a system treated as a unit for the purpose of configuration management.

See also: Configuration Baseline.

configuration management

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The procedure by which a system is managed throughout its lifecycle to ensure that modifications to the design and implementation are made in a controlled manner and that the level of security originally achieved is maintained.

See also: Configuration Control.

configuration management board

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Group of people responsible for the management of changes to a system, to include assessment of their impact on security.

Note: The certifier should be represented on the Configuration Management Board for a certified system.

confinement

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The prevention of information flow.

construction

[ITSEC Ver 1.2 1991]

The process of creating a Target of Evaluation.

consumers

[FC Ver 1.0 Dec 1992]

Individuals or groups responsible for specifying requirements for IT product security (e.g., policy makers and regulatory officials, system architects, integrators, acquisition managers, product purchasers, and end users.

contextual information

[ISO/IEC CD 10181-3 Oct 1991]

Information derived from the context in which an access is made (e.g., time of day).

control attribute package

[ECMA-138 Dec 1989]

A collection of control attributes associated with a security object.

control attributes

[ECMA TR/46 Jul 1988]

Attributes, associated with a security object, that when matched against the privilege attributes of a security subject, are used to grant or deny access to the security object.

control attributes

[POSIX.6/D13 Nov 1992]

Attributes associated with an object that, when matched against security attributes of a subject, are used to grant or deny access to that object.

control objective

[FC Ver 1.0 Dec 1992]

Required result of protecting information within an IT product and its immediate environment.

corporate security policy

[ITSEC Ver 1.2 1991]

The set of laws, rules and practices that regulate how assets including the sensitive information are managed, protected and distributed within a user organisation.

correctness

[ITSEC Ver 1.2 1991]

A property of a representation of a Target of Evaluation such that it accurately reflects the stated security target for that system or product.

countermeasure

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Synonymous with Security Measure.

countermeasure

[FC Ver 1.0 Dec 1992]

Action, device, procedure, technique, or other measure that reduces the vulnerability of an AIS. [NSTISSI 4009]

covert channel

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A channel which allows information to flow in violation of the System Security policy.

Note: Covert channels can occur via mechanisms other than explicitly designed channels. For example, a covert timing channel may transmit information by inducing variations in system response time.

covert channel

[FC Ver 1.0 Dec 1992]

Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an AIS security policy. (See Covert channel and exploitable channel.) [NSTISSI 4009]

covert channel

[ITSEC Ver 1.2 1991]

The use of a mechanism not intended for communication to transfer information in a way which violates security.

covert channel

[POSIX.6/D13 Nov 1992]

A communications channel that allows a process to transfer information in a manner that violates the system’s security policy. A covert channel typically communicates by exploiting a mechanism not intended to be used for communication.

covert channel

[TCSEC Dec 1985]

A communications channel that allows a process to transfer information in a manner that violates the system’s security policy.

See also: Covert Storage Channel, Covert Timing Channel.

covert storage channel

[FC Ver 1.0 Dec 1992]

Covert channel that 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. [NSTISSI 4009]

> 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

[TCSEC Dec 1985]

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 storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

covert timing channel

[FC Ver 1.0 Dec 1992]

Covert channel in which one 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. [NSTISSI 4009]

covert timing channel

[TCSEC Dec 1985]

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.

credentials

[ECMA TR/46 Jul 1988]

Data that serve to establish the claimed identity of a security subjective relative to a given security domain.

credentials

[ISO 7498-2:1989]

Data that is transferred to establish the claimed identity of an entity.

critical mechanism

[ITSEC Ver 1.2 1991]

A mechanism within a Target of Evaluation whose failure would create a security weakness.

cryptanalysis

[ISO 7498-2:1989]

The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

cryptographic checkvalue

[ISO 7498-2:1989]

Information which is derived by performing a cryptographic transformation (see cryptography) on a data unit.

Note: The derivation of the checkvalue may be performed in one or more steps and is a result of a mathematical function of the key and data unit. It is usually used to check the integrity of a data unit.

cryptography

[ISO 7498-2:1989]

The discipline which embodies principles, means, and the methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

Note: Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or methods is cryptanalysis.

customer

[ITSEC Ver 1.2 1991]

The person or organisation that purchases a Target of Evaluation.

data

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Representations of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human and/or automatic means.

Note: The interpretation of data as information requires a convention (eg. a language).

data

[TCSEC Dec 1985]

Information with a specific physical representation.

data integrity

[ISO 7498-2:1989]

The property that data has not been altered or destroyed in an unauthorized manner.

data integrity

[TCSEC Dec 1985]

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.

decipherment

[ISO 7498-2:1989]

The reversal of a corresponding reversible encipherment.

decomposition

[FC Ver 1.0 Dec 1992]

Requirement in a protection profile that spans several components.

Note: The decomposition of a specific requirement becomes necessary when that requirement must be assigned to multiple components of the generic product requirements during the interpretation process.

decryption

[ISO 7498-2:1989]

See Decipherment.

dedicated security mode

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A system operating in this mode is one whose users are all cleared for, need to know about and have access to all the data stored on and/or processed by it.

See also: Multilevel Security Mode, System High Security Mode and Compartmented Security Mode.

default ACL

[POSIX.6/D13 Nov 1992]

An ACL which is used in determining the initial discretionary access control information for objects created within a directory.

definition

[FC Ver 1.0 Dec 1992]

An informal statement expressing the essential characteristics of one or more facts.

deliverable

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

An item produced or used during development of a system that is required to be made available to the evaluators for evaluation purposes.

Note: Includes support and access to computers.

delivery

[ITSEC Ver 1.2 1991]

The process whereby a copy of the Target of Evaluation is transferred from the developer to a customer.

demonstration

[FC Ver 1.0 Dec 1992]

An act or process of producing conclusive evidence for one or more facts. (A demonstration is more rigorous than an explanation and less rigorous than a proof).

denial of service

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

1. The unauthorized withholding of information or resources.

2. The prevention of legitimate access.

Note: This may result from either accidental or malicious causes.

denial of service

[ISO 7498-2:1989]

The prevention of authorized access to resources or the delaying of time-critical operations.

denial of service

[POSIX.6/D13 Nov 1992]

The unauthorized prevention of authorized access to resources or the delaying of time-critical operations.

departmental security officer

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The person responsible to the Permanent Head of a Government Department for establishing and enforcing Departmental Security policy; this includes the application of minimum standards of security and system accreditation.

dependency

[FC Ver 1.0 Dec 1992]

Condition in which the correctness of one or more functions (or assurances) is contingent (depends for its correctness) on the correctness of another function(s) (or assurances). Notion also used in describing the relationships among TCB subsets [NCSC-TG-021]. A TCB subset A depends for its correctness on TCB subset B if and only if the (engineering) arguments of the correct implementation of A with respect to its specification assume, wholly or in part, that the specification of B has been implemented correctly.

description

[FC Ver 1.0 Dec 1992]

An enumeration of facts and their characteristics.

descriptive top-level specification (DTLS)

[TCSEC Dec 1985]

A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

descriptor

[POSIX.6/D13 Nov 1992]

An internal representation which uniquely identifies data objects.

designated approving authority (DAA)

[FC Ver 1.0 Dec 1992]

Official with the authority to formally assume responsibility for operating an IT product, an AIS, or network at an acceptable level of risk.

detailed design

[ITSEC Ver 1.2 1991]

A phase of the Development Process wherein the top level definition and design of a Target of Evaluation is refined and expanded to a level of detail that can be used as a basis for implementation.

developer

[ITSEC Ver 1.2 1991]

The person or organisation that manufacturers a Target of Evaluation.

developer security

[ITSEC Ver 1.2 1991]

The physical, procedural and personnel security controls imposed by a developer on his Development Environment.

development assurance

[FC Ver 1.0 Dec 1992]

Sources of IT product assurance ranging from how a product was designed and implemented to how it is tested, operated and maintained.

development assurance component

[FC Ver 1.0 Dec 1992]

Fundamental building block, specifying how an IT product is developed, from which development assurance requirements are assembled.

development assurance package

[FC Ver 1.0 Dec 1992]

Grouping of development assurance components assembled to ease specification and common understanding of how an IT product is developed.

development assurance requirements

[FC Ver 1.0 Dec 1992]

Requirements in a protection profile which address how each conforming IT product is developed including the production of appropriate supporting developmental process evidence and how that product will be maintained.

development environment

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The set of procedures, methods, tools and standards used during system development.

See also: Operational Environment.

development environment

[ITSEC Ver 1.2 1991]

The organisational measures, procedures and standards used whilst constructing a Target of Evaluation.

development process

[ITSEC Ver 1.2 1991]

The set of phases and tasks whereby a Target of Evaluation is constructed, translating requirements into actual hardware and software.

digital fingerprint

[ISO/IEC CD 10181-1:Dec 1992]

A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that will possess the same characteristics.

digital fingerprint

[ISO/IEC DIS 10181-2 Jul 1991]

A characteristic of a data item, such as a cryptographic check-value or a result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that will possess the same characteristic.

digital signature

[ISO 7498-2:1989]

Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

disabled

[POSIX.6/D13 Nov 1992]

When applied to privilege: a privilege that is inactive, i.e., has its effective flag cleared.

disciplined development

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Development of a system or part of a system where the documentation and evidence of testing against the documentation is to normal industry standards.

See also: Rigorous, Structured, Verified Development.

discretionary access control

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Access control based on access rights granted by users other than the System Security Officer.

Note: [1] Normally enforced by reference to the identity of users and the groups to which they belong.

[2] A subject with an access right may pass it to another subject, unless

a. prevented by Mandatory Access Control or

b. constrained from so doing by an explicit System Security Policy (perhaps backed up by audit).

discretionary access control

[FC Ver 1.0 Dec 1992]

Methods of restricting access to objects or other resources based primarily on the instructions of arbitrary unprivileged users.

discretionary access control

[TCSEC Dec 1985]

A means of restricting access to objects based on the identity 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 (unless restrained by mandatory access control).

discretionary access control (DAC)

[POSIX.6/D13 Nov 1992]

A means of restricting access to objects. The restrictions are discretionary in the sense that the subjects granted/denied access, and the type of access granted/denied, are at the discretion of the object owner. In many systems, the controls are also discretionary in the sense that a subject with a certain access permission is capable of passing that permission on to any other subject.

distinguishing identifier

[ISO/IEC DIS 10182-2]

Data which unambiguously distinguishes an entity in the authentication process. This [Recommendation | Part of this International Standard] requires that such an identifier be unambiguous at least within a security domain.

distributed application

[ECMA TR/46 Jul 1988]

A set of information processing resources distributed over one or more open systems which provides a well defined set of functionality to (human) users, to assist a given (office) task.

documentation

[ITSEC Ver 1.2 1991]

The written (or otherwise recorded) information about a Target of Evaluation required for an evaluation. This information may, but need not, be contained within a single document produced for the specified purpose.

domain

[FC Ver 1.0 Dec 1992]

Unique context (e.g., access control parameters) in which a program is operating.

> Note: A subject's domain determines which access-control attributes an object must have for a subject operating in that domain to have a designated form of access.

domain

[TCSEC Dec 1985]

The set of objects that a subject has the ability to access.

dominance

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Term used to describe the relationship between security clearances and security classes or between different security classes. Access rights are normally only granted when a subject dominates an object; information flow is allowed only to a receiving object that dominates the source object.

See also: Lattice.

dominate

[POSIX.6/D13 Nov 1992]

An implementation-defined relation between the values of MAC labels or Information Labels which satisfies partial order algebraic property.

dominate

[TCSEC Dec 1985]

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.

downgrade

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Change the security class of an object to one which does not dominate the original.

downgrade

[POSIX.6/D13 Nov 1992]

To change a MAC label or Information Label to a value that does not dominate the current label. Downgrade includes changing a label to value that is incomparable with the current label.

ease of use

[ITSEC Ver 1.2 1991]

An aspect of the assessment of the effectiveness of a Target of Evaluation, namely that it cannot be configured or used in a manner which is insecure but which an administrator or end-user would reasonably believe to be secure.

echo suppression

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The procedure by which characters entered into a system are not physically revealed.

Note: Often employed when passwords are entered so that they are not disclosed to casual observers.

effectiveness

[ITSEC Ver 1.2 1991]

A property of a Target of Evaluation representing how well it provides security in the context of its actual or proposed operational use.

electronic emission security (ELSEC)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The technical and non-technical measures taken to protect all classified non-communications electromagnetic emissions. It also takes account of the security aspects of any directly associated electromagnetic communications transmissions.

electronic information processing system (EIP System)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

An assembly of computer hardware, software and firmware, configured for the purpose of processing, storing or forwarding information.

Note: [1] The term embraces all sorts of computer systems (with or without links to remote sites), networks and also a wide range of electronic equipment capable of processing, storing or forwarding information, including message switches, personal computers and word processors.

[2] EIP systems are now more commonly called IT systems.

electronic information systems security (INFOSEC)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The technical measures to ensure the security of information handled by communications, non-communications and computer systems.

Note: A general term covering COMSEC, COMPUSEC, TEMPEST and ELSEC.

electronic security environment

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The ESE defines the system in security terms, identifying boundaries of security significance. These boundaries may be:

a. internal, ie, security partitions within the system, or

b. external, ie manual or electronic interfaces to the LSE or the GSE (eg terminals, printers or communications lines to other systems).

emerging standard

[POSIX.0/D15 Jun 1992]

A specification that is under consideration by an accredited standards body, but has not completed the process of approval by the sponsoring body.

Emerging standards are often subject to significant change prior to approval.

enabled

[POSIX.6/D13 Nov 1992]

When applied to privilege: a privilege that is active, i.e., has its effective flag set.

encapsulated object

[FC Ver 1.0 Dec 1992]

A data structure whose existence is known, but whose internal organization is not accessible, except by invoking the encapsulated subsystem that manages it.

encapsulated subsystem

[FC Ver 1.0 Dec 1992]

A collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the encapsulated subsystem that the procedures may be called only at designated domain entry points. Encapsulated subsystem, protected subsystem, and protected mechanisms of the TCB are terms that may be used interchangeably.

encipherment

[ISO 7498-2:1989]

The cryptographic transformation of data (see cryptography) to produce ciphertext.

Note Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

encryption

[ISO 7498-2:1989]

See encipherment.

end-to-end encipherment

[ISO 7498-2:1989]

Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (See also link-by-link encipherment.)

end-user

[ITSEC Ver 1.2 1991]

A person in contact with a Target of Evaluation who makes use only of its operational capacity.

environment

[FC Ver 1.0 Dec 1992]

All entities (users, procedures, conditions, objects, AISs, other IT products) that interact with (affect the development, operation and maintenance of) that IT product.

equivalent

[POSIX.6/D13 Nov 1992]

An implementation-defined relation between the values of MAC labels or of Information Labels. Two labels are equivalent if each of the labels dominates the other.

evaluation

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The detailed examination of a system or a product to search for vulnerabilities and to determine the extent to which the required or claimed security functions are upheld by its implementation.

Note: [1] Security functions are normally described in a System Electronic Information Security Policy, which forms the basis of the evaluation baseline.

[2] The examination may cover aspects of the development and operational environment.

See also: Certification, Information Technology Security Evaluation and Certification Scheme.

evaluation

[FC Ver 1.0 Dec 1992]

Technical assessment of a component's, product's, subsystem's, or system's security properties that establishes whether or not the component, product, sub-system, or system meets a specific set of requirements.

Note: Evaluation is a term that causes much confusion in the security community, because it is used in many different ways. It is sometimes used in the general English sense (judgement or determination of worth or quality). Based on common usage of the term in the security community, one can distinguish between two types of evaluation: (1) evaluations that exclude the environment, and (2) evaluations that include the environment. This second type of evaluation, an assessment of a system's security properties with respect to a specific operational mission, is termed certification within this document. Evaluations that exclude the environment, the type of evaluations considered herein, are assessments of the security properties against a defined criteria.

evaluation

[ITSEC Ver 1.2 1991]

The assessment of an ITSEC system or product against defined evaluation criteria.

evaluation assurance

[FC Ver 1.0 Dec 1992]

Source of IT product assurance based on the kind and intensity of the evaluation analysis performed on the product.

evaluation assurance component

[FC Ver 1.0 Dec 1992]

Fundamental building block, specifying the type and the rigor of required evaluation activities, from which evaluation assurance requirements are assembled.

evaluation assurance package

[FC Ver 1.0 Dec 1992]

Grouping of evaluation assurance components assembled to ease specification and common understanding of the type and the rigor of required evaluation activities.

evaluation assurance requirements

[FC Ver 1.0 Dec 1992]

Requirements in a protection profile which address both the type and the rigor of activities that must occur during product evaluation.

evaluation baseline

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Documentation that formally defines the security functions of a system or product against which its evaluation is performed.

Note: A System Electronic Information Security Policy forms the basis of the evaluation baseline for a system.

evaluation observation report (EOR)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Report issued by a CLEF to report any problem, other than those already covered by an SFN, relating to the Target of Evaluation (TOE). Initial distribution should be to the UK Certification Body.

See also: Security Fault Notification.

evaluation unit

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

An organisation working directly for CESG whose purpose is to perform evaluations.

evaluator

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Member of an Evaluation Facility assigned to a particular evaluation.

evaluator

[ITSEC Ver 1.2 1991]

The independent person or organisation that performs an evaluation.

evaluator actions

[ITSEC Ver 1.2 1991]

A component of the evaluation criteria for a particular phase or aspect of evaluation, identifying what the evaluator must do to check the information supplied by the sponsor of the evaluator, and the additional activities he must perform.

evaluators

[FC Ver 1.0 Dec 1992]

Individuals or groups responsible for the independent assessment of IT product security (e.g., product evaluators, system security officers, system certifiers, and system accreditors).

exchange authentication information (exchange AI)

[ISO/IEC DIS 10181-2 Jul 1991]

Information exchanged between a claimant and a verifier during the process of authenticating a principal.

explanation

[FC Ver 1.0 Dec 1992]

A description and its justification; an enumeration of facts, their characteristics, and their cause or reason. (An explanation is less rigorous than both a demonstration and a proof.)

explicit services

[POSIX.0/D15 Jun 1992]

Services that can be accessed from an application program, via an API, and are generally provided only when requested.

exploitable channel

[FC Ver 1.0 Dec 1992]

Covert channel that is usable or detectable by subjects external to the AIS's trusted computing base and can be used to violate the AIS's technical security policy. (See covert channel.)

exploitable channel

[TCSEC Dec 1985]

Any channel that is usable or detectable by subjects external to the Trusted Computing Base.

exportable data

[POSIX.6/D13 Nov 1992]

Opaque data, originally created by the system, for which certain minimal characteristics are defined.

Exportable data is self-contained and persistent. As a result, it can be copied or stored freely.

extended ACL

[POSIX.6/D13 Nov 1992]

An ACL that contains other entries in addition to the required entries.

external environment

[POSIX.0/D15 Jun 1992]

A set of external entities to the application platform with which information is exchanged.

External entities include people, exchangeable media that is not mounted in the platform, communication wiring, and all other platforms.

external environment interface (EEI)

[POSIX.0/D15 Jun 1992]

The interface between the application platform and the external environment across which information is exchanged.

The External Environment Interface is defined primarily in support of system and application interoperability.

The primary services present at the External Environment Interface comprise:

- Human/Computer Interaction Services
- Information Services
- Communication Services

external security controls

[FC Ver 1.0 Dec 1992]

Measures which include physical, personnel, procedural, and administrative security requirements and a separate certification and accreditation process that govern physical access to an IT product.

> Note: These measures constitute assumptions and boundary conditions that are part of the environment described in a protection profile.

fence

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The boundary of a trusted region.

fence penetrability

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The ability of features outside a trusted region to penetrate a fence - thus leading to a potential or actual breach of the System Security Policy.

file ACL class

[POSIX.6/D13 Nov 1992]

The property of a file indicating access permissions for a process related to the process' user or group identification.

A process is in the file acl class of a file if the process is not in the file owner class and the effective user ID of the process matches the user ID of a user entry in the ACL associated with the file; or if the process is not in the file owner or file group class and the effective group ID or one of the supplementary group IDs of the process matches a group ID of a group entry in the ACL associated with the file.

file other class

[POSIX.6/D13 Nov 1992]

The property of a file indicating access permissions for a process related to the process' user and group identification.

