November 1998

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

COMMON CRITERIA: LAUNCHING THE INTERNATIONAL STANDARD

The Common Criteria (CC) for Information Technology (IT) Security Evaluation is the new standard for specifying and evaluating the security features of computer products and systems. The CC is intended to replace previous security criteria used in North America and Europe with a standard that can be used everywhere in the world. The CC will become International Standard (IS) 15408 in early 1999.

Developing the CC has been a five-year international project involving NIST and the National Security Agency (NSA), on behalf of the United States, and security organizations in Canada, France, Germany, the Netherlands, and the United Kingdom. They have worked in close cooperation with the International Organization for Standardization (ISO).

In the United States, the new international standard CC has formed the basis for the National Information Assurance Partnership (NIAP), a joint activity of NIST and NSA to establish an IT product security evaluation program supported by a number of accredited, independent testing laboratories. The main goals of NIAP are to establish cost-effective evaluation of security-capable IT products and to promote the wide availability of tested products to federal agencies and others, thus playing a crucial role in helping to protect the U.S. information infrastructure. (Note: A glossary at the end of the bulletin defines key terms used throughout the document.)

Purpose of CC

The CC will be used as the basis for evaluation of the security properties of IT products and systems. By using such a common criteria base, a wider audience may find the results of an IT security evaluation meaningful. The CC permits comparability among the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and the assurance measures applied to them during a security evaluation.

The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them must meet. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The CC supports the development of standardized sets of well understood IT product security requirements by user communities in the form of Protection Profiles (PPs) for use in procurements and advice to manufacturers. Manufacturers can use similar sets of CC-based requirements to describe the security capabilities of their products. These are called Security Targets (STs), which can then be used as the basis for security evaluations of those products. Security evaluations are formalized testing and analytic processes that use the CC to determine whether IT products have been correctly developed to specification and whether they are effective in countering the security problems as

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since January 1997:

claimed. Users can integrate evaluated IT products into their systems with increased confidence that their claimed security features will operate as intended.

Earlier Security Criteria Work

The CC represents the outcome of a long series of efforts to develop criteria for the security evaluation of IT products and systems that can be broadly useful within the international community. In the early 1980s, NSA developed the Trusted Computer System Evaluation Criteria (TCSEC or "Orange Book"). NSA has used the TCSEC extensively since then in its IT security product evaluation program.

In the succeeding decade, various countries initiated the development of evaluation criteria that built upon the concepts of the TCSEC but were more flexible and adaptable to the evolving nature of IT.

- In Europe, the European Commission published the Information Technology Security Evaluation Criteria (ITSEC) in 1991 after joint development by France, Germany, the Netherlands, and the United Kingdom.

- In Canada, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) were published in early 1993 as a combination of the ITSEC and TCSEC approaches.

- In the United States, NIST and NSA jointly developed the draft Federal Criteria for Information Technology Security (FC) version 1.0, which was also published in early 1993 as a second approach to combining North American and European concepts for evaluation criteria.

Work began in 1990 in ISO to develop an international standard evaluation criteria for general use. The new criteria were to be responsive to the need for mutual recognition of standardized security evaluation results in a global IT market. This task was assigned to the Joint Technical Committee 1 - Information Technology (JTC1), subcommittee 27 - Security Techniques (SC27), Working Group 3 - Security Criteria (WG3).

Development of the Common Criteria

In June 1993, the seven organizations responsible for all the North American and European security criteria (listed at end of bulletin) pooled their efforts to align their separate criteria into a single set of widely useful international IT security criteria. This joint multi-national activity, named the CC Project, sought to resolve the conceptual and technical differences among the source criteria. The results were to be delivered to WG3 as a contribution to the international standard criteria under development.

The CC Project sponsoring organizations formed the CC Editorial Board (CCEB) to develop the CC. They established a formal cooperative liaison with WG3 and contributed several early versions of the CC to WG3's work, which were in turn influenced by WG3 experts' interaction. Beginning in 1994, WG3 adopted these versions as successive working drafts of the ISO criteria.

