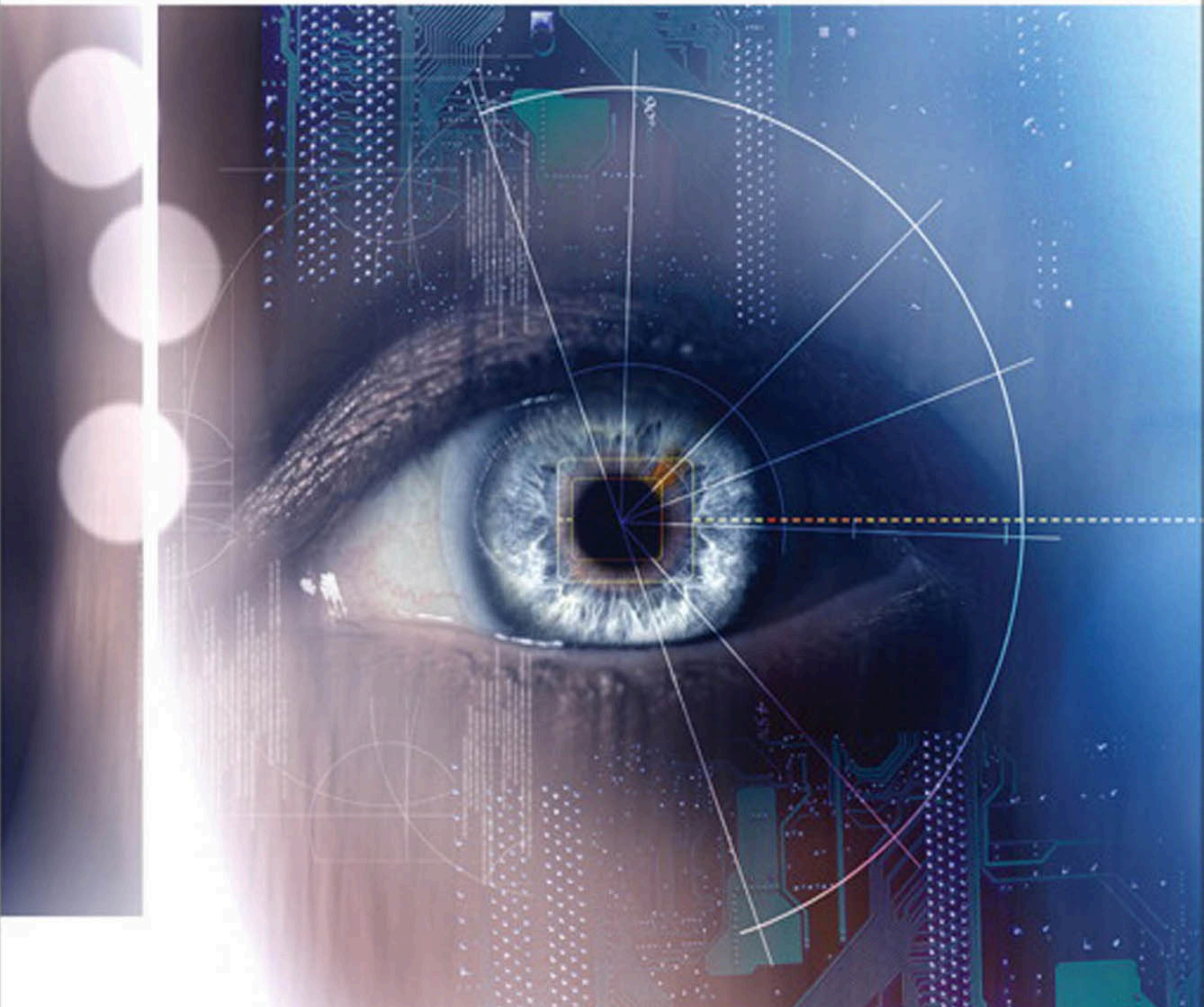

INFORMATION SECURITY

PRINCIPLES AND PRACTICES

SECOND EDITION

MARK S. MERKOW • JIM BREITHAUPT

Information Security: Principles and Practices

Second Edition

Mark S. Merkow
Jim Breithaupt

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

The Common Criteria

Joint efforts among the United States (TCSEC), Canada (CTCPEC), and Europe (ITSEC) began in 1993 to harmonize security evaluation criteria to enable true comparability for the results of independent security evaluations. These joint activities were designed to align international separate criteria into a single set of IT security criteria that could be broadly used. The activity, named the Common Criteria (CC) Project, was intended to resolve the conceptual and technical differences in the various source criteria and to deliver the results to the International Organization for Standardization (ISO) as a proposed international standard under development.

FYI: Formal Security Testing in the Real World

These concepts and processes might seem a bit of overkill, but serious buyers of security products should never ignore assurance of commercial products. To better understand how security evaluations work in practice and what their value is to government and commercial buyers of security products, visit the Common Criteria Portal at www.commoncriteriaportal.org.

Representatives of the sponsoring organizations formed the CC Editorial Board (CCEB) to develop the CC, and the CCEB and ISO Working Group 3 (WG3) established a liaison relationship. The CCEB contributed several early versions of the CC to WG3 via the liaison. As a result of the interaction between WG3 and the CCEB, successive versions of the CC were adopted as working drafts of the various parts of the CC beginning in 1994. Work continued for the next 5 years to harmonize requirements. In June 1999, the Common Criteria for IT Security Evaluation became ISO International Standard 15408. It focuses on security objectives, the related threats (malicious or otherwise), and the functional requirements relevant to security.

The market force driving the need for harmonized criteria is best understood by an example. Imagine that a vendor of firewalls in Germany wanted to sell its ITSEC-evaluated product to an American government agency. If the U.S. agency required the product for a classified government system, the German firewall vendor would have no choice but to sponsor a separate evaluation of its product in the United States using TCSEC criteria, adding tremendous cost and time to the process of successfully selling its products beyond the German border.

