Sviluppo di sistemi operativi sicuri

Lezione 19 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2007-8

Indice

principi di progetto della protezione

alcuni principi di progetto proposti da (Saltzer & Schroeder, 1975):

- minimo privilegio
- economia del meccanismo
- struttura aperta (pubblicità)
- mediazione completa
- basato su autorizzazione
  - esplicita (i.e., default: negazione)
- separazione dei privilegi
  - molteplicità di condizioni per l'accesso
- minimo meccanismo comune
  - separazione fisica o logica per ridurre i rischi della condivisione
- facilità d'uso

caratteristiche di sicurezza nei s.o.

caratteristiche di normali sistemi operativi rilevanti alla sicurezza:

- autenticazione degli utenti
- protezione della memoria
- controllo degli accessi a file e periferiche I/O
- autorizzazione, allocazione e controllo degli accessi a oggetti generici
- controllo della condivisione
  - ad es., controlli di integrità
- fairness, o equità di servizio
- sincronizzazione e comunicazione fra processi (IPC)
  - deve essere mediata dai meccanismi di controllo di accesso
- protezione dei dati di protezione del s.o.
  - di evidentemente cruciale importanza

funzionalità di protezione nei s.o. sicuri

"sicuro" = degno di fiducia

- autenticazione e identificazione degli utenti
- controllo degli accessi obbligatorio (MAC)
- controllo degli accessi discrezionale (DAC)
- protezione dal riuso di oggetti
  - ad es.: fenomeno della **rimanenza magnetica**
- mediazione completa
- Trusted Path Execution (TPE)
  - per la prevenzione dello spoofing
- responsabilità e controllo
- riduzione del registro di **log**
- rilevamento delle intrusioni

progetto basato su kernel di sicurezza

in questo approccio, il kernel di sicurezza (KdS) è incorporato nel kernel del sistema operativo

perché isolare le funzionalità di protezione in un KdS?

- copertura
- separazione
- unità
- modificabilità
- compattezza
- verificabilità

componente essenziale: **monitor di riferimento** (v. appresso)

- per il controllo degli accessi agli oggetti

svantaggi del kernel di sicurezza

i vantaggi dell'isolamento delle funzioni di protezione del sistema operativo in un KdS si pagano con alcuni svantaggi:

- degrado delle **prestazioni**, causato dalle "forche caudine" poste dal KdS tra applicazioni e risorse
- la mera presenza del KdS non garantisce la disponibilità di **tutte** le funzioni di protezione necessarie alle applicazioni
  - né la **correttezza** di quelle presenti!
- il KdS ha un certo **ingombro**, che in dipendenza dalle funzioni realizzate può essere notevole

un buon progetto di sistema operativo sicuro dovrà tener conto di questi aspetti, per limitarne l'impatto

monitor di riferimento

un concetto astratto, realizzato (fra l'altro, ma non solo) dal KdS:

- una macchina astratta di **controllo degli accessi** di soggetti a oggetti

perché sia efficace, il monitor di riferimento deve essere:

- a prova di intrusione
- invocato per tutti gli accessi a qualsiasi oggetto protetto
- abbastanza piccolo e ben strutturato, sì da poter essere analizzato e verificato per ottenere garanzie di correttezza e completezza

la definizione del concetto di monitor di riferimento **non** implica la sua collocazione nel kernel del sistema operativo:

- il KdS realizza il monitor di riferimento per il sistema operativo, ma ...
- possono ben esservi **altri** monitor di riferimento per applicazioni specifiche, o per particolari ambienti di esecuzione (ad es., realizzati da interpreti)

riferimenti

Saltzer & Schroeder (1975) :

The Protection of Information in Computer Systems,
Proc. of the IEEE **63**:9, 1278-1308, 1975.
http://www.acsac.org/secshelf/papers/protection_information.pdf