# CIS-481: Introduction to Information Security

## InfoSec Chapter Exercise #6

**Team:**
**Participants:**

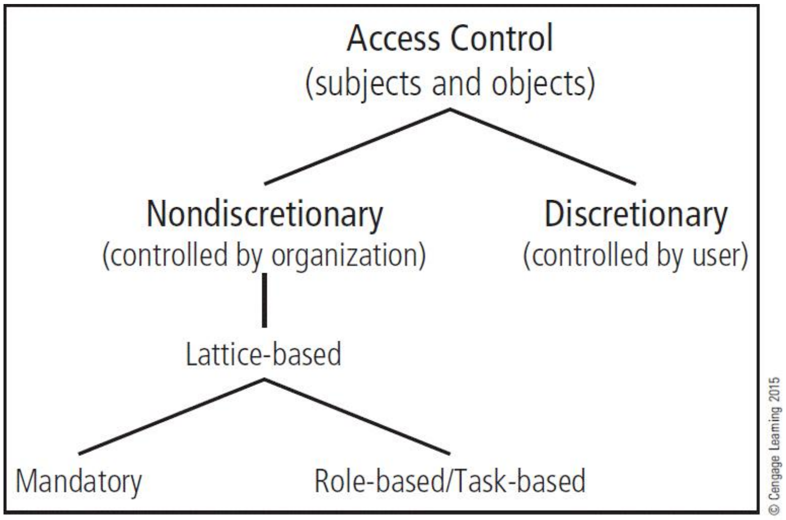
### Logistics

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:

- 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



© Cengage Learning 2015

**Figure 6-1** Access control approaches

*(15 points)*

**Subjects in access control are the user or system. An object in access control is a resource. The subject has permissions or privileges on an object.**

**Discretionary access control provides the ability to share resources in a peer-to-peer environment that allows users to control and even provide access to the information and objects at their disposal. Non-discretionary access controls are managed by the central authority of the organization to implement access controls.**

**Lattice-based access controls are a form of non-discretionary access control that assign users into a matrix of authorizations to grant areas of access. They specify the level of access each subject has to each object.**

**Mandatory access controls are a form of lattice based, nondiscretionary access control that give users and data owners limited control to access information resources.**

**Role based access controls are nondiscretionary controls that are granted based on the duties a user performs in an organization. This makes it easier for each job to have the access level they need to work effectively.**

**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 type of packet inspection that tracks each network connection between internal and external systems using a table. The table is used to easily filter the connections. State information is maintained in the state table. The state table records which station sent what packet and at what time. They also filter packet information by expediting incoming packets responding to internal requests.**

**The main disadvantage of state inspection is the additional processing power needed. Since the state table compares and filters the packets as they come in, the system could easily get overwhelmed if there isn't enough processing power. That leaves it open to denial of service attacks who would take advantage of the thorough filtering.**

**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 differs from a host based IDPS in the type of information assets they protect. A network based IDPS focuses on protecting network information assets and does so by examining network communications traffic. A host based IDPS protests the server's information assets and does so by monitoring the files stored on the system, and even the actions of the users. A network based IDPS can detect more types of attacks than a host based, but it has a more complex configuration and maintenance program. However, a network based IDPS cannot analyze encrypted packets while a host based IDPS can. That allows the host based IDPS to make decisions about possible or actual attacks.**