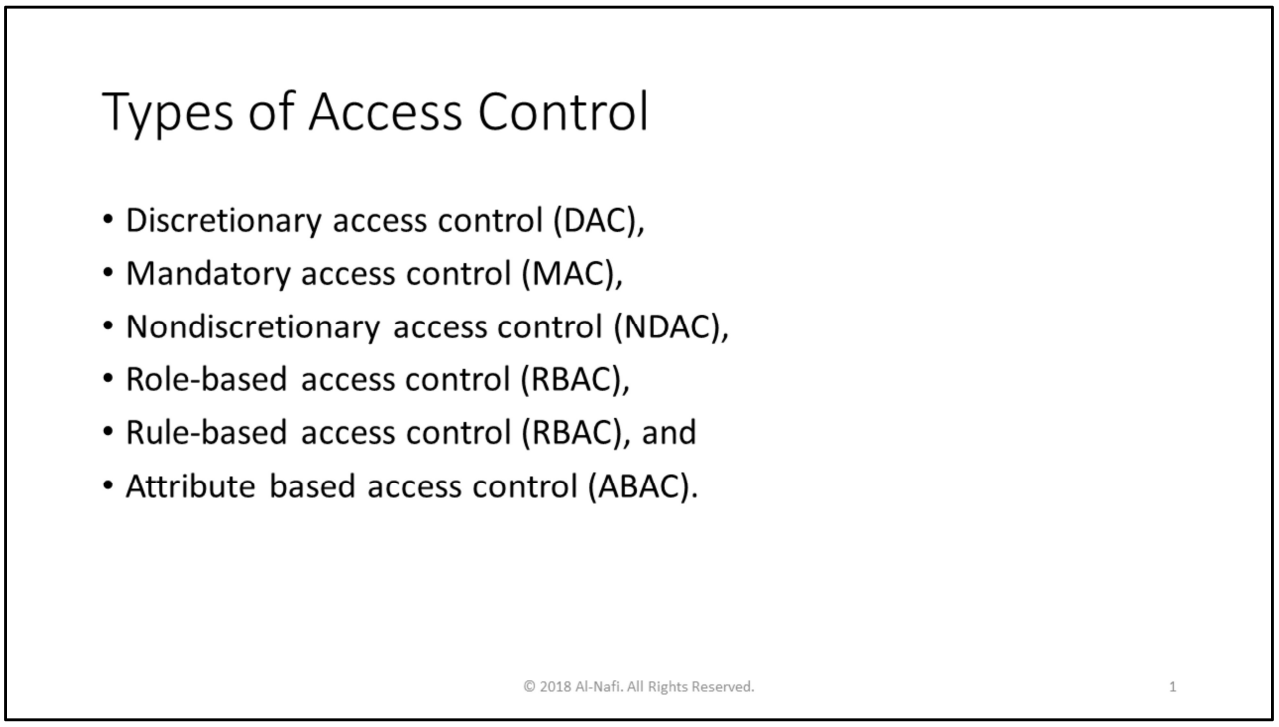
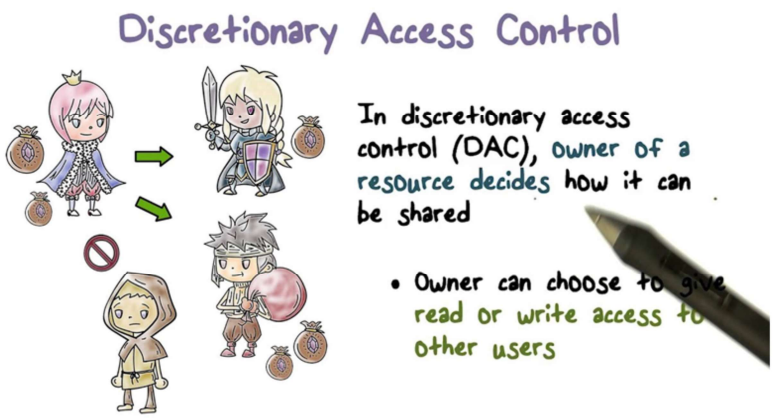


Types of Access Control

NIST SP 800-192 specifies access control models as “formal presentations of the security policies enforced by AC systems, and are useful for proving theoretical limitations of systems. AC models bridge the gap in abstraction between policy and mechanism.” The access control types addressed in this module are discretionary access control (DAC), mandatory access control (MAC), nondiscretionary access control (NDAC), role-based access control (RBAC), rule-based access control (RBAC), and attribute based access control (ABAC).

