CS ??? Computer Security

Access Control

Lecture slides by Lawrie Brown
Modified By Yasser F. O. Mohammad

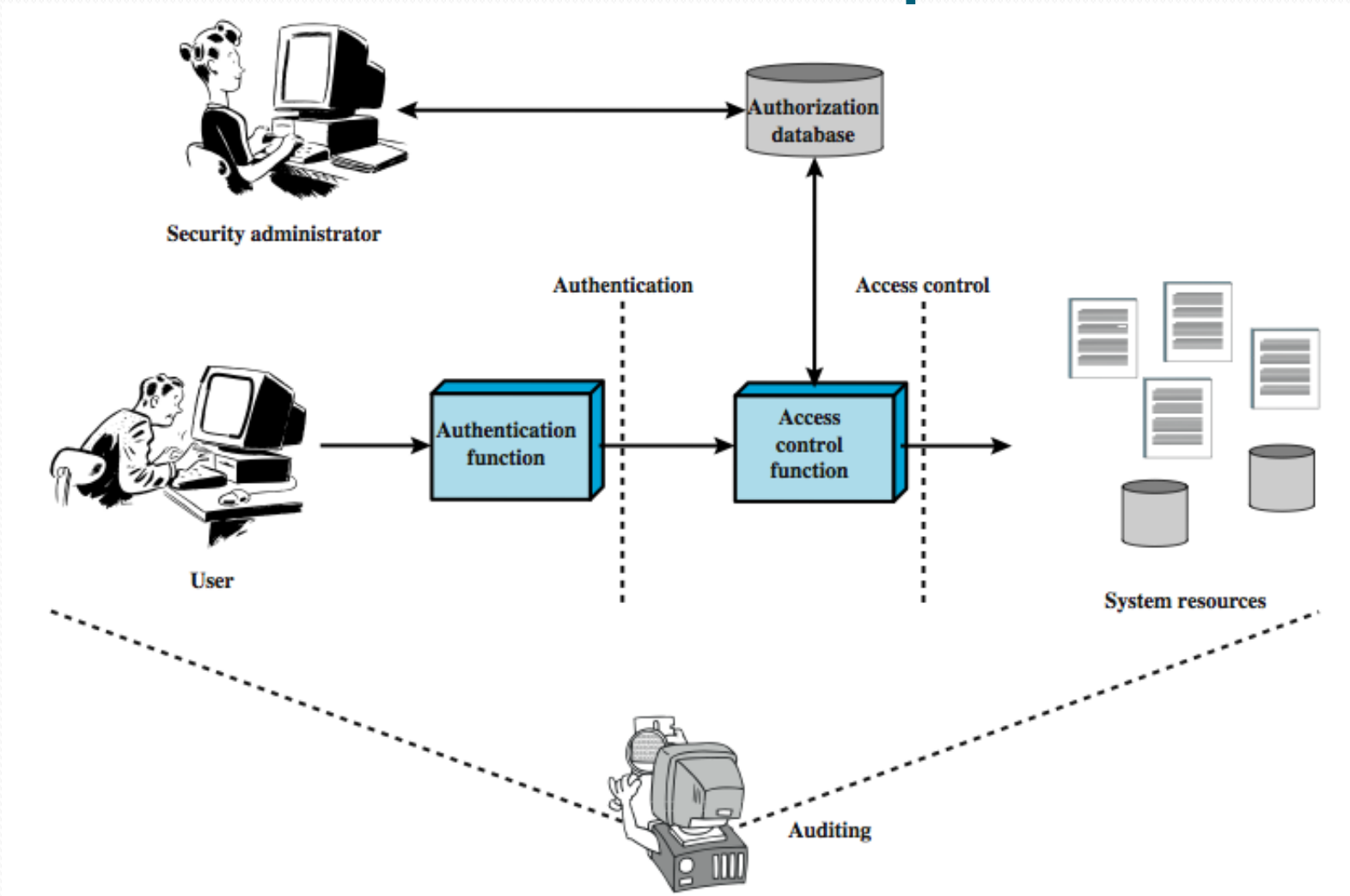
Notice

- We will have a quiz by the end of this lecture in the content of THIS lecture
- This will be the rule from now on!!!
- Be attentive