A process is in the file other class of a file if the process is not in the file owner class, file group class, or file acl class.

file privilege attribute

[POSIX.6/D13 Nov 1992]

A per-file privilege value that specifies global behaviour for all privileges defined in the implementation.

file privilege flag

[POSIX.6/D13 Nov 1992]

A per-privilege attribute of a file that is used during exec() processing in computing the privileges of any process executing that file.

file privilege state

[POSIX.6/D13 Nov 1992]

A state variable that identifies a value for all defined file privilege flags for all privileges defined in an implementation and a value for all file privilege attributes defined in an implementation.

flaw

[FC Ver 1.0 Dec 1992]

Error of commission, omission, or oversight in an IT product that may allow protection mechanisms to be bypassed.

flaw

[TCSEC Dec 1985]

An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed.

flaw hypothesis methodology

[TCSEC Dec 1985]

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 the ease of exploiting it and on the extent of control or compromise it would provide. The prioritized list is used to direct the actual testing of the system.

formal model of security policy

[ITSEC Ver 1.2 1991]

An underlying model of security policy expressed in a formal style, i.e. an abstract statement of the important principles of security that a TOE will enforce.

formal proof

[TCSEC Dec 1985]

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.

formal security policy model

[FC Ver 1.0 Dec 1992]

Mathematically precise statement consisting of (a) a formal technical security policy (given by constraints on a Product's external interface and/or constraints on the handling of controlled entities internal to the Product), (b) rules of operation that show how the definition of security is to be enforced, and (c) a formal proof showing that the rules of operation guarantee satisfaction of the definition of security. [NCSC-TG-010]

formal security policy model

[POSIX.6/D13 Nov 1992]

A mathematically precise statement of a system security policy. Some formal modelling techniques include: state transition models, temporal logic models, denotational semantics models, and algebraic specification models.

formal security policy model

[TCSEC Dec 1985]

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 s "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 in reference [2].

See also: Bell-LaPadula Model, Security Policy Model.

formal specification

[FC Ver 1.0 Dec 1992]

Statement about a product made using the restricted syntax and grammar of a formal reasoning system and a set of terms that have been precisely and uniquely defined of specified.

> Note: The formal statement should be augmented by an informal explanation of the conventions used and the ideas being expressed. A well-formed syntax and semantics with complete specification of all constructs used must be referenced.

formal top-level specification (FTLS)

[TCSEC Dec 1985]

A Top-Level Specification that is written in a formal mathematical language to allow theorems showing correspondence of the system specification to its formal requirements to be hypothesized and formally proven.

formal verification

[TCSEC Dec 1985]

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.

front-end security filter

[TCSEC Dec 1985]

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.

functional component

[FC Ver 1.0 Dec 1992]

Fundamental building block, specifying what an IT product must be capable of doing, from which functional protection requirements are assembled.

functional package

[FC Ver 1.0 Dec 1992]

Grouping of functional components assembled to ease specification and common understanding of what an IT product is capable of doing.

functional protection requirements

[FC Ver 1.0 Dec 1992]

Requirements in a protection profile which address what conforming IT products must be capable of doing.

functional testing

[TCSEC Dec 1985]

The portion of security testing in which the advertised features of a system are tested for correct operation.

functional unit

[ITSEC Ver 1.2 1991]

A functionally distinct part of a basic component.

functionality

[FC Ver 1.0 Dec 1992]

Set of functional protection requirements to be implemented in IT products.

functionality class

[ITSEC Ver 1.2 1991]

A predefined set of complimentary security enforcing functions capable of being implemented in a Target of Evaluation.

general–purpose system

[TCSEC Dec 1985]

A computer system that is designed to aid in solving a wide variety of problems.

generic threat

[FC Ver 1.0 Dec 1992]

Class of threats with common characteristics pertaining to vulnerabilities, agents, event sequences, and resulting misfortunes.

global security environment

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A security domain in a System Security policy. The GSE is the general security environment in which the system is located. It covers everything outside the control of the System or Project Manager which may have a bearing on the security of the system and which is therefore deemed to be the responsibility of the DSO.

See also: Electronic Security Environment, Local Security Environment.

granularity

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A measure of the fineness or coarseness of definition and implementation of a System Security policy.

granularity

[FC Ver 1.0 Dec 1992]

Relative fineness or coarseness to which an access control mechanism or other IT product aspect can be adjusted.

Note: Protection at the file level is considered course granularity, whereas protection at the field level is considered to be finer granularity.

granularity

[TCSEC Dec 1985]

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.

granularity of a requirement

[FC Ver 1.0 Dec 1992]

Determination of whether a requirement applies to all the attributes of users, subjects or objects, and all TCB functional components.

group

[FC Ver 1.0 Dec 1992]

Named collection of user identifiers.

hardware

[POSIX.0/D15 Jun 1992]

Physical equipment used in data processing as opposed to programs, procedures, rules, and associated documentation.

harmonization

[POSIX.0/D15 Jun 1992]

The process of making separate profiles consistent with one another in areas where they overlap.

hash function

[ISO/IEC CD 10181-1:Dec 1992]

A function that maps values from a (possibly very) large set of values to a smaller range of values.

hash function

[ISO/IEC DIS 10181-2 Jul 1991]

A (mathematical) function which maps values from a (possibly very) large set of values into a smaller range of values.

human/computer interface

[POSIX.0/D15 Jun 1992]

The boundary across which physical interaction between a human being and the application platform takes place.

identification

[FC Ver 1.0 Dec 1992]

Process that enables recognition of an entity by an IT product.

identity

[ECMA-138 Dec 1989]

A unique piece of information which is recognised as denoting a particular entity within a security domain. The identity information is only unique within the domain.

identity-based security policy

[ISO 7498-2:1989]

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.

implementation

[ITSEC Ver 1.2 1991]

A phase of the Development Process wherein the detailed specification of a Target of Evaluation is translated into actual hardware and software.

implicit services

[POSIX.0/D15 Jun 1992]

Services that a platform provides without a direct request.

incomparable

[POSIX.6/D13 Nov 1992]

An implementation-defined relation between the values of MAC labels or Information Labels. Two labels are incomparable if neither label dominates the other, that is the two labels are disjoint.

independent security domains

[ECMA-138 Dec 1989]

Two security domains are independent if and only if:

- they are administered by different administrations, and:
- no dependency relationship exists between the security domains.

inference

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Indirect access to information, without access to the data which represents it.

informal specification

[FC Ver 1.0 Dec 1992]

Statement about (the properties of) a product made using the grammar, syntax, and common definitions of a natural language (e.g., English).

> Note: While no notational restrictions apply, the informal specification is also required to provide defined meanings for terms which are used in a context other than that accepted by normal usage.

information

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The meaning assigned to data by means of the convention and context used in its representation.

Note: Information is represented by data and is not directly accessible except through data.

information flow

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

See Covert Channels.

information label

[POSIX.6/D13 Nov 1992]

The item visible at the POSIX.6/D13.1 interface that is used for associating labelling information with object data. This information is not related to mandatory access control.

information label floating

[POSIX.6/D13 Nov 1992]

The operation whereby one information label is combined with another information label. The specific algorithm used to define the result of a combination of two labels is implementation defined.

information label policy

[POSIX.6/D13 Nov 1992]

The implementation-defined policy that determines to what degree information labels associated with data are automatically adjusted as data flows through the system.

information protection policy

[FC Ver 1.0 Dec 1992]

Set of laws, rules, and practices that regulate how an IT product will, within specified limits, counter threats expected in the product’s assumed operational environment.

information technology security evaluation criteria (ITSEC)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The European ITSEC represent the harmonised evaluation criteria for secure products and systems for use within the European Community (EC). These criteria encompass both functionality and assurance ("correctness" and "effectiveness") aspects of IT security and form the basic standards against which UK evaluations and certifications are carried out within the UK IT Security Evaluation and Certification Scheme.

information technology security evaluation manual (ITSEM)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The methodology to complement the ITSEC.

information technology security evaluation and certification scheme

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The UK IT Security Evaluation and certification Scheme (known as "the Scheme") is designed to meet the needs of UK Government and Industry for cost effective and efficient security evaluation of IT products and systems and to provide a basis for mutual international recognition of evaluation and certification results, based on the European harmonised Information technology Security Evaluation Criteria. In particular, the Scheme has been adopted by HMG for the certification of all UK systems used to store, process or forward nationally classified information.

information technology systems (IT Systems)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Synonymous with EIP Systems (qv)

initial system security policy

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A preliminary statement of the basic security-relevant facts about a system.

Note: An initial System Security Policy constitutes the basis for the Departmental Security Officer's risk assessment and Security requirement.

initiator

[ISO/IEC CD 10181-3 Oct 1991]

An entity (e.g., human user or computer based entity) that attempts to access other entities.

initiator access control decision information (initiator ADI)

[ISO/IEC CD 10181-3 Oct 1991]

ADI associated with the initiator.

initiator access control information (initiator ACI)

[ISO/IEC CD 10181-3 Oct 1991]

Access control information relating to the initiator.

integrity

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The prevention of the unauthorised creation, amendment or deletion of information.

integrity

[ECMA TR/46 Jul 1988]

A security property of an object that prevents or is used to prevent:

- its condition of existence being changed and/or
- its contents being changed.

This property is relative to some subject population and to some agreed degree of security.

integrity

[FC Ver 1.0 Dec 1992]

Correctness and appropriateness of the content and/or source of a piece of information.

integrity

[ISO 7498-2:1989]

See Data Integrity.

integrity

[ITSEC Ver 1.2 1991]

The prevention of the unauthorised modification of information.

integrity

[POSIX.6/D13 Nov 1992]

The property that the existence of an object and/or its contents not be destroyed or altered by an unauthorized user. Also, the property that the contents of an object not be altered to unauthorized values.

interdomain authority

[ECMA-138 Dec 1989]

an authority recognised by two or more Security Administrations as a trusted source of security information used between the respective Security Domains.

interface

[POSIX.0/D15 Jun 1992]

The shared boundary between two functional units, defined by functional characteristics and other characteristics, as appropriate.

internal security controls

[FC Ver 1.0 Dec 1992]

Mechanisms implemented in the hardware, firmware, and software of an IT product which provide protection for the IT product.

internationalization

[POSIX.0/D15 Jun 1992]

The process of designing and developing a product with a set of features, functions, and options intended to facilitate the adaption of the product to satisfy a variety of cultural environments.

interoperability

[POSIX.0/D15 Jun 1992]

The ability of two or more systems to exchange information and to mutually use the information that has been exchanged.

key

[ISO 7498-2:1989]

A sequence of symbols that controls the operations of encipherment and decipherment.

key management

[ISO 7498-2:1989]

The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

label

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A machine readable representation of a marking.

language-binding API

[POSIX.0/D15 Jun 1992]

The interface between applications and application platforms based on language-independent binding APIs and consistent with the paradigms used for a specific programming language.

language-independent service specification

[POSIX.0/D15 Jun 1992]

A specification that facilitates the management and development of consistent language-binding standards.

lattice

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A partially ordered mathematical set for which every pair of elements has a greater lower bound and a least upper bound.

Note: A lattice may be used to represent the relationship between security classes. A security clearance specifies the least upper bound of security classes of objects for which access rights may be granted.

See also: Dominance.

lattice

[TCSEC Dec 1985]

A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound.

least privilege

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The principle of granting only such access rights as are required for subjects to perform their authorised tasks.

Note: Extension of the principle of need-to-know covering all access rights, not just "read access".

See also: Role.

least privilege

[FC Ver 1.0 Dec 1992]

Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. [NSTISSI 4009]

Note: Application of this principle limits the damage that can result from accident, error, or unauthorized use of an AIS.

least privilege

[TCSEC Dec 1985]

This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

life cycle

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The phases of development and operation of a system from the initial concept to final disposal.

link-by-link encipherment

[ISO 7498-2:1989]

The individual application of encipherment to data on each link of a communications system.

Not: The implication of link-by-link encipherment is that the data will be in cleartext form in relay entities.

See also: End-To-End Encipherment.

local adaption

[POSIX.0/D15 Jun 1992]

The process of modifying a product that has hard-coded biases of one culture to the hard-coded biases of another culture.

local security environment

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

That part of the security domain of a system which is under the control of the System Manager.

See also: Electronic Security Environment, Global Security Environment.

locale

[POSIX.0/D15 Jun 1992]

A description of a cultural environment.

localization

[POSIX.0/D15 Jun 1992]

The process of utilizing the internationalization features to create a version of a product for a specific culture.

MAC label

[POSIX.6/D13 Nov 1992]

An attribute of a subject or object which represents the sensitivity of the subject or object and is used for mandatory access control decisions. The contents of MAC labels are implementation defined.

mandatory access control

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Access control based on access rights granted by the System Security Officer.

Note: Normally enforced by reference to security clearances of subjects and security classes of objects in accordance with the rules specified in the System Security Policy.

mandatory access control

[FC Ver 1.0 Dec 1992]

Means of restricting access to objects based on the sensitivity (as represented by a la- bel) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. (See non-discretionary access control.)

mandatory access control

[TCSEC Dec 1985]

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.

mandatory access control (MAC)

[POSIX.6/D13 Nov 1992]

A means of restricting access to objects based on their MAC labels and the use of the implementation-defined dominate operator. The restrictions are mandatory in the sense that they are always imposed by the system, while discretionary access control is imposed at the discretion of the object owner.

manipulation detection

[ISO 7498-2:1989]

A mechanism which is used to detect whether a data unit has been modified (either accidently or intentionally).

marking

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Human readable word or phrase acting as an indicator of all or part of the security constraints that apply to a document so marked.

See also: Label.

masquerade

[ISO 7498-2:1989]

The pretence by an entity to be a different entity.

mechanism

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The software, hardware, procedures, etc. by which a function (eg. a security function) is implemented.

mechanism

[FC Ver 1.0 Dec 1992]

Operating system entry point or separate operating system support program that performs a specific action or related group of actions.

minimum ACL

[POSIX.6/D13 Nov 1992]

An ACL that contains only the required entries.

minimum standards

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

National Security standards which must be observed by all Government Departments and List X companies so that they may pass information to each other with confidence that it will be handled with adequate care by all recipients.

Note: minimum computer security standards are based on a risk assessment combined with an assessment of the value of assets to be protected.

multi-class

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Comprising or containing information of more than one security class.

multi-class device

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A device required to store or process information of more than one security class simultaneously.

multilevel device

[TCSEC Dec 1985]

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.

multilevel secure

[TCSEC Dec 1985]

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users obtaining access to information for which they lack authorization.

multilevel security (MLS) Mode

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A system operating in this mode is one which stores and/or processes data at various classifications etc, but for which there are users not cleared for or who need to know about all the data and whose access is restricted appropriately.

See also: Dedicated Security Mode, System High Security Mode, Compartmented Security Mode.

need-to-know

[FC Ver 1.0 Dec 1992]

Access to, or knowledge or possession of, specific information required to carry out official duties. [NSTISSI 4009]

need-to-know

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

1. Security principle that the dissemination of classified information should be no wider than is required for the efficient conduct of the business in hand and restricted to those who are authorised to have access.

2. Access right granted in accordance with this principle.

See also: Least Privilege.

node

[ECMA TR/46 Jul 1988]

A data processing facility that provides information processing resources as part of a network. A node may support user application processes, server application processes or a combination of both kinds of processes.

non-discretionary access control

[FC Ver 1.0 Dec 1992]

Means of restricting access to objects based largely on administrative actions.

normal operation

[FC Ver 1.0 Dec 1992]

Process of using a system. [ITSEC]

notarization

[ISO 7498-2:1989]

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.

object

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A passive entity within a system that contains or receives information.

Examples: records, blocks, pages, segments, files, etc.

Note: [1] Access to an object implies potential access to the information it contains.

[2] An entity (eg a program) may be both a subject and an object. Which it is depends on consideration of the type of access in which it participates.

[3] The range of valid objects is restricted by the available types of operations that can be performed, eg read, write, execute, etc.

See also: Subject.

object

[ECMA TR/46 Jul 1988]

Abbreviation of security object.

object

[FC Ver 1.0 Dec 1992]

Controlled entity that precisely gives or receives information in response to access attempts by another (active) entity.

Note: Access to an object implies access to the information contained in that object. Examples of objects include: subjects, records, blocks, pages, segments, files, directories, directory trees and programs, as well as bits, bytes, words, fields, processors, I/O devices, video displays, keyboards, clocks, printers, and network nodes.

object

[ITSEC Ver 1.2 1991]

A passive entity that contains or receives information.

object

[POSIX.6/D13 Nov 1992]

A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains.

Examples of items that may be considered 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.

object

[TCSEC Dec 1985]

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.

object encapsulation

[FC Ver 1.0 Dec 1992]

viz., encapsulated object.

object reuse

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Reuse of a storage medium for a different object.

Note: [1] A vulnerability may exist if the medium contains residual data from a previous object.

[2] This is now the accepted term, despite the fact that it is the storage medium, not the object, that is reused.

See also: Purge.

object reuse

[TCSEC Dec 1985]

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).

off-line authentication certificate

[ISO/IEC DIS 10181-2 Jul 1991]

A particular form of authentication information binding an entity to a cryptographic key, certified by a trusted authority, which may be used for authentication without directly interacting with the authority.

on-line authentication certificate

[ISO/IEC DIS 10181-2 Jul 1991]

A particular form of authentication information,certified by a trusted authority, which may be used for authentication following direct interaction with the authority

one-way encryption

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A method of encryption used where a requirement exists to prevent the decryption of the cipher text, given full information about the algorithm.

Note: Often used for encryption of passwords and integrity checksums.

one-way function

[ISO/IEC CD 10181-1:Dec 1992]

A function which is easy to compute but whose inverse is computationally intractable.

one-way function

[ISO/IEC DIS 10181-2 Jul 1991]

A (mathematical) function which is easy to compute but whose inverse is computationally intractable.

one-way regulator

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A component which allows the transfer of information from one system to another, whilst providing a high level of confidence that information flow in the reverse direction is prevented.

Note: [1] Used where the security class of the receiving system dominates that of the sender.

[2] The CESG OWR development programme aims to satisfy this requirement.

opaque data objects

[POSIX.6/D13 Nov 1992]

A mechanism by which a program can manipulate data structures of any format, without knowing what that format might be.

open specifications

[POSIX.0/D15 Jun 1992]

Public specifications that are maintained by an open, public consensus process to accommodate new technologies over time and that are consistent with international standards.

open system

[POSIX.0/D15 Jun 1992]

A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software:

- to be ported with minimal changes across a wide range of systems
- to interoperate with other applications on local and remote systems
- to interact with users in a style that facilitates user portability.

open system application program interface

[POSIX.0/D15 Jun 1992]

A combination of standards-based interfaces specifying a complete interface between an application program and the underlying application platform.

open system environment (OSE)

[POSIX.0/D15 June 1992]

The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or portability of applications, data, or people, as specified by information technology standards and profiles.

operating procedure

[ITSEC Ver 1.2 1991]

A set of rules defining the correct use of a Target of Evaluation.

operation

[ITSEC Ver 1.2 1991]

The process of using a Target of Evaluation.

operational documentation

[ITSEC Ver 1.2 1991]

The information produced by the developer of a Target of Evaluation to specify and explain how customers should use it.

operational environment

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The set of procedures, methods, tools and standards used during system operation.

See also: Development Environment.

operational environment

[ITSEC Ver 1.2 1991]

The organisational measures, procedures and standards to be used whilst operating a Target of Evaluation.

orange book

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Nickname name for the United States Department of Defense "Trusted Computer System Evaluation Criteria".

organizational security policy

[FC Ver 1.0 Dec 1992]

Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

output

[TCSEC Dec 1985]

Information that has been exported by a TCB.

overt channel

[FC Ver 1.0 Dec 1992]

Communications path within a computer system or network that is designed for the authorized transfer of data. (See covert channel) [NSTISSI 4009]

owner

[FC Ver 1.0 Dec 1992]

User granted privileges with respect to security attributes and privileges affecting specific subjects and objects.

passive threat

[ISO 7498-2:1989]

The threat of unauthorized disclosure of information without changing the state of the system.

password

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A character string used for authentication.

password

[FC Ver 1.0 Dec 1992]

Protected/private character string used to authenticate an identity or to authorize access to data. [NSTISSI 4009]

password

[ISO 7498-2:1989]

Confidential authentication information, usually composed of a string of characters.

password

[POSIX.6/D13 Nov 1992]

A private character string that is used to authenticate an identity.

password

[TCSEC Dec 1985]

A private character string that is used to authenticate an identity.

peer-entity authentication

[ISO 7498-2:1989]

The corroboration that a peer entity in an association is the one claimed.

penetration test

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A test of a system which attempts to breach the System Security policy. Also known as "pen-test".

penetration testing

[FC Ver 1.0 Dec 1992]

Security testing in which evaluators attempt to circumvent the security features of an AIS based on their understanding of the system design and implementation. [NSTISSI 4009]

penetration testing

[ITSEC Ver 1.2 1991]

Tests performed by an evaluator on the Target of Evaluation in order to confirm whether or not known vulnerabilities are actually exploitable in practice.

penetration testing

[TCSEC Dec 1985]

The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users.

performance

[POSIX.0/D15 Jun 1992]

A measure of a computer system or subsystem to perform its functions; for example, response time, throughput, number of transactions per second.

performance evaluation

[POSIX.0/D15 Jun 1992]

The technical assessment of a system or system component to determine how effectively operating objectives have been achieved.

performance requirement

[POSIX.0/D15 Jun 1992]

A requirement that specifies a performance characteristic that a system or system component must possess; for example speed, accuracy, frequency.

persistent

[POSIX.6/D13 Nov 1992]

A state in which data retains its original meaning as long as the system configuration remains unchanged, even across system reboots. However, any change to the system configuration (such as adding or deleting user IDs, and modifying the set of valid sensitivity labels) may render data non-persistent.

personal identification device (PID)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A physical device possessed by a user for authentication purposes.

physical security

[ISO 7498-2:1989]

The measures used to provide physical protection of resources against deliberate and accidental threats.

platform profile

[POSIX.0/D15 Jun 1992]

A profile whose focus is on functionality and interfaces for a particular type of platform (e.g., workstation, personal computer, time sharing, symmetric multiprocessing).

policy

[ISO 7498-2:1989]

See: Security Policy.

