SISTEMI OPERATIVI

File System
Protezione

Lezione 2 – Tecniche di realizzazione della protezione

Vincenzo Piuri

Università degli Studi di Milano

Sommario

- Matrice d’accesso
- Liste di controllo degli accessi
- Liste di capacità dei domini

Realizzazione dei domini di protezione

Rappresentazione

- Matrice degli accessi

Implementazioni

- Matrice completa
- Liste di controllo degli accessi
- Liste di capacità dei domini
- Meccanismo serrature-chiavi (lock-key)

Matrice d'accesso

dominio \ oggetto	F_1	F_2	F_3	stampante
D_1	leggi		leggi	
D_2				stampa
D_3		leggi	esegui	
D_4	leggi scrivi		leggi scrivi	

Matrice d'accesso con domini

oggetto / dominio	F_1	F_2	F_3	stampante laser	D_1	D_2	D_3	D_4
D_1	leggi		leggi			switch		
D_2				stampa			switch	switch
D_3		leggi	esegui					
D_4	leggi scrivi		leggi scrivi		switch			

Matrice di accesso con diritti di copia

dominio \ oggetto	F_1	F_2	F_3
D_1	esegui		scrivi*
D_2	esegui	leggi*	esegui
D_3	esegui		

Prima della copiatura

Dopo la copiatura

dominio \ oggetto	F_1	F_2	F_3
D_1	esegui		scrivi*
D_2	esegui	leggi*	esegui
D_3	esegui	leggi	

Matrice di accesso con diritti di proprietà

dominio \ oggetto	F_1	F_2	F_3
D_1	proprietario esegui		scrivi
D_2		leggi* proprietario	leggi* proprietario scrivi*
D_3	esegui		

Prima della copiatura

Dopo la copiatura

dominio \ oggetto	F_1	F_2	F_3
D_1	proprietario esegui		
D_2		proprietario leggi* scrivi*	leggi* proprietario scrivi*
D_3		scrivi	scrivi

Uso della matrice di accesso

Raccoglie tutte le informazioni sui diritti di uso

Supporta meccanismi di protezione dinamica

Liste di controllo degli accessi

Per ogni risorsa viene conservata la lista dei diritti per ogni dominio

risorsa: {<dominio,diritto>}

dominio \ oggetto	F_1	F_2	F_3	stampante laser	D_1	D_2	D_3	D_4
D_1	leggi		leggi			switch		
D_2				stampa			switch	switch
D_3		leggi	esegui					
D_4	leggi scrivi		leggi scrivi		switch			

Liste di capacità dei domini

Per ogni dominio viene conservata la lista dei diritti per ogni risorsa

dominio: {<risorsa,diritto>}

oggetto / dominio	F_1	F_2	F_3	stampante laser	D_1	D_2	D_3	D_4
D_1	leggi		leggi			switch		
D_2				stampa			switch	switch
D_3		leggi	esegui					
D_4	leggi scrivi		leggi scrivi		switch			

Revoca dei diritti (1)

Lista di controllo degli accessi

- Rimuovere i domini e/o i diritti dalla lista della risorsa
- Revoca immediata
- Revoca generale o selettiva
- Revoca totale o parziale
- Revoca permanente o temporanea

Revoca dei diritti (1)

Liste delle capacità dei domini

- Diritti sparsi nelle liste
- Riacquisizione
- Puntatori alle capacità
- Indirezione
- Chiavi

Confronto

Liste di controllo degli accessi

- Possono essere specificate dagli utenti
- Informazioni globali
- Inefficienti su grandi sistemi

Liste delle capacità dei domini

- Relative agli oggetti
- Informazioni localizzate
- Revoca inefficiente

Meccanismo serratura-chiave

lock-key

Serratura e chiave definite da stringhe di bit

Il processo può eseguire
una operazione su una risorsa
se la sua chiave
combacia
con la serratura
per l'operazione indicata

Sistemi operativi basati sulle capacità

Mettono a disposizione un approccio nativo all'uso di risorse basato sulle capacità

- Utenti possono definire e controllare capacità

Protezione basata sul linguaggio (1)

Protezione può essere incorporata nel linguaggio di programmazione

- Gestione affidata al compilatore
- Riferimenti verificati in fase di compilazione o in esecuzione

Protezione basata sul linguaggio (2)

Controllo più granulare

- Progettista (meccanismi, regole base)
- Amministratore (politiche)
- Utente/programmatore (diritti aggiuntivi)

Rispetto ad una protezione basata sul kernel:

- minor sicurezza
- maggior flessibilità
- maggior efficienza

In sintesi

Abbiamo visto:

- Matrice d'accesso
- Liste di controllo degli accessi
- Liste di capacità dei domini

Notiamo che:

- Alcuni sistemi permettono all'utente di definire diritti aggiuntivi
- Linguaggi di programmazione orientati alla protezione permettono una granularità più fine dei diritti d'accesso