The Common Criteria addresses this problem through a mutual recognition of the final certificates granted to successfully evaluated products and eliminates the need for multiple evaluations and their associated costs and time requirements.

The Common Criteria, also known as ISO 15408, combines the best features of the TCSEC with the ITSEC and the CTCPEC, and synergizes them into a single international standard.

Many countries and organizations participated in the development of the Common Criteria:

- **Canada:** Communications Security Establishment
- **France:** Service Central de la Securite des Systémes d’Information

- **Germany:** Bundesamt fur Sicherheit in der Informationstechnik
- **The Netherlands:** Netherlands National Communications Security Agency
- **United Kingdom:** Communications-Electronics Security Group
- **United States:** National Institute of Standards and Technology and the National Security Agency

The CC provides a common language and structure to express IT security requirements and enables the creation of catalogs of standards broken down into components and packages. The CC breaks apart the functional and assurance requirements into distinct elements that users can select for customized security device implementation.

Packages permit the expression of requirements that meet an identifiable subset of security objectives. Packages are reusable and can be used to construct larger packages as well. Using the CC framework, users and developers of IT security products create protection profiles (PPs) as an implementation-independent collection of objectives and requirements for any given category of products or systems that must meet similar needs (such as firewalls). Protection profiles are needed to support defining functional standards and serve as an aid in specifying needs for procurement purposes.

Whereas protection profiles work as a generic description of product and environmental requirements, targets of evaluation (TOE) are the specific products or systems that fall into an evaluation against an existing PP. The sets of evidence about a TOE and the TOE itself form the inputs to a security target (ST) that certified independent evaluators use as the basis for evaluation.

Again, two types of security requirements exist: functional and assurance. Functional requirements describe what a product needs to do, and assurance requirements describe how well it meets the functional requirements. Consumers need both pieces of data to effectively judge the merits of one product over another.

