ETSI
TECHNICAL COMMITTEE
REFERENCE TECHNICAL REPORT

TCR-TR 028

July 1995

Source: ETSI TC-NA/STAG

Reference: DTR/NA-002503

ICS: 33.080

Key words: Security, vocabulary

Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

New presentation - see History box

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1995. All rights reserved.

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been produced by the Network Aspects Security Techniques Advisory Group (NA/STAG) Technical Committee of the European Telecommunications Standards Institute (ETSI). It was given the classification of TCR-TR by the 19th TC Chairmens' Co-ordination (TCC) meeting and approval by the 21st Technical Assembly (TA).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI Technical Committee (TC) or Sub-Technical Committee (STC) studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilised by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

Blank page

1 Scope

This Technical Committee Reference Technical Report (TCR-TR) should be taken as the normative reference for all security terminology definitions and abbreviations used in documentation produced by Network Aspects Security Techniques Advisory Group (NA/STAG). Also all ETSI STC's should use security terms and abbreviations as defined in this document for the purposes of all their deliberations and documentation on security matters. This TCR-TR has been compiled using information from other publications and/or temporary documents submitted and discussed at various meetings of NA/STAG. It is a living document and will be updated from time to time as new definitions or changes in the present ones arise.

Notes are entered, where appropriate, to clarify the use of definitions and the relationships with definitions in other reference documents. Where more then one definition is available preference is given to the definition derived as part of the CEC DG-XIII Security Investigations undertaken in INFOSEC Task S2001 [15] because there is evidence that great care has been taken in this activity to ensure that the set of individual definitions is non self referential, and that they are consistent.

2 References

This TCR-TR incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this TCR-TR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] European ITSEC Version 1.2, June 1991.

[2] CCITT Recommendation X.509 (1988): "The Directory - Authentication framework".

[3] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architechture".

[4] ISO 7812: "Identification cards - Numbering system and registration procedure for issuer identifiers".

[5] ISO 8732: "Banking - Key management (wholesale)".

[6] ISO 10202-1: "Financial transaction cards - Security architechture of financial transaction systems using integrated circuit cards - Part 1: Card life cycle".

[7] ISO CD 11166: "Banking: Key MAnagement by means of Asymmetric algorithms".

[8] ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory - Part 8: Authentication framework".

[9] ISO/IEC 9796: "Information technology - Security techniques - Digital signature scheme giving message recovery".

[10] ISO/IEC 9798-1: "Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model".

[11] ISO/IEC 10116: "Information technology - Modes of operation for an n-bit block cipher algorithm".

[12] ISO DIS 10164-8: "Information technology - Open Systems Interconnection - Systems Management: Security audit trail function".

[13] ISO/IEC 10181-2: "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems".

[14] ISO/IEC POSIX Security.

[15] CEC DG-XIII INFOrmation SECurity Task S2001 (INFOSEC Task S2001).

3 Abbreviations and acronyms.

NOTE: Not all abbreviations or acronyms listed below are defined in Clause 4.

ACK	Acknowledge
ACL	Access Control Lists
ADDMD	ADministration Directory Management Domain
AI	Artificial Intelligence
ANSI	American National Standards Institute
API	Application Program Interface
CRC	Cyclic Redundancy Check
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DMD	Directory Management Domain
DMO	Domain Management Organization
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ID	IDentifier
INFOSEC	INFOrmation SECurity
IT	Information Technology
ITAEGV	Information Technology Advisory Experts Group on Security (reports to ITSTC)
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
ITSTC	Information Technology Steering Committee of CEN/CENELEC/ETSI
IV	Initialisation Vector
KDM	Key Distribution Mechanism
MAC	Message Authentication Code
NLSP	Network Layer Security Protocol
NOSA	NATO OSI Security Architecture
OSI	Open System Interconnection
PIN	Personal Identification Number
PRDMD	PRivate Direct Management Domain
SAGE	Security Algorithm Group of Experts
SHA	Secure Hash Algorithm
SOG-IS	Senior Officials Group for Information Systems Security
STAG	Security Techniques Advisory Group of ETSI
TCSEC	Trusted Computer System Evaluation Criteria
TLSP	Transport Layer Security Protocol
TOP	Technical and Office Protocol
TTP	Trusted Third Party
ULSM	Upper Layers Security Model

4 Definitions of terms

Access: the ability to use or be in contact with Information or IT Resources within an information system. (INFOSEC Task S2001 [15])

Access control: the prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner. (ISO 7498-2)

Access control list: a list of entities, together with their access rights, which are authorised to have access to a resource. (ISO 7498-2 [3])

Accidental threat: a threat whose origin does not involve any malicious intent. (INFOSEC Task S2001 [15])

Accountability: the principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation. (INFOSEC Task S2001 [15])

NOTE 1: Alternative definition:

The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO 7498-2 [3])

Accreditation: the procedure for accepting a system for use within a particular environment.

Active attack: the realization of an active threat.

Active threat: the threat of a deliberate unauthorised change to the state of the system. (ISO 7498-2 [3])

Activity logging: a feature of an information system which enables activities on the system to be traced to individuals or identities. (INFOSEC Task S2001 [15])

Anonymity: the principle whereby ones identity is witheld from other parties.

Assurance: the confidence, based on some form of analysis, that an objective or requirement or a set of objectives and/or requirements is being/will be achieved. (INFOSEC Task S2001 [15])

NOTE 2: Alternative definition:

The confidence that may be held in the security provided by a target of evaluation. (European ITSEC [1])

Assurance profile: an assurance requirement for a target of evaluation whereby different levels of confidence are required in different security enforcing functions. (European ITSEC [1])

Asymmetric authentication method: method for demonstrating knowledge of a secret, in which not all authentication information is shared by both entities. (ISO/IEC 10118-2)

Audit attribute: a piece of information about an audit event or about one of the subjects or objects involved in an event. (ISO/IEC POSIX Security [14])

Audit description: a part of an audit record that describes one of the subjects and/or objects involved in the audit event. (ISO/IEC POSIX Security [14])

Audit event: an action, detected internally by the system which may generate an audit record. If an event causes an audit record to be generated (for recording in the audit trail), it is a "recorded event" otherwise, it is an "unrecorded event". The system decides, as each event is detected, whether to generate an audit record by the audit pre-selection algorithm. The set of audit events is based upon a system's security policy. (ISO/IEC POSIX Security [14])

Audit event class: a way of characterising auditable events into groups on the basis of audit event types. An audit event type may belong to more than one audit event class. (ISO/IEC POSIX Security [14])

Audit of security: an independent review, for predefined purposes, of the security of an information system. (INFOSEC Task S2001 [15])

Audit post-selection: the process by which the auditor selects records from the audit trail for analysis. Post selection provides the auditor with flexibility in selecting records. (ISO/IEC POSIX Security [14])

Audit pre-selection: the process by which the system decides whether to generate an audit record for a particular occurrence of an auditable event. Pre-selection provides the auditor a means for reducing the volume of audit records generated while still generating those records that are important for analysis. (ISO/IEC POSIX Security [14])

Audit record: the discrete unit of data recorded in the audit trail on the occurrence of a recorded event. An audit record consists of a set of audit descriptions, each of which has a set of audit attributes associated with it. Every audit record always has an audit description for the record's header, and usually has additional audit descriptions describing the subject(s) and object(s) involved in the event. (ISO/IEC POSIX Security [14])

Audit trail: evidence, in documentary or other form which enables a review of the functioning of elements of an information system. (INFOSEC Task S2001 [15])

NOTE 3: Alternative definition:

The historic data and information which are available for examination in order to prove the correctness and integrity with which the agreed security procedures related to a key or transaction(s) have been followed and which allows breaches in security to be detectable. (ISO 8732 [5])

Authenticated identity: an identity of a principal that has been assured through authentication. (ISO/IEC 10118-2)

Authentication: a property by which the correct identity of an entity or party is established with a required assurance.

Authentication algorithm: an authentication algorithm is a sequence of security information known by the user, or maintained in an access device. It is used to provide secure access to the service. This may involve complex algorithms.

Authentication certificate: 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. (ISO/IEC 10118-2)

Authentication information: information used to establish the validity of a claimed identity. (ISO 7498-2 [3])

Authentication token: information conveyed during a strong authentication exchange, which can be used to authenticate its sender. (ISO/IEC 9594-8 [8], CCITT Recommendation X.509 [2])

Authenticity: the avoidance of a lack of completeness or accuracy in authorised modifications to information. (INFOSEC Task S2001 [15])

Authorisation: permission granted by an owner for a specific purpose. (INFOSEC Task S2001 [15])

NOTE 4: Alternative definitions:

The granting of rights, which includes the granting of access based on access rights. (ISO 7498-2 [3])

A property by which the acess rights to resources are established and enforced.

Availability: avoidance of unacceptable delay in obtaining authorised access to information or IT resources. (INFOSEC Task S2001 [15])

NOTE 5: Alternative definition:

The property of being accessible and useable upon demand by an authorised entity. (ISO 7498-2 [3])

Baseline controls: control procedures which constitute minimum good practice levels of protection. (INFOSEC Task S2001 [15])

Block chaining: the encipherment of information such that each block of ciphertext is cryptographically dependent upon the preceding ciphertext block. (ISO 8372)

Block cipher algorithm (n-bit): a block cipher algorithm with the property that plaintext blocks and ciphertext blocks are n bits in length. (ISO/IEC 10116 [11])

NOTE 6: Alternative definition:

A cryptographic system for which plain text and cipher text are divided in blocks.

Breach of security: the unauthorised disclosure, modification or withholding of information. (INFOSEC Task S2001 [15])

Capability: a token used as an identifier for a resource such that possession of the token confers access rights for the resource. (ISO7498-2)

Cardholder: the person to whom the card has been issued. (ISO 10202-1 [6])

Card issuer: an institution which issues cards to cardholders, and is responsible for the common data file and the allocation of application data files. (ISO 10202-1 [6])

Certificate (user): the public keys of a user, together with some other information, rendered unforgeable by encipherment with the secret key of the certification authority which issued it. (ISO/IEC 9594-8 [8], CCITT Recommendation X.509 [2])

Certificate serial number: an integer value, unique within the issuing certification authority, which is unambiguously associated with a certificate issued by that certification authority. (ISO/IEC 9594-8 [8], CCITT Recommendation X.509 [2])

Certification: the issue of a written statement by a recognised body confirming that the security features of an IT Object have undergone a proper evaluation and been found to comply with stated criteria. (INFOSEC Task S2001 [15])

NOTE 7: Alternative definition:

The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used are correctly applied. (European ITSEC [1])

Certification authority: an authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys. (ISO/IEC 9594-8 [8], CCITT Recommendation X.509 [2])

Certification body: an independent and impartial national organisation that performs certification. (European ITSEC [1])

Certification path: an ordered sequence of certificates of objects in the directory information tree which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. (ISO/IEC 9594-8 [8], CCITT Recommendation X.509 [2])

Ciphertext: data produced through the use of encipherment. The semantic content of the resulting data is not available. (ISO 7498-2 [3])

Claim authentication information: information used by a claimant to generate exchange AI needed to authenticate a principal. (ISO/IEC 10181-2 [13])

Claimant: an entity which is or represents a principal for the purposes of authentication exchange on behalf of that entity. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal. (ISO/IEC 9798-1 [10] and ISO/IEC 10181-2 [13])

Claims language: a restricted subset of a natural language, used to reduce ambiguities in the description of needs for and claimed functionalities of safeguards. (INFOSEC Task S2001 [15])

Classification: a particular level in a finite set of hierarchical levels at which the information owner deems a piece of sensitive information should be placed. (INFOSEC Task S2001 [15])

Clearance: an attribute of a user permitting information access in respect of all sensitive information up to and including a given classification. (INFOSEC Task S2001 [15])

Cleartext: intelligible data, the semantic content of which is available. (ISO 7498-2 [3])

Collision-resistant: the property of a function that it is computationally infeasible to construct distinct inputs which give the same output. (ISO/IEC CD10118-1)

Confidentiality: the avoidance of the disclosure of information without the permission of its owner. (INFOSEC Task S2001 [15])

NOTE 8: Alternative definition:

The property that information is not made available or disclosed to unauthorised individuals, entities or processes. (ISO 7498-2 [3])

Continuity plan: a comprehensive consistent statement of the actions to be taken to allow recovery following a major violation. (INFOSEC Task S2001 [15])

Corporate security policy: the set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation. (European ITSEC [1])

Correctness: the extent to which claimed functionality can be, or has been, proven. (INFOSEC Task S2001 [15])

Countermeasures: security services or mechanisms designed to counter a particular threat.

