# Controllo di accesso

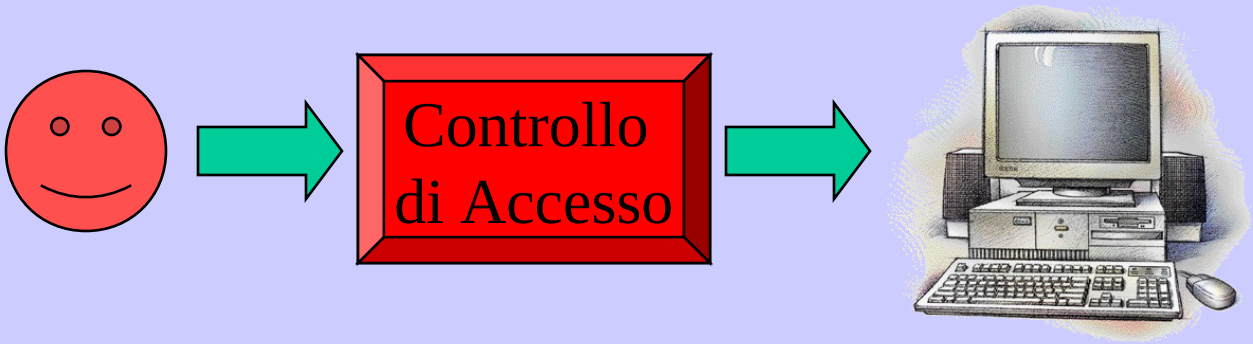
**Prof. Francesco Bergadano**

**Dipartimento di Informatica**

**Università di Torino**

# Sicurezza del file system

**Non basta verificare <u>se</u> un utente è autorizzato a entrare nel sistema, occorre anche indicare <u>quali</u> <u>risorse</u> può utilizzare**



# Sicurezza del file system

- **DAC: Discretionary Access Control**
- **MAC: Mandatory Access Control**
- **RBAC: Role-based Access Control**

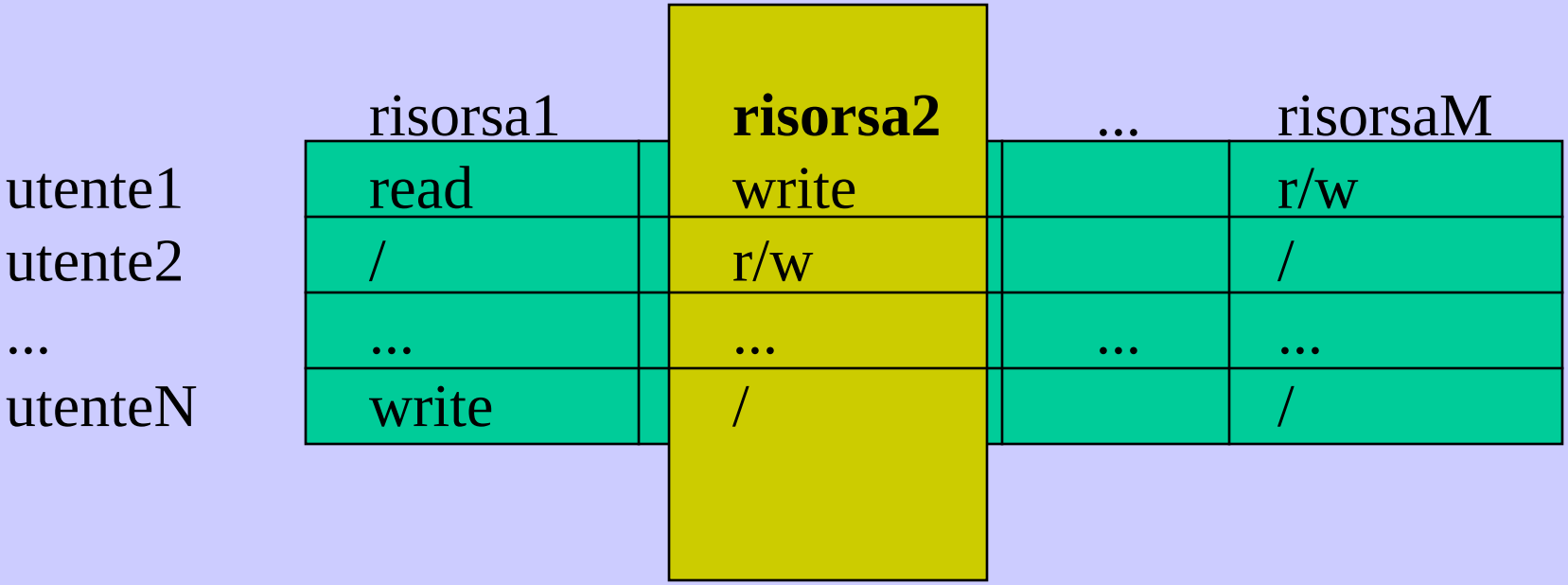
# Sicurezza del file system

- **Con matrice di accesso (DAC)**
- **Con liste di accesso (access list) (DAC)**
- **Con permessi espliciti (capabilities) (DAC)**
- **Con permessi relativi a gruppi (Unix) (DAC)**
- **Con “ruoli” (RBAC)**
- **Con sicurezza a livelli (multilevel security) (MAC)**

# Matrice di accesso

| | risorsa1 | risorsa2 | ... | risorsaM |
|---|---|---|---|---|
| utente1 | read | write | | r/w |
| utente2 | / | r/w | | / |
| ... | ... | ... | ... | ... |
| utenteN | write | / | | / |

# Access Control List (ACL)



# Capability list (o tickets)

# Unix

| | risorsa1 | risorsa2 | ... | risorsaM |
|---|---|---|---|---|
| owner | read | write | | r/w |
| group | / | r/w | | r/w/e |
| others | write | exec | | / |
| bit S | 0 | 1 | | 0 |

# Sicurezza del file system a livelli (multilevel security)

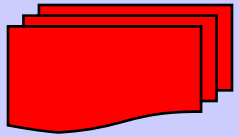
- **Gli utenti sono divisi in livelli di sicurezza**
- **A un livello più alto si hanno più permessi di accesso**
- **Al tempo stesso un livello più alto deve essere più protetto**
- **Applicazioni militari (specie in USA)**

# Sicurezza del file system a livelli (multilevel security)

---

-

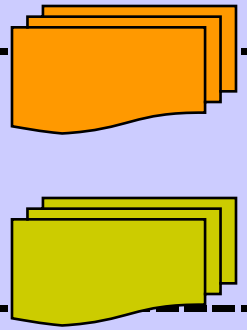
Utenti livello ‘top-secret’



---

-

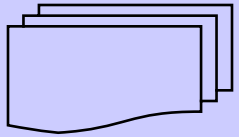
Utenti livello ‘secret’



---

-

Utenti livello ‘autorizzato’



---

-

Utenti livello ‘esterni’

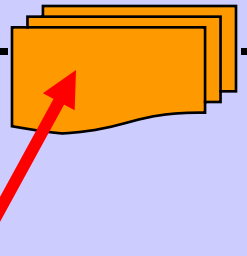
# Modello di Bell-Lapadula

---

Utenti livello ‘top-secret’

---

Utenti livello ‘secret’




---

Utenti livello ‘autorizzato’

---

Utenti livello ‘esterni’

# Modello di Bell-Lapadula