BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Security Architecture: Policies, Models and Mechanisms

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Agenda

- Introduction to security policies, models and mechanisms
- The Nature of Security Policies
- Types of Security Policies
- The Role of Trust
- Types of Access Control
- Policy Languages
- The CIA Classification:
  - Confidentiality Policies:
  - Integrity Policies:
  - Availability Policies:

Access Control

Access Control

Overview

- Access Control is all about protecting objects
  - such as, files, tables, hardware devices, or network connections, and other resources
- Basic access control means
  - "A subject is permitted to access an object in a particular mode, and only such authorized accesses are allowed."
    - --Scott Graham and Peter Denning
- Need to have different ways of access control. For example:
  - Certain users can have read only access
  - Others can have modification access
  - Some others have no access at all
- Techniques used for this must be robust, easy to use, and efficient.

Access Control

Overview

- Access control is the central element of computer security
- Access control implements a security policy
- The primary objectives of computer security:
  - to prevent unauthorized users from gaining access to resources
  - to prevent legitimate users from accessing resources in an unauthorized manner, and
  - to enable legitimate users to access resources in an authorized manner.
- A security policy specifies
  - who or what (e.g., a process or program) may have access to each specific system resource and the type of access that is permitted or denied in each instance

Access Control

innovate achieve lead

Definition of Access Control

- NISTIR 7298 – Glossary of Key IS Terms
  - Access Control is the process of granting or denying specific requests to:
    - (1) obtain and use information and related information processing services; and
    - (2) enter specific physical facilities
- RFC 4949 – Internet Security Glossary
  - Access Control is a process by which
    - use of system resources is regulated according to a security policy and
    - is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy
  - Refer to this site for complete definition
    - https://datatracker.ietf.org/doc/html/rfc4949

Access Control

innovate achieve lead

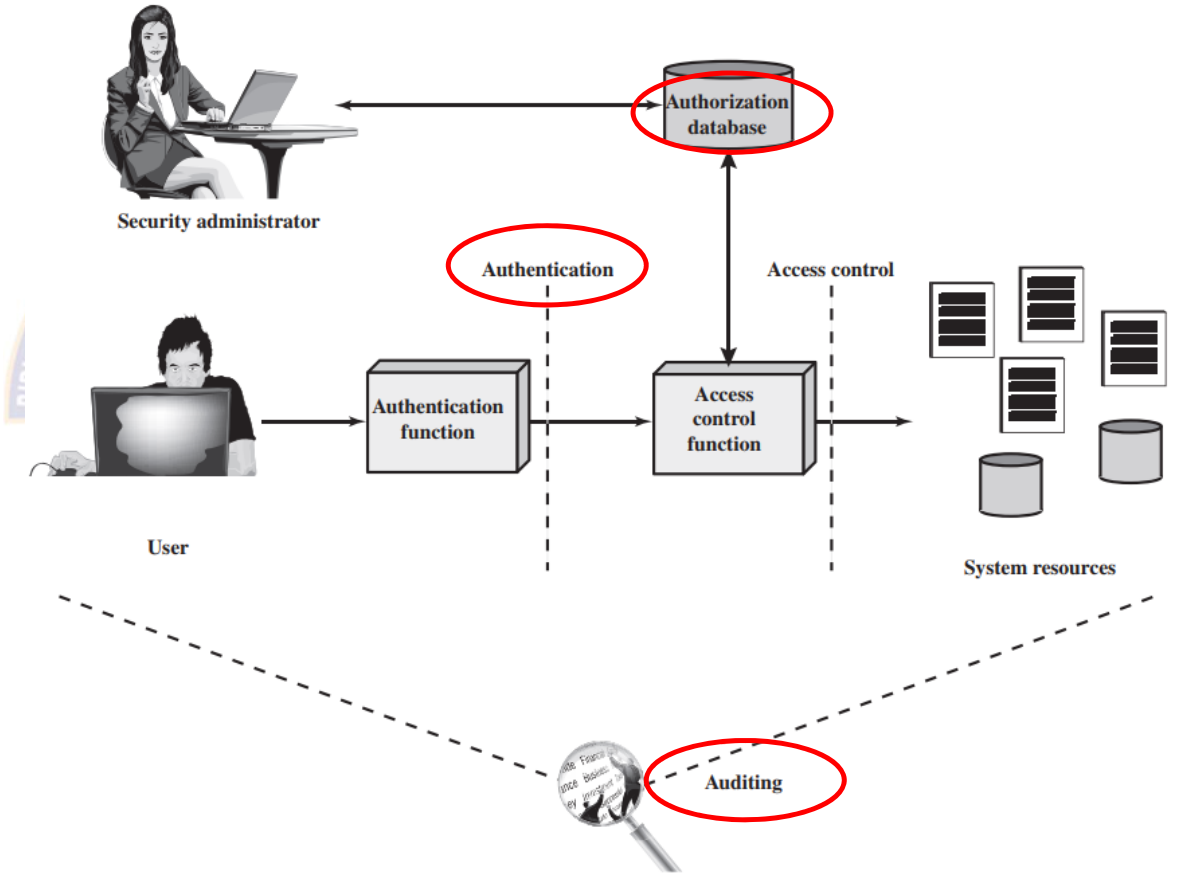
Terms

- Subjects:
  - Are human users, often represented by surrogate programs running on behalf of users
- Objects (System Resources)
  - Are things on which an action can be performed. For example,
    - Files, tables, programs, memory objects, hardware devices, strings, data fields, network connections, and processors
    - Users, or programs or processes representing users
      - E.g., an operating system (a program representing the system administrator) can allow a user to execute a program, halt a user, or assign privileges to a user
- Access modes or rights
  - Are any controllable actions of subjects on objects
  - Describe the way in which a subject may access an object. For example
    - Read, write, modify, delete, execute, create, destroy, copy, export, import, and so forth

Access Control

Context

- In addition to access control, the context involves the following entities and functions:
  - Authentication
  - Authorization
  - Audit



