Subject

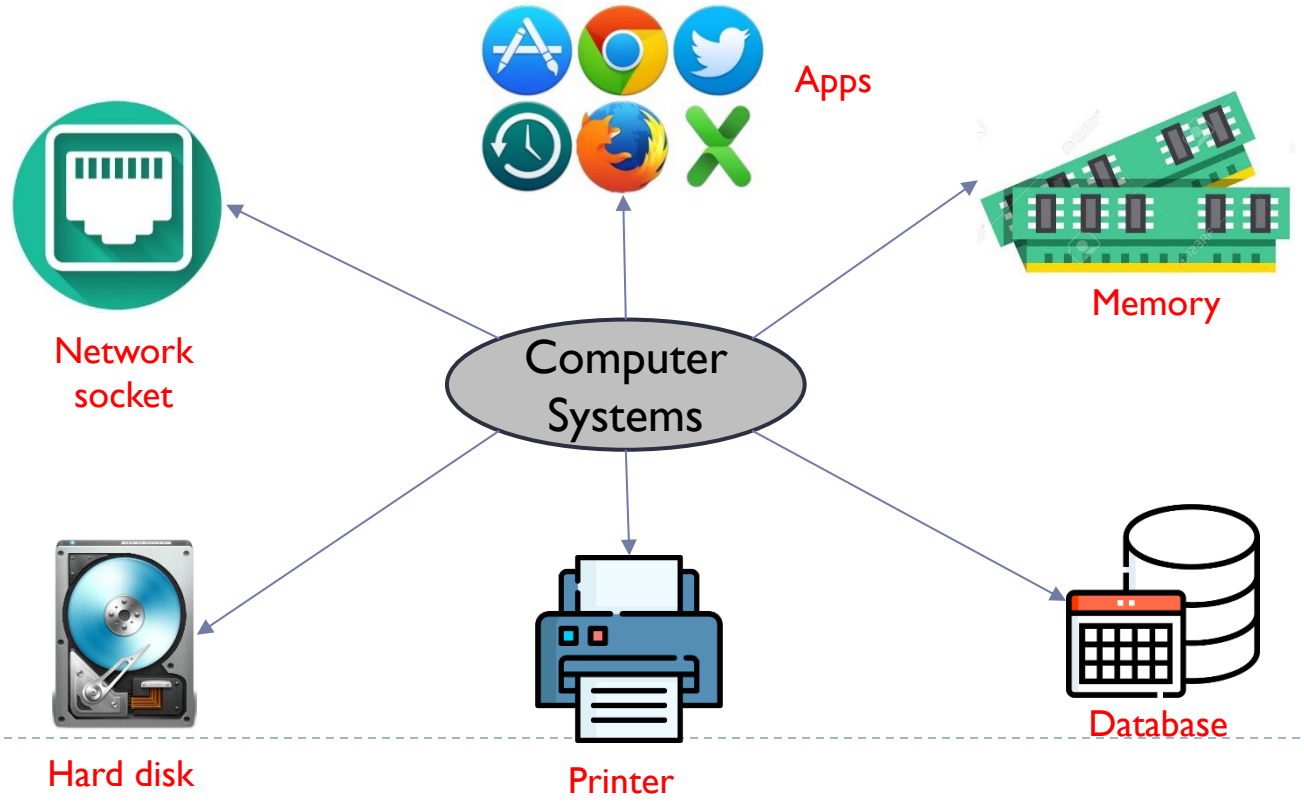
A subject is typically held accountable for the actions they have initiated. There can be three types of subjects.

- **Owner:** this may be the creator of a resource. For system resources, ownership may belong to a system administrator.
- **Group:** in addition to individual users, privileges can also be assigned to a group of users. A user joining the group will automatically have the corresponding privileges, while a user quiiting the group will loss the corresponding permissions. A user may belong to multiple groups. The concept of groups makes it easier to manage and update the permissions.
- **Other:** the least amount of access is granted to users who are able to access the system but are not included in the categories of owner and group for this resource.

Object

An object is a resource to which access is controlled.

- An entity used to contain and/or receive information.
- Examples: records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs.



Operation

Describes the way in which a subject may access an object

- Read: user may view information in a system resource (e.g., a file, selected records in a file, selected fields within a record, or some combination). Read access includes the ability to copy or print.
- Write: user may modify data in the system resource (e.g., files, records, programs).
- Execute: user may execute specified programs.
- Delete: user may delete certain system resources, such as files or records.
- Create: user may create new files, records, or fields.
- Search: user may list the files in a directory or otherwise search the directory.

Access Control Matrix

A popular implementation of access control policy.

