CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

User Authentication, Access Control, and Operating System

AC Types of Access Control

Video Summary

- What is Discretionary Access Control (DAC)
- What is Role-based Access Control (RBAC)
- What are the limitations of RBAC
- What is Attribute-based Access Control (ABAC)
- What is Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

- DAC: an entity may be granted access rights that permit the entity, if they choose so, to enable another entity to access a resource
- Common access control scheme in operating systems and database management systems
- Access Matrix specifies access rights of subjects on objects

Discretionary Access Control (DAC)

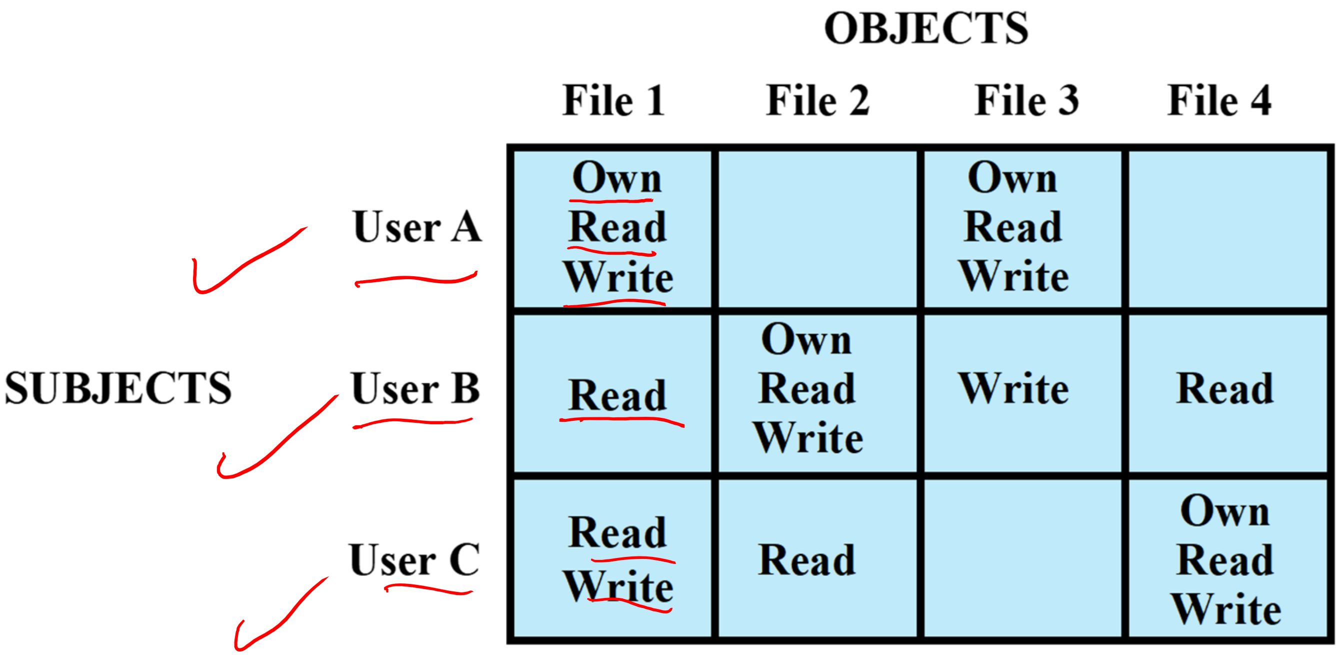
- In practice, access matrix is sparse, so implement as either:

  Access Control Lists (ACL) For each object, list subjects and their access rights

  Capability Lists For each subject, list objects and the rights the subject have on that object

- Alternative implementation: authorization table listing subject, access mode and object; easily implemented in database

Example of DAC: Access Matrix

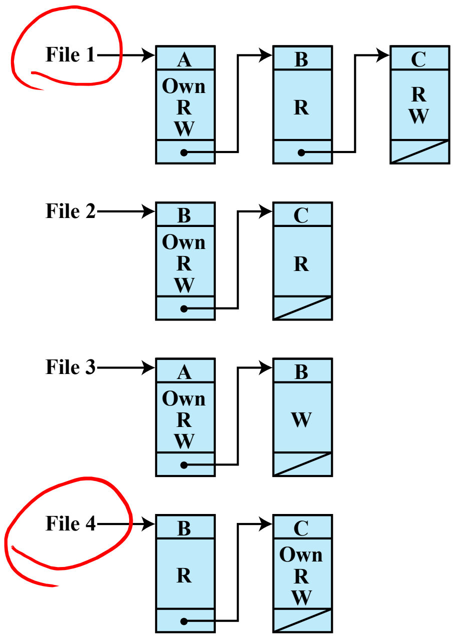


		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	✓ User A	Own Read Write		Own Read Write	
	✓ User B	Read	Own Read Write	Write	Read
	✓ User C	Read Write	Read		Own Read Write

(a) Access matrix

Figure 4.2 Example of Access Control Structures

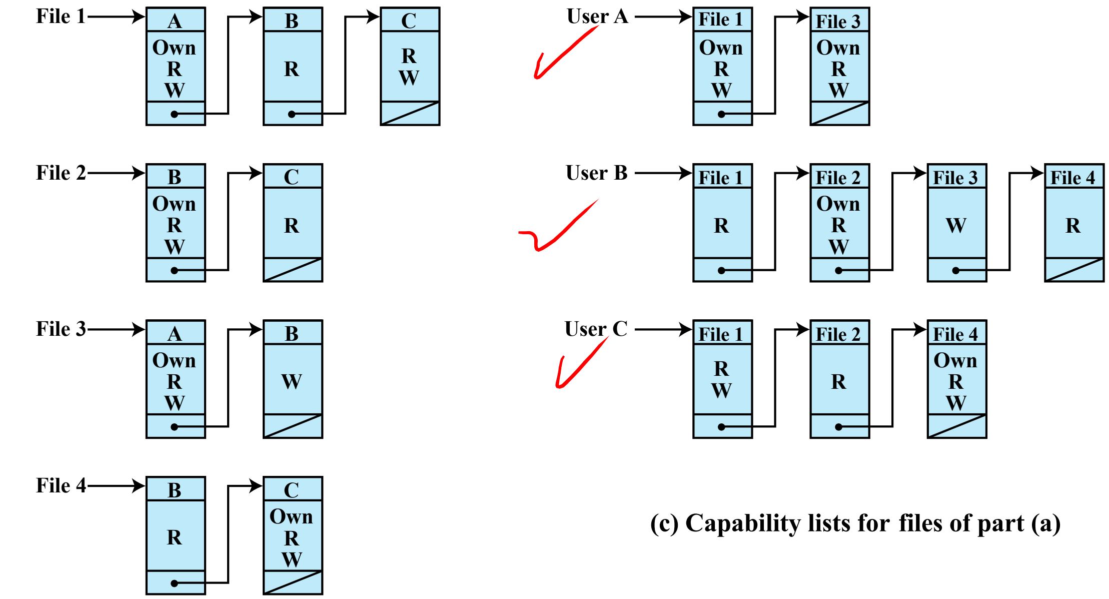
Example of DAC: Access Control List



(b) Access control lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Example of DAC: Capability lists



File 1 → A: Own, R, W → B: R → C: R, W

File 2 → B: Own, R, W → C: R

File 3 → A: Own, R, W → B: W

File 4 → B: R → C: Own, R, W

(b) Access control lists for files of part (a)

User A → File 1: Own, R, W → File 3: Own, R, W

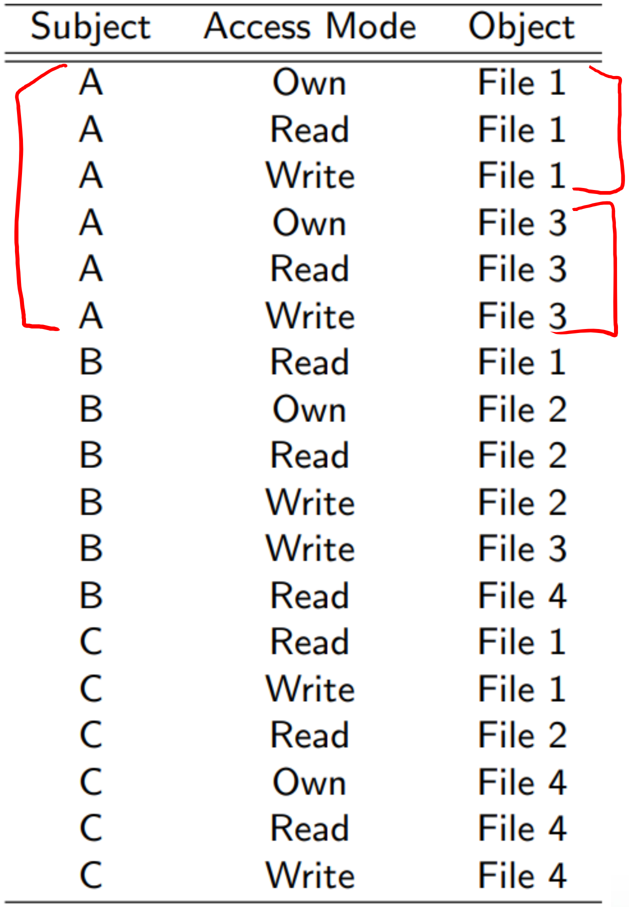
User B → File 1: R → File 2: Own, R, W → File 3: W → File 4: R

User C → File 1: R, W → File 2: R → File 4: Own, R, W

(c) Capability lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Example of Authorization Table



Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

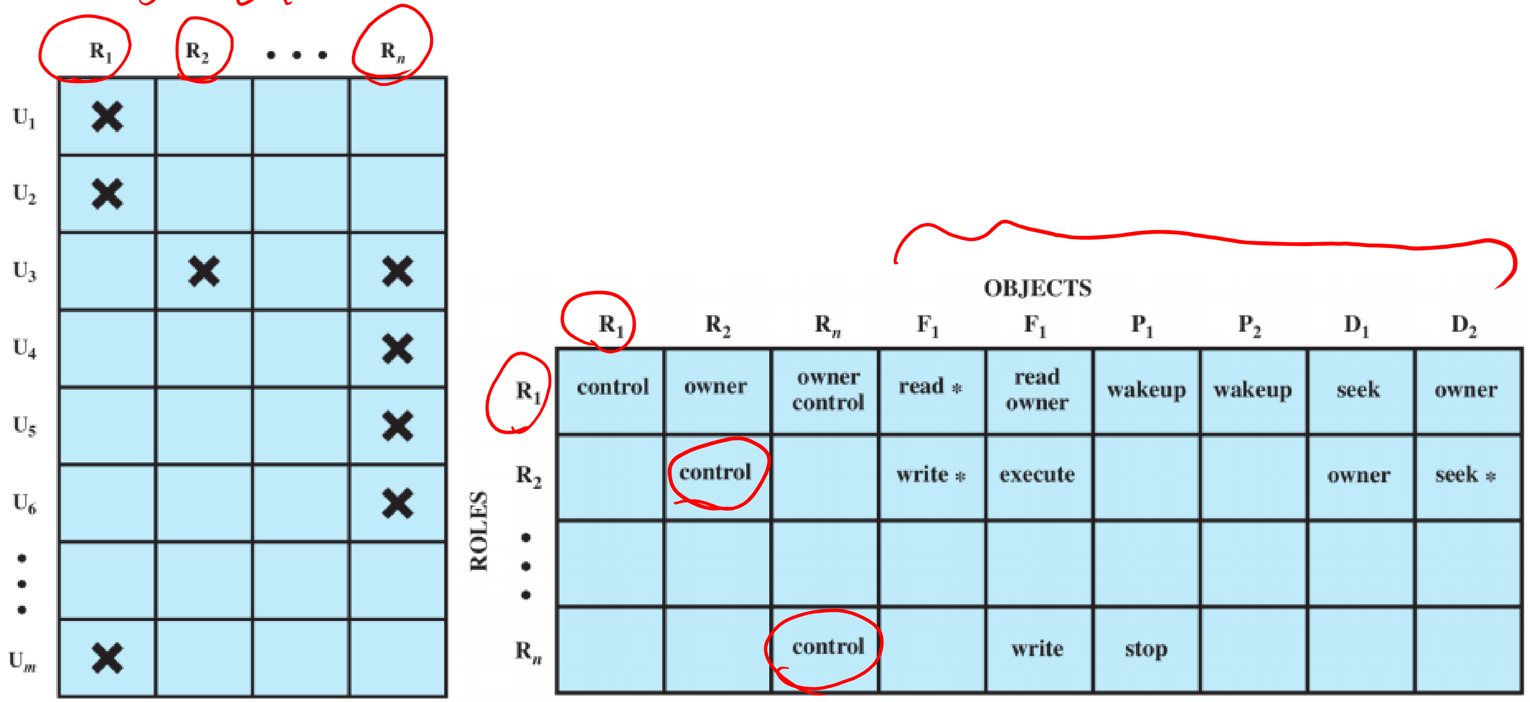
Role-Based Access Control

- RBAC: users are assigned to roles; access rights are assigned to roles
- Roles typically job functions and positions within organisation, e.g. senior financial analyst in a bank, doctor in a hospital
- Users may be assigned multiple roles; static or dynamic
- Sessions are temporary assignments of user to role(s)
- Access control matrix can map users to roles and roles to objects

Role-Based Access Control Matrix

Role

User

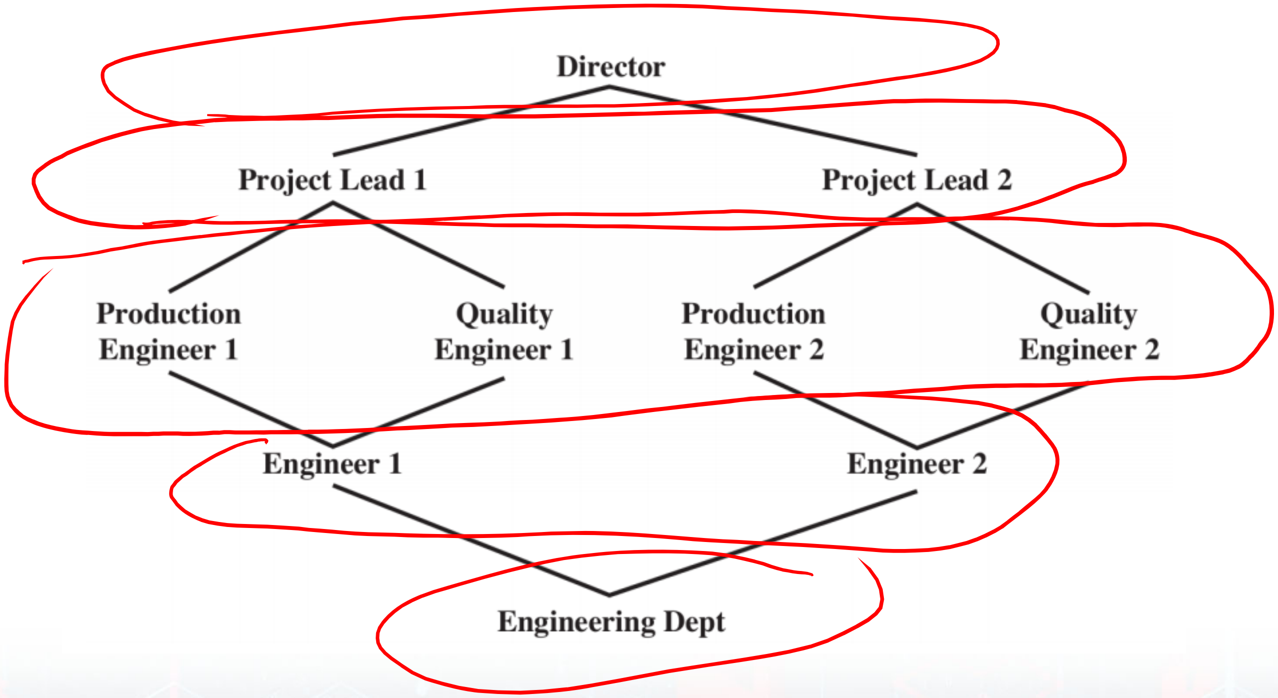


	R_1	R_2	• • •	R_n
U_1	✖			
U_2	✖			
U_3		✖		✖
U_4				✖
U_5				✖
U_6				✖
• • •				
U_m	✖			

				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			

Hierarchies in RBAC

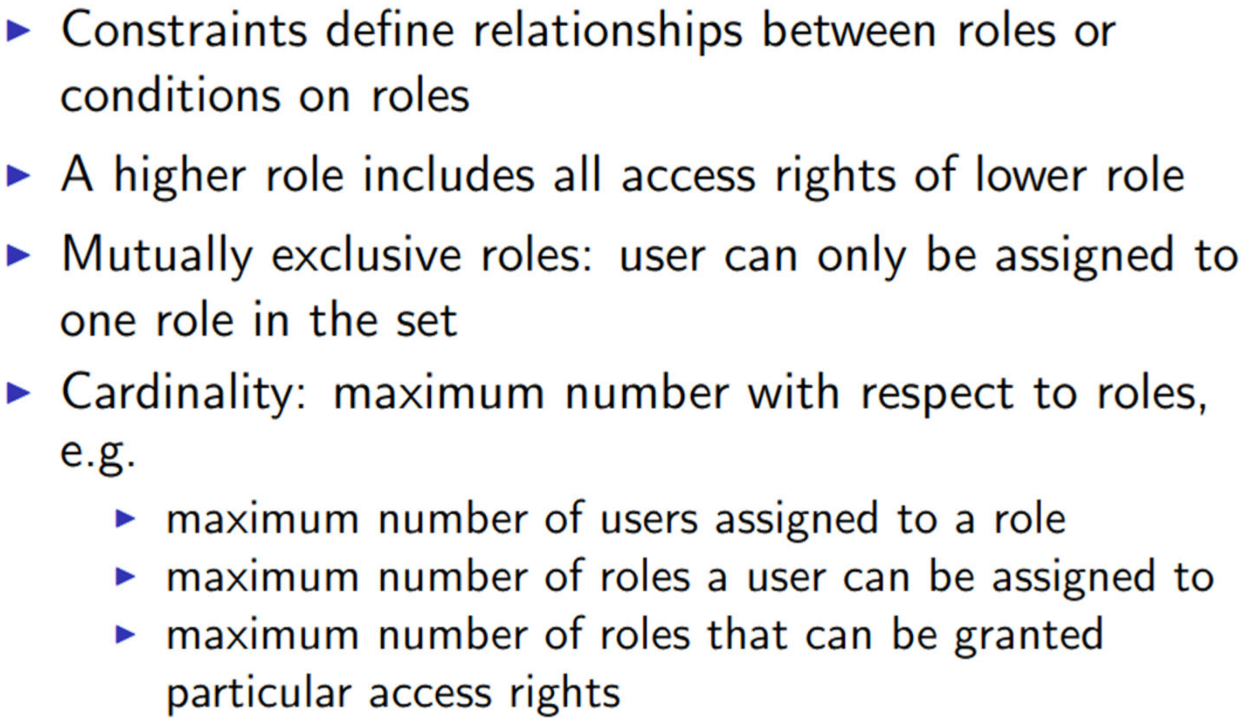
- Hierarchy of an organisation can be reflected in roles
- A higher role includes all access rights of lower role



Constraints in RBAC

- Constraints define relationships between roles or conditions on roles
- A higher role includes all access rights of lower role
- Mutually exclusive roles: user can only be assigned to one role in the set

Constraints in RBAC



- Constraints define relationships between roles or conditions on roles
- A higher role includes all access rights of lower role
- Mutually exclusive roles: user can only be assigned to one role in the set
- Cardinality: maximum number with respect to roles, e.g.
  - maximum number of users assigned to a role
  - maximum number of roles a user can be assigned to
  - maximum number of roles that can be granted particular access rights

Constraints in RBAC

- Constraints define relationships between roles or conditions on roles
- A higher role includes all access rights of lower role
- Mutually exclusive roles: user can only be assigned to one role in the set
- Cardinality: maximum number with respect to roles, e.g.
  - maximum number of users assigned to a role
  - maximum number of roles a user can be assigned to
  - maximum number of roles that can be granted particular access rights
- Prerequisite: condition upon which user can be assigned a role, e.g.
  - user can only be assigned a senior role if already assigned a junior role

Video Summary

- What is Discretionary Access Control (DAC) ✓
- What is Role-based Access Control (RBAC) ✓
- What are the limitations of RBAC →
- What is Attribute-based Access Control (ABAC) →
- What is Mandatory Access Control (MAC) →