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

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

**Exercise #6**

**Team: 3**

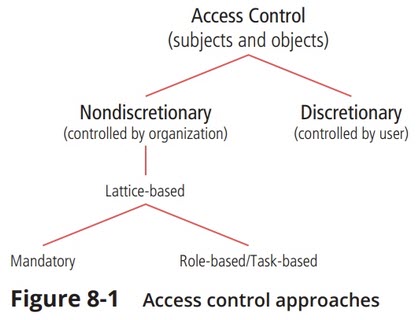
**Participants: *Dustin Thompson, Destinee Matsoumou, Bryce Watson, George Flarsheim, Bradley Lawton***

**Logistics**

1. Get together with other students on your assigned **Team** in person and/or 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 and may impact your performance on assessments, especially with respect to the essay questions.
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** *(15 points)*

Review Figure 8-1 from your text and explain the following terms:

* subjects and object (in access control) - The subject of the access is the user or system that makes a request to access a resource. The object, or resource, is the process a user or system is attempting to access.
* discretionary and non-discretionary access control - Discretionary access controls are the ones that are implemented at the judgement or option of the data user.

Nondiscretionary access controls are access controls that are implemented by a central authority.

* lattice-based access control - A variation on mandatory access controls that assign users a matrix of authorization for particular areas of access, incorporating the information assets of subjects such as users and objects.
* mandatory access control - A required, structured data classification scheme that assigns a sensitive or classification rating to each collection of information as well as each user.
* role-based access control - A nondiscretionary control where privileges are tied to the role or job a user performs in an organization and are inherited when a user is assigned to that role.
* attribute-based access control - An access control approach whereby the organization specifies the use of objects based on some attributes 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](https://www.microsoft.com/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/) 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](https://www.cpomagazine.com/cyber-security/back-to-school-an-introduction-to-zero-trust-architecture-and-identity-and-access-management/). Read the article and answer the following questions (*2 points each*).

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

Kindervag noted that the point of entry was not the target location. Hackers moved laterally through the system until they reached their target. Thus, by using a no trust policy, you introduced verification in multiple points on the system.

1. How has the pandemic influenced the increase in popularity of Zero Trust?

With the onset of the pandemic, many organizations have shifted their workforce to remote working. As the article referenced in the question states this shift in workforce has also migrated applications and data from traditional onsite storage to cloud-based storage offsite. The change in storage combined with multi device access outside of traditional perimeter security has led to the increase in popularity of Zero Trust.

1. Name and briefly describe the first planning step when building a Zero Trust Architecture in an organization.

The first step in building a zero trust architecture is to identify the ‘protect surface’. This encompasses the most important data, assets, applications, and services. This revolves around the users and systems they need to access. This can first be controlled by an identity and access management strategy. Next, decision-makers will need to decide what is allowed to cross their network how, and when. They’ll need to monitor and examine how users are currently using the network and then make a plan based on this.

1. Does Single Sign-On (SSO) still have a place in a Zero Trust enterprise? Explain.

Yes, SSO still has a place in Zero Trust architecture. The end-user needs to be identified before proceeding through the network of assets. It is the first step in the architecture, the first line of defense. SSO allows the users to access multiple systems seamlessly with one password which can often be complex and difficult to remember. SSO maximizes security by preventing credential-sharing and enforcing safer password practices.

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

Zero Trust architecture is built around the idea that nothing should be implicit, since you are likely to have users that will change devices and locations often within the enterprise it is best to have a higher standard of security. Multifactor Authentication is a simple method to increase this security by requiring more than one input for users to log in. Most often these added inputs are also a different form of authentication, such as biometrics or digital reading. Anyone with malicious intents would tend to need to gain access to the actual user they are attempting to impersonate. In short Multifactor Authentication is one of the best ways to ensure that a Zero Trust enterprise is secure.