Access Control

Overview

- Access control function and policies
- Access control matrix
- Access control list
- Capability list
- Role based access control

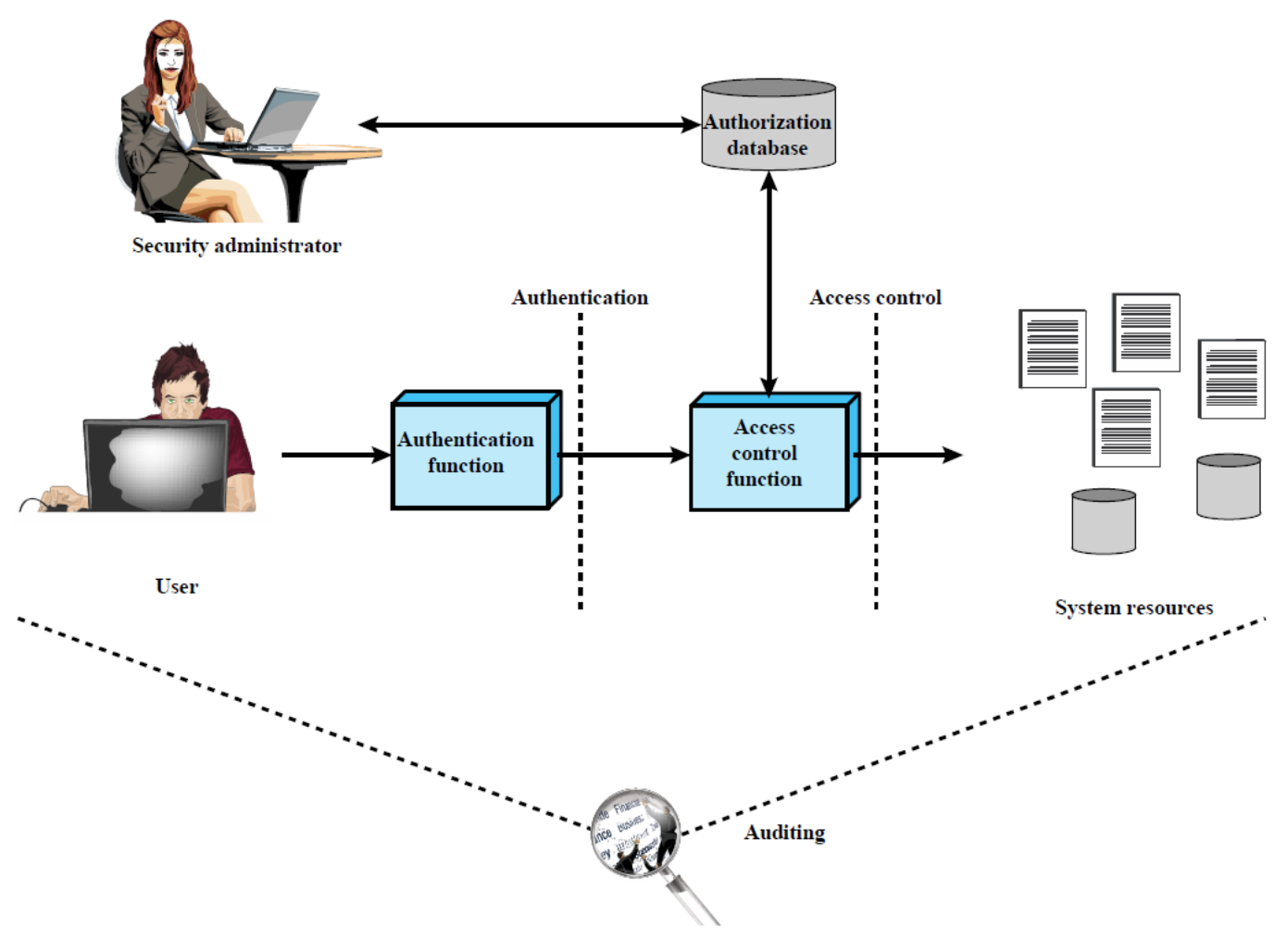
Access Control Definitions

RFC 4949 defines access control as:

1. Protection of system resources against unauthorized access.
2. A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.
3. /formal model/ Limitations on interactions between subjects and objects in an information system.
4. "The prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner."
5. A system using physical, electronic, or human controls to identify or admit personnel with properly authorized access to a SCIF.

