CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 6

Names of team members: Ross Doherty, Kevin Bush, Hasan Mohammad, Jared Borah

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don't just assign different problems each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1

Review Figure 6-1 from your text and explain the following terms:

- **subjects and object (in access control, not attack) → Access control models have a subject and an object. The subject - the human user - is the one trying to gain access to the object - usually the software. In computer systems, an access control list contains a list of permissions and the users to whom these permissions apply. Such data can be viewed by certain people and not by other people and is controlled by access control. This allows an administrator to secure information and set privileges as to what information can be accessed, who can access it and at what time it can be accessed.**

- **discretionary access control → An access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.**

- **non-discretionary access control → Access controls that are implemented by a central authority. A form of non-discretionary access controls is called lattice-based access control (LBAC), in which users are assigned a matrix of authorizations for particular areas of access.**

- **lattice-based access control → A variation on the MAC form of access control, which assigns users a matrix of authorizations for particular areas of access, incorporating the information assets of subjects such as users and objects.**

- **mandatory access control → A required, structured data classification scheme that rates each collection of information as well as each user. These ratings are often referred to as sensitivity or classification levels.**

- **role-based access control → An example of a nondiscretionary control where privileges are tied to the role a user performs in an organization, and are inherited when a user is assigned to that role. Roles are considered more persistent than tasks. RBAC is an example of an LDAC.**

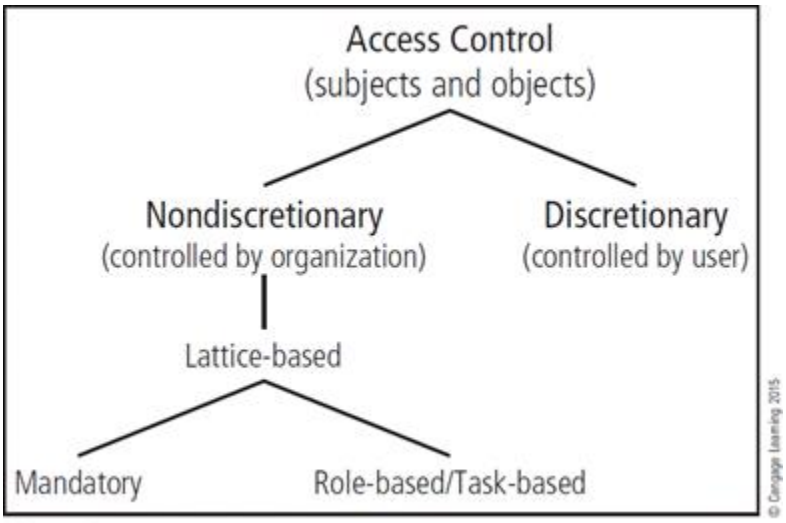

Figure 6-1 Access control approaches

(15 pts.)

Problem 2

What is stateful inspection? How is state information maintained during a network connection or transaction? What is the primary drawback to the use of this approach? (5 pts.)

Stateful inspection is a firewall type that keeps track of each network connection between internal and external systems using a state table and that expedites the filtering of those communications. Also known as a stateful inspection firewall. State information is maintained in a state table which contains the familiar IP and port source and destination The primary drawback to this approach is additional processing is needed in order to manage and verify packets. If additional processing is not used in stateful inspection, the system is going to suffer from DOS or DDOS attacks.

Problem 3
How does a network-based IDPS differ from a host-based IDPS? Which has the ability to analyze encrypted packets? (5 pts.)

A network based IDPS (NIDPS) resides on a network segment and monitors activities across that segment. They can be deployed into a network with little or no disruption. They are not usually susceptible to direct attack.
A host based IDPS (HIDPS) resides on a particular server, known as a host, and monitors activity only on that system. They can detect local events on the host system and detect attacks that NIDPS may have missed. The HIDPS works on only one computer system, all the traffic it examines traverses that system.
A HIDPS has the ability to analyze encrypted packets.