4

Common Criteria for IT Security Evaluation - Update report

Developments in harmonisation of evaluation criteria

Author: Dr. Ir. Paul L. Overbeek
TNO Physics and Electronics Laboratory - p/a P.O.-Box 495 - 2600 AL Delft - Netherlands
Phone: ++ 31 70 3264221 - Fax: ++ 31 70 3280961 - Email: overbeek@fel.tno.nl

1. Introducing the Common Criteria

The European Community, the United States of America and Canada have embarked on a project which results in the next generation of criteria for the evaluation of security in IT-products. The outcome of this project is known as the Common Criteria (CC). The CC aligns the following existing and emerging criteria:

- ITSEC (Europe)
- USA New Federal Criteria including TCSEC (Orange Book)
- CTCPEC (Canada)
- ISO SC27 WG3 security evaluation criteria.

The CC defines a common set of criteria with the potential to ease the mutual recognition of evaluation results between nations. This is intended to facilitate the supply of security-evaluated products by eliminating the costs of multiple evaluations.

Goals of the Common Criteria (CC):
Backwards compatibility: The primary goal of the CC is to remain compatible with the individual source criteria and thus protect previous and ongoing investments in these criteria.

Flexibility: Another primary goal of the CC is to provide sufficient flexibility to allow a wide range of producers and consumers of IT products or systems to choose security functionality and assurance levels that adequately represent their IT security needs and match their business needs, now and in the future.

Furthermore, the CC provides a *yardstick* for producers and consumers and *stimulates* IT security by providing guidance for development to producers as well as guidance to consumers in the selection and specification of security functionality and assurance.

1.1 Current status

In November 1994 draft 0.9 of the CC was released. This release included:

- Part 1: the general model for evaluation.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

- Part 2: catalogue of security functions. This catalogue includes *functional components* grouped in the following classes: Identification and Authentication; Trusted Path; Audit; TOE Entry; User Data Protection; Resource Utilisation; Protection of the Trusted Security Functions; Privacy (preliminary) and Communication. These functions can be grouped in so called *functional packages* offering the functionality needed in a specific (business) case.
- Part 3: defines the *assurance components*, grouped in the following classes: Development; Tests; Vulnerability assessment; Configuration management; Life-cycle support; Guidance documentation; and Delivery and Operation. Seven *assurance levels*, created from the components will be defined, four are available in the current draft.
- Example *Protection Profiles*: a Protection Profile (PP) is a definition of the security needs in a generic threat environment. The security functionality in a PP is expressed in the functional components of Part 2. Furthermore, the PP includes an assurance level.
- Guidance documentation: technical rationale, mapping tables, etc. The guidance documentation explains how the concepts of the source criteria are preserved and how mapping between the source criteria and the CC is performed.

1.2 Review process

Draft 0.9 is distributed to experts in the field of IT security for review and comments. The review period will officially end in March 1995. The following is organised to guide the review: supporting guidance documentation; electronic comment services; and possibly a workshop.

1.3 Workplan

A definitive workplan for completion of the CC will depend on the comments received in the review process. Currently it is anticipated that in 1995: the current draft will be progressed towards the 1.0 version (in liaison with ISO); development of the evaluation methodology will start; trial evaluations will begin; enabling activities for, e.g. mutual recognition will start.

2. International harmonisation of evaluation criteria

The *history* of security evaluation criteria starts, unobserved, somewhere in the seventies when the first ideas of the Orange Book [9] were born. The Orange Book was published in 1985 and remained the single baseline for security evaluations for a long time.
Significant evolution of security evaluation criteria has taken place since 1990. In Europe, national evaluation criteria became prominent. In a European harmonisation effort, driven by France, the UK, Germany and the Netherlands, these national criteria

were combined in the ITSEC [6]. The ITSEC was published in June 1991 and is in wide use within Europe now. Within ISO/SC27 work on security evaluation criteria started in 1991. In Canada the CTCPEC was published in 1993, and, also in 1993, in the US the first draft new Federal Criteria (FC) came out to replace the Orange Book.

