Protezione nei Sistemi Operativi

Return

Indice

Protezione e Sicurezza

Sicurezza:

Riguarda l'insieme delle **tecniche per regolamentare l'accesso** degli utenti al sistema di elaborazione. La sicurezza impedice accessi non autorizzati al sistema e i conseguenti tentativi dolosi di alterazione e distruzione dei dati.

Le tecnologie di sicurezza di un sistema informatico realizzano meccanismi per **l'identificazione, l'autenticazione** e **l'autorizzazione** di utenti "fidati"

Protezione:

Insieme di attività volte a garantire il controllo dell'accesso alle risorse logiche e fisiche da parte degli utenti autorizzati all'uso di un sistema di elaborazione.

Per ogni utente **identificato, autenticato e autorizzato, è necessario stabilire:**

- quali siano le **risorse** alle quali può accedere
- con quali **operazioni** può accedervi

Questo è stabilito dal **sistema di protezione** tramite le tecniche di **controllo degli accessi**.

In un sistema il **controllo degli accessi** si esprime tramite la definizione di **tre** livelli concettuali:

- **modelli**
- **politiche**
- **meccanismi**

Modelli

Un **modello di protezione** definisce soggetti, oggetti ai quali si soggetti hanno accesso ed i **diritti** di accesso:

- **oggetti** costituiscono la parte **passiva**, cioè le risorse fisiche e logiche alle quali si può accedere e su cui si può operare.

  > Esempio: file, processi, dispositivi di I/O

- **soggetti** rappresentano la parte attiva di un sistema, cioè le entità che possono richiedere l'accesso alle risorse.

  > Esempio: utenti, processi

- **diritti di accesso** sono le modalità con cui i soggetti possono accedere agli oggetti.

Politiche

Le **politiche di protezione** definiscono le regole che determinano quali operazioni possono essere eseguite su quali oggetti da parte di quali soggetti.

Classificazione delle politiche:

- **Discretional Access Control (DAC)**: per ogni oggetto si individua un solo soggetto che stabilisce le regole di accesso per quell'oggetto, devisione diritti decentralizzata.
- **Mandatory Access Control (MAC)**: decisione dei diritti centralizzata, sistemi ad alta sicurezza

- **Role Based Access Control (RBAC)**: l'accesso è basato sui ruoli che un utente può avere all'interno di un sistema.

Principio del privilegio minimo

Ad ogni soggetto sono garantiti i diritti di accesso solo agli oggetti strettamente necessari per svolgere il proprio compito.

> **POLA** (Principle of Least Authority)

Meccanismi

I **meccanismi di protezione** sono le procedure e le strutture dati che implementano le politiche di protezione. Tutto ciò che il S.O. usa per garantire il rispetto delle politiche.

Principi di realizzazione

- **Flessibilità** del sistema di protezione: I meccanismi di protezione devono essere sufficientemente generali per consentire l'applicazione di diverse politiche di protezione.
- **Separazione** tra meccanismi e politiche: La politica definisce cosa va fatto ed il meccaniscmo come va fatto. È desiderabile la massima indipendenza tra le due componenti

Dominio di protezione

Ad ogni soggetto è associato un dominio che rappresenta l'ambiente di protezione nel quale il soggetto esegue, il dominio specifica i diritti di accesso posseduti dal soggetto nei confronti di ogni risorsa.

Le operazioni vengono svolte da processi che operano per conto di soggetti (a cui sono associati i domini)

Un dominio di protezione è **unico per ogni soggetto**, mentre un processo può eventualmente **cambiare dominio** durante l'esecuzione.

> DEF: Un dominio definisce un insieme di coppie, ognuna contenente l'identificatore di un oggetto e l'insieme delle operazioni che il soggetto associato al dominio può eseguire su ciascun oggetto (diritti di accesso):

$$ D = { <o, diritti> | o\ è\ un\ oggetto, diritti\ è\ un\ insieme\ di\ operazioni } $$

Ogni dominio è associato ad un **soggetto**, il soggetto può accedere solo agli oggetti definiti nel suo dominio, utilizzando i diritti specificati dal dominio.

Domini disgiunti o domini con diritti di accesso in comune

Possibilità per due o più soggetti di effettuare alcune operazioni comuni su un oggetto condiviso:

Le operazioni vengono svolte da processi che operano per conto di soggetti (a cui sono associati i domini)

In ogni istante della sua esecuzione, il processo esegue in uno ed un solo dominio.

