CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 6

Names of team members: Volodymyr Bestiyanets, Nick Cunningham, Timothy Mahan, and Shawn Nasr.

Logistics

A. Get into your regular team
B. Discuss and complete the assignment together. Don't just assign different problems to 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:

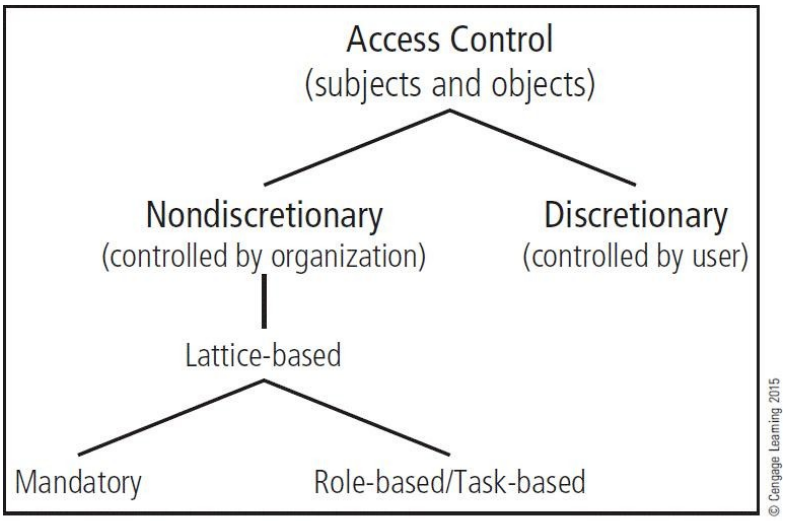

Figure 6-1 Access control approaches

- subjects and object (in access control, not attack)
- discretionary and non-discretionary access control
- lattice-based access control
- mandatory access control
- role-based access control

(15 pts.)

Subject of access control: User or system.
Object of access control: A resource.
Discretionary access control: Access controls that are implemented at the discretion or option of the data user.
Non-discretionary access control: Access controls that are implemented by a central authority.
Lattice-based access control: A variation on the MAC form of access controls, that assigns users a matrix of authorizations for areas of access, incorporating the information assets of subjects such as users and objects.
Mandatory access control: A required, structure data classification scheme that rates each collection of information as well and each user as well that are referred to as sensitivity or classification levels.
Role-based access control: A type of non-discretionary control that has privileges connected to the role a user performs in an organization, and are inherited when a user is assigned to that role. Roles are more persistent that tasks.

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.)

A stateful inspection is a firewall type that keeps track of each network connection between internal and external systems using a state table. The state table makes the filtering of those communications quicker by tracking the state and context of each packet in the conversation by recording which station sent what pack and when it was sent. The disadvantage to this firewall is the additional processing required to manage and verify packets against the state table.

Problem 3

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

Network-based IDPS is placed on the network segment where it can monitor all network traffic. Host-based IDPS are placed on each individual endpoint, typically in the form of a sensor that monitors file changes and makes decisions by comparing the changes to a baseline. The host-based IDPS can analyze encrypted packets as the packets are decrypted upon arriving at the host. Network-based IDPS cannot analyze encrypted packets at all without breaking the encryption.