POSIX Open System Environment (POSIX OSE)

[POSIX.0/D15 Jun 1992]

The Open System Environment in which the standards included are not in conflict with ISO/IEC 9945 and are:

- International Standards and Profiles (developed by ISO, IEC, or CCITT)
- Regional Standards and Profiles (developed by a group recognized as an official standards body by a regional governmental entity, such as the European Community)
- National Information Technology Standards and Profiles (developed by a national standards body recognized as such by ISO, IEC, or CCITT, as appropriate)

This guide represents the POSIX OSE as it existed when the guide was approved.

POSIX OSE Cross-Category Services

[POSIX.0/D15 Jun 1992]

A set of tools and/or features that has a direct effect on the operation of one or more components of the POSIX Open System Environment, but is not in and of itself a stand-alone component.

POSIX Standardized Profile (POSIX SP)

[POSIX.0/D15 Jun 1992]

A standardized Profile that specifies the application of certain POSIX base standards in support of a class of applications and does not require any departure from the structure defined by the POSIX.0 Reference Model for POSIX systems.

Note: A decision on which POSIX base standards form the basis of the POSIX SPs is still open.

primitive

[FC Ver 1.0 Dec 1992]

Orderly relation between TCB subsets based on dependency. [NCSC-TG-021]

Note: A TCB subset B is more primitive than a second TCB subset A (and A is less primitive than B) if A directly depends on B or a chain of TCB subsets from A to B exists such that each element of the chain directly depends on its successor in the chain.

principal

[ECMA-138 Dec 1989]

An initiator that is capable of initiating interactions on objects, which is not acting on behalf of, or by proxy, of another object. A Principal can be either a human user or an active object.

principal

[ISO/IEC DIS 10181-2 Jul 1991]

An entity whose identity can be authenticated.

principle of least privilege

[POSIX.6/D13 Nov 1992]

A security design principle that states that a person, process, or program be granted only those privileges necessary to accomplish a legitimate function, and only for the time that such privileges are actually required.

The proper application of this principle limits the damage that can result from accident, error, or unauthorized use of available privileges by a process.

privacy

[ISO 7498-2:1989]

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.

private key

[ISO/IEC CD 10181-1:Dec 1992]

A key used in an asymmetric algorithm. Possession of this key is restricted, usually to only one entity.

private key

[ISO/IEC DIS 10181-2 Jul 1991]

The key, used in an asymmetric algorithm, that is known to only one entity.

privilege

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

See: Access Right.

privilege

[FC Ver 1.0 Dec 1992]

Special authorization that is granted to particular users to perform security relevant operations.

privilege

[POSIX.6/D13 Nov 1992]

The ability to exercise a controlled or restricted service.

privilege attribute certificate

[ECMA-138 Dec 1989]

A certificate containing Privilege Attributes.

privilege attributes

[ECMA TR/46 Jul 1988]

Attributes, associated with a security subject that, when matched against control attributes of a security object are used to grant or deny access to that security object.

process

[FC Ver 1.0 Dec 1992]

A program in execution on a processor which represents a scheduling and accounting (and sometimes a concurrency and recovery) entity in a computer system.

process

[POSIX.0/D15 Jun 1992]

An address space and one or more threads of control that execute within that address space, and their required system resources.

process

[TCSEC Dec 1985]

A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

process privilege flag

[POSIX.6/D13 Nov 1992]

A per-privilege attribute of a process that is used to determine if the privilege it is associated with is currently usable or controllable by the process, or to indicate that the privilege is to be passed on to the next process image.

process privilege state

[POSIX.6/D13 Nov 1992]

A per-process state variable that identifies a value for all defined process privilege flags for all privileges defined in an implementation.

producers

[FC Ver 1.0 Dec 1992]

Providers of IT product security (e.g., product vendors, product developers, security analysts, and value-added resellers).

product

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Hardware and/or software intended for use in more than one system.

product

[FC Ver 1.0 Dec 1992]

Package of IT software and/or hardware designed to perform a specific function either stand alone or once incorporated into an IT system.

product

[ITSEC Ver 1.2 1991]

A package of ITSEC software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

product rationale

[FC Ver 1.0 Dec 1992]

Overall justification; including anticipated threats, objectives for product functionality and assurance, technical security policy, and assumptions about the environments and uses of conforming products; for the protection profile and its resulting IT product.

product rationale

[ITSEC Ver 1.2 1991]

A description of the security capabilities of a product, giving the necessary information for a prospective purchaser to decide whether it will help to satisfy his system security objectives.

production

[ITSEC Ver 1.2 1991]

The process whereby copies of the Target of Evaluation are generated for distribution to customers.

profile

[FC Ver 1.0 Dec 1992]

Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IT product or AIS. (See Protection Profile.)

profile

[POSIX.0/D15 Jun 1992]

A set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards, necessary for accomplishing a particular function.

profile assurance

[FC Ver 1.0 Dec 1992]

Measure of confidence in the technical soundness of a protection profile.

programming language API

[POSIX.0/D15 Jun 1992]

The interface between applications and application platforms traditionally associated with programming language specifications, such as program control, math functions, string manipulation, etc.

programming languages and compilers

[ITSEC Ver 1.2 1991]

The tools used within the Development Environment in the construction of the software and/or firmware of a Target of Evaluation.

proof

[FC Ver 1.0 Dec 1992]

The process of establishing the validity of one or more statements; the process of establishing a the truth of a fact. (A proof is more rigorous than both a demonstration and an explanation.)

proprietary information

[FC Ver 1.0 Dec 1992]

Information that is owned by a private enterprise and whose use and/or distribution is restricted by that enterprise.

> Note: Proprietary information may be related to the company's products, business, or activities, including but not limited to: financial information, data or statements; trade secrets; product research and development information; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and trade secrets or other company confidential information.

protected mechanism

[FC Ver 1.0 Dec 1992]

See encapsulated subsystem.

protection philosophy

[FC Ver 1.0 Dec 1992]

Informal description of the overall design of an IT product that shows how each of the supported control objectives is dealt with.

protection philosophy

[TCSEC Dec 1985]

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.

protection profile

[FC Ver 1.0 Dec 1992]

Statement of security criteria; shared by IT product producers, consumers, and evaluators; built from functional, development assurance, and evaluation assurance requirements; to meet identified security needs through the development of conforming IT products.

protection profile family

[FC Ver 1.0 Dec 1992]

Two or more protection profiles with similar functional requirements and rationale sections but with different assurance requirements.

protection-critical portion of the TCB

[TCSEC Dec 1985]

Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects.

protocol

[POSIX.0/D15 Jun 1992]

A set of semantic and syntactic rules that determine the behaviour of entities in performing communication functions.

prove a correspondence

[FC Ver 1.0 Dec 1992]

Provide a formal correspondence, using a formal reasoning system (e.g., typed lambda calculus) between the levels of abstraction.

> Note: This involves proving that required properties continue to hold under the interpretation given in the formal correspondence.

proxy (1)

[ECMA-138 Dec 1989]

An entity in a system that acts on behalf of another entity in invoking some operation.

proxy (2)

[ECMA-138 Dec 1989]

Privileges that allow an entity to act on behalf of another entity.

public key

[ISO/IEC CD 10181-1:Dec 1992]

The key, used in an asymmetric algorithm, that is publicly available.

public key

[ISO/IEC DIS 10181-2 Jul 1991]

The key, used in an asymmetric algorithm, that is publicly available.

public specifications

[POSIX.0/D15 Jun 1992]

Specifications that are available, without restriction, to anyone for implementation and distribution (i.e., sale) of that implementation.

purge

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The erasure of data from a system or component using conventional techniques (eg. overwriting).

See also: Object Reuse, Remanence.

query

[POSIX.6/D13 Nov 1992]

Any operation which obtains either data or attributes from an object.

radiation security

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Measures to defend against TEMPEST attacks.

rating

[ITSEC Ver 1.2 1991]

A measure for the assurance that may be held in a Target of Evaluation, consisting of a reference to its security target, an evaluation level established by assessment of the correctness of its implementation and consideration of its effectiveness in the context of actual or proposed operational use, and a confirmed rating of the minimum strength of its security mechanisms.

read

[POSIX.6/D13 Nov 1992]

A fundamental operation that results only in the flow of information from an object to a subject.

read

[TCSEC Dec 1985]

A fundamental operation that results only in the flow of information from an object to a subject.

read access

[TCSEC Dec 1985]

Permission to read information.

read-only memory (ROM)

[TCSEC Dec 1985]

A storage area in which the contents can be read but not altered during normal computer processing.

redirection

[POSIX.0/D15 Jun 1992]

A system profile construction method of starting at a base platform and adding new services by allowing a service component to ask the base platform to redirect all requests for that type of service to the service component.

reference data transfer

[ECMA TR/46 Jul 1988]

an information transfer between two server application processes acting cooperatively on instructions from a third application process.

reference model

[POSIX.0/D15 Jun 1992]

A set of conventions and concepts, mutually agreed upon between the information system user and provider communities.

reference monitor

[FC Ver 1.0 Dec 1992]

Access mediation concept that refers to an abstract machine that mediates all accesses to objects by subjects.

reference monitor concept

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

An access control concept that refers to monitoring of all accesses to objects by subjects.

reference monitor concept

[TCSEC Dec 1985]

An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

reference validation mechanism

[FC Ver 1.0 Dec 1992]

Portion of a trusted computing base, the normal function of which is to mediate 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.

refinements

[FC Ver 1.0 Dec 1992]

Requirement in a protection profile taken to a lower level of abstraction than the component on which it is based.

Note: The refinement of a component requirement is necessary when multiple environment-specific requirements must be assigned to a single component requirement.

remanence

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The persistence of information on computing or communications media or equipment even following a purge.

Note: Normally used to refer to residual information which would only be accessible using specialist techniques.

Example: magnetic remanence.

