ETSI

ETSI TECHNICAL REPORT

ETR 367

February 1997

Source: ETSI TC-SEC

Reference: DTR/SEC-002701

ICS: 33.020

Key words: Security

Telecommunications Security; Guidelines on the relevance of security evaluation to ETSI standards

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 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Telecommunications Security (SEC) Technical Committee of the European Telecommunications Standards Institute (ETSI).

This ETR details the aspects of the security standards policy concerned with security criteria, evaluation, testing and accreditation, and describes the standards and recommendations which should be used during the specification of an ETSI standard if some, or all, of the security features in the system being standardized are expected to be met and to be evaluated against certain security criteria.

Introduction

The standardization and certification processes play two symmetric roles in the development of a mature European telecommunications market for services and products. If creating standards is a condition for enabling the development and circulation of telecommunication products, likewise the certification process represents a necessary condition for full-fledged procurement activities.

Owners need to be confident that the countermeasures (or safeguards) are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats. The owners themselves may not have the capability to judge all aspects of the countermeasures and may therefore seek evaluation of the countermeasures. The result of an evaluation is a statement about the extent to which the countermeasures can be trusted to reduce the risks to the protected assets. This statement assigns assurance to the countermeasures, i.e. the property of the countermeasure which gives grounds for confidence in their proper operation. The owner of the assets can use this statement to decide whether to accept the risk of exposing the assets to the threats. These relationships are shown in figure 1.

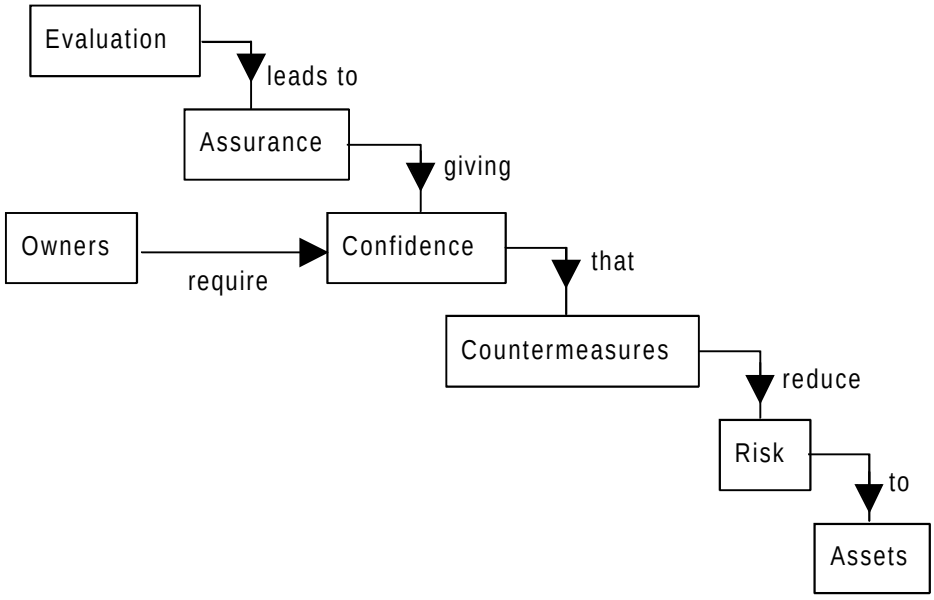

Figure 1

Major efforts have been spent, and still are being spent in ETSI, on the standardization of innovative telecommunications services, the specification of the most suitable security architectures, functions and mechanisms, in the perspective of delivering such services using products that conform to the specified ETSI standards.

The need exists, therefore, to introduce in the security standards produced by ETSI suitably detailed indications concerning the security evaluation of the products built to those standards.

Blank page

1 Scope

This ETSI Technical Report (ETR) describes and investigates existing relationships between security evaluation procedures and the production of ETSI standards including security features.

It is to be stressed that no standardization work on security evaluation has been completed at the moment and so stable standards are not available yet. Currently the main standardization activity in the field of security evaluation is carried out by ISO/IEC/JTC1/SC27/WG3, with the aim of defining harmonized criteria starting from the most important existing criteria. Given the relatively slow progression that the security evaluation standards are experiencing, this ETR mainly refers to the Information Technology Security Evaluation Criteria / Information Technology Security Evaluation Manual (ITSEC [2]/ITSEM [3]) approach which is the most consolidated in Europe and is supported by the European Union. When the ISO criteria and the corresponding evaluation facilities are available this ETR may be updated.