Version 1.0 of the CC was completed in January 1996 and distributed by ISO in April 1996 as a Committee Draft (CD). The CC Project used this version to perform a number of trial evaluations. A widespread public review of the document was also conducted.

The CC Implementation Board (CCIB) extensively revised the CC based on the results of trial use, public review, and interaction with ISO. Working closely with WG3, the CCIB completed CC version 2.0 in April 1998 and it was sent out by ISO for balloting as a Final Committee Draft. In October 1998, WG3 slightly revised the document and approved it as Final Draft International Standard 15408, for final balloting in the winter of 1998. The document is expected to become IS 15408 in early 1999 without further change.

For historical and continuity purposes, ISO has accepted the continued use of the term "Common Criteria" (CC) within the document, while recognizing that the official ISO name for the new IS 15408 is "Evaluation Criteria for Information Technology Security."

CC Project Sponsoring Organizations

The seven European and North American governmental organizations provided nearly all of the effort that went into developing the CC from its inception to its completion. These organizations are also "evaluation authorities," managing product security evaluation programs for their respective national governments. They have committed themselves to replacing their respective evaluation criteria with the new IS 15408. Their goal is mutual recognition of each other's security product evaluation results, permitting a wider global market for good IT security products.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Interim Mutual Recognition

In April 1996, NIST in cooperation with NSA published a bulletin called "Guidance on the Selection of Low Level Assurance Evaluated Products." The bulletin recommended TCSEC Class C2 - "Controlled Access Protection" as an acceptable minimum set of security criteria for general use in low-threat environments. The bulletin also publicly acknowledged that the Canadian CTCPEC and the European ITSEC contained similar requirements.

The NIST bulletin recognized that, while full equivalency among these three criteria was not easy to establish, enough similarities existed to recommend the use of low-level assurance products evaluated under any of them. The bulletin also noted that equivalency should cease to be an issue once the CC is adopted and implemented by the participating countries.

With the advent of CC version 2.0 and its ISO counterpart, IS 15408, supported by the CC-based Mutual Recognition Arrangement signed by these countries in October 1998 (see end of bulletin), equivalency is no longer an issue.

Three Parts of the CC

Part 1 - Introduction and General Model

Part 1 introduces the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also defines constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. These constructs are called Protection Profiles (PPs), Security Targets (STs) and packages, and are described in a later section. In addition, Part 1 describes the usefulness of each part of the CC in terms of each of the target audiences.

Part 2 - Security Functional Requirements

Part 2 contains a catalog of well-defined and understood security functional requirements that are intended to be used as a standard way of expressing the security requirements for IT products and systems. The catalog is organized into classes, families, and components.

- Classes are high-level groupings of families of requirements, all sharing a common security focus (e.g., identification and authentication).
- Families are lower-level groupings of requirement components, all sharing specific security objectives but differing in rigor or emphasis (e.g., user authentication).
- Components are the lowest selectable requirements that may be included in PPs, STs, or packages (e.g., unforgeable user authentication).

Part 2 also includes an extensive annex of application notes for applying the material that it contains. While it is possible to explicitly state functional requirements not included in the Part 2 catalog in building CC-based constructs (PPs, STs, and packages), that course is not advised unless it is clearly not practical to use Part 2 components. Using functional requirements not part of the catalog could jeopardize widespread acceptance of the result.

Part 3 - Security Assurance Requirements

Part 3 contains a catalog that establishes a set of assurance components that can be used as a standard way of expressing the assurance requirements for IT products and systems. The Part 3 catalog is organized into the same class - family - component structure as Part 2. Part 3 also defines evaluation criteria for PPs and STs. Part 3 presents the seven Evaluation Assurance Levels (EALs), which are predefined packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems.

The EALs have been developed with the goal of preserving the concepts of assurance drawn from the source criteria (TCSEC, ITSEC, and CTCPEC) so that results of previous evaluations remain relevant. For example, EALs levels 2-7 are generally equivalent to the assurance portions of the TCSEC C2-A1 scale. Note, however, that this equivalency should be used with caution as the levels do not derive assurance in the same manner, and exact mappings do not exist.

