Cyber security -Module 4

Identity and Access Management

Access Control Models

Access Control Models:

- Rule-based access control (RuBAC)
- Role-based access control (RBAC)
- Mandatory access control (MAC)
- Discretionary access control (DAC)

Mandatory Access Control (MAC): • Only system owner manages access control. • End user has no control over any privileges.	**Based Access Control (RBAC):** • Provides access based on the position an individual has in an organization.
Discretionary Access Control (DAC): • Least restrictive model. • Allows an individual complete control over any objects they own.	**Rule Based Access Control (RBAC).** • Dynamically assign roles to users based on criteria defined by owner or system administrator.

Mandatory Access Control

MAC

1. The Mandatory Access Control, or MAC, model gives only the owner and custodian management of the access controls. This means the end user has no control over any settings that provide any privileges to anyone. Now, there are two security models associated with MAC: **Biba and Bell-LaPadula.**

The **Biba** model is focused on the integrity of information, whereas the Bell-LaPadula model is focused on the confidentiality of information. Biba is a setup where a user with low-level clearance can read higher-level information (called “read up”) and a user with high-level clearance can write for lower levels of clearance (called “write down”). The Biba model is typically utilized in businesses where employees at lower levels can read higher-level information and executives can write to inform the lower-level employees.

MAC

Bell-LaPadula, on the other hand, is a setup where a user at a higher level (i.e. Top Secret) can only write at that level and no lower (called “write up”), but can also read at lower levels (called “read down”). Bell-LaPadula was developed for governmental and/or military purposes where if one does not have the correct clearance level and does not need to know certain information, they have no business with the information.

Role-Based Access Control

Admin assigns users to appropriate roles

Users are assigned to roles

Roles define authority level

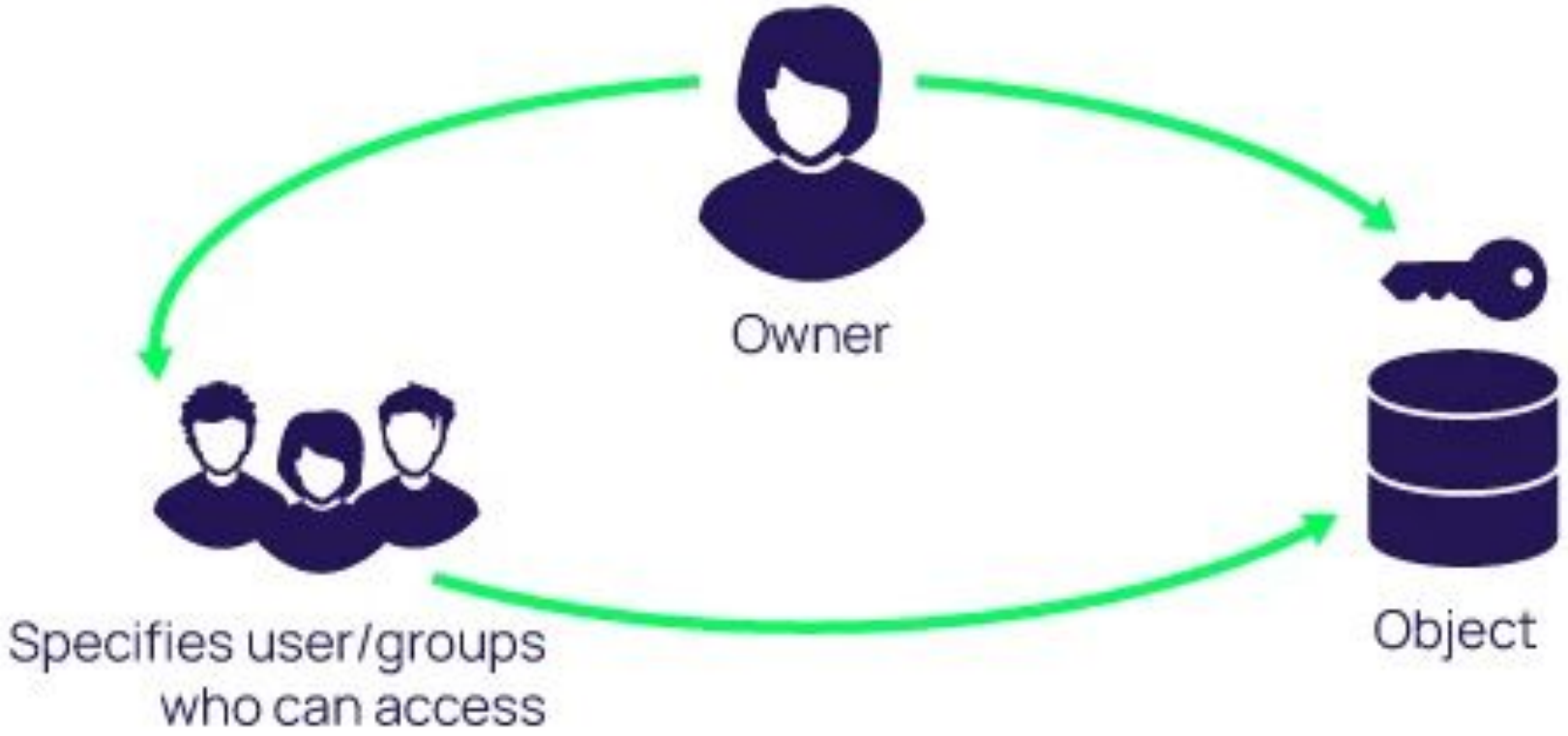
Permissions are authorized for specific rols

Role-Based Access Control, or RBAC

2. The Role-Based Access Control, or RBAC, model provides access control based on the position an individual fills in an organization. So, instead of assigning Alice permissions as a security manager, the position of security manager already has permissions assigned to it. In essence, Alice would just need access to the security manager profile.

RBAC makes life easier for the system administrator of the organization. The big issue with this access control model is that if Alice requires access to other files, there has to be another way to do it since the roles are only associated with the position; otherwise, security managers from other organizations could possibly get access to files for which they are unauthorized.

Discretionary Access Control (DAC)



The Discretionary Access Control

3. The Discretionary Access Control, or DAC, model is the least restrictive model compared to the most restrictive MAC model. DAC allows an individual complete control over any objects they own along with the programs associated with those objects.

This gives DAC two major weaknesses. First, it gives the end-user complete control to set security level settings for other users which could result in users having higher privileges than they're supposed to.

Secondly, and worse, the permissions that the end-user has are inherited into other programs they execute. This means the end-user can execute malware without knowing it and the malware could take advantage of the potentially high-level privileges the end-user possesses.

Rule-Based Access Control

System Admin

Defines access criteria

RBAC dynamically assigns roles to users

Rule-Based Access Control

The fourth and final access control model is Rule-Based Access Control, also with the acronym RBAC or RB-RBAC. Rule-Based Access Control will dynamically assign roles to users based on criteria defined by the custodian or system administrator.

For example, if someone is only allowed access to files during certain hours of the day, Rule-Based Access Control would be the tool of choice.