See also: Object Reuse, Purge.

repudiation

[ISO 7498-2:1989]

Denial by one of the entities involved in a communication of having participated in all or part of the communication.

requirements

[FC Ver 1.0 Dec 1992]

Phase of the Development Process wherein the top level definition of the functionality of the system is produced.

requirements

[ITSEC Ver 1.2 1991]

A phase of the Development Process wherein the security target of a Target of Evaluation is produced.

requirements for content and presentation

[ITSEC Ver 1.2 1991]

A component of the evaluation criteria for a particular phase or aspect of evaluation identifying what each item of documentation identified as relevant to that phase or aspect of evaluation shall contain and how its information is to be presented.

requirements for evidence

[ITSEC Ver 1.2 1991]

A component of the evaluation criteria for a particular phase or aspect of evaluation defining the nature of the evidence to show that the criteria for that phase or aspect have been satisfied.

requirements for procedures and standards

[ITSEC Ver 1.2 1991]

A component of the evaluation criteria for a particular phase or aspect of evaluation identifying the nature and/or content of procedures or standard approaches that shall be adopted or utilised when the TOE is placed into live operation.

residual risk

[FC Ver 1.0 Dec 1992]

Portion of risk that remains after security measures have been applied. [NSTISSI 4009]

resource

[FC Ver 1.0 Dec 1992]

Anything used or consumed while performing a function.

Note: The categories of resources include: time, information, objects (information containers), or processors (the ability to use information) Specific examples include: CPU time; terminal connect time; amount of directly-addressable memory; disk space; and number of I/O requests per minute.

resource

[TCSEC Dec 1985]

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.

resource authority

[ECMA-138 Dec 1989]

An authority recognised in a Security Domain as a trusted source of security information which relates to resources (security object).

retained ACI

[ISO/IEC CD 10181-3 Oct 1991]

ACI which has been retained by an ADF from earlier access control decisions for use in future access control decisions.

rigorous development

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Development of a system or part of a system where the transformation from one representation to another is demonstrated to be consistent by convincing argument.

See also: Disciplined, Structured, Verified Development.

risk

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The likelihood that a successful attack will be mounted against a computer system. Risk is a function of both vulnerability and threat.

risk

[FC Ver 1.0 Dec 1992]

The expected loss due to, or impact of, anticipated threats in light of system vulnerabilities and strength or determination of relevant threat agents.

risk assessment

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The process of reviewing the threats to and vulnerabilities of a system to determine the level of risk to which it is exposed.

See also: Minimum Standards.

role

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The description of a user's sphere of responsibility.

Note: May be used for enforcing access control in accordance with the principle of least privilege.

Example: System Administrator.

role

[FC Ver 1.0 Dec 1992]

A distinct set of operations (actions) performed on encapsulated data objects.

routing control

[ISO 7498-2:1989]

The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.

rule-based security policy

[ISO 7498-2:1989]

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.

scalability

[POSIX.0/D15 Jun 1992]

The ease with which software can be transferred from one graduated series of application platforms to another.

scope of a requirement

[FC Ver 1.0 Dec 1992]

Determination of whether a requirement applies to: all users, subjects and objects of the TCB; all the TCB commands and application programming interfaces, to all TCB elements; all configurations, or only a defined subset of configurations.

seal

[ECMA-138 Dec 1989]

A checksum, which may be cryptographic, computed over some data to provide integrity for that data.

seal

[ISO/IEC CD 10181-1:Dec 1992]

A cryptographic checkvalue that supports integrity but does not protect against forgery by the recipient (i.e., it does not support non-repudiation). When a seal is associated with a data element, that data element is ’sealed’.

secret key

[ISO/IEC CD 10181-1:Dec 1992]

In a symmetric cryptographic algorithm the key shared between two entities.

secret key

[ISO/IEC DIS 10181-2 Jul 1991]

In a symmetric encipherment algorithm the key shared between two entities.

secure interaction policy

[ISO/IEC DIS 10745 May 1992]

The common aspects of the security policies in effect at each of the communicating application-processes.

security

[FC Ver 1.0 Dec 1992]

The combination of confidentiality, integrity and availability. [ITSEC]

security

[ITSEC Ver 1.2 1991]

The combination of confidentiality, integrity and availability.

security

[POSIX.0/D15 Jun 1992]

The protection of computer hardware, software, and data from accidental or malicious access, use, modification, destruction, or disclosure.

Tools for the maintenance of security are focused on availability, confidentiality, and integrity.

security

[POSIX.6/D13 Nov 1992]

The combination of confidentiality, integrity, and availability.

security administration

[ECMA-138 Dec 1989]

A human authority which establishes a security policy and identifies the entities to which the policy applies.

security administrator

[ECMA TR/46 Jul 1988]

An authority (a person or group of people) responsible for implementing the security policy for a security domain.

security administrator

[POSIX.6/D13 Nov 1992]

An authority (a person or a group of people) responsible for implementing the security policy for a security domain.

security architecture

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A high level description of the structure of a system, with security functions assigned to components within this structure.

security attribute

[ECMA-138 Dec 1989]

A security attribute is a piece of security information which is associated with an entity in a distributed system.

security attribute

[POSIX.6/D13 Nov 1992]

Attributes associated with processes and files and used to determine access rights of a subject to an object.

security attributes

[ECMA TR/46 Jul 1988]

A general term covering both privilege attributes and control attributes. The use of security attributes is defined by a security policy.

security audit

[ISO 7498-2:1989]

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.

security audit message

[ISO/IEC CD 10181-7 Aug 1992]

A message generated following the occurrence of an auditable security-related event.

security audit record

[ISO/IEC CD 10181-7 aug 1992]

A single record in a security audit trail corresponding to a single security-related event.

security audit trail

[FC Ver 1.0 Dec 1992]

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. [TCSEC]

security audit trail

[ISO 7498-2:1989]

Data collected and potentially used to facilitate a security audit.

security auditor

[ISO/IEC CD 10181-7 Aug 1992]

An individual or a process allowed to have access to the security audit trail and to build audit reports.

security certificate

[ISO/IEC CD 10181-1:Dec 1992]

A set of security relevant data which is protected by integrity and data origin authentication from an issuing security authority, and includes an indication of a time period of validity.

Note: All certificates are deemed to be security certificates (see the relevant definitions in 7498-2). The term "security certificate" is adopted in order to avoid terminology conflicts with [X.509 | ISO 9594-8] (i.e. the directory authentication standard).

security class

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The combination of classification, categories and caveats associated with an object.

Example: "SECRET CORPORATE UK EYES A"

Note: Used only in the context of, and at the granularity of, a system's ability to distinguish between security classes.

See also: Label, Lattice, Single Class, Multi-class.

security clearance

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

1. The formal authorization by the Departmental Security Officer for an individual to have access to classified information, following appropriate vetting.

2. An attribute of a subject that specifies the security classes of objects for which access rights may be granted.

See also: Lattice.

security communications function

[ISO/IEC DIS 10745 May 1992]

A function supporting the transfer of security-related information between open systems.

security domain

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

An area of responsibility for the security of a system as defined in a System Security policy.

Note: The terms Global Security Environment (GSE), Local Security Environment (LSE) and Electronic Security Environment (ESE) are used to categorise security domains.

security domain

[ECMA TR/46 Jul 1988]

A bounded group of security objects and security subjects to which applies a single security policy executed by a single security administrator.

security domain

[ECMA-138 Dec 1989]

A set of entities that is subject to a given security policy and a single security administration.

security domain

[ISO/IEC CD 10181-1:Dec 1992]

A set of elements, a security policy, a security authority and a set of security relevant activities in which the set of elements are subject to the security policy, administered by the security authority, for the specified activities.

security domain

[POSIX.6/D13 Nov 1992]

A complete set of objects, subjects and policies which determine the local definition of "security".

security enforcing

[ITSEC Ver 1.2 1991]

That which directly contributes to satisfying the security objectives of the Target of Evaluation.

security event manager

[ISO/IEC CD 10181-7 Aug 1992]

An individual or process allowed to specify and manage the events which may generate a security message and to establish the action(s) to be taken for each security message type.

security exchange

[ISO/IEC DIS 10745 May 1992]

The transfer of protocol-control-information between open systems as part of the operation of a security mechanism.

security facility

[ECMA TR/46 Jul 1988]

A set of logically associated security functions as used in the security framework.

security facility interaction

[ECMA TR/46 Jul 1988]

The invocation of a function a security facility by another security facility.

security fault notification

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Report prepared by a CLEF and initially distributed to the Certification Body (CB). It describes situations whereby the Security policy of the Target of Evaluation (TOE) may be violated.

See also: Evaluation Observation Report.

security function

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A discrete aspect of the performance of a system by which it enforces security automatically on behalf of the System Manager and /or system users.

Note: [1] Access control, authentication, accounting and audit are defined as major security functions which can be broken down into "functional elements".

[2] The term is normally used at the requirements stage of a system life cycle, eg. in a System Electronic Information Security policy.

See also: Mechanism, Trusted Function.

security interaction policy

[ISO/IEC CD 10181-1:Dec 1992]

Common aspects of security policies necessary in order for interactions to take place between domains.

security kernel

[FC Ver 1.0 Dec 1992]

An encapsulation of key security-relevant portions of an operating system that prevent unauthorized subject access to objects.

security kernel

[TCSEC Dec 1985]

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.

security label

[ISO 7498-2:1989]

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Note: The marking may be explicit or implicit.

security level

[TCSEC Dec 1985]

The combination of hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of information.

security measure

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A means by which a System Security Policy is enforced.

Note: A general term, covering technical, procedural and management aspects of security.

security mechanism

[ITSEC Ver 1.2 1991]

The logic or algorithm that implements a particular security enforcing or security relevant function in hardware and software.

security model

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A mathematical or conceptual representation for specifying and proving system security.

Examples: Non-interference model, Information Flow model, Bell-LaPadula model.

security object

[ECMA TR/46 Jul 1988]

An entity in a passive role to which a security policy applies.

security objectives

[ITSEC Ver 1.2 1991]

The contribution to security which a Target of Evaluation is intended to achieve.

security operating procedures (SyOPs)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Documentation specifying the procedures that are to be carried out by system users (including the System Administrator and operators) to uphold all aspects of security devolved to the System Manager by the Departmental Security officer in the System Security Policy. Also abbreviated to SECOPS and SOPs.

See also: System Security Officer.

security policy

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The overall principles, regulations, requirements, and/or procedures which govern security as expressed by a responsible security authority.

Examples: National security policy, Departmental security policy.

Note: Responsibility for security may be delegated by Departmental Security Officers to System Managers in accordance with a System Security Policy.

security policy

[ECMA TR/46 Jul 1988]

A set of rules that specify the procedures and mechanisms required to maintain the security of a system, and the security objects and the security subjects under the purview of the policy.

security policy

[ECMA-138 Dec 1989]

A set of rules which define and constrain the types of security-relevant activities of entities.

security policy

[ISO 7498-2:1989]

The set of criteria for the provision of security services (see also identity-based and rule-based security policy.)

Note: A complete security policy will necessarily address many concerns which are outside the scope of OSI.

security policy

[ITSEC Ver 1.2 1991]

See Corporate Security Policy, System Security Policy, Technical Security Policy.

security policy

[POSIX.6/D13 Nov 1992]

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

security policy

[TCSEC Dec 1985]

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

security policy model

[POSIX.6/D13 Nov 1992]

An informal presentation of a formal security policy model.

security policy model

[TCSEC Dec 1985]

An informal presentation of a formal security policy model.

security policy model (SPM)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A logically precise distillation of all or part of a System Electronic Information Security Policy, developed to avoid ambiguities and inconsistencies and to form a sound basis for subsequent stages of the development of a system.

Note: A Security Policy Model may be formal (ie. based on principles of mathematics).

security relationship

[ISO/IEC DIS 10745 May 1992]

A relationship between two real open systems or components thereof, which governs the secure communication of information using OSI protocols.

security relevant

[ITSEC Ver 1.2 1991]

That which is not security enforcing, but must function correctly for the Target of Evaluation to enforce security.

security relevant event

[FC Ver 1.0 Dec 1992]

Any event that attempts to change the security state of the system (e.g., change access controls, change the security level of a user, change a user password). Also, any event that attempts to violate the security policy of the system (e.g., too many logon attempts). [TCSEC]

security relevant event

[TCSEC Dec 1985]

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.).

security requirement

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The statement by the Departmental Security Officer (DSO) of the minimum standards to be met by a specific system and particular threats which are to be countered.

Note: A Security requirement should be stated in response to an Initial System Security Policy and should then be incorporated in the System Security policy. It should include a statement of the confidence level to be met by trusted hardware and software.

security service

[ECMA-138 Dec 1989]

A set of operations designed to support some aspect of security in a distributed system.

security service

[ISO 7498-2:1989]

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

security state

[ISO/IEC DIS 10745 May 1992]

State information that is held in an open system and which is required for the provision of OSI security services.

security sub-domain

[ECMA-138 Dec 1989]

A proper subset of a security domain's entities which are subject to a security policy which possesses the following properties:

1. it includes all of the rules of the super-domain's policy where they apply;

2. additional rules are defined for the sub-domain policy action types where permitted by the policy of the super-domain;

3. it is administered by an Administration authorised by the super-domain's Administration.

security subject

[ECMA TR/46 Jul 1988]

An entity in an active role to which a security policy applies.

security target

[FC Ver 1.0 Dec 1992]

Product-specific description, elaborating the more general requirements in a protection profile and including all evidence generated by the producers, of how a specific IT product meets the security requirements of a given protection profile.

security target

[ITSEC Ver 1.2 1991]

A specification of the security required of a Target of Evaluation, used as a baseline for evaluation. The security target will specify the security enforcing functions of the Target of Evaluation. It will also specify the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

security testing

[TCSEC Dec 1985]

A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification.

See also: Functional Testing, Penetration Testing, Verification.

security token

[ISO/IEC CD 10181-1:Dec 1992]

A set of security relevant data which is protected by integrity and data origin authentication from a source which is not considered a security authority.

selective field protection

[ISO 7498-2:1989]

The protection of specific fields within a message which is to be transmitted.

sensitive information

[TCSEC Dec 1985]

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.

sensitivity

[ISO 7498-2:1989]

The characteristic of a resource which implies its value or importance, and may include its vulnerability.

sensitivity label

[TCSEC Dec 1985]

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.

separation

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The concept of keeping information of different security classes apart in a system.

Note: Separation may be implemented by temporal, physical, logical or cryptographic techniques.

server application process

[ECMA TR/46 Jul 1988]

An application process that implements all or part of the functionality defined by a service definition.

service

[ECMA TR/46 Jul 1988]

This term is used as a generic reference to distributed applications that provide "services" to other applications.

session

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The association for a particular time of a user identification, a subject and a security clearance.

shall

[FC Ver 1.0 Dec 1992]

Indication that a requirement must be met unless a justification of why it cannot be met is given and accepted.

should

[FC Ver 1.0 Dec 1992]

Indication of an objective requirement that requires less justification for non-conformance and should be more readily approved.

Note: Should is often used when a specific requirement is not feasible in some situations or with common current technology.

side effect

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Any way in which one representation differs from previous representations, but which is not revealed by the verification methods adopted, and can lead to failure to satisfy the security requirements.

signature

[ISO 7498-2:1989]

See Digital Signature.

simple security condition

[TCSEC Dec 1985]

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.

simple security property

[FC Ver 1.0 Dec 1992]

An invariant state property allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

single class

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Comprising or containing only one security class.

single class device

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A device which can only be used to process information of a single security class at a time.

single-level device

[TCSEC Dec 1985]

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.

software

[POSIX.0/D15 Jun 1992]

The programs, procedures, rules, and any associated documentation pertaining to the operation of a data processing system.

specification

[FC Ver 1.0 Dec 1992]

One or more detailed, precise statement(s) expressing the essential characteristics of one or more facts.

specification

[POSIX.0/D15 Jun 1992]

A document that prescribes, in a complete, precise, verifiable manner, the requirements, design, behaviour, or characteristics of a system or system component.

sponsor

[ITSEC Ver 1.2 1991]

The person or organisation that requests an evaluation.

standardized profile

[POSIX.0/D15 Jun 1992]

A balloted, formal, harmonized document that specifies a profile.

standards

[POSIX.0/D15 Jun 1992]

Documents, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

standards developer

[POSIX.0/D15 Jun 1992]

An organization that develops standards and is accredited by its National Body, as appropriate.

star (*) property

[FC Ver 1.0 Dec 1992]

An invariant state property 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)

[TCSEC Dec 1985]

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. Also known as the Confinement Property.

state

[FC Ver 1.0 Dec 1992]

Give required information with no attempt or implied requirement, to justify the information presented.

storage object

[ITSEC Ver 1.2 1991]

an object that supports both read and write accesses. [TCSEC]

storage object

[TCSEC Dec 1985]

An object that supports both read and write accesses.

strength of a requirement

[FC Ver 1.0 Dec 1992]

Definition of the conditions under which a functional component withstands a defined attack or tolerates failures.

strength of mechanism

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A measure of the effectiveness of a security mechanism to prevent a breach of the System Security policy, assuming it has been correctly implemented.

strength of mechanism

[ITSEC Ver 1.2 1991]

An aspect of the assessment of the effectiveness of a Target of Evaluation, namely the ability of its security mechanisms to withstand direct attack against deficiencies in their underlying algorithms, principles and properties.

structured development

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Development of a system or part of a system where components at lower levels are traceable from those at the higher level.

See also: Disciplined, Rigorous, Verified Development.

structured text

[POSIX.6/D13 Nov 1992]

Text for which a well-defined, unambiguous internal structure is defined. Such text shall be human readable and interpreted identically by all conforming implementations.

subject

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

An active entity, generally in the form of a person, process, executing programme or device, that causes information to flow among objects or changes the system state.

Examples: process, executing program.

See also: Object.

subject

[ECMA TR/46 Jul 1988]

Abbreviation of security subject.

subject

[FC Ver 1.0 Dec 1992]

Active entity in an IT product or AIS, generally in the form of a process or device, that causes information to flow among objects or changes the system state.

subject

[ITSEC Ver 1.2 1991]

an active entity, generally in the form of a person, process, or device. [TCSEC]

subject

[POSIX.6/D13 Nov 1992]

An active entity that causes information to flow between objects or changes the system state; a process.

subject

[TCSEC Dec 1985]

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.

subject authority

[ECMA-138 Dec 1989]

An authority recognised in a Security Domain as a trusted source of security information concerning security subjects (human beings and Applications).

suitability of function

[ITSEC Ver 1.2 1991]

An aspect of the assessment of the effectiveness of a Target of Evaluation, namely the suitability of its security enforcing functions and mechanisms to in fact counter the threats to the security of the Target of Evaluation identified in its security target.

supportive security application

[ECMA TR/46 Jul 1988]

Specific type of application that provides security services or security management capabilities at application level rather than embedded in the communication architecture.

symmetric authentication method

[ISO/IEC DIS 10181-2 Jul 1991]

Method for demonstrating knowledge of a secret, in which both entities share a common authentication information.

system

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

See : Electronic Information Processing System (EIP System).

system

[FC Ver 1.0 Dec 1992]

IT products assembled together; either directly or with additional computer hardware, software, and/or firmware; configured to perform a particular function within a particular operational environment.

system

[ITSEC Ver 1.2 1991]

A specific ITSEC installation, with a particular purpose and operational environment.

system administrator

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The person responsible to the System Manager for the day-to-day operation of a system.

See also: System Security officer.

system definition

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The identification of the boundaries of a system to establish a firm basis for any interconnection with other systems.

system electronic information security policy (SEISP)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A detailed statement of the technical aspects of a System Security Policy.

Note: A System Electronic Information Security Policy provides the baseline for evaluation.

system entry

[FC Ver 1.0 Dec 1992]

Mechanism by which an identified and authenticated user is provided access into the system.

system high security mode

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A system operating in this mode is one whose users are all cleared for and have access to all the information stored on and/or processed by it, but not all of whom actually need to know about all of the data.

See also: Dedicated Security Mode, Multilevel Security Mode, Compartmented Security Mode.

system interconnection security policy (SISP)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A bilateral memorandum of agreement between two System Managers on the security aspects of an interconnection between their two systems.

See also: Community Security Policy.

system internal interface (SII)

[POSIX.0/D15 Jun 1992]

The interface between application platform service components within that platform; it may be standardized or non-standard.

system manager

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The person ultimately responsible for the production and enforcement of a System Security Policy.

See also: System Administrator, System Security Officer.

system security function

[ISO/IEC DIS 10745 May 1992]

A capability of an open system to perform security-related processing.

system security object

[ISO/IEC DIS 10745 May 1992]

An object that represents a set of related system security functions.

system security officer

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The person responsible to the System Manager for writing, enforcing and reviewing Security Operating Procedures (SyOPs).

system security policy

[ITSEC Ver 1.2 1991]

The set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system.

system security policy (SSP)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A statement by a System Manager/Project Manager defining a system, its Security Requirement, the security measures to be enforced and the allocation of responsibilities for enforcing them.

Note: When an SEISP is required it will conform with the policy set out in the relevant SSP.

See also: Initial System Security policy.

system services

[POSIX.0/D15 Jun 1992]

Firmware and software that provide an aggregation of network element functions into a higher level function; provide an interface to the data contained in the system.

system services API

[POSIX.0/D15 Jun 1992]

An interface providing access to services associated with the application's internal resources.

system software

[POSIX.0/D15 Jun 1992]

Application-independent software that supports the running of application software and manages the resources of the application platform.

target

[ISO/IEC CD 10181-3 Oct 1991]

An entity to which access may be attempted.

target access control decision information (target ADI)

[ISO/IEC CD 10181-3 Oct 1991]

ADI associated with the target.

target access control decision information (target ADI)

[ISO/IEC CD 10181-3 Oct 1991]

ADI associated with the target.

target access control information (target ACI)

[ISO/IEC CD 10181-3 Oct 1991]

Access control information relating to the target.

target of evaluation

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A product or system to be evaluated.

target of evaluation

[ITSEC Ver 1.2 1991]

An ITSEC system or product which is subject to security evaluation.

task inaugural meeting

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The first formal meeting between the major organisations concerned with an evaluation.

