Name:

Information Assurance: Homework 7

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.
    a. Does the security target follow a protection profile (PP)? If so, what PP?
    b. If it follows a PP, does it specify any additional security functional requirements? If so, list one of the additional requirements.
    c. If it does not follow a PP, list two of the security functional requirements from the security target.
    d. What EAL was the product was certified at?
    e. Where there any extensions to a standard EAL? If so what?
    f. What EAL was the PP (if any) certified at?
    g. Which country was the product certified in?
    h. Which company (or companies) performed the evaluation?

    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?
    j. Would all the product certifications you examined in parts a-h 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.

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.

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.

a. Propose a set of privileges for a Unix system that should be sufficient to operate a system backup program.
b. Propose a set of privileges for a Unix system that should be sufficient for the password updating program.
c. What are the security benefits of associating finer grained privileges with system programs?

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

a. EAL1
b. EAL4
c. EAL7