GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Name: Nor Aza Ramli
Title: Protection Profile, A Key Concept in The Common Criteria
Version: GSEC Practical Assignment Version 1.4b

Table of Contents

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract
This paper will give a description of the roadmap to the Common Criteria (CC) that basically explains the distinct but related parts and how three key CC user groups namely the consumers, developers and evaluators use them. One of the key concepts in CC is the Protection Profile (PP). A structure of it will be discussed taking an evaluated PP as an example. This is to demonstrate the structure of a PP and how the requirements are achieved from the beginning by considering the security environment and understanding of the Target of Evaluation (TOE). Some issues with regards to PP will also be discussed and that will bring to the conclusion of having a PP as a tool for determining the most suitable product or system that can address the required security features.

Introduction
IT people have to deal with a lot of challenges when it comes to planning and recommending the product or systems that would fit best in their organizations. There are so many choices available in the market and most of them claim to be the leading products. It is difficult to choose without any checklist and baseline as guidance to determine all requirements such as functionality and security are met. With the emerging of technology, security is not something that can be pushed aside. As a matter of fact, security is the number one criteria that must be looked into. Acknowledging this wide spread requirement the ISO has thus recognised CC version 2.1 as a standard for security specifications and evaluations, ISO 15408.

CC Key Terminologies
Before we proceed with the discussion, it is necessary to understand a few terminologies that are being used by CC.

1) Target of Evaluation (TOE)

Target of Evaluation is an IT product or system, which is subject to an evaluation. TOE includes all material like documentation and administrator guides that are delivered with it. [1] TOE might not be a full system or product as it could be referring to only a particular module or part of it. The security features in a TOE would be corresponding to the requirements as claimed in a Security Target in the case of a vendor. It could also be addressing the requirements put forth by a Protection Profile from a consumer point of view.

2) Protection Profile (PP)

A protection profile defines an implementation-independent set of security requirements and objectives for a category of TOEs, which meet similar consumer needs for IT security. [2] Examples are PP for application-level firewall and intrusion detection system. PP answers the question of 'what I want or need' from the point of view of various parties. It could be written by a user group to specify their IT security needs. It could also be used as a guideline to assist them in procuring the right product or systems that suits best in their environment. Vendors who wish to address their customers' requirements formally could also write PP. In this case, the vendors would work closely with their key customers to understand their IT security

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

requirements to be translated into a PP. A government can translate specific security requirements through a PP. This usually is to address the requirements for a class of security products like firewalls and to set a standard for the particular product type.

3) Securities Target (ST)

A security target contains the IT security objectives and requirements of a specific identified TOE and define the functional and assurance measures offered by that TOE to meet stated requirements. [3] Unlike the PP, ST is more product-specific as it is used as a basis for agreement between developers, evaluators and sometimes consumers on the TOE security properties. ST answers the question of 'what I have to offer' from the point of view of a product vendors, developers or integrators. The content of an ST is an extension to that of a PP. The additional information is TOE Summary Specification (TSS) and statement of conformance to one PP or more. The TSS describes TOE security functions and its assurance measures. Any PP conformance claims must be complete as no partial conformant is permitted for CC evaluation. The underlying requirement is such that an ST has a clear, complete and unambiguous content. This is to ensure ST evaluation can be carried out.

What is Common Criteria?

The CC represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. [4] Scope of the CC is dedicated to the IT security well being. CC is used as a basis for evaluation of IT security properties of any systems or product. i.e. the TOE. It addresses the protection of information from unauthorized disclosure, modification or loss of use in line with the standard security requirements for confidentiality, integrity and availability. The TOE could be hardware, software of a firmware. However, physical aspects of IT security are not its scope. CC is itself a tool. It is a means of constructing IT security requirements for a product or a system by providing a list of standard and a set of tools. CC has been organized in three distinct but related parts. CC User Guide defines the parts, as below:

Part 1, Introduction and general model is the introduction to the CC. It defines general concepts and principles of IT security evaluation and presents a general model evaluation. Part 1 also presents how IT security requirements (functional and assurance) could be constructed from understanding the security environment that would lead to the security objectives of the TOE.