- One dimension consists of identified subjects that may attempt access to the resources
- The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

Objects

Subjects	File 1	File 2	File 3	File 4
User A	Read Write Execute		Read Write Execute	
User B	Read	Read Write Execute	Write	Read
User C	Read Write	Read		Read Write Execute

Update Access Control Matrix

Possible changes over Access Control Matrix

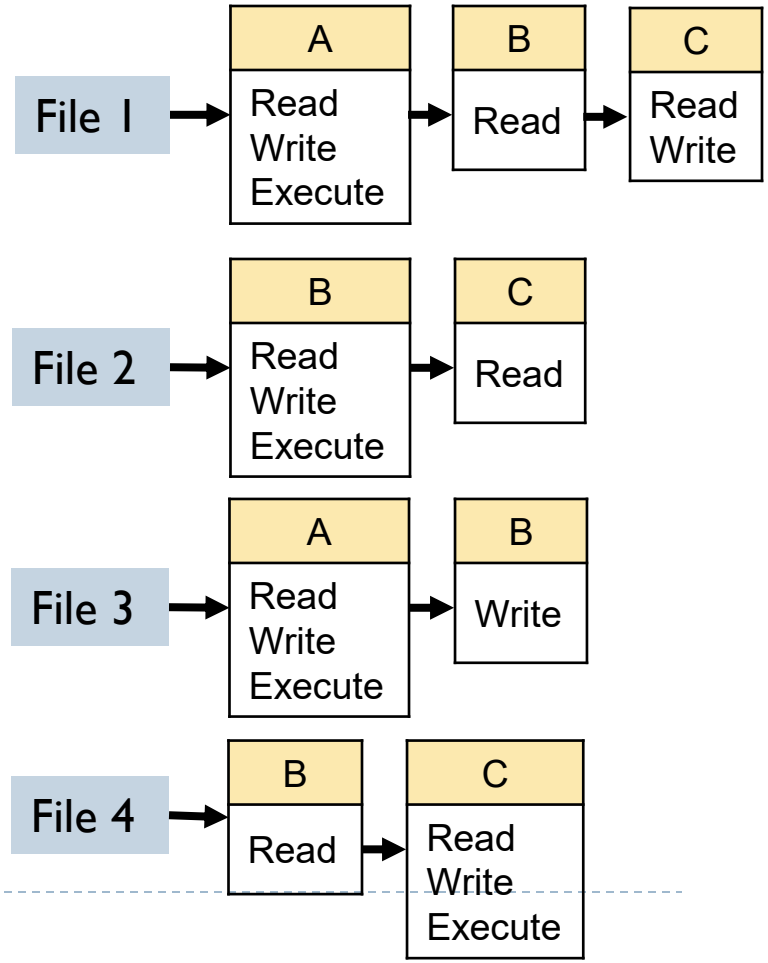
- Create subject s: add a new row *s*. This is typically done by the system administrator.
- Create object o: create a new column *o*. This is typically done by the system administrator.
- Grant permission r for subject s over object o: enter *r* to entry $M_{s,o}$. This is typically done by the resource owner or system administrator.
- Revoke permission r for subject s over object o: delete *r* from entry $M_{s,o}$. This is typically done by the resource owner or system administrator.
- Destroy subject s: delete the row *s*. This is typically done by the system administrator.
- Destroy object o: deletes the column o. This is typically done by the system administrator.

Access Control List (ACL)

In practice, an access control matrix is usually sparse and can be implemented by decomposition in one of two ways

Decomposition by columns

- For each object, ACL lists users their permitted access rights.
- ACL is convenient when determining which subjects have which access to a particular resource.

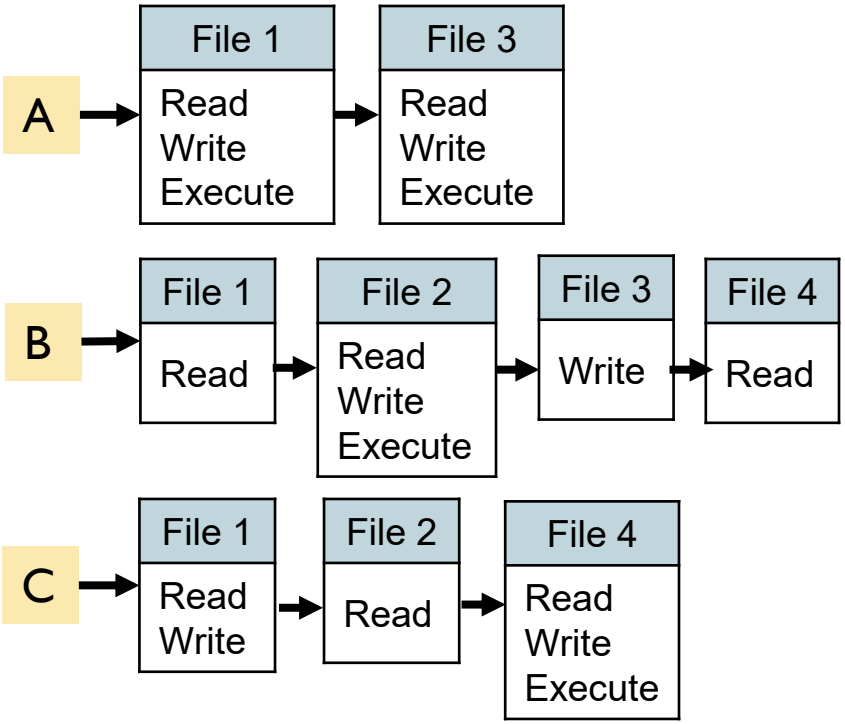


Capability List (C-List)

In practice, an access control matrix is usually sparse and can be implemented by decomposition in one of two ways

Decomposition by rows

- C-list specifies authorized objects and operations for a particular user.
- C-List is convenient when determining the access rights available to a specific user.



Example: Resource Management in Unix OS

Files, directories, memory devices, I/O devices are uniformly treated as resources

- These resources are the objects of access control.
- Each resource has a single user owner and group owner