Universidad de Los Andes
Arquitectura y Diseño de Software

Términos y Definiciones. Tomado de ISO/IEC 15408-1, second edition. Páginas 2-6

2.1 assets information or resources to be protected by the countermeasures of a TOE.
2.2 assignment the specification of an identified parameter in a component.
2.3 assurance grounds for confidence that an entity meets its security objectives.
2.4 attack potential the perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
2.5 augmentation the addition of one or more assurance component(s) from ISO/IEC 15408-3 to an EAL or assurance package.
2.6 authentication data information used to verify the claimed identity of a user.
2.7 authorised user a user who may, in accordance with the TSP, perform an operation.
2.8 class a grouping of families that share a common focus.
2.9 component the smallest selectable set of elements that may be included in a PP, an ST, or a package.
2.10 connectivity the property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange
of data by wire or by wireless means, over any distance in any environment or configuration.
2.11 dependency a relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
2.15 evaluation authority a body that implements ISO/IEC 15408 for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
2.16 evaluation scheme the administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community.
2.17 extension the addition to an ST or PP of functional requirements not contained in ISO/IEC 15408-2 and/or assurance requirements not contained in ISO/IEC 15408-3.
2.18 external IT entity any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
2.19 family a grouping of components that share security objectives but may differ in emphasis or rigour.
2.20 formal expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
2.21 guidance documentation guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in a PP or ST.
2.22 human user any person who interacts with the TOE.
2.23 identity a representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.
2.24 informal expressed in natural language.
2.26 element an indivisible security requirement.
2.26 evaluation assessment of a PP, an ST or a TOE, against defined criteria.
2.27 evaluation assurance level (EAL) a package consisting of assurance components from **2.28 iteration** the use of a component more than once with varying operations.
2.29 object an entity within the TSC that contains or receives information and upon which subjects perform operations.
2.30 organisational security policies one or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.
2.31 package a reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
2.32 product a package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
2.33 protection profile (PP) an implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
2.34 reference monitor the concept of an abstract machine that enforces TOE access control policies.
2.35 reference validation mechanism an implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.
2.36 refinement the addition of details to a component.
2.37 role a predefined set of rules establishing the allowed interactions between a user and the TOE.
2.38 internal communication channel
a communication channel between separated parts of TOE.
2.39 internal TOE transfer communicating data between separated parts of the TOE.

2.40 inter-TSF transfers communicating data between the TOE and the security functions of other trusted IT products.
2.41 security function policy (SFP) the security policy enforced by an SF.
2.42 security objective a statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
2.43 security target (ST) a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
2.44 selection the specification of one or more items from a list in a component.
2.45 semiformal expressed in a restricted syntax language with defined semantics.
2.46 strength of function (SOF) a qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.
2.47 SOF-basic a level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
2.48 SOF-medium a level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
2.49 SOF-high a level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.
2.50 subject an entity within the TSC that causes operations to be performed.
2.51 secret information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
2.52 security attribute characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.
2.53 security function (SF) a part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
2.54 TOE security functions (TSF) a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
2.55 TOE security functions interface (TSFI) a set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
2.56 TOE security policy (TSP) a set of rules that regulate how assets are managed, protected and distributed within a TOE.
2.57 TOE security policy mode a structured representation of the security policy to be enforced by the TOE.
2.58 transfers outside TSF control communicating data to entities not under control of the TSF.
2.59 trusted channel a means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
2.60 trusted path a means by which a user and a TSF can communicate with necessary confidence to support the TSP.
2.61 TSF data data created by and for the TOE, that might affect the operation of the TOE.
2.62 TSF scope of control (TSC) the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
2.63 user any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
2.64 user data data created by and for the user, that does not affect the operation of the TSF.
2.65 system a specific IT installation, with a particular purpose and operational environment.
2.66 target of evaluation (TOE) an IT product or system and its associated guidance documentation that is the subject of an evaluation.
2.67TOE resource anything useable or consumable in the TOE.