Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Common Criteria ISO/IEC 15408 - The Insight, Some Thoughts, Questions and Issues

With the rise of security breaches and the running of technology at its highest gear on the information superhighway, protection of confidential and vital information never has been more crucial. This paper provides an overview of an international effort called Common Criteria (CC), an IT Security evaluation methodology, developed to define and facilitate consistent evaluations of security products and systems, fostering international recognition and trust in the quality of security products and systems throughout the ...

Copyright SANS Institute

Author Retains Full Rights

AD

THE COMMON CRITERIA ISO/IEC 15408– THE INSIGHT, SOME THOUGHTS, QUESTIONS AND ISSUES

By Ariffuddin Aizuddin

(As part of the requirement of GSEC Examination)

With the rise of security breaches and the running of technology at its highest gear on the information superhighway, protection of confidential and vital information never has been more crucial. The needs to have some kind of assurance that the products and the systems used, that provide an adequate security to the security objective started since the "Orange Book"- TCSEC (1985), in the US. Various countries then began their initiatives to develop evaluation criteria that builds upon the concepts of TCSEC; in Europe – ITSEC (1991), Canada – CTCPEC (1993), US - Federal Criteria (Draft 1993). The Common Criteria – ISO/IEC 15408 – Evaluation Criteria for Information Technology Security represents the outcome of series of efforts to develop criteria for evaluation of IT Security that are broadly useful within the international community.

The security assurance that user required can come from various method; rely upon the word of manufacturer/service provider, test the system themselves, or rely on an impartial assessment by an independent body (evaluation). Therefore, the evaluation criteria can be a yardstick for users to assess systems or products, a guarantee for manufacturers of secure systems or products and a basis for specifying security requirements.

The Common Criteria (CC) was developed to facilitate consistent evaluations of security products and systems. It is an international effort to define an IT Security evaluation methodology, which would receive mutual recognition between customers and vendors throughout the global economy. The theory behind CC, is that CC will advance the state of security by encouraging various parties to write Protection Profiles outlining their needs and desires, in return it will push vendors to meet the resulting Protection Profiles. The theory proposes that, as users profile desired capabilities that are not currently available, the vendors will attempt to gain market share by taking up the challenge.

In brief, the CC is a useful guide for the development of products and systems with IT security functions and a guide for procurement of commercial products and systems with security functions. CC philosophy will provide assurance based upon an evaluation (active investigation) of the IT product or system that is to be trusted. The validity of documentation, and resulting IT product or system, is measured by Expert Evaluators with increasing emphasis on scope, depth, and severity.

CC – The Introduction

ISO Support. The acceptance by ISO will ensure that CC rapidly becomes the world standard for security specifications and evaluations. The adoption as a world standard and wide recognition of evaluation results will provide benefits to all parties. A Wider choices of evaluated products for consumers, greater understanding of consumer requirements, and a greater access to markets for developers.

CC Certified Product. The information can be found in evaluation schemes publications or on scheme web sites. Care should be exercise when selecting products from the lists, to ensure that the same version of products are being used, and that the intended environment is consistent with that evaluated.

Guarantees. The certification/validation of evaluation results can provide a sound basis for confidences that security measure are appropriate to meet a given threat, and they

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

are correctly implemented. However, it is not an absolute guarantee of security. As IT Security propose, the term security should always be viewed in relation to particular set of threats and assumptions about the environment. Nevertheless, CC includes an assurance scale (Evaluation Assurance Levels) that can be applied to help generate different levels of confidence in the security products.

Interested Parties:

Consumers – The CC evaluations satisfy the needs of consumers, as this is the fundamental purpose and justification for evaluation process. The results will help them to decide an evaluated product or system to suit their security needs. CC gives implementation independent structure, the Protection Profile (PP) in which to express their special requirements for IT security measures.

Developers and Products Vendors – The developers need to understand how PPs work, since matching a PP is one of the best ways to ensure that a product provides the user requirements. Those that seek CC certification/validation need to understand CC approach, and what an evaluation facility that is require from them.

Evaluators and Certifiers/Validators/Overseers – CC model provides the separation roles of evaluator and certifier/validators. Certificates are awarded by national scheme based on evaluation carried out by independent evaluation facilities (testing laboratories).

Accreditors and approvers – They are the authorities that has the mandate to ascertain the security standard to be achieved using the CC. Acceditors need to understand how the Evaluation Assurance Levels (EAL) can be used as objective measures of risk reduction, when applied to critical security functions in IT system.

