TRUSTED SYSTEMS

WHAT IS TRUSTED SYSTEM?

Trusted Systems are special systems designed to serve the purpose of providing security. Safety is ensured by trusted system in a manner by protecting the system against malicious softwares and third party intruders

DATA ACCESS CONTROL

This type of Trusted system provides additional security to the verified process of log-in. It helps in setting permissions for different users, giving them limited access and restricting any additional accesses granted.

- Following successful logon, the user has been granted access to one or set of hosts and applications. This is generally not sufficient for a system that includes sensitive data in its database.

- Through the user access control procedure, a user can be identified to the system. Associated with each user, there can be a profile that specifies permissible operations and file accesses.

- The operating system can then enforce rules based on the user profile.

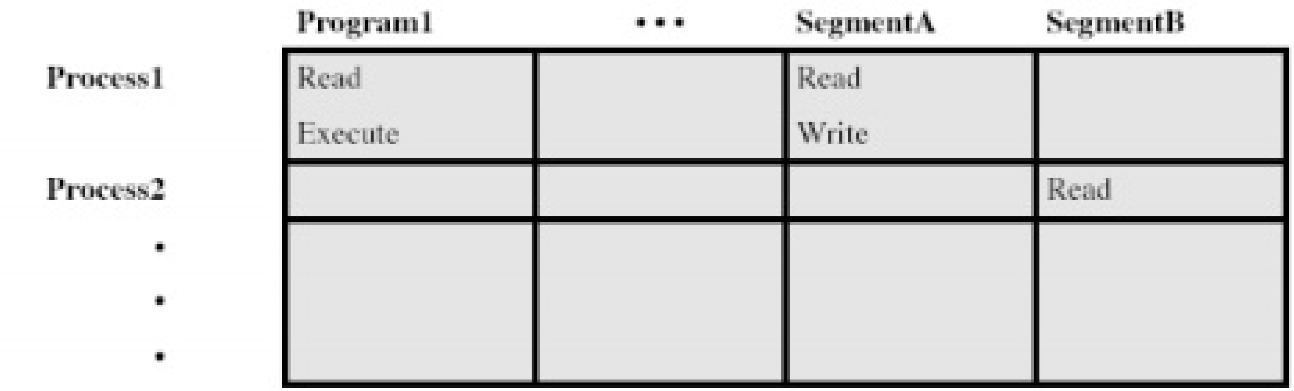
- There are three basic models of Data Access Control

ACCESS MATRIX

They are composed of three parts:-

- Subject:- An entity capable of accessing objects
- Object :-Anything to which access is controlled. Examples include files, portion of files, programs, and segments of memory.
- Access right:-The way in which the object is accessed by a subject. Examples are read, write and execute.

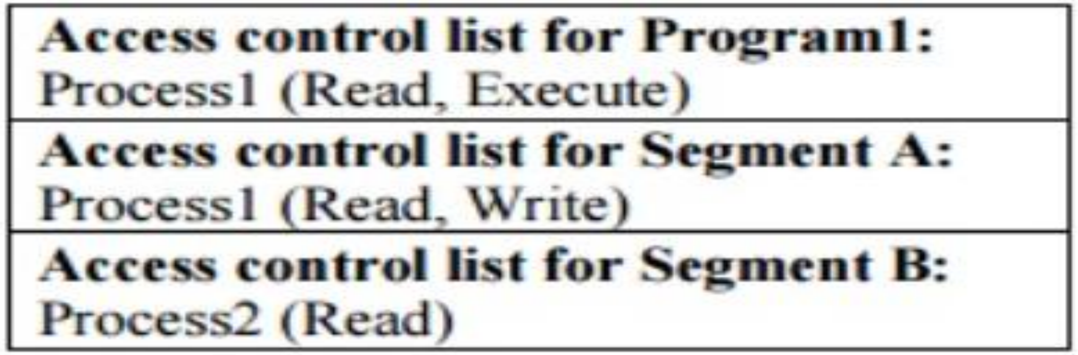
REPRESENTATION:



	Program1	• • •	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
• • •				

- Each entry in the matrix indicates the access rights of that subject for that object.

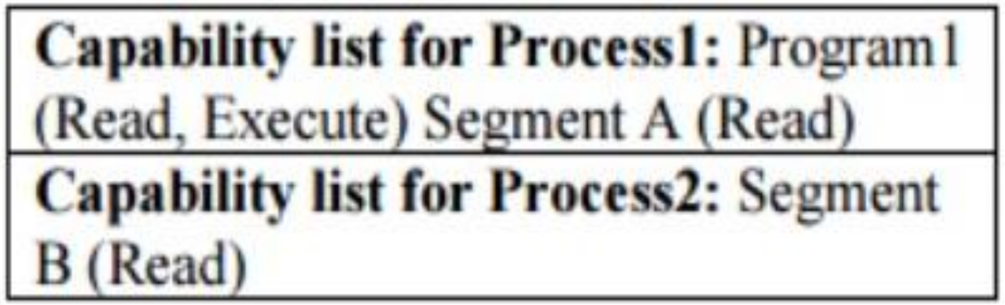
ACCESS CONTROL LISTS



Access control list for Program1: Process1 (Read, Execute)
Access control list for Segment A: Process1 (Read, Write)
Access control list for Segment B: Process2 (Read)

- The matrix may be decomposed by columns, yielding **access control lists.** Thus, for each object, an access control list lists users and their permitted access rights.

Capability List



Capability list for Process1: Program1 (Read, Execute) Segment A (Read)
Capability list for Process2: Segment B (Read)

- Decomposition by rows yields **capability tickets**. A capability ticket specifies authorized objects and operations for a user. Each user has a number of tickets and may be authorized to loan or give them to others.

Multilevel Security

- This type of Trusted system ensures that security is maintained at different levels of the computer system. It ensures that the information is prevented from being at risk.

- The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or noncomparable level unless that flow accurately reflects the will of an authorized user.
  - Top Secret Level
  - Secret Level
  - Confidential Level
  - Unclassified Level

A multilevel secure system must enforce:

- **No read up:** A subject can only read an object of less or equal security level. This is referred to as **simple security property.**
- **No write down:** A subject can only write into an object of greater or equal security level.

Recollect that this is the same concept from one of the security models.
Can you identify the security model?

Reference Monitor concept

- The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object.

- The reference monitor has access to a file, known as the security kernel database that lists the access privileges (security clearance) of each subject and the protection attributes (classification level) of each object.

The reference monitor enforces the security rules and has the following properties:

- **Complete mediation:** The security rules are enforced on every access, not just, for example, when a file is opened.
- **Isolation:** The reference monitor and database are protected from unauthorised modification.
- **Verifiability:** The reference monitor‟s correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation. Important security events, such as detected security violations and authorized changes to the security kernel database, are stored in the audit file

REFERENCE MONITOR

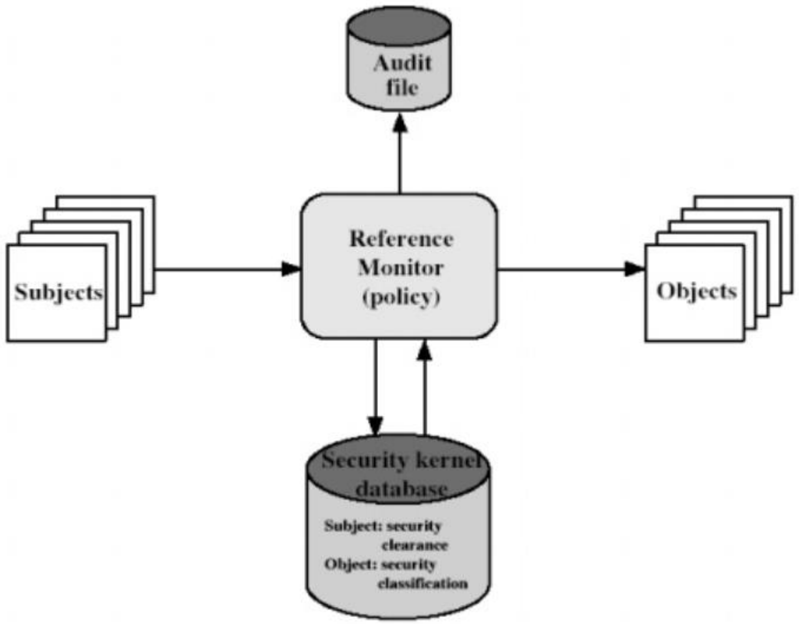

Audit file
Subjects
Reference Monitor (policy)
Objects
Security kernel database
Subject: security clearance
Object: security classification

Fig:Reference Monitor Concept

Summary

- Trusted System description
- Components:
    - Data Access Control
        - Access Control Matrix
        - Access Control List
        - Capability List
    - Multilevel Security
        - Security Models:
            - Bilba, Bell LaPadula, Clark Wilson, Mandatory Access Control, Role-Based Access Control, Discretionary Access Control
    - Reference Monitor
        - Mediation
        - Isolation
        - Verifiability