TCB subset

[FC Ver 1.0 Dec 1992]

Set of software, firmware, and hardware (where any of these three could be absent) that mediates the access of a set S of subjects to a set O of objects on the basis of a stated access mediation policy P and satisfies the properties:

(1) M mediates every access to objects in O by subjects in S;

(2) M is tamper resistant; and

(3) M is small enough to be subject to analysis and tests, the completeness of which can be assured.

technical policy

[FC Ver 1.0 Dec 1992]

Set of rules regulating access of subjects to objects enforced by a TCB subset. [NCSC-TG-021]

technical security policy

[FC Ver 1.0 Dec 1992]

Specific protection conditions and /or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

technical security policy

[ITSEC Ver 1.2 1991]

The set of laws, rules and practices regulating the processing of sensitive information and the use of resources by the hardware and software of an ITSEC system or product.

TEMPEST

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The unintentional radiation or conduction of compromising emanations from communications, non-communications and/or computer systems.

See also: Radiation Security.

TEMPEST

[TCSEC Dec 1985]

The study and control of spurious electronic signals emitted from ADP equipment.

thread

[POSIX.0/D15 Jun 1992]

A single flow of control within a process.

threat

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The likelihood of an attack being mounted against a computer system.

See also: Risk, Vulnerability.

threat

[FC Ver 1.0 Dec 1992]

Sequence of circumstances and events that allows a (human or other) agent to cause an information-related misfortune by exploiting a vulnerability in an IT product.

threat

[ISO 7498-2:1989]

A potential violation of security.

threat

[ITSEC Ver 1.2 1991]

an action or event that might prejudice security.

tool

[ITSEC Ver 1.2 1991]

A product used in the construction and/or documentation of a Target of Evaluation.

top-level specification (TLS)

[TCSEC Dec 1985]

A non-procedural description of system behaviour at the most abstract level. Typically a functional specification that omits all implementation details.

trace a correspondence

[FC Ver 1.0 Dec 1992]

Explain a correspondence, using natural language prose, between levels of abstraction.

traceability

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Property of the development of a system that allows requirements to be traced from one representation to another.

traffic analysis

[ISO 7498-2:1989]

The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).

traffic flow confidentiality

[ISO 7498-2:1989]

A confidentiality service to protect against traffic analysis.

traffic padding

[ISO 7498-2:1989]

The generation of spurious instances of communication, spurious data units and/or spurious data within data units.

transaction

[FC Ver 1.0 Dec 1992]

Set of subject actions and their associated data storage accesses.

transaction

[POSIX.0/D15 Jun 1992]

A unit of work consisting of an arbitrary number of individual operations all of which will either complete successfully or abort with no effect on the intended resources.

A transaction has well defined boundaries. A transaction starts with a request from the application program and either completes successfully (commits) or has no effect (abort). Both the commit and abort signify a transaction completion.

transaction application program

[POSIX.0/D15 Jun 1992]

A program written to meet the requirements of a chosen Transaction Processing (TP) application.

Such programs allow a sequence of operations that involve resources such as terminals and databases. The transaction application process specifies transaction boundaries. The transaction application process as defined here is a logical entity and may involve an arbitrary number of processes.

trap door

[FC Ver 1.0 Dec 1992]

Hidden software or hardware mechanism that can be triggered to permit protection mechanisms in an automated information system to be circumvented. [NSTISSI 4009]

> Note: A trap door is usually activated in some innocent-appearing manner (e.g., a special random key sequence at a terminal). Software developers often write trap doors in their code that enable them to reenter the system to perform certain functions.

trap door

[TCSEC Dec 1985]

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).

trojan horse

[FC Ver 1.0 Dec 1992]

Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allow unauthorized collection, falsification or destruction of data. [NSTISSI 4009]

trojan horse

[TCSEC Dec 1985]

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.

trust

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

reliance upon Security Measures to uphold the Security policy.

Note: The term is not synonymous with "trustworthy". The trustworthiness of trusted items may be established (eg. by evaluation) at a later stage.

trust

[ISO/IEC CD 10181-1:Dec 1992]

A relationship between two elements, a set of activities and a security policy in which element X trusts element Y if and only if X has confidence that Y will behave in a well defined way (with respect to the activities) that does not violate the given security policy.

trust (in security sense)

[ECMA TR/46 Jul 1988]

Confidence, that may be based on assurances which are outside the scope of this Report, 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. trust is always restricted to specific functions or ways of behaviour (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.

trusted computer system

[TCSEC Dec 1985]

A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

trusted computing base

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The security protection mechanisms within a system's hardware, firmware and software which are responsible for enforcing the security policy.

Note: In evaluation terms this means a region that contains no untrusted functions.

trusted computing base (TCB)

[FC Ver 1.0 Dec 1992]

Totality of protection mechanisms within an IT product, including hardware, firmware, software and data, the combination of which is responsible for enforcing a technical security policy.

Note: The ability of an organization to achieve an organizational security policy depends jointly on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and on adherence to associated usage security policies by authorized users.

trusted computing base (TCB)

[TCSEC Dec 1985]

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 correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by the system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

trusted function

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A function whose correct operation is relied upon for the security policy to be upheld.

Note: The term is normally used after the establishment of the evaluation baseline, to relate to representations produced subsequent to the system requirements (eg. functional specification and design specification).

See also: Security Function.

trusted functionality

[ISO 7498-2:1989]

That which is perceived to be correct with respect to some criteria, e.g., as established by a security policy.

trusted network

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The subnetwork formed by an association of interconnected Trusted Network Interface Units and one or more Access control Systems.

See also Trusted Network Interface Unit below.

trusted network interface unit (TNIU)

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

TNET (see Trusted Network above) will be realised by the development of a number of components including the TNIU and ACS. The TNIU is located between the end system and the network that provides separation, integrity, access control and authentication services by means of encryption across the network and supports the operation of the TNIUs by providing them with the current security clearances such as user identification, authentication and binding to particular end systems.

trusted path

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A mechanism by which a user can communicate directly with a trusted function.

Example: A trusted path is required when a user changes his password.

trusted path

[FC Ver 1.0 Dec 1992]

Mechanism by which a person using a terminal can communicate directly with the TCB. [NSTISSI 4009]

Note: Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.

trusted path

[TCSEC Dec 1985]

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.

trusted recovery

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The property of a system which ensures that it can be returned to a secure operating state following a system failure, in accordance with the Security Policy.

trusted region

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Part of a system that contains trusted functions.

trusted software

[TCSEC Dec 1985]

The software portion of a Trusted Computing Base

trusted third party

[ISO/IEC CD 10181-1:Dec 1992]

A security authority or its agent, trusted by other entities with respect to security-related activities.

trusted third party

[ISO/IEC DIS 10181-2 Jul 1991]

A security authority or its agent, trusted by other entities with respect to security-related activities. In the context of this standard a trusted third party is trusted by a claimant and/or verifier for the purposes of authentication.

unprivileged subject

[POSIX.6/D13 Nov 1992]

A subject without appropriate privileges to perform an operation.

unstructured text

[POSIX.6/D13 Nov 1992]

Text for which no internal structure is defined and is unambiguously understood by a typical user.

upgrade

[POSIX.6/D13 Nov 1992]

To change a MAC label or Information Label to a label that dominates the current label but is not equivalent to the current label.

usage security policy

[FC Ver 1.0 Dec 1992]

Assumptions regarding the expected environment and intended method of IT product use.

user

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A person who interacts with a system.

user

[FC Ver 1.0 Dec 1992]

Person or process accessing an IT product by direct connections (e.g., via terminals) or indirect connections; an individual who is accountable for some identifiable set of activities in a computer system.

Note: Indirect connection relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual.

user

[POSIX.6/D13 Nov 1992]

Any person who interacts with a computer system.

user

[TCSEC Dec 1985]

Any person who interacts directly with a computer system.

user documentation

[ITSEC Ver 1.2 1991]

The information about a Target of Evaluation supplied by the developer for use by its end-users.

user identification

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

A character string which uniquely identifies a user to a system.

See also: Password.

user identifier (User ID)

[FC Ver 1.0 Dec 1992]

Unique symbol or character string that is used by an IT product to uniquely identify a specific user.

validation

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The checking of a representation of a system or part of a system for conformance with its requirements.

validation

[POSIX.0/D15 Jun 1992]

The process of evaluating a ported application, software, or system to ensure compliance with requirements.

verification

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The checking of conformance between two representations of a system or part of a system.

verification

[TCSEC Dec 1985]

The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated.

verification authentication information (verification AI)

[ISO/IEC DIS 10181-2 Jul 1991]

Information used by a verifier to verify an identity claimed through exchange AI.

verified development

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

Development of a system or part of a system where the transformation from one representation to another is mathematically proven, or demonstrated to be consistent by an argument of equivalent value.

verifier

[ISO/IEC DIS 10181-2 Jul 1991]

An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

virus

[FC Ver 1.0 Dec 1992]

Self replicating, malicious program segment that attaches itself to an application or other executable system component and leaves no external signs of its presence. [NSTISSI 4009]

vulnerability

[CESG Memorandum No.1 Issue 1.2 Oct 1992]

The likelihood that an attack, if mounted, would be successful. This results from the scale and type of technical security weakness present in computer systems.

See also: Risk, Threat.

vulnerability

[FC Ver 1.0 Dec 1992]

Weakness in an information system or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to produce an information-related misfortune.

vulnerability

[ITSEC Ver 1.2 1991]

A security weakness in a Target of Evaluation (for example, due to failures in analysis, design, implementation, or operation).

vulnerability assessment

[ITSEC Ver 1.2 1991]

An aspect of the assessment of the effectiveness of a Target of Evaluation, namely whether known vulnerabilities in that Target of Evaluation could in practice compromise its security as specified in the security target.

write

[POSIX.6/D13 Nov 1992]

A fundamental operation that results only in the flow of information from a subject to an object.

write

[TCSEC Dec 1985]

A fundamental operation that results only in the flow of information from a subject to an object.

write access

[TCSEC Dec 1985]

Permission to write an object.

zero knowledge technique

[ISO/IEC DIS 10181-2 Jul 1991]

A class of asymmetric algorithms which may be used for authentication, where any exchange AI transferred cannot be used to produce valid exchange AI and where a single verification AI may be sufficient to verify exchange AI produced by different claimants.