# CIS-481: Introduction to Information Security

## Module 8 - Security Technology - Access Controls, Firewalls, VPNs

## Exercise #6

**Team: 5**
**Participants: Abril Beascoechea, Charles Degboe, Nicholas Zhang, Ricardo ,Sam Martin**

**Logistics**

A. Get together with other students on your assigned **Team** in person and/or 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 and may impact your performance on assessments, especially with respect to the essay questions.
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 8-1 from your text and explain the following terms:

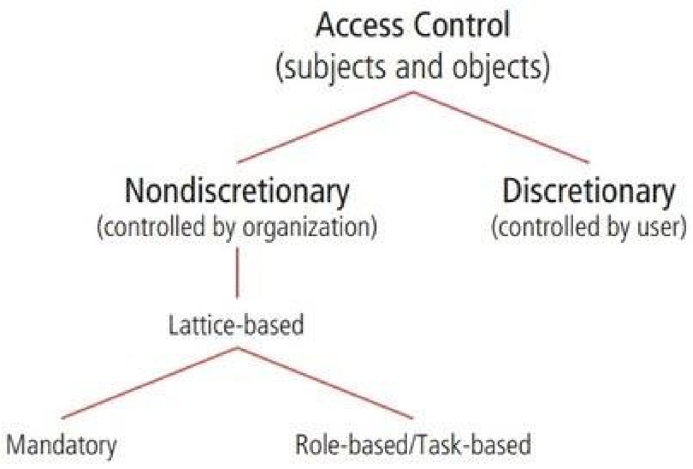

**Figure 8-1** Access control approaches

- 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
- attribute-based access control

-Subjects and object: the subject is the user or system, and the object is the resource that the subject is going to access.
-Discretionary and non-discretionary access control: discretionary access control gives the ability to share resources on a peer-to-peer configuration and non-discretionary access control is managed by a central authority in the organization.
-Lattice-based access control: its a form of non-discretionary access control, where users are assigned to a matrix of authorizations for particular areas of access.

-Mandatory access control: are a form of lattice-based access control that uses data classifications schemes.
-Role-based access control: is a non-discretionary control where privileges are tied to the role or the job a user performs in an organization.
-Attribute-based access: the organization specifies the use of objects based on some attribute of the user or system.

**Problem 2** *(10 points)*
The text provides a very brief introduction to *Zero Trust Architecture* (ZTA) on p. 308 but a recent survey by Microsoft reveals that ZTA is now their top security priority! Given this, a deeper dive into ZTA seems appropriate. CPO Magazine online recently published An Introduction to Zero Trust Architecture. Read the article and answer the following questions (*2 points each*).

a) What key insight about many cyber attacks motivated John Kindervag to formally introduce Zero Trust in 2009?

Kindervag introduced Zero trust after noticing that on most of the cyber attacks the point of entry was through a vulnerability in one area and then moved through the network until reaching the intended target, rather than entering through the target directly

b) How has the pandemic influenced the increase in popularity of Zero Trust?

The pandemic boosted interest in Zero Trust due to pandemic-driven migrations of applications to the cloud and staff accessing data from a wide variety of devices and locations—something traditional perimeter-centric security models can't handle.

c) Name and briefly describe the first planning step when building a Zero Trust Architecture in an organization.
Identifying the "protect surface," which consists of the most important information, resources, programs, and services, and comprehending how users interact with it are the initial steps in developing a zero trust architecture.

d) Does Single Sign-On (SSO) still have a place in a Zero Trust enterprise? Explain.
SSO definitely still has a place in a Zero Trust enterprise. SSO will allow all the employees to access different data and apps while only using a single set of credentials. This is important in the workplace as if you have to constantly log in to different sources, a MFA will slow you down and may lead to you being less productive. SSO still enforces security by preventing credential sharing and enforcing safer passwords.

e) What role does Multifactor Authentication (MFA) play in a Zero Trust enterprise? Explain.

The role that MFA plays in a Zero Trust enterprise is to enhance the security of the enterprise. A hacker can guess a password, but then they will have an extra step to successfully get into the account. These steps can be one of any of the following, SMS, biometric, mobile app based, and RFID authentication. All of these are MFA and will enhance security.