Discretionary access control (DAC),



Discretionary Access Control (DAC)

DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be. DAC allows for the greatest flexibility in controls along with the greatest vulnerabilities. The object's owner can pass on control weaknesses that can contribute to access and privilege aggregation.

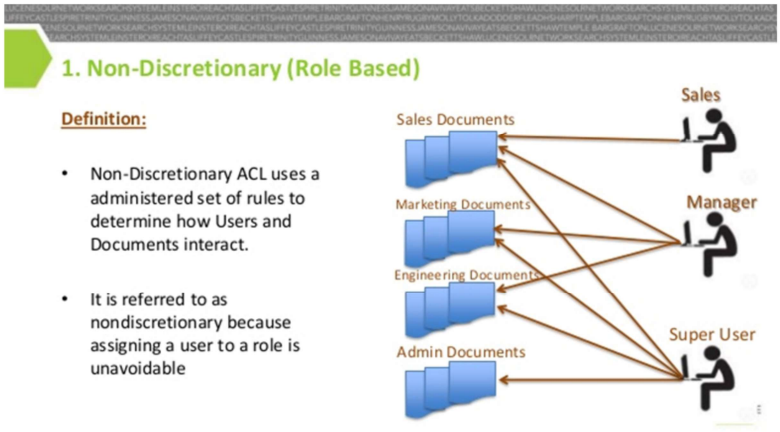
Mandatory access control (MAC)

Mandatory Access Control (MAC) Models

- User works in a company and the company decides how data should be shared
  - Hospital owns patient records and limits their sharing
    - Regulatory requirements may limit sharing

Mandatory Access Control (MAC)
MAC means that access control policy decisions are made by a central authority and not by the individual owner of an object. User cannot change access rights. An example of MAC occurs in military security, where an individual data owner does not decide who has a top-secret clearance, nor can the owner change the classification of an object from top-secret to secret.

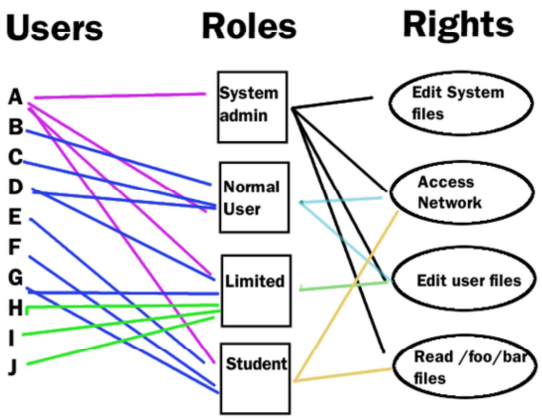
Nondiscretionary access control (NDAC)



Nondiscretionary Access Control (NDAC)

In general, all AC policies other than DAC are grouped under the category of nondiscretionary AC (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Nondiscretionary policies establish controls that cannot be changed by users but only through administrative action.

Role-based access control (RBAC)



Role-Based Access Control (RBAC)

RBAC is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. Access can be granted by the owner as with DAC and applied with the policy according to MAC.

Rule-based access control (RBAC)

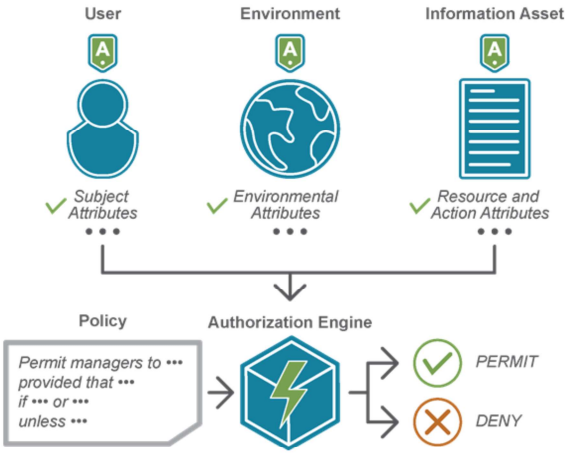
Rule Based Access Control

- Uses specific rules that indicate what can and cannot happen between a subject and an object.
- Not necessarily identity based.
- Traditionally, rule based access control has been used in MAC systems as an enforcement mechanism.

