Access Control Mechanisms

Access Control

- Mechanism to restrict access to resources (files, data, systems) based on permissions
- ***Subjects: H***uman users, often represented by surrogate programs running on behalf of the users.
- ***Objects: T****hings on which an action can be performed: Files, tables,* programs, memory objects, hardware devices, strings, data fields, network connections, and processors are examples of objects.
- ***Access modes:*** *Any controllable actions of subjects on objects, including, but* not limited to, read, write, modify, delete, execute, create, destroy, copy, export and import

Access Control

- **Setting Access policies**: which will then drive all the access control rules.
- **Tracking**: Sometimes administrators need to revisit the access policy to determine whether it is working as it should.
- **Granularity**: the fineness or specificity of access control.
- **Access Logs**: Every access to every object is recorded automatically in log file for later analysis.

Implementing Access Control

- Access control depends on a combination of hardware and software that is
  - Always invoked; validates every access attempt
  - Immune from tampering
  - Assuredly correct
- **Reference monitor: access control that is always invoked, tamperproof, and verifiable.**

Implementing Access Control

- Ensures Confidentiality, Integrity and Availability
- Common Models
  - DAC
  - MAC
  - RBAC
  - ABAC

Mandatory Access Control

- Mandatory Access Control (MAC) is a system to allow or deny access to private information in an organization.
- Access is controlled by a **central authority** based on system-wide policies.
- Works on criteria defined by the administrator.
- Users cannot change permissions.
- Often used in **government, military, and critical systems**.

Mandatory Access Control

- MAC is a pre defined set of capabilities and access to information.
  - Not flexible
  - Most secure model
  - Must be carefully thought out and planned ahead of time.
  - Easy to spot breaches or deviations
- Eg: SELinux – Security Enhanced Linux

Discretionary Access Control

- DAC is identity-based access control.
- DAC mechanisms will be controlled by user identification such as username and password.
- The owner decides who can access (read/write/execute)
- Owner can determine the access privileges.
- Implemented using **Access Control Lists (ACLs)** or file permissions.

Attributes of DAC

- Users can transfer their object ownership to another user.
- The access type of other users can be determined by the user.
- Authorization failure can restrict the user access after several failed attempts.
- Unauthorized users will be blind to object characteristics called file size, directory path, and file name.

MAC vs DAC

Characteristics	MAC	DAC
Access control enforced by	Administrators and operating system	Administrators and users
Form of access control policy	Confidentiality levels and clearances	Access-control lists with user identities
Flexibility	No	Yes
Scalability	No	Yes
Simplicity	No	Yes
Maintenance	Hard	Easy
Implementation Cost	High	Low
Granularity	High (admins adjust clearances for each user and object manually)	High (admins adjust clearances for each user and object manually)

Role Based Access Control

- Access is based on the **user's role** in an organization.
- Roles → Permissions → Users inherit permissions.

Student role: view grades.

Faculty role: upload grades.

Admin role: manage accounts.

Attribute Based Access Control

- Access is based on **attributes** of users, resources, and environment.
- Uses **policies** like: “IF user.department = finance AND access.time < 6PM → allow access”.
- A doctor can view patient records **only if** they are assigned to that patient AND accessing from hospital network.

MAC vs DAC

Easy to use	–	✓
Security level	High	Low
Useful for	Government, military, law enforcement	Small and medium-sized companies
Trusted users	Only administrators	All users
Baseline for gaining access decisions	Tasks and objects that have their own IDs	Ownership and users IDs

Information Flow Control

- Procedure to ensure that information transfers within an information system are not made in violation of the security policy.
- system may track data movement from one location to another and stop it if it isn't wanted.
- What data can be exchanged between entities?
- There is an initiator, a target, and a path for every information flow.
- This might be over a network or merely within a single computer's memory area.
- Ensures that sensitive data does not flow from a higher security context to a lower security context.

IFC – Advantages

- Protecting Private Information

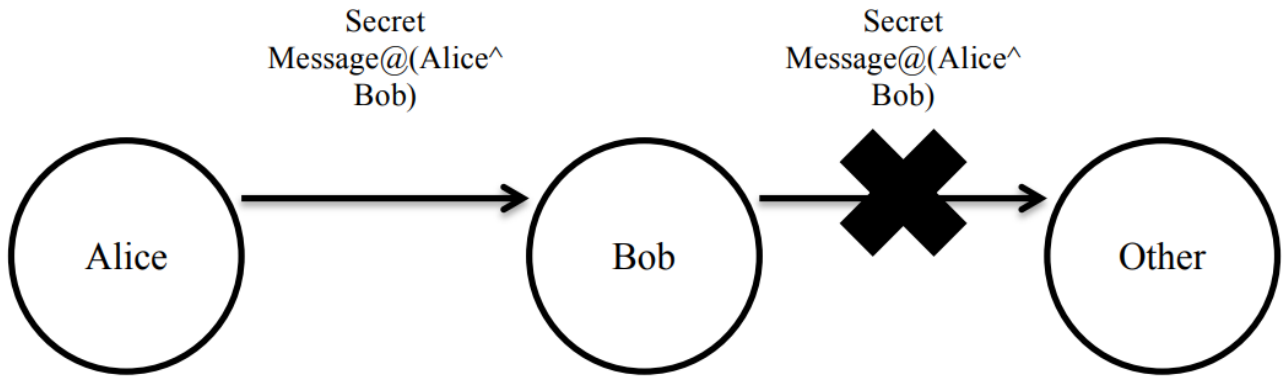

Figure 2: Alice sends Bob a message that is labeled only for the two of them. When Bob tries sending that message to Other, the type system does not let him. Thus preventing a leak in formation

IFC – Advantages

- **Protecting Against Covert Channels**
  - **A *channel*** can be defined as a communication path by which information can flow within a computer system.
- **An overt channel** is one which is designed for the authorised transfer of data.
- **A covert channel** is, by contrast, a path that can allow information to flow in a manner that violates the security policy of a system, allowing the transfer of information by an unauthorised process.

Covert Channel

- Communicate information between two computer processes that are not allowed to communicate, by hiding information into shared resources

Storage Channels

- Involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process

A *storage channel* is a (side or covert) channel that transmits data through some explicit element of the machine or system state, e.g. a register, a shared memory location, or some kernel state such as the scheduler queue.

Covert Timing Channel

- A **timing channel** is one example of a covert channel for passing unauthorized information, in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.

Indentifying Covert Channels

- Shared resource Matrix
  - Since the basis of a covert channel is a shared resource, the search for potential covert channel involves finding all shared resources and determining which processes can write to and read from the resources.
- Information Flow Model
  - Analyzing the information flow, so that the information flow potentials can be detected while a program under development.