What is the CC?

Overview.

The CC document consists of:

Part 1 - Introduction and General Model. Part 1 defines general concepts and principles of IT security evaluation and presents a general model of evaluation. This part also presents the constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, it provides the usefulness of each part of the CC in terms of each of the target audiences.

Part 2 - Security Functional Requirements. This part establishes a set of security functional components as a standard way of expressing the security requirements for IT products and systems. The catalog is organized into classes, families, and components.

Part 3 - Security Assurance Requirements. This part produces a catalog of establishes 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. 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.

Consumers' use of CC – Consumer use of CC relates to the specification of functional and assurance requirements of products and systems under procurements. Part 2 of the CC is used when specifying the security functional requirements, and Part 3 is used when specifying the assurance requirements. Consumer can then use this statement of requirements as a specification to vendors of products or system integrators.

Developers' use of CC – The CC should be used to produce deliverables to meet the (CC) requirements. They may specify the functional and assurance requirements in a Security Target, or may have them specified by the consumer in the form of a Protection Profile. The

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

functional requirements, specified using Part 2 of CC, are those with which the products are required to conform. Part 3 of the CC contains developer actions that are to be followed when formulating deliverables for evaluations to a particular set of assurance requirements.

Evaluators use of CC – CC contains mandatory statements of evaluation criteria that used when determining whether a Target of Evaluation (TOE) meets its claimed security functionality and assurance requirements. Guidance on the application of the CC is given in the Common Evaluation Methodology (CEM).

Key Terminology & Concepts.

Protection Profiles.

Definition: Implementation independent *statement* of security requirements for a category of TOEs (target of evaluation) that meet specific customer needs to address a specified security environment.

A Protection Profile describes a set of requirements that are specified with the aim of countering specified threats in a specified environment. The Protection Profile may not describe the optimal solution, but it is anticipated that it will be consistent, correct, and complete. In other words, it will not be self-contradicting. It will contain all the pertinent information to adequately talk about the problem space it seeks to address. It is anticipated that a Protection Profile may be written by any of several parties. A Protection Profile may be written by a user community as a means of stating a need that is not adequately met by the current offerings on the market. An accrediting body such as a government, industry group, or insurance firm might also author a Protection Profile. This might be done as a means of standardizing for interoperability. It also can be done to set a minimum standard for protection. Protection Profiles - (*what the customer wants*) - is designed to answers the question: "What do I need in a security solution?"

Security Target.

Definition: Are a basis against which an evaluation is performed. It's contains the TOE security threat, objectives, requirements, and summary specification of security functions and assurance measures.

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. Security Targets is actually designed to answers the question: "What do you provide in a security solution?" The Security Target - (*what the developer claims*) - authors are product vendors, developers and integrators.

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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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. In short, TOE - (*the product*) - is an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

CC Building Blocks.

Security Functional Requirements.

Security functional requirement are grouped into classes. Classes are the most general grouping of security requirements, and all members of a class share a common focus. There are 11 functionality classes within Part2 of the CC. These are as follows:

Audit, Identification and Authentication, Resource Utilizations, Cryptographic support, Security management, TOE Access, Communications, Privacy, Trusted Path/Channels, User Data Protection, Protection of the TOE Security Functions.

Each of these classes contains a number of families. The requirements within each family share security objectives, but differ in emphasis or rigor.

Security Assurance Requirements.

Security assurance requirement are grouped into classes. Classes are the most general grouping of security requirements, and all members of a class share a common focus. There are 8 assurance classes within Part3 of the CC.

These are as follows:

Configuration management, Guidance documents, Vulnerability assessment, Delivery and operation, Life cycle support, Assurance maintenance, Development, and Test.

Two additional classes contain the assurance requirements for PPs and STs.

The CC has provided 7 predefined assurance packages known as Evaluation Assurance Levels (EALs).

Brief explanations of EAL:

EAL1 - Functionally Tested: This where the applicable where threat to security is not serious, however some confidence in current operation is required. In the evaluation, there is no assistance from TOE developer. The requirements are: Configuration Management, Delivery and Operation, Development, Guidance documents and Tests.

EAL2: Structurally Tested**.** This assurance level is applicable where low to moderate level of independently assured security is required. Here, it requires some cooperation from the developer. It will definitely require no more than good vendor commercial practices. To add to the previous requirements are developer testing, vulnerability analysis, and more extensive independent testing.

