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

**InfoSec Chapter Exercise #6**

**Team: Project Team 11**

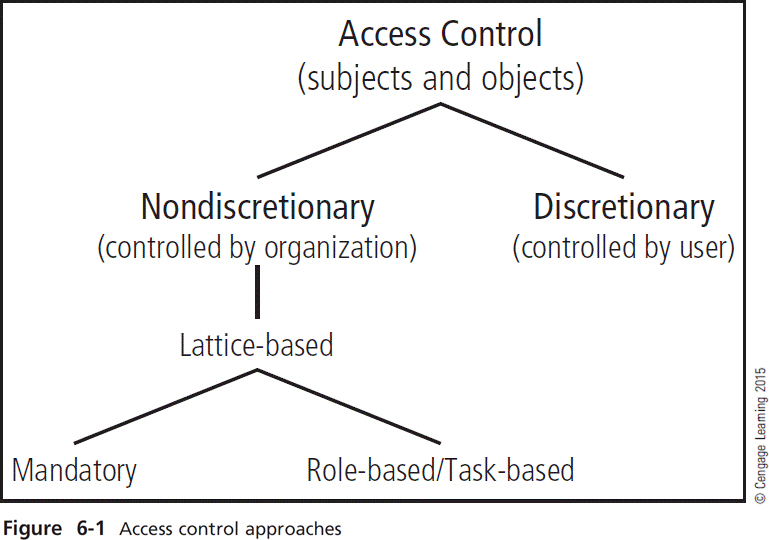
**Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson**

**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 **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)*

**subjects and object (in access control, not attack)**

**⦁ discretionary and non-discretionary access control:**

1. **Discretionary Access Control: -** It is referred to be as a sort of security get to control that awards or confines object get to by means of an entrance strategy controlled by an article's proprietor gathering as well as subjects. Permits clients to control and conceivably give access to data/assets available to them
2. **Non-Discretionary Access Control:** It could be referred as the general structure regulator (or a solitary administration body) inside an affiliation solidly controls access to all advantages for everybody on a framework. Carefully upheld rendition of that are overseen by a focal power.

**⦁ lattice-based access control:** The security in a lattice-based model is divided into various security levels, basically it relates as a whole, combination of objects being stated in level such that to per-use to various data security access controls.

**⦁ mandatory access control:** It alludes that kind of access control by using that working framework which obliges the capacity of a security subject and the initiator to getting the most part play out a type of activity of anything to be pursued that leads to an opportunity for a better security model. Use information arrangement plans.

**⦁ role-based access control:** It refers to be as a strategy leading to a limiting system get too dependent on the jobs of individual clients inside an undertaking. Role Based Access Controls lets workers approach rights just to the data they have to carry out their responsibilities and keeps them from getting to data that doesn't relate to them.

**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 basically an approach which can provide improved ways to overlook the people accessing the sensitive network of an organization, it leads to efficiency by detecting each n every person accessing by their I.P addresses (Internet Protocol) it not only detects but provides the data security like a firewall. State information can be maintained using a network connection by accreditation of high security models for transactions would be (IPS) protection model and for better controls and network connections, accreditation of other models such as CMMC, ISO 27000 family and GDP. It monitors each system association among inside and outer frameworks utilizing a (state) table.

State information can be maintained by making modules and saving the information in tables whether if using only network connection or transactions/ all the things are included in a state information. The drawback of this approach is only that the data in the tables could be stolen and this immures to a devastating approach.

**Problem 3**

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

IDPS is abbreviated as an Intrusion Detection Prevention System – the main obligation of IDPS is to detect and protect the system from malware software.

* Network-Based IDPS: It has a network of computer or systems conjoined together to detect or prevent any malware from within the whole network of systems.
* Host-Based IDPS: Host is known to be a single computer. This type of IDPS is used to detect and prevent the malware from a single computer.

Network based intrusion detection prevention has an ability to check the encrypted (encoded) packets