Access Control

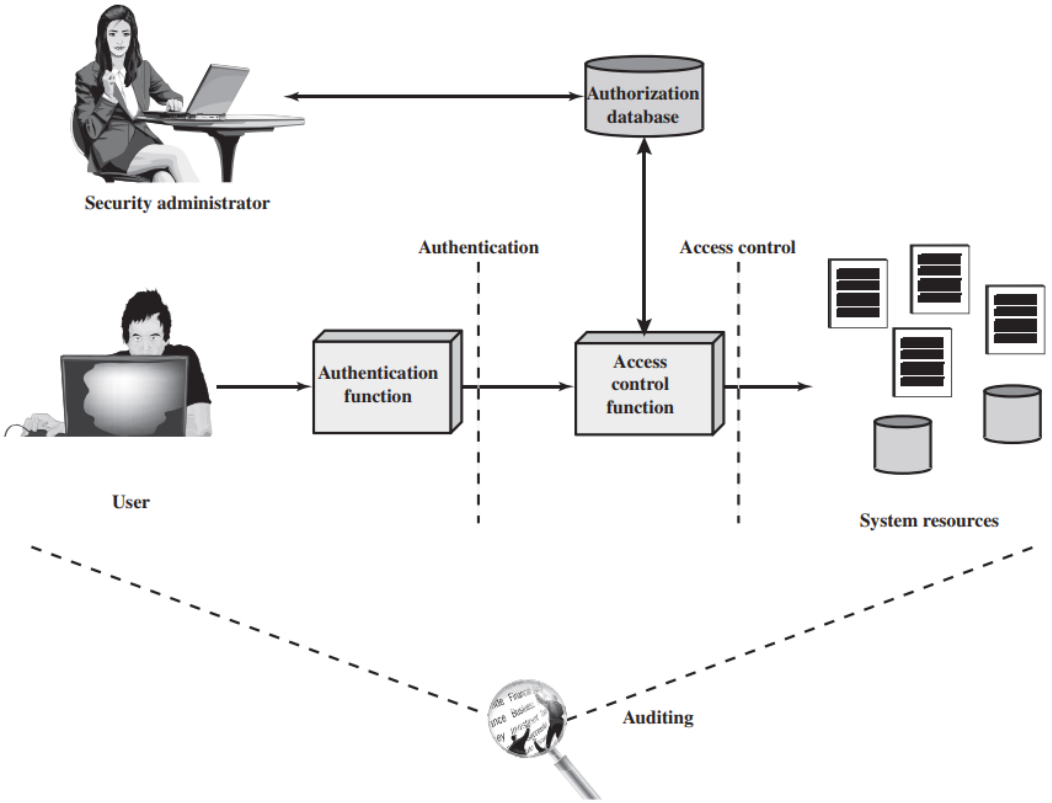
Context

- Authentication:
  - Verification that the credentials of a user or other system entity are valid.
- Authorization:
  - The granting of a right or permission to a system entity to access a system resource
  - This function determines who is trusted for a given purpose.
- Audit:
  - An independent review and examination of system records and activities in order
    - to test for adequacy of system controls
    - to ensure compliance with established policy and operational procedures
    - to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

Access Control

Context

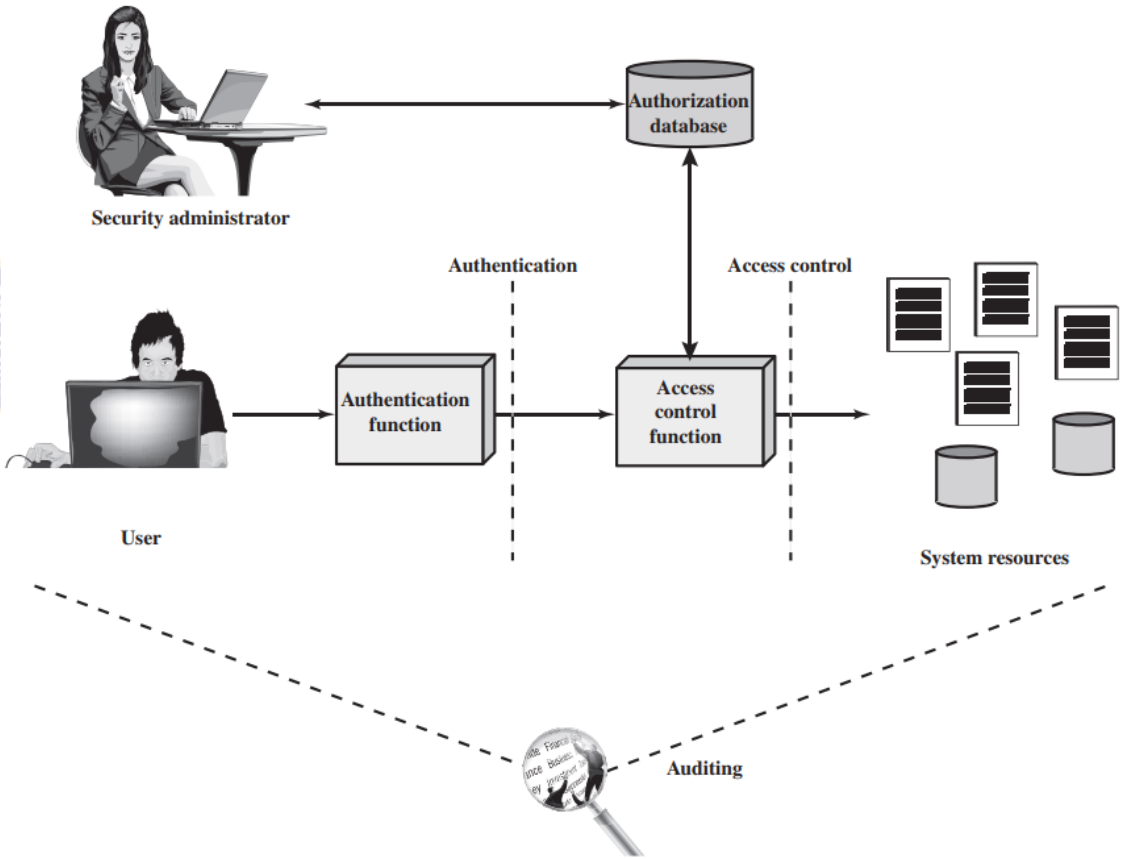
- An access control mechanism mediates between a subject and objects
- The system must first authenticate an entity seeking access
- Typically, the authentication function determines whether the user is permitted to access the system at all
- Then the access control function determines if the specific requested access by this user is permitted



