October 2000

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

AN OVERVIEW OF THE COMMON CRITERIA EVALUATION AND VALIDATION SCHEME

By Patricia Toth, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Introduction

Recent advances in information technologies and the proliferation of computing systems and networks worldwide have raised the level of concern about security in both the public and private sectors. Security concerns are motivated by an increasing use of information technology (IT) products and systems throughout government and industry in a variety of areas—from electronic commerce to national defense. Consumers have access to a growing number of security-enhanced IT products with different capabilities and limitations and must make important decisions about which products provide an appropriate degree of protection for their information.

To help consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace, NIST and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance using international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for IT Security, or Common Criteria Scheme in abbreviated form, is a partnership between the public and private sectors.

What is Product Evaluation and Validation?

IT security is defined as the protection of information from unauthorized disclosure, modification, or loss of use by countering threats to that information arising from human or systems-generated activities, malicious or otherwise. Countering threats to an IT product (e.g., firewalls, databases, operating systems) and mitigating risk helps to protect the confidentiality and integrity of information and also ensure its availability.

Consumers of IT products need to have confidence in the security features of those products. Consumers need to be able to compare various products to understand their capabilities and limitations. Confidence in a particular IT product can be based on the reputation of the developer, past experience with the developer, or the demonstrated competence of the developer in building products through recognized assessments. The consumer could also test the product directly and obtain the necessary results. Dependence on reputation lacks measurable results and testing requires substantial, costly duplication of effort.

The Common Criteria Scheme enables consumers to obtain an impartial assessment of an IT product by an independent laboratory. This security evaluation includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. The specific IT product being evaluated is referred to as the Target of Evaluation (TOE). The security requirements for that product are described in its security target. IT security evaluations are composed from analysis and testing, distinguishing these activities from the more traditional forms of conformance testing in other areas. All of these activities are carried out using recognized standards and procedures.

To increase consistency among IT security laboratories, the CCEVS reviews the final evaluation results. This review provides independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the

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 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since April 1999

- ❒ *Guide for Developing Security Plans for Information Technology Systems*, April 1999
- ❒ *Computer Attacks: What They Are and How to Defend Against Them,* May 1999
- ❒ *The Advanced Encryption Standard: A Status Report,* August 1999
- ❒ *Securing Web Servers,* September 1999
- ❒ *Acquiring and Deploying Intrusion Detection Systems*, November 1999
- ❒ *Operating System Security: Adding to the Arsenal of Security Techniques,* December 1999
- ❒ *Guideline for Implementing Cryptography in the Federal Government*, February 2000
- ❒ *Security Implications of Active Content*, March 2000
- ❒ *Mitigating Emerging Hacker Threats*, June 2000
- ❒ *Identifying Critical Patches with ICAT,* July 2000
- ❒ *Security for Private Branch Exchange Systems*, August 2000
- ❒ *XML Technologies*, September 2000

scheme and that the conclusions of the laboratory are consistent with the facts presented in the evaluation. This review, known as validation, is intended to promote consistency of IT security evaluations and comparability of results for all evaluations conducted within the scheme.

The evaluation, the independent validation of evaluation results, and the documentation resulting from these processes provide valuable information for consumers about the security capability of IT products. However, consumers will still need to review this information carefully and assess its applicability to their needs (e.g., the situation and operating environment in which the product will actually be used).

Scheme Objectives

NIAP has the following objectives in developing, operating, and maintaining an evaluation and validation scheme:

- To meet the needs of government and industry for cost-effective evaluation of IT products;
- To encourage the growth of independent commercial security testing laboratories and the development of a private sector security testing industry;
- To ensure that security evaluations of IT products are performed using specific international standards;
- To increase the availability of evaluated IT products; and
- To participate in international recognition arrangements.

The scheme is intended to serve many communities of interest with very diverse roles and responsibilities, including IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and accreditors (individuals deciding the fitness for operation of those products within their respective organizations). Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

Scheme Overview

The principal participants in the NIAP Common Criteria Evaluation and Validation Scheme are:

- Sponsors of IT Security Evaluations
- NIAP Validation Body (NIST/NSA)
- Common Criteria Testing Laboratories

In addition to the principal participants listed above, the NIST National Voluntary Laboratory Accreditation Program (NVLAP) plays an important role in supporting the scheme requirements for the use of accredited laboratories to perform IT evaluations.