EAL3: Methodically Tested and Checked. It is applicable where moderate level of independently assured security is required. The cooperation from the developer is requires. It

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

places additional requirements on testing, development environment controls and configuration management. The additional requirement is the Life Cycle support.
EAL4: Methodically Designed, Tested, and Reviewed. This is applicable where moderate to high level of independently assured security is required. It is to ensure that there is some security engineering added to commercial development practices. This currently the highest level likely for retrofit of an existing product. There are additional requirements on design, implementation, vulnerability analysis, development and configuration management.
EAL5: Semiformally Designed and Tested. It is applicable where high level of independently assured security is required. It requires rigorous commercial development practices and moderate use of specialist engineering techniques with additional requirements on specification, design, and their correspondence.
EAL6: Semiformally Verified Design and Tested. This evaluation level is applicable where assets are valuable and risks are high and do requires a rigorous development environment. The additional requirements are on analysis, design, development, configuration management, and vulnerability/covert channel analysis.
EAL7: Formally Verified Design and Tested. This is applicable where assets are highly valuable and risks are extremely high. However, practical use is functionally limited for amenability to formal analysis. The assurance is gained through application of formal methods. The additional requirements for these is testing and formal analysis.

Supporting Documents & Tools

Common Evaluation Methodology (CEM)

The evaluation methodology of CC is the CEM, the companion methodology document - Common Evaluation Methodology for Information Technology Security Evaluation (CEM). It is a companion to the CC documentation. Its focuses on the actions evaluators must take to determine that CC requirements have been complied with. In other word, its described the actions and activities to be performed by an evaluator in order to conduct a CC evaluation. CEM is used by the evaluation schemes to ensure consistent application of CC requirements across multiple evaluations and multiple schemes. CEM is an important component of mutual recognition. However, CEM have yet to support all of Part 3 of the CC. Part 1 of CEM contains universal principles and general model of evaluation (it is currently obsolescent). Part 2 provides the detailed methodology for evaluations at EAL1 to EAL4. CEM is currently at version 1.0; future expansion of the scope and possible reorganization of CEM is under consideration.

ISO Guide to Writing PPs and STs

ISO has produced a guide to the construction of Protection Profiles (PPs) and Security Target (STs) that is consistent with the CC. The document is primarily aimed at those who are involved in the development of PPs and STs. However, it is also likely to be useful to evaluators of PPs and STs, and those who are responsible for defining and monitoring the application of the methodology for PP and ST evaluations.

CC ToolBox & CC Profiling Knowledge Database.

It is the language for describing IT product and system security and the grammar for organizing the security requirements into coherent security specification documents. It's a software tools to facilitate transition to CC and facilitates writing PPs and STs. CC Profiling Knowledge Base™ is a database of sample security engineering information. The audience is the PP and ST authors, Novice CC users, and experienced authors. CC Toolbox goal is to promote the international use of the CC. The product is to assist in drafting PPs and STs and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

can save ST development time if the PP "rds" file is provided to the vendor. The tools help to enforce standard PP and ST format labor extensive work into automated. The tool suggests Policy, Threats, Assumptions, and Objectives statements. The tools provide the front end and/or back end interfaces. The tool is logically and technically solid coding. It is the freeware provided by NSA, whom encourages an open distribution. Download CC Toolbox™ and CC Profiling Knowledge Base™ at http://niap.nist.gov/tools/cctool.html, and http://niap.nist.gov/classes/classdescrip.html

Checklist for Procuring CC Products.

- √ Certification/Validated product required by organizational policy?
- √ Product certified/validated?
  - √ Certified/Validated against a PP?
    - √ PP endorsed by a relevant organization?
- √ Product in Evaluation?
  - √ What stage has the product reached?
  - √ Can vendor claim be independent verified (e.g. evaluation facility)?
- √ Product not in evaluation?
  - √ Are there plans to enter?
  - √ Are plans credible?
  - √ Does the vendor have any incentive to achieve certification/validation?
  - √ Does vendor have other evaluated products?
- √ Does the PP address the relevant risks?
  - √ Is the intended environment consistent?
    - √ Hardware platform?
    - √ IT environment available?
  - √ Are risks countered sufficiently?
  - √ Are the assurance measures adequate?
- √ Is the vendor committed to maintaining certification/validation for future release of the products?