Access Control

Context

- A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user
- The access control function consults this database to determine whether to grant access
- An auditing function monitors and keeps a record of user accesses to system resources



Types of Access Control

Types of Access Control

Overview

- There are three main types of access control
  - Discretionary Access Control (DAC) or Identity-based Access Control (IBAC)
    - Individual user sets access control mechanism to allow or deny access to an object
  - Nondiscretionary Access Controls
    - Mandatory Access Control (MAC), occasionally called a Rule-based Access Control
      - System mechanism controls access to object, and individual cannot alter that access
    - Role-based access control (RBAC)
    - Attribute-based access control (ABAC)
  - Originator-controlled Access Control (ORCON or ORGCON)
    - Originator (creator) of information controls who can access information

Types of Access Control

innovate achieve lead

Discretionary Access Control (DAC)/IBAC

- Most widely known access control
- An individual user can set an access control mechanism to allow or deny access to an object
  - Also called an *identity-based access control* (IBAC).
- DACs base access rights on the identities of the subject and the object involved
  - Identity is the key here
- The owner of the object decides who can access it by allowing only particular subjects to have access

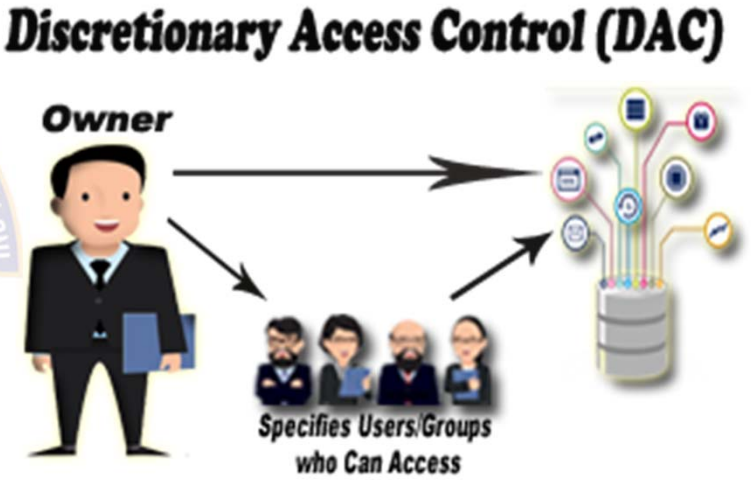


Image Source: https://www.digibrains.com/access-controls/

Types of Access Control

DAC/IBAC - Example

- If you create a file, you are the owner and can grant permissions to any other user to access the file
- The New Technology File System (NTFS), used on Microsoft Windows operating systems, uses the DAC model
- For example
  - If a user creates a new spreadsheet file, that user is both the creator of the file and the owner of the file
  - As the owner, the user can modify the permissions of the file to grant or deny access to other users
  - Data owners can also delegate day-to-day tasks for handling data to data custodians, giving data custodians the ability to modify permissions

Types of Access Control

DAC/IBAC Model – Access Control Lists

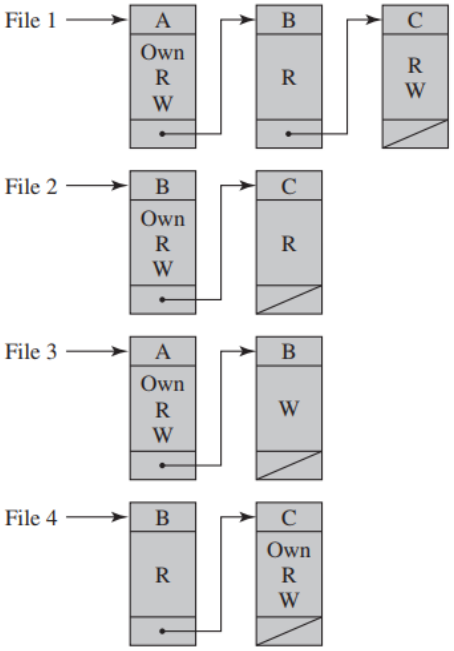
- A DAC model is implemented using access control lists (ACLs) on objects
- Each ACL defines the types of access granted or denied to subjects
- It does not offer a centrally controlled management system because owners can alter the ACLs on their objects at will
- Microsoft Windows systems use the DAC model to manage files
- Each file and folder has an ACL identifying the permissions granted to any user or group and the owner can modify permissions
- Within a DAC environment, administrators can easily suspend user privileges while they are away, such as on vacation
- Similarly, it's easy to disable accounts when users leave the organization

Types of Access Control

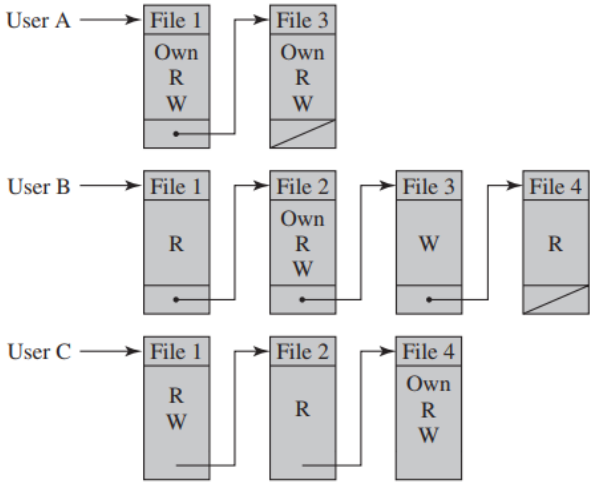
DAC/IBAC Model – Access Control Lists

SUBJECTS	OBJECTS: File 1	File 2	File 3	File 4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

