

NISCC Technical Note 02/03: Understanding Common Criteria Evaluation

Background

The Common Criteria is an ISO (International Standards Organisation) standard for security evaluation of software products. It is used by IT product vendors as a benchmark for security of their product, thus offering a measurable level of assurance to those responsible for incorporating such products into systems. This technical note aims to provide a brief description of what Common Criteria can achieve and what the expectation of security officers, system owners and potential purchasers should be. A brief indication of the evaluation process is also included. The production of this note has been driven by the successful completion of the evaluation of Microsoft Windows 2000, which will be used to illustrate the points made in the note.

What is Common Criteria?

As noted above, Common Criteria is an ISO standard (ISO 15408) for IT security evaluations. In the following discussion of Common Criteria, it will be assumed that the evaluation concerns an IT product. It is possible to use Common Criteria to evaluate systems composed of different products, but this topic is beyond the scope of this note. As a standard the main purpose of Common Criteria is to ensure that IT security evaluations world wide are performed against a common set of requirements, and that, where possible, the security claims are expressed unambiguously in a common way.

The following is a non-exhaustive list of useful resources available on the world wide web:

- <http://www.commoncriteria.org>
- <http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm>
- <http://niap.nist.gov>
- http://www.cse.dnd.ca/en/services/common_criteria/common_criteria.html
- <http://www.aisep.gov.au>
- <http://www.bsi.de/zertifiz/index.htm> (mainly German language)
- <http://www.ssi.gouv.fr/fr/confiance/evalcertif.html> (mainly French language)

Security Target

The security claims of the product, the scope of the evaluation and the intended operational environment of the product are defined in a document called the *security target*. The security claims are divided into:

- A set of security requirements, of which a large number are available in template form in the Common Criteria documentation [1]
- Details of the security functions which meet those requirements

The security target also includes details of how much assurance is claimed in those security functions. The Common Criteria documentation [2] provides a list of standard assurance levels, labelled Evaluation Assurance Level (EAL) 1 to EAL 7. EAL 1, offers the least assurance, that the security functions have been tested, while EAL 7 offers the highest assurance, a thoroughly tested product with a

formally verified design that has been tested. Each assurance level comprises a number of assurance components, covering aspects of the product's design, development and operation. At EAL 4, which provides assurance that the product has been methodically designed, tested and reviewed, these components are:

- Configuration management
- Delivery, installation, generation and startup
- Product design and implementation
- Administrative and user documentation
- Development and support processes
- Testing security functions
- Vulnerability analysis and testing

Common Criteria was designed as a toolkit: assurance levels can be tailored according to particular evaluation requirements, and security requirements can be selected as needed and new ones created if the documentation does not have an appropriate template. It is increasingly common, for instance, to see the standard assurance levels augmented by assurance components taken from the Common Criteria documentation.

To standardise security claims across evaluations and to provide a baseline for product security requirements, there is a class of evaluation documents called protection profiles. Protection profiles are, in effect, templates for creating security targets. They provide a minimum assurance requirement and a minimum set of security requirements. A wide range of protection profiles is available on the web sites mentioned at the start of this note. Unless they are in draft the protection profiles will have been evaluated to ensure that they meet the requirements of Common Criteria.

In the case of Microsoft Windows 2000, at the time of writing the security target is available on the US National Information Assurance Partnership (NIAP) web site at:

<http://niap.nist.gov/cc-scheme/CCEVS-VID402.html>

and on the Microsoft web site, at:

<http://download.microsoft.com/download/win2000srv/CCSecTar/2.0/NT5/EN-US/W2KCCST.pdf>

The assurance claim made for Windows 2000 was for EAL 4 augmented by the systematic flaw remediation assurance component which provides confidence in the Microsoft support process for the resolution of flaws and bugs. The security requirements are based on those of the Controlled Access protection profile for operating systems providing fine-grained discretionary access control [3] which are designed to protect assets in a moderate risk environment. The Windows 2000 security requirements cover the areas of:

- Identification and authentication
- Accounting and auditing
- Access control
- System security management
- User data protection
- Security function protection
- Cryptographic support
- Resource utilisation
- Session locking

- Configurable access banners
- Internal data replication
- Session initialisation
- Trusted path

What to expect from a successful evaluation?

It is very important to note that the assurance claims, and the potential vulnerabilities considered, *only* apply to:

- Versions of the product identified in the security target
- Components of the product identified in the security target
- The environment specified in the security target

It is usual for the evaluation not to assess product components that may be installed in a default installation of the product but that are not present in the evaluated configuration. Similarly, some classes of vulnerability may not apply if the product is used in a certain way or is protected from attack by physical means.

In the case of Windows 2000, the high-level components of the product evaluated were:

- Security
- Input/Output
- Kernel
- Winlogon
- Win32
- Services
- Operating System Support
- Network Support
- Administration Graphical Interfaces
- Hardware

These high-level components are broken down into lower level components in Appendix B of the security target. By meeting the Controlled Access protection profile, the operating environment is assumed to be benign or non-hostile, although the Windows 2000 security target does counter threats that are not present in the Controlled Access protection profile. Nevertheless, the Windows 2000 security target assumes that:

- Any network to which the product is connected are under the same security policy constraints as the network on which the product is operating (assumption A.PEER)
- Users are expected to act in a co-operative manner in a benign environment (assumption A.COOP)

The following services were outside the scope of the evaluation:

- Email services
- Certificate authorities
- Web based applications
- Firewall functionality

A successful Common Criteria evaluation will demonstrate that the set of product components evaluated work together in a secure way within the assumed environment. This will have been achieved by looking at the product

documentation, specification of the product's design and, at EAL 4 and above, implementation details such as source code, as well as by performing functional and vulnerability testing. Furthermore, the evaluation will have assessed the developer's processes and determined that they lead to the secure development and delivery of the product.

For these reasons many software vendors regard security evaluation as an essential part of the process of checking the security of their products and of their development environments. Common Criteria also has an assurance component called "assurance maintenance" which aims to ensure that the processes and procedures that lead to the development of secure products continues after a particular version of the product has successfully completed evaluation.

System owners and potential purchasers of the product need to be cognisant of the security target, and, in particular, be aware of limitations of scope of the product evaluation and of the environment in which the product is assumed to operate. The evaluation of Windows 2000 did not, for example, include the Microsoft Internet Information Services (IIS) web server, which has a history of vulnerabilities (see <http://www.sans.org/top20/>). Vulnerabilities in components outside the scope of the evaluation will not affect the validity of the evaluation results unless those components are part of the operational environment of the product and could be used to undermine the security of the evaluated components. Similarly, Windows 2000 has been evaluated in a moderate risk, non-hostile environment. If Windows 2000 were connected to an untrusted, potentially hostile network, then the security of the product would not necessarily be upheld.

Evaluated products are a good place to start if security is a concern. However, you will still need to understand the type of environment for which the product was designed to be secure; and if this is not equivalent to your organisation's environment, additional security measures will be needed. In the case of connecting to untrusted networks, the use of a stateful firewall that allows only internally initiated connections for services for which there is a business need, would help mitigate the risk. Other measures include a process for applying patches and implementing best practice security configurations for the applications exposed to the potentially hostile environment.

Evaluation Process

To conclude this note, it may be helpful for vendors considering evaluation and to system owners who may wish to purchase evaluated products to provide a brief overview of the evaluation process and the outputs from the process made available to product users.

The details of the evaluation process will vary from country to country, but they will all be of a comparable standard owing to mutual recognition between a number of European, North American and Australasian nations [4]. Nations which have active evaluation schemes are:

- Australia/New Zealand
- Canada
- France
- Germany
- United Kingdom
- United States

There are at least three distinct evaluation roles. The sponsor, who is usually the product developer, draws up the security target and funds the evaluation. The evaluators evaluate the product according to Common Criteria, its supporting methodology and the quality standards imposed upon them as a testing laboratory. The certifier, called the validator in the USA, checks the validity of the evaluation results. In the UK, CESG, the national authority for information assurance, provides a certification body as part of its administration of the UK IT security evaluation and certification scheme. The product developer, if different from the sponsor, may also be involved in the evaluation process, and will need to be involved at EAL2 and above to help with preparation of evaluation documentation and to be the subject of development and delivery process reviews.

The most significant information examined or generated by the evaluation is the security configuration, administrator and user guidance supplied by the sponsor, the security target and a certification report, also known as a validation report, which is produced by the certification body. The validation report for Windows 2000 is available from [Http://niap.nist.gov/cc-scheme/CCEVS-VID402.html](http://niap.nist.gov/cc-scheme/CCEVS-VID402.html). For Windows 2000, in addition to these Microsoft has provided security templates that can be used to automate the process of conforming to the EAL4 secure operating system configuration as Appendix F of the security configuration guide. Details of how to install the templates are available in Chapter 4 of the security configuration guide. The documentation and the templates are available by following the Common Criteria link from the Microsoft Technet web site, <http://www.microsoft.com/technet/security/prodtech/secureev.asp>.

Notes

- [1] See Common Criteria Part 2: Security functional requirements, Version 2.1, CCIMB-99-032, August 1999. Available at <http://commoncriteria.org/cc/cc.html>.
- [2] See Common Criteria Part 3: Security assurance requirements, Version 2.1, CCIMB-99-033, August 1999. Available at <http://commoncriteria.org/cc/cc.html>.
- [3] See http://niap.nist.gov/cc-scheme/PP_CAPP_V1.d.html
- [4] See <http://www.commoncriteria.org/registry/NatScheme.html> for details.