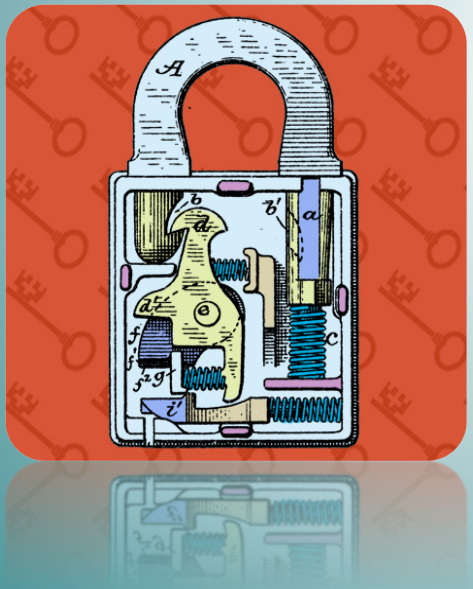
Garantía y Seguridad en Sistemas y Redes

Tema 4. Access Control

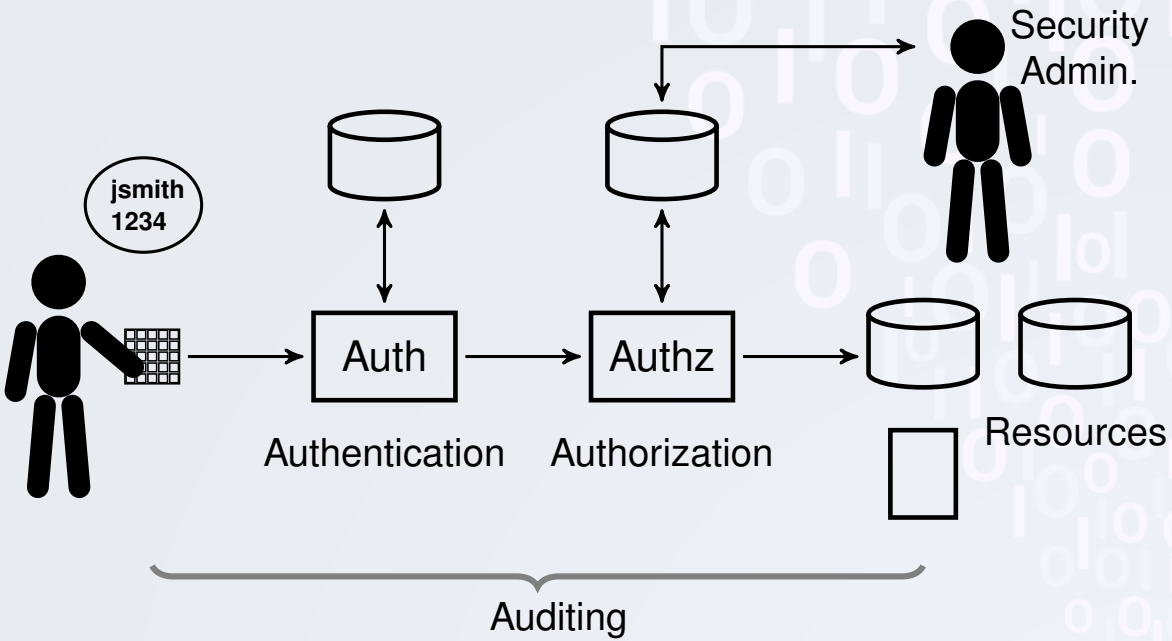


Esteban Stafford

Departamento de Ingeniería Informática y Electrónica

Contents

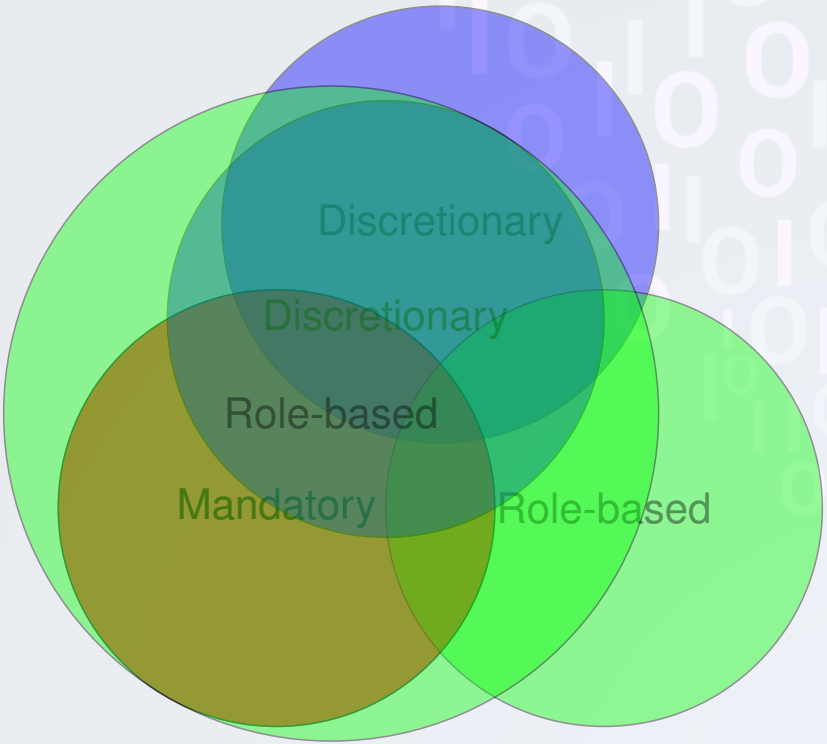
Access Control



Access Control Requirements

- Reliable input.
- Support for fine and coarse specifications.
- Least privilege.
- Separation of duty.
- Open and closed policies.
- Policy combinations and conflict resolution.
- Right relinquishing.

Access Control Policies



Subjects, Objects and Access Rights

Subjects	Rights	Objects	Location	Auth
User	Read	Device	Kernel	Password
Group	Write	Filesystem	User space	Token
Role	Execute	Directory	Localhost	Biometric
World	Delete	File	Intranet	
	Create	Application	Wireless	
	Search	Database	VPN	
	Authorise	Table	Internet	
		Column		
		Row		

Discretionary Access Control

- **Subject** with a certain **Right** can **Pass** it to any other subject. (Unix filesystem, SQL)
- Rights are organised in an **Access Matrix**

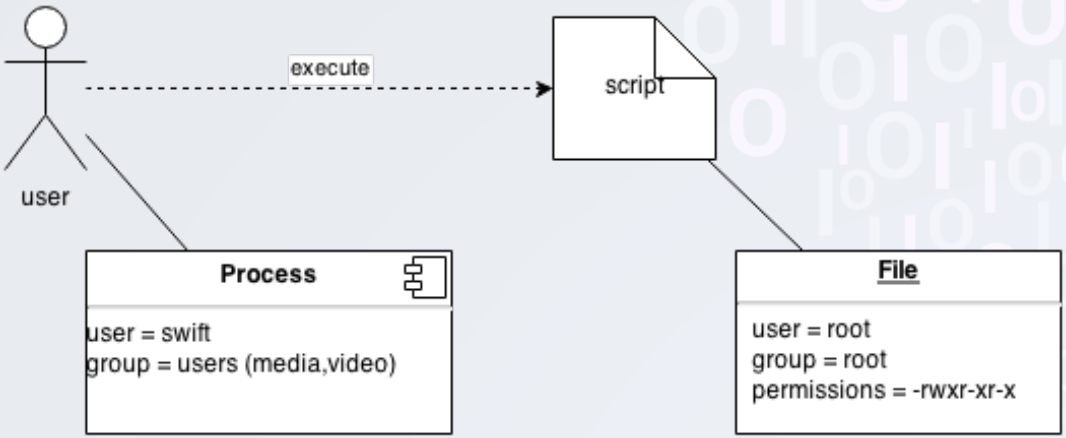
	File 1	File 2	File 3	File 4
User A	Own, Read, Write		Own, Read, Write	
User B	Read	Own, Read, Write	Write	Read
User C	Read, Write	Read		Own, Read, Write

