University of Pittsburgh
School of Information Science

IS2820/TEL2813 - Security Management

Lab assignment #3

Common Criteria Methodology for Information Technology Security Evaluation (CEM)

GSA: Saubhagya Joshi

I. Lab resources for this assignment

Environment:

PC running on the Windows 2000 operating system

Role:

Administrator (no password)

Facility:

Internet Access

II. Preliminary Questions

1. *What is the difference between Protection Profile (PP) and Security Target (ST)?*

   CC provides a common ground on which products may be evaluated. The PP and ST play major roles in determining the functional as well as assurance requirements. What purposes do PP an ST serve?

2. *How is the Evaluation Assurance Level (EAL) of a product determined*?

   Products may be evaluated for various levels of assurance depending upon the capability of the product. What are the factors that help determine the appropriate EAL level for which any product should be evaluated?

3. *What is the process of validating a product?*

   CC follows a rigorous methodology in validating a product called the CEM. How is the methodology used to ensure that the validation is correct and complete?

4. *How is the TOE Security Function (TSF) for a product evaluated?*

   The activities involved in validating a product comprises of evaluating whether or not the product satisfies the TSFs. What are the work units that are performed in this process?

III. Lab objective:

ADVISORY: Read the whole lab assignment before doing the tasks!!!

Part A: Evaluation of PP, ST and TOE

Task 1. Evaluate a given PP from [1].
(refer to Part IV, section A for evaluation guidelines)

Task 2. Evaluate a given ST from [2].
(refer to Part IV, section A for evaluation guidelines)

Task 3. Evaluate the TSF of Windows 2000 operating system using the ST given in [2].
(refer to Part IV, section B for TSF evaluation guidelines)

NOTE: Please read the Lab Questionnaire before you proceed !

Part B: Generation of ST

Task 1. Generate ST for the product: Cisco PIX 501 Firewall, given PP from [1].
(refer to CC documentation – also discussed in class)

IV. Technical details

A. General Evaluation Guidelines

Types of evaluation

1. **PP evaluation**
   The PP evaluation is carried out against the evaluation criteria for PPs contained in CC Part 3. The goal of such an evaluation is to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a statement of requirements for a TOE.

2. **ST evaluation**
   The evaluation of the ST for the TOE is carried out against the evaluation criteria for STs contained in Part 3. The goal of such an evaluation is twofold: first to demonstrate that the ST is complete, consistent, and technically sound and hence suitable for use as the basis for the corresponding TOE evaluation; second, in the case where an ST claims conformance to a PP, to demonstrate that the ST properly meets the requirements of the PP.

3. TOE evaluation

The TOE evaluation is carried out against the evaluation criteria contained in CC Part 3 using a substantially complete ST as the basis. A substantially complete ST reduces the risk of problems later on in the evaluation process and is where all sections have been completed to an extent acceptable by the evaluation scheme and for which no significant evaluation hurdles are foreseen. The result of a TOE evaluation is to demonstrate that the TOE meets the security requirements contained in the evaluated ST.

Evaluation Methodology

Evaluation methodology can be obtained from the CEM official version from [3].

Evaluation Verdicts

The CEM recognizes three mutually exclusive verdict states:

a) Conditions for a *pass* verdict are defined as an evaluator completion of the CC evaluator action element and determination that the requirements for the PP, ST or TOE under evaluation are met. The conditions for passing the element are defined as the constituent work units of the related CEM action.
b) Conditions for an *inconclusive* verdict are defined as an evaluator incompletion of one or more work units of the CEM action related to the CC evaluator action element.
c) Conditions for a *fail* verdict are defined as an evaluator completion of the CC evaluator action element and determination that the requirements for the PP, ST, or TOE under evaluation are not met.

All verdicts are initially inconclusive and remain so until either a pass or fail verdict is assigned. The overall verdict is pass if and only if all the constituent verdicts are also pass. If the verdict for one evaluator action element is fail then the verdicts for the corresponding assurance component, assurance class, and overall verdict are also fail.

Evaluation Example

The following example provides three TOEs, all of which are based upon the same virtual private networking (VPN) firewall product, but which yield different evaluation results because of the differences in the STs.

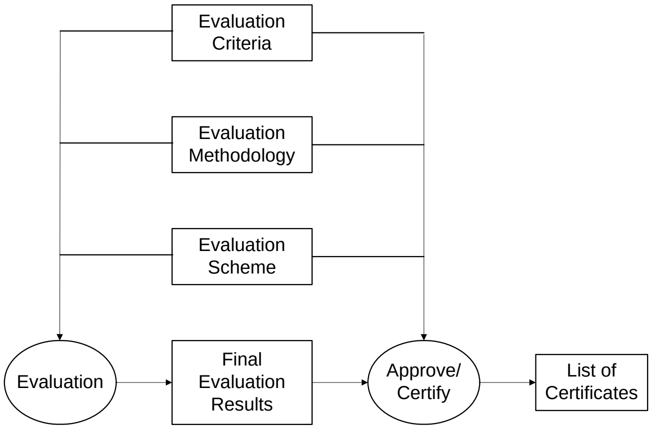

Figure 1: Evaluation Context

Case 1: A VPN-firewall, which is configured in such, a way that the VPN functionality is turned

off. All threats in the ST are concerned with access to the safe network from the unsafe network.
The TOE is the VPN-firewall configured in such a way that the VPN functionality is turned off. If the administrator were to configure the firewall such that some or all VPN functions were enabled, the product would not be in an evaluated configuration; it would therefore be considered to be unevaluated, and so nothing could be stated about its security.

Case 2: A VPN-firewall, where all threats in the ST are concerned with access to the safe network from the unsafe network.
The TOE is the entire VPN-firewall. The VPN functions are part of the TOE, so one of the things to be determined during the evaluation would be whether there are means to gain access to the safe network from the unsafe network through the VPN functions.

Case 3: A VPN-firewall, where all threats in the ST are concerned with either access to the safe network from the unsafe network or confidentiality of traffic on the unsafe network.
The TOE is the entire VPN-firewall. The VPN functions are part of the TOE, so one of the things to be determined during the evaluation would be whether the VPN functions permit the realization of any of the threats described in the ST.

CC / CEM Relationship
CC validation is based on the evaluation criteria, the evaluation method as well as the evaluation scheme as shown in Figure 1. There is a distinct mapping between the CC specifications with the activities in the CEM as shown in Figure 2.
Different parties involved in the CC validation may use the mapping in order to cross-validate correctness and completeness of the validation and the validation methodology.

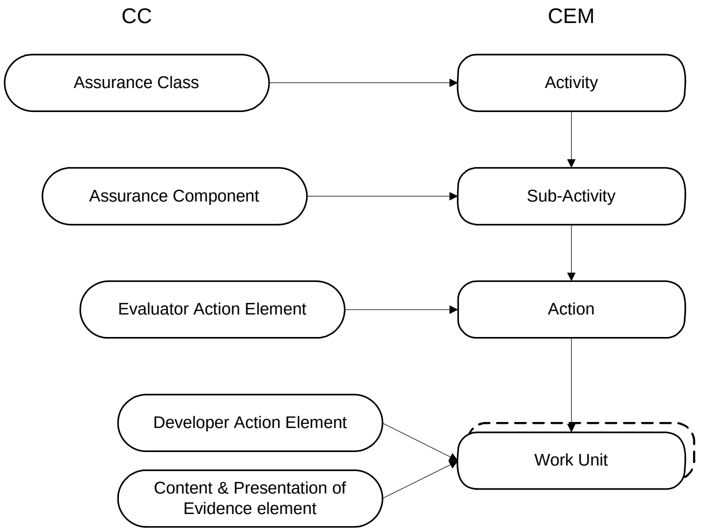

Figure 2: Mapping of CC and CEM structures

B. Evaluation of Functional requirements of TOE

Functional Requirements to be Validated

1. Audit Function

The Audit Function in the Microsoft Windows 2000 Server serves as a TSF function to perform the following basic functions:

a. Audit collection
b. Audit review
c. Audit log overflow protection
d. Audit log restricted access protection

By default, at installation, only application logs and error logs are collected and stored by the Audit function. The server administrator must enable security auditing on the machine.

Audit Collection

Every machine has one security log. The Event Logger service creates the security event log, which contains the security relevant audit records collected on a system.

Audit log Review

The administrator is able to view all the security log records using an event viewer administrator tool and differentiate security logs from application and system logs.

Audit log overflow protection

Failure to log requested events may have severe implications on the server. It is important that log records are always successful. Therefore there needs to be some mechanism that will alert the administrator before the logged records reach full capacity.

Audit log restricted access protection

Audit log viewer is restricted.

2. Security Management Function

Security Management is performed using several security management functions as well as roles.

Roles

Each user is classified in to one or many user role groups. Roles can be basically distinguished into two states: authorized administrator role and authorized user role. Administrators are those users that have the right to take ownership privilege.

Security Management Functions

The TOE supports several features that enable appropriate management. The majority of security management functions are restricted to the authorized administrator only.