Covert channel: the use of a mechanism not intended for communication to transfer information in a way which violates security. (European ITSEC [1])

Credentials: data that is transferred to establish the claimed identity of an entity. (ISO 7498-2 [3])

Critical mechanism: a mechanism within a target of evaluation that is not protected by other mechanisms and whose failure would create a security weakness. (European ITSEC [1])

Cryptanalysis: the analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext. (ISO 7498-2 [3])

Cryptographic checkvalue: information which is derived by performing a cryptographic transformation (see cryptography) on the data unit. (ISO 7498-2 [3])

Cryptographic device: the electronic hardware part, or subassembly, which implements the encryption algorithm. (ISO 8732 [5])

Cryptographic equipment: equipment in which cryptographic functions (e.g. encryption, authentication, key generation) are performed. (ISO 8732 [5])

Cryptographic key: a parameter used with an algorithm to validate, authenticate, encrypt or decrypt a message. (ISO 8732 [5])

Cryptographic synchronization: the co-ordination of the encipherment and decipherment process. (ISO 8372)

Cryptographic system, cryptosystem: a collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm. (ISO/IEC 9594-8 [8], CCITT Recommendation X.509 [2])

Cryptography: the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. (ISO 7498-2 [3])

Cryptoperiod: the time span during which a specific key is authorised for use or in which the keys for a given system may remain in effect. (ISO 8732 [5])

Damage limitation: reduction, by means of appropriate steps and actions, of the impact resulting from a violation. (INFOSEC Task S2001 [15])

Data integrity: the property that data has not been altered or destroyed in an unauthorised manner. (ISO 7498-2 [3])

Data origin authentication: the corroboration that the source of data received is as claimed. (ISO 7498-2 [3])

Decipherment: the reversal of a corresponding reversible encipherment. (ISO 7498-2 [3])

Deliberate threat: a human threat involving malicious intent. (INFOSEC Task S2001 [15])

Denial of service: the prevention of authorised access to resources or the delaying of time-critical operations. (ISO 7498-2 [3])

Detection: establishment of the occurrence of an incident or a violation. (INFOSEC Task S2001 [15])

Detective controls: detection and the undertaking of appropriate remedial actions. (INFOSEC Task S2001 [15])

Digital fingerprint: a characteristic of a data item, such as a cryptographic check-value 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 characteristic. (ISO/IEC 10181-2 [13])

Digital signature: 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. (ISO 7498-2 [3])

Distinguishing identifier: information which unambiguously distinguishes an entity in the authentication process. (ISO/IEC 9798-1 [10])

Distributed security: information system security when an information system is spread ("distributed") across two or more interconnected systems, often in different geographical locations which need to co-operate to achieve the requirements. (INFOSEC Task S2001 [15])

Domain: see security domain.

Dual control: a process of utilising two or more separate entities (usually persons), operating in concert, to protect sensitive functions of information whereby no single person is able to access or utilise the materials, e.g. a cryptographic key. (ISO 8732 [5])

Effective privilege: a privilege that is currently active for use by a process. Only effective privileges are considered by the system when making access control or other security policy-related decisions. (ISO/IEC POSIX Security [14])

Emanation security: the control of unwanted electromagnetic, acoustic or electrical signals emitted from IT equipment. (INFOSEC Task S2001 [15])

Encipherment: the cryptographic transformation of data (see cryptography) to produce ciphertext. (ISO 7498-2 [3])

End-to-end encipherment: encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (ISO 7498-2 [3])

Entity authentication: the corroboration that an entity is the one claimed. (ISO/IEC 9798-1 [10])

Exchange authentication information: information exchanged between the claimant and the verifier during the process of authenticating the principal. (ISO/IEC 9798-1 [10] and ISO/IEC 10181-2 [13])

Formal security policy model: a mathematiclly precise statement of a security policy. (European ITSEC [1])

Functionality class: a predefined set of safeguards described in a generic way. (INFOSEC Task S2001 [15])

NOTE 9: Alternative definition:

A predefined set of complementary security enforcing functions capable of being implemented in a target of evaluation. (European ITSEC [1])

Generic security function: an object that models security-related processing, whose specification fall outside the scope of OSI but which can be invoked by OSI entities. (ISO/IEC and CCITT ULSM)

Hash code: the result of applying a hash-function to data bits. (ISO/IEC CD10118-1)

Hash function: a (mathematical) function which maps values from a (possibly very) large set of values into a smaller range of values. (ISO/IEC 10181-2 [13])

Hazard: the likelihood of a violation. (INFOSEC Task S2001 [15])

Human threat: a threat which originates from the actions of a human being. (INFOSEC Task S2001 [15])

Human vulnerability: a vulnerability arising from human beings who form part of the IT system. (INFOSEC Task S2001 [15])

Identity: a system-unique tag applied to a user. (INFOSEC Task S2001 [15])

Identity-based security policy: a security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. (ISO 7498-2 [3])

Impact: the loss of value, increased costs or other damage that would occur consequent upon a particular violation. (INFOSEC Task S2001 [15])

Incident: an event which may represent the materialisation of a threat. (INFOSEC Task S2001 [15])

Incident Detection: establishing the occurrence of an Incident. (INFOSEC Task S2001 [15])

Information Access: the ability to use particular information within an information system. (INFOSEC Task S2001 [15])

Information access control: limiting information access to users who have authorisation. (INFOSEC Task S2001 [15])

Information availability: the avoidance of the temporary or permanent withholding of information from those users who have received authorisation. (INFOSEC Task S2001 [15])

Information back up: a duplicate copy of information which could be used to allow recovery. (INFOSEC Task S2001 [15])

Information label: the item visible at the POSIX interface that is used for associating labeling information with data. This information is not related to mandatory access control. (ISO/IEC POSIX Security [14])

Information label floating: the operation whereby one information label is combined with another information label. The result of the operation may be a change in one of the information labels being combined (e.g. when a process having one information label writes to a file having a different information label, the label on the file may change), or the return of a new information label. The information label resulting from a float operation is implementation defined. (ISO/IEC POSIX Security [14])

Information label policy: the implementation defined policy that determines to what degree information labels associated with data are automatically adjusted as data flows through the system. A conforming implementation may associate information labels with file attributes even though it is not required. (ISO/IEC POSIX Security [14])

Information security: the combination of confidentiality, validity, authenticity, integrity and information availability. (INFOSEC Task S2001 [15])

Inheritable privilege: a privilege for which the inheritable process privilege flag is set. (ISO/IEC POSIX Security [14])

Initialisation vector: a random number which is regularly updated and transmitted via a control channel and is used to initialise an encryption algorithm.

Initialising value: value used in defining the starting point of an encipherment process. (ISO 8732 [5])

Integrity: the avoidance of the unauthorised modification of information**.** (INFOSEC Task S2001 [15])

NOTE 10: Alternative definitions:

The prevention of the unauthorised modification of information. (European ITSEC [1])

A property by which the information contents of an object is prevented from being modified.

Key: a sequence of symbols that controls the operations of encipherment and decipherment. (ISO 7498-2 [3])

Key component: one of at least two parameters having the format of a cryptographic key that is combined with one or more like parameters by means of modulo-2 addition to form a cryptographic key. (ISO 8732 [5] and ISO CD 11166 [7])

Key certification centre: a facility operated by the certification authority which generates and returns certificates. (ISO CD 11166 [7])

Key generator: a type of cryptographic equipment used for generating cryptographic keys and where needed initialisation vectors. (ISO 8732 [5] and ISO CD 11166 [7])

Key loader: an electronic, self contained unit which is capable of storing at least one cryptographic key and transferring that cryptographic key, upon request, into cryptographic equipment. (ISO 8732 [5] and ISO CD 11166 [7])

Key management: the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy. (ISO 7498-2 [3])

Key management facility: a protected enclosure (e.g. room or cryptographic equipment) and its contents where cryptographic elements reside. (ISO 8732 [5] and ISO CD 11166 [7])

Key offset; offset: the process of modulo-2 adding a counter to a key. (ISO 8732 [5])

Keying material; cryptographic keying material: the data (e.g. keys and initialising values) necessary to establish and maintain a keying relationship. (ISO 8732 [5] and ISO CD 11166 [7])

Keying relationship: the state existing between a communicating pair during which time they share at least one data key. (ISO 8732 [5] and ISO CD 11166 [7])

Link-by-link encipherment: the individual application of encipherment to data on each link of a communications system (see also end-to-end encipherment). (ISO 7498-2 [3])

Manipulation detection: a mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally). (ISO 7498-2 [3])

Masquerade: the pretence by an entity to be a different entity. (ISO 7498-2 [3])

NOTE 11: Alternative definition:

An attack on a system which involves an unauthorised entity pretending to be an authorised one in order to gain acess to system assets.