(a) Access matrix



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

Types of Access Control

DAC/IBAC Model – Access Control Lists

Authorization Table for Files

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

Types of Access Control

DAC/IBAC – Pros and Cons

- Pros
  - User-friendly
    - Users can manage their data and quickly access data of other users.
  - Flexible
    - Users can configure data access parameters without administrators.
  - Easy to maintain
    - Adding new objects and users doesn't take much time for the administrator.
  - Granular
    - Users can configure access parameters for each piece of data.
- Cons
  - Low level of data protection
    - DAC can't ensure reliable security because users can share their data however they like.
  - Obscure
    - There's no centralized access management, so in order to find out access parameters, you have to check each ACL.

Source: https://www.ekransystem.com/en/blog/mac-vs-dac

Types of Access Control

Nondiscretionary Access Controls

- The major difference between discretionary and nondiscretionary access controls is in how they are controlled and managed
- Nondiscretionary access controls are centrally administered and administrators can make changes that affect the entire environment
- In contrast, DAC models allow owners to make their own changes, and their changes don't affect other parts of the environment.
- In a non-DAC model, access does not focus on user identity
  - Instead, a static set of rules governing the whole environment manages access
- Non-DAC systems are easier to manage, but are less flexible
- These include:
  - Mandatory Access Control (MAC)
  - Role-based access control (RBAC)
  - Attribute-based access control (ABAC)

Types of Access Control

Mandatory Access Control (MAC)

- Sometimes called as Rule-based Access Control (RAC)
- Rules describe the conditions under which access is allowed.
- Here, a mechanism controls access to an object, and individual user cannot alter that access
- MAC is based on fiat (official sanction), and identity is irrelevant:
- Access rules are manually defined by system administrators and strictly enforced by the operating system or security kernel
- Neither the subject nor the owner of the object can determine whether access is granted
- Typically, the system mechanism checks attributes associated with both the subject and the object to determine whether the subject should be allowed to access the object

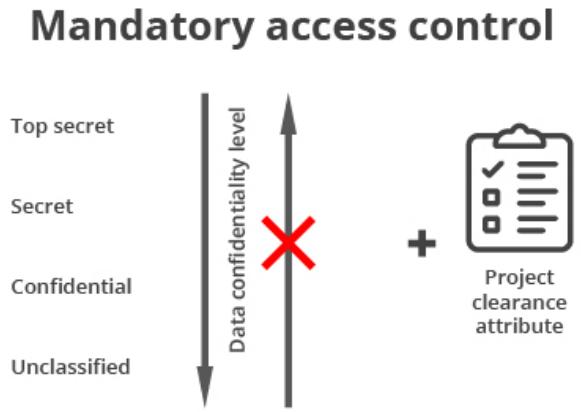


Image Source: https://www.ekransystem.com/en/blog/mac-vs-dac

Types of Access Control

MAC/RAC – Example

- Example 1: In the case of operating systems,
  - a subject is usually a process or thread
  - objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, IO devices, etc.,.
  - Subjects and objects each have a set of security attributes
  - Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place
  - Any operation by any subject on any object is tested against the set of authorization rules (aka policy) to determine if the operation is allowed
- Example 2: Military security
  - 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

Source: https://en.wikipedia.org/wiki/Mandatory_access_control

Types of Access Control

MAC/RAC

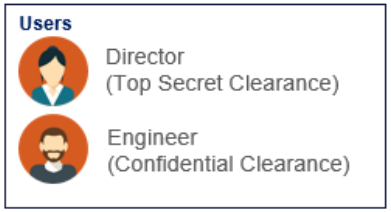
- A MAC model relies on the use of classification labels
- Each classification label represents a security domain, or a realm of security
- A security domain is a collection of subjects and objects that share a common security policy

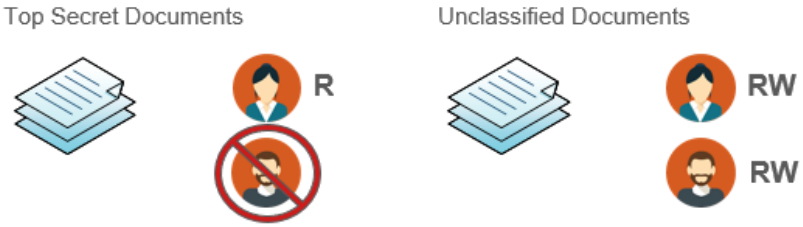
- For example
  - If a security domain has the label "Secret," the MAC model would protect all objects with the "Secret" label in the same manner
- Subjects are only able to access objects with the "Secret" label when they have a matching "Secret" label

Image Source: https://www.digibrains.com/access-controls/

Types of Access Control

MAC/RAC





- Users have labels assigned to them based on their clearance level, which is a form of privilege
- Objects have labels, which indicate their level of classification or sensitivity
- For example
  - The U.S. military uses the labels of Top Secret, Secret, and Confidential to classify data
  - Administrators can grant access to Top Secret data to users with Top Secret clearances
  - However, administrators cannot grant access to Top Secret data to users with lower-level clearances such as Secret and Confidential
- Governments use labels mandated by law, organizations in private sector are free to choose their labels, such as
  - confidential (or proprietary), private, sensitive, and public

Image Source: https://community.aras.com/b/english/posts/access-control-methods-in-innovator

