CIS-481: Introduction to Information Security

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

Exercise #6

Team: 4

Participants: Aneesa Bell, Paige Hensley, Patrick Nguyen, Logan Whaley, Emily Wyland

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:

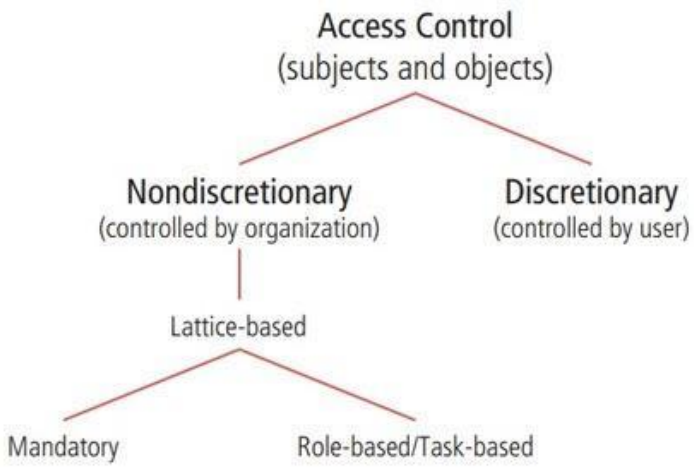

Figure 8-1 Access control approaches

- 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

A subject is the user or system. An object is a resource.

Discretionary access control is a control that is implemented at the judgement of the data user. Nondiscretionary access control is a control that is implemented by a central authority.

Lattice-based access control is a form of nondiscretionary access control. Under this form, users are assigned a matrix of authorizations for particular areas of access.

Mandatory access control is a form of lattice-based access control. Under this form, a data classification scheme is used to assign a sensitivity rating to each collection of information as well as each user.

Role-based access control is a type of nondiscretionary control where privileges are tied to the role a user performs in the organization. These privileges are inherited when a user is assigned to that role.

Attribute-based access control is a new approach to lattice-based access control. 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 noted that in many cyber-attacks the point of entry was not the target location. Hackers would identify a vulnerability in one area and then move laterally towards their target.
b) How has the pandemic influenced the increase in popularity of Zero Trust?
   The increase in popularity has been catalyzed by the pandemic. Organizations have migrated some applications to the cloud. Therefore, data is increasingly stored off premises. Additionally, employees access sensitive data from a range of devices, locations, and geographies. As a result, the traditional perimeter-centric security model is no longer fit for its purpose. ZTA is the replacement. Notably, the White House has begun transitioning towards a Zero Trust Architecture under the Biden Administration as of January 26, 2022.
c) Name and briefly describe the first planning step when building a Zero Trust Architecture in an organization.
   The first step is developing a "Zero Trust Policy." Organizations must identify the "protect surface," understand user interactions with it, and determine who is allowed to cross it (how and when).
d) Does Single Sign-On (SSO) still have a place in a Zero Trust enterprise? Explain.
   Yes. SSO maximizes security by preventing credential-sharing and enforcing safer password practices.
e) What role does Multifactor Authentication (MFA) play in a Zero Trust enterprise? Explain.
   MFA aids in authentication and access management. MFA ensures a user is who they say they are. It adds an important layer of security to ward off cybercriminals.