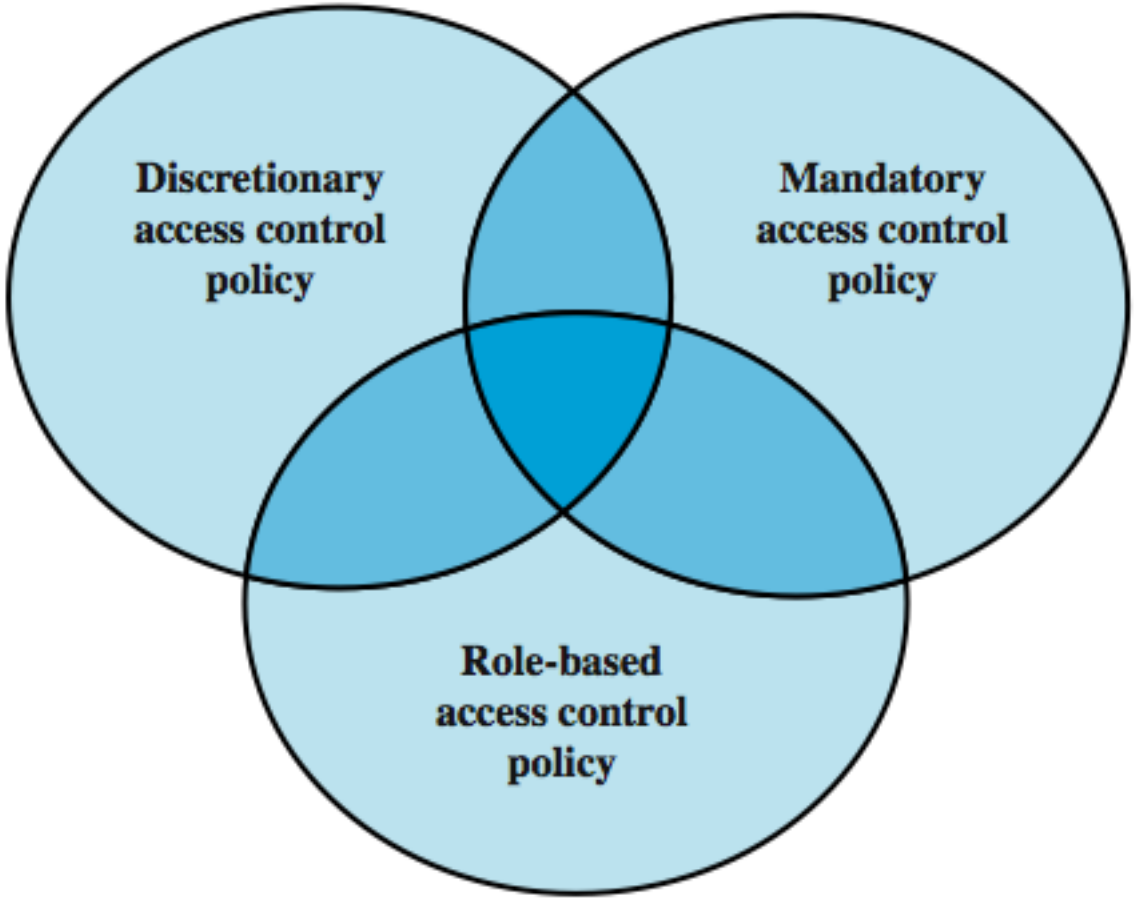
Access Control

- “The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner“
- central element of computer security
- assume have users and groups
  - authenticate to system
  - assigned access rights to certain resources on system

Access Control Principles



Access Control Policies



Access Control Requirements

- reliable input
- fine and coarse specifications
- least privilege
- separation of duty
- open and closed policies
- policy combinations, conflict resolution
- administrative policies

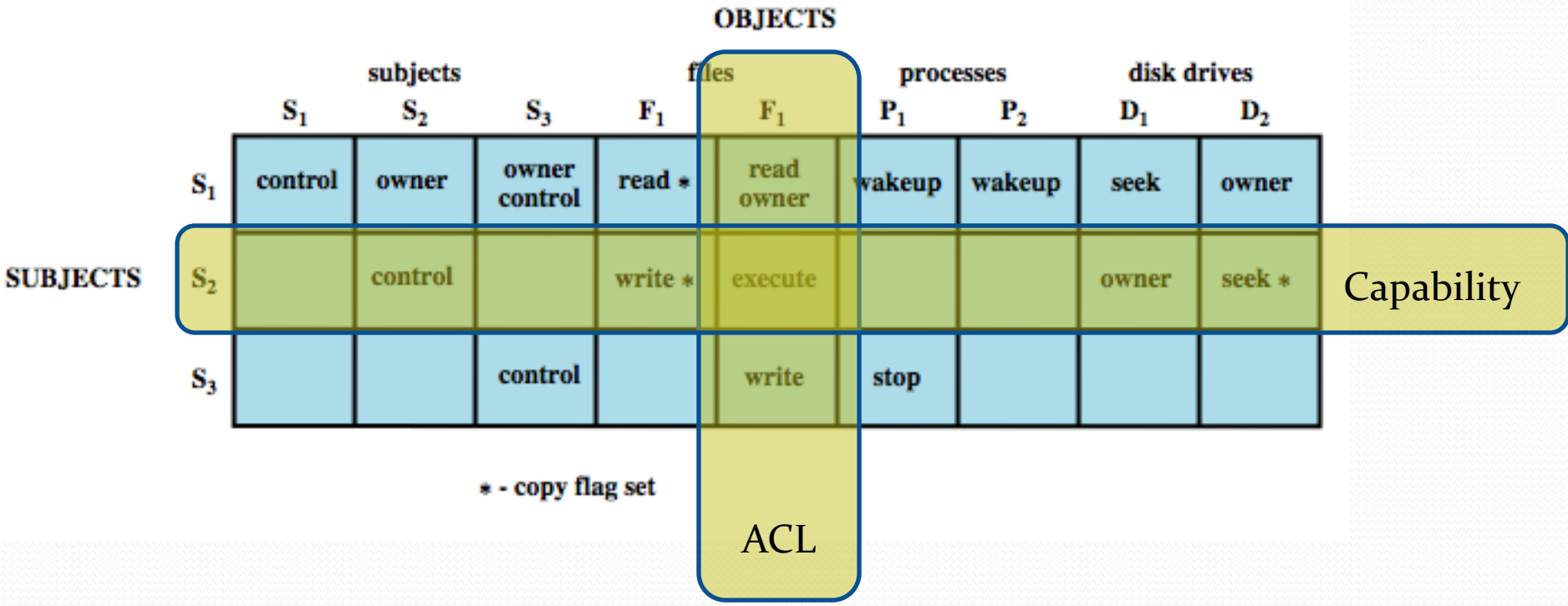
Access Control Elements

- subject - entity that can access objects
  - a process representing user/application
  - often have 3 classes: owner, group, world
- object - access controlled resource
  - e.g. files, directories, records, programs etc
  - number/type depend on environment
- access right - way in which subject accesses an object
  - e.g. read, write, execute, delete, create, search

Discretionary Access Control

- often provided using an access matrix
  - lists subjects in one dimension (rows)
  - lists objects in the other dimension (columns)
  - each entry specifies access rights of the specified subject to that object
- access matrix is often sparse
- can decompose by either row or column

