Trusted Computing Base

Lezione 20 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 2008-9

Indice

1. Trusted Computing Base
2. definizione della TCB
3. funzioni della TCB
4. implementazione di una TCB
5. separazione e isolamento
6. virtualizzazione
7. stratificazione

definizione della TCB

TCB: minima collezione di componenti del sistema operativo sufficiente a garantire la corretta operatività della sua politica di sicurezza

- ogni componente della TCB è **necessario** all'operatività di qualche aspetto della politica di sicurezza
- l'operatività della politica di sicurezza non dipende da componenti esterni alla TCB

collaudo *"tiger team"*:

- permettere la manomissione di qualsiasi componente esterno alla TCB
- verificare che la sicurezza del sistema non può in tal modo venire indebolita

qualità essenziali della TCB:

- **correttezza**
- **completezza**
  - *un sistema operativo è "sicuro" sse lo è la sua TCB*

funzioni della TCB

costituenti tipici della TCB, ovvero componenti interni al suo "perimetro":

- ***hardware, driver*** di dispositivi I/O
- alcune proprietà (di sicurezza) dei **processi**
- alcuni **file** critici per la sicurezza
- **memoria protetta**, ad es. per il monitor di riferimento
- alcune **comunicazioni fra processi**, tipicamente quelli della TCB

interazioni di base controllate dalla TCB:

- attivazione di processi
- cambio del dominio di esecuzione
- protezione della memoria (riservatezza e integrità dei domini)
- operazioni di I/O

implementazione di una TCB

le funzioni di protezione realizzate dalla TCB sono pertinenti a diverse attività del sistema operativo, tipicamente realizzate da moduli distinti e separati

problema: isolare la TCB rispettando la modularità del sistema operativo

l'architettura software del sistema operativo è tipicamente **stratificata** (v. appresso), con un kernel di sicurezza (KdS) distribuito su più strati in base alle funzioni di controllo di accesso realizzate

la TCB include il KdS, e spesso lo estende con ulteriori funzioni necessarie all'operatività della politica di sicurezza

il KdS **può** essere collocato in un solo strato (il più basso sopra l'hardware) dell'architettura del sistema operativo

anche in tale approccio al progetto del sistema operativo, la TCB sarà generalmente distribuita su più strati ***(perché?)***

separazione e isolamento

per la soluzione del problema di isolamento della TCB enunciato sopra, è utile richiamare le quattro principali **forme di separazione** introdotte in una lezione precedente:

- fisica
- temporale
- crittografica
- logica, detta anche "isolamento"

tutte queste forme di separazione sono utilmente impiegabili per la soluzione del problema in questione

la separazione logica è spesso basata su caratteristiche inerenti l'architettura software dello stesso sistema operativo, che semplificano il disegno del monitor di riferimento; esaminiamo due di tali caratteristiche, di notevole generalità:

la **virtualizzazione** e la **stratificazione**

virtualizzazione

storicamente, la virtualizzazione è apparsa in alcuni sistemi operativi degli anni '60 quale tecnica di estensione dello spazio di indirizzamento oltre i limiti della memoria fisica

la **memoria virtuale** disponibile all'utente, realizzata per il tramite della **paginazione**
- non solo **estende** lo spazio di indirizzamento logico di ciascun utente
- ma anche lo **separa** da quelli degli altri utenti

il concetto di ***macchina virtuale***, apparso nel decennio successivo, generalizza quello di memoria virtuale alla virtualizzazione di tutte le risorse disponibili nella sessione di lavoro di ciascun utente: processore, file, dispositivi di I/O, etc.

si ottiene in tal modo non solo la separazione fra gli utenti, ma anche la separazione fra processi di utente e risorse hardware
- questo approccio ha una significativa incidenza sulle **prestazioni**, per il costo computazionale dei meccanismi di traduzione fra livelli distinti del software e di protezione delle risorse effettive, nascoste agli utenti

la stratificazione riduce la complessità delle tecniche di protezione nei sistemi operativi

stratificazione

la stratificazione tipica dell'architettura software di un sistema operativo è concepita per livelli di astrazione rispetto alle risorse fisiche
- si può ben adottare lo stesso approccio alla stratificazione delle funzioni di protezione della TCB per livelli di fiducia, dove la sicurezza garantita da software di un dato livello dipende da quella garantita da software degno di maggior fiducia

il vantaggio generale della stratificazione risiede nell'**incapsulamento** delle funzionalità realizzate da una pila di strati nei **servizi** offerti all'interfaccia superiore della pila stessa
- l'implementazione di ciascun modulo della TCB, al quale sia delegata una data funzionalità di protezione, può ben dover essere realizzata in più strati contigui

ad es., autenticazione di utente, che richiede l'esecuzione di:
- interazione con l'interfaccia di utente
- ricerca dell'identificatore di utente nel DB di autenticazione
- confronto dei dati di autenticazione immessi con quelli nel DB
- eventuale aggiornamento dei dati di autenticazione