Access Control Models

Access Control:

Nobody in an organization should have free rein to access any resource. Access control is the combination of policies and technologies that decide which authenticated users may access which resources. Security requirements, infrastructure, and other considerations lead companies to choose among the four most common access control models:

- **Discretionary Access Control (DAC)**
- **Mandatory Access Control (MAC)**
- **Role-Based Access Control (RBAC)**

Discretionary Access Control (DAC)-

Discretionary access control decentralizes security decisions to resource owners. The owner could be a document's creator or a department's system administrator. DAC systems use access control lists (ACLs) to determine who can access that resource. These tables pair individual and group identifiers with their access privileges.

The sharing option in most operating systems is a form of DAC. For each document you own, you can set read/write privileges and password requirements within a table of individuals and user groups. System administrators can use similar techniques to secure access to network resources.

Advantages of DAC

Conceptual simplicity — ACLs pair a user with their access privileges. As long as the user is in the table and has the appropriate privileges, they may access the resource.

Responsiveness to business needs — Since policy change requests do not need to go through a security administration, decision-making is more nimble and aligned with business needs.

Disadvantages of DAC

Over/underprivileged users — A user can be a member of multiple, nested workgroups. Conflicting permissions may over- or under privilege the user.

Limited control — Security administrators cannot easily see how resources are shared within the organization. And although viewing a resource's ACL is straightforward, seeing one user's privileges requires searching every ACL.

Compromised security — By giving users discretion over access policies, the resulting inconsistencies and missing oversight could undermine the organization's security posture.

Mandatory Access Control (MAC)-

Mandatory access control uses a centrally managed model to provide the highest level of security. A non-discretionary system, MAC reserves control over access policies to a centralized security administration.

MAC works by applying security labels to resources and individuals. These security labels consist of two elements:

Classification and clearance — MAC relies on a classification system (restricted, secret, top-secret, etc.) that describes a resource's sensitivity. Users' security clearances determine what kinds of resources they may access.
Compartment — A resource's compartment describes the group of people (department, project team, etc.) allowed access. A user's compartment defines the group or groups they participate in.
A user may only access a resource if their security label matches the resource's security label.
MAC originated in the military and intelligence community. Beyond the national security world, MAC implementations protect some companies' most sensitive resources. Banks and insurers, for example, may use MAC to control access to customer account data.

Advantages of MAC
Enforceability — MAC administrators set organization-wide policies that users cannot override, making enforcement easier.
Compartmentalization — Security labels limit the exposure of each resource to a subset of the user base.
Disadvantages of MAC
Collaboration — MAC achieves security by constraining communication. Highly collaborative organizations may need a less restrictive approach.
Management burden — A dedicated organizational structure must manage the creation and maintenance of security labels.

Role-Based Access Control (RBAC)-
Role-based access control grants access privileges based on the work that individual users do. A popular way of implementing "least privilege " policies, RBAC limits access to just the resources users need to do their jobs.
Implementing RBAC requires defining the different roles within the organization and determining whether and to what degree those roles should have access to each resource.
Accounts payable administrators and their supervisor, for example, can access the company's payment system. The administrators' role limits them to creating payments without approval authority. Supervisors, on the other hand, can approve payments but may not create them.
Advantages of RBAC
Flexibility — Administrators can optimize an RBAC system by assigning users to multiple roles, creating hierarchies to account for levels of responsibility, constraining privileges to reflect business rules, and defining relationships between roles.
Ease of maintenance — With well-defined roles, the day-to-day management is the routine on-boarding, off-boarding, and cross-boarding of users' roles.
Centralized, non-discretionary policies — Security professionals can set consistent RBAC policies across the organization.
Lower risk exposure — Under RBAC, users only have access to the resources their roles justify, greatly limiting potential threat vectors.

Disadvantages of RBAC

Complex deployment — The web of responsibilities and relationships in larger enterprises makes defining roles so challenging that it spawned its own subfield: role engineering.

Balancing security with simplicity — More roles and more granular roles provide greater security, but administering a system where users have dozens of overlapping roles becomes more difficult.

Layered roles and permissions — Assigning too many roles to users also increases the risk of over-privileging users.