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

A. Get together with other students on your assigned team in person and 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.
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
Review Figure 6-1 from your text and explain the following terms:

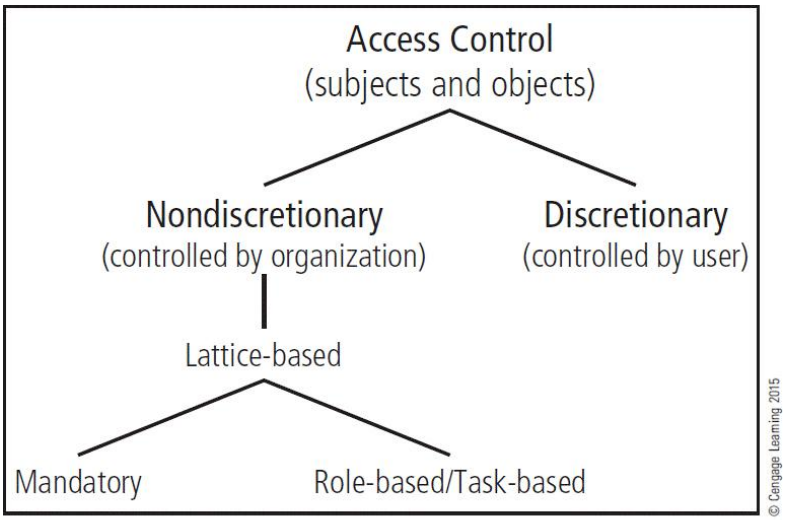

Figure 6-1 Access control approaches

- 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

(15 points)

Access controls: "The selective method by which systems specify who may use a particular resource and how they may use it." Access controls are put into place for the benefit of the resources of the object within a system. Users or subjects can access the resources if the system specifies that they can.

- **subjects and object (in access control, not attack)**
  - **subject:** a subject can be described as a user or a system. A subject can only access an object if they have permission to.
  - **object:** an object can be described as a resource. How long, from where and how the subject may use the object is also specified.

- **discretionary and non-discretionary access control:**
    - **Discretionary Access Controls (DACs):** "Access controls that are implemented at the discretion or option of the data user." Discretionary access controls give subjects the ability to control. They can control who has access and who doesn't have access to the resources at their disposal. They can also give access to a specific group of people.
    - **Non-Discretionary Access Controls (NDACs):** "Access controls that are implemented by a central authority." Non-Discretionary access controls are structured controls. These controls are managed by a central authority in an organization. This type of control is the opposite of DAC. In DAC a single entity can choose who has access, but in NDAC a group or an authority will make the decisions.
- **Lattice-based access control (LBAC):** "A variation on the MAC form of access control, which assigns users a matrix of authorizations for particular areas of access, incorporating the information assets of subjects such as users and objects." Resources are put into sections of authorization. Users can access the resources based on their level of authority. Classifications for each group will vary. Each subject has a different level of access, and that's what makes LBAC unique.
- **Mandatory access controls (MACs):** "A required, structured data classification scheme that rates each collection of information as well as each user." MAC is a data classification form of security. Each resource is rated based on how sensitive the information is, and each user is rated to specify the level of information that they may access. These ratings are sensitivity levels put in place to classify how important data is and what level of sensitivity can access that data.
- **Role-based access controls (RBACs):** "An example of a non-discretionary control where privileges are tied to the role a user performs in an organization and are inherited when a user is assigned to that role. Roles are considered more persistent than tasks" RBACs are given to users based on their role in an organization. Organizations can give access to resources if the user has the specified role that is associated with these resources. Access can also be taken away by simply changing the role of the user. This simplifies giving and taking away access.

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 Packet Inspection (SPI) firewall:** "A firewall type that keeps track of each network connection between internal and external systems using a state table and that expedites the filtering of those communications. Also known as a stateful inspection firewall." Stateful inspection is a type of firewall, this firewall uses a state table to monitor network connections. (Whiteman)
- A state table tracks the state and context of each packet by taking note of who sent it and when was it sent. "A stateful firewall can expedite incoming packets that are responses to internal requests. If the stateful firewall receives an incoming packet that it cannot match in its statetable, it refers to its ACL to determine whether to allow the packet to pass." Regular firewalls deny access based on address, but SPI firewalls deny access via internal request. Since information is stored on a packet basis data can be rejected or accepted easily. (Whiteman)

- Because it operates as a packet-based firewall, it is prone to DOS or DDOS attacks. Hackers will send a large number of external packets at once, the system will be overloaded and denied access.

Problem 3

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

Intrusion detection and prevention system (IDPS): "The general term for a system that can both detect and modify its configuration and environment to prevent intrusions. An IDPS encompasses the functions of both intrusion detection systems and intrusion prevention technology." The main obligation of IDPS is to detect and protect the system from malware software. IDPS can function as a multifaceted system detects intruders and prevents intruders from breaking in.

- **Network-Based IDPS:** "An IDPS that resides on a computer or appliance connected to a segment of an organization's network and monitors traffic on that segment, looking for indications of ongoing or successful attacks." Network based IDPS deal with everything that happens to a single network. It protects network assets by monitoring network traffic. This system is put into place to detect and prevent malware breaking into the network.
- **Host-Based IDPS:** "An IDPS that resides on a particular computer or server, known as the host, and monitors activity only on that system. Also known as a system integrity verifier." Host based IDPS deal with everything that happens to a host or server. It protects server assets by monitoring users connected to the server.

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

Work Cited

Whitman, M. E., & Mattord, H. J. (2018). Chapter 6 Security Technology: AccessControls, Firewalls, and VPNs. In *Principles of information security* (pp. 325-383). Australia: Cengage Learning.