Types of Access Control

MAC/RAC – Pros and Cons

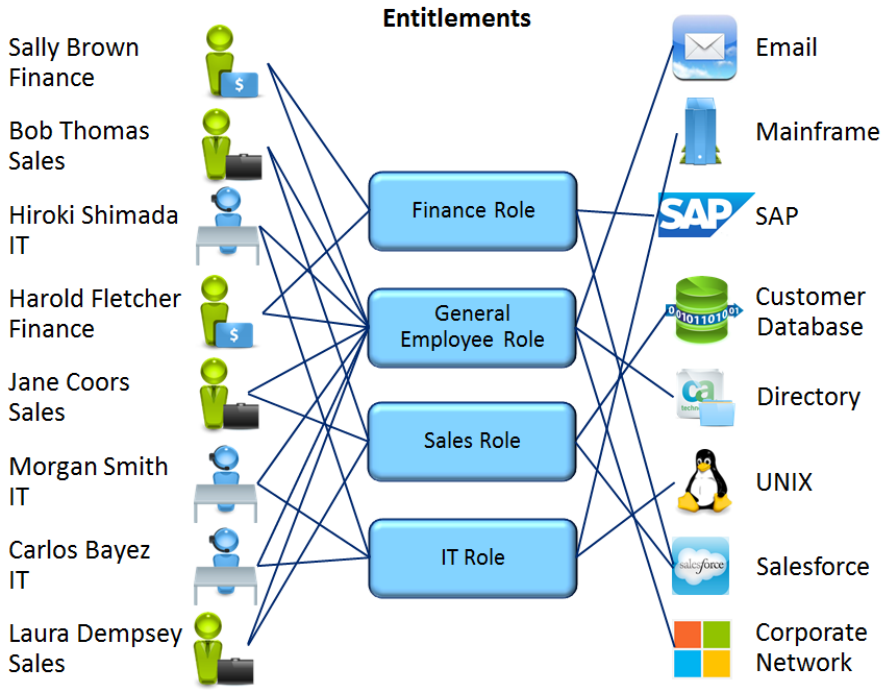
- Pros
  - High level of data protection
    - An administrator defines access to objects, and users can't edit that access.
  - Control
    - An administrator controls user access rights and object access parameters manually
  - Immune to Trojan Horse attacks
    - Users can't declassify data or share access to classified data
- Cons
  - Maintainability
    - Manual configuration of security levels and clearances requires constant attention from administrators.
  - Scalability
    - MAC doesn't scale automatically.
  - Not user-friendly
    - Users have to request access to each new piece of data
    - Users can't configure access parameters for their own data

Source: https://www.ekransystem.com/en/blog/mac-vs-dac

Types of Access Control

Role Based Access Control (RBAC)

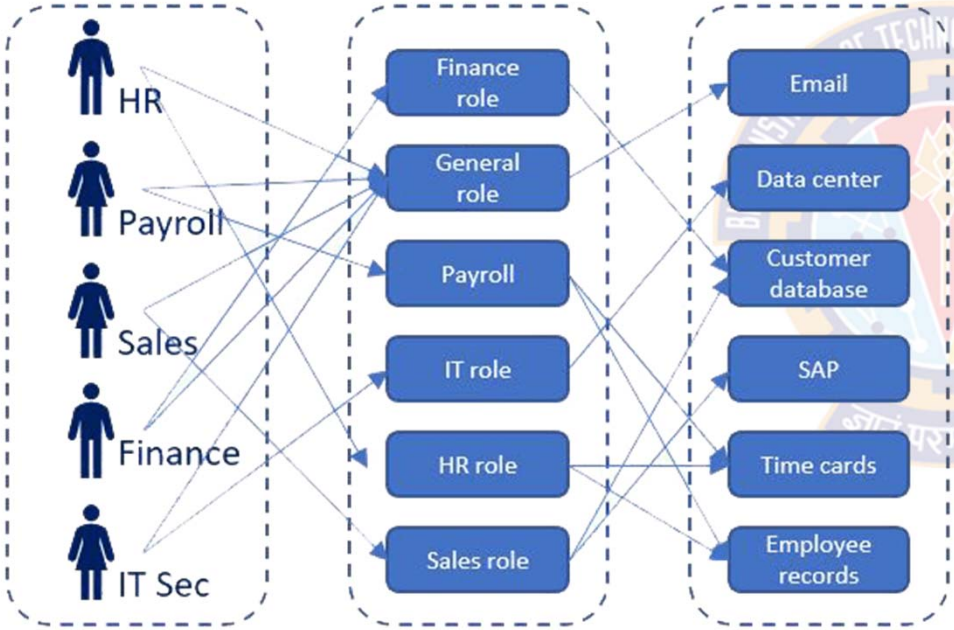
- Role-based or task-based access controls define a subject's ability to access an object based on the subject's role or assigned tasks
- Role Based Access Control (RBAC) is often implemented using groups



Types of Access Control

innovate achieve lead

Role Based Access Control (RBAC)



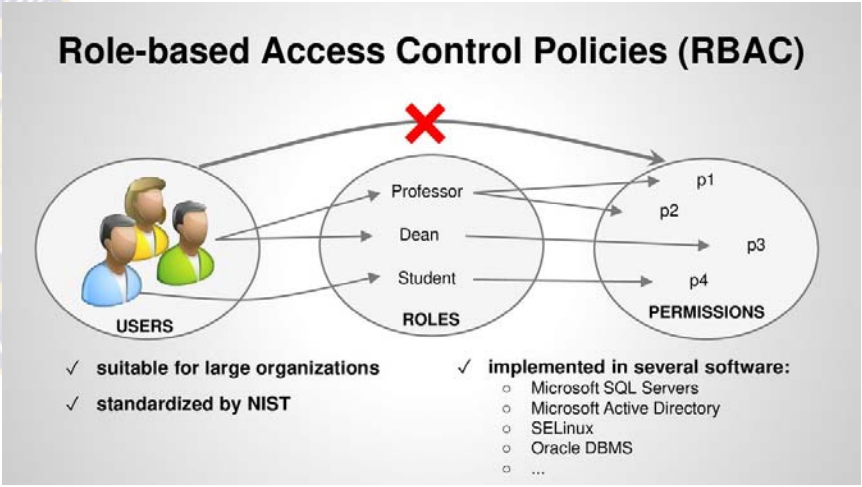
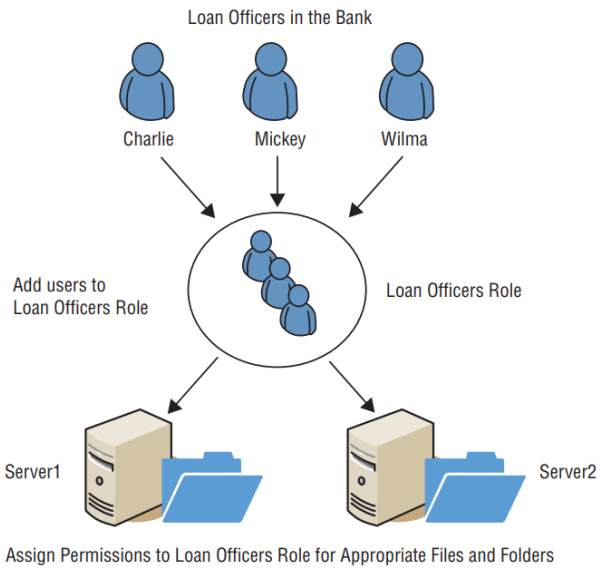