The security functions available are: audit policy, account policy, account database, user rights policy, domain policy, group policy, IP Security policy, Encrypted File System (EFS) Policy and Disk Quota.

3. Resource Utilization Function

Disk space resources in the computer's storage devices may be controlled using a disk-space quota management tool. By default this control is disabled. Users with the administrative rights can enable quota management.

4. User Data Protection Function

Data Protection for the user is provided through cryptographic and access control methods. The Controlled Access PP (CAPP) requires that the cryptographic support be in the form of FIPS compliant encrypting/decrypting algorithms. The access control has to be Discretionary Access Control.

5. Cryptographic Support

Microsoft Windows 2000 provides an option to use FIPS compliant algorithms for encryption/decryption. This can be enabled to comply with the requirement.

6. Identification and Authentication Functions

Identification and authentication are very important security functions. The requirements put forward are of the following categories:

a. Authentication Failure Handling
b. User Attribute Definition
c. Verification of Secrets
d. User Authentication before any Action
e. Protected Authentication Feedback
f. User Identification before any Action
g. User Subject Binding

Authentication

Users that are trying to get authenticated should have a limited number of attempts. If these attempts exceed a pre-configured limit then the account they are trying to log into should be disabled. Windows allows the Administrator to set the number of attempts that a user can make to authenticate himself, after which the account can be disabled for some pre-defined time.

8. User Attributes

The user's security attributes should be stored along with user information. The significant user attribute are user identity, group memberships, authentication data, security-relevant roles, private keys, privileges and logon rights.

9. Protected Data Transfer

The Microsoft Windows systems use IPSec for protected data transfer between different parts of the system. IPSec settings can be fixed in the Policy editors.

10. Session Locking Functions

Session Locking Functions fulfill protected session access and management functions. The functions that the exercises will cover are:

a. Session Locking
b. Access Banners
c. Session Establishment

Session Locking

Session locking can be user-initiated or even done automatically after some duration of idleness. To unlock, the user authenticates himself with his username and password

Session Establishment

The session ticket expires and automatically the session is closed after certain duration of idleness.

Validation Action Guidelines

Evaluation is carried out by policy configurations of the system. Two methods can be used to validate all of the above functional requirements:

(i) registry editor using *regedit.exe* or *regedt32.exe* from the command prompt.
(ii) group policy editor using *gpedit.msc* from the command prompt.

(Resources available in the Internet can provide how-to-guidelines for the above methods.)

V. Lab Questionnaire

(NOTE: please reply in separate sheet)

Question 1: Which users/ groups have access to audit logs?

Question 2: Why are audit policies disabled by default?

Question 3: What is the difference between security logs and system logs?

Question 4: What is the minimum size of the log allowed?

Question 5: Why is the default size very different from the minimum?

Question 6: What size would you choose as the maximum?

Question 7: Which other user can access the even viewer?

Question 8: Why is the audit view limited to specific users only?

Question 9: Does the local policies cover security management functions for administrators also?

Question 10: Can different security functions be created for each user?

Question 11: Which of the above mentioned security management functions can be performed by user other than the administrator group?

Question 12: Can the user data be situated at a remote machine in a trusted domain within the network?

Question 13: How does the group policy relate to local policy?

Question 14: Why are policies for administrator in user-configuration and computer-configuration different?

Question 15: Which other user other than from the administrator group enable or disable quota management?

Question 16: Is the quota limit applicable to all the users? Is there any user that is not limited by the quota management?

Question 17: What encryption function is used by operating system?

Question 18: Does it provide any information about what the password could be? Or whether even the username was correct?

Question 19: How are all the security-relevant information captured in the displayed information?

Question 20: Can anyone else unlock the computer apart from the user who locked it?

Question 21: What is the difference between the User Ticket and Service Ticket?

Question 22: Do you think it is more important to have a service Ticket timeout than a User Ticket timeout?

VI. Lab report

The lab report for this laboratory should include the following:

1. Evaluation reports for PP, ST and TOE.
2. ST for Cisco PIX 501 (basic framework).
3. Answers to the Lab Questionnaire.

VII. References:

1. http://niap.nist.gov/cc-scheme/pp/PP_ALFWPP-LR_V1.0.html
2. http://niap.nist.gov/cc-scheme/st/ST_VID4002-ST.pdf
3. http://www.commoncriteriaportal.org/public/files/cemv2.3.pdf
4. Other Resources:
    - http://niap.nist.gov
    - http://msdn.microsoft.com
    - http://www.cisco.com