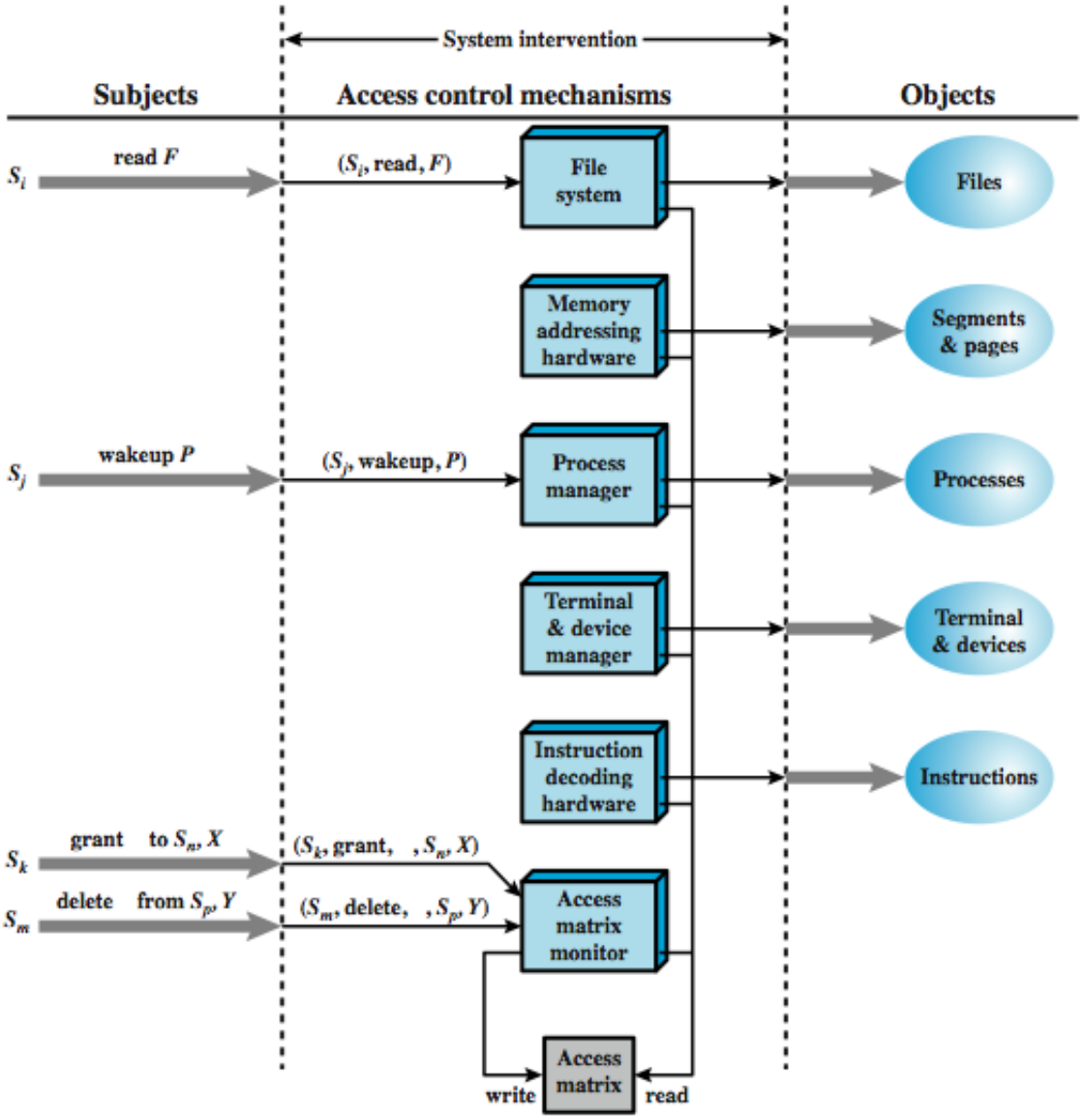
Access Control Model



DISCUSSION POINTS

- Capabilities vs. ACLs
- Closed vs. Open systems
- Should we have both *allow* and *deny* attributes?

Access Control Function



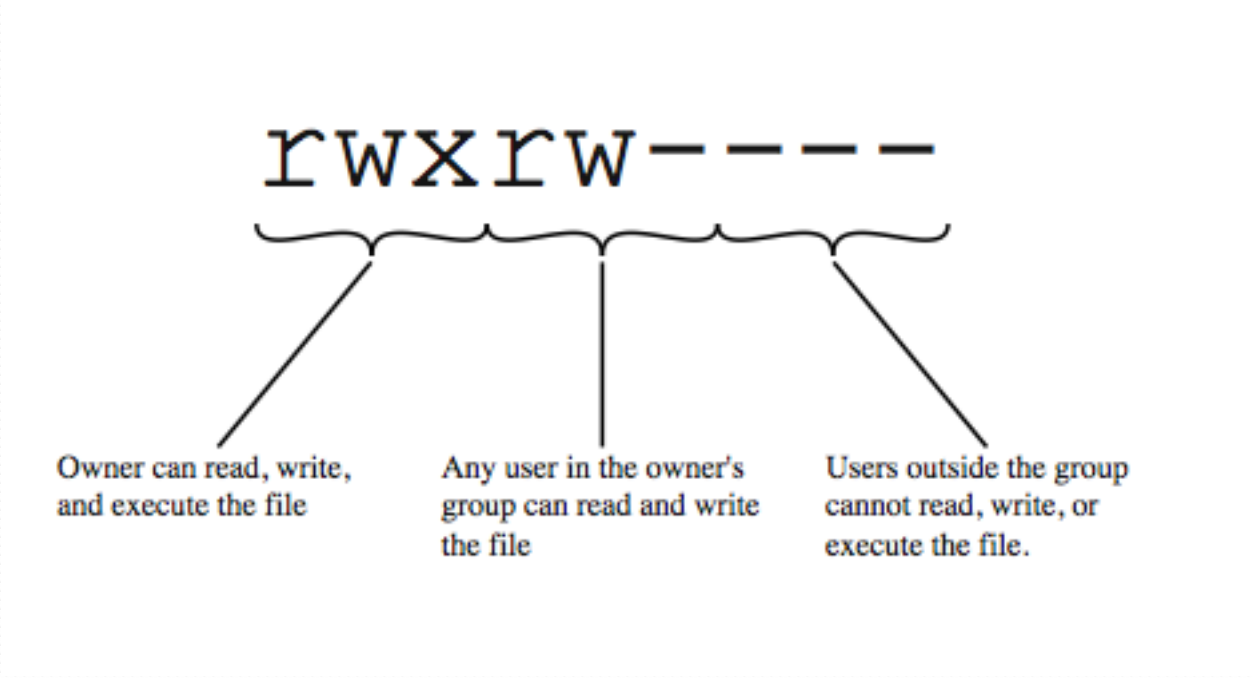
Protection Domains

- set of objects with associated access rights
- in access matrix view, each row defines a protection domain
  - but not necessarily just a user
  - may be a limited subset of user's rights
  - applied to a more restricted process
- may be static or dynamic

