



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Evolving Information Technology Security Standards

With the rapid advance in computer technology comes a need for standards and certifications. Standards and certifications are being developed everywhere. E-commerce has developed standards for web transactions. SANS and universities are developing certifications for IT professionals. But what about security standards and certifications for the products we are using? How do we know that a certain firewall product meets our security needs and requirements? What level of security assurance does that product provide? How do we know that it will protect us against the threats facing our system in our specific environment? The truth is at the moment we don't know. The rapid development of computer products has outstripped the development of standards and certifications but with the development of common criteria for IT security that gap is narrowing with the development of new computer security standards.

In the early 1980's, the Trusted Computer System Evaluation Criteria (TCSEC) was developed. This was commonly referred to as the orange book. As a result of security developments in other countries, the U.S. Federal Criteria was developed in 1993 to incorporate these new developments into the TCSEC. Further developments led to a new approach to security standards in January 1996. It is called the Common Criteria for Information Technology Security Evaluation or Common Criteria (CC). After two years of review and trials, version 2.0 was published and Canada, France, United Kingdom and the United States signed an historic Mutual recognition Arrangement (MRA) for CC based evaluations. This version of the CC was adopted by the International Organization for Standards (ISO) as International Standard (ISO 15408) in 1999 and in May 2000, a new MRA was signed with the addition of Australia, New Zealand, Finland, Greece, Italy, Norway and Spain. As a result of these recent developments, the CC has become a world standard for security criteria and evaluation.

What is the Common Criteria for Information Technology Security Evaluation? The CC defines a set of IT requirements that are used to establish security requirements for developing and evaluating products and systems. The CC is organized into three parts: Part 1 is the introduction and general model. It defines the principles, concepts and a general model of IT security evaluation. Part 2 establishes a standard method of expressing functional security requirements. Part 3 establishes a standard method of expressing security assurance requirements. The CC is built on building blocks that form key concepts.

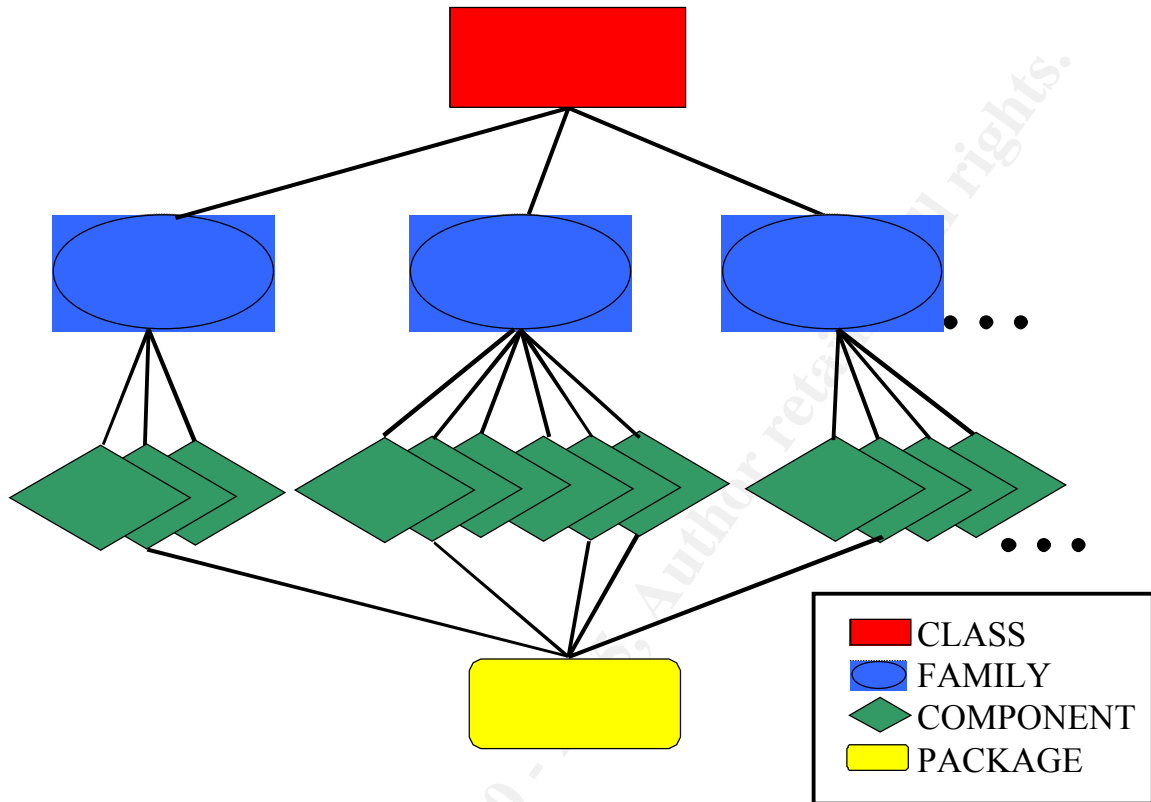


Figure 1 Common Criteria Building Blocks¹

Common Criteria building blocks start with the concept of a Target Of Evaluation (TOE). A TOE is a part of a product or system that is under evaluation. The description of the TOE is combined with the organizations security policies and threats to form the TOE security objectives. These are translated into TOE security requirements. These security requirements are further divided into security functionality and security assurance requirements. To better define these requirements, the CC groups these requirements into classes. There are 11 security functionality classes and 8 security assurance classes defined in the current version of the CC. The security functionality classes are:

- Resource Utilization
- Cryptographic Support
- Communications
- User Data Protection
- Identification and Authentication
- Security Management
- Trusted Path/Channels
- Protection of the TOE Security Functions
- Audit
- TOE access
- Privacy