As with Part 2, it is possible but not necessarily advisable to explicitly state assurance requirements not from Part 3 or to augment EAL packages with additional Part 3 components. Mutual recognition of product evaluation results is based largely on the EAL, so use of unique combinations of assurance requirements could jeopardize international acceptance of products evaluated against them.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today.

Key Concepts

The CC defines three useful constructs for putting IT security requirements from Parts 2 and 3 together: the PP, the ST, and the package. The CC has been developed around the central notion of using in these constructs, wherever possible, the security requirements in Parts 2 and 3 of the CC, which represent a well-known and understood domain.

Protection Profile

The PP is an implementation-independent statement of security needs for a set of IT security products that could be built. The PP contains a set of security requirements, preferably taken from the catalogs in Parts 2 and 3, which should include an EAL. A PP is intended to be a reusable definition of product security requirements that are known to be useful and effective.

A PP could be developed by user communities, IT product developers, or other parties interested in defining such a common set of requirements. A PP gives consumers a means of referring to a specific set of security needs and communicating them to manufacturers. The PP also helps future product evaluation against those needs.

The PP contains the following items:

- PP introduction - identification and overview information, which allows users to identify PPs useful to them.
- Target of evaluation (TOE) description - description of the IT product and its purpose, not necessarily from a security perspective.
- TOE security environment - description of the security aspects of the environment in which the product is intended to be used and the manner in which it is expected to be employed. This statement includes the following:
  - ❒ Assumptions about the security aspects of the product's expected usage and operating environment, such as value of assets and limitations of use. Assumptions also describe the environment's physical, personnel, and connectivity aspects.
  - ❒ Threats against which the product or its supporting environment must specifically provide protection.
  - ❒ Organizational security policies or rules with which the product must comply. These can be any explicit statements of IT security needs that the product must meet.
- Security objectives - a high-level statement of what the product and its environment are intended to accomplish in covering the threats, policies, and assumptions.
- IT security requirements - the detailed statement of IT security functional and assurance requirements that the product and its operating environment must satisfy to meet the objectives.
- Application notes - additional supporting information that may be useful for the construction, evaluation, or use of the product.
- Rationale - the evidence describing how the PP is complete and cohesive and how a product built against it would be effective in meeting the objectives.

Security Target

An ST is a statement of security claims for a particular IT security product or system. The ST parallels the structure of the PP, though it has additional elements that include product-specific detailed information. The ST contains a set of security requirements for the product or system, which may be made by reference to a PP, directly by reference to CC functional or assurance components, or stated explicitly. An ST is the basis for agreement among all parties as to what security the product or system offers, and therefore the basis for its security evaluation. The ST contains a summary specification, which defines the specific measures taken in the product or system to meet the security requirements.

Package

An intermediate combination of security requirement components is termed a package. The package permits the expression of a set of either functional or assurance requirements that meet some particular need, expressed as a set of security objectives. A package is intended to be reusable and to define requirements that are known to be useful and effective in meeting the identified objectives. A package may be used in the construction of more complex packages or PPs and STs. The seven evaluation assurance levels (EALs) contained in Part 3 are predefined assurance packages.

Target of Evaluation

The TOE is an IT product or system to be evaluated, the security characteristics of which are described in specific terms by a corresponding ST, or in more general terms by a PP. In CC philosophy, it is important that a product or system be evaluated against the specific set of criteria expressed in the ST. This evaluation consists of rigorous analysis and testing performed by an accredited, independent laboratory. The scope of a TOE evaluation is set by the EAL and other requirements specified in the ST. Part of this process is an evaluation of the ST itself, to ensure that it is correct, complete, and internally consistent and can be used as the baseline for the TOE evaluation.

Uses of the CC

The CC is used in two general ways:

- As a standardized way to describe security requirements, e.g., PPs and STs for IT products and systems; and
- As a sound technical basis for evaluating the security features of these products and systems.

The following hypothetical scenarios describe these two uses.