In defining security requirements for a trusted product or system, users and developers need to consider the threats to the environment. The Common Criteria provides a catalog of components (Part 2 of the CC) that developers of PPs use to form the requirements definition. Assurance requirements (defined in Part 3 of the CC) contain two classes from which evaluation assurance requirements can be selected, along with a class for assurance maintenance.

Protection Profile Organization

A protection profile is organized as follows:

- Introduction section, which provides descriptive information needed to identify, catalog, register, and cross-reference a PP. The overview provides a summary of the PP as a narrative.
- Target of evaluation (TOE) description, which describes the TOE to aid in understanding its security requirements and addresses the product type and general features of the TOE, providing a context for the evaluation.

- Security environment, which consists of three subsections:
    - Assumptions
    - Threats
    - Organizational security policies

These sections describe the security aspects of the environment in which the TOE will be used and the manner in which it will be used. Assumptions describe the security aspects of the environment in which the TOE will be used, including information about the intended usage, aspects about the intended applications, potential asset value, and possible limitations of use. The threats section covers all the threats for which specific protection within the TOE or its environment is needed. It includes only threats that are relevant to secure TOE operation. Organizational security policies identify and explain any security policies or rules that govern the TOE or its operating environment.

- Security objectives address the entire security environment aspects identified in earlier sections of the PP. These objectives define the intent of the TOE to counter identified threats and include the organizational security policies and assumptions. This section defines in detail the security requirements that by the TOE or its environment must satisfy. TOE security requirements describe the supporting evidence needed to satisfy security objectives. Functional requirements are selected from the CC functional components (Part 2).
- Assurance requirements are stated as one of the evaluation assurance levels (EALs) from the CC Part 3 assurance components.
- Rationale presents the evidence used by a PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a compliant TOE provides an effective set of IT security countermeasures within the security environment.

Security Functional Requirements

The following are classes of security functional requirements (component catalog):

- **Audit:** Security auditing functions involve recognizing, recording, storing, and analyzing information related to security-relevant activities. The resulting audit records can be examined to determine which security-relevant activities took place and which user is responsible for them.
- **Cryptographic support:** These functions are used when the TOE implements cryptographic functions in hardware, firmware, or software.
- **Communications:** These functional requirements are related to ensuring both the identity of a transmitted information originator and the identity of the recipient. These functions ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it.
- **User data protection:** This class of functions is related to protecting user data within a TOE during import, export, and storage.

- **Identification and authentication:** These functions ensure that users are associated with the proper security attributes (including identity, groups, and roles).
- **Security management:** These functions are intended to specify the management of several aspects of the TOE security functions security attributes and security data.
- **Privacy:** These requirements protect a user against discovery and misuse of identity by other users.
- **Protection of the TOE security functions (TSF):** These requirements relate to the integrity and management of the mechanisms that provide the TSF and to the integrity of TSF data.
- **Resource utilization:** These functions support the availability of required resources such as CPU and storage capacity. Fault tolerance protects against unavailability of capabilities caused by failure of the TOE. Priority of service ensures that the resources will be allocated to the more important or time-critical tasks and cannot be monopolized by lower-priority tasks.
- **TOE access:** These requirements control the establishment of a user's session.

Evaluation assurance classes include the following:

- Configuration management helps ensure that the integrity of the TOE is preserved through required discipline and control in the processes of refinement and modification of the TOE and other related information. Configuration management prevents unauthorized modifications, additions, or deletions to the TOE and provides assurance that the TOE and documentation used for evaluation are the ones prepared for distribution.
- Delivery and operation classes define the requirements for the measures, procedures, and standards concerned with secure delivery, installation, and operational use of the TOE. This ensures that the security protection the TOE offers is not compromised during transfer, installation, startup, and operation.
- Development classes define the requirements for the stepwise (proceeding in steps) refinement of the TOE security functions (TSF) from the summary specification in the security target, down to the actual implementation. Each of the resulting TSF representations provides information to help the evaluator determine whether the functional requirements of the TOE have been met.
- Guidance documents define the requirements for coherence, coverage, and completeness of the operational documentation the developer has provided. This documentation, which provides two categories of information (for users and for administrators), is an important factor in the secure operation of the TOE.
- Lifecycle support defines the requirements for adopting a well-defined lifecycle model for all the steps of the TOE development, including flaw remediation procedures and policies, correct use of tools and techniques, and the security measures used to protect the development environment.