Access Control Function and Policies

Access Control Function



Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

Discretionary Access Control

Subjects, Objects, and Access Rights

Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search

Discretionary Access Control (DAC)

- Scheme in which an entity may enable another entity to access some resource
- Often provided using an access matrix
  - One dimension consists of identified subjects that may attempt data 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

Access Control Matrix

Access Control 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

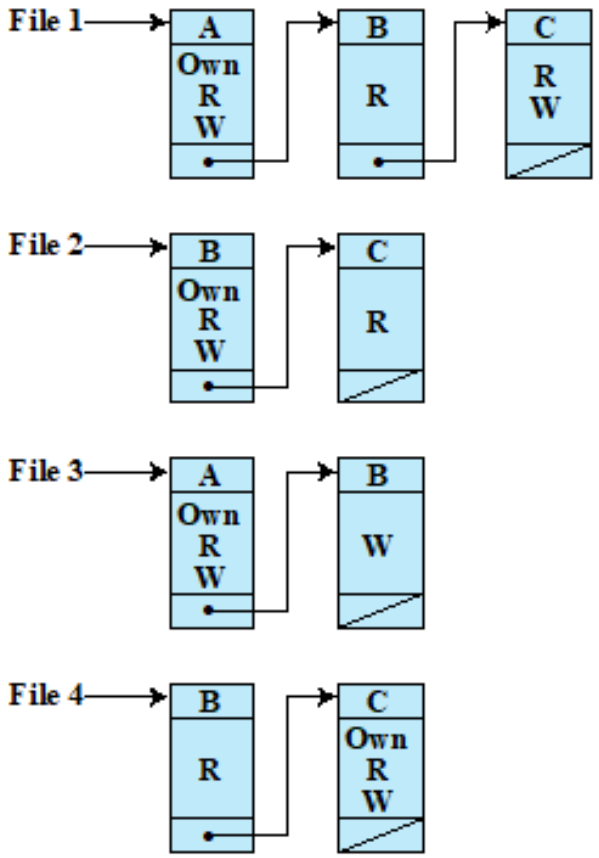
Extended ACM

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

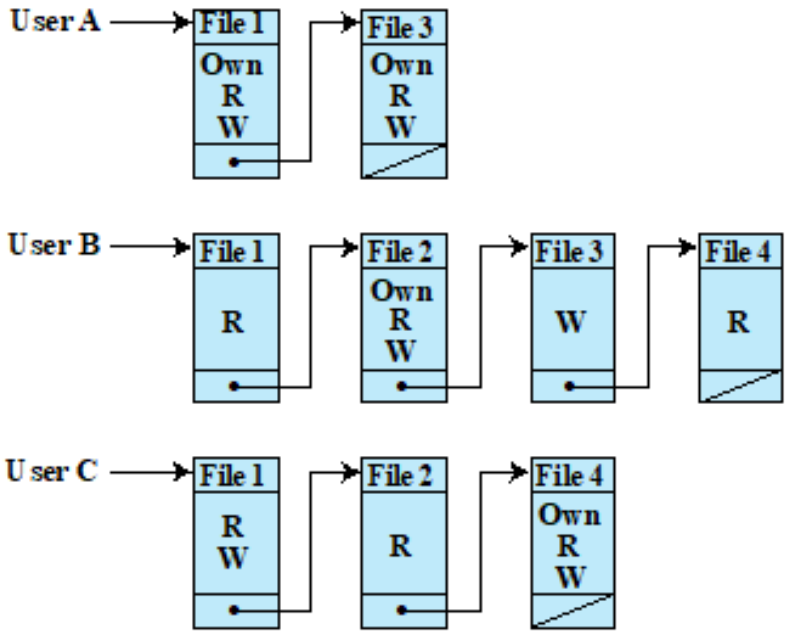
* - copy flag set

Access Control List and Capability List

Access Control List and Capability List

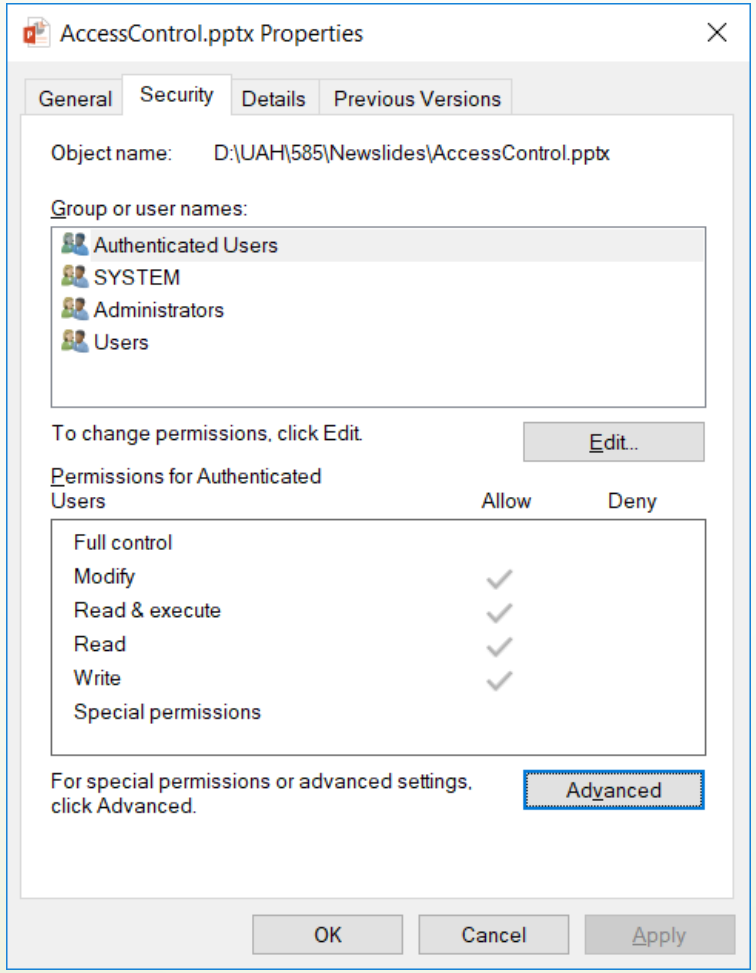


(b) Access control lists for files of part (a)