Part 2, Security functional requirements, establishes a set of security functional components as a standard way of expressing the security functional requirements for TOEs. It describes the functional classes, families and the associated components.

Part 3, Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. The structure is similar to Part 2 with description of the assurance classes, families and the associated components. Part 3 defines evaluation

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

criteria for PPs and STs. The Evaluation Assurance Levels (EALs) is presented in this section which define the predefined CC scale for TOEs evaluation rating assurance.
[5]

The IT security requirements constructed using CC would act as useful guidelines to at least three groups of intended recipients; consumers, developers and evaluators. As summarized by Mr Gene Troy from the U.S. National Institute of Standards and Technology (NIST) CC is a way to define IT security requirements for some IT products from the users' point of view. For the developers, it is a way to describe security capabilities of their product. And finally for the evaluators, it is a tool to measure the confidence we may place in the security of a product. [6] Further discussion for each group of CC recipients can be defined as below:

Consumers – CC is used as guidance and reference in writing down their IT security functional requirements using Part 2 and specifying the IT security assurance requirements using Part 3. The functional and assurance requirements can be used as a specification to either system, product or system integrator vendors. The consumers will produce a Protection Profile to spell out their requirements. They could also use CC as reference to understand any Protection Profile or Security Target to assist them in making decisions for procurement.

Developers – CC is used as guidance and reference in interpreting or constructing statements of functional requirements and assurance requirements. These requirements could be stated by the consumers in any Protection Profiles or could also been developed by themselves in a Security Target. Basically, the developer may use CC Part 2 and Part 3 to ensure conformance of their product or system to the requirements.

Evaluators – Part 2 and Part 3 CC are used as mandatory statements to ensure the product or system under evaluation meets its security functional and assurance requirements claims. The evaluators are trained in IT security and must understand the CC thoroughly. They usually come from commercial testing laboratories that have been given the mandate from national schemes. CC describes general action but does not specify exact procedures for the evaluators to follow in carrying out the evaluation exercise.

How does CC come about?
Since early 1980's there have been several ideas and initiatives made to address the need to come out with a standard of IT security evaluation. These however were done at national levels and resulted in several standards e.g. the Trusted Computer System Evaluation Criteria (TCSEC) in the United States, the European Information Technology Security Evaluation Criteria (ITSEC) and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) to name a few. The International Organisation for Standard (ISO) has started work in 1990 with the aim of developing an international standard criterion that could be used and mutually recognized by the international community. In June 1993, the sponsoring organizations of the existing US,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Canadian, and European criterias started the CC Project to align their separate criteria into a single set of IT security criteria. [7] The CC has been developed with consideration of various national experiences and this is an advantage to the CC. The first version was completed in January 1996 and it was then revised considering the feedbacks from public reviews and also incorporating the results of several numbers of trial evaluations. CC Version 2.0 was produced in April 1998 and it became the ISO International Standard 15408 in 1999. The CC Project subsequently incorporated the minor changes that had resulted in the ISO process, producing CC version 2.1 in August 1999. With this latest publication, there are no technical differences between CC and ISO15408.