It became very clear that the driving factors for security evaluations were changing, and lead to new market needs for information security. Most important factors are:

- More and more the manufacturers act as sponsors of evaluations (especially in Europe), where in the past a government agency acted as the initiator of an evaluation. The motivation for a manufacturer is quite different from that of a national agency. For manufacturers, some motivations are: access to different markets with evaluated products, improvement of the products, international marketing value of a certificate. But, for a manufacturer it is also important that evaluations are synchronised with his normal development process and release schedule.
- Information technology (IT) has developed considerably since the birth of the Orange Book, and will continue to do so in the future. This requires a flexible framework for evaluation criteria; take for example the changing needs for security in open, distributed systems, requiring evaluation of subsystems and an architecture for assurance in these composite systems [9].
- The usage of IT has changed as well. New security requirements arise, for example in mission and safety critical systems with emphasis on the availability and integrity aspects of information security.
- Market trends ask for 'globalisation' of security evaluations. Both manufacturers and end-users of IT-products work internationally nowadays.
- One of the major goals of evaluation criteria is to stimulate and improve IT security both for developers and end-users. Realistically speaking, this goal can only be achieved within a limited financial bandwith. Or, to state it differently, costs of evaluations *is* a vital issue.

A larger world-wide view on security evaluations is highly desirable, and that is the major driving force for the Common Criteria for Information Technology Security Evaluation (CC).

The development of the CC started in late 1993. The first public 'preliminary draft' was published in late 1994. The development of the CC is a cooperative activity of the European Union (or, to be more precise: France, Germany, United Kingdom, and the Netherlands), the USA (NSA and NIST) and Canada.
The CC aligns the following existing and emerging criteria:

- ITSEC (Europe)
- USA New Federal Criteria, including TCSEC (Orange Book)
- CTCPEC (Canada)

- ISO SC27 WG3 security evaluation criteria.

The CC defines a common set of criteria with the potential to ease the mutual recognition of evaluation results between nations. This is intended to facilitate the supply of security-evaluated products by eliminating the costs of multiple evaluations. The CC is being developed by the Common Criteria Editorial Board, in which the 'shepherds' of the existing criteria are all represented. This is ensure that the CC is indeed compatible with these criteria.

3. The Common Criteria

3.1 Usage and goals of the Common Criteria

IT security evaluations are formal investigations of the security properties of products and systems. Three groups of people with a general interest in these evaluations can be identified:

- *Consumers* or *procurers* of IT products or systems.
  The consumers or procurers can use the evaluation results to help decide whether an evaluated product or system fulfils their security needs. The CC also gives consumers, especially in consumer groups and societies, a structure in which to express their special requirements for IT security measures in a product or system which can then be built to meet those requirements. This requirements structure is called a Protection Profile (PP), a term which is explained below.
- *Developers* or *producers* of IT products or systems.
  The intent of the CC is also to support the developers or producers in preparing for and assisting in the evaluation of their products or systems appropriately. The clear and precise structure provided by the CC for stating security requirements aids the developers or producers in identifying those requirements to be satisfied by their own product or system to be evaluated. Moreover, the developers can use the CC to determine their responsibilities and actions in supporting the evaluation. The CC describes the actions a developer is to carry out and defines all the deliverables a developer is to provide for an evaluation.
- *Evaluators* of IT products or systems.
  The evaluators can find evaluation requirements in the CC. The CC describes the specific actions the evaluator is to carry out.

Goals of the Common Criteria (CC) are:

- *Backwards compatibility*: The primary goal of the CC is to remain compatible with the individual source criteria and thus protect previous and ongoing investments in these criteria.

- *Flexibility*: Another primary goal of the CC is to provide sufficient flexibility to allow a wide range of producers and consumers of IT products or systems to choose security functionality and assurance levels that adequately represent their IT security needs and match their business needs, now and in the future. One example is that the CC is independent of a specific security policy.
- Furthermore, the CC provide a *yardstick* for producers and consumers and *stimulate* IT security by providing guidance for development to producers as well as guidance to consumers in the selection and specification of security functionality and assurance.

3.2 Scope and boundaries of the Common Criteria

There are a lot of expectations about what the CC is, but it should be noted that in this stage of international harmonisation, the CC is an alignment effort. This alignment goes, in my view, slightly beyond 'just' alignment of criteria. It is also a matter of alignment of minds and of concepts surrounding the evaluation process: recognising cultural differences between the evaluating authorities. Furthermore, the CC must be seen in the interest of cooperation between nations and in the interest in removing barriers for international trade (as promoted in the GATT).

Inside the scope of the CC are:

- Evaluation of IT security aspects of IT products or systems.
- Protection of information from human or other threats of disclosure (confidentiality, exclusivity), modification (integrity) and denial (availability).
- Technical aspects of security. Not: organisation, procedures, and physical security.
- Usage and interfacing with cryptographic functions, but not the cryptographic algorithms itself since this is considered to be 'national interest'.

Outside the scope of the CC are:

- Evaluation of non-technical aspects.
- Cryptographic algorithms.
- Methodology for evaluation. A 'Common ITSEM' [7] is needed for mutual recognition. Start of development is scheduled for 1995 (see 'Current plans').

3.3 Structure and concepts

The following key concepts are used in the Common Criteria: Protection Profile, Security Target, Functional Specification, and Assurance Levels. These concepts are discussed briefly below.

3.3.1 Protection Profile

A Protection Profile (PP) is a definition of the security needs in a generic threat environment. A PP's security *objectives* describes the purpose or goals to be achieved (WHY protection is needed). The PP's security *requirements* describe the functionality

that is needed to fulfil the objectives (WHAT functionality is needed to offer the protection we want). In addition the assurance level (see below) indicates the degree of trustworthiness that is needed in the threat environment.

Currently, two example PPs are furnished for review.
One is named CC/CS1 (Commercial Security 1). CC/CS1 maps to ITSEC F-C2/E2, Orange Book C2, FC CS1 and CTCPEC 'CS1'. Profile CC/CS1 addresses the security needs for general purpose multi-user operating systems, for use in a commercial environment. For government environments, CC/CS1 compliant operating systems are intended to process 'sensitive-but-unclassified' information or 'single level' classified information. Some typical 'threat agents' in this environment are: unauthorised employees (insiders), careless authorised users, hostile authorised users and hostile outsiders. Functional requirements include specific functionality (called 'functional components') for access control, object reuse, identification and authentication, audit, and system's integrity. Architectural constraints are defined in the following areas: domain separation, administration, and mediation of access to objects.
The assurance requirements for CC/CS1 consist of Assurance Level AL3, 'Structurally Tested'. Assurance components of AL3 include: informal architecture, design, and model; testing and guidance for end-users and administrators.

The second example PP is CC/CS3 (Commercial Security 3).
CC/CS3 exceeds CC/CS1 in additional functionality for availability and data integrity. The grouping of assurance components is named AL3 - Augmented "Advanced Commercial Security". This is an augmentation of AL3 "Structurally Tested" with additional components, e.g. how to deal with flaws and incidents and the development life-cycle.

These are just two examples. To give some ideas, other PPs could be developed for: a security 'firewall', the POSIX security interfaces, ANSI banking standards, an access control mechanism based on biometrics, security in client-server applications. Also more general PPs can be developed, e.g. PPs for privacy-related applications, PPs for the medical environment, PPs for the mission or safety critical environments and PPs for business-to-business purposes (EDI, E-mail).

A PP is developed by a community of interest, typically a group of users with common IT security needs. That PP is then evaluated and is made available for general use via registration.

3.3.2 Security Target

The Security Target (ST) serves both as a definition of the security functions and of the assurance measures of the product which will be evaluated. It forms the basis for

agreement between the developers, the evaluators and possibly the end-users of the product.

There are clear relationships between PP and ST. A developer, perceiving the market demand represented by the PP develops a (yet, potentially conformant) IT product in response. The developer of the product produces a ST that describes the implementation of the PP in the product. The ST is checked for conformity to the PP, and the product is in turn evaluated for conformity to the ST.

The ST may or may not claim conformance to a PP. If a product is just an implementation of a PP, the ST is simply a claim of conformance to that PP. If the product does not conform to a PP, or adds additional functions to an existing PP, the ST itself is evaluated in a similar manner as a PP is evaluated (the obvious idea springs to mind that the evaluated ST could serve as the basis for a new PP).

3.3.3 Security Functional Specification

The PP/ST-level describes WHY protection is needed in a generic (for PP) or more specific (for ST) environment. The PP/ST-level also describes WHAT functionality is needed to offer that protection. Now the Security Functional Specification describes HOW that functionality is offered. The functional specification is used as the first step into the assurance part of the criteria, in a range from informal, semiformal to formal specification.

3.3.4 Assurance Levels

The use of assurance levels provides graduated classes of assurance which differ in an increasing degree of assurance. Seven assurance levels are defined, numbered AL1 to AL7. AL0 is reserved for products that failed in the evaluation. Each assurance level is a set of assurance components (see below). Beside a number, each assurance level is given a popular name to characterize the level.

The levels are:

- AL0 Unassured
- AL1 Tested
- AL2 Structurally tested
- AL3 Methodically tested and checked
- AL4 Methodically tested and reviewed
- AL5 Semiformal design
- AL6 Semiformally verified design
- AL7 Formally verified design

Currently, four levels are fully described.

3.3.5 Assurance classes

The CC recognises assurance aspects, called *assurance classes*. The most important classes are:

- Development, subdivided in:
  - Functional specification
  - Trusted Security Functionality, internals and interfaces
  - High- and low-level design
  - Implementation
- Testing
- Vulnerability assessment
- Configuration management
- Life-cycle support
- Documentation and guidance
- Delivery and operation

Each assurance class is further subdivided in (hierarchically ordered) *assurance components*, thus offering a very flexible way to define assurance aspects while retaining a high level of granularity. An assurance level is composed of these components.

3.3.6 Functionality classes

A catalogue of security functions is available in Part 2 of the CC. The security functions, or *functional components*, are also grouped in classes. Currently, the following classes are defined:

- Identification and Authentication
- Trusted Path
- Audit
- Product Entry (session management)
- User Data Protection (access control)
- Resource Utilisation
- Protection of the Trusted Security Functions
- Privacy (preliminary)
- and Communication.

These functions can be grouped in so called *functional packages* offering the functionality needed in a specific (business) case. A functional package plus an assurance level is a good start for a protection profile.

4. Current plans

In November 1994 draft 0.9 of the CC was released. Currently, the ideas to progress the CC include the following activities.

4.1 Review process

Draft 0.9 is distributed to experts in the field of IT security for review and comments. Result of the review period will be presented at the conference. To benefit the most from this review supportive review guidance and electronic comment forms are available. There are plans for a workshop, and major conferences are selected to advertise the CC and its benefits to a wide knowledgeable audience.

4.2 Workplan

A definitive workplan for completion of the CC will depend on the comments received in the review process. Currently the following activities are schedule for 1995:

- The current draft will be progressed towards the 1.0 version. This will be done in liaison with ISO. At several places in the CC 0.9-version 'TBD' (to be defined) indicates where the current draft is yet incomplete.
- Development of a common evaluation methodology: criteria alone are not sufficient to come to identical, predictable, repeatable and independent evaluation results. Therefore an evaluation methodology is needed, comparable with the European ITSEM [7] which serves as the evaluation methodology for the ITSEC.
- Trial evaluations
- Enabling activities, e.g. for mutual recognition.

5. References

1 *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC), version 3.0, CSSC, CSE, Jan. 1993

2 *Code of Practice for Information Security Management*, BSI DISC PD0003, DTI September 1993

3 *Common Criteria for Information Technology Security Evaluation*, (parts 1-3), version 0.9, October 1994

4 *Evaluation Criteria for IT Security*, parts 1-3, developed by ISO/IEC/JTC1 SC27/WG3

5 *Federal Criteria for Information Technology Security* (FC), draft 1.0, NIST/NSA, Jan. 1993

6 *Information Technology Security Evaluation Criteria* (ITSEC), version 1.2, June 1991

7 *Information Technology Security Evaluation Manual* (ITSEM), version 1.0, September 1993

8 *Towards secure open systems*, Overbeek P.L., ISBN 90-9005824-9, 2nd ed. July 1993

9 *Trusted Computer Systems Evaluation Criteria* (TCSEC or Orange Book), US DoD 5200.28-STD, Dec. 1985