The Common Criteria

Nancy R. Mead, Software Engineering Institute [vita[3]]

2006-08-10; Updated 2008-09-22

L4 / L[4]

The Common Criteria enable an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements. Although the focus of the Common Criteria is evaluation, it presents a standard that should be of interest to those who develop security requirements.

The Common Criteria (CC) were developed through a combined effort of six countries: the United States, Canada, France, Germany, the Netherlands, and the United Kingdom. This effort built on earlier standards, including Europe's Information Technology Security Evaluation Criteria (ITSEC), the United States' Trusted Computer System Evaluation Criteria (TCSEC), and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [Caplan 99[5]]. The CC is an international standard (ISO[6]/IEC[7] 15408) for computer security. A Common Criteria evaluation allows an objective evaluation to validate that a particular product satisfies a defined set of security requirements. The focus of the Common Criteria is evaluation of a product or system, and less on development of requirements. Nevertheless, its evaluation role makes it of interest to those who develop security requirements. The Common Criteria allow for seven Evaluation Assurance Levels (EALs), which will be discussed further.

An overview of the common criteria can be found at http://en.wikipedia.org/wiki/Common_Criteria. A definitive source of current information about the Common Criteria is the Common Criteria Portal[9]. Much of the material in this discussion is drawn from an earlier report [Mead 03[10]].

Common Criteria Overview

The Common Criteria contain a grouping of 60 security functional requirements in 11 classes [Abrams 00[13]]. This grouping allows specific classes of requirements to be evaluated in a standard way in order to arrive at an Evaluation Assurance Level.

A package is an intermediate combination of requirements components that allows expression of a set of functional or assurance requirements that meet a subset of security objectives. A Protection Profile (PP) is an implementation-independent set of security requirements for a class of Targets of Evaluation (TOEs) that meet specific consumer needs. An example of a TOE is an IT product or system, together with its documentation and administration, that is the subject of a CC evaluation. Other examples of TOEs can be found in [CC 06[14]].

A PP allows security requirements to be expressed using a template in an implementation-independent way, and is thus reusable. This provides benefits when implementing a family of related products or a product line. A Security Target (ST) contains a set of security requirements that can be stated explicitly. An ST includes detailed product-specific information. It can be viewed as a refinement of the PP, and forms the agreed-upon basis for evaluation. This hierarchy is shown in Figure 1. Note that in Figure 1, development

3. daisy:230-BSI (Mead, Nancy)
5. #refs
6. http://en.wikipedia.org/wiki/International_Organization_for_Standardization
7. http://en.wikipedia.org/wiki/International_Electrotechnical_Commission
9. http://www.commoncriteriaportal.org
10. #refs
13. #refs
14. #cc06

of security objectives would precede identification of security requirements. Another way to view this is to consider the refinement of specifications, as shown in Figure 2, which has a waterfall-like quality. Figure 2 links the specification framework to the TOE or product/system.

