CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #6

Team: 5
Participants: Ethan Grimes, Holli Grubbs, Gregory Ellis, James Hoagland

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 *(15 points)*
Review Figure 6-1 from your text and explain the following terms:

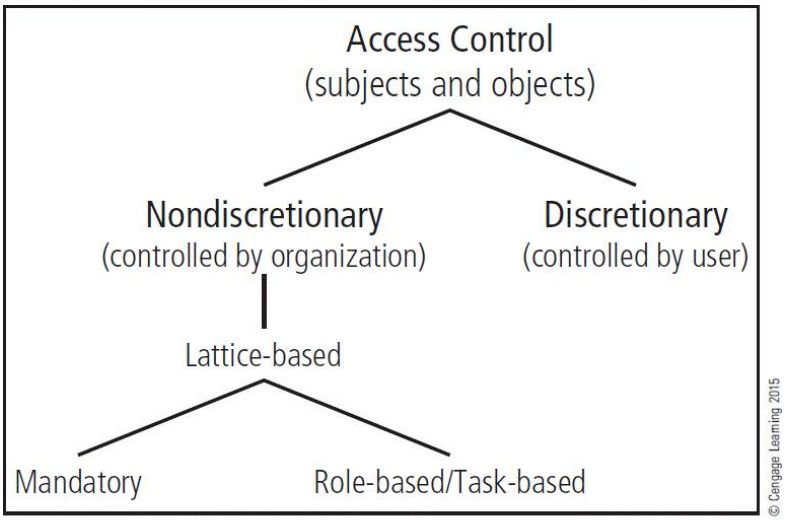

Figure 6-1 Access control approaches

- 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

Subjects and Objects (Access Control)- the subject of access control is the user or system and the object is the resource. An access control is the selective method by which systems specify who may use a particular resource and how they may use it.

Discretionary Access Control- access controls that are implemented at the discretion or option of the data user.

Nondiscretionary Access Control- access control that is implemented by a central authority.

Lattice-based Access Control- a form of nondiscretionary access control that users are assigned a matrix of authorizations for particular areas of access.

Mandatory Access Control- a required, structured data classification scheme that rates each collection of information as well as each other.

Role-based Access Control- a form of lattice-based access control associated with the duties a user performs in an organization.

Problem 2 *(5 points)*
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?

A stateful packet inspection (SPI), is a firewall type whose purpose is to keep track of every network connection between internal and external systems. It does this by using a state table that accelerates the filtering of those communications. It's also referred to as a stateful inspection firewall.

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

Network-based IDPS is an IDPS that resides on a computer or appliance connected to a segment of an organization's network and monitors traffic on that segment; they check for indications of attacks. Host-based IDPS is an IDPS that resides on a certain computer or server, known as the host, and monitors activity only on that system. The main difference between the Network-based and host-based is that the ladder monitors activity on 1 computer/server unlike the former which monitors activity across an entire network. Another difference is that a Host-based IDPS can analyze and access encrypted packets when traveling through the network. A Network-based IDPS is not able to analyze encrypted packets. With a Host-based IDPS being able to analyze encrypted packets this gives them the necessary data to make decisions on potential attacks.