Describing security requirements

In a typical PP development scenario, a community of users (e.g., a banking consortium) will determine that a standardized set of security capabilities should be used in software or hardware on their systems. They will begin to construct a PP to express those common requirements. They will first identify the type of product or products envisioned and the general IT features needed. They will then consider the environment in which it will operate, in particular identifying the security problems and challenges that must be addressed. That activity is, in essence, a risk analysis and leads to a statement of general needs or security objectives to be met both by the product and by its environment.

Security objectives are transformed by use of the CC Part 2 catalog into a set of coherent and mutually supportive IT security functional requirements statements. Based on the desired level of confidence in the security of products to be built, an EAL from Part 3 is assigned. (Note that the higher the EAL, the greater the burden on the product developer, and consequently the more time and money needed to bring the product to complete availability.)

The outcome of the process just described is a PP. It is desirable that the PP be submitted to an independent testing laboratory for evaluation, to ensure that it is correct, complete, and internally consistent. The PP may then be entered into a central registry for use by the community to communicate the product security needs to manufacturers, either informally or by incorporation into procurement documents.

The preceding scenario involving a user community is only one possible approach to developing a PP, although it is the most commonly expected approach. It is also possible for one or several manufacturers to develop a PP that incorporates the features of their products, as a means of communication with potential users, ensuring interoperability via standardization or for other purposes.

Evaluating product security

In a typical product evaluation scenario, a manufacturer identifies a market niche for an IT product with security capability. This niche may be represented by a PP incorporating the product desires of a group of users and potential customers. The manufacturer builds the product, following the PP-specified functional requirements from CC Part 2 and the developer assurance requirements in the EAL from Part 3. Once the product is built, the manufacturer prepares an ST, which in the simplest case makes a claim of compliance with a particular PP, thereby covering the functional and assurance requirements for the product. The manufacturer also develops as part of the ST a summary specification of the ways that the product's features meet these requirements. The manufacturer then submits the ST, the product, and accompanying documentation to an accredited, independent testing laboratory for evaluation.

The laboratory evaluates the ST, to determine that it is a sound baseline for evaluation of the product and that any claims of PP compliance are supportable. The laboratory then proceeds to evaluate the product and its documentation against the ST. If the product passes evaluation, it can be submitted to an evaluation authority for validation of the evaluation results.

While definitely preferable, it is not necessary for a product to claim compliance with a PP. In the absence of PP claims, the ST is prepared in a process similar to that described for the PP. The evaluation of the ST and then the corresponding product can proceed as before, but no PP compliance claims will be examined.

Validating the results

An integral part of the CC-based process, as described in its Part 1, is the independent validation of evaluation results in order to ensure that a product's evaluation was conducted properly. An evaluation authority is a body that implements the CC for a specific community, responsible for setting the standards and monitoring the quality of evaluations conducted by testing laboratories within that community. Each of the CC partners is an evaluation authority for the government of its respective country. NIST and NSA work together as a single U.S. authority, as described below. The evaluation authority is responsible for overseeing all evaluations in its jurisdiction, qualitatively reviewing the results, and certifying or validating the findings. The term "validation" is used in the U.S. for this process, while the other CC partners use "certification," but the process is the same. Upon validation of a successful product evaluation, the product is awarded a CC certificate and is added to an official validated products list available to the public.

Evaluating installed systems

Another way that the CC process can be used is to evaluate installed systems for such purposes as system certification and accreditation programs used in several federal agencies. The organization responsible for certifying a system's secure operation could develop an ST describing the system architecture, its functions and operational environment, and the security features it embodies. An independent entity, such as an accredited testing laboratory, could then perform an on-site evaluation of the system against the ST, providing a report to support a request for accreditation.

CC Evaluation Programs

Numerous organizations throughout the world are now implementing the CC, including all of the CC project partners (listed below), as well as other European Union nations, Australia, New Zealand, Japan, Korea, and parts of the former Soviet Union. It is expected that this number will grow significantly as soon as the CC is formally published as International Standard 15408 in early 1999.

In the U.S., NIST and NSA jointly operate the National Information Assurance Partnership (NIAP). NIAP is a broadly based program that operates principally as the CC-based evaluation authority for the federal government. NIAP is dedicated to demonstrating the value of independent testing and validation as a measure of security and trust in IT products. Through its efforts, NIAP fosters the establishment and accreditation of commercial IT product security testing laboratories in the U.S.