Associazione tra processo e dominio

Statica

L'insieme delle risorse disponibili ad un processo rimane fisso durante il suo tempo di vita.

Osservazioni:

- L'insieme globale delle risorse che un processo potrà usare può non essere un'informazione disponibile prima dell'esecuzione del processo.
- L'insieme minimo (politica del minimo privilegio) delle risorse necessarie ad un processo cambia dinamicamente durante l'esecuzione.

> L'associazione statica non è adatta nel caso si voglia limitare per un processo l'uso delle risorse a quello strettamente necessario (privilegio minimo)

Dinamica

Associazione tra processo e dominio varia durante l'esecuzione del processo.

In questo modo si può mettere in pratica il principio del privilegio minimo, in ogni fase della sua esecuzione il processo acquisisce diritti diversi (solo quelli necessari).

- Occorre un meccanismo per consentire il passaggio da un dominio all'altro del processo.

Cambio di dominio esempio

Standard dual mode (kernel mode e user mode)

- Cambio di dominio associato alle system call: quando un processo deve eseguire un'istruzione privilegiata avviene un cambio di dominio.

Non realizza la protezione tra utenti ma solo tra kernel e utente.

Matrice degli accessi

Un sistema di protezione può essere rappresentato a livello astratto utilizzando la matrice degli accessi.

- Ogni riga è associata ad un soggetto (riga=dominio)
- Ogni colonna è associata ad un oggetto

La matrice consente di rappresentare il modello e le politiche valide nel sistema considerato, specificando:

- Soggetti
- Oggetti
- Diritti accordati ai soggetti sugli oggetti

Le informazioni contenute nella matrice possono variare nel tempo per effetto di operazione che ne consentono la modifica: (creazione di nuovi soggetti, creazione di nuovi oggetti, modifica dei diritti di accesso)

Le infomrazioni contenute nella matrice all'istante t rappresentano lo stato del sistema di protezione in quel momento.

La matrice degli accessi offre ai meccanismi di protezione le informazioni che consentono di verificare il rispetto dei vincoli di accesso.

Meccanimsi

Il meccanismo:

- ha il compito di verificare se ogni richiesta di accesso che proviene da un processo che opera in un determinato dominio è consentita oppure no.
- Autorizza l'esecuzione delle richieste consentite e impedisce quelle vietate.
- Esegue la modifica (in modo controllato) dello stato di protezione in seguito ad ogni richiesta autorizzata da parte di un processo.

Verifica del rispetto dei vincoli di accesso:

Il meccanismo consente di assicurare che un processo che opera nel dominio D_i può accedere solo agli oggetti specificati nella riga i e solo con i diritti di accesso indicati.

Quando un'operazione M deve essere eseguita nel dominio D_i sull'oggetto O_j il meccanismo verifica che l'operazione M sia consentita dal diritto di accesso specificato nella cella $access(i,j)$ della matrice degli accessi.

In caso affermativo l'operazione può essere eseguita. In caso negativo si ha una situazione di errore.

Modifica dello stato di protezione

Chi può modificare lo stato di protezione?

-**MAC (Mandatory Access Control)**: il sistema decide chi può modificare lo stato di protezione, entità centrale. -**DAC (Discretionary Access Control)**: il proprietario dell'oggetto può modificare lo stato di protezione.

Modello di Graham-Denning

Il modello di Graham-Denning è un modello di protezione che definisce un insieme di regole per la protezione delle risorse di un sistema.

8 Primitive:

1. create object
2. delete object
3. create subject
4. delete subject
5. read access right
6. grant access right
7. delete access right
8. transfer access right

creazione, eliminazione di righe e colonne (1,2,3,4). Modifica dei diritti di accesso, cancellazione e propagazione (5,6,7,8).

Propagazione dei diritti di accesso

La possibilità di copiare un diritto di accesso per un oggetto da un dominio ad un altro della matrice di accesso è indicato un un asterisco (*), (copy flag):

- Un soggetto S_i può trasferire un diritto di accesso α per un oggetto X ad un altro soggetto S_j solo se S_i possiede il diritto di accesso α per l'oggetto X, e α ha il copy flag.

Diritto Owner

Assegnazione di un qualunque diritto di acesso su un oggetto X ad un qualunque soggetto S_j da parte di un soggetto S_i.