Figure 1. Common Criteria modular component hierarchy

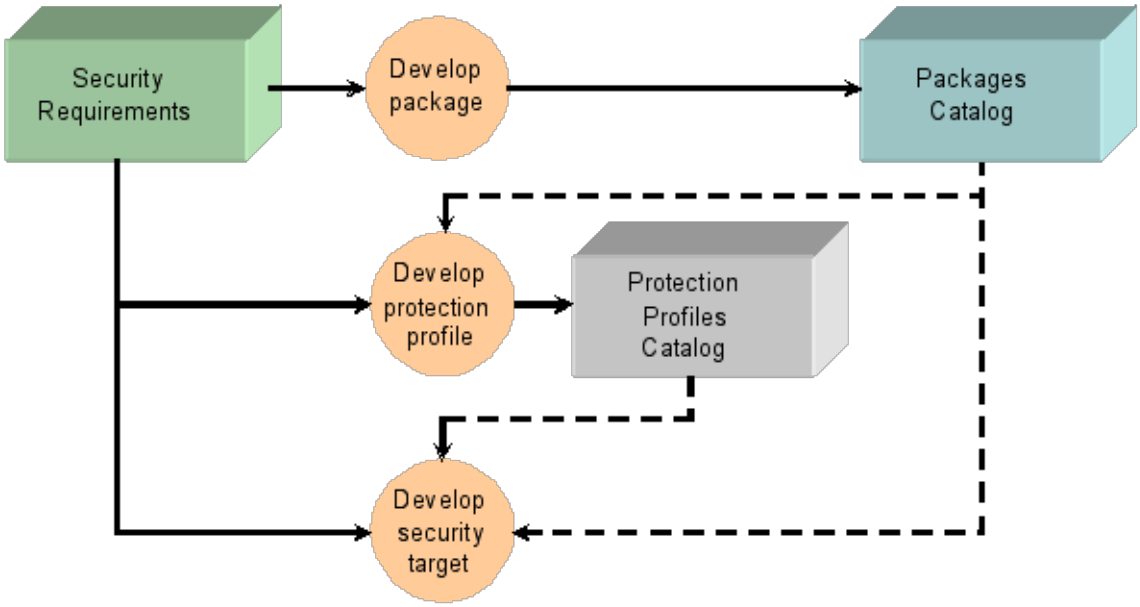
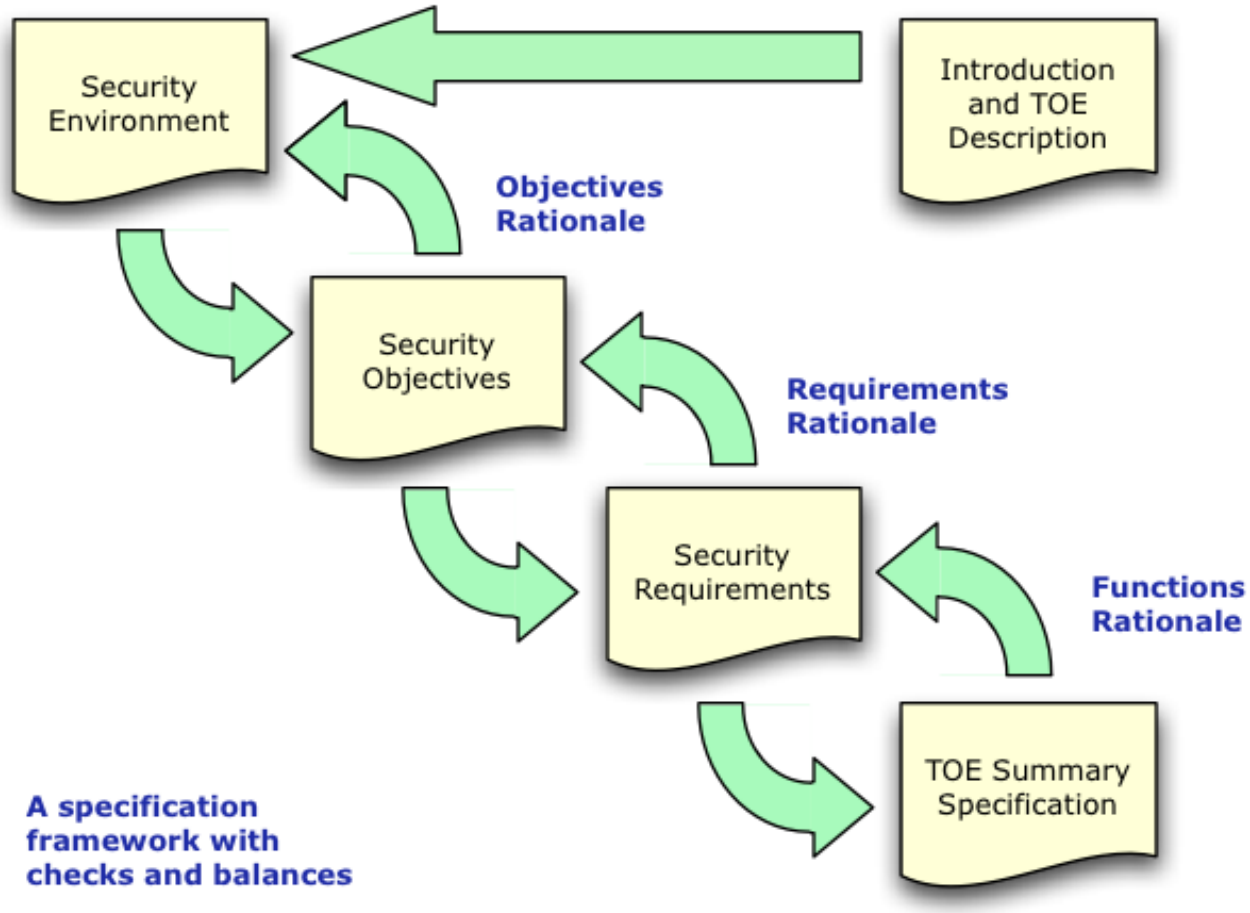


