Requisiti di protezione delle basi di dati

Lezione 23 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

integrità fisica e logica

integrità fisica:

immunità dei dati da problemi fisici, ad es. cadute di alimentazione

integrità logica:

protezione della struttura logica della base di dati

ad es. **località** delle modifiche ai valori dei singoli elementi

più in generale: rispetto di **vincoli d'integrità**

la protezione dell'integrità fisica richiede la predisposizione di procedure automatiche di **back-up periodico** dei dati, ma non solo...

il ripristino dal **back-up** più recente non dovrebbe costringere gli utenti a ripetere le transazioni successive ad esso

il mantenimento di un **registro delle transazioni** è la soluzione comunemente adottata per soddisfare questo requisito

integrità dell'elemento

per **integrità degli elementi** di una base di dati si intende la loro correttezza e accuratezza

responsabilità degli utenti autorizzati ...

... ma errare è umano, dunque sono utili meccanismi di ausilio al rilevamento e alla correzione di errori nel momento in cui vengono introdotti

tre tipi di meccanismi comunemente presenti nei DBMS a tal fine:

controlli di campo

locali all'insieme dei valori ammissibili per il tipo di dato dell'elemento, o in relazione ai valori di altri elementi

controllo degli accessi

non solo per assicurare che le modifiche siano autorizzate, ma anche per prevenire errori causati da modifiche concorrenti

registro delle modifiche

permette di ripristinare valori corretti, erroneamente modificati

verificabilità

la verificabilità delle operazioni compiute su una base di dati presuppone l'esistenza di una registrazione di tutti gli accessi

- **sia in lettura che in scrittura**

le funzionalità tipicamente offerte dai sistemi operativi non sono adeguate, per l'insufficiente **granularità** di oggetti e operazioni controllati

- ad es. file e procedure, laddove nelle basi di dati occorre il controllo a livello di record e di singole istruzioni del DBMS

la registrazione degli accessi in un DBMS può sia sottostimare che sovrastimare l'informazione a cui un utente ha effettivamente ottenuto accesso:

- sovrastima: problema **pass-through**
- sottostima: deduzione di informazione da altra informazione a cui si accede

controllo degli accessi

i requisiti generali di controllo degli accessi alle basi di dati non sono diversi da quelli già visti per i sistemi operativi, tuttavia ...

... in pratica, il controllo degli accessi è più complesso nei DBMS, per varie ragioni:

- granularità più fine dei dati
  - viste, relazioni, campi, record, elementi, ...
- maggiore articolazione delle modalità di accesso
- esistenza di correlazioni fra i dati
  - problema dell'**inferenza** di dati da altri

limiti alle possibilità di controllo dell'inferenza derivano da:

- necessità di garantire la **disponibilità** dei dati ad accesso autorizzato
- vincoli sulle **prestazioni** del DBMS

autenticazione utente

anche in questo caso, i requisiti di accertamento dell'identità degli utenti sono simili a quelli dei sistemi operativi, tuttavia ...

... l'autenticazione di utente di un DBMS **deve** essere **indipendente** da quella del sistema operativo, poiché:

- gli utenti di un DBMS non sono necessariamente utenti registrati del sistema operativo
  - il DBMS viene tipicamente eseguito come applicazione sul sistema operativo
- non esistono dunque **percorsi trusted** dal DBMS al sistema operativo

è tuttavia possibile dotare un DBMS di interfacce a servizi di autenticazione condivisi con altre applicazioni

- ciò può risultare conveniente sia agli amministratori sia agli utenti

disponibilità

i requisiti di disponibilità dei dati di un DBMS vanno considerati contestualmente a quelli di

- garanzia di riservatezza e integrità
- controllo di accessi concorrenti
- efficienza delle prestazioni

questi problemi sono trattati più in dettaglio nella prossima lezione