L'operazione è consentita solo se il diritto OWNER appartiene a $A[S_i,X]$.

Diritto Control

Eliminazione di un diritto di accesso per un oggetto X nel dominio di S_j da parte di S_i.

L'operazione è consentita solo se il diritto CONTROL appartiene a $A[S_i,S_j]$. oppure OWNER appartiene a $A[S_i,X]$.

ACL (Access Control List)

Per ogni risorsa del sistema si ha una lista contenente le coppie `<soggetto, diritti>` che possono accedere alla risorsa.

Molti sistemi hanno il concetto di gruppo di utenti.

I gruppi possono essere inclusi nella ACL `<uid, gid, diritti>`.

Capability list

Per ogni soggetto del sistema si ha una lista contenente `<tipo, diritti, oggetto>`

Revoca dei diritti di accesso

In un sistema può essere necessario revocare i diritti di accesso per un oggetto.

Può essere:

- Generale o Selettva: per tutti gli utenti che hanno quel diritto o per una parte.
- Totale o Parziale: per tutti i diritti o solo alcuni.
- Temporanea o Permanente: per un periodo di tempo o definitiva.

L'utilizzo di solo ACL o CL può non essere ottimale, infatti con ACL tutti i diritti di un soggetto sono sparsi e con CL lo sono quelli di un oggetto. in un caso più facile lavorare con soggetti nell'altro con oggetti.

Soluzione: **ACL e CL insieme**.

Sicurezza Multilivello

Modello di sicurezza in cui oggetti e soggetti sono classificati in livelli.

I modelli multilivello più diffusi sono: **Bell-LaPadula** e **Biba**, entrambi basati su due regole MAC (Mandatory Access Control):

Bell-LaPadula

- **Proprietà di semplice sicurezza:** un processo può leggere solo oggetti al suo livello o inferiore
- **Proprietà :* Un processo può scrivere oggetti solo al suo livello o superiore

Queste regole si affiancono alle informazioni contenute nella matrice degli accessi. Il flusso di informazioni è dal basso verso l'alto, il modello non assicura l'integrità delle informazioni, ne assicura la riservatezza, infatti è possibile sovrascrivere l'informazione appartenente ad un livello superiore.

> **Esempio cavallo di Troia**: Un utente crea il File con informazioni riservate, i permessi di lettura/scrittura solo per processi che appartengono a lui. Utente ostile ottenuto accesso al sistema, installa file Cavallo di Troia e copia nel file system un file privato che verrà utilizzato come backdoor. Ostile ha permessi di lettura e scrittura per il file. Ostile da a utente il permesso di scrittura su Fm Ostile da a utente il diritto di esecuzione su CT Ostile fa eseguire il Cavallo di Toria a utente Il CT eseguito da utente ha quindi permessi di lettura e scrittura su File riservato, e ne copia il contenuto su backdoor.

Soluzione: Venono fissati due livelli di sicurezza:

- Ai processi e ai file di utente viene assegnato il livello di sicurezza riservato
- A quelli di Ostile il livello pubblico

BIBA

Obiettivo integrità dei dati

1. **Proprietà di semplice sicurazza:** Un processo può scrivere solamente oggetti al suo livello o inferiore
2. **Proprietà :* Un processo può leggere solo oggetti al suo livello o superiore

I due modelli sono complementari, Bell-LaPadula assicura la riservatezza, mentre Biba l'integrità. Non possono essere utilizzati contemporaneamente.

Sistemi ad eleavata sicurezza

Reference Monitor: Un componente dell' O.S. che regola l'accesso alle risorse e impone le regole di sicurezza

Trusted Computing Base: Parte dell' O.S. che implementa il Reference Monitor contiene i privilegi dei soggetti e gli attributi degli oggetti

Ogni operazione è salvata su file di audit

Nella realizzazioone di un RM andrebbero rispettate le proprietà:

- Mediazione completa: Le regole di sicurezza vengono controllate ad ogni accesso e non solo, per esempio, durante l'apertura di un file. Questo è oneroso a livello di computazionale, preferibile quindi l'uso di Hardware dedicato.
- Isolamento: Referemce Monitor e TCB devono essere isolati dal resto del sistema, in modo che non possano essere alterati.
- Verificabilità: Deve essere possibile verificare che il RM e il TCB siano corretti e che non contengano errori.