UNIX File Concepts

- UNIX files administered using inodes
  - control structure with key info on file
    - attributes, permissions of a single file
  - may have several names for same inode
  - have inode table / list for all files on a disk
    - copied to memory when disk mounted
- directories form a hierarchical tree
  - may contain files or other directories
  - are a file of names and inode numbers

UNIX File Access Control



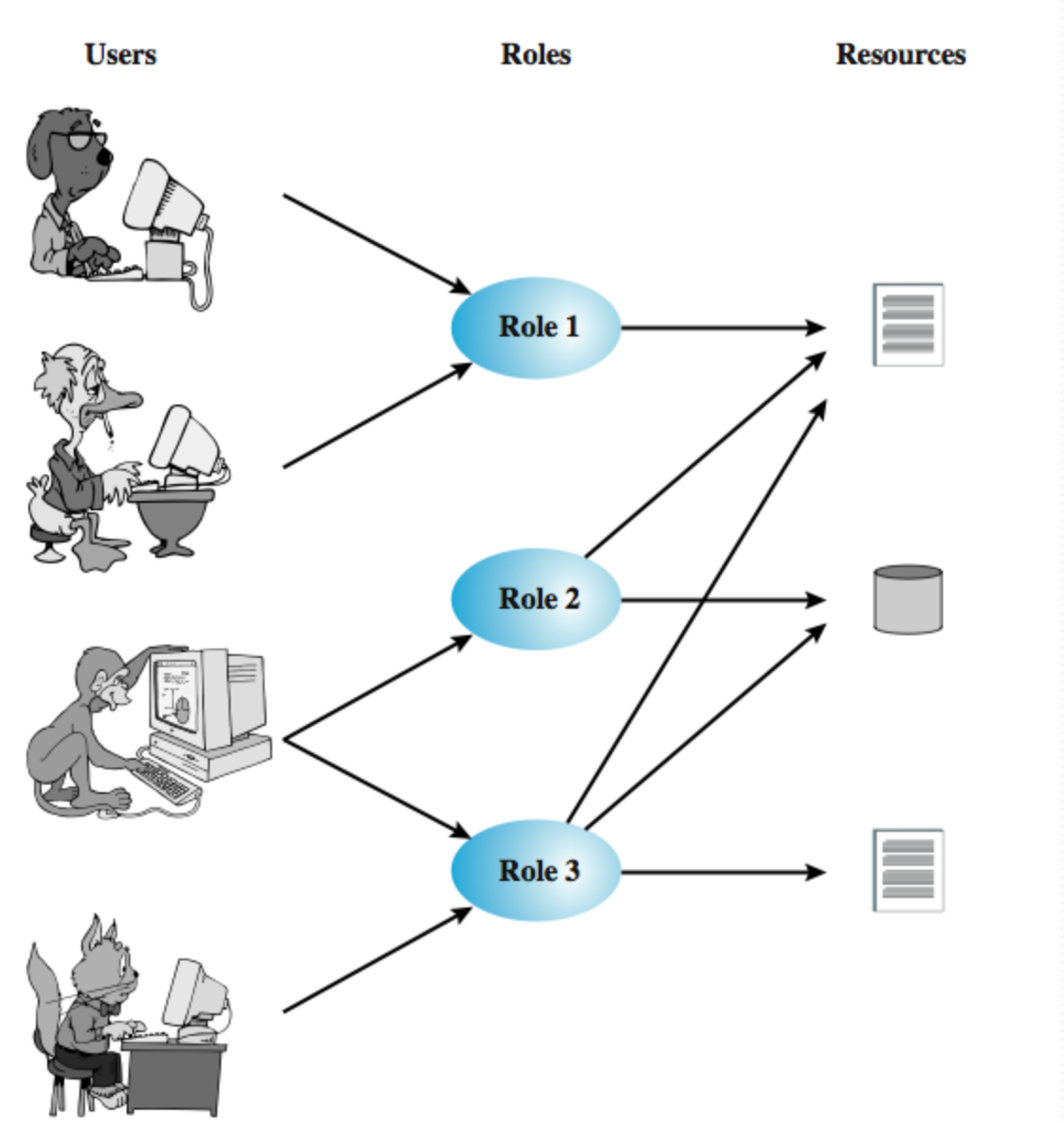
UNIX File Access Control

- "set user ID"(SetUID) or "set group ID"(SetGID)
  - system temporarily uses rights of the file owner / group in addition to the real user's rights when making access control decisions
  - enables privileged programs to access files / resources not generally accessible
- sticky bit
  - on directory limits rename/move/delete to owner
- superuser
  - is exempt from usual access control restrictions