- Access Control Lists(ACL) = columns of Access Matrix
- Capability Lists = rows of Access Matrix

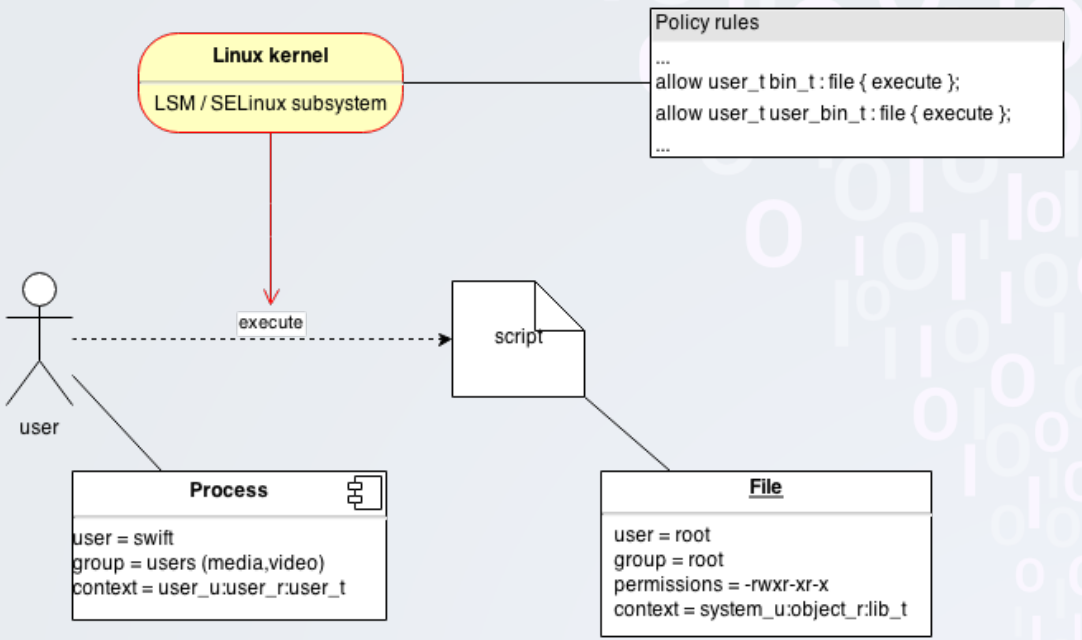
Mandatory Access Control

- Centrally controlled by a security policy administrator.
- Subjects do not have the ability to override the policy.
- SELinux, PolicyKit, Mandatory Integrity Control.

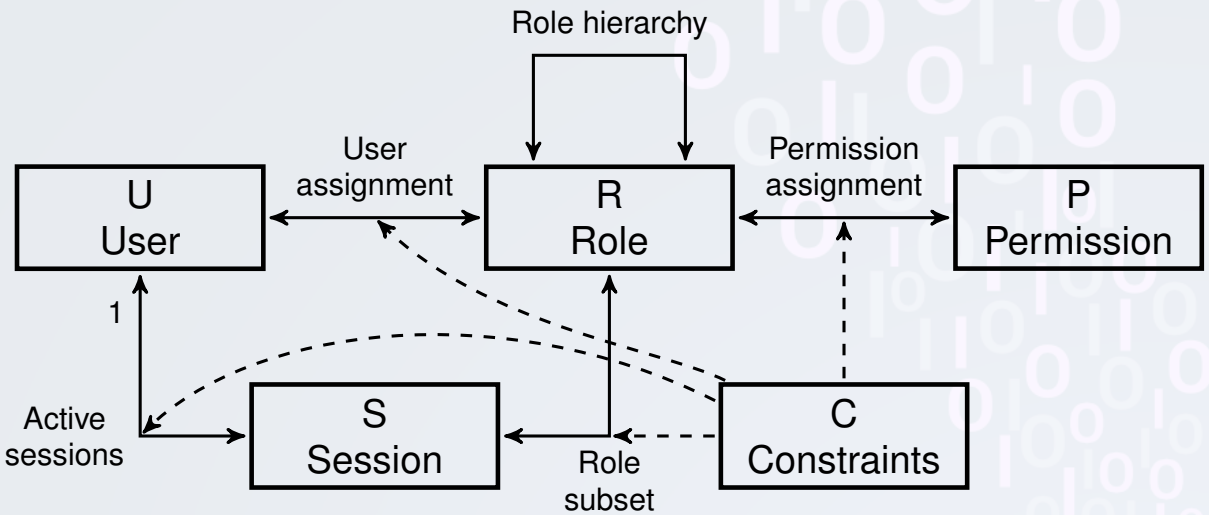
Linux DAC + MAC (SELinux)



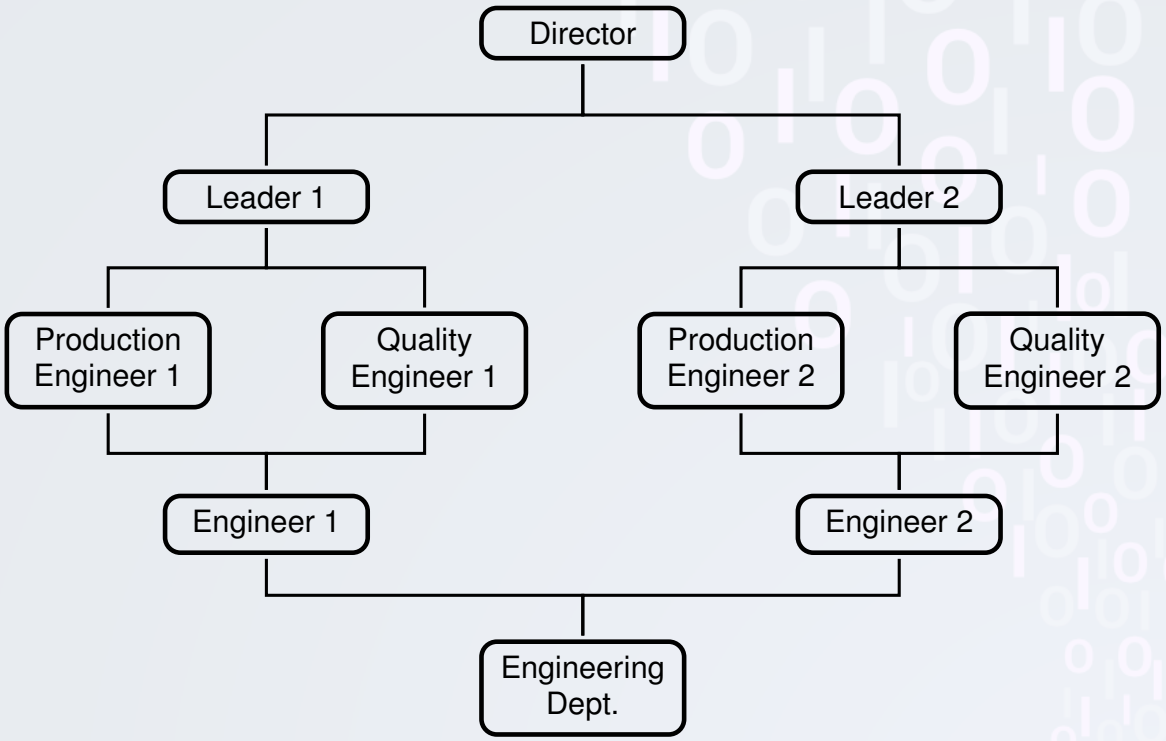
Linux DAC + MAC (SELinux)



Role-Based Access Control



Role hierarchy



Role constraints

- **Mutual exclusivity** forces a user to belong to only one role of a set. Useful to implement **separation of duty**.
- Maximum **cardinality**
  - Number of roles for a user or session.
  - Number of users with a given role.
  - Number of roles with a given permission.
- **Prerequisites** can establish requirements for belonging to special roles. Useful to implement **least privilege** structures.