The evaluation of a system or product built to a standard may fail not only due to implementation deficiencies but also due to possible standard deficiencies. In order to minimize the probability that the standard has to be modified, it is recommended in this ETR that at least the optional feasibility study, included in the first phase of the evaluation process described in ITSEM [3], be carried out. This implies that the security target, the main evaluation document defined in the ITSEC [2], be written before the standard completion and that an Information Technology Security Evaluation Facility (ITSEF) be contacted in order to obtain at least a review of it. In order to help this review it will be necessary to provide the ITSEF also with the complete standard thus allowing the evaluators to derive all the information requested for their analyses. The ITSEF's review can be made less time-consuming if the standardization body writes also some parts of the additional evaluation documentation. The review of the security target can minimize the probability that possible standard deficiencies, especially in the field of effectiveness, could not allow a successful evaluation of the system built to that standard (see Computer & Security Vol.13, n.8 [8]). Even better, the ITSEF could be contacted at the beginning of the standard development, according to the concurrent evaluation described in the ITSEM [3]. In this case the security target is drafted as the standard development progresses and possible standard deficiencies can be rapidly fixed. Obviously a complete evaluation cannot be performed due to the unavailability of the Target Of Evaluation (TOE) (the system under standardization), therefore, also in this case the ITSEF involvement should be seen as pre-evaluation consultation. In order to provide the ETSI Bodies with the knowledge required in writing the security target a complete description of this evaluation document is included. A description of other parts of the evaluation documentation that can be written during the standard development is also provided.

2 References

For the purposes of this ETR, the following references apply:

[1] DOD 5200.28-STD US Department of Defence (December 1985): "Trusted Computer System Evaluation Criteria".

[2] Office for Official Publications of the EC (June 1991): "Information Technology Security Evaluation Criteria" (ITSEC, version 1.2).

[3] Office for Official Publications of the EC (September 1993): "Information Technology Security Evaluation Manual" (ITSEM, version 1.0).

[4] National Institute of Standards and Technology and National Security Agency (December 1992): "Federal Criteria For Information Technology Security, Volume I, Protection Profile Development, Version 1.0".

[5] National Institute of Standards and Technology and National Security Agency (December 1992): "Federal Criteria For Information Technology Security, Volume II, Registry of protection profiles, Version 1.0".

[6] Canadian Systems Security Center Communications Security Establishment, Government of Canada (January 1993): "The Canadian Trusted Computer Product Evaluation Criteria" (CTCPEC, version 3.0e).

[7] Common Criteria Editorial Board (January 1996): "Common Criteria for Information Technology Security Evaluation" (Version 1.0).

[8] Computer & Security Vol.13, n.8, 1994, pp.647-650: "Security Evaluation in Information Technology Standards" F. Gentile, L. Giuri, F. Guida, E. Montolivo and M. Volpe.

3 Abbreviations and definitions

3.1 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

CC	Common Criteria
CCEB	Common Criteria Editorial Board
FC	Federal Criteria
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
INFOSEC	Information Security
NCSC	National Computer Security Council
NIST	National Institute for Standard and Technology
NSA	National Security Agency
SEF	Security Enforcing Function
TOE	Target Of Evaluation
TCSEC	Trusted Computer System Evaluation Criteria

3.2 Definitions

For the purposes of this ETR, the following definitions apply:

assurance: The confidence that may be held in the security provided by a Target of Evaluation (ITSEC [2]).

correctness: A property of a representation of a Target of Evaluation such that it accurately reflects the stated security target for that system or product (ITSEC [2]).

effectiveness: A property of a Target of Evaluation representing how well it provides security in the context of its actual or proposed operational use (ITSEC [2]).

evaluation: The assessment of an Information Technology (IT) system or product against defined evaluation criteria (ITSEC [2]).

functionality class: A pre-defined set of complementary security enforcing functions capable of being implemented in a Target of Evaluation (ITSEC [2]).

security enforcing: That which directly contributes to satisfying the security objectives of the Target of Evaluation (ITSEC [2]).

security mechanism: The logic or algorithm that implements a particular security enforcing or security relevant function in hardware and software (ITSEC [2]).

security objectives: The contribution to security which a Target of Evaluation is intended to achieve (ITSEC [2]).

security policy: at the **corporate level**, is the set of laws, rules and practices that regulate how assets including sensitive information, are managed, protected and distributed within a user organization;

at **system level**, is the set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system;

at the **technical level**, is the set of laws, rules and practices that regulate the processing of sensitive information and use of resources by the hardware and software of an IT system or product. (ITSEC [2])

security relevant: That which is not security enforcing, but must function correctly for the Target of Evaluation to enforce security (ITSEC [2]).

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 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 (ITSEC [2]).

target of evaluation: An IT system or product which is subjected to security evaluation (ITSEC [2]).

4 Evolution of the security evaluation criteria

The root of the activities on security evaluation can be traced back to the development of the **Orange Book** in 1983, Trusted Computer System Evaluation Criteria (TCSEC [1]), by the US National Computer Security Council (NCSC), which was then adopted by the US DoD. Since then the TCSEC [1] has been used by the US government as the basis for evaluation of the security of EDP systems.

The TCSEC document [1] (well known as Orange Book) are mainly concerned of the data confidentiality problem, considering data integrity and availability secondary issues. This was a typical military approach at the release time of these criteria. The Orange Book defines seven classes of systems (called D, C1, C2, B1, B2, B3, A1, in ascending order of provided security). Four main issues have to be considered to classify a system:

1) the security policy adopted by the system;
2) the capability of tracing the system activities in order to record the occurrence of security relevant events (accountability);
3) the trust that may be held in the security level provided by the system (assurance);
4) the accuracy of the documentation.

Each class specifies both functionality and assurance requirements. A system belongs to one of these classes only if it satisfies both the pre-defined functionality and assurance requirements of that class. Obviously the higher the class is, the more the requirements are restrictive.

In Europe, around the end of the 1980s, some countries started defining their own national security evaluation programs, developing and publishing country-specific security evaluation criteria. This documents were subsequently revised and harmonized, in a scheme promoted and supported by the EC Commission, giving rise in June 1991 to the Information Technology Security Evaluation Criteria (ITSEC [2]). A companion document, defining operational methodologies for performing security evaluation, the Information Technology Security Evaluation Manual (ITSEM [3]) was also published in April 1992.

The ITSEC [2] approach, more accurately described in the next section, is different from the TCSEC [1] one and is considered more flexible and adaptable to the evaluation of any IT system or product. As we have seen, TCSEC classifies systems through a hierarchy of classes and for each class both functionality and assurance requirements are strictly specified. The security functions of each class are chosen in such a way to withstand some typical threats in the area of operating systems. The effectiveness of these functions has been assessed once for all during the definition of the classes. According to the ITSEC [2], the security functions can be instead arbitrarily chosen, but their effectiveness in satisfying the stated security objectives in the system operational environment and with the stated threats has to be assessed during the evaluation. A consequence of this approach is the independence between security functionality provided by the system and the evaluation level it can aim to. This implies that two systems with distinct security functionality could be successfully evaluated at the same level. In the ITSEC [2] seven assurance evaluation levels are defined that represent an ascent trust in the system capability to satisfy its security objectives throughout the security functions.

In North-America, after the TCSEC [1], both the US and Canada have started further activities on the subject of security evaluation. The first version of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC [6]) was published in 1989 (last published version is 3.0e [6], January 1993). In the US, in 1991, the National Institute for Standard and Technology (NIST) and the National Security Agency (NSA) started a joint project called Federal Criteria (FC) project, which resulted, in December 1992, in the first draft of the FC [4] and [5]. However this project has been paused since the US effort in this field moved toward another set of criteria called Common Criteria (CC). These new criteria include some important FC [4] and [5] concepts. The standardization work of the ISO working group ISO/IEC/JTC1/SC27/WG3 (Evaluation Criteria for IT Security) completes this concise survey on the existing evaluation criteria. The aim of this group, started in 1990, is to define standard criteria before 1998. Since 1993, WG3 work proceed together with the work of the Common Criteria Editorial Board (CCEB), a group of European, US and Canadian experts. The goal of CCEB is to harmonize the ITSEC [2], the FC [4] and [5] and the CTCPEC [6] in a new set of criteria called CC. Hopefully this new criteria will permit international mutual recognition of the evaluation results and they will be compatible with all the above mentioned criteria. The last version of the CC [7] is numbered v1.0 and has been issued on January 1996. A brief overview of the various parts of the CC is provided in annex A.