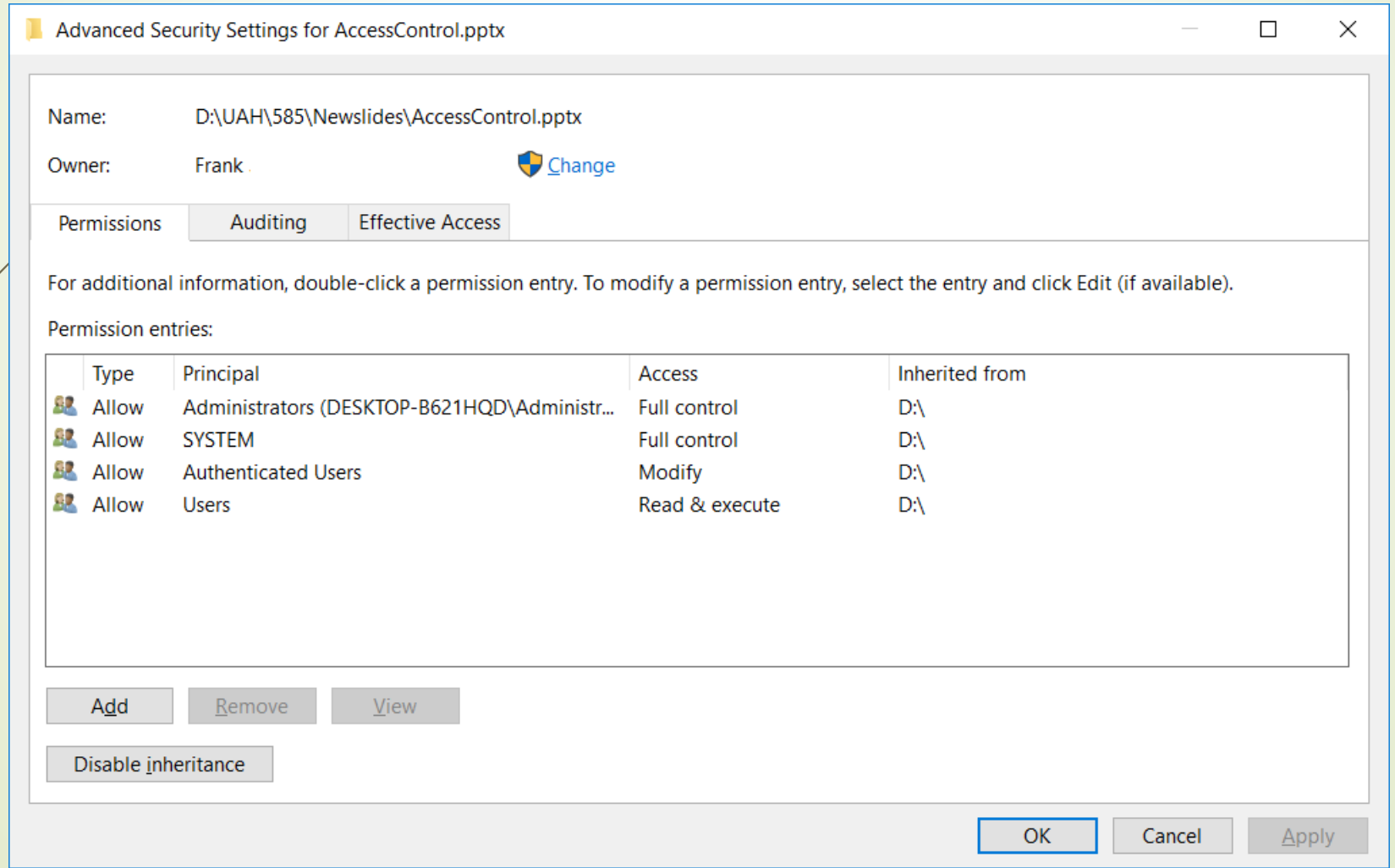


(c) Capability lists for files of part (a)

Windows ACLs - Example



Windows ACLs - Permissions



Windows 10 NTFS ACLs

- Different sets of rights
  - Basic: read, write, execute, delete, change permission, take ownership
  - Generic: no access, read (read/execute), change (read/write/execute/delete), full control (all), special access (assign any of the basics)
  - Directory: no access, read (read/execute files in directory), list, add, add and read, change (create, add, read, execute, write files; delete subdirectories), full control, special access

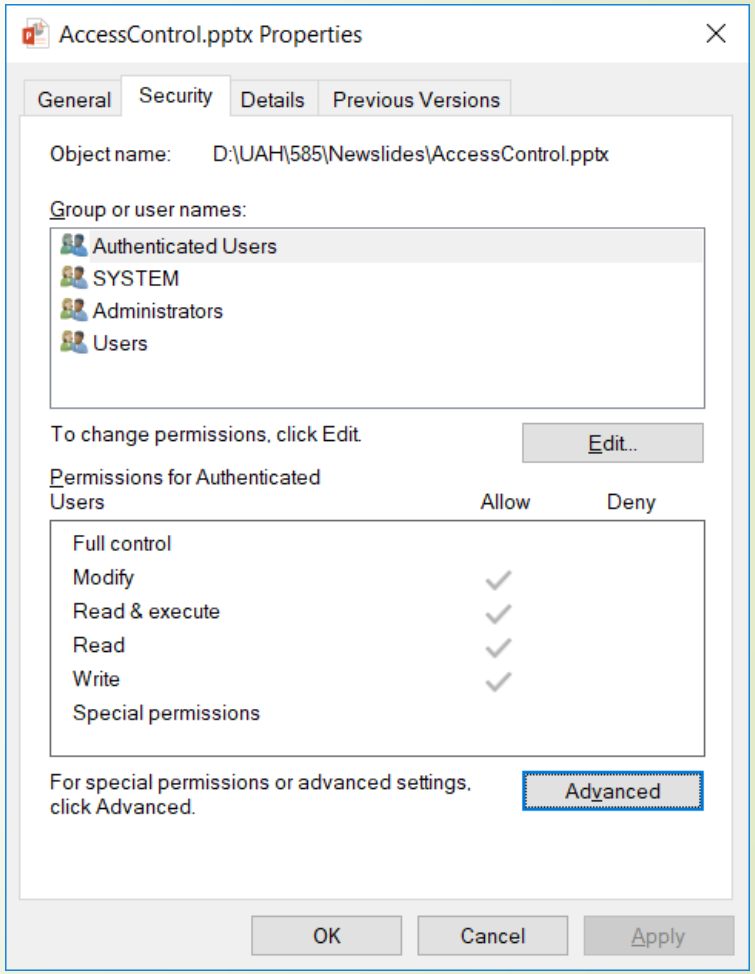
Conflicts, Default Permissions, and Revocation