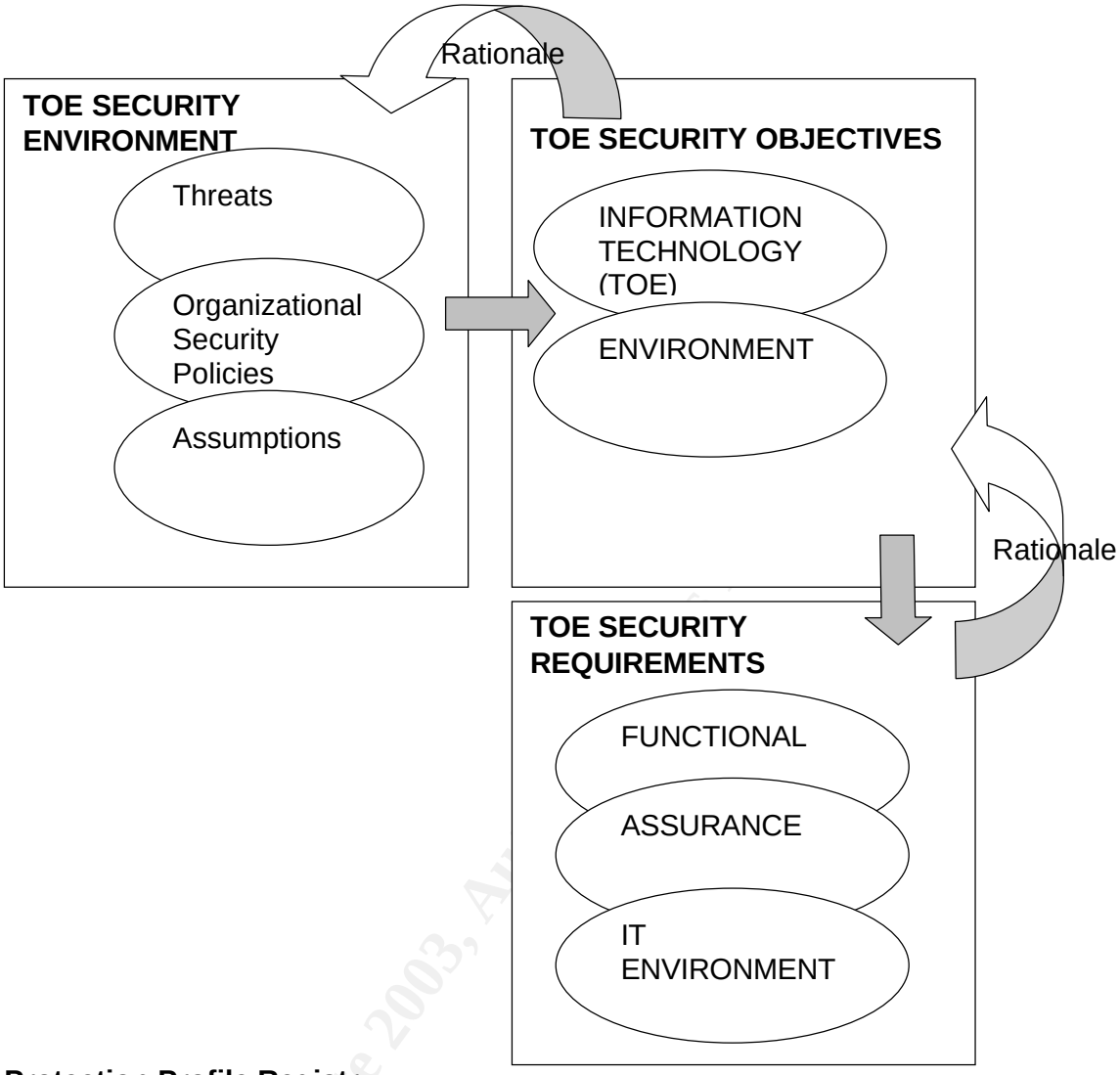
Mutual Recognition

Common Criteria Recognition Arrangement (CCRA), initially known as Mutual Recognition Arrangement (MRA) was signed in 1998 by the government agencies in Canada, France, Germany, the United Kingdom and the United States. [8] By this agreement, evaluations carried out in any of the countries are mutually accepted and recognized by the member countries. This agreement is a non-binding agreement such that a new member can be admitted subject to unanimous consent of the current members. Details of the arrangement could be found in the CC website; reference http://www.commoncriteria.org/registry/mr.html

What is Protection Profile and Where Does It Fit in The CC?