5 Main concepts in the ITSEC

According to the ITSEC [2] terminology an IT system is a specific IT installation with a particular purpose and known operational environment. An IT product is a hardware and/or software package that can be bought off the shelf and incorporate into a variety of systems. From the point of view of security the main difference between systems and products lies in what is certain about their operational environment. An IT system is designed to meet the requirements of a specific group of end users. It has a real world environment which can be defined and observed in every detail. In particular the characteristics and requirements of its end users will be known and the threats to its security are real threats which can be determined. An IT product needs to be suitable for incorporation in many systems. The product designer can only make general assumptions about the operational environment of a system of which it may become a component. According to the ITSEC [2] approach the same criteria are used for both IT products and IT systems.

In the ITSEC [2] an IT system or product which is subjected to security evaluation is called Target Of Evaluation (TOE) while the person or organization that requests an evaluation is called sponsor. The evaluation of a TOE is performed with respect to a set of specifications (security target) that includes: the security objectives for the TOE and the threats to those objectives; the description of the Security Enforcing Functions; the description of any specific security mechanisms that will be employed. Examples of security enforcing functions are: auditing functions, error recovery functions, access control functions, etc. The construction of the security target needs to be carried out by the sponsor.

Unlike the TCSEC [1] approach, the ITSEC [2] approach permits one to freely select security enforcing functions. However there is a suggestion in ITSEC [2] that these functions are selected with respect to pre-defined functionality classes. Ten functionality classes, based on the German national criteria and the Orange Book, are described in the ITSEC [2]. The evaluation process is highly simplified if functions belonging to those classes are used. In particular, it is possible to obtain Orange Book comparable evaluations choosing one of the first five pre-defined classes.

Table 1: Assurance effectiveness criteria

Group	Aspect
Construction	Suitability of functionality
	Binding of functionality
	Strength of mechanisms
	Construction vulnerability assessment
Operation	Ease of use
	Operational vulnerability assessment

The confidence that may be held in the security provided by a TOE is referred to as assurance. This notion is very important in the ITSEC [2]. Assurance addresses confidence in both effectiveness and correctness of the security enforcing functions and mechanisms.

The aim of the effectiveness assessment (see table 1) is to determine whether:

- the TOE can be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure (using only the user and administration documentation for guidance);

- when the TOE is securely configured and used, the security enforcing functions and mechanisms are able to withstand indirect and direct attacks or accidental events that could compromise the security objectives in;

- there are no exploitable vulnerabilities related to non-IT (physical, procedural and personnel) countermeasures.

The aim of the correctness evaluation is to determine if the provided security enforcing functions have been correctly implemented. The degree of confidence in the correctness of the security enforcing functions is expressed through seven hierarchical evaluation levels (E0 - E6). The lowest level E0 represents inadequate assurance.

Effectiveness and correctness evaluation are performed by taking into consideration construction and operation aspects (see tables 1 and 2). The first group of aspects concerns the way the TOE is developed, the second one concerns the way it will be used. In the correctness criteria the construction aspects are further classified in development process and development environment aspects while the operation aspects are classified in operational documentation and operational environment aspects (table 2).

Table 2: Assurance correctness criteria

Group	General Aspect	Aspect
Construction	Development process	Requirements
		Architectural design
		Detailed design
		Implementation
	Development Environment	Configuration Control
		Programming languages and compiler
		Developers security
Operation	Operational Documentation	User documentation
		Administration documentation
	Operational Environment	Delivery and configuration
		Start-up and operation

For each aspect the following items are identified:

1) the documentation that needs to be provided for examination;
2) the requirements for documentation content and presentation;
3) the evidence required to show that the criteria in question have been met;
4) the actions to be performed by the evaluator.

The effectiveness assessment causes the evaluator to perform the same analysis and tests for every evaluation level. However the depth of such analyses and tests depends on the evaluation level because they need to be performed using the documents provided by the sponsor for the correctness assessment. Table 3 (ITSEC [2], figure 4) specifies the information that at least needs to be considered in the effectiveness evaluation for each evaluation level.