Some Thoughts, Questions & Issues:

Protection Profiles & Security Target - Issue.

What is not as commonly realized is that a vendor may write a PP. The clever vendor might first describe their product in PP format, perhaps with the help of key customers. He would then write the product-specific Security Target in a way that points back to the PP. Not surprisingly, the product matches the requirements perfectly.

A Security Target by itself, being inherently product specific, and would not be as useful to the vendor. The Security Target, by contrast, is implementation specific, and is the document which product evaluations are conducted against. Thus, the Security Target format will not be used to state requirements. The vendor can have his product evaluated against the ST to provide potential customers with the independent testimony as to the truth of the claims he makes about his product.

Pushing a vendor to go to the PP route, rather than using the Security Target alone, should be taken into account as a possible factor in CC projections and strategies. Given that the PP is the anticipatory document, while the Security Target is an expression of what has already been implemented, we can safely say that Security Targets will be of only minimal influence in driving the future course of the security marketplace.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

One of the major beneficial functions of the whole CC plan is that those who write PPs will be able to drive the market. The users may have a desire to push the vendors to provide more functionality, and they may choose to use the PP to do so. Which strategy should they pick for the optimal result? The user community can write a PP, that they know can be met by currently available products. This will set a minimum standard. By doing so, however, they get no improvement above the current state of the practice, they may not even get any substantial product differentiation. In the case of a PP, which calls out standards that all competing products easily meet, the user community will at minimum get the benefit of independent evaluation of the products against their profile. The more interesting situation comes when the PP writer wishes to push beyond either the state of the practice or the state of the art. In these cases, the user must weigh the cost against the potential benefit. Clearly, if the user writes a PP with which to push the vendor to greater efforts, the trick will be to push, but not push too far. One wants to write a PP that will inspire the vendors to produce products with new or better functionality. If one sets the standard too high, though, the vendor may either not be able to reach it, or may choose to not try, deeming the cost too high for the perceived benefit.

The "all or nothing" nature of the current evaluation strategy may be misguided in some cases. If, there are no products, which successfully meet the PP, it is in the best interests of both the user community and the vendors to allow dissemination and confirmation of the details of the evaluation results, if the vendor chooses to release them. Given a product, which failed all tests and a product, which failed only one test when evaluated referring to the same PP, the customer would definitely benefit from knowing which product had the better results, even if both failed. Even in cases where one product passed and one product failed by a small margin, the customer may wish to know this. A substantial price difference or the nature of the test that the one product failed may make the failed product the better buy for some applications.

An Alternative Assurance Methodology.

Let us look at the alternatives to the Common Criteria assurance approach.
The general assurance alternatives is to characterize the assurance approaches on a high level concept, one way is to distinguish between process or product evaluation. Another dimension would be to distinguish between different phases; design and development on the one hand or operation on the other hand.The WG 27 of ISO have come up with the ISO project 15443 "A framework for IT security assurance (FrITSA)" studies and categorizes a number of assurance methods. The intent of the framework is to be an aid for the understanding and application of assurance methods. The common criteria approach is a product and system approach, which covers the design and development phase of those products and systems, not the operation phase. The same is true for the approaches represented by the other evaluation criteria, which formed the basis for the Common Criteria, the TCSEC, the European ITSEC and the Canadian CTCPEC.

The methods like the ISO Technical Report "Guidelines for the Management of IT Systems, the Code of Practice which is a British standard and the Baseline Protection Manual deal with the general security situation within one organization and have thus a very different focus. The most obvious alternatives to the Common Criteria assurance approach are the process approaches of the design and development phase.

These are also characterized as "developmental assurance". Those include the SSE-CMM approach, the System Security Engineering Capability Maturity Model and the Trusted Capability Maturity Model. Both models are quite concrete and are based on a Capability Maturity Model developed by the Software Engineering Institute. Other approaches like the developer's Pedigree, the Warranty Assurance and the Supplier's declaration are on a more

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

general level. The well-known ISO 9000 quality assurance standard is also process oriented. The evaluation rating maintenance, which becomes relevant after an evaluation has been completed, is very closely related to the assurance approaches represented by all evaluation criteria.Given this situation with several assurance approaches it is appropriate that the Common Criteria project is open for alternatives. This is explicitly expressed in the scope of the Common Criteria. It is additionally indicated by the openness for assurance requirements from outside the Common Criteria, which was not the case for all the basic criteria, and it is expressed by the existence of the Alternative Assurance Working Group (AAWG) of the Common Criteria project.