The Goal of Mutual Recognition

On October 5, 1998, six of the seven CC project partners officially signed a Mutual Recognition Arrangement (MRA). The purpose of the MRA is to bring about an international situation in which IT products and PPs that earn a CC certificate can be procured and used in different jurisdictions without the need for them to be evaluated and certified/validated more than once. By recognizing the results of each other's evaluations, products evaluated in one MRA member nation can be accepted in the other member nations. It is anticipated that, as other nations develop high quality IT product security evaluation programs, they too may seek to join the MRA. This path is open to other evaluation authorities upon demonstration that they can fulfill the stringent technical and procedural conditions for mutual recognition laid down in the MRA.

As product evaluations can be costly and time-consuming, both manufacturers and users have welcomed the MRA breakthrough. The anticipated outcome is a "level playing field" for multi-national IT product manufacturers, leading to a much wider availability of useful IT security products to secure the global information infrastructure.

These two factors have been the major goal of the CC project from its inception and have been the driving force and vision that empowered the ISO criteria activity as well. The joint development of the CC has created an environment of mutual respect among the partners, and the CC itself has formed the technical basis for mutual recognition, both of which were necessary for the inception of the MRA.

Glossary

The following key terms used in this bulletin are adapted from CC definitions.

Assurance - grounds for confidence that an IT product or system meets its security objectives.

Evaluation - assessment of an IT product or system against defined security functional and assurance criteria, performed by a combination of testing and analytic techniques.

Evaluation Assurance Level (EAL) - one of seven increasingly rigorous packages of assurance requirements from CC Part 3. Each numbered package represents a point on the CCs predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system.

Package - a reusable set of either functional or assurance components (e.g., an EAL), combined together to satisfy a set of identified security objectives.

Product - IT software, firmware and/or hardware, providing functions designed for use or incorporation within a multiplicity of systems.

Protection Profile (PP) - an implementation-independent set of security functional and assurance requirements for a category of IT products that meet specific consumer needs.

Security Functional Requirements - requirements, preferably from CC Part 2, that when taken together specify the security behavior of an IT product or system.

Security Objective - A statement of intent to counter specified threats and/or satisfy specified organizational security policies and assumptions.

Security Target (ST) - a set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified product or system.

System - a specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE) - another name for an IT product or system described in a PP or ST. The TOE is the entity that is subject to security evaluation.

For More Information

■ *References:*

- NIST CSL Bulletin, April 1996
- Common Criteria for IT Security v.2.0
- ISO FDIS 15408, Parts 1-2-3
- Common Criteria Mutual Recognition Arrangement, October 1998

■ *Web sites:*

- Common Criteria Project: http://csrc.nist.gov/cc
- NIAP: http://niap.nist.gov

■ *CC Project Organizations:*

• CANADA	Communications Security Establishment E-mail: criteria@cse-cst.gc.ca WWW: http://www.cse-cst.gc.ca/cse/english/cc.html
• FRANCE:	Service Central de la Sécurité des Systèmes d'Information (SCSSI) E-mail: ssi20@calva.net
• GERMANY:	Bundesamt für Sicherheit in der Informationstechnik (BSI) German Information Security Agency (GISA) E-mail: cc@bsi.de WWW: http://www.bsi.bund.de
• NETHERLANDS:	Netherlands National Communications Security Agency E-mail: criteria@nlncsa.minbuza.nl WWW: http://www.tno.nl/instit/fel/refs/cc.html
• UNITED KINGDOM:	Communications-Electronics Security Group E-mail: criteria@cesg.gov.uk WWW: http://www.cesg.gov.uk/cchtml
• UNITED STATES - NIST:	National Institute of Standards and Technology E-mail: criteria@nist.gov WWW: http://csrc.nist.gov/cc
• UNITED STATES - NSA:	National Security Agency E-mail: common_criteria@radium.ncsc.mil WWW: http://www.radium.ncsc.mil/tpep/

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195

Official Business
Penalty for Private Use $300

Address Service Requested