The Access Control Matrix

Subjects \ Objects	1	2	3	4	5
1		R		R	
2			R,W		R,W
3	R,X	R,W	R,W		
4			R		

objects: the things to be protected, e.g., files

subjects: users, groups, roles

matrix entries: access rights, i.e., operations allowed by a subject on an object

A common implementation is an *access control list* for each object.

Access Control Administration

- there must be a mechanism for changing the access rights describe in the access control matrix
  - set of subjects is dynamic
  - set of objects is dynamic
  - access rights may need to change
- some approaches
  - encode access control change rights in the access control matrix
    - add "owner" as a possible access right. Subject with owner rights on object x can change access rights in x's column.
  - new users/subjects can inherit rights from others

Example: Access Rights in Unix

- subjects are users and groups (group membership is maintained separately)
- each object has an owner and a group
- access rights are specified for the owner, for the group, and for everyone else
- object access rights can be modified by the object owner
- major access rights are read, write, and execute
- access controls can be applied to files, devices, shared memory segments, and more.

Authentication

- object access is performed by processes
- to apply access controls, it is necessary to associate processes with users
- this requires user *authentication*
- some authentication techniques:
  - passwords
  - cryptographic (e.g., public key methods)
  - physical tokens (e.g., smart cards)
  - biometrics