6 Impact of security evaluation on ETSI standards

The development of an Information Technology (IT) system or product, that needs to conform to a standard, depends on both developer's choices and standard specifications. Therefore, the security evaluation of such a system or product may fail either because of wrong developer choices or because of standard specifications that are considered inadequate by the security evaluator. In the latter case no IT system or product built to that standard could be successfully evaluated as the standard itself, rather than the system or the product, is rejected by the evaluator. To solve these problems, it would be necessary to make use of security evaluation criteria that permit the preliminary validation of the overall standard security specification. The validation process might consist of a security evaluation performed without having the implemented system or product at disposal, and using only a part of the required documentation for the target evaluation level. A validated standard will ensure that it is possible to implement a system or a product that conforms to the standard specification and is capable to pass evaluation at the evaluation level and minimum strength of mechanisms claimed in the security target. If the evaluation of this system or product fails, then the failure reason resides in its implementation and is not due to the standard specification. Therefore, if the standard is previously validated, then no question about it will arise whenever a conforming system or product fails the security evaluation. Unfortunately currently available or in development security evaluation criteria do not deal with such a validation.

Of course, even in the case of a system or product not built to a specified standard there is no guarantee that the security target written by the sponsor will allow a successful evaluation. To reduce the risk of evaluation failure, the first phase of the evaluation process described in the ITSEM [3] includes an optional feasibility study. This study will at least involve a review of the security target (ITSEM [3], subclause 1.2.17) and will assess the likelihood of a successful evaluation (ITSEM [3], subclause 4.2.20).

A more powerful way for reducing evaluation risk is to contact the ITSEF at the beginning of the standard development, according to the concurrent evaluation described in ITSEM [3], subclause 1.2.24. In this case the security target is drafted as the system or product development progresses and possible design deficiencies can be rapidly fixed.

Due to the lack of criteria which consider the standard validation it is possible at present to minimize the risk of unsuccessful evaluations due to standard deficiencies using the tools of the feasibility study or the concurrent evaluation. In the latter case a complete evaluation cannot be performed due to the unavailability of the TOE (the system under standardization), therefore also in this case the ITSEF involvement should be seen as pre-evaluation consultation.

7 Writing a security target

The security target should be provided by the sponsor together with all the other evaluation documents. However, as discussed above, in this case it is necessary that the standard developer (such as ETSI) writes it. The main reason for it is to allow the evaluator to perform a feasibility study, but lower costs of the evaluation are also expected as a useful consequence. Evaluations are indeed very expensive and a not negligible part of their cost is due to the preparation of the evaluation documentation. If the security target is provided by the standard developer, the sponsor will not be requested to perform a heavy reverse engineering starting from the standard specifications.

The required contents of a security target can be summarized as follows:

a) either a system security policy or a product rationale;

b) a specification of the required security enforcing functions;

c) a definition of required security mechanisms (optional);

d) the claimed rating of the minimum strength of mechanisms;

e) the target evaluation level.

Each of these is described in greater detail below.

7.1 System security policy or product rationale

The first part of the security target includes the security objectives, the intended environment, the threats and the list of the SEFs. For a system this part is the system security policy, for a product is the product rationale.

For a system, the actual operational environment is known and the threats to the system can be predicted. Existing countermeasures (which may be some combination of electronic, physical, procedural, and personnel countermeasures) can be taken into account and the security objectives of the system can be derived by the sponsor.

A product may be used in any number of different system and operational environments and so the actual operational environment of the product is not known. The product rationale can only define an intended method of use and make assumptions about the operational environment in which it is to be used and the threats that its SEFs are designed to encounter. For a product, the product rationale will comprise a list of claims made about the TOE by the sponsor aimed at providing a potential user with sufficient information to determine whether a product is suitable to satisfy some or all of his system security objectives.

A security policy or product rationale should express, without considering the design of the TOE, the assets to be protected and the rules governing the handling of the assets.

Security objectives

The security objectives are expressed in terms of the assets requiring protection (information to be handled by the TOE, processes to be automated by the TOE, etc.). There are three kinds of security objectives:

- availability objectives;
- integrity objectives; and
- confidentiality objectives.

