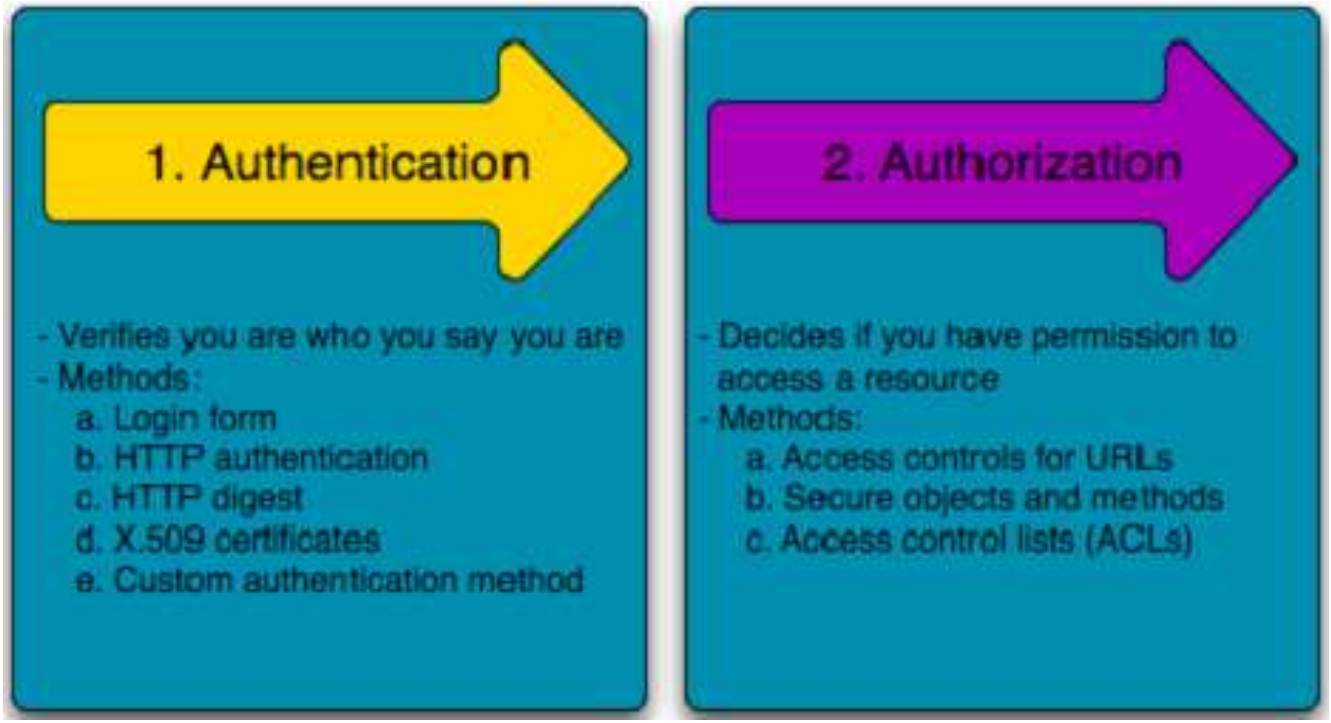
Lesson 5.