Image Source: https://thorteaches.com/cissp-certification-rbac/
Image Source: https://slideplayer.com/slide/14609327/

Types of Access Control

Role Based Access Control (RBAC) - Example

- A bank may have loan officers, tellers, and managers
- Administrators can:
  - create a group named Loan Officers
  - place the user accounts of each loan officer into this group,
  - and then assign appropriate privileges to the group
- If a new loan officer joins the organization,
  - administrators simply add the new loan officer's account into the Loan Officers group
- Administrators would take similar steps for tellers and managers



Types of Access Control

Role Based Access Control (RBAC)

- This helps enforce the principle of least privilege
- Prevents privilege creep, where users to accrue privileges over time as their roles and access needs change
- Ideally, administrators revoke user privileges when users change jobs within an organization
- However, when privileges are assigned to users directly, it is challenging to identify and revoke all of a user's unneeded privileges

Types of Access Control

innovate achieve lead

Role-based Access Control – Pros and Cons

Pros

- **Flexibility:** The company only assigns roles to an employee as required. Any modifications to the organizational structure or permissions are quickly applied to all employees when the company modifies the corresponding role.
- **Reduced administration work:** Time-consuming process of individually assigning permissions is avoided
- **Less error prone:** Assigning permissions individually is a more complex process and is thus more error prone than using role-based access control for assigning permissions.
- **Increased efficiency:** Reducing the amount of work and error rate increases the efficiency of IT and other employees. There is no longer any need for manual modifications, error handling, wait times or individual permission requests.
- **Security:** Access permissions are defined exclusively via the role model which prevents you from giving more permissions than needed to individual employees. This is in line with the Principle of Least Privilege (PoLP).
- **Transparency:** The naming of roles is usually straightforward and thus increases transparency and comprehensibility for users.

Cons

- **Labor-intensive setup:** Translating organizational structures into the RBAC model requires a lot of work.
- **Temporary assignments:** If a user only needs extended access permissions temporarily, it is easier to forget about them when using RBAC than when assigning permissions individually.
- **Application:** In small companies, creating and maintaining roles would be more labor intensive than assigning permissions individually. Therefore, the RBAC model is only used when a certain number of roles and employees has been reached. However, even in large companies, role-based access control suffers from the drawback that it is easy to end up creating a large number of roles. If a company has ten departments and ten roles, this will already result in 100 different groups.

Source: https://www.ionos.com/digitalguide/server/security/what-is-role-based-access-control-rbac/

Types of Access Control

Rule-based Access Controls

- Uses specific rules that indicate what can and cannot happen between a subject and an object
- Before a subject can access an object, it must meet a set of predefined rules
- Example:
  - *"If the user is accessing the system between Monday and Friday 8AM to 5PM, and if the user's security clearance equals or dominates the object's classification, then the user can access the object"*
- Traditionally, rule-based access control has been used in MAC systems as an enforcement mechanism
- In traditional rule-based model, no user identities are involved – meaning, no tracking possible
- In implementation, identity tracking is often required and added to rule-based access controls
  - this violates the classic/traditional rule-based model

Types of Access Control

Rule-based Access Controls

- A rule-based access control model uses a set of rules, restrictions, or filters to determine what can and cannot occur on a system
- Distinctive characteristic:
  - Rule(s) apply to all regardless of who the user is
  - They have global rules that apply to all subjects
- Examples
  - Routers & Firewall rules: examines all the traffic going through it and only allows traffic that meets one of the rules
  - Disk or mail quotas
  - Data Loss Prevention (DLP): for making sure that end users do not send sensitive or critical information outside the corporate network

Types of Access Control

Rule-based Access Controls

- Firewalls include a final rule (referred to as the implicit deny rule) denying all other traffic
- For example
  - The last rule might be deny all to indicate the firewall should block all traffic in or out of the network that wasn't previously allowed by another rule
- In other words, if traffic didn't meet the condition of any previous explicitly defined rule, then the final rule ensures that the traffic is blocked
- This final rule is sometimes viewable in the ACL so that you can see it
- Other times, the implicit deny rule is implied as the final rule but is not explicitly stated in the ACL

Types of Access Control

Attribute Based Access Controls (ABAC)

- Rule-based access control models include global rules that apply to all subjects equally
- An advanced implementation of a rule-based access control is an Attribute Based Access Control (ABAC) model
- ABAC models use policies that include multiple attributes for rules
  - E.g., Attributes are characteristics of users, the network, and devices on the network
- Many software-defined networking applications use ABAC models

User	Object	Environment
Title	Type	Geo-Location
Group	Date	Network
Department	Sensitivity	Time of Day
Devices		Network