In the context of the Common Criteria Scheme, a sponsor is the party requesting and paying for the security evaluation of an IT product or protection profile by an accredited testing laboratory. The sponsor is often the product or profile developer, but could also be a government agency, industry consortium, or other organization seeking to obtain an IT security evaluation.

CCEVS establishes policies and procedures in the interest of the public and private sectors. It also provides technical guidance to those laboratories, validates the results of IT security evaluations for conformance to the Common Criteria, and serves as an interface to other nations on the recognition of such evaluations.

Commercial testing laboratories accredited by NVLAP and recognized by the NIAP Validation Body conduct IT security evaluations. These approved testing laboratories are called Common Criteria Testing Laboratories (CCTLs). NVLAP accreditation is the primary requirement for becoming a CCTL. The purpose of the NVLAP accreditation is to ensure that laboratories meet the requirements of ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories*, and are competent to perform the test methods used for IT security evaluations.

The NIAP Validation Body assesses the results of a security evaluation conducted by a CCTL within the scheme and when appropriate, issues a Common Criteria certificate. The certificate, together with its associated validation report, confirms that an IT product or protection profile has been evaluated at an accredited testing laboratory using the Common Methodology for conformance to the Common Criteria. The certificate also confirms that the IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the testing laboratory are consistent with the evidence presented during the evaluation.

The CCEVS maintains a NIAP Validated Products List containing all IT products and protection profiles successfully completing evaluation and validation under the scheme. CCEVS will also provide a means to list products and profiles validated by international arrangement partners.

Guidance to Consumers

It is important that consumers of IT products and protection profiles understand how to interpret the results of IT security evaluations and validations. These results are described in evaluation technical reports produced by CCTLs and summarized in the associated validation reports and Common Criteria certificates published by the NIAP Validation Body.

An IT product is typically evaluated in a controlled laboratory setting. In that regard, there are some general assumptions made about the opera-

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. Our Web site is http://www.itl.nist.gov/.

tional environment where the product is ultimately to be employed subsequent to the security evaluation. In some cases, an evaluated IT product may be integrated into a more complex configuration of products that compose an IT system. The actual environment of use may also be significantly different from the one described in the original assumptions set forth in the security target. In the end, consumers must assess the overall contribution to assurance made by the evaluated IT product. When making assessments, there are several things a consumer should consider. They must realize that

- The accuracy and completeness of security evaluation results are dependent on the accuracy and completeness of the information and documentation provided to the CCTL by the sponsor of the evaluation;
- The quality of a security target (i.e., security specification) and the reported results of an IT product evaluated against that security target are a function of how well the product is able to be described under the Common Criteria and the degree to which the Common Methodology and the derivative test methods are able to measure conformance to the security target; and
- The security evaluation results are only applicable to that particular version and release of the product in its evaluated configuration.

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 from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your 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.

Common Criteria	US TCSEC	European ITSEC
-	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

Consumers are responsible for determining the security impact of installing or operating an evaluated IT product in a configuration other than the configuration in which it was evaluated.

Evaluation Assurance Levels

The Common Criteria Evaluation Assurance Levels (EALs) have been developed with the goal of preserving the concepts drawn from the U.S. TCSEC and European ITSEC so that results of previous evaluations remain relevant. Using the table above, general equivalency statements are possible but should be made with caution, as the levels do not define assurance in the same manner.

Assurance levels define a scale for measuring the criteria for the evaluation of Protection Profiles and Security Targets. EALs are constructed from assurance components. EALs provide an increasing scale of requirements that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs listed below. The increase in assurance across the levels is accomplished by substituting hierarchically higher assurance components from the same assurance family and by the addition of assurance components from other assurance families.

The seven EALs are as follows:

EAL1 - functionally tested

EAL2 - structurally tested

EAL3 - methodically tested and checked

EAL4 - methodically designed, tested and reviewed

EAL5 - semi-formally designed and tested

EAL6 - semi-formally verified design and tested

EAL7 - formally verified design and tested

Conclusion

The CCEVS will help consumers select commercial off-the-shelf IT products that meet their security requirements. The CCEVS will also provide for consistent evaluation and validation results. Valuable information for consumers about the security of IT security products will be provided.

For More Information

Additional information on the Common Criteria Evaluation and Validation Scheme can be found at:
http://niap.nist.gov/cc-scheme.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

NIST CENTENNIAL

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8901
Gaithersburg, MD 20899-8901