Now that we have the background and some introduction of the CC, we can go a bit deeper into one of its key concepts i.e. the Protection Profile, PP. As mentioned earlier, PP defines the security requirements. It does so by providing a framework that describes the TOE security environment, and objectives from which the requirements could be derived.
To establish the security environment, the TOE must be first identified and described. The diagram below depicts how the threats, organizational policies and assumptions from the TOE security environment become an input to determining the TOE security objectives. Having determined the TOE security objectives, the TOE security requirements can be drawn up using CC Part 2 and Part 3. The requirements and objectives shall be traceable to the inputs and this shall be demonstrated in the rationale statements as evidence that the PP is complete, coherent and consistent internally.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Protection Profile Registry

In order to provide a single point of reference for consistent and current information on all certificates authorised under the CCRA (Common Criteria Recognition Arrangement), a Centralised Certified Product List (CCPL) for IT security products and a Protection Profile Registry (PPR) for Protection Profile is maintained on the CC Information Web Site. [9] The reference address for the registry of all product categories listed under CCPL is http://www.commoncriteria.org/ccc/epl/productType/eplinfo.jsp?id=99. The registry contains copies of all PPs, which have been evaluated and certified. Draft versions and PP under development are listed as well. Products under evaluation are listed under the repository section and can be found at the following address; http://www.commoncriteria.org/index_ccra_iepl.htm.

Protection Profile Structure

In describing the content of a PP, a walkthrough of its structure will be based on a firewall PP which is being published in the CCPL registry website as above. This PP in entitled the U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments. The PP is of version 1.0, dated June 2000 and can be viewed at http://www.commoncriteria.org/ccc/protection_profiles/ppdetail.jsp?id=PP-015.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The content of a PP as required in CC Part 1, Annex B comprises of

1) PP Introduction (Identification and Overview)

   PP introduction shall contain its identification and overview information. The identification shall include a title, as in the example above is U.S Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments. Other information necessary would be the referenced CC version number with interpretation details, and PP version. Other information like the name of authors and sponsors can be included as well. The PP overview shall have enough information for potential users to determine whether they have found the suitable PP to address their interest and needs.

2) TOE Description

   TOE description is the product description under the scope of the evaluation. In the case of the above example, the PP shall describe the application-level firewall features that relate to the security requirements. One of the TOE descriptions in the above PP is "The TOE mediates information flows between clients and servers located on internal and external networks governed by the TOE". As the PP is implementation-independent, the features described may be assumptions.

3) TOE Security Environment (Threats, Assumptions and Organizational Security Policies)

   This shall describe the TOE security environment at which the TOE is expected to operate. The security environment shall be expressed by writing statements of threats and assumptions as well as incorporating any organizational security policies, which the TOE must comply.

   3a) Assumptions:

   Some statements of assumptions taken from the example above are:

   A.PHYSEC The TOE is physically secure.

   A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

   A.PUBLIC The TOE does not host public data.

   A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

   3b) Threats:

   The statement shall include all known or potential threats to the assets that the TOE or its environment shall protect. Some examples from the PP above are:

   T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

   T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3c) Organizational Security Policies
Organizational security policies or rules that the TOE must comply with. This can be omitted if the requirements are derived only from the other two inputs, threats and assumptions. An example from the PP above is:
P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).

4) Security Objectives

Security objectives of the TOE and its environment are derived from the three factors in the security environment. They must traced back to the threats and/or organizational policies and assumptions. The objectives must be complete, coherent and internally consistent within the same PP. The IT objectives of the TOE shall be addressed by imposing technical requirements on the TOE implementation. However, the non-IT objectives i.e. the security environment objectives will be managed through process and procedures in implementing and operating the TOE. Some objective statements taken from the PP above are:

4a) INFORMATION TECHNOLOGY (IT) - TOE
O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

4b) ENVIRONMENT
O.PUBLIC The TOE does not host public data.
O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

5) Security Requirements

CC Part 2 and Part 3 requirements catalogue are used to specify functionalities and assurance components for the TOE. Assurance

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

packages can be derived to meet distinct needs or chosen from a pre-defined assurance packages i.e. EALs. Taken from the PP above, some of the functional requirements are:

FIA_ATD.1 User attribute definition
FIA_UID.2 User identification before any action
FIA_UAU.5 Multiple authentication mechanisms

The assurance requirements for this PP compose EAL2 Augmented. This is taking the pre-defined EAL2 package with additional family and components included. Evaluation Assurance Level (EAL) is a predefined evaluation packages in CC Part 3. There are seven levels from EAL1 up to EAL7. However, the CCRA covers only EAL1 to EAL4.

