Protection and Security

- Protection is any mechanism for controlling the access of processes to the resources of a computer system. This mechanism must provide a means for specification of the control to be imposed and a means of enforcement.

- Security ensures user authentication preventing malicious destruction or alteration of the information stored in a computer system.

Protection

• A general protection system may be subdivided in three levels

- ❑ models
- ❑ policies
- ❑ mechanisms

Models

• The protection model defines the subjects, the objects to which the subjects may access and the access rights, that is the operations by which subjects can access to objects.

• The subjects are the active part of the system (processes)

• The objects are the passive part of the system (physical and logical resources).

•A subject may have access rights either to objects or other subjects (a process can control other processes) .

• A process has different access rights to objects, depending on what task is currently doing.

• The particular set of rigts a process has at any given time is referred to as its protection domain.

Policies

The protection policy define the rules by which the subjects can access to the objects:

• Discretional access control (DAC). The owner of an object controls the access rigths for that object. (UNIX).

• Mandatory access control (MAC). The access rigths are centrally managed (hospital organizations). Rules are defined in order to establish the access rights of the users. The rules cannot be modified by the users.

• Role Based Access Control (RABC). Specific access rights are assigned to useres depending to their role in the organization. A user can belong to different roles.

Mechanisms and policies are different concepts

Example:

- UNIX provides a *mechanism* to define for each file three bits (*read, write and execute)* for the *owner* of the file*,* for the *group* and for the *others*

- The user defines the value of the three bits (*policy*)

Changing the protection state

Standard dual mode (monitor-user mode)

• Two protection state:user mode and monitor o kernel mode.

• Domain changing associated to the system calls

• When a process must execute a privileged instruction (access to files, I/O operations…) a change of domain happens.

•It is not possible to have protection among users.

Access matrix

	O1	O2	O3
S1	read,write	execute	write
S2		execute	read,write,

Access matrix implementation

:

- Matrix dimension
- Sparse matrix

Access Control List (ACL).

The matrix may be decomposed by columns: to each object an access control list is associated. It contains all the subjects that can access to the object and the permitted access rigths.

.Capability List

The matrix is decomposed by rows: to each subject is associated a list that contains the objects accessible by the the subject and the relative access rights.