CIS-481: Introduction to Information Security

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

Exercise #6

Team: 3
Participants: Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen

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:

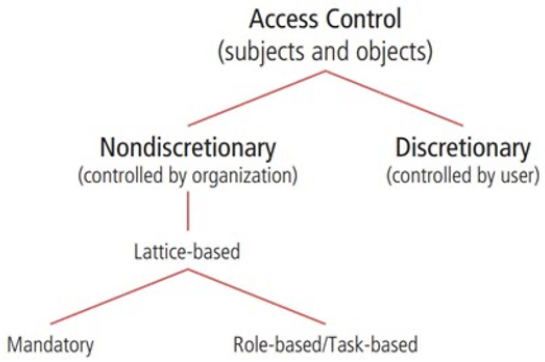

Figure 8-1 Access control approaches

· 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 objects (in access control, not attack): In access control, the subject is the user, system, or organization that uses or manages the access control. An object is the resource that the subject is trying to use or have access to.
Discretionary access control: Discretionary access controls are controlled by the user, where the user can gain access to information or resources, and have the option to give other people access to it.

Non-discretionary access control: Non-discretionary access controls are implemented by a central authority, or an organization, instead of being managed by a user.
Lattice-based access control: Lattice based access control is a form of non-discretionary access control that gives users a matrix of authorizations for particular areas of access.
Mandatory access control: Mandatory access control is where data and users are rated, where the rating specifies the level of access to information the user can have.
Role-based access control: Role-based controls are tied to the user's duties in an organization, such as a position or temporary role. For example, gaining a temporary role like a project manager gives them access to some resources.
Attribute-based access control: Attribute-based access control is another approach of lattice-based access control, where the system uses attributes such as name, date of birth, home address, training record, and job function to regulate access to data.

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 noted that during cyber attacks' the target locations are not usually how they infiltrate the system. This reveals that cyber criminals examine the system and hack the most vulnerable component then move throughout the system to more protected and valuable information.

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

   The pandemic has significantly increased virtual communication and network traffic due to increased software and application use. All these things make organizations more vulnerable to Cyber attacks and in response they are shifting to more foul proof security methods. Zero Trust architecture helps ensure that remote interactions occur between authorized members only.

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

The first planning step when building (ZTA) requires businesses and organizations to identify their “protect surface.” This requires them to narrow down all important assets, data, service, and applications and their relationship with users.

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

Single Sign-On is an authentication process that enables employees to access the business’s resources with a single set of credentials. SSO still has a place in a Zero Trust enterprise and is still one of the most useful authentication and management tools. SSO removes repetitive manual logins and complex passwords, and can maximize security and enforce safer password practices.

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

MultiFactor Authentication helps provide an additional layer of protection as it helps verify users and their login attempts. This is a safeguard that increases the level of difficulty for cyber criminals to hack accounts and access unauthorized information. MFA can exist through a variety of different methods each with different levels of nuance.