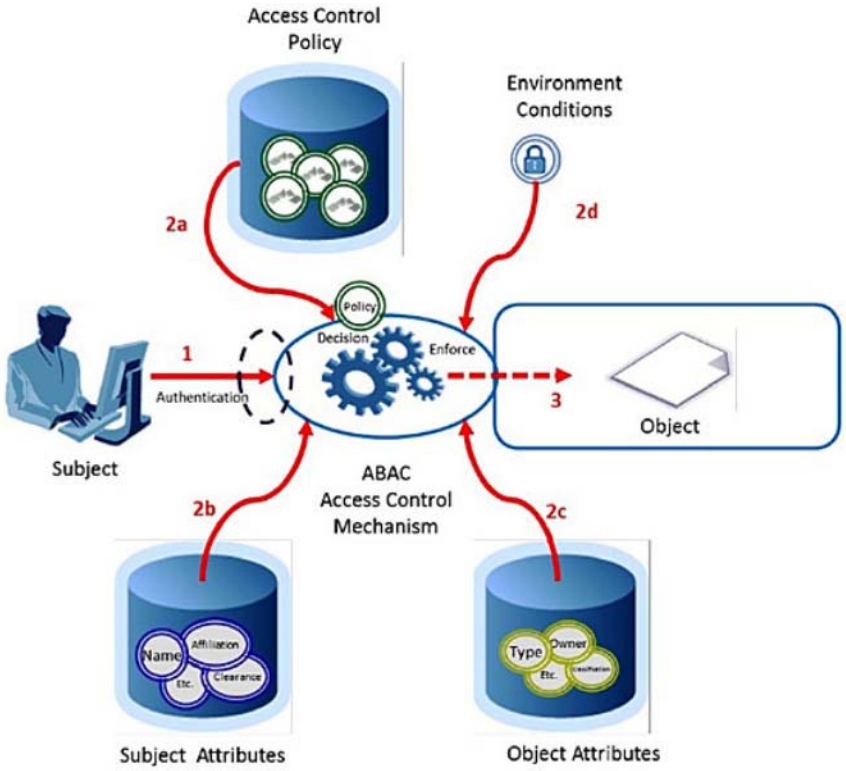
Types of Access Control

innovate achieve lead

Attribute Based Access Controls (ABAC)

- Subject requests access to an object
- Access Control Mechanism accesses
  - a) Rules
  - b) Subject attributes
  - c) Object attributes
  - d) Environmental conditions

  to determine authorization
- Subject is:
  - Given Access to the object if Authorized
  - Denied Access if Not Authorized

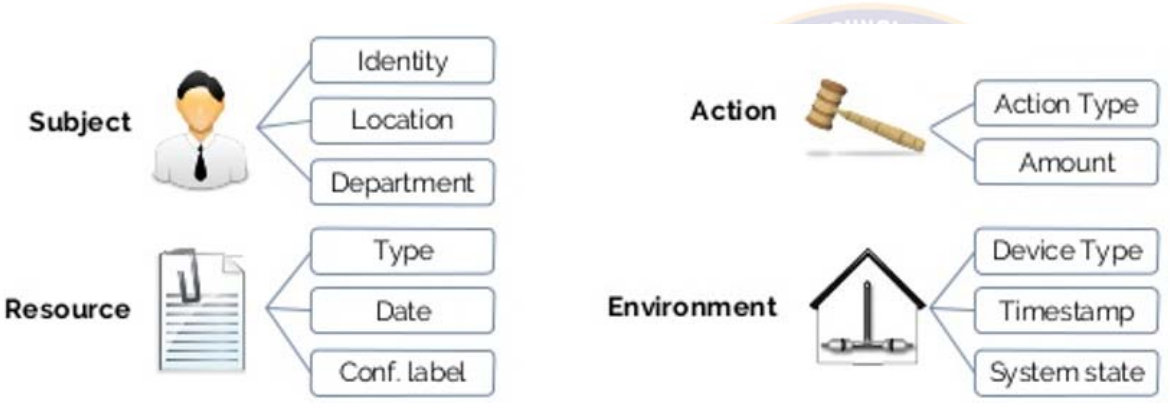


Source: https://www.bankinfosecurity.com/nist-publication-aims-to-ease-access-control-a-6612

Types of Access Control

innovate achieve lead

Attribute Based Access Controls (ABAC)



Managers of the *auditing department* in *Brussels* can *inspect* the *financial reports* from the *current financial year* within *office hours*

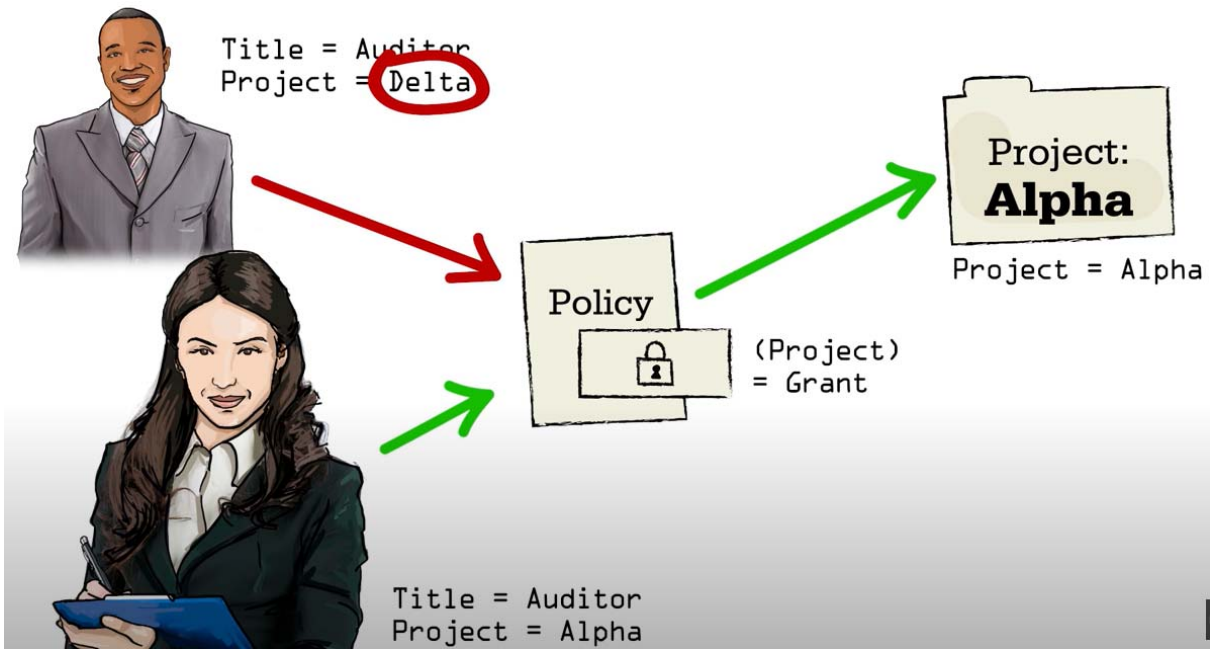
- Subject
  - Managers
  - Auditing Department
  - Brussels
- Action
  - Inspect
- Resource
  - Financial reports
  - Financial year
- Environment
  - Current
  - Office Hours