Handling Default Permissions

- Default is deny
  - Principle of fail-safe defaults

Conflicts

- Apply first entry matching subject
- Deny access if any entry would deny access
  - AIX: if any entry denies access, *regardless or rights given so far*, access is denied

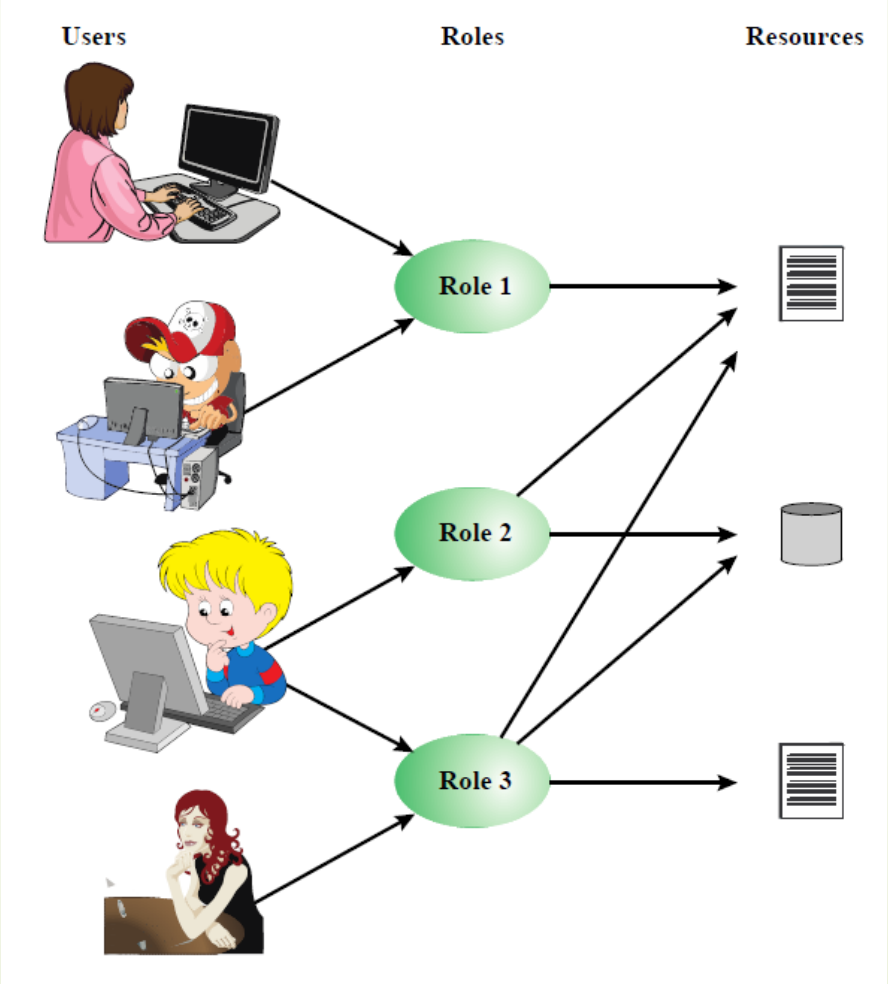


Revocation

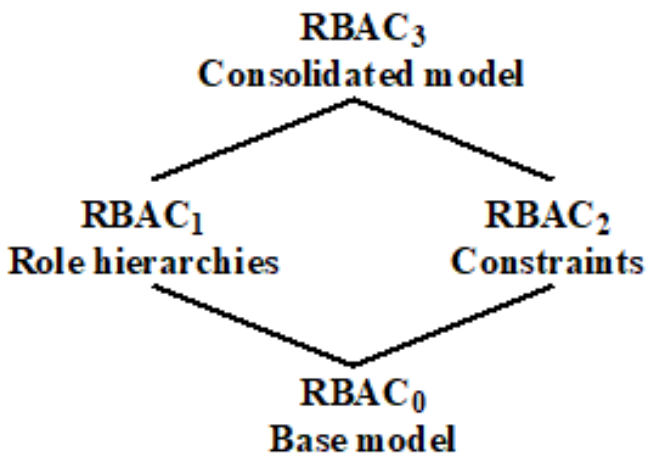
- How do you remove subject's rights to a file?
  - Owner deletes subject's entries from ACL, or rights from subject's entry in ACL

