SLIIT

Discover Your Future

IE2022 - Introduction to Cyber Security

Lecture - 10

Access Control

Mr. Amila Senarathne

Reading Assignment:

- W. Stallings and L. Brown, “Computer Security, Principles and Practice,, Pearson, Chapter 4.
- Other related materials

Access Control

ITU-T Recommendation X.800's definition

Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Access control is a critical element in computer security because the main objective of computer security is

- To prevent unauthorized users from accessing resources
- To prevent legitimate users from accessing unauthorized resources
- To enable users to access resources in an authorized way

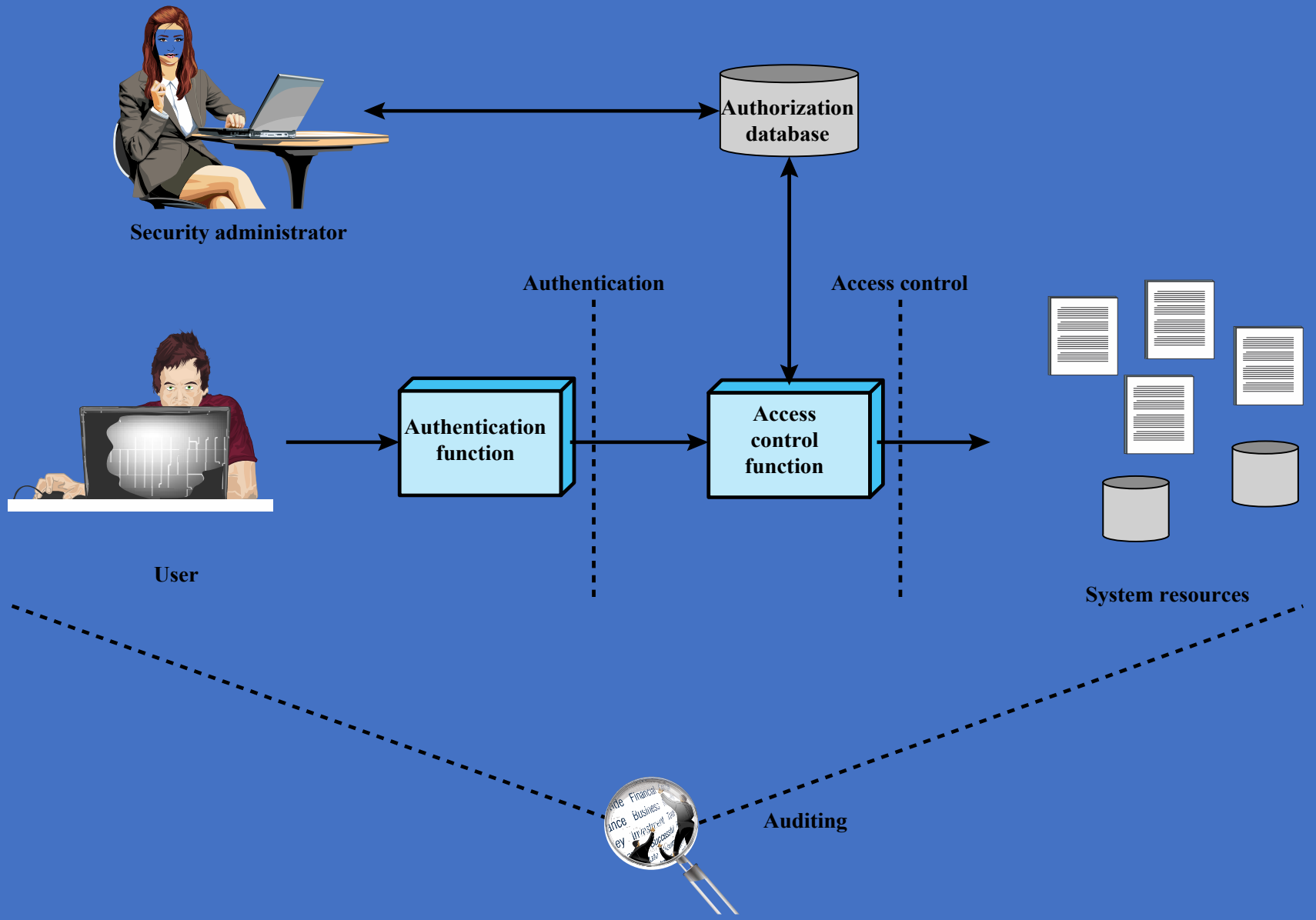


Figure 4.1 Relationship Among Access Control and Other Security Functions

Access Control Policies

An access control policy, which can be embodied in an authorization database, dictates what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following categories:

- **Discretionary Access Control (DAC)**
- **Mandatory Access Control (MAC)**
- **Role-Based Access Control(RBAC)**

Discretionary Access Control (DAC)

Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. This policy is termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

Access Control Policies

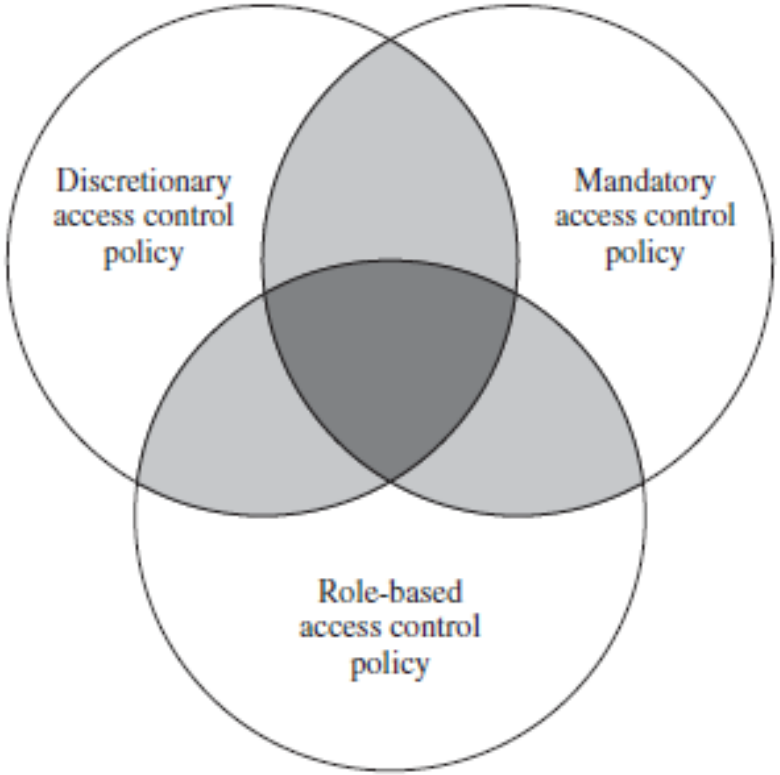
Mandatory access control (MAC):

Controls access based on comparing Security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

Role-based access control (RBAC):

Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

Access Control Policies



DAC, MAC, and RBAC are not mutually exclusive. A system may implement two or even three of these policies for some or all types of access.

Elements of Access Control

- **Subject: an entity that accesses object**

  A subject is an application or a user that is represented by a process in the system that takes on the user's attribute, e.g., access right

  Three classes of subject: owner, group, world

- **Object: the resource which access is to be controlled**

  Example: records, files, mailbox, program, messages

- **Access Right: the way a subject may access an object**

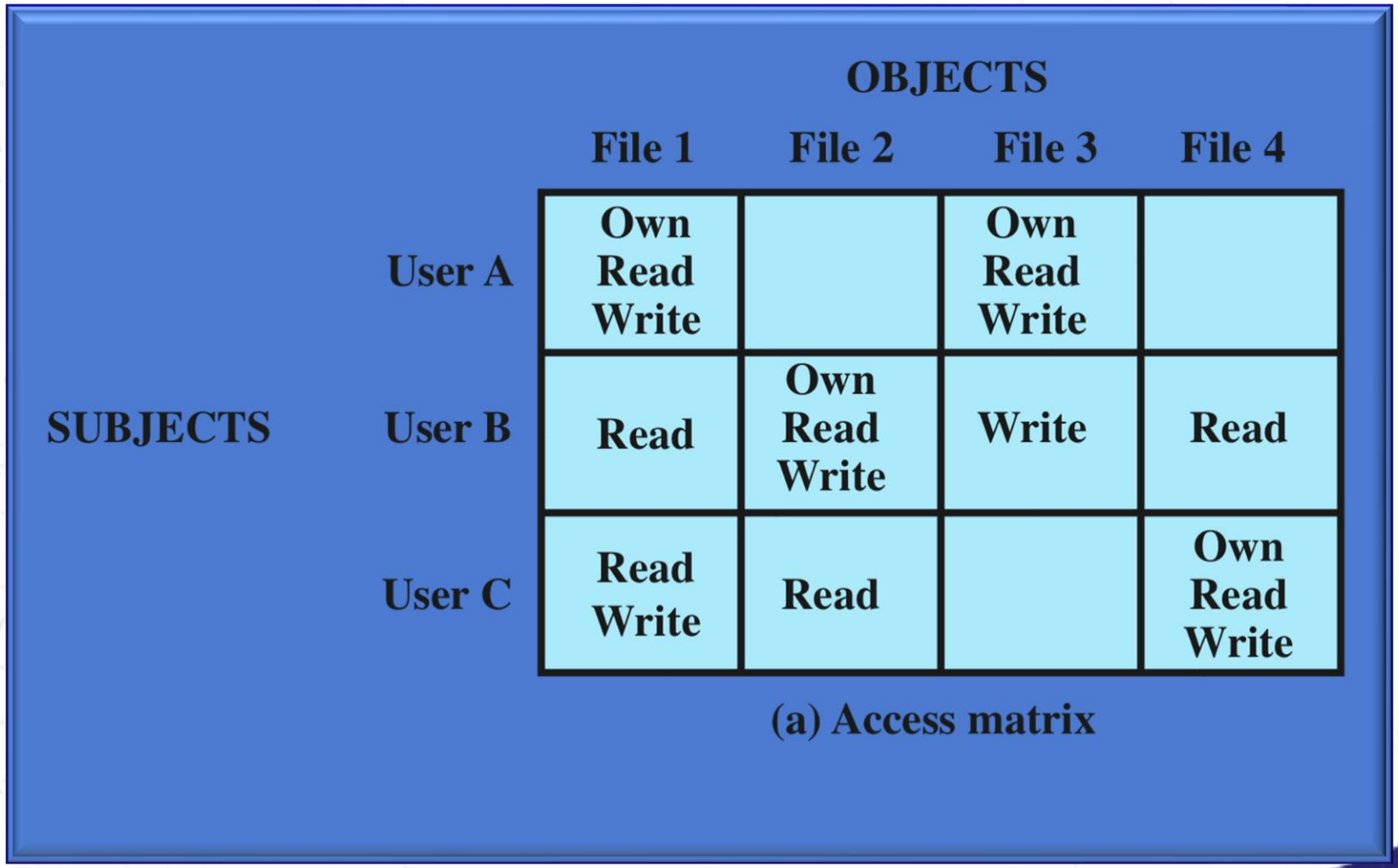
  Access right includes: read, write, execute, delete, create, search

Discretionary Access Control

General access control in OS uses an access matrix

- One dimension (column) consists of subjects that need to access objects
- The other dimension (row) lists the objects that can be accessed
- Each entry in the matrix contains access rights of the subject in that row for the object in that column

Access Matrix



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	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

ACLs and Capability Tickets

Access matrix is usually sparse, and implemented by decomposing it into one or two ways:

- By columns resulting in Access Control Lists (ACLs) for all objects
- By rows resulting in capability list/tickets for all subjects/users

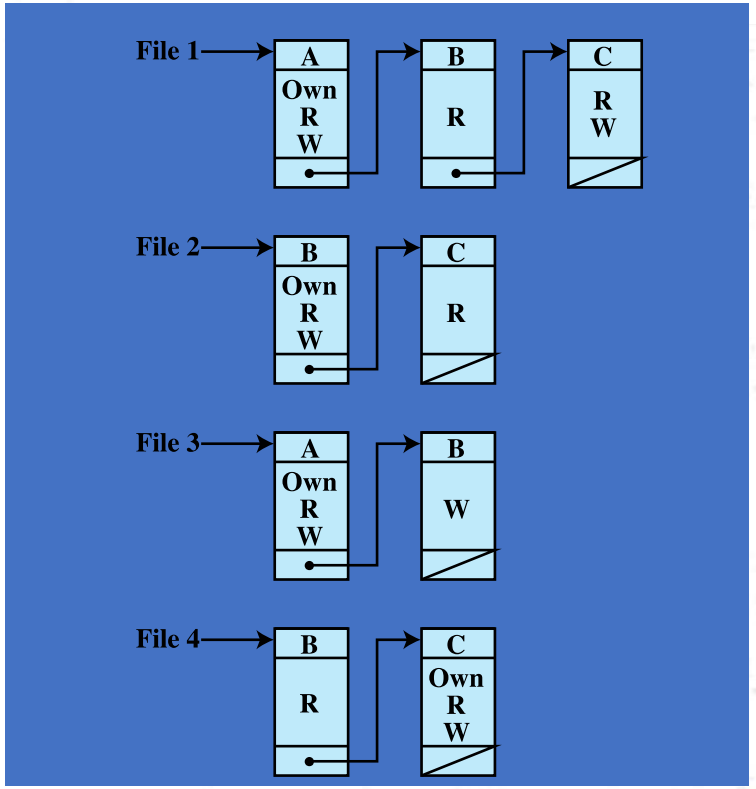
Each list for an object in ACL lists users and their access rights to access the object

- ACL may contain a default or public entry to allow users that are not explicitly listed to have a default access right
- Access rights should follow the least privilege or read-only access
- Elements in the list can be an individual or group users

Access Control Lists (ACLs)

ACL is efficient when we want to know which subjects have what access rights to a particular object

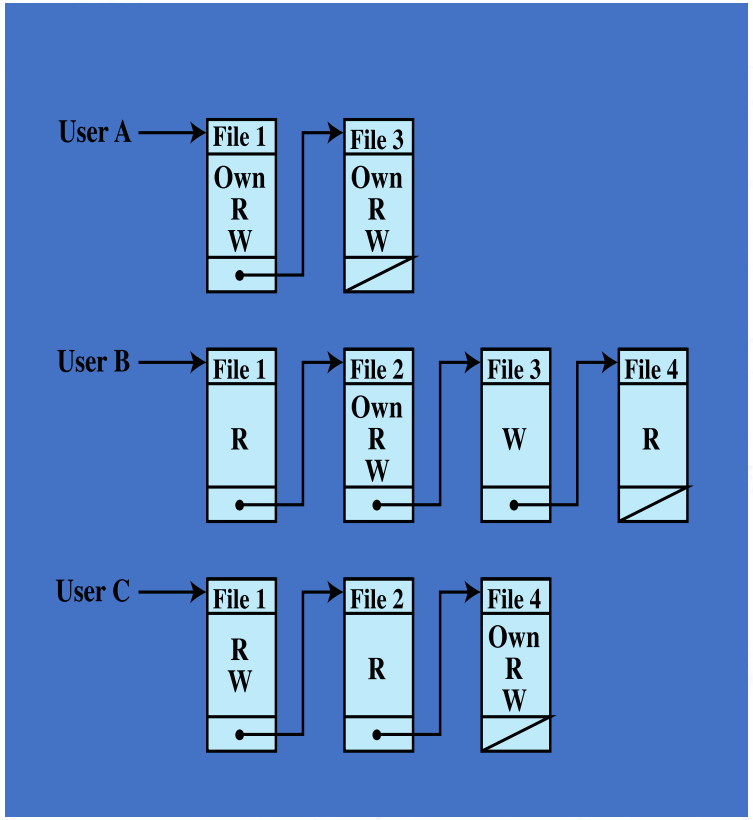
- However, it it harder to determine what access rights a specific user has on which objects



Capability Tickets

Each capability ticket what access rights a particular user has on the objects in the list

- Each user has a number of tickets and they can loan or give the tickets to other users



Capability Tickets

Tickets may be spread around the system

- The tickets cause a greater security problem than ACL

The OS must protect and guarantee the integrity of each ticket; the ticket must be unforgeable

- OS keeps all tickets for the user in a memory region inaccessible by users
- Users must use a system call to request for their tickets

For distributed system, the ticket is in a form of a token

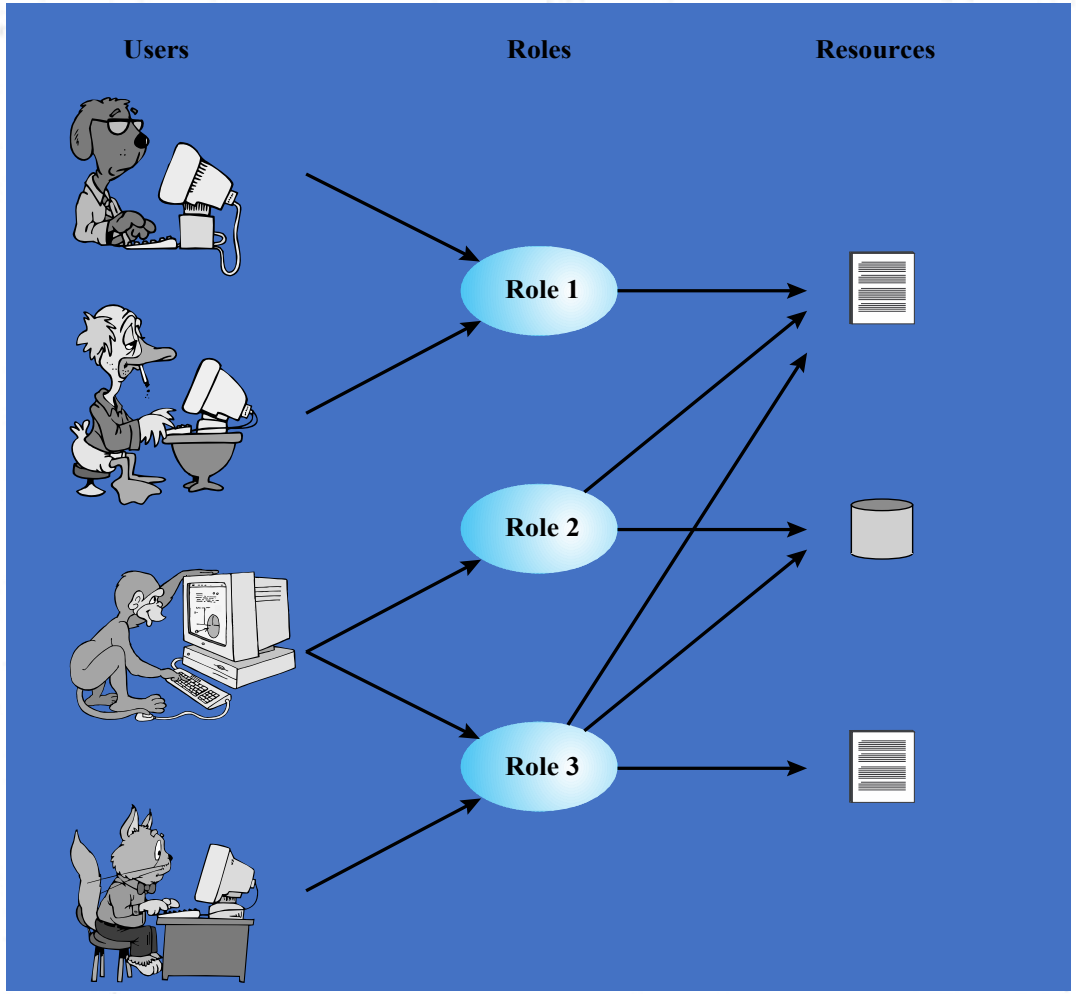
- A token can be a large random password, or a cryptographic message authentication code whose value is verified by the corresponding resource when requesting for access

Role-based Access Control (RBAC)

RBAC defines the access rights based on the roles the users assume in the system rather than the user's identity like in DAC

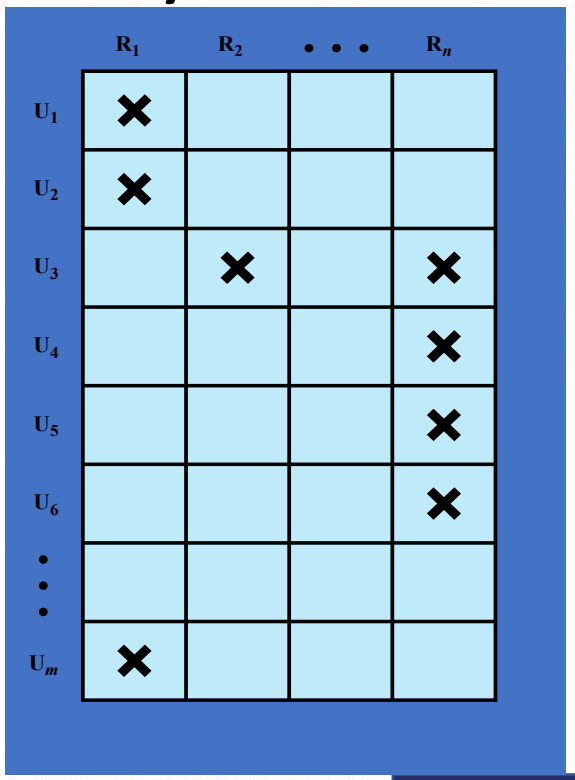
- Role is a job function in the organization
- RBAC assign rights to the roles, not the users
- Users are assigned roles either statically or dynamically
- The relationship between users and roles are many-to-many

Role-based Access Control (RBAC)



Role-based Access Control (RBAC)

- Access matrix representation can be used to describe the key elements of RBAC;



ROLES	OBJECTS								
	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
. . .									
R_n			control		write	stop			

Access Control Requirements

Concepts and features that should be supported by an access control system

- Reliable Input
- Support for fine and coarse specifications
- Least privilege
- Separation of duty
- Open and Closed policy
- Policy combination and conflict resolution
- Administrative policy
- Dual control

Access Control Requirements

Reliable Input

An access control system assumes that a user is authentic; thus, an authentication mechanism is needed as a front end to an access control system. Other inputs to the access control system must also be reliable. For example, some access control restrictions may depend on an address, such as a source IP address or medium access control address. The overall system must have a means of determining the validity of the source for such restrictions to operate effectively.

Access Control Requirements

Support for fine and coarse specifications : The access control system should support fine-grained specifications, allowing access to be regulated at the level of individual records in files, and individual fields within records. The system should also support fine-grained specification in the sense of controlling each individual access by a user rather than a sequence of access requests. System administrators should also be able to choose coarse-grained specification for some classes of resource access, to reduce administrative and system processing burden.

Least privilege : This is the principle that access control should be implemented so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work. This principle tends to limit damage that can be caused by an accident, error, or fraudulent or unauthorized act.

Access Control Requirements

Separation of duty : This is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process. This is primarily a policy issue; separation of duty requires the appropriate power and flexibility in the access control system, including least privilege and fine-grained access control. Another useful tool is history-based authorization, which makes access dependent on previously executed accesses.

Open and closed policies: The most useful, and most typical, class of access control policies are closed policies. In a closed policy, only accesses that are specifically authorized are allowed. In some applications, it may also be desirable to allow an open policy for some classes of resources. In an open policy, authorizations specify which accesses are prohibited; all other accesses are allowed.

Access Control Requirements

Policy combinations and conflict resolution: An access control mechanism may apply multiple policies to a given class of resources. In this case, care must be taken that there are no conflicts such that one policy enables a particular access while another policy denies it. Or, if such a conflict exists, a procedure must be defined for conflict resolution.

Administrative policies: As was mentioned, there is a security administration function for specifying the authorization database that acts as an input to the access control function. Administrative policies are needed to specify who can add, delete, or modify authorization rules. In turn, access control and other control mechanisms are needed to enforce the administrative policies.

Dual control: When a task requires two or more individuals working in tandem.

Questions?

End of Lecture 10