UNIX Access Control Lists

- modern UNIX systems support ACLs
- can specify any number of additional users / groups and associated rwx permissions
- ACLs are optional extensions to std perms
- group perms also set max ACL perms
- when access is required
  - select most appropriate ACL
    - owner, named users, owning / named groups, others
  - check if have sufficient permissions for access

Role-Based Access Control

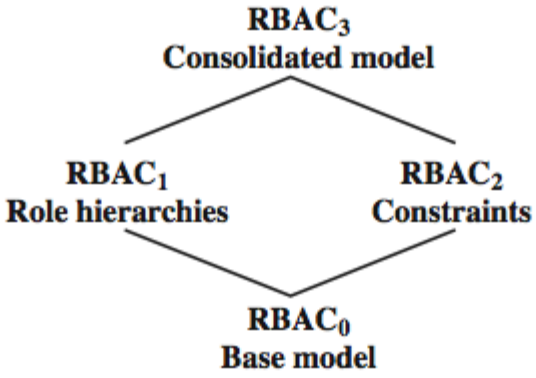


Role-Based Access Control

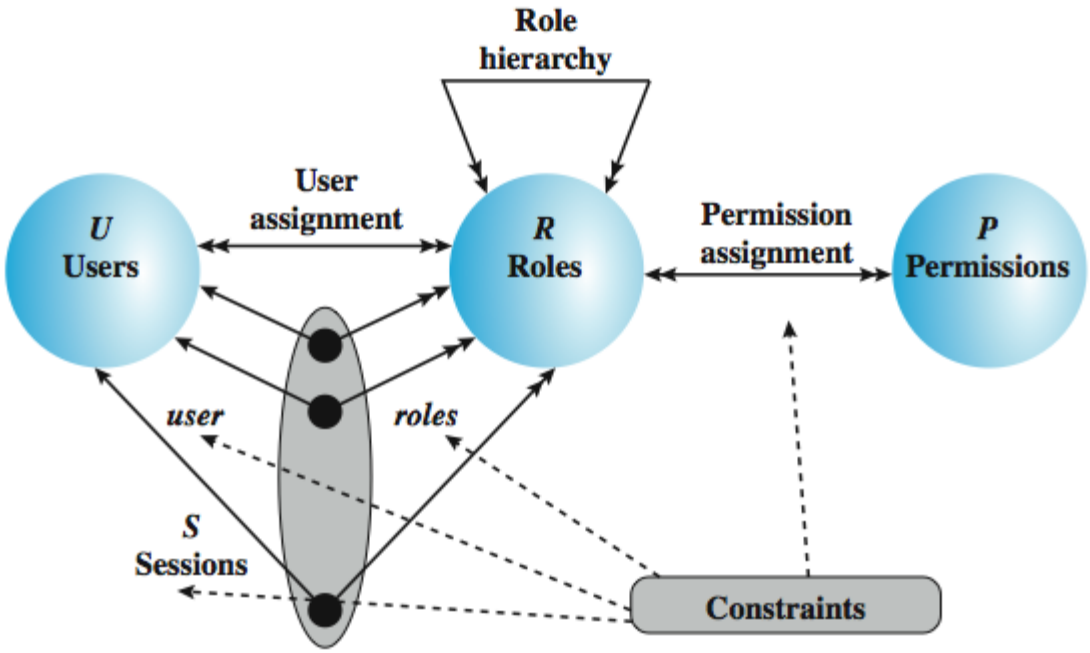
	R_1	R_2	...	R_n
U_1	✕			
U_2	✕			
U_3		✕		✕
U_4				✕
U_5				✕
U_6				✕
...				
U_m	✕			