Availability objectives are described in terms of status, capabilities, service duration, response times, priorities, and degradation tolerance.

Integrity objectives are described as one of:

a) conformance to standards specifications and references;
b) conformance to an initial state or condition;

c) rules to be observed for consistency and coherence.

Confidentiality objectives explain the expected use of each resource, rather than addressing vulnerabilities to be avoided (e.g. disclosure, context substitution, goal tampering).

The author of the security target should endeavour to make this section as complete as possible, since the security objectives ultimately form the baseline for the evaluation. Any feature of the TOE which cannot be traced back to a security objective cannot be considered security enforcing.

Intended environment

This section should define the:

a) purpose and boundary of the TOE;

b) information to be handled, and how it is to be handled;

c) personnel using the TOE (users, administrators, etc.);

d) the equipment necessary to support the TOE's operation;

e) location and topology of the TOE, including physical security measures;

f) operational modes and procedures;

g) organization and its procedures.

The threats

The perceived threats to the assets are actions that may violate the security objectives. Threat assessment is more difficult than determining the security objectives since it is impossible to address all possible modes of attack. Risk analysis methods can be helpful during threat assessment since they can provide a list of generic threats that can be readily applied to the TOE concerned.

Security target authors should be aware that they are responsible for the accuracy and completeness of the threats (and security objectives). Evaluators cannot verify the completeness of this information but will verify the accuracy and the consistency.

The list of SEFs

It is suggested that all SEF's should be listed grouping them according to the following generic headings:

a) identification and authentication;
b) access control;
c) accountability;
d) audit;
e) object re-use;
f) accuracy;
g) reliability of service;
h) data exchange.

7.2 Specification of the required security enforcing functions

In the case of a system, the security enforcing functions shall be correlated to the security objectives, so that it can be seen which functions satisfy which objectives. (A function may satisfy, or help to satisfy, more than one objective.) Every function in the specification of security enforcing functions shall at a minimum help to satisfy at least one objective. The specification of security enforcing functions shall also show why the functions are adequate to counter the identified or stated threats to the security objectives.

In the case of a product, the security enforcing functions shall be correlated to the intended method of use of the product and the assumptions about the environment into which the product will be installed given in the product rationale. This correlation shall include any dependencies on other security enforcing functions and non-IT security measures assumed to be provided by the environment.

From the point of view of evaluation, the specification of security enforcing functions is the most important part of the security target. These functions shall always be specified in an informal style, using natural language. In addition, at higher evaluation levels they also need to be specified using a semi-formal or formal style of presentation. Details of such presentation styles are given in the ITSEC [2].

7.3 Definition of the required security mechanisms

A security target may optionally prescribe or claim the use of particular security mechanisms. All security mechanisms included in a security target shall be correlated to its security enforcing functions, so that it can be seen which mechanisms implement each function (a mechanism may implement several functions, and a function may be implemented through the combination of several mechanisms).

Where security mechanisms are prescribed by the security target, it is the task of the developer to implement the required mechanisms. Otherwise, it is the task of the developer of the TOE to develop and produce mechanisms which, when combined, implement the required security enforcing functions. Obviously, in the case considered here (security standard), all the security mechanisms described in the standard specification need to be included in the security target.

7.4 Claimed rating of minimum strength of mechanisms

Every security target shall specify a claimed rating of the minimum strength of mechanisms against direct attack. This shall be one of the ratings:

- basic;
- medium; or
- high.

The minimum strength of mechanisms is the minimum strength of the critical mechanisms of the TOE. A critical mechanism is a mechanism whose failure would create a security weakness, i.e. the violation of one security objective at least. The strength of each critical mechanism can be rated as described in subclause 8.3. The strength of cryptographic mechanisms is outside the scope of the ITSEC [2], as are the key management mechanisms. An appropriate authority should state that the cryptographic and key management mechanisms of the TOE satisfy the claimed minimum strength of mechanisms rating.