Role-Based Access Control

RBAC

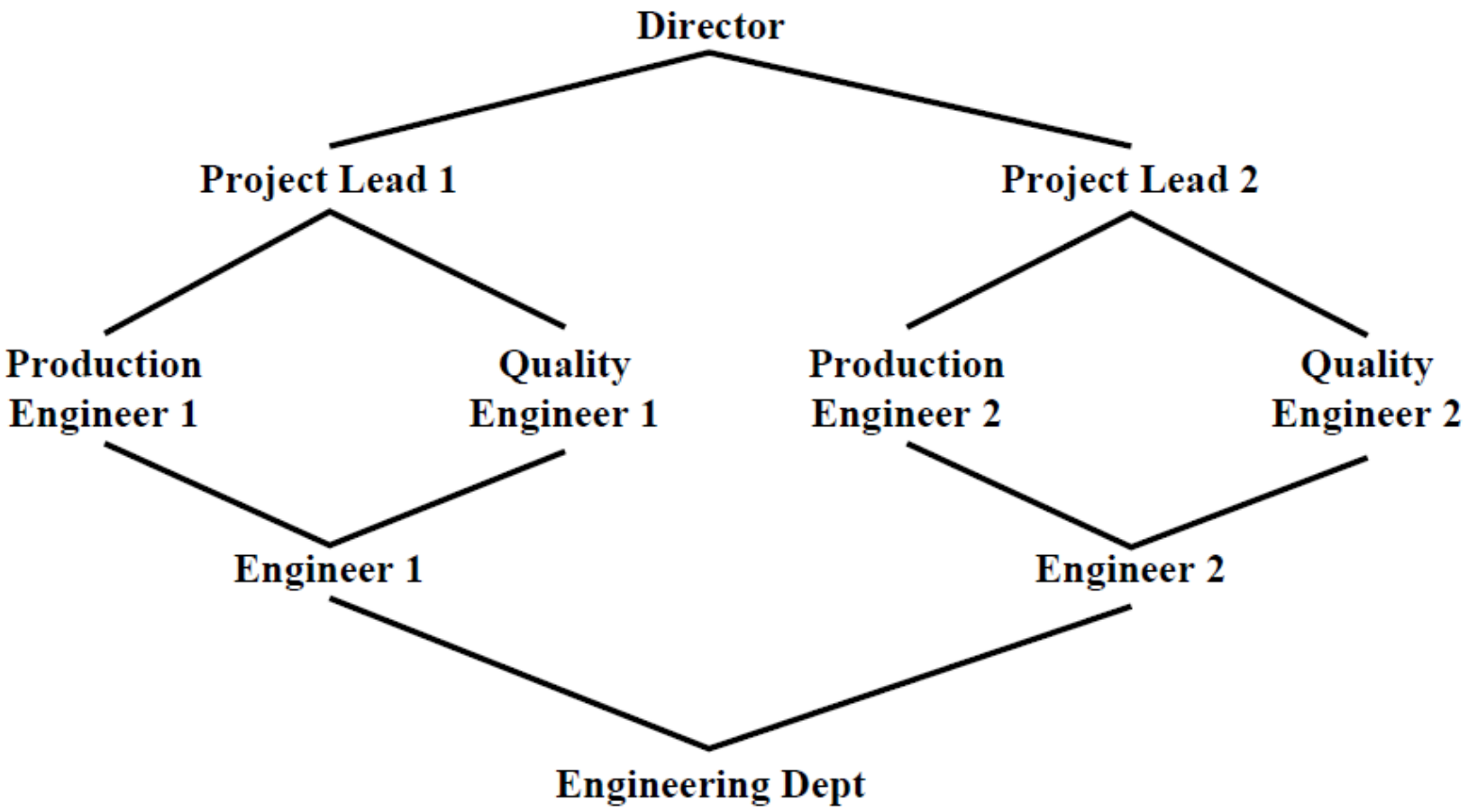


RBAC Models



Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes

Hierarchical RBAC



Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles

Mutually exclusive roles	Cardinality	Prerequisite roles
• A user can only be assigned to one role in the set (either during a session or statically) • Any permission (access right) can be granted to only one role in the set	• Setting a maximum number with respect to roles	• Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role

Key Points

Key Points

- Three types of access control policies
- ACM, ACL, Capability list
- Conflicts, default permissions, revocation
- 4 types of RBAC