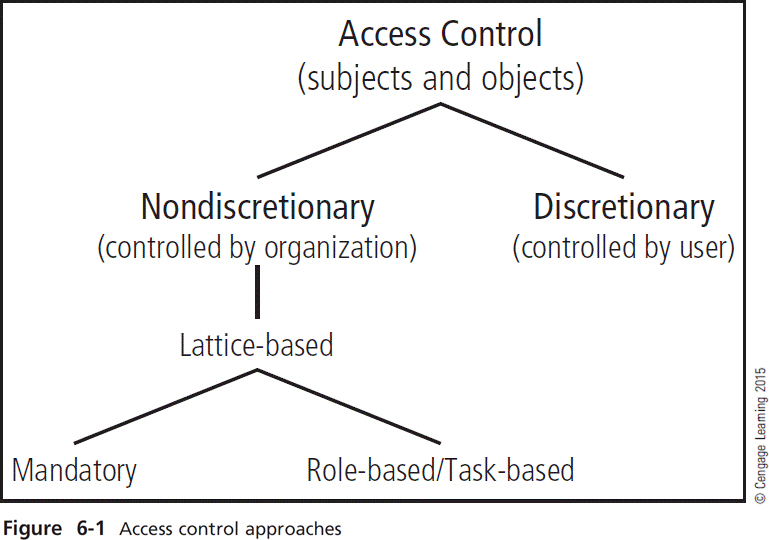
**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 6-7**

Grading ID: A7386

**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 pts.)

Subject – A user/group/organization/system that has sent an access request to a system.

Object – Something that a user is requesting access to.

Discretionary access control – The owner of an object explicitly decides who is allowed access to an object as well as what privileges that they have.

Non-Discretionary access control – Access to an object and user permissions on that object are determined by a user’s role in the system.

Lattice-based access control – a mathematical lattice model is used to determine the level of security that is placed on an object. A user may only access this object if his security level is higher than that of the object.

Mandatory access control – a user may only access an object if an explicit rule exists that allows that user to do so.

Role-based access control – Access to an object and user permissions on that object are determined by a user’s role in the system. These policies are determined by the system, not the owner of the object.

**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 pts.)

Stateful inspection is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. Stateful inspection firewalls keep track of each network connection between internal and external systems using a state table. The primary drawback to the use of this approach is that vulnerabilities in individual protocols used by the firewall could be exploited, allowing a hacker to gain control of the entire firewall.

**Problem 3**

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

A network-based IDPS is focused on protecting network information assets. Often times, these are used to examine traffic flow on a network and identify abnormal patterns. A host-based IDPS resides on a particular server/computer and only monitors activity on that system. However, these have the advantage of being able to analyze encrypted data packets.