5. Controllo degli Accessi

Sicurezza dell'Informazione

Cos’è il controllo degli accessi

Una decisione binaria:

- L’accesso è consentito oppure negato.

Difficile da gestire in modo efficiente:

- Sistemi con migliaia di file e diversi utenti necessitano un algoritmo efficiente per la verifica dei permessi.
- Necessità di definire delle *regole*.

Chi lo fa? Il Reference Monitor

È il componente che applica le politiche di controllo degli accessi. Tutti i sistemi operativi moderni includono un'implementazione di un Reference Monitor.

Requisiti del Reference Monitor:

- A prova di manomissione (Tamper-proof).
- Non aggirabile (Cannot be bypassed).
- Sufficientemente piccolo da poter essere verificato/testato.

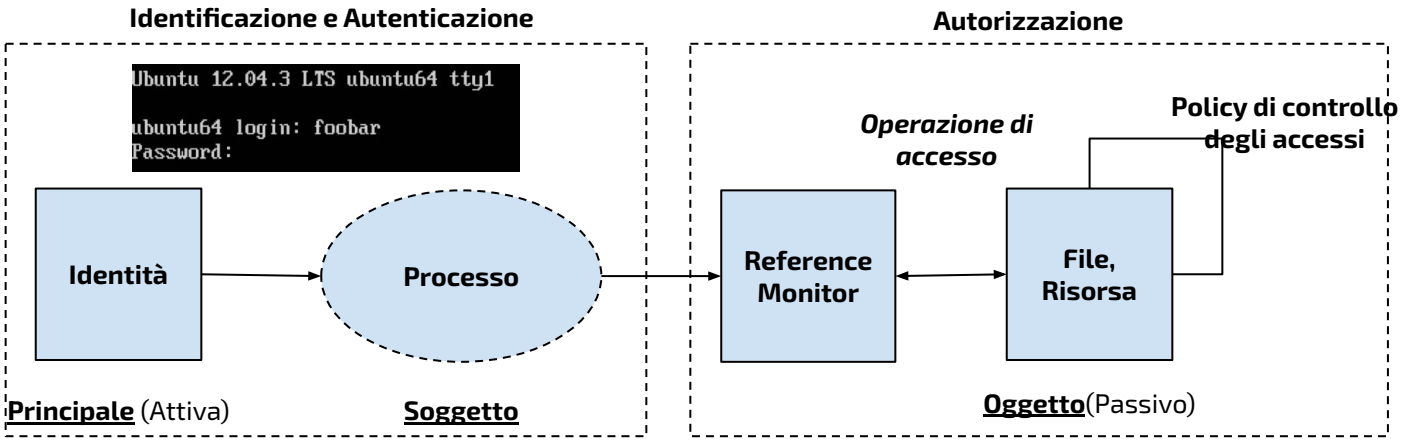
Autenticazione e autorizzazione

Il reference monitor **deve individuare e valutare la politica di sicurezza rilevante per la richiesta in questione**:

- Verifica l'identità del soggetto che effettua la richiesta.
- Decide se l'accesso è consentito o negato.

"Tutto sommato facile" nei sistemi centralizzati, ma nei sistemi distribuiti…

- Come trovare tutte le politiche rilevanti?
- Come prendere decisioni se alcune politiche potrebbero mancare?



Modelli di controllo degli accessi

I più noti:

- **Discretionary Access Control (DAC)**.
- **Mandatory Access Control (MAC)**.
- Role-Based Access Control (RBAC).
- …

La principale differenza tra DAC e MAC è chi assegna i privilegi.

Discretionary Access Control (DAC)

Il proprietario della risorsa decide a propria discrezione i privilegi di accesso.

- Stefano crea un file e assegna a Federico il privilegio di leggerlo.

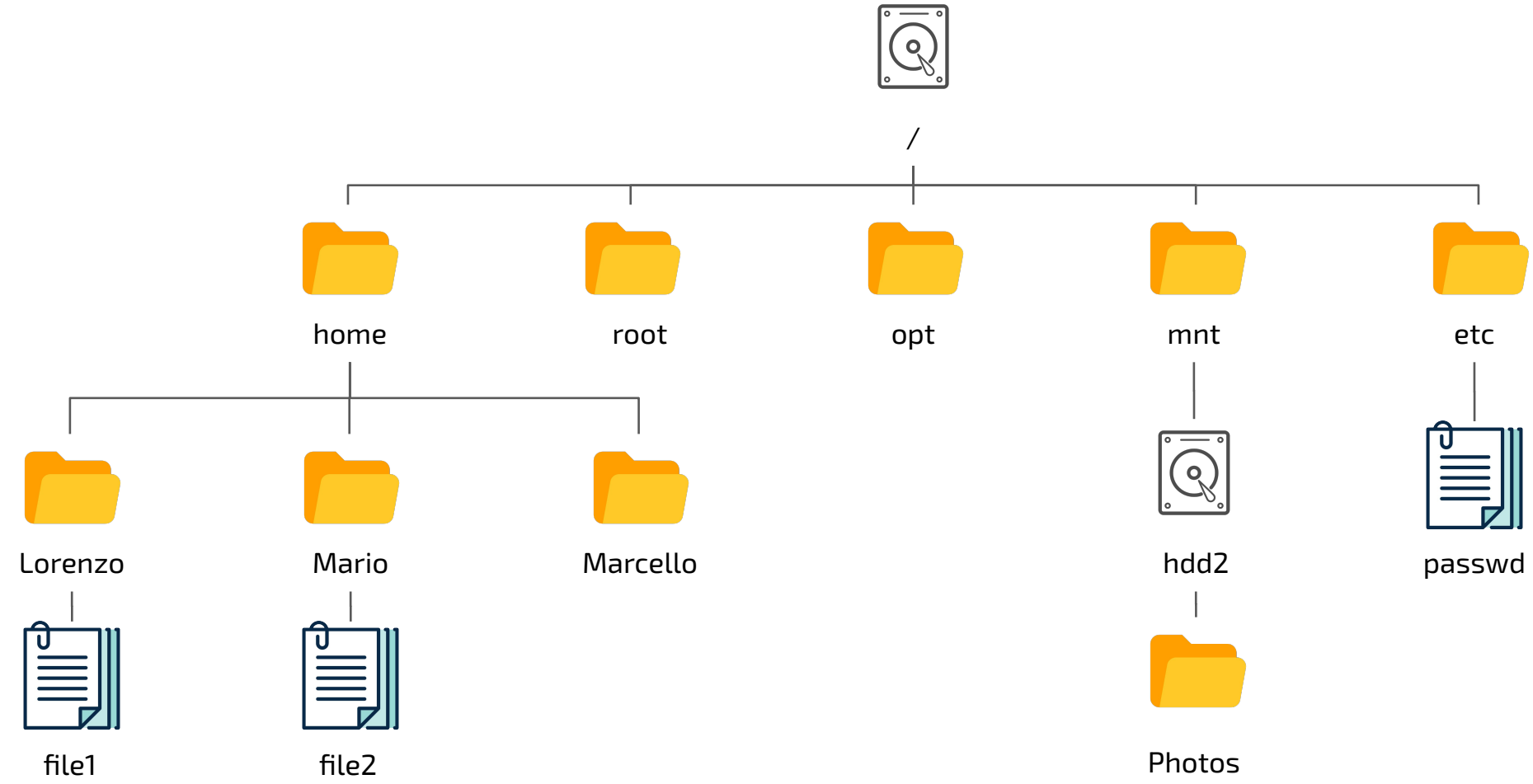
Tutti i sistemi operativi commerciali implementano il **DAC** (Discretionary Access Control):

- Windows
- Linux e altre varianti di UNIX
- Mac OS X
- Anche molte applicazioni e social network utilizzano prevalentemente il modello DAC!

Esempi di sistemi DAC

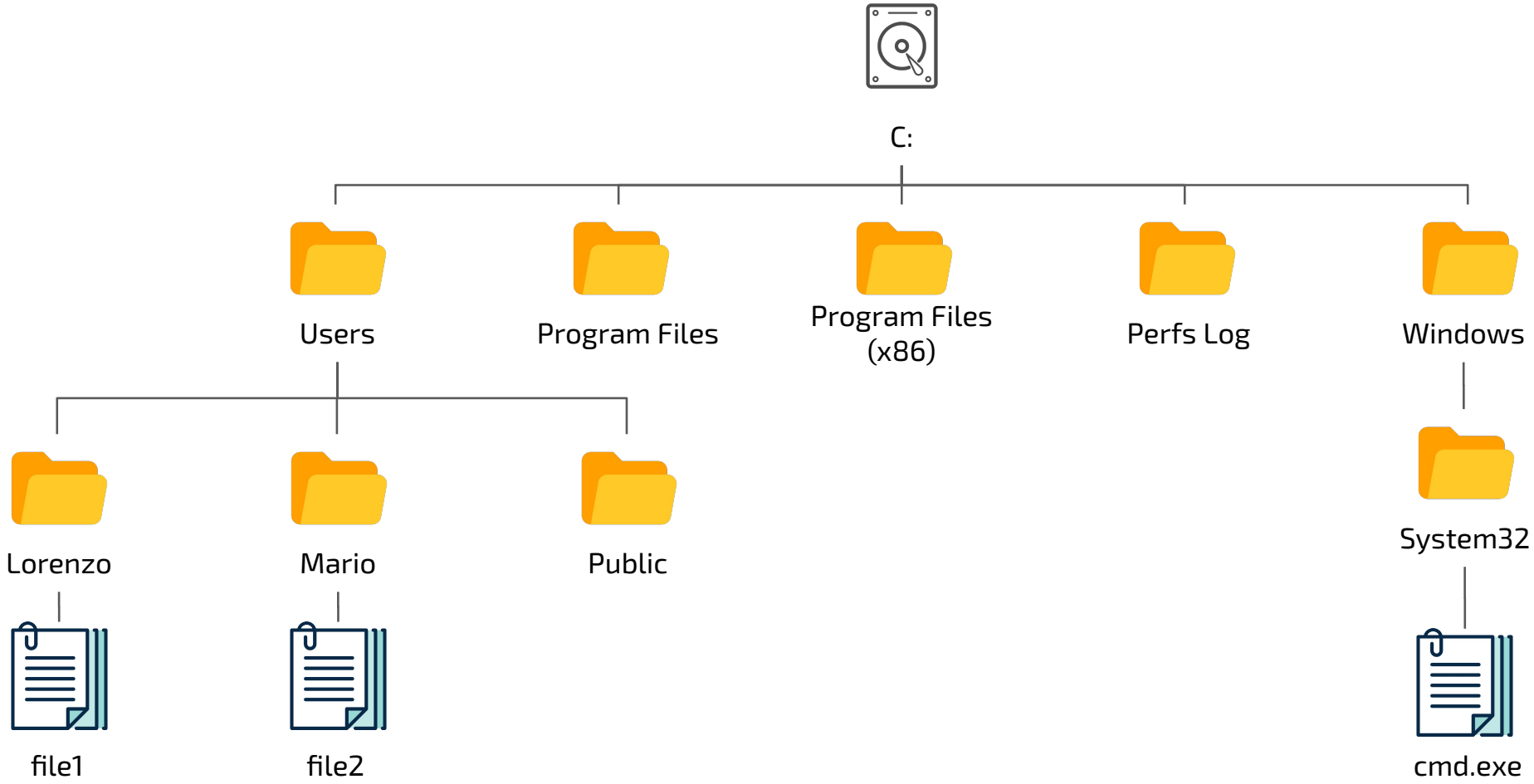
- **UNIX**
  - **Soggetti**: utenti, gruppi
  - **Oggetti**: file
  - **Azioni**: leggi (read), scrivi (write), esegui (execute)
- **Windows**
  - **Soggetti**: con ruoli al posto del gruppo, proprietà multipla di utenti e ruoli sui file
  - **Oggetti**: file
  - **Azioni**: cancella, leggi, scrivi, esegue, cambia permessi, cambia proprietà

Percorsi nei sistemi UNIX



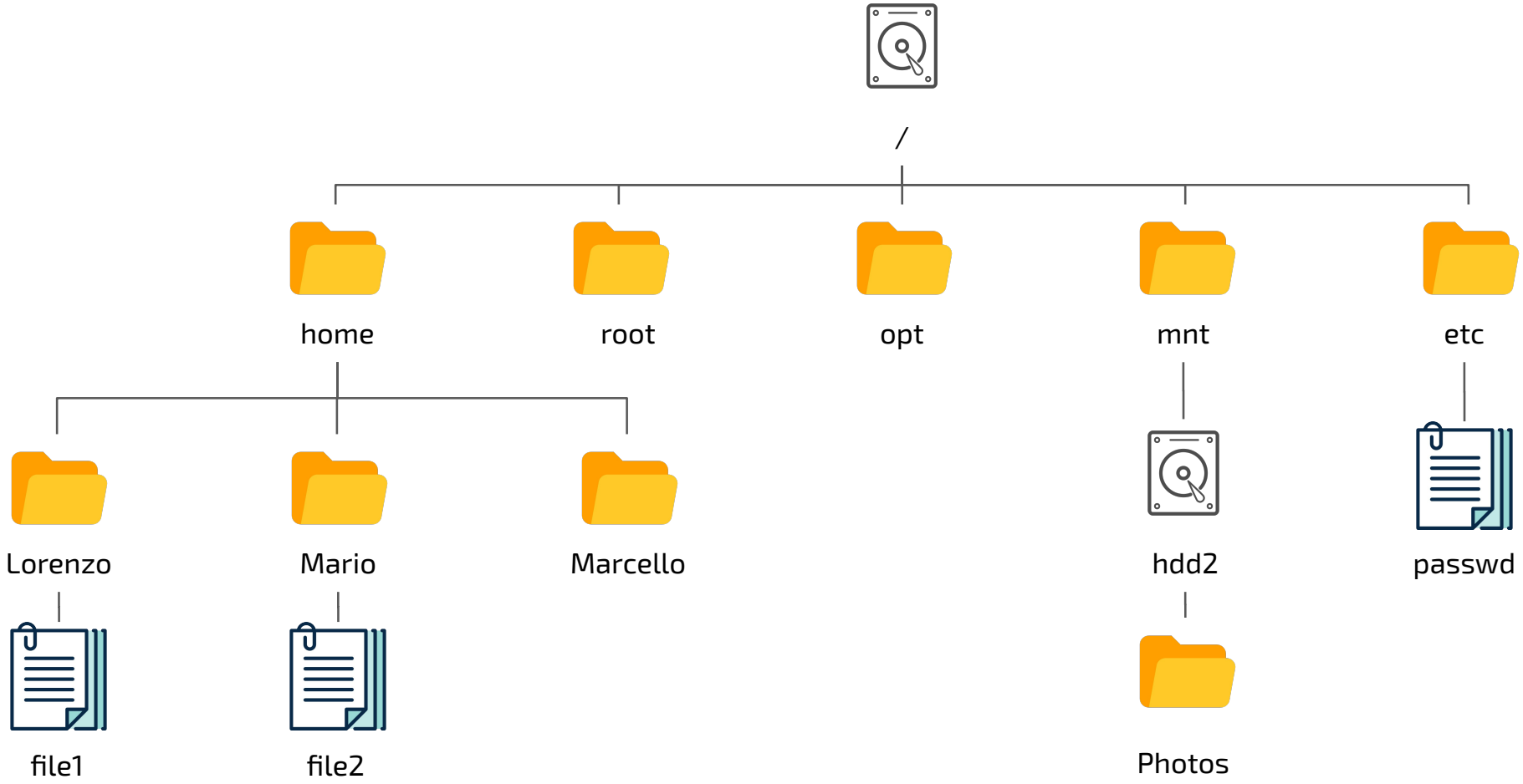

```
/home/Lorenzo/file1
/etc/passwd
```

Percorsi nei sistemi Windows



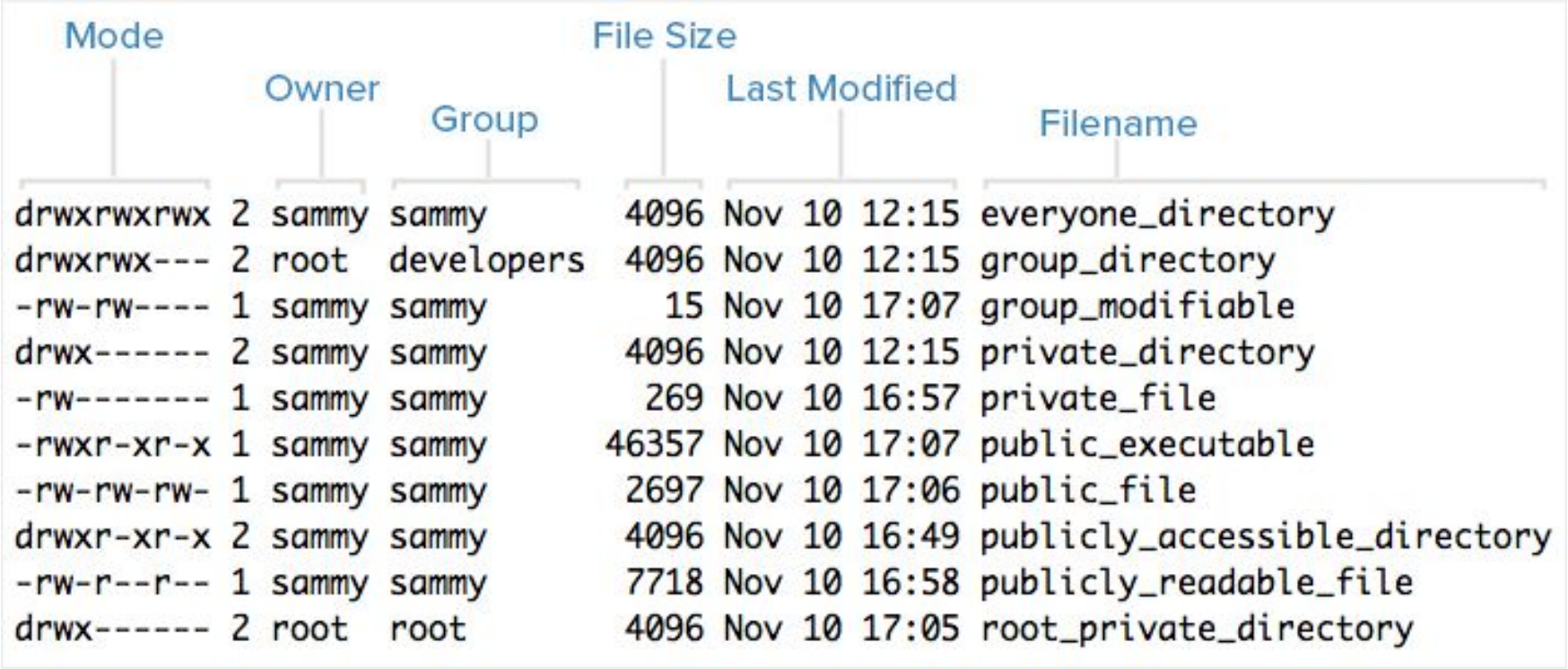

```
C:/Users/Lorenzo/file1
C:/Windows/System32/cmd.exe
```

Percorsi relativi

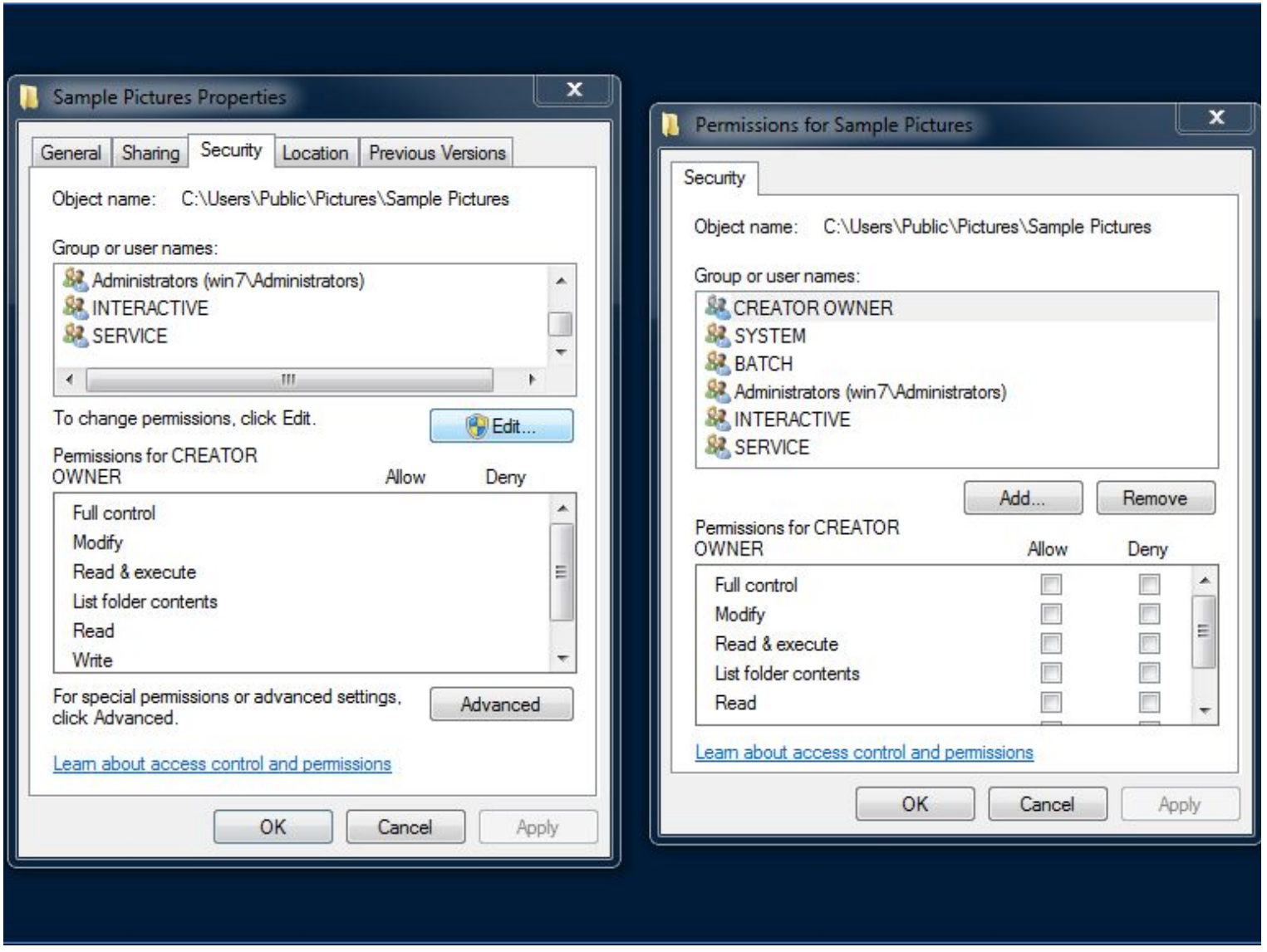


Dalla cartella **Mario**: ../../etc/passwd (Relativo)
Equivalente a: /etc/passwd (Assoluto)

Permessi nei sistemi UNIX



Permessi nei sistemi Windows



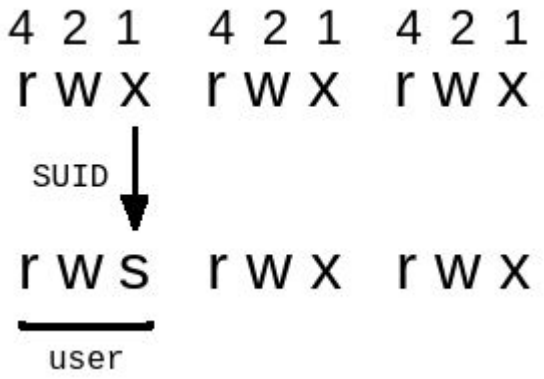
Modello generale di un sistema DAC

- Dobbiamo modellare le seguenti entità:
  - **Soggetti** che possono esercitare privilegi (o diritti).
  - **Oggetti** sui quali vengono esercitati i privilegi.
  - **Azioni** che possono essere esercitate.
- **Stato di protezione**: una tripla (S, O, A)
  - A: matrice con S righe e O colonne
  - A[s, o]: privilegi del soggetto sull'oggetto o

	Percorso file 1	**Percorso file 2**	**Percorso directory 1**
Alice	Read	Read, Write, Execute	
Bob	Read, Write, Execute	Read	Read, Write, Execute
Charlie	Read, Write		Read

Concessione di privilegi

In alcuni casi, un utente può eseguire un file con i permessi del proprietario (occorre avere il permesso di esecuzione su “others”).



Mandatory Access Control (MAC)

Idea: non lasciare la scelta dei privilegi agli utenti.

I privilegi sono impostati da un amministratore:

- Ad esempio, definisce una classificazione dei soggetti (o “livelli di autorizzazione”) e degli oggetti (o “livelli di sensibilità”).

La classificazione è composta da:

- Un insieme strettamente ordinato di livelli di segretezza.
- Un insieme di etichette.

Livelli di segretezza (US)

Top Secret

>

Secret

>

For Official Use Only (FOUO)

>

Unclassified

Livelli di segretezza (NATO)

COSMIC Top Secret

>

NATO Secret

>

NATO Confidential

>

Unclassified

Etichette (Labels)

Policy

Energia

Finanza

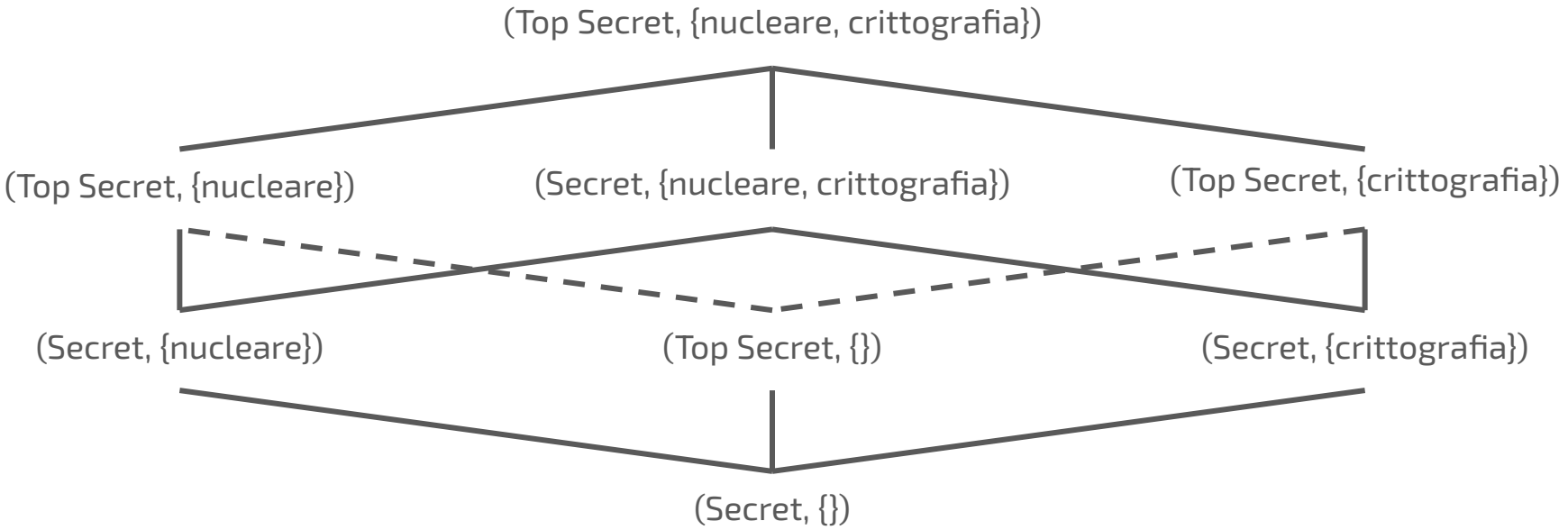
Nucleare

others…

Classificazione = una relazione d'ordine parziale.

La dominanza in un reticolo è definita come:

$$\{C_1, L_1\} \geq \{C_2, L_2\} \Leftrightarrow C_1 \geq C_2 \text{ e } L_2 \subseteq L_1$$



Conclusioni

Il **controllo degli accessi**, o autorizzazione, definisce i soggetti, gli oggetti e le azioni in un sistema.

I **modelli** di controllo degli accessi definiscono come le azioni vengono (o non vengono) assegnate ai soggetti e agli oggetti.

I **DAC (Discretionary Access Control)** sono più comuni e "naturali" dei **MAC (Mandatory Access Control),** ma possono coesistere.