- Tests cover the testing requirements needed to demonstrate that the TSF satisfies the TOE security functional requirements. This class addresses coverage, depth of developer testing, and functional tests for independent lab testing.
- Vulnerability assessment defines the requirements directed at identifying exploitable vulnerabilities. Specifically, it addresses vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.
- Protection profile evaluation demonstrates that the PP is complete, consistent, and technically sound, and that an evaluated PP is suitable as the basis for developing an ST.
- Security target evaluation demonstrates that the ST is complete, consistent, and technically sound, and is suitable as the basis for the corresponding TOE evaluation.
- Maintenance of assurance provides the requirements intended for application after a TOE has been certified against the Common Criteria. Maintenance of assurance requirements help ensure that the TOE will continue to meet its security target as changes are made to the TOE or its environment. Such changes include the discovery of new threats or vulnerabilities, changes in user requirements, and the correction of bugs found in the certified TOE.

Evaluation Assurance Levels

Assurance levels define a scale for measuring the criteria for evaluating PPs and STs. Evaluation Assurance Levels (EALs) provide an increasing scale that balances the levels of assurance claimed with the cost and feasibility of acquiring such assurance. Table 5.3 indicates the CC EAL levels, along with backward compatibility to the Orange Book and ITSEC criteria levels.

TABLE 5.3 Security Criteria Compared

Common Criteria Assurance Level	Orange Book Criteria Level	ITSEC Criteria Level
—	D: Minimal protection	E0
EAL1	—	—
EAL2	C1: Discretionary security protection	E1
EAL3	C2: Controlled access protection	E2
EAL4	B1: Labeled security protection	E3
EAL5	B2: Structured protection	E4
EAL6	B3: Security domains	E5
EAL7	A1: Verified design	E6

Evaluation Assurance Level 1

EAL1 applies when some confidence in correct operation is required, but the threats to security are not viewed as serious. It is valuable when independent assurance is required to support the contention that due care has been exercised in protecting personal or similar types of information. The intention is that an EAL1 evaluation can be successfully conducted without assistance from the developer of the TOE, at a low cost. An evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation and that it provides useful protection against identified threats. Think of EAL1 as kicking the tires on a vehicle that you're considering for purchase.

Evaluation Assurance Level 2

EAL2 requires a developer's cooperation in terms of the delivery of design information and test results, but it does not demand more effort from the developer than is consistent with good commercial practice; it also should not require a substantially increased investment of money or time. EAL2 is applicable when developers or users require a low to moderate level of independently assured security, in the absence of ready availability of the complete development record. Such a situation might arise when securing legacy systems or when access to the developer is limited.

Evaluation Assurance Level 3

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. EAL3 applies when developers or users require a moderate level of independently assured security; it requires a thorough investigation of the TOE and its development without substantial reengineering.

Evaluation Assurance Level 4

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices that, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is applicable when developers or users require a moderate to high level of independently assured security in conventional off-the-shelf TOEs. Additional security-specific engineering costs could be involved.

Evaluation Assurance Level 5

EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE likely is designed and developed with the intent of achieving EAL5 assurance. EAL5 is applicable when developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs for special security engineering techniques.

Evaluation Assurance Level 6

EAL6 permits developers to gain high assurance from applying security engineering techniques to a rigorous development environment, to produce a premium TOE for protecting high-value assets against significant risks. EAL6 is applicable to developing security TOEs in high-risk situations, when the value of the protected assets justifies additional costs.