6) PP Rationale

The rationale of selecting the functional and assurance components for the TOE. This section presents the evidence for evaluation that supports the claims that the PP is complete and coherent. This can be achieved by going through the objectives and by making sure that they are traceable to the security environment elements and sufficient to counter them. The requirements shall in turn be traceable to the security objectives. A summary of mappings in table forms is the easiest and fastest way of crosschecking for completeness and coherence.
An extract of the table of summary of mappings between threats, policies and security objectives from the example above:

	T.NOAUTH	T.REPEAT	P.CRYPTO
O.IDAUTH	X		
O.SINUSE		X	
O.SECSTA	X		
O.ENCRYP	X		X

From the table above, we can easily identify that all the threats have had at least one objective to address them. It also shows that one objective can address many threats.

An extract of the table of summary of mappings between functional requirements and it security objectives from the example above:

	O.IDAUTH	O.SINUSE	O.ACCOUN	O.SECFUN
FIA_ATD1	X			X
FIA_UID2	X		X	
FIA_UAU5	X	X		

Similarly, we can see that at least one functional requirements of the TOE has addressed the security objectives and vice versa. Therefore the relationship is as such it could either be one to one, one to many or many to one.
As for the assurance requirements, the rationale would be in a form of justification summary why the assurance package has been chosen; in this example is the EAL2 Augment. Explanation and justification are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

presented as to why the extra family and components have been chosen. This PP has also included a rationale for not satisfying all dependencies in the functional components. Generally, this may be allowed based on the justification and its implication to the TOE.

7) Application Notes

This is an optional part of the PP. It may contain additional information about the TOE. No application notes added in the example above.

Issues and Challenges

1) Writing Protection Profiles.

Writing a Protection Profile is not an easy task especially for those who are still new with CC concepts. Not any IT person can write a Protection Profile or fully understand all the CC concepts and masters its jargons. CC Part 1 has in its definitions, common terms which are used in a specialised way throughout the CC. To start writing a PP, one should first understand the security issues that he wants to address and write the requirements using simple terms and familiar jargons. It can then be translated into CC language. Dr. Ayer from Visa International had shared his experience applying CC to smart cards. "Once you get started, expect to be thoroughly confused at some point. What you need to do then is go back to your original statement of what you're trying to accomplish and see if you can do the translation both ways - from your jargon in to Common Criteria and then back again from Common Criteria to your own jargon. Only then will you be sure that you have mastered the translation and have some hope of solving the security problem". [10] The most important thing in writing a PP is that the author or authors must be definite of their requirements of the TOE. Otherwise, the effort will be a losing battle. The CC implementation is not without challenges. Acknowledging this, the forthcoming annual CC conference have set in its Track A new challenges and methods for a new millennium in using the CC as well as Common Evaluation Method (CEM) in IT security properties verification. [11]

2) Interested Parties

As much as the users want to have their requirements addressed in a PP, they might not have the resources to start the effort of writing one. Even if they are successful in writing a PP, more resources in terms of time and especially money are needed to go through the process of evaluation and certification. Therefore, even though the PP is promoted to meet common consumer needs for IT security, only those with the right fund would be able to construct PPs. Currently, there are eighteen certified PP as published by the CC website as of 15th March 2003; reference www.commoncriteria.org. Out of this, 50% of them have been sponsored by the U.S. National Security Agency, while the vendor group and user/working group have constructed 11% each of the validated PPs. One PP was developed by Consignia or U.K. Royal Mail Group plc, which represents the user group. This statistics show that at present, consumers would be relying on the standard drawn up by specific groups if they wish to use the PP in specifying their requirements. The good part of it is that everyone will then be using the same standard and guidelines. However, this might not be relevant in the case of different implementation

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

environment and application. For example, security concerns of a military organization are different as compared to those required by a research organization. For the latter to look into a PP produced by the former is all right but they must work further to tailor it to their own security requirements, looking again into the environment, threats and organizational security policy. It can be used as a guideline but not without any extra effort to get the requirements right. However, with the right initiatives and support from the IT community, CC will still hold the strength as an accepted international standard and one way or another it would lead the way in IT security evaluation and mutual recognition of its results throughout the whole world

