— Chapter # 04 —

→ Access control is the process of granting or denying specific requests to

- ↳ obtain & use info and related info processing services
- ↳ enter specific physical facilities

→ See table 4.1

→ An access control mechanism ~~mediates~~ ~~to~~ act as a bridge b/w a user & sys resources

→ Authentication — verification that the credentials of a user or other system entity are valid

→ Authorization — The granting of a right or permissi on to a system's entity to access sys resource

→ Audit — An independent review & examination of sys. records & activities to ~~&~~ ensure compliance with the established policy

- Access Control Policies

↳ Discretionary Access Control (DAC)

↳ Controls access based on the identity of the requestor and on access rules (authorization) stating what requestors are /or are not allowed.

↳ Access is controlled by owner

↳ Owner decides who can access their files or data

↳ Eg: You share a doc with friend & give them read access

↳ Mandatory Access Control (MAC)

↳ Access is controlled by a centeral authority based on security levels

↳ Eg: Used in military or gov. – A doc is labelle as "Top Secret". Only users with "Top Sec clearance can access it.

↳ Rules are mandatory – no user can override them

↳ Role Based Access Control (RBAC)

↳ Access depends on user's role in organization

↳ Eg: Manager can approve leave request
Employee 〃 only create 〃 〃.

- Attribute Based Access Control (ABAC)
  - Access is determined by multiple attributes – users attributes, resource attributes, envionmental attributes
  - A cloud system might allow:
    - A manager (user attribute) to access financial report (resource attribute) only during office hrs (env attribute)

• SUBJECT, OBJECT AND ACCESS RIGHT

▷ Subject :

- A subject is an entity capable of accessing object
- Process / Application → User → Subject
- A subj is accountable for it's action which are monitored thru audit trail
- Following are three classes of subject :

① Owner :
- Creater of a resource, like a file

② Group:
- A named grp of users granted the rights, such that any user in that group gets the access rights automatically

③ World :
- The least amount of access is granted to users who are able to access the system but are not either an owner or included in a group.

▷ Object:

- A resource to which the access is controlled
- Examples : Records, blocks, pages, directories

- Access Right :
  - ↳ The way in which a subject may access an object
  - ↳ Access rights could include the following
    - ↳ Read , Write , Execute , Delete , Create , Search

- ROLE BASED ACCESS CONTROL (RBAC)

→ RBAC controls access based on roles rather than individual identities

→ A role is typically defined as a job function or responsibility within an organization

→ Access rights are assigned to roles , & users are assigned to roles (not directly to permission)

→ This allows centralized, scalable & efficent permission management

- User ↔ Role Relationship – Many to Many
  - ↳ A single user can have multiple roles
  - ↳ A " role " " assigned to multiple users

- Role ↔ Resource Relationship – Many to Many
  - ↳ Each role has defined permissions for various reso
  - ↳ Multiple roles can access the same resource with diff privileges

→ RBAC is a non-discretionary & access control mechanism

→ Roles are assigned to user either statically or dyanamically.

→ Roles can be assigned to or revoked from a user.

→ Higher roles can inherit permissions from lower role (Adim > Manager > Employee)

→ Supports three well know security principles

① Least Privilege

↳ Only min necessary rights should be assigned to a subject that request access to a resource

② Seperation of Duties

↳ Achieved by ensuring that mutually exclusive roles must be invoked to complete a sensitive task

③ Data Abstraction

↳ Achieved by replacing technical data permissions (read / write) with abstract, business-oriented (credit / debit → for a financi accounting sys).

• How RBAC simplifies administration:

→ ~~Roles are assigned~~ Access rights are assigned to roles instead of individual users.

→ When new users join, admins just assign roles rather than configuring multiple permissions

→ If a company hires 50 new accountants, the admin just assign them "Accountant" role, no need ~~to give~~ individually set 10+ permissions per user

• How RBAC Supports Seperation of Duties (SoD)

→ SoD ensures that no single user can perform all steps of sensitive task

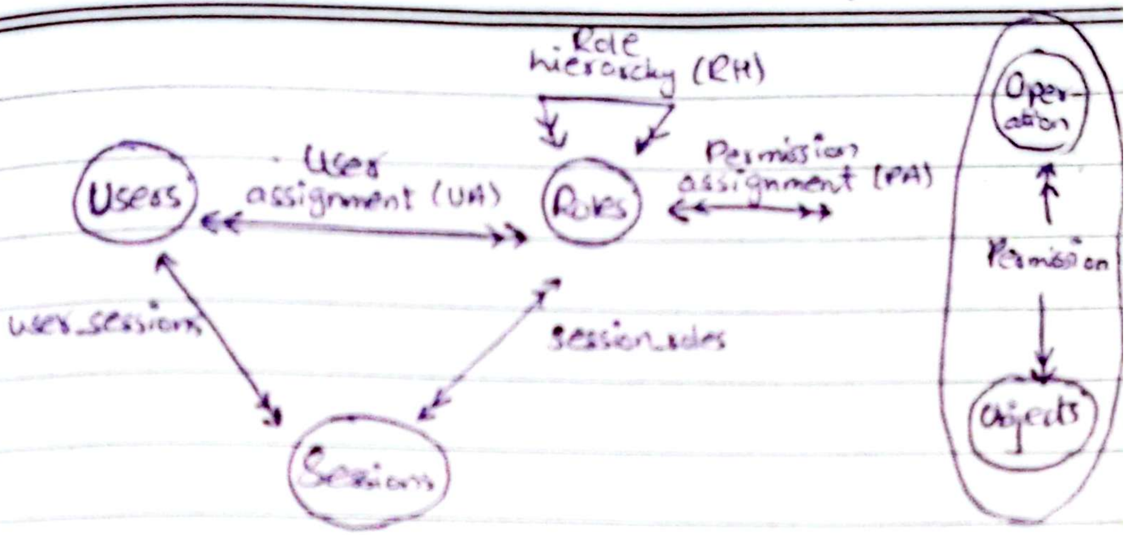
→ Each critical function is assigned to a diff role

→ ~~A user with the role~~

• How RBAC Provides Good Auditing and Accountabil

→ Actions are recorded based on roles, making it easy to track who did what under which role

→ Since permissions are tied to roles, auditor ca verify access rights by reviewing roles, not every user



▲ RBAC Model

- ATTRIBUTE BASED ACCESS CONTROL (ABAC)

→ ABAC is an advanced access control model where access decisions are made based on a combination of attributes of:

↳ Subject → Role, Department, location

↳ Object → Data type, ownership

↳ Environment → time of access, device typ etc.

→ There are three key elements to an ABAC model

- Attributes, which are defined for entities in a configuration
- Policy (Rule), which defines the ABAC policies
- Architecture Model, which applies to policies that enforce access control.

- Attributes

↳ Predefined Characteristics

▹ Subject Attribute

↳ User ID, Name, Department, Job title, Role

↳ Used to ~~identify~~ define the identity & characteristics of the requester

↳ Rule: " Access allowed if subject.department = "HR" AND subject.role = "Manager"

▹ Object Attribute

↳ Describe what resource is being accessed

↳ Filename, owner, type, creation date, metadata

↳ Rule: "Allow access if object.classification = "Public"."

▹ Enviornment Attributes

↳ Describe the context or conditions under which access occurs

↳ current date / time

↳ Rule: "Acces allowed if env.time < 6pm"

- Policy

→ In ABAC, policies are the rules that decide w can do what, on which resource, and under what conditions

Date ____________ Day ____________

→ Each policy considers subject attr., obj. attr. and env. attr.

→ Policies are defined by authorities.

⇒ See Slide # 34 (Week-07)