7.5 Target evaluation level

Every security target shall specify a target evaluation level for evaluation of the TOE. This shall be one of the ratings **E1, E2, E3, E4, E5 or E6** as defined in chapter 4 of the ITSEC [2]. The choice of the target evaluation level should be made taking into account that:

1) the higher the evaluation level, the higher the likelihood that some vulnerabilities of the TOE or possible standard deficiencies may be found during the evaluation process (effectiveness assessment failure) since at the higher evaluation levels more detailed and formal evaluation documentation is requested (see table 3);

   NOTE: If ETSI provided no additional evaluation documentation, the evaluator would analyse the standard specifications more deeply in order to extract the detailed information requested at the target evaluation level.

2) the higher the evaluation level, the higher the likelihood that some errors in the implementation of the TOE built to the standard will be found by the evaluator (correctness assessment failure).

8 Writing additional evaluation documentation

In order to make the ITSEFs pre-evaluation consulting less time-consuming, the standardization body can write some parts of the additional evaluation documentation that in a typical evaluation the sponsor needs to provide together with the security target. More precisely, some or all of the following analyses in the field of effectiveness assessment can be carried out considering, at minimum, all of the information given in table 3 for the target evaluation level (architectural design, detailed design, etc.). Such information, that has to be extracted from the standard specification, may be also provided as additional evaluation documentation.

8.1 Suitability analysis

This analysis has to show that the security enforcing functions and mechanisms of the TOE will in fact counter all the threats identified in the security target and, as a consequence, all the security objectives are met. In this analysis it is not requested to take into account the composition of mechanisms (i.e. it is not requested to consider the architectural design of the TOE), but only to identify at least one function or mechanism that can counter each threat. Alternatively, the suitability analysis could be carried out in terms of security objectives. This approach may be preferable in the case of a product or where the threats are expressed at a higher level of granularity.

Table 3: Information obtained from a correctness assessment which is used to perform a vulnerability analysis

INFORMATION	E1	E2	E3	E4	E5	E6
Security Target (threats, objectives, functions, mechanisms, evaluation level, S of M)	-	-	-	-	-	-
Formal Model of Security Policy				-	-	-
Functions (informal)	-	-	-	-	-	-
Functions (semiformal)				-	-	
Functions (formal)						-
Architectural Design (informal)	-	-	-			
Architectural Design (semiformal)				-	-	
Architectural Design (formal)						-
Detailed Design (informal)			-			
Detailed Design (semiformal)				-	-	-
Implementation (hardware drawings and source code)				-	-	-
Implementation (object code)						-
Operation (user/administrator documents, delivery and configuration, start-up and operation)	-	-	-	-	-	-
	STATE		**DESCRIBE**		**EXPLAIN**	
	LEVEL OF RIGOUR					

8.2 Binding analysis

This analysis has to show that the security enforcing functions and mechanisms of the TOE will be able to work together in a way that is mutually supportive and will provide an integrated and effective whole. All potential interrelationships between security enforcing functions and mechanisms have to be investigated in order to show that it is not possible to cause any security enforcing function or mechanism to conflict with or contradict the intent of other security enforcing functions or mechanisms.

8.3 Strength of mechanisms analysis

This analysis has to show that all the critical security mechanisms are able to withstand direct attacks that do not require more resources, expertise and opportunity than those corresponding to the claimed minimum strength of mechanisms (basic, medium, or high). Since strength of mechanisms concerns resources, expertise and opportunity, it is necessary to expand on the meaning of these terms.

- **Resources** concern the resources an attacker needs to expend to successfully attack the TOE. Two types of resources are considered in the ITSEM [3]: **time and equipment.** Time is the time taken by an attacker to perform an attack, not including study time. Equipment includes computers, electronic devices, hardware tools, and computer software. **Unaided** means no special equipment is required to effect an attack; **domestic equipment** is equipment which is readily available within the operational environment of the TOE, or is a part of the TOE itself, or can be purchased by the public; **special equipment** is special-purpose equipment for carrying out an attack.

- **Expertise** concerns the knowledge required for persons to be able to successfully attack the TOE. A **layman** is someone with no particular expertise; a **proficient** is someone familiar with the internal workings of the TOE; an **expert** is someone familiar with the underlying principles and algorithms involved in the TOE.

- **Opportunity** covers factors which would generally be considered outside an attacker's control, such as whether another person's assistance is required (collusion) the likelihood of some specific circumstances arising (chance), and the likelihood and consequences of an attacker being caught (detection). These factors are difficult to rate in the general case and, as a consequence, the only case of collusion is covered in the ITSEM [3]. The following form of collusion are discussed: **alone** if no collusion is required; **with a user** if collusion is required between an attacker and an untrusted user of the TOE for an attack to succeed; **with an administrator** if collusion with a highly trusted user of the TOE is required.