Message authentication: verification that a message was sent intact, unchanged and by the purported originator to the intended recipient. (INFOSEC Task S2001 [15])

Message Authentication Code (MAC): a data field used to verify the authenticity of a message. (ISO 8732 [5])

Monitoring: a continuous process of detection designed to ensure the identification of incidents or violations as and when they occur. (INFOSEC Task S2001 [15])

Multilevel directory: a file system object, similar to an ordinary directory, but with special pathname lookup semantics which depend on the message authentication code label of the subject. (ISO/IEC POSIX Security [14])

Non repudiation: proof of the sending or delivery of data by communicating IT assemblies which prevent subsequent false denials by a user of transmission or receipt, respectively, of such data or its contents. (INFOSEC Task S2001 [15])

NOTE 12: Alternative definition:

A property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

Notarization: the registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, time and delivery. (ISO 7498-2 [3])

Objective: the maximum residual overall risk that the information owner or his representative is prepared to accept. (INFOSEC Task S2001 [15])

Off-line authentication certificate: a particular form of authentication information binding an identity to a cryptographic key, certified by a trusted authority, which may be used for authentication without directly interacting with the authority. (ISO/IEC 10181-2 [13])

On-line authentication certificate: a particular form of authentication, certified by a trusted authority which may be used for authentication following direct interaction with the authority. (ISO/IEC 10181-2 [13])

One-way function: a (mathematical) function which is easy to compute but whose inverse is computationally intractable. (ISO/IEC 10181-2 [13])

Operating procedures: a set of rules defining correct use of a target of evaluation. (European ITSEC [1])

Passive attack: the realization of a passive threat.

Passive threat: the threat of unauthorised disclosure of information without changing the state of the system. (ISO 7498-2 [3])

Password: a private character string that is used in user authentication. (INFOSEC Task S2001 [15])

NOTE 13: Alternative definition:

Confidential authentication information, usually composed of a string of characters. (ISO 7498-2 [3])

Peer entity authentication: the corroboration that a peer entity in an association is the one claimed. (ISO 7498-2 [3])

Permitted privilege: a privilege for which the permitted process privilege flag is set. (ISO/IEC POSIX Security [14])

Personal data: any information relating to an identifiable individual.

Personal data integrity: the property that personal data has not been altered or destroyed in an unauthorised manner.

Personal Identification Number (PIN): the PIN is the 4 to 12 position alphanumeric code or password the customer possesses for authentication. This is used to provide authentication of the user with the access device.

Physical protection: devices and procedures designed to protect the components of an information system, and the structures housing it from damage resulting from physical threats. (INFOSEC Task S2001 [15])

Physical security: the measures used to provide physical protection of resources against deliberate and accidental threats. (ISO 7498-2 [3])

Physical threat: a threat whose consequence would consist of physical damage to an information system. (INFOSEC Task S2001 [15])

PIN assignment: the process of establishing the relationship between customer authentication and identification data.

PIN issuance: the act of conveying PIN information to a consumer.

PIN verification: verification of a customer's authenticity by the issuer.

Prevention: the stopping of actual or potential threats from resulting in violations. (INFOSEC Task S2001 [15])

Preventive measure: a measure designed to achieve prevention in the case of specific types of threat. (INFOSEC Task S2001 [15])

Primary account information: data at a financial institution that serves to identify an individual and relate that individual to accounts.

Primary account number: the assigned number that identifies the card issuer and the cardholder. This number is composed of an issuer identification number, individual account identification and an accompanying check digit, as defined in ISO 7812 [4]. (ISO 10202-1 [6])

Principal: an entity whose identity can be authenticated. (ISO/IEC 10181-2 [13])

Privacy: 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. (ISO 7498-2 [3])

Privilege: the ability to exercise a controlled or restricted service. (ISO/IEC POSIX Security [14])

Privilege bracketing: the practice of enabling a privilege only during the period for which it is required for the completion of a specific function. (ISO/IEC POSIX Security [14])

Process privilege flag: each process in a compliant system may have a number of privilege flags associated with it. The state of the associated privilege flags determines if that privilege is currently usable or controllable by the process. (ISO/IEC POSIX Security [14])

Process privilege state: a state variable that identifies a value for all defined process privilege flags for all privilege defined on an implementation. (ISO/IEC POSIX Security [14])

Rating: 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 in the context of that use. (European ITSEC [1])

Read access control: information access control for initiating transfer of specific Information or data from a specific information system. (INFOSEC Task S2001 [15])

Redundancy: the replication of (critical) components within an information system in a way which mitigates the effect of failures. (INFOSEC Task S2001 [15])

Repudiation: denial by one of the entities involved in a communication of having participated in all or part of the communication. (ISO 7498-2 [3])

Residual hazard: the hazard that would remain after any relevant safeguards have been implemented. (INFOSEC Task S2001 [15])

Residual overall risk: the overall risk that would remain after any relevant safeguards have been have been implemented. (INFOSEC Task S2001 [15])

Risk: the product of impact and hazard. (INFOSEC Task S2001 [15])

NOTE 14: In this definition, the hazard and impact should both refer to the same specific threat-vulnerability combination. The risks for each individual threat-vulnerability combination calculated this way can then be summed to arrive at an overall risk. In practice the term risk is often used rather more coarsely than this using a restricted range of levels for both hazard and impact, (such as high, low or medium), leading to a similar restricted range of levels for risk. Risk represents the probable loss of value or increased costs that could occur as a consequence of a particular threat-vulnerability combination.

