Name:

Information Assurance: Homework 7 – Answers

Due Nov 2, 2009

1. This question works with the list of products evaluated by the Common Criteria http://www.commoncriteriaportal.org/products.html. In particular, you will be looking at products "**Cisco ASA 5505, 5510, 5520, 5540, and 5550 (Release 7.2(4)), Cisco VPN Client Release 5.0.03.0560**" and "**IBM AIX 5L for POWER V5.3, Technology level 5300-05-02 with Argus Systems Group PitBull Foundation Suite 5.0 and optional IBM Virtual IO Server (VIOS) Version 1.3"**. For each of these products answer questions a – h.

(40 points – 2 points per section)

For Cisco ASA

a. Does the security target follow a protection profile (PP)? If so, what PP?

No

b. If it follows a PP, does it specify any additional security functional requirements? If so, list one of the additional requirements.

N/A

c. If it does not follow a PP, list two of the security functional requirements from the security target.

Security function requirements are itemized in section "TOE security funciton requrements" on page 18 of the security target. Two of these requrements are:

- *FAU_GEN.1 – Audit data generation*
- *FCS_CKM.1(1) – Cryptographic key generation. RSA*

d. What EAL was the product was certified at?

EAL4+

e. Where there any extensions to a standard EAL? If so what?

ALC_FLR.1 – basic flaw remediation

f. What EAL was the PP (if any) certified at?

Name:

N/A

g. Which country was the product certified in?

This is described in the certification report. This evaluation was done in the United States.

h. Which company (or companies) performed the evaluation?

SAIC performed the evaluation.

For IBM AIX

a. Does the security target follow a protection profile (PP)? If so, what PP?

LSPP

b. If it follows a PP, does it specify any additional security functional requirements? If so, list one of the additional requirements.

Table 2 of the security target identifies the origin of all security functional requirements. Here are two that did not come from the protection profile:

- *FDP.ACC.1(1)*
- *FDP.ACF.1(2)*

c. If it does not follow a PP, list two of the security functional requirements from the security target.

N/A

d. What EAL was the product was certified at?

EAL 4+

e. Where there any extensions to a standard EAL? If so what?

ALC_FLR.1 – basic flaw remediation

f. What EAL was the PP (if any) certified at?

EAL3. Identified in the LSPP write up.

g. Which country was the product certified in?

Identified in the certification report. It was evaluated under the German interpretation of the Common Criteria.

h. Which company (or companies) performed the evaluation?

It is a bit unclear to me which is the German office in charge of verifying the evaluation and which is the lab that performed the actual evaluation. I'm guessing that the evaluating lab is "Bundesamt für Sicherheit in der Informationstechnik".

Answer the following question in general.

i. What is the highest level certification you see in the list? What is a product rated at that level?

Tenix Interactive Link Data Diode Device, Gigabit Variant, Version 3.0

Has an EAL7+. Tenix also has another product that is only EAL7.

j. Would all the product certifications you examined in parts a-h be acceptable to the US Government?

Yes. The ASA product is evaluated under the US interpretation. Germany is also a member of the common criteria, so products evaluated under their interpretation must also be acceptable to the US government.

Name:

2. Consider the following system design sketch. Identify and describe at least one one of Saltzer and Schroeder's design principles that is represented by this design and at least one principle that the design does not exemplify.

(20 points, 10 for each required principle)

The DesignVault 2100 is a high assurance design document repository. It is designed to run on Windows 7 platforms. It has passed an EAL2 common criteria certification.

The DesignVault allows roles to be associated with users. The roles include reader, editor, and administrator. On system login, the user selects one of the roles assigned to him. He operates within the restrictions of that role for the remainder of the session.

When authenticating, the DesignVault verifies the user's AD credentials. In addition, it asks the user to solve a numbered sudoku puzzle. The puzzle book should have been distributed to the user when they were entered into the system. The user must enter all the cells of the solved puzzle in row major order to be fully authenticated with the system.

On every data request, the DesignVault rechecks the user's credentials and rights before acting on the request. Though encryption, the DesignVault ensures that its controls cannot be bypassed to access the design documents meaningfully directly in the data store.

Principles Exemplified:
Least Privilege – Role separation means that a holder of many roles is not running with unnecessary privilege while acting in one role.
Complete Mediation – credentials are checked on every data request
Least Common Mechanism – encrypting the data store means that other processes sharing the system cannot access the data in the shared file system.

Principles not exemplified:
Psychological Acceptability – Requiring the solution to a sudoku puzzle on authentication will not be acceptable to most users and slow down real users too much.
Economy of mechanism – The sudoku puzzle authentication could also be argued to fail the economy of mechanism principle.

Name:

3. In a traditional Unix system, the root user has the ultimate privilege. The standard security rules do not apply to the processes running as root. Windows and trusted Unix/Linux provide finer grained privileges.

(20 points: 6 points per section, 2 points for free)

There was a fair amount of confusion on this question between privilege and access rights. Paul McNabb discussed least privilege systems during his guest lecture. As identified in the news group, privileges are the identification of how a process can violate parts of the normal security model, e.g. A privilege to ignore write DAC. Access rights are how normal programs are constrained when accessing objects.

a. Propose a set of privileges for a Unix system that should be sufficient to operate a system backup program.

Ignore Read Discretionary access control (DAC). The backup program needs to read all files to copy them. It only needs to write files in a special backup area, so we can rely on regular write DAC to give access to the backup files.

We could use read DAC to explicitly give the backup process read access to all files. This is cumbersome. It is easy to forget to add that access, and with the Unix three octet DAC it may not be expressible. In general relying on a privilege that allows the back up process to run out side the security policy with respect to read DAC is an easier, more reliable way to go.

b. Propose a set of privileges for a Unix system that should be sufficient for the password updating program.

The password program is normally dealt with by running the program as another user (Set-UID). The user is "root". So normal user, Bob, invokes passwd. Passwd runs as "root". It takes Bobs password information and updates Bob's entry in the password file.

If we have a set-uid system to invoke processes running as other users, we don't need any other special privilege. The password program runs as user X. User X is the only one that has write privilege on the password file.

One could argue that the ability to invoke a process as another user is outside the normal security model and is a special privilege.

c. What are the security benefits of associating finer grained privileges with system programs?

Name:

If a process runs with unnecessary privilege, the process may cause damage if it is subverted by malicious code. Or if the process attempts to perform an action accidentally it may cause unnecessary damage on the system.

For example, consider the back up process. It really only needs the privilege to ignore read DAC. If the back up process runs as root with no security checks made, that process could be made to replace system binaries or erase key files.

4. Consider different sources of system assurance. Identify one source of assurance that would satisfy each of the following common criteria EALs.

(20 points, 6 points per section plus two free)

Looking for assurance elements that are required that the specified level but not specified at the next lower level. This is discussed in Section 21.8.5 of the text book. Also discussed in assurance document on the common criteria web site.

A number of people tried to map Policy, design, and operational assurance to the different levels. Each EAL will require different levels of all types of assurance.

a. EAL1

Independent testing.

Analysis of security functions using functional and interface specifications.

b. EAL4

Provide documentation of the low level design.

A complete interface description.

An informal model of the product or system security policy.

Automated configuration management.

c. EAL7

Formal presentation of the functional specification and a high-level design.

The product or system design must be simple.

Independent confirmation of the developer test results must be complete.

Name: