

Una politica di sicurezza definisce ciò che è consentito, è analogo ad un insieme di leggi.

Esempio: uno studente ha pieno accesso alle info. da lui create, studenti non hanno accesso a risorse create da altri studenti.

SECURITY POLICIES:

Il controllo degli accessi può essere raggruppato in 3 classi principali

- DISCRETIONARY (DAC)
- MANDATORY (MAC)
- ROLE-BASED (RBCA)

-DISCRETIONARY ACCESS CONTROL (DAC)

Il proprietario di una risorsa è in grado di modificare la sua autorizzazione a sua discrezione, di solito possono anche decidere di trasferire la proprietà ad altri utenti.

Era molto flessibile, ma è aperto ad errori, abusi (ad es: un cavallo di Troia) o negligenze (richiede che tutti gli utenti comprendano e rispettino la politica di sicurezza).

-ACCESS CONTROL MATRIX MODEL:

Quadro semplice per descrivere un sistema di protezione:

SOGGETTI: utenti, processi, gruppi ...

OGGETTI: dati, banche di memoria, processi ...

PRIVILEGI: leggere, scrivere, modificare

formano la tripla $(S \times O \times P)$, essa viene definito uno stato di protezione

→
è una matrice che
definisce i privilegi
per ogni $(S \times O)$

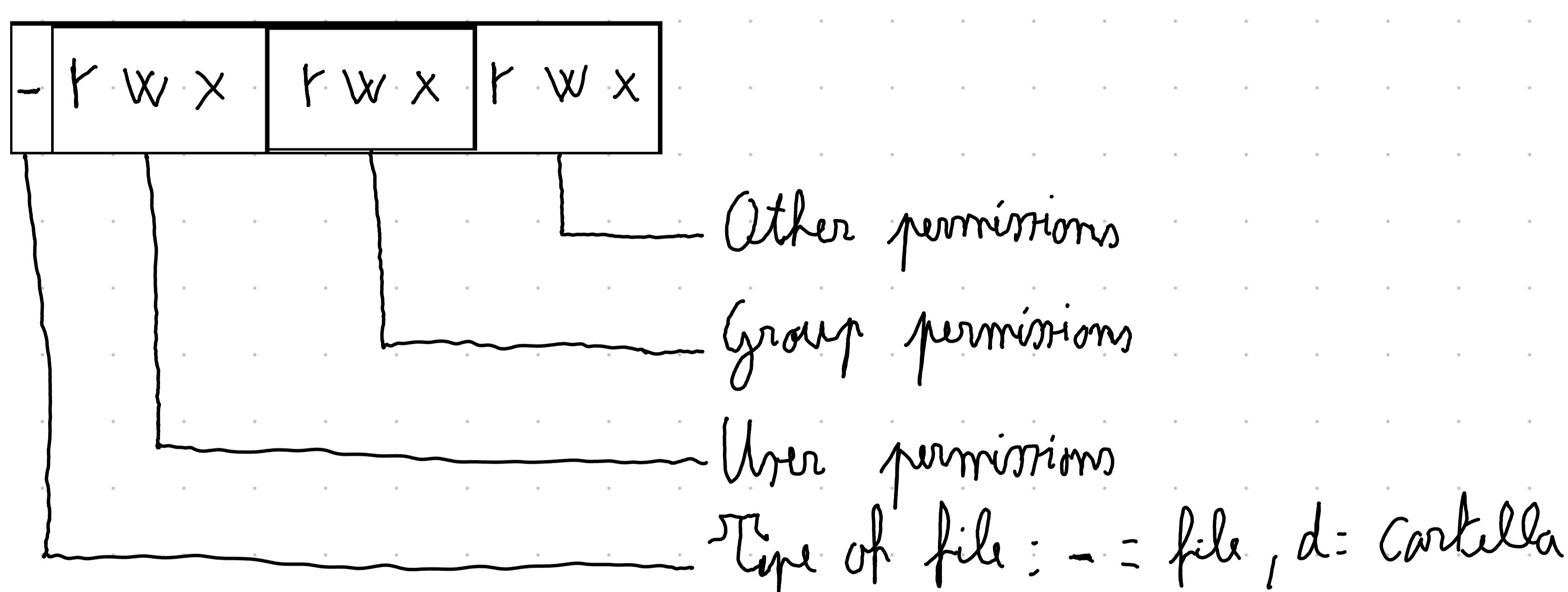
DAC usato su UNIX:

Unix ha un semplice meccanismo basato su un ACL semplificato per una classe stretta di policy della DAC.

Control Acces per oggetto usano lo schema dei permessi: OWNER/GROUP/OTHER

Gli oggetti sono assegnati ad un singolo utente (owner) ed un singolo gruppo di appartenza, possono essere poi cambiate con i comandi UNIX: CHOWN (change owner) e CHGRP (change group)

I bit di permesso sono assegnati ad un oggetto dal suo OWNER o da root tramite il comando CHMOD



Poi esistono anche i SPECIAL MODE BITS: essi riguardano solo i file eseguibili (.exe)

- MANDATORY ACCESS CONTROL (MAC)

Decisione CA formalizzata confrontando le etichette, le quali indicano la criticità degli oggetti.

Esempio militare: utenti e oggetti assegnati ad un livello di sicurezza "secret" o "top-secret", gli utenti possono leggere solo oggetti di uguale o inferiore livello.

Più rigido del DAC ma anche più sicuro.

Esistono vari tipi di modelli di sicurezza MAC

- BELL-LAPADULA (BLP): viene sviluppato per soddisfare le richieste di sicurezza e riservatezza del Dipartimento di Sicurezza Americana.

LP modella la riservatezza combinando aspetti del DAC e MAC, infatti i permessi di accesso sono definiti sia attraverso una matrice A (che attraverso livelli di sicurezza, sicurezza multilivello (MLS): le politiche obbligatorie impediscono il flusso di informazioni verso il basso da un alto livello di sicurezza verso uno basso).

$$\text{read} \rightarrow X_s \geq X_o \rightarrow X_o \leq X_s$$

$$\text{write} \rightarrow X_o \geq X_s \rightarrow X_s \leq X_o$$