The Alternative Assurance Working Group concentrated on developmental assurance. They decided that the fundamental target should be to develop alternative ways to meet the objectives of the Common Criteria Evaluation Assurance Levels (EALs). The Alternative Assurance Working Group laid the focus of their activities on EAL3. They developed an Alternative Assurance Package (AAP3), which is asserted to satisfy the objectives of EAL3. It is clear that the alternative assurance package AAP3 cannot cover all aspects of EAL 3 by developmental assurance methods. So it is split into two parts: Developmental Assurance Level (DAL) and a Subset Evaluation Assurance Level (SEAL).The Developmental Assurance Level part contains the EAL3 requirements covered by the "underlying approaches". These are five more or less well known assurance approaches from the public domain. The Subset Evaluation Assurance Level part contains those EAL3 requirements, which are not covered by the underlying approaches.

Here are the underlying approaches:

- X/Open Security Branding, the assurance method which, provides assurance by conformance testing, vendor warranty and trade mark, where X/Open is a consortium, of companies creating open standards to provide an open system environment.
- ISO 9000 Part 3, the application of ISO 9001 to the development, supply and maintenance of software.
- Trusted Capability Maturity Model.
- System Security Engineering Capability Maturity Model (SSE_CMM).
- B-Method Engineering Environment, which is based on formal specification, design and proofs.

Combinations of the approaches are possible, for example SSE_CMM and X/Open Security Branding.The Alternative Assurance Working Group recommends using the SSE_CMM model as the underlying approach. It is claimed that the Alternative Assurance Package 3 provides coverage of EAL3 requirements for almost all developer action elements, several content and presentation of evidence elements and some evaluator action elements related to testing. The Alternative Assurance Package 3 has certainly the potential of an increase of efficiency for example in cases where many similar products are designed and developed in the same environment and all shall be evaluated. However, on the other hand Alternative Assurance Package 3 still awaits practical application. This is one reason why Alternative Assurance Package 3 cannot be considered as a result of the Common Criteria project being jointly supported by all Common Criteria project organizations.

The lack of practical application experience is the main reason that no developmental assurance requirements have been incorporated in the Common Criteria. If the Common Criteria open for explicitly defined assurance requirements, principally it would be possible to base an evaluation on alternative assurance methods. However, it involved scheme and should include the environment of that specific evaluation. The Common Criteria based evaluations provide "non technical" assurance, which should be considered as an important value over and above what the Common Criteria and the Common Criteria based evaluations provide technically.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Common Criteria evaluations are based on a published and approved evaluation methodology. The alternative assurance approaches normally do not provide such "non-technical assurance". This should be considered when analyzing the advantages of applying the Common Criteria. The evolution of alternative assurance approaches is important to get the necessary flexibility. The "alternative" will mean that in some cases the alternative assurance approach is the better one and in others the "traditional" CC evaluation approach.
It would be an ideal situation if an appropriate and effective assurance approach is available for each IT product or system depending on its specific environment and background.

Application of Common Criteria – The Finding.

In the a case study in Computer Security Journal, Volume XVII, Number 2, 2001 have shown how US FAA have applied the Common Criteria to a large system; i.e., the development of Protection Profile for the National Air Space Infrastructure Management System. The scope of the Security services comprises of Application Level Security, Facility Level Security and the WAN Level Security, which involve Telecommunication vendor. The telecommunication service challenges are to define what does an EAL mean in the context of system, in services contract and after the initial C&A. In the context of a system it reflects the degree of confidence that the collective security architecture has met its security objectives. EAL in the context of services contract represents the security integrity of the functions specified in the PP and measured by QoS parameters. After the initial C&A, the security assurance addresses the operations and maintenance, it's aimed at assuring that the TOE will continue to meet its security target as changes are made to the TOE or its environment. These include the discovery of new threats or vulnerabilities, changes in user requirements, the correction of bugs found in the certified TOE, and other updates to the functionality provided. They are also studying into supplementing the Common Criteria security assurance with periodic System Security Engineering Capability Maturity Model (SSE-CMM) to ensure the product and process issue related to security engineering receive appropriate scrutiny and attention. Common Criteria was known only apply to products and systems (including computer network), however the case study concludes that it is logical and feasible to broaden their application to services contracts, especially telecommunications.

