**CIS-481: Introduction to Information Security**

**In-Class Exercise #6**

**IQ Team: IQ Team 3**

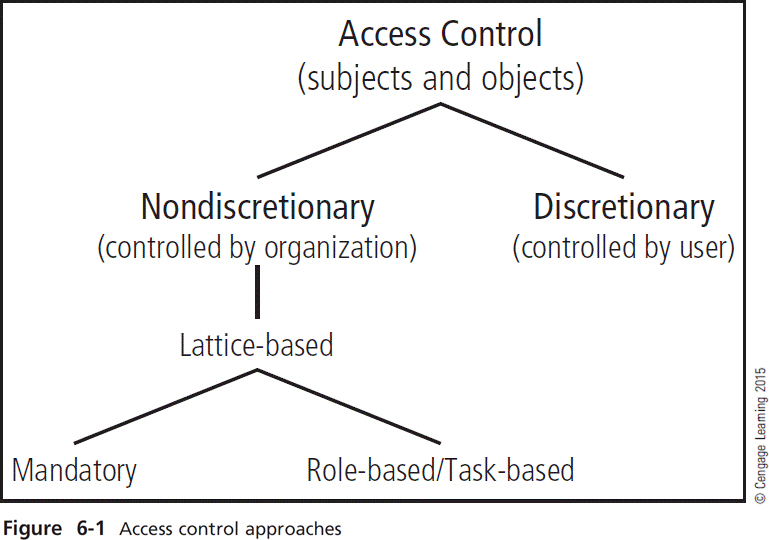
**Names of team members: Trevor Rawleigh, Samantha Conway, Noah Smith, Elise Timmons**

**Logistics**

1. Get together with other students on your assigned team in person and virtually.
2. 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.
3. 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:

* 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)*

**Answer 1**

Access Control – Access Controls are methods by which systems determine whether a system should admit and how to admit a subject, also known as a user, into a trusted area of an organization. This includes access to resources or specific areas of data known as objects. The main focus is on every question to do with the data and user relationship: who has access to what, how can the user access, where can they access, and when can anything be accessed.

Discretionary - DACs allow users to control and possibly provide access to information/resources at their disposal. This can be on a peer-to-peer configuration that allows a coworker to share non-sensitive information with other same level coworkers. Can use share control functions for this.

Nondiscretionary – Nondiscretionary controls are strictly-enforced version of MACs that are managed by a central authority. This means that nothing should go past central authority. This includes lattice-based access.

Lattice-based – This is where the matrix of authorization is assigned to the users for the specific access areas. This control specifies the level of access that each subject has to an object.

Role-based/Task-based - Role-based controls refer to when a user performs their duties in the organization. Like if a manager fills up a confidential document. A task-based control provides more detailed control over the particular task restrictions. It is considered to be a sub-role access control.

Mandatory – Mandatory controls use data classification schemes. Limited access and resources are provided to the users and data owners. In the data classification schemes, all the data/information is rated, therefore all the users are rated to specify the data they will have access to. Often these ratings are referred to as a sensitive level, which specifies the confidentiality levels.

**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)*

**Answer 2**

Stateful Inspection is a subnet of packet filtering firewalls. Packet-filtering firewalls can be broken down into three subnets. These are static packet filtering, dynamic packet filtering, and stateful packet inspection. Stateful Inspection is used to monitor current active connections. These network connections can be tracked between internal and external systems.

State information is maintained during a network connection in a state table that tracks sources, destination IP addresses, information on protocols, connections from said info to ports, TCP/UDP, and time. TCP/UDP connections/streams are allowed entry as long as they are defined in the security policy. Any packets that do not match the defined state tables are denied entry.

The primary drawback for this approach is that additional processing is required to manage verifying packets, for processing power, and the systems are actually vulnerable to attacks such as DoS or DDoS. A large attack of multiple packets could weaken the state table and therefore let other packets in if the hardware is not strong enough. It may not be as cost efficient to put in such strong hardware and therefore state tables are at a disadvantage.

**Problem 3**

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

**Answer 3**

A network based IDPS is used to monitor any activity that is on a network. This includes looking for any odd behaviors or changing patterns within a networks traffic. While a host based IDPS is used to monitor activity that is on a server. Both of these IDPS types are used for intrusion detection, data collection, help to restore normal operations within a network/server/host. Once an anomaly is found, the IDPS activates an alarm. All IDPSs cannot compensate for a weak security infrastructure and poor software management practices. If your system is weak, they can alarm you to the upcoming threat, but they cannot stop a threat. A host based IDPS is at an advantage because it can analyze encrypted packets which may result in the prevention of an upcoming attack.