Image Source: https://www.slideshare.net/elimity/iam-innovation-tech-startup-experiences-a-deeper-look-into-rbac-vs-abac

Types of Access Control

innovate achieve lead

Attribute Based Access Controls (ABAC)



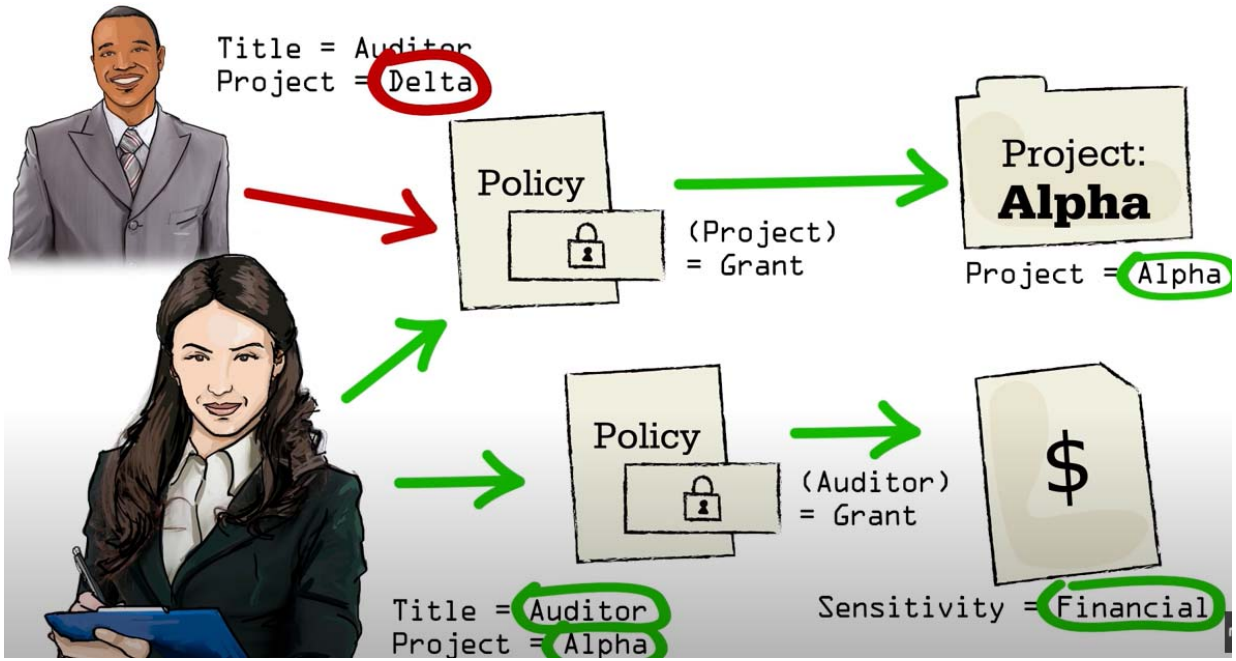
- Subject
  - Auditor
- Action
  - Read, Write
- Resource
  - Financial reports
  - Project = Alpha
  - Project = Delta
- Environment
  - Project Duration

Image Source: YouTube: https://youtu.be/cgTa7YnGfHA

Types of Access Control

innovate achieve lead

Attribute Based Access Controls (ABAC)



- Subject
  - Auditor
- Action
  - Read, Write
- Resource
  - Financial reports
  - Project = Alpha
  - Project = Delta
- Environment
  - Project Duration

Image Source: YouTube: https://youtu.be/cgTa7YnGfHA

Types of Access Control

ORCON or ORGCON

- Definition
  - An Originator Controlled Access Control (ORCON or ORGCON) bases access on the creator of an object (or the information it contains)
- Combines the features of MAC and DAC models
- This access control allows the originator of the file (or of the information it contains) to control the dissemination of the information
- The owner of an object cannot change the access controls of the object
- The creator (originator) of the object can alter the access control restrictions on a per-subject or per-object basis
- When the object is copied, the access control restrictions of the source are copied as well

Types of Access Control

ORCON or ORGCON – Example

- Bit Twiddlers, Inc., an embedded systems company contracts with Microhackers Ltd., a company famous for its microcoding abilities
- The contract requires Microhackers to develop a new microcode language for a particular processor
  - which is designed to be used in high-performance embedded systems
- Bit Twiddlers gives Microhackers a copy of its specifications for the processor
- The terms of the contract require Microhackers to obtain permission before it gives any information about the processor to its subcontractors
- This is an originator controlled access mechanism because, even though Microhackers owns the file containing the specifications, it may not allow anyone to access that information unless the creator of that information, Bit Twiddlers, gives permission

Types of Access Control

ORCON or ORGCON – Advantages/Characteristics

- Keeps unauthorized recipients from reading the object
- Prevent re-dissemination from authorized subjects to unauthorized entities or subjects
  - Creator must always give permission
- Authorized subjects must be able to write to the object, but Not to change Original Permissions


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!