This particular concept and its definition is most useful when a proper statistical calculation can be performed on a sufficiently large scale to be valid, for example by the insurance industry. A single organisation usually has to rely on coarser assessments of hazard and impact.

Risk analysis: an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurence of those events.

Risk transfer: measures taken to reduce impact on the information owner and / or the system owner or their organisation through reassignment of all or part of a potential Impact to a third party. (INFOSEC Task S2001 [15])

Routing control: the application of rules during the process of routing so as to chose or avoid specific networks, links or relays. (ISO 7498-2 [3])

Rule-based security policy: a security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. (ISO 7498-2 [3])

Safeguard: a measure designed to stop a violation or limit its effects. (INFOSEC Task S2001 [15])

Secure interaction policy: the common aspects of the security policies in effect at each of the communicating application-processes.

Security: the protection of information availability, integrity and confidentiality. (INFOSEC Task S2001 [15])

NOTE 15: Alternative definition:

The combination of confidentiality, integrity and availabily. (European ITSEC [1])

Security administration: a human authority who establishes a security policy and identifies the entities and parties to which the policy applies.

Security architecture: the architecture of parties and entities relevant to security, and the complete set of security procedures and information flows for the realization of security features.

Security audit: 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. (ISO 7498-2 [3])

Security audit trail: data collected and potentially used to facilitate a security audit. (ISO 7498-2 [3])

Security domain: a set of entities and parties that is subject to a single security policy and a single security administration.

Security enforcing: that which directly contributes to the enforcement of security. (European ITSEC [1])

Security exchange: the transfer of protocol control information between open systems as part of the operation of a security mechanism.

Security label: the marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. (ISO 7498-2 [3])

Security life: the time span over which cryptographically protected data has value. (ISO 8732 [5])

Security management: handling of the network and service management aspects of security, including administrative, operational and maintenance issues.

Security mechanism: the logic or algorithm that implements a particular security function in hardware and software. (European ITSEC [1])

Security object: an entity in a passive role to which access is granted or denied according to an authorisation policy.

Security objectives: the contribution to security which a target of evaluation is intended to achieve. (European ITSEC [1])

Security policy: the set of criteria for the provision of security services (see also Identity-based and rule-based security policy). (ISO 7498-2 [3])

NOTE 16: Alternative definition:

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

Security related event: an event which is considered to have relevance to security. (ISO DIS 10164-8 [12])

Security relevant: that which could compromise the enforcement of security. (European ITSEC [1])

Security service: a service provided by a layer of communicating open systems, which ensures adequate security of the systems or of the data transfers. (ISO 7498-2 [3])

Security state: state information which is held in an open system and which is required for the provision of OSI security services.

Security subject: security accessing entity (i.e. an entity in an active role that is granted or denied access to security objects according to an authorisation policy.

Security target: a specification of the security required of a target of evaluation, used as a baseline for evaluation. The security target will specify the security functions of the target of evaluation. It may also specify the security objectives, the threats to those objectives and the particular security mechanisms that will be employed. (European ITSEC [1])

Selective field protection: the protection of specific fields within a message which is to be transmitted. (ISO 7498-2 [3])

Sensitive information: information whose disclosure, modification or withholding without authorisation may cause perceptible loss or damage to someone or something. (INFOSEC Task S2001 [15])

Sensitivity: a measure of importance assigned to sensitive information by the information owner to denote its need for protection. (INFOSEC Task S2001 [15])

NOTE 17: Alternative definition:

The characteristic of a resource which implies its value or importance, and may include its vulnerability. (ISO 7498-2 [3])

Separation of duties: a procedure ensuring that at least two people in an organisation are involved in any work involving (particularly) sensitive information. (INFOSEC Task S2001 [15])

Signature: string of bits resulting from the signature process. (ISO/IEC 9796 [9]); see digital signature. (ISO 7498-2 [3])

Split knowledge: a condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key. (ISO 8732 [5])

Starting value: variable derived from the initialising value and used in defining the starting point of the modes of operation. (ISO 8372)

Stream cipher algorithm: a cryptographic system for which plain text and cipher text are processed as a continuous stream.

