CIS-481: Introduction to Information Security

In-Class Exercise #6

IQ Team: 4
Names of team members: Daniel Kearl, Mohammed Al Madhi, Yuxuan Chen, Joseph Baxter

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 **IQ Team**.

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

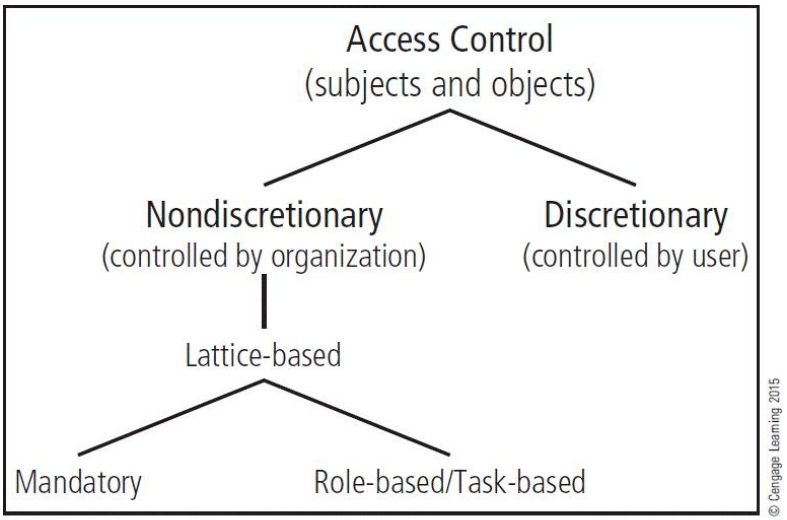

Figure 6-1 Access control approaches

- 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)

Access control subjects are systems or users that have controls applied to them to appropriately control their access to objects. These objects are protected by access controls. For example, access controls are placed on users accessing a file share so that only administrators can access backup objects.

Discretionary access controls are more flexible controls that are set by the user of the data which is accessed. An example of this is sharing a document with someone on google drive. In contrast, nondiscretionary access controls are implemented centrally, and are typically much more rigid. A good example of these would be access privileges to a network drive, set by an administrator.

Mandatory access control is a system that rates data and users on different levels, where users with a certain level of access can only interact with data on that level or below, but no higher.

These ratings are typically referred to sensitivity or classification levels, and we can look toward the widely known levels of classification used by the U.S. Government: Top Secret, then Secret, Classified, and so on down.

Lattice-based access control is similar to mandatory access control, but instead of working with levels of classification, this access control method labels data and users with different "areas" of access, with the idea that users only have access to data that falls into one of their areas. This is similar to a "need-to-know" basis of access control.

Role-based access control operates on the idea that a person in an organization has specific roles, and people with such a role require access to certain data, but nobody else. For example, a CPA at a firm may have an "Accountancy" role on a file server, allowing them necessary access to financial information that they would need to fulfill their role within the organization. This method of access control is nondiscretionary and more permanent than the similar method of task-based control.

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 a main feature of a type of firewall that keeps track of network connections between systems using a state table, then uses the characteristics of a packet (connection source and destination, etc.) to determine whether it should be filtered. State tables carry information about packets (for a certain amount of time – typically up to 60 minutes) that can also allow further incoming packets to be expedited to the source. If a packet cannot be matched to one existing in the state table, the firewall uses its access control list as a fallback to refer to.

The primary downside to this approach is the processing overhead that takes place when under load. A normal firewall simply checks against static rules and lets a packet pass or not; a stateful inspection firewall must consider the entire context of a packet before deciding to hold or send it, which requires more processing power.

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

A network-based IDPS focuses on network activity, while a host-based IDPS resides on one machine and focuses its monitoring on that host. They both have their advantages and disadvantages, but one very notable downside of a network-based IDPS is that it cannot analyze encrypted packets, because either end of the "transaction" has a key that can decrypt said packet, and the IDPS does not. This means a host based IDPS must be relied upon to catch changes made by potentially malicious encrypted packets.