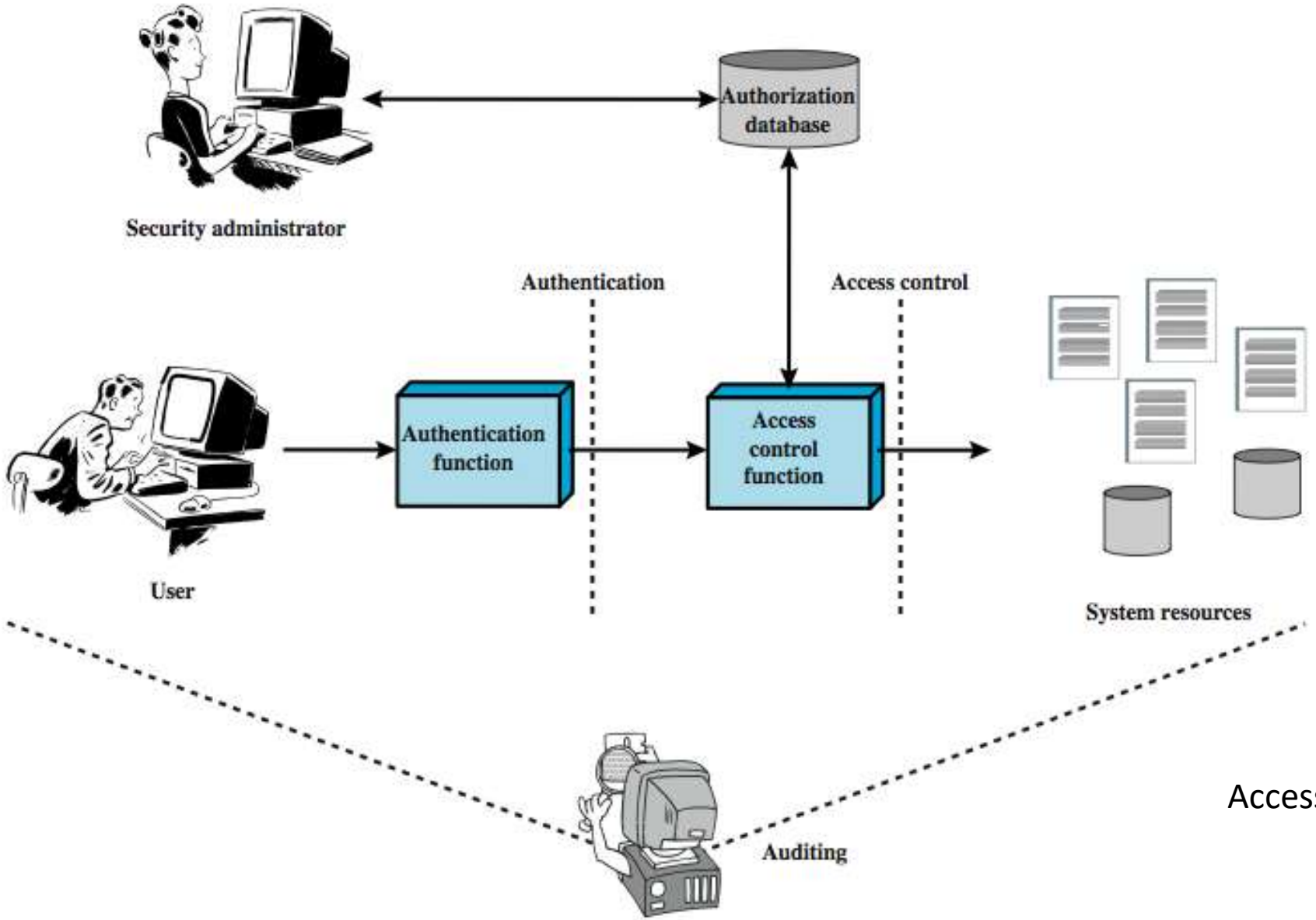
# Access Control

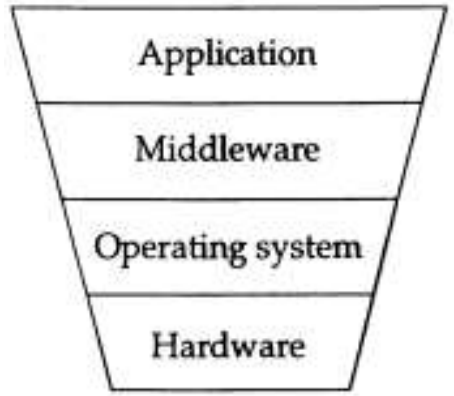


# Outline

1. Introduction
2. Access control types
3. Access control Terminology
4. Access control models
5. Access control matrix
6. Access control monitoring
7. Lab
8. summary

# Relationship among Access Control and Other security functions




Access controls at different levels in a system

# Introduction


- **Access control** is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system.
- It permits management to specify **what users can do**, **which resources they can access**, and **what operations they can perform on a system**.
- The goal of access control is to minimize the security risks of unauthorized access to physical and logical systems
- It consists of two main components: authentication and authorization