Once the above mentioned factors have been evaluated for a particular mechanism, two numbers have to be found by looking up tables 4 and 5.

Table 4: Time and collusion

	COLLUSION		
TIME	**alone**	**with a user**	**with an administrator**
within minutes	0	12	24
within days	5	12	24
months/years	16	16	24

Table 5: Expertise and equipment

	EQUIPMENT		
EXPERTISE	**unaided**	**using domestic equipment**	**using specialist equipment**
layman	1	n/a	n/a
proficient	4	4	n/a
expert	6	8	12

Finally, the strength of the mechanism can be calculated by adding the two numbers together and by using the following rules:

- if the result is 1 then the strength is not even **basic**;

- if the result is greater than 1 but not higher than 12 then the strength is **basic**;

- if the result is greater than 12 but not higher than 24 then the strength is **medium**;

- if the result is greater than 24 then the strength is **high**.

8.4 Vulnerability analysis

This analysis has to show that the known vulnerabilities in construction and operation (associated with physical and administrative procedures external to the TOE) are not exploitable in practice, i.e. that:

- each vulnerability is adequately covered by other, uncompromised, security mechanisms; or

- the vulnerability is irrelevant to the security target, will not exist in practice, or is countered by technical, personal, procedural, or physical countermeasures outside the TOE.

8.5 Ease of use analysis

This analysis has to show that it is not possible to configure or use the TOE in a manner which is insecure but which an administrator end-user of the TOE would reasonably believe to be secure. The analysis should identify possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation. It also needs to show that any human or other error in operation that deactivates or disables security enforcing functions or mechanisms will easily be detectable.

9 Conclusions

The evaluation of a system or product built to a security standard requires additional costs not only in the phase of the evaluation itself, but also in the phase of the security standard development. The need of avoiding evaluation failures caused by possible standard deficiencies leads to require a pre-evaluation consultancy before the standard completion. Such a consultancy requires that some parts of the evaluation documentation be written by the standardization body before the standard be finalized. As a consequence, a not negligible increase of the standard development time and cost is expected and it is foreseeable that security evaluation will be rarely included as a standard specification.

Annex A: Common criteria document

In 1990 work began in ISO/IEC on the internationalisation of evaluation criteria. The new criteria was to be responsive to the need for mutual recognition of standardized security evaluation results in a global IT market. This task assigned to the JTC1 subcommittee SC27. In June 1993, the authors of the CTCPEC [6], FC [4] and [5], TCSEC [1] and ITSEC [2] pooled their efforts and began a project to align their criteria and create a single draft CC document. The intent of the project was to resolve the conceptual and technical differences found in the source criteria and then, to deliver the results to ISO as a contribution toward its work in progressing the international standard. The CC document is composed of four Parts, which are briefly described in the following.

Part 1: Introduction and general model

This is an introduction to the CC and defines general concepts and principles of IT security evaluation. It also presents a general model of evaluation. Part 1 presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the target audience is described, with pointers to the various parts of the CC where their individual interests with respect to security criteria and evaluation are covered.

Part 2: Security functionality requirements

This establishes a set of functional components as a standard way of expressing the functional requirements for TOEs. Part 2 catalogues the set of functional components, families and classes.

Part 3: Security assurance requirements

This presents evaluation assurance levels that define the CC scale for rating assurance for TOEs. Part 3 establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families and classes. Part 3 also defines evaluation criteria for protection profiles and security targets.

Part 4: Pre-defined protection profiles

This initially contains examples of protection profiles that represent functional and assurance requirements which have been identified in source criteria, including CTCPEC [6], FC [4] and [5], ITSEC [2] and TCSEC [1], as well as those requirements not represented in the source criteria. Part 4 will ultimately become the registry for protection profiles which have completed the registration process.

Part 5: Registration procedures

These are the procedures necessary to register additional protection profiles and to maintain in an international register.

History

Document history	
February 1997	First Edition

ISBN 2-7437-1301-1
Dépôt légal : Février 1997