3) Public Awareness

CC is a new concept. For United States and European countries where work for TCSEC and ITSEC have started much earlier, CC is more established as compared to other countries for example those in the Asia Pacific region. National Institute of Standards and Technology (NIST), an agency of the U.S. Commerce Department's Technology Administration has organized the first International Common Criteria Conference in May 2000. It has one out of the four tracks available discussing about Protection Profiles, guidance and tools. Several speakers presented the application of common criteria from implementation and evaluation point of view. The conference is a very good means of transferring CC knowledge and experience and this has been proven successful in all the three conferences that have been held annually since year 2000. The fourth International Common Criteria Conference will be held in Stockholm, Sweden on September 7th – 9th 2003 with 'Trust for Economic Growth' as its theme.

4) Vendors' Respond to PP

The PPs information used in this discussion are taken from the registry in the CC information website as of 15th March 2003. The CC information website reference is http://www.commoncriteria.org/epl/index.html. There are only two PPs listed under the database category. Both PPs are sponsored by Oracle Corporation to specify the IT security requirements for database management system. In relation to this Oracle Corporation has in the registry of the certified product, two certified database management systems that claim conformance to the PPs that they have produced. Table 4.0 below has all the details as taken from the CCPL and PPR lists.

Table 4.0: Database Category

Certified PP	Certified Product
PP-008 (Oracle DMBS Protection Profile)	Oracle 8 Release 8.1.7
PP-030 (Oracle Government Database Management System)	Oracle 8 Release 8.0.5

In the networking category there are three certified firewall PPs sponsored by the U.S. National Security Agency to define the minimum security requirements for firewalls used by the U.S. Government including the Department of Defense. There is no product in the CCPL that meets up the requirements as set in any of the PPs as listed in Table 4.1 below. However

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Check Point FireWall-1 Version 4.0 (SP5), which was certified in October 1999, has claim conformance to a draft version of the U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments, Version 1.d, Draft, September 1999. Similarly, certified in June 2002, Symantec Enterprise Firewall has claimed conformance to the U.S. Department of Defense, Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22 2000. This has shown positive responds from the vendors group to the CC community efforts and objectives in streamlining the IT security requirements that will be accepted mutually across the world.

Table 4.1: Networking Category (Firewall)

Certified PP	Certified Product
(PP-005) Traffic Filter Firewall Protection Profile For Medium Robustness Environments	NIL
(PP-010) Traffic Filter Firewall Protection Profile for Low Risk Environments (Version 1.1)	NIL
(PP-015) Application-level Firewall Protection Profile For Medium Robustness Environments	NIL

Conclusion

Common Criteria is a product of international efforts and as such it is capable in addressing the IT security requirements and contributes towards a healthy IT practises and environment. Protection Profile, a key concept in CC is a very structured way to define IT security requirements for any groups in the IT world including but not limited to end-users, vendors and governments agencies. Although at present, there are very limited numbers of PPs available for reference, the trend has shown that vendors are keen in participating towards the establishment of the world standard in putting the IT security requirements right. With appropriate support and right incentives from the governments and other sponsors, CC can be adopted fairly easily by all groups of recipients, as it is a set of tools made available by putting forth all possible inputs during its inception back in 1999.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[1], [5]
http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf
[2], [3]
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf
[4]
http://www.commoncriteria.org
[6]
Gene Troy
U.S. National Institute of Standards and Technology (NIST)
Introduction to the Common Criteria
http://niap.nist.gov/niap/archive/iccc/TrackA/troy/sld003.htm
[7]
http://csrc.nist.gov/cc/
[8]
http://www.commoncriteria.org/registry/mr.html
[9]
http://www.commoncriteria.org/epl/index.html
[10]
K. Ayer, VISA International, USA
Developing Protection Profiles - Getting Started
http://niap.nist.gov/niap/archive/iccc/kayer-nj.html#top
[11]
http://www.iccconference.com/agenda/tracks.asp

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.