# Access control types

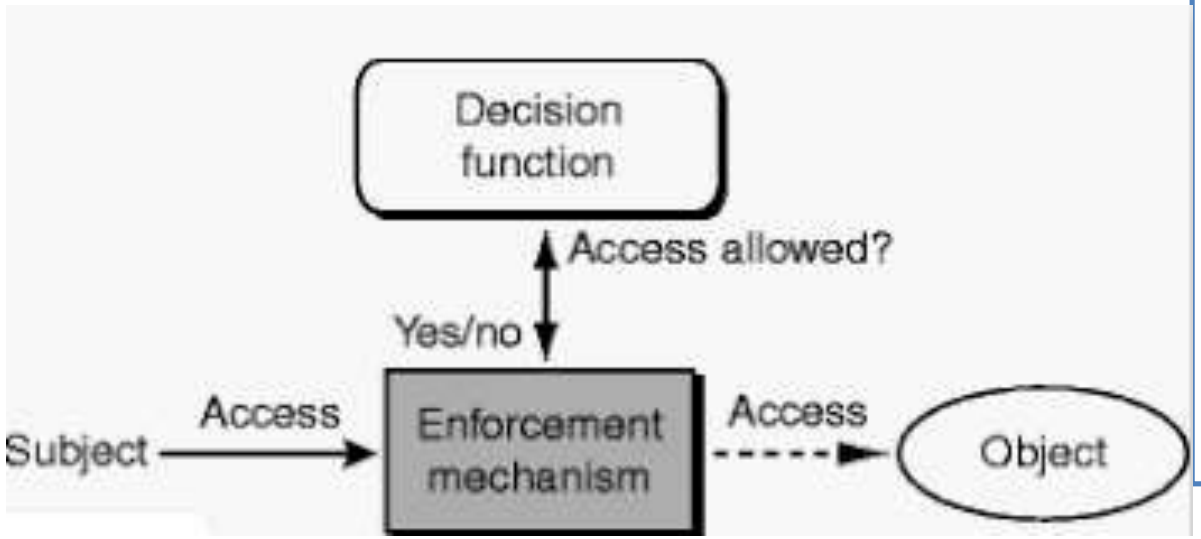
- **Physical access control**: limits access to campuses, building, rooms, and physical IT assets. (Fencing, hardware door locks,… that limit contact with devices)
- **Technical access control**: technology restrictions that limit users on computers from accessing data

**Access controls encompass:**

- ✓ **File permissions**, such as the right to create, read, edit or delete a file.
- ✓ **Program permissions**, such as the right to execute a program.
- ✓ **Data permissions**, such as the right to retrieve or update information in a database.

# Components

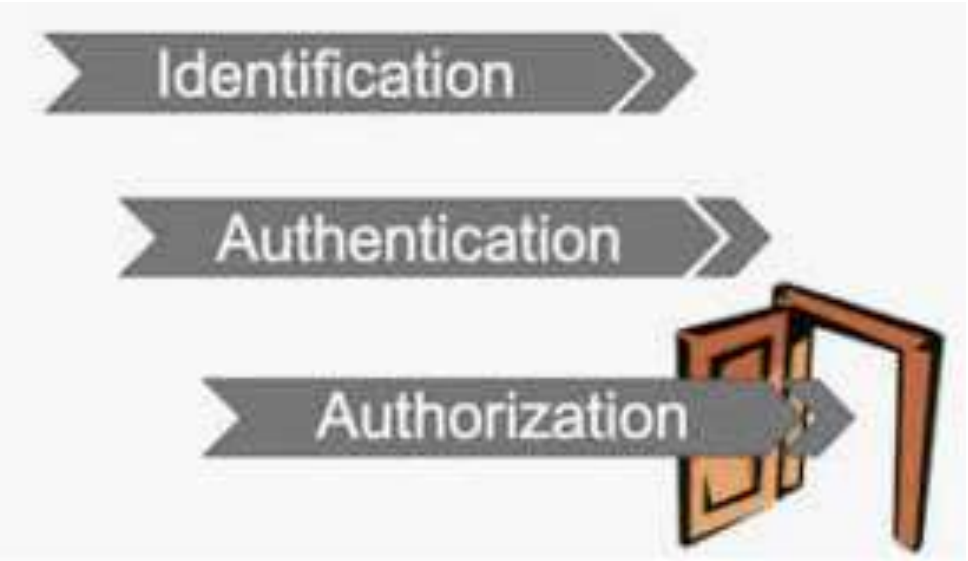
- The security features that control how users and systems communicate and interact with one another.




- **Access:** The flow of information between subject and object
- **Subject:** An active entity that requests access to an object or the data in an object
- **Object:** A passive entity that contains information

# Access Control Terminology

Identification, authorization, and authorization are distinct functions.




- **Identification**

  Method of establishing the subject's (user, program, process) identity.

- **Authentication**

  Method of proving the identity

- **Authorization**

  Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.

# Identification

- Method of establishing the subject's (user, program, process) identity.
  - Use of user name or other public information
  - Know identification component requirements.

- When using identification values to users, the following should be in place:
  - Each value should be unique, for user accountability;
  - A standard naming scheme should be followed;
  - The value should be non-descriptive of the user's position or tasks

# Authentication

- Method of proving the identity
  - ✓Something a person is, has, or does.
  - ✓Use of biometrics, passwords, passphrase, token, or other private information.


- Strong authentication is important

  To be properly authenticated, the subject is usually required to provide a second piece to the credential set (i.e., password, passphrase, key, PIN, token etc(.

# Authorization

- Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.
- Grating access rights to subjects should be based on the level of trust a company has in a subject and the subject's need to know.
- Is a core component of every operating system and established whether a user is authorized to access a particular resource and what actions he is permitted to perform on the resource.

# Authorization

## Access criteria can be thought of as:

- Roles:

  Is an effective way to assign rights to a type of user who performs a certain task (job assignment or function).

- Groups:

  When several users require same type of access to information and resources

- Location:

  To restrict unauthorized individuals from being able to get in and reconfigure the server remotely

- Time:

  Restrict the times that certaun actions or services can be accessed

- Transaction type:

  Can be used to control what data is assesses during certain types of functions and what commends can be carried out on the data

# Authorization

- **Problems in controlling access to assess:**
  - Different levels of users with different levels of access
  - Resources may be classified differently
  - Diverse identity of data
  - Corporate environments keep changing



- **Solutions that enterprise wide and single sign on solutions**
  - User provisioning
  - Password synchronization and reset
  - Centralized auditing and reporting
  - Integrated workflow (increase in productivity)
  - Regulatory compliance

# Access Control models

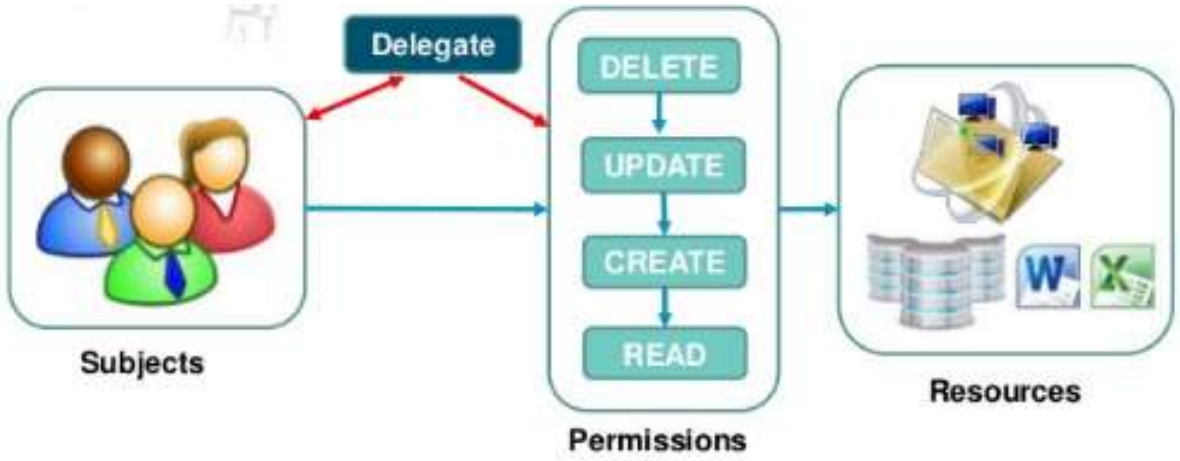
- How does someone grant the right level of permission to an individual so that they can perform their duties? Access control models define how permissions are assigned.
- Access control model – hardware and software predefined *framework* that custodian can use for controlling access
- Access control models have four flavors:
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Role-Based access control
  - Rule-Based access control
  - Attribute-based access control

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

# Mandatory Access Control (MAC)

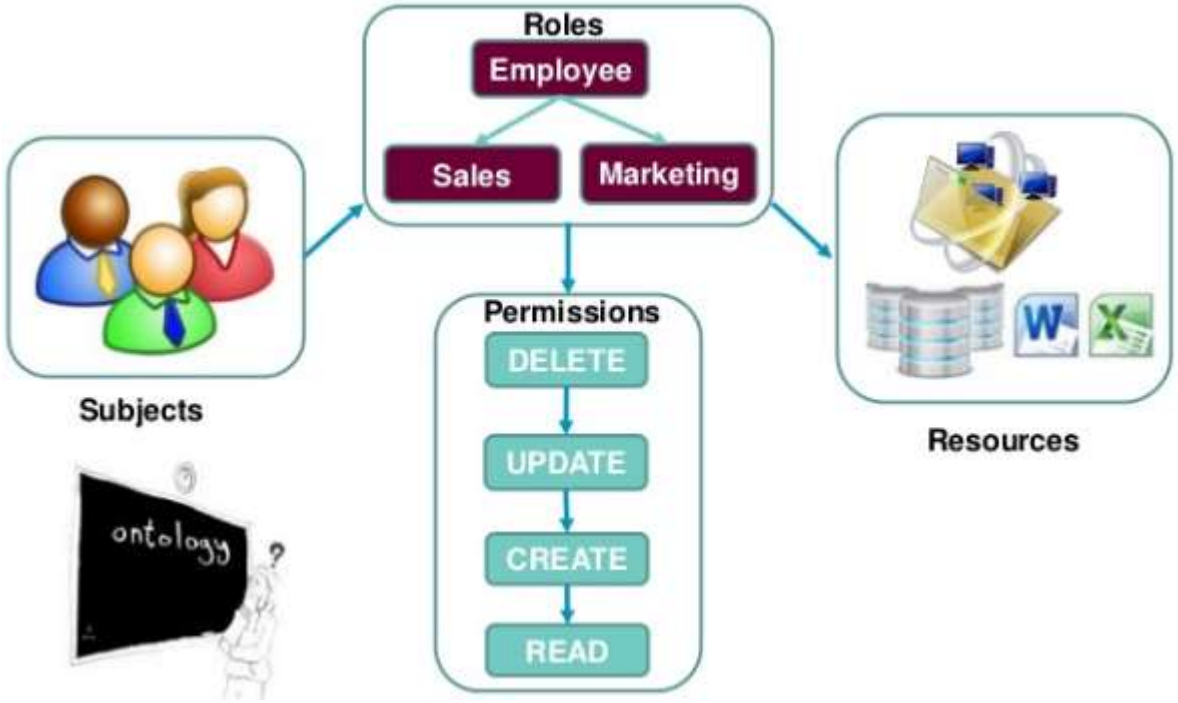
- This is a security model in which access rights are regulated by a central authority based on multiple levels of security.
- This means the end user has no control over any settings that provide any privileges to anyone.

# Discretionary Access Control (DAC)




- DAC allows an individual complete control over any objects they own along with the programs associated with those objects.

# Role-Based Access Control (RBAC)




- Provides access control based on the position an individual fills in an organization.

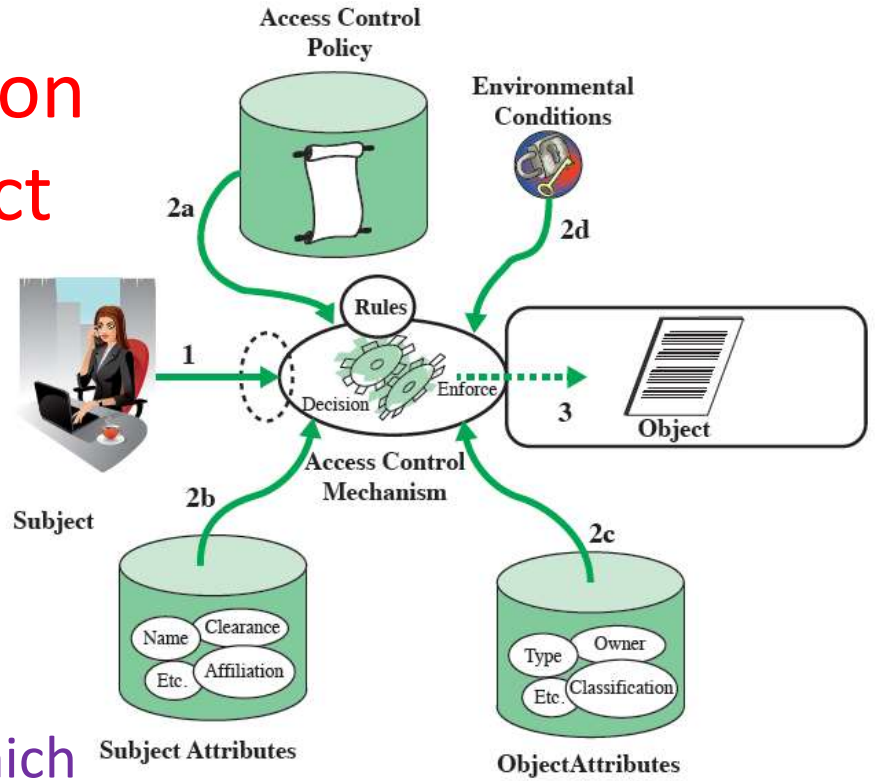

- Restricts access to computer resources based on individuals or groups with defined business functions.

# Rule-Based Access Control

- This is a security model in which the system administrator defines the rules that govern access to resource objects.
- These rules are based on conditions, such as time of day or location.
- 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.

# Attribute-based Access Control (ABAC)

- Define authorizations that express conditions on properties of both the resource and the subject
- Types of attributes
  - Subject attributes: Name, Organization, Job title
  - Object attributes: Title, Author, Date
  - Environment attributes: Describe the operational, technical, and even situational environment or context in which the information access occurs: Current date, Network security level, Current virus/hacker activities



# Implementing Access Control

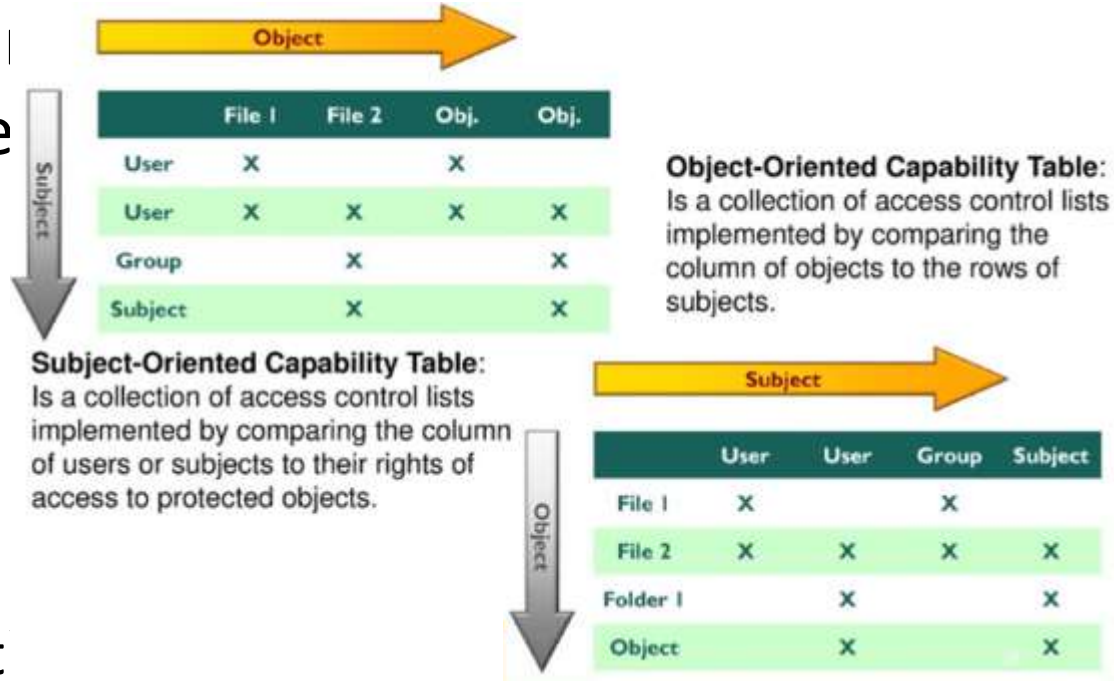
- Access control is a process that is integrated into an organization's IT environment. It can involve identity management and access management systems.
- These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.
- When a user is added to an access management system, system administrators use an automated provisioning system to set up permissions based on access control frameworks, job responsibilities and workflows.
- Access control requirement: **least privilege**

# Access Control Matrix

– Is a table of subjects and objects indicati
what actions individual subjects can take
upon individual objects

– Two types:

- Capability table (bound to a subject)
- Access control List (bound to an object



**Ex1:** Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file **alicerc**, and Bob and Cyndy can read it. Cyndy can read and write the file **bobrc**, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file **cyndyrc**, which she owns. Assume that the owner of each of these files can execute it.

**a. Create the corresponding access control matrix.**

| | alicerc | bobrc | cyndyrc |
|---|---|---|---|
| Alice | --xo | r--- | ---- |
| Bob | r--- | --xo | ---- |
| Cyndy | r--- | rw-- | rwxo |

**b. Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix.**

| | alicerc | bobrc | cyndyrc |
|---|---|---|---|
| Alice | --xo | r--- | r--- |
| Bob | ---- | --xo | ---- |
| Cyndy | r--- | rw-- | rwxo |

Ex2: Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z

a) Write a set of **access control lists** for this situation. Which list is associated with which file?
b) Write a set of **capability lists** for this situation. With what is each list associated?

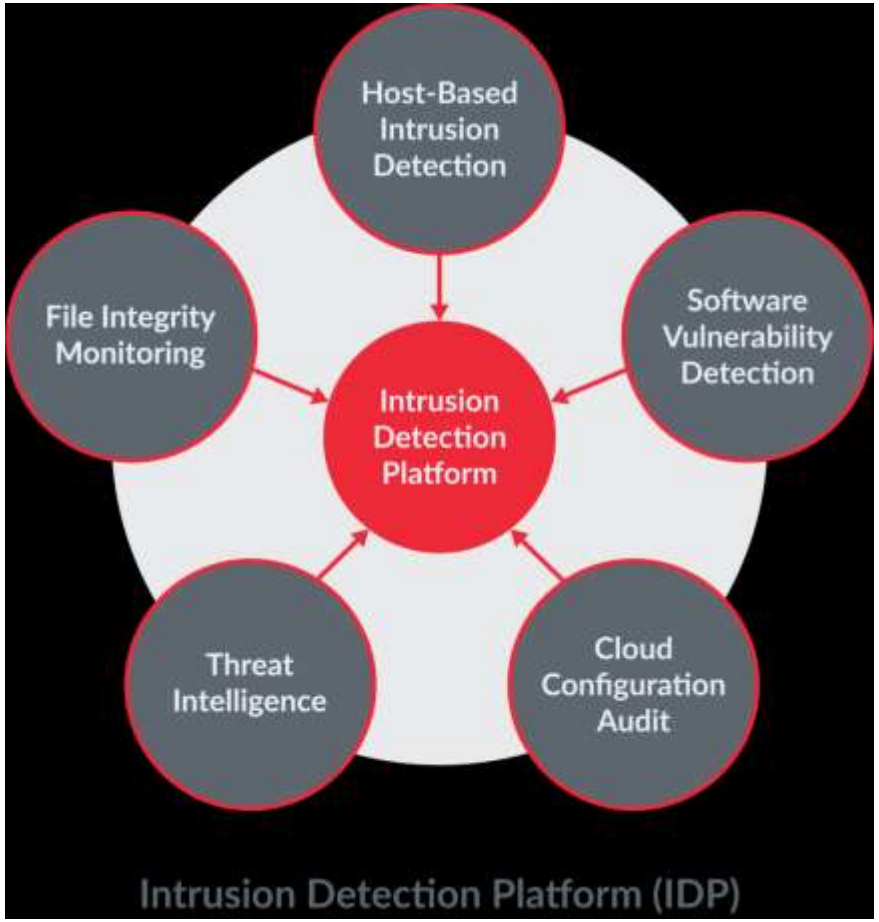
Set of access control lists. They are object focused so each list is associated with a file.
ACL(FileX) = Alice: {read, write}, Bob: {read}
ACL(FileY) = Alice: {read}, Bob: {read, write}
ACL(FileZ) = Alice: {execute}, Bob: {}

Set of capability lists. They are subject focused, so each list is associated with a user.
CList(Alice) = FileX: {read, write}, FileY: {read}, FileZ: {execute}
CList(Bob) = FileX: {read}, FileY: {read, write}, FileZ: {}

# Access Control Monitoring

## Intrusion detection

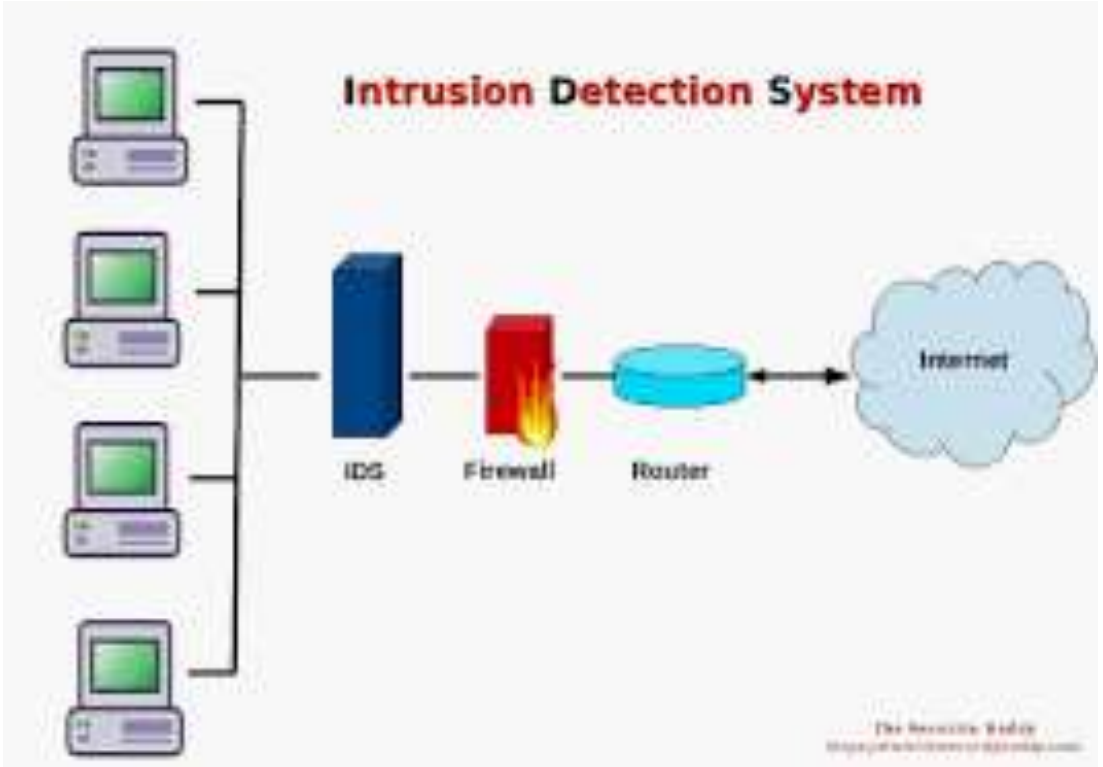
- **Three common components**
  - Sensors
  - Analyzers
  - Administrator Interfaces
- **Common types**
  - Intrusion detection
  - Intrusion prevention
  - Honeypots
  - Network sniffers



# Access Control Monitoring

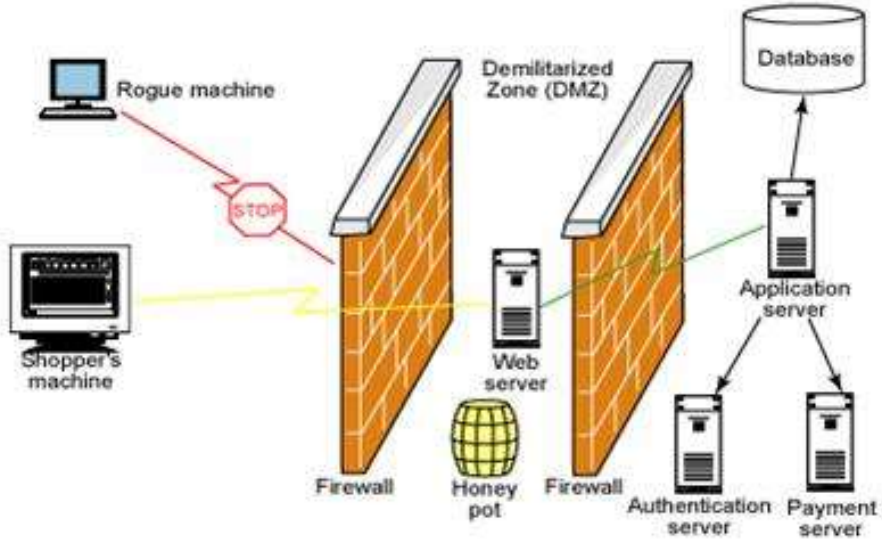
- **Two main types of Intrusion Detection Systems**
  - ✓ Network Based (NIDS)
  - ✓ Host Based (HIDS)

- **HIDS & NIDS can be**
  - – Signature Based
  - – Statistical Anomaly Based
    - Protocol anomaly based
    - Traffic anomaly based
  - – Rule Based



# Access Control Monitoring

- **Intrusion Prevention System**
  - Is a **preventive and proactive** technology, IDS is a detectve technology
  - Two types: Network Based (NIPS) and Host Based (HIPS)
- **Honeypots**
  - An attractive offering that hopes to **lure attackers** away from critical systems
- **Network sniffers**
  - A general term for programs or devices that are **able to examine traffic** on a LAN segment.




# Lab

- Linux: chmod
- Windows: NTFS permission

# Summary

- Access control is a fundamental component of data security.
- Access control policy
- Access control models
- Access control matrix