	OBJECTS								
ROLES	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			

Role-Based Access Control

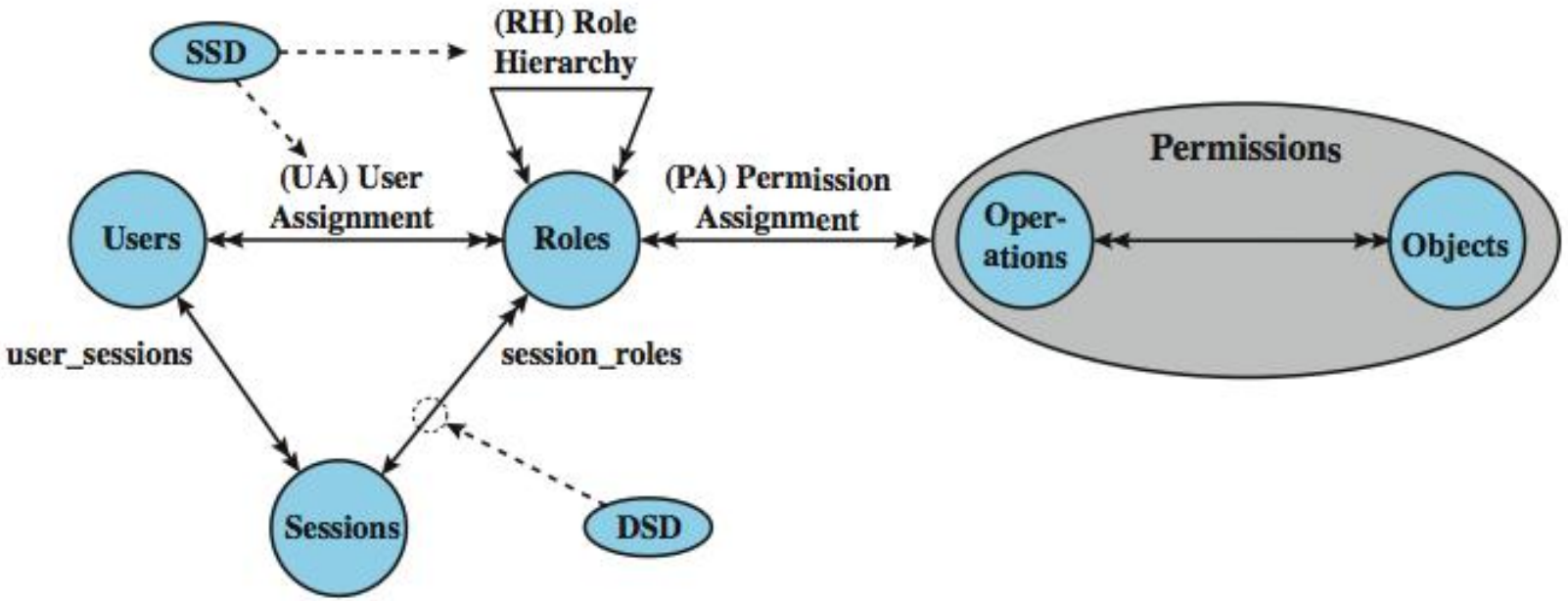


(a) Relationship among RBAC models



(b) RBAC models

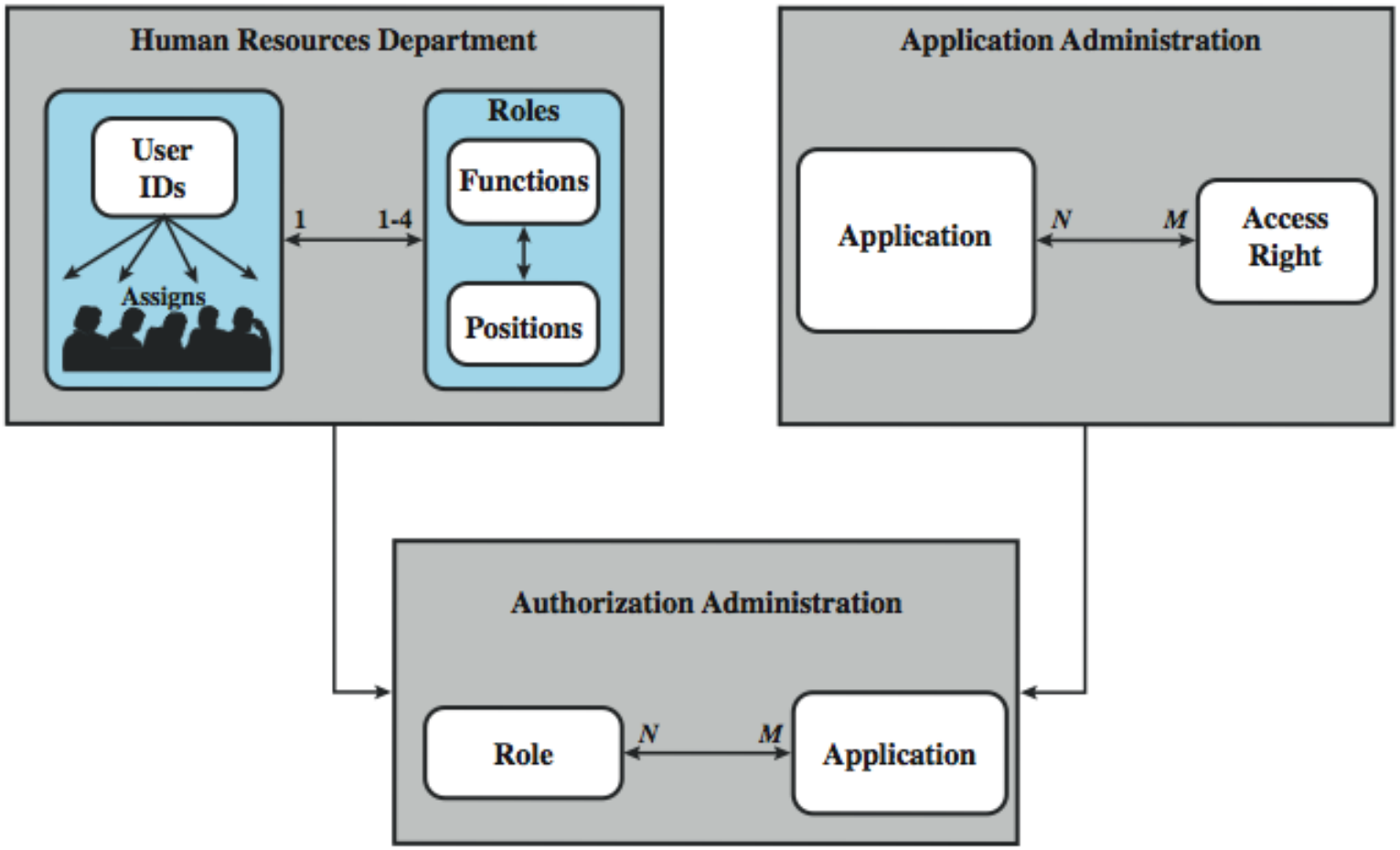
NIST RBAC Model



NIST RBAC role Hierarchies

- General Role Hierarchies
- Limited Role Hierarchies

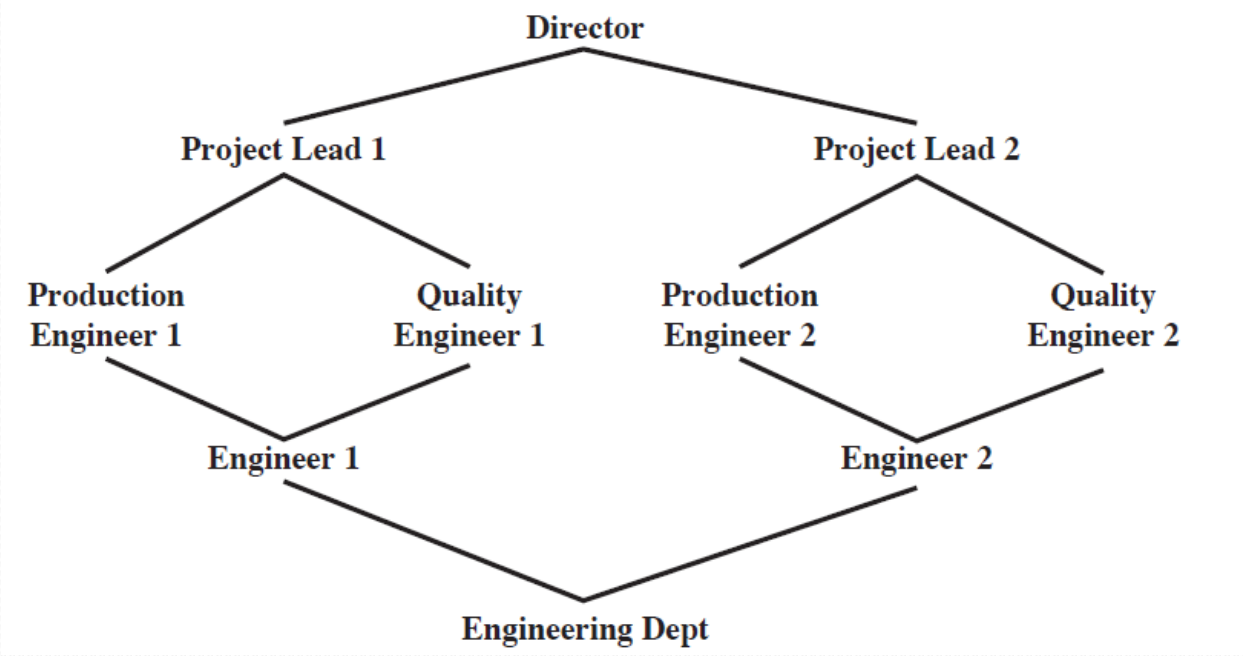
RBAC For a Bank



Summary

- introduced access control principles
  - subjects, objects, access rights
- discretionary access controls
  - access matrix, access control lists (ACLs), capability tickets
  - UNIX traditional and ACL mechanisms
- role-based access control
- case study

Quiz



- What are the immediate descendents of “Project Lead 1”?
- What of these relations is not compatible with NIST RBAC Limited role Hierarchies