Figure 2. The PP/ST specification framework



The successful use of the Common Criteria depends on an ability to define the required security capabilities. This should be done in a way that gives consideration to the mission or business, the assets requiring protection, and the purpose of the system under evaluation (the TOE). As the Common Criteria have matured, a number of protection profiles have been developed by the National Security Agency (NSA) and then by NSA in conjunction with the National Institute of Standards and Technology (NIST). A working group called the Protection Profile Review Board (PPRB) was formed to review all proposed Protection Profiles and to work with the authors toward achieving a goal of consistency across PPs. Such consistency would presumably result in more consistency in applying the Common Criteria to various TOEs. A number of recommendations toward this end have been collected in one document [PP 02[20]].

Common Criteria Evaluation Assurance Levels

Functional and assurance security requirements are the basis for the Common Criteria. There are seven Evaluation Assurance Levels (EALs). The higher the level, the more confidence you can have that the security functional requirements have been met. The levels are as follows:

- **EAL1: Functionally Tested.** Applies when you require confidence in a product's correct operation, but do not view threats to security as serious. An evaluation at this level should provide evidence that the target of evaluation functions in a manner consistent with its documentation and that it provides useful protection against identified threats.

20. #refs

- **EAL2: Structurally Tested.** Applies when developers or users require low to moderate independently assured security but the complete development record is not readily available. This situation may arise when there is limited developer access or when there is an effort to secure legacy systems.
- **EAL3: Methodically Tested and Checked.** Applies when developers or users require a moderate level of independently assured security and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.
- **EAL4: Methodically Designed, Tested, and Reviewed.** Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs.
- **EAL5: Semi-Formally Designed and Tested.** Applies when developers or users require high, independently assured security in a planned development and require a rigorous development approach that does not incur unreasonable costs from specialist security engineering techniques.
- **EAL6: Semi-Formally Verified Design and Tested.** Applies when developing security targets of evaluation for application in high-risk situations where the value of the protected assets justifies the additional costs.
- **EAL7: Formally Verified Design and Tested.** Applies to the development of security targets of evaluation for application in extremely high-risk situations, as well as when the high value of the assets justifies the higher costs.

Common Criteria Usage

One way in which the Common Criteria can be used is in conjunction with system acquisition [Abrams 00[39]]. A mapping between CC features and system acquisition elements is shown in Table 1. In the first row, the protection profile concept helps to identify, among other things, customer requirements. These can in turn be used in a Request for Proposal (RFP). The fact that there are many protection profile templates in existence is very helpful to this part of the effort. The notion of the security target in the second row gives an indication of how the requirements might be satisfied by specific suppliers. Of course, the TOE is intended to be a specific system or collection of components that can be evaluated. Finally, the evaluated and accepted system should support consistency of the outputs of the previous three rows. From the point of view of a model, this provides a series of representations that can be checked and compared to one another. This is consistent with acquisition activities at the Federal Aviation Administration (FAA). This sort of example of consistency suggests broad application of the Common Criteria, particularly to critical infrastructure systems.

Table 1. Mapping between CC features and system acquisition elements

CC Paradigm	System Acquisition Paradigm	Observations Regarding Commonality Among CC and Acquisition Paradigms
Protection Profile (PP)	Request for Proposals	Provides customer desires, needs, and requirements: "What is wanted"
Security Target (ST)	Proposals	Indicates how the above will be satisfied by suppliers: "What will be provided"

39. #refs

Target of Evaluation (TOE)	Delivered System	Is the supplier's physical manifestation of above
Evaluated System	Accepted System	Shows that the three preceding representations are sufficiently consistent

The FAA's National Airspace System Infrastructure Management System (NIMS) provided a venue for development of its own PP. Specific requirements were derived from and linked to the CC components. A set of eight example requirements is provided [Abrams 00[42]]. This is followed by a discussion of system integration and acceptance test considerations that result from application of the CC. As a result of several reviews, by a wide spectrum of FAA staff members, the NIMS protection profile was broadly accepted by the community it served. Many Microsoft products have undergone CC evaluation at EAL level 4 (see [MS TechNet 05]). Recent studies [Keblawi 06] suggest that a more unified approach to security requirements engineering is needed if use of the Common Criteria and its system-level protection profiles (SLPPs) is to be successful.

Benefits/Business Case

The FAA Telecomm services provided a source for a CC case study [Herrmann 01[45]]. In this study the FAA Telecommunications Infrastructure (FTI) project provides an example of a services contract that uses the CC. FTI provides integrated voice, data, and video telecommunications services in the continental U.S., with connectivity to Hawaii, Alaska, and U.S. territories. FTI requirements are expressed in terms of service classes and service interfaces. In this particular case, the vendor is required to demonstrate EAL3. The authors discuss the meaning of an EAL in the context of a services contract, and also the effort involved in maintaining an EAL during the entire systems life cycle, after systems development. Both the Common Criteria and process assessments were used to maintain a balanced security assurance program.

Another example, the PalME project, an electronic purse application for Palm handhelds, provides a case study for application of the Common Criteria [Vetterling 02[46]]. It was felt that there was some documentation overhead associated with use of the CC, but nevertheless using the CC for this project was practical.

Recent experience [Barnes 06] indicates that achievement of higher EAL levels is feasible and cost-effective.

Maturity of Practice

Common Criteria is a mature practice, although most projects are evaluated at the lower assurance levels EAL1 through EAL3.

References

[Abrams 00] Abrams, M. D. & Brusil, P. J. "Application of the Common Criteria to a System: A Real-World Example." 11-21. *Computer Security Journal.* 16. 2. Spring 2000.

42. #refs
45. #refs
46. #refs

[Barnes 06] Barnes, J., Chapman, R., Cooper, D., Everett, B., Johnson, R., Widmaier, J. "Engineering the Tokeneer Enclave Protection Software", *Proceedings of the 1st International Symposium on Secure Software Engineering*, IEEE, March, 2006.

[Caplan 99] Caplan, K. & Sanders, J. L. "Building an International Security Standard." 29-34. *IEEE IT Professional.* 1. 2. March/April 1999.

[CC 06] Common Criteria for Information Technology Security Evaluation[49], Part 1: Introduction and general model, Version 3.1, Revision 1 (CCMB-2006-09-001), September 2006.

[Herrmann 01] Herrmann, D. & Keith, S. "Application of Common Criteria to Telecomm Services: A Case Study." 21-28. *Computer Security Journal.* XVII. 2. Spring 2001.

[Keblawi 06] Keblawi, F., Sullivan, D., "Applying the Common Criteria in Systems Engineeering." 50-55. *IEEE Security & Privacy*, 4. 2. March/April 2006

[Mead 03] Mead, N. *International Liability Issues for Software Quality* (CMU/SEI-2003-SR-001, ADA416434). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. http://www.sei.cmu.edu/publications/documents/03.reports/03sr001.html

[MS TechNet 05] Microsoft TechNet. Common Criteria Certification: Microsoft Windows Platform Products[51], December 14, 2005.

[PP 02] *Protection Profile (PP) Consistency Guidance for Basic Robustness, Release 1.1*. September 2002. http://www.iatf.net/protection_profiles/

[Vetterling 02] Vetterling, M.; Wimmel, G.; & Wisspeintner, A. "Secure Systems Development Based on the Common Criteria: The PalME Project." 129-138. *Proceedings of SIGSOFT 2002/FSE-10.* Nov. 18-22, 2002. Charleston, SC. New York, NY: Association for Computing Machinery, 2002.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. http://www.sei.cmu.edu/about/legal-permissions.html