CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #6

Team: Seven
Participants: Jackson Dillingham, Matt Jackson, Hilton Siaffa, Tabor Payne, and Emily Wantland

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

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

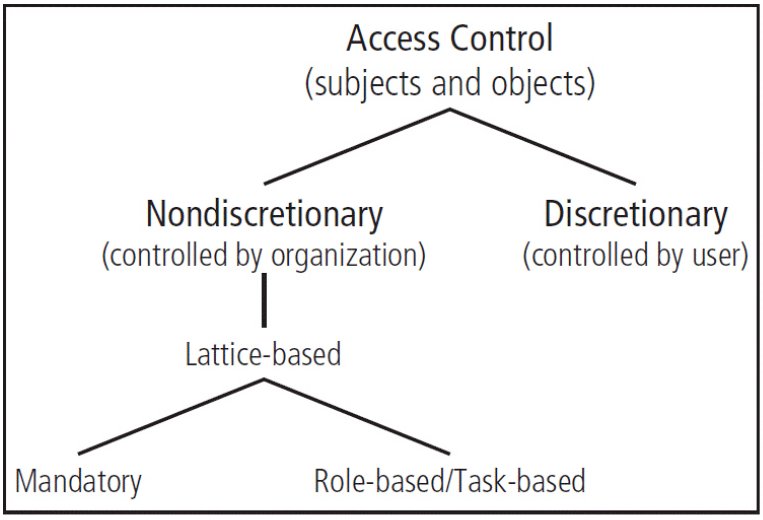

Figure 6-1 Access control approaches

- 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 points)

- Subjects (Access control) - A user or a system. In the domain of access controls, a subject may be granted permissions or privileges to access an object (resource). The access may include rules controlling if, where, when, and how the resource may be use by a subject.
- Objects (Access control) – A resource of interest. In terms of access control this would refer to the resource that an organization is interested in controlling; a trusted area.
- 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 Controls - A variation on the MAC form of access control, which assigns users a matrix or authorizations for particular areas of access, incorporating the information assets of subjects such as users and objects.

- Mandatory Access Control - A required, stricter 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 no discretionary 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.

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 points)*

- Stateful inspection is the process of monitoring and assessing all active connections present and based on which information the connection which has the ability to be allowed through the firewall is decided as well.
- This is a type of firewall technology that is dynamic and has the ability to maintain state information by recording the details of the session like the port number and IP address and analyzes the application layer as well, both the incoming and outgoing packets in this context are tracked over a particular time period that helps maintaining the information during the network connection or transaction as well.
- The primary drawback to the use of this approach is that it requires additional processing required to manage and verify packets against the state table. Without this processing, the system is vulnerable to a DOS or DDoS attack. An attack like this would slow down the firewall.

Problem 3

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

- The difference between Network based IDPs and Host Based IPDS is that network based IDPS is a standalone hardware system that has capabilities of detection the intrusion in real time, it can be implemented at a low price, it requires less administration training, it is not versatile and the traffic from individual computer cannot be monitored while Host Based IPDS is very costly, does not offer true real time detection, requires comparatively more administration and training and it can be helpful in monitoring the to and from traffic from a specific computer.
- A host-based IDPS has the ability to analyze encrypted packets because of its ability to use the content of otherwise encrypted communications to make decisions about possible or successful attacks.