Cost Effectiveness of Evaluation – The Need.

The security market dilemma on evaluated product is the cost. Consumers "want" an absolute security at no additional cost, no impact on performance and it is available now. The vendors "provide" largest market (profits) at no additional cost to them. It is – "Consumer want a lot for a little" and "Vendor want a little for a lot". So what is the reasonable enough cost that we are looking for? What and When is enough and How do we keep the costs low enough to be reasonable with effective trade off – a technically sound products at a reasonable cost.

Beside the fee paid for evaluation, we need to take into account of indirect costs like the time devoted to producing evidence and the training of evaluators. The evaluation sponsor can spread the cost to the number of large customer; in other case the sponsor or single customer may have to bear all the costs on their own.

Other Issues.

There are few other issues that required further consideration by the board of the CC such as the following:

1. The interpretation of CC, There could be an interpreted drift by different scheme. Currently the interpretation is handle by the CCIMB.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2. The CC evaluation does not cover the assessment of the algorithm strength. Cryptography evaluation must go together with the FIPS 140-1, the cryptography standard.
3. Evaluation Methodology of the CC is using CEM. CEM however, currently only cover up to EAL4.
4. Using of the CC in other application such as the critical infrastructure, the telecommunication sector.
5. Need to work closely with ISO SC 27 which have the common criteria related activities such as CD 15292 – protection profile registration procedure, PTDR 15446 Guide on the production of protection profile and security target and WD 15443 conformance declaration for IT security.
6. More research should be put forward for more automated tools that will assist the usage of CC and the evaluation process.
7. There are some misunderstandings of usage of the CC in IT security communities.
8. The acceptance of the CC among the IT Security vendors and industry.

CONCLUSION

The international presence of the Common Criteria delivers proof of quality and reliability of the product internationally and offers comparability with globally competitive categorical product. The Common Criteria provides an added advantage to its security evaluation: it endows international recognition and trust in the quality of the security product. Specification of security properties of IT systems and products that address unauthorized disclosure (confidentiality, privacy), unauthorized modification (integrity), loss of use (availability) serves the scope of the CC. The CC is the basis for the comparison of results of independent evaluations. CC is applicable to IT security countermeasures implemented in HW, SW, and firmware. The CC is independent of technology, in user-defined combinations. Outside the Scope of the CC are the "People-based" and physical security countermeasure implementations.

However, CC does not run without flaws and it needs further thought and improvement. There is a need for us to look at more effective and efficient evaluation methodology that is internationally accepted. We should look at the interpretation and rational of the assurance evaluation of CC at other perspective and out of the box. There should be more effort in developing automated tools for the CC. The most concern of all is the cost of evaluation; there should be some mechanism to reduce the cost of evaluation.

Nevertheless, the CC and assurance evaluation do not solve all the security issues! The CC can only assist the IT security communities to have the assurance they need and may push the vendor and developer for better security solution. IT Security is a process, which requires the effort from every individual and management in every organization. It is not just managing the risk and managing the threat; it is the security processes of Assessment, Prevention, Detection and Response; it is a cycle.

References:

1. http://www.niap.nist.gov/cc-scheme
2. http://www.commoncriteria.org
3. http://niap.nist.gov/cc-scheme/iccc/program.html, 1st International CC conference proceeding materials.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4. Van Essen, Ulrich, "CC and Alternative Assurance, Future Applications of CC, Common Criteria and Developmental Assurance",1st International CC conference, German Information Security Agency (BSI)
5. Grainger, Gray, "Common Criteria Tool", 1st International CC conference.
6. Syntegra Inc, UK, "Common Criteria User Guide", 1999.
7. http://niap.nist.gov/tools/cctool.html
8. http://niap.nist.gov/classes/classdescrip.html
9. http://csrc.nist.gov/cc/info/infolist.htm
10. http://www.radium.ncsc.mil/tpep/library/ccitse/cc_over.html
11. http://csrc.nist.gov/cc/ccv20/ccv2list.htm
12. Olthoff, Kenneth G, "Thoughts and Questions on Common Criteria Evaluation", National Security Agency.
13. Herrmann, Debra and Keith, Stephen, "Application of Common Criteria to Telecomm Services: A Case Study." Computer Security Journal, Volume XVII, Number 2, 2001 page 21-28.
14. Gollmann, Dieter, "Security Evaluation" Computer Security, John Wiley & Sons – Chapter 9.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced