Unit 3
Access Control

Access Control

- The mechanism which defines user access is called *access control*.

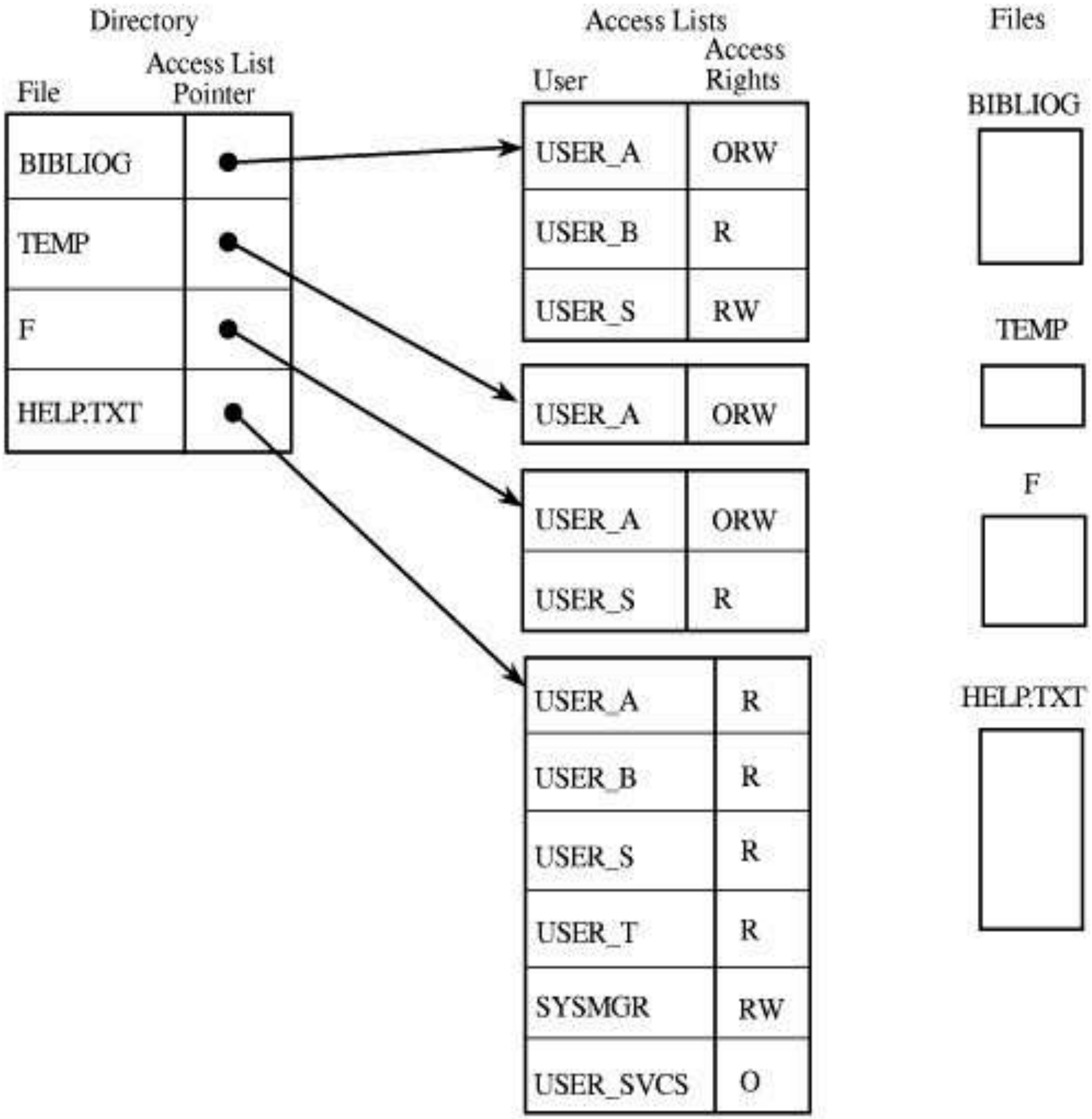
- When the server receives a request, it uses the authentication information provided by the user and the access control instructions (ACIs) to allow or deny access to directory information.

- The server can allow or deny permissions for actions on entries like read, write, search, and compare.

Access Control Principles

- Access control is not a stand alone component of a security system
- Access control coexists with other security services
- Access control works closely with audit control
- Access matrix is a good tool to specify permissions
- Access Control List (ACL) details are placed in Access Matrix

Access Control List



Directory

File	Access List Pointer
BIBLIOG	●
TEMP	●
F	●
HELP.TXT	●

Access Lists

User	Access Rights
USER_A	ORW
USER_B	R
USER_S	RW

User	Access Rights
USER_A	ORW

User	Access Rights
USER_A	ORW
USER_S	R

User	Access Rights
USER_A	R
USER_B	R
USER_S	R
USER_T	R
SYSMGR	RW
USER_SVCS	O

- •There is one such list for each object, and the list shows all subjects who should have access to the object and what their access is.

Discretionary Access Control

- Discretionary Access Control (DAC) is a type of access control in which a user has complete control over all the programs it owns and executes, and also determines the permissions other users have to those files and programs.

- Restricts access to objects based solely on the identity of users who are trying to access them.

- Because DAC requires permissions to be assigned to those who need access, DAC is commonly described as a "need-to-know" access model.

Discretionary Access Control

- Relies on the object owner to control access.
- Strength of DAC: Flexibility
- Limitations of DAC:
  - **Global policy:** DAC lets users to decide the access control policies on their data, regardless of whether those policies are consistent with the global policies.
  - **Information flow:** information can be copied from one object to another, so access to a copy is possible even if the owner of the original does not provide access to the original copy.
  - **Malicious software:** DAC policies can be easily changed by owner, so a malicious program (e.g., a downloaded untrustworthy program) running by the owner can change DAC policies on behalf of the owner.

Mandatory Access Control

- Mandatory Access Control (MAC) is a type of access control in which only the administrator manages the access controls.
- The administrator defines the usage and access policy, which cannot be modified or changed by users, and the policy will indicate who has access to which programs and files.
- MAC is most often used in systems where priority is placed on confidentiality.

Role-based Access Control

- Role-based access control (RBAC) is a type of access control in which access is based on the roles of individual users within an enterprise.
- Roles are defined according to job competency, authority, and responsibility within the enterprise.
- A user has access to an object based on the assigned role.
- The object is concerned with the user’s role and not the user.
- Role of the user in the organization determines the access level for the database
- Roles can define specific individuals allowed access or extent of access to resources for multiple individuals

Role-based Access Control

- RBAC supports the following security principles:
  - Least privilege (only the needed permissions are assigned to roles)
  - Separation of duties (use of mutually exclusive roles – e.g., accountant writes cheque and manager signs the cheque)
  - Data Abstraction (instead of read/write/execute permissions such as credit/debit are established)
- RBAC is independent of MAC and DAC
- RBAC can support MAC and DAC separately

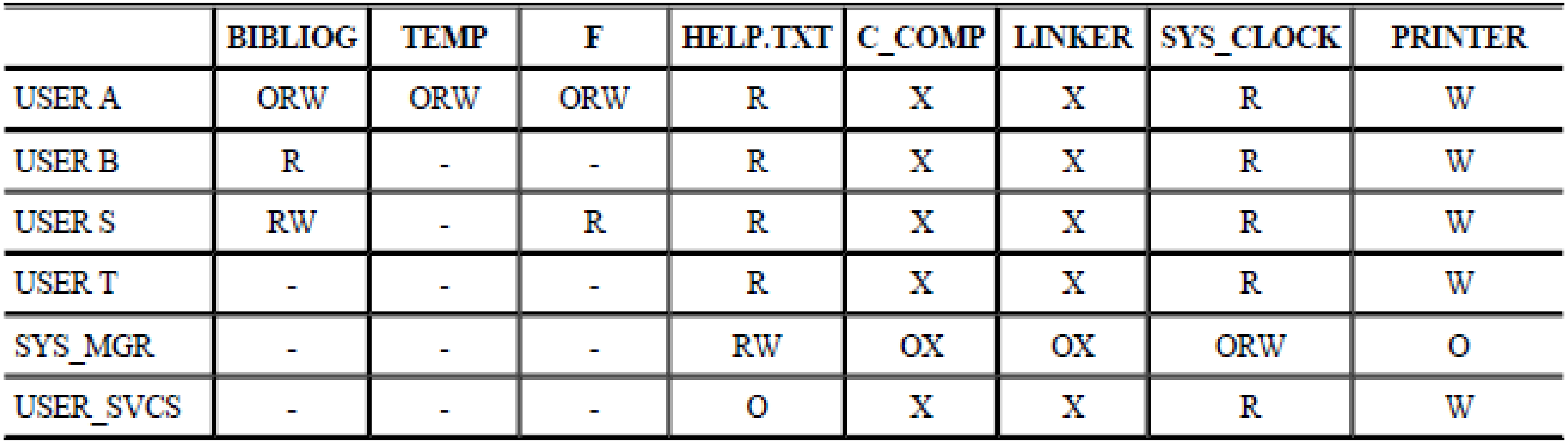
Access control matrix model

- The *access control matrix model* is the most precise model used to describe a protection state.
- It characterizes the rights of each *subject* (active entity, such as a process) with respect to every other entity.

Matrix Model

- Matrix model consists of:
  - Objects (data)
  - Subjects (user processes like queries)
  - Rights (permissions for read, etc)
- Rows of the matrix are objects and columns are subjects and the content of each cell is the rights
- Protection domain consists of a collection of access rights

Table 4-1. Access Control Matrix.



	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	-	-	R	X	X	R	W
USER S	RW	-	R	R	X	X	R	W
USER T	-	-	-	R	X	X	R	W
SYS_MGR	-	-	-	RW	OX	OX	ORW	O
USER_SVCS	-	-	-	O	X	X	R	W

Matrix Model

- Matrix model consists of:
  - Access lists

    Access list identifies people who have access to a particular object
  - Capability lists

    Capability list identifies each object and its operations

- A **capability** is an unforgeable token that gives the possessor certain rights to an object.

- The algebra allows policies to be restricted (by posing constraints on their authorizations) and closed with respect to inference rules