Rule-Based Access Control (RBAC)

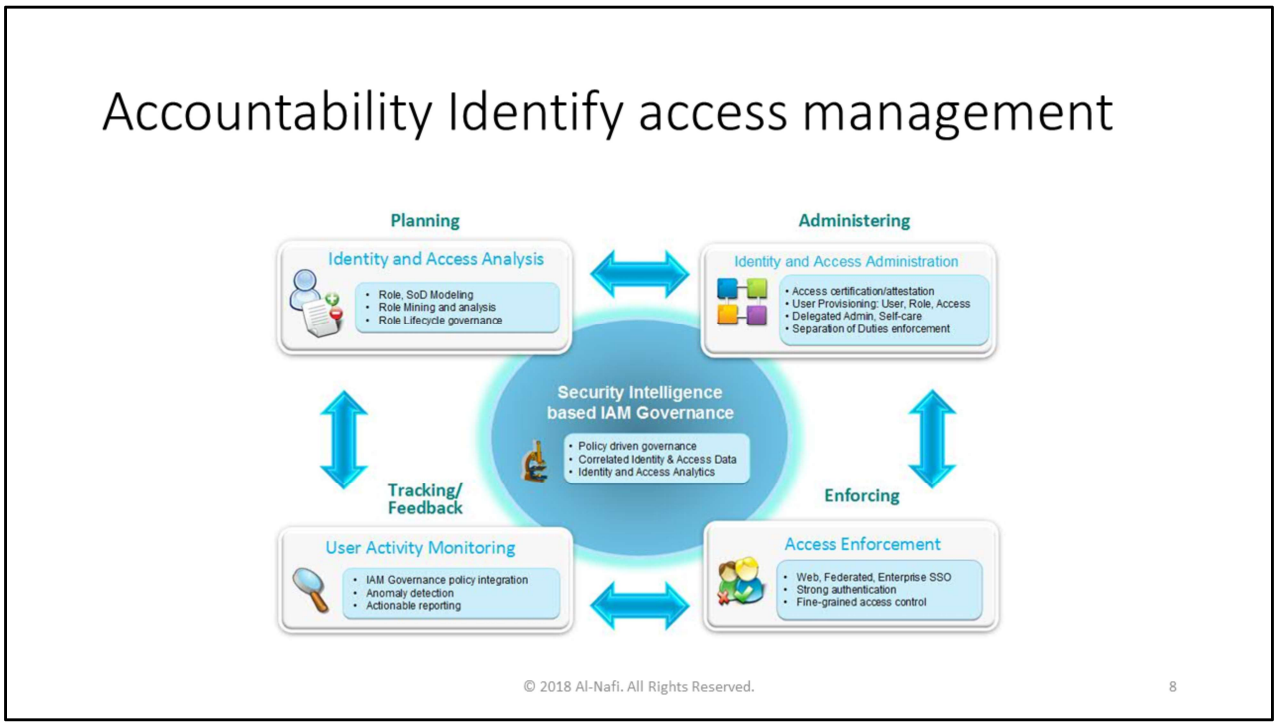
This is based upon a pre-defined list of rules that can determine access with additional granularity controls such as when, where, and if the system will allow read, write, or execute based upon special conditions. RBACs are managed by the system owner and represent an implementation of DAC.

Attribute based access control (ABAC)



Attribute-Based Access Control (ABAC)

ABAC is an access control paradigm whereby access rights are granted to users with policies that combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, environment attributes etc.).



Accountability

Ultimately one of the drivers behind strong identification, authentication, auditing, and session management is accountability. Fundamentally, accountability is being able to determine whom or what is responsible for an action and can be held responsible. Accountability ensures that account management has assurance that only authorized users are accessing the system and that they are using the system properly.

A closely related information assurance topic is non-repudiation. Repudiation is the ability to deny an action, event, impact, or result. Non-repudiation is the process of ensuring a user may not deny an action. Accountability relies heavily on non-repudiation to ensure users, processes, and actions may be held responsible. A primary activity in establishing accountability is to log relevant accesses and events within a system and to have a process that includes log review analysis.

جزاك اللهُ

To ask questions, Join the Al Nafi Official Group

https://www.facebook.com/groups/alnafi/

(This group is only for members to ask questions)