Strength of mechanism: 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. (European ITSEC [1])

Symmetric authentication method: method for demonstrating knowledge of a secret, in which both entities share common authentication information. (ISO/IEC 10181-2 [13])

System access control: limiting system access to users who have authorisation. (INFOSEC Task S2001 [15])

System integrity: the property that data and the methods of handling the data cannot be altered or destroyed in an unauthorised manner.

System security policy: the set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system. (European ITSEC [1])

Target of evaluation: an IT system or product which is subjected to security evaluation. (European ITSEC [1])

Technical security policy: 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 IT system or product. (European IT SysITSEC)

Technical threat: a threat originating from a technological failure outside the IT system. (INFOSEC Task S2001 [15])

Technical vulnerability: a vulnerability originating from a failure of a technology component of an IT system. (INFOSEC Task S2001 [15])

Threat: a potential action or event which may cause a loss of one or more aspects of information systems security. (INFOSEC Task S2001 [15])

NOTE 18: Alternative definitions:

An action or event that may prejudice security; (European ITSEC [1]) or

A potential violation of security. (ISO 7498-2 [3])

Time variant parameter: a data item used by an entity to verify that a message is not a replay. (ISO/IEC 9798-1 [10])

Token: exchange authentication information conveyed during an authentication exchange.

Traffic analysis: the inference of information from observation of traffic flows (presence, absence, amount, direction and frequency). (ISO 7498-2 [3])

Traffic flow confidentiality: a confidentiality service to protect against traffic analysis. (ISO 7498-2 [3])

Traffic padding: the generation of spurious instances of communication, spurious data units and/or spurious data within data units. (ISO 7498-2 [3])

Trap-door: 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: 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.

Trusted functionality: that which is perceived to be correct with respect to some criteria e.g. as established by a security policy. (ISO 7498-2 [3])

Trusted third party: a security authority, or its agent, trusted by other entities with respect to security related activities. In particular, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

Unauthorised: without the specific permission of the owner for that purpose. (INFOSEC Task S2001 [15])

Unprivileged subject: a subject without appropriate privileges to perform an operation. (ISO/IEC POSIX Security [14])

User authentication: the process designed to verify the truth of a user's claim to an identity. (INFOSEC Task S2001 [15])

User identification: the process which enables an IT system to recognise a user as corresponding to one previously described to the system. (INFOSEC Task S2001 [15])

Validation: the process of checking the integrity of a message, or selected parts of a message. (ISO 8732 [5])

Validity: total accuracy and completeness of information. (INFOSEC Task S2001 [15])

Verification authentication information: information used by the verifier to verify an identity claimed through exchange authentication information. (ISO/IEC 10181-2 [13])

Verfier: an entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges. (ISO/IEC 10181-2 [13])

Violation: an event in which one or more of authenticity, availability, confidentiality, integrity or validity has been compromised. (INFOSEC Task S2001 [15])

Violation detection: establishing the occurrence of a violation. (INFOSEC Task S2001 [15])

Virus: a code fragment that copies itself into another program, also known as a "host program", modifying that program. It is not an independent program and executes only when the host program is run. The virus replicates itself, infecting other programs causing unplanned behaviour or corruptions of data and/or programs.

Vulnerability: a weakness in an information system that might allow a violation. (INFOSEC Task S2001 [15])

NOTE 19: Alternative definition:

A security weakness in a target of evaluation due to failures in analysis, design, implementation or operation. (European ITSEC [1])

Vulnerability assessment: an aspect of the assessment of the effectiveness of a target of evaluation, namely whether known vulnerabilities in the target of evaluation could in practice compromise its security as specified in the security target. (European ITSEC [1])

Worm: an independent program that reproduces by copying itself from one computer to another, usually over a network. It is different from a virus in that it does not corrupt data/programs or exhibit unplanned behaviour, however, it can cause unnecessary loading of communication links and storage capacity.

Write access control: information access control for modifying specific information or data within a specific information system. (INFOSEC Task S2001 [15])

History

Document history			
July 1994	Draft for endorsement by	TCC 19	1995-02-14 to 1995-02-16
March 1995	Final draft for approval by	TA 21	1995-03-27 to 1995-03-29
July 1995	First Edition		
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)		