**Altri metodi di autenticazione**

Usano dei Token:

* carte magnetiche
* smart card
* bluetooth tokens
* nfc tokens

i token generano una password per l’autenticazione a 2 fattori

autenticazione biometrica, non vengono solitamente usate in modo singolo, ma come conferma o avere una chiave registrata sul sistema e si sblocca tramite la scansione biometrica

**Autorizzazione**

Ci sono 3 tipi di autorizzazione:

* DAC: controllo discrezionale
* MAC: controllo obbligatorio
* RBAC: basato sui ruoli

**DAC (**Discretionary Access Control)

Discretionary Access Control (DAC) è un tipo di modello di controllo degli accessi che consente agli utenti di controllare l'accesso alle risorse di cui sono proprietari o a cui è stato concesso l'accesso. In un sistema DAC, gli utenti sono responsabili di specificare chi è autorizzato ad accedere alle proprie risorse ea quale livello di accesso. In un sistema DAC, l'accesso alle risorse viene generalmente concesso in base all'identità dell'utente o del processo che richiede l'accesso. Utenti e processi sono in genere associati a uno o più identificatori di sicurezza, come un nome utente o un'appartenenza a un gruppo, che vengono utilizzati per determinare i loro diritti di accesso.

DAC è spesso in contrasto con altri modelli di controllo degli accessi, come il controllo degli accessi obbligatorio (MAC) e il controllo degli accessi basato sui ruoli (RBAC), che hanno approcci diversi per specificare e applicare le regole di controllo degli accessi. DAC è spesso considerato più flessibile di questi altri modelli, in quanto consente agli utenti di specificare le proprie regole di controllo degli accessi e di modificarle secondo necessità.

I sistemi DAC sono spesso utilizzati in ambienti in cui gli utenti hanno diversi livelli di accesso alle risorse e in cui il livello di accesso dipende dall'identità dell'utente. Esempi di tali ambienti includono reti aziendali, in cui i dipendenti possono avere diversi livelli di accesso alle risorse in base al loro ruolo lavorativo, e reti domestiche, in cui i membri della famiglia possono avere diversi livelli di accesso alle risorse condivise.

Il proprietario della risorsa decide chi può accedervi

Il problema del dac è che l’amministratore di sistema sa chi ha accesso , ma gli altri no

Esempio permesso di unix sono DAC

Immagine che contiene testo

Descrizione generata automaticamente

**MAC (**Mandatory Access Control)

L’amministratore di sistema può imporre dei vincoli agli utenti che non possono aggirare

**Immagine che contiene tavolo

Descrizione generata automaticamente**

Vi sono 2 propietà basate sul dac e livelli di sicurezza multipli:

* Simple security condition: un utente o processo non può accedere a informazioni targettizate con un livello di sicurezza più alto
* \*(start) property: un utente o processo non può scrivere su un livello di classificazione inferiore

Immagine che contiene testo

Descrizione generata automaticamente

**Implementazioni MAC**

**LSM (Linux Security Modules)**

È un framework che fornisce i collegamenti nel kernel per interagire con le system calls per accedere agli oggetti del kernel

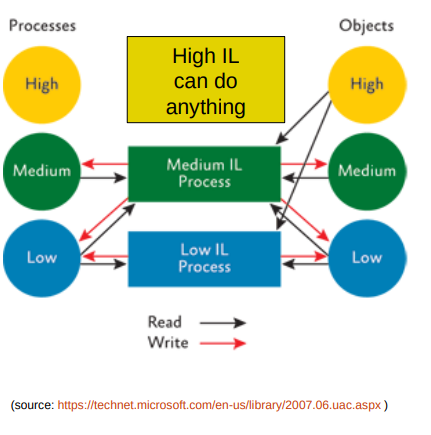
su Ubuntu si usa AppArmor e basa le policy sui profili

**SELinux**

SELinux supporta anche RBAC che consente di avere dei ruoli specifici con permessi diversi

**Il kernel verifica prima i permessi DAC e successivamente i MAC, questi due permessi convivono sui sistemi.**

In windows il MAC è costituito dagli Integrity Levels che hanno il compito di mantenere l’integrità



I livelli possono operare del livello attuale a tutti i livelli inferiori ad esso.

Su MAC OSX usa TrustedBSD / Seatbelt

TrustedBSD è un MAC implementato per FREEBSD e anche usato da MACOS

Sopra seatbelt è possibile creare dei profili.