The security assurance classes are:

¹ Based on a table in “Common Criteria Version 2: An Introduction.” November 1998 Pg 7

- Configuration Management
- Vulnerability Assessment
- Life Cycle Support
- Guidance Documents
- Delivery and Operation
- Assurance Maintenance
- Tests
- Development

Each class contains a number of families. Families are groups of components, which share security objectives. The requirements within each family share security objectives but differ in emphasis. The components in each family identify and define permitted operations. Components may be dependent on other components. These component dependencies may exist between security functionality components and security assurance components but rarely between security functionality and security assurance components. These components can be combined to meet a subset of security objectives. These subsets are called packages. They define known effective requirements for reusability. The CC defines seven predefined security assurance packages. These are called Evaluation Assurance Levels (EAL). They provide an increasing scale of security protection. There are seven EALs arranged from one to seven with seven being the strictest. At each level the increase in assurance is balanced with the cost and feasibility of acquiring that level of assurance. The seven EAL levels are:

- EAL 1 - Functionally tested
- EAL 2 - Structurally tested
- EAL 3 - Methodically tested and checked
- EAL 4 - Methodically designed, tested and reviewed
- EAL 5 - Semiformally designed and tested
- EAL 6 - Semiformally verified designed and tested
- EAL 7 - Formally verified designed and tested²

EAL 1 is the entry level. EAL 1 through EAL 4 do not require significant specialized security engineering techniques. And can generally be met by retrofitting pre-existing products and systems. EAL 5 and above require TOEs that have been designed or developed with the intent of meeting those requirements. The EAL packages are backward compatible with TCSEC access protection levels using the following scale:

- EAL 1 -
- EAL 2 - C1 Discretionary security protection
- EAL 3 - C2 Controlled access protection
- EAL 4 - B1 Labeled security protection
- EAL 5 - B2 Structured protection
- EAL 6 - B3 Security domains
- EAL 7 - A1 Verified design³

The TOE, components, packages, security requirements and objectives are used to build

²“Common Criteria for Information Technology Security Evaluation.” User Guide. October 1999. Pg 8

³“Common Criteria Version 2: An Introduction.” November 1998. Pg 11

the key CC concepts of Protection Profile (PP) and Security Target (ST). These concepts are necessary to define the product requirements, evaluation criteria and the level of security required by the implementation.

A PP is a standardized set of security requirements that meet a consumer or developers needs in a product or system. Some examples of PPs are:

- Specific Requirements for hospitals that satisfy HIPAA guidelines.
- An organization wants to purchase an intrusion detection system having specific requirements.
- A consumer group wants to specify security requirements for a certain application (i.e. Business to business e-commerce)

PPs specify security functionality and assurance requirement components and contain a statement of the security problem that the compliant product is intended to solve. PPs are divided into six sections: Introduction, Security Objectives, TOE description, IT Security Requirements, TOE security requirements and Rational. PP requirements form the functional basis for standards for the TOE. To be able to test the TOE, an ST is defined.

An ST is a set of security requirements, objectives and specifications. It defines the functionality and assurance measures in a TOE based on the security requirements. The ST also describes the security functions of the TOE. An ST has seven parts: Introduction, Security objectives, TOE description, IT security requirements, TOE summary specification, TOE security environment PP claims and rational.

The CC presents a framework for the evaluation of IT products or systems against specific criteria. The CC has four distinct stages of evaluation: PP, ST, TOE and assurance maintenance. The specific procedures and processes of evaluations are contained in a supporting document called Common Evaluation Methodology (CEM). The CC and CEM are used by accredited testing laboratories to conduct TOE evaluation. In the United States, testing is done under a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency called the National Information Assurance Partnership (NIAP). The NIAP a program called the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for information technology security. Testing is also done in laboratories in other countries. Testing, design review and implementation review help reduce the security risk in a product (More information on this program can be found at <http://niap.nist.gov>). Part of the CC process is validation of the evaluation results. The CC has set up independent validation of the evaluation results to insure that the evaluation was conducted properly.

With the ever increasing threat to the security of our systems and the value of the data that it stores, we have got to have viable, tailored, verifiable security standards that can be applied to IT products and systems. The US government has taken the lead in requiring products that meet CC testing requirements. Effective 1 January 2001, preference will be given to the acquisition of information assurance engineered products

and by 1 July 2002, acquisition of these products will be limited to those that have been evaluated and validated. With the government mandating products that have passed CC/CEM testing and validation can private industry systems be far behind?

References:

“Advisory Memorandum of the Strategy for Using the National Information Assurance Partnership (NIAP) for the Evaluation of Commercial Off-The-Shelf (COTS) Security Enabled Information Technology Products.” NSTISSAM INFOSEC/2-00. February 2000.

Roback, Edward A. “Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.” Recommendations of the National Institute of Standards and Technology. Computer Security. NIST Special Publication 800-23. August 1999.

“Common Criteria Evaluation and Validation Scheme: NIAP Validated Products List”. URL: <http://niap.nist.gov/cc-scheme/Validated Products.html> (28 November 2000).

Syntegra. “Common Criteria Version 2: An Introduction.” November 1998. URL: http://csrc.nist.gov/cc/info/cc_brochure.pdf (28 November 2000)

“Common Criteria for Information Technology Security Evaluation.” User Guide. October 1999. URL: <http://www.commoncriteria.org/docs> (27 November 2000)

“Common Criteria for Information Technology Security Evaluation.” Version 2.1 CCIMB-99-031. August 1999.

Troy, Eugene F. “Common Criteria: Launching the International Standard” 24 November 1998. URL: http://csrc.nist.gov/cc/info/cc_bulletin.htm (1 December 2000)

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS