Sistemi di protezione del software, dei dati/documenti

Versione 1.7

4 marzo 2006 – 23 marzo 2015

Andrea Nicchi

Bibliografia

- Andrew S. Tanenbaum, Maarten van Steen, *Distributed Systems*, Prentice Hall 2002;
- Gary Govanus, *TCP/IP*, Mc Graw Hill 2005;
- F.Baiardi, A. Tomasi, M. Vanneschi, *Architetture dei sistemi di elaborazione*, Franco Angeli, 1990;
- M. Fugini, F. Maio, P. Plebani, *Sicurezza dei sistemi informatici*, Apogeo 2001;
- Danilo Bruschi, *Il ruolo del software sull'insicurezza dei sistemi ICT*, Mondo Digitale Dicembre 2003;
- Neil Daswani, Christoph Kern, Anira Kesavan, Foundations of Security, Apress 2007.

Protezione del software

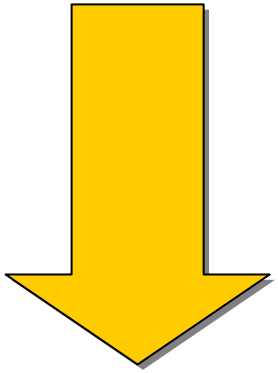
La protezione degli applicativi è fortemente legata alla sicurezza a livello di sistema operativo.

Infatti molte misure di sicurezza realizzabili a livello applicativo si basano e dipendono fortemente dalla sicurezza del sottostante sistema:

- dai meccanismi di autenticazione utente
- e di protezione di risorse (quali file, aree di memoria, device, programmi,...) messi in atto dal sistema operativo.

Protezione "del software"

- È una proprietà globale;
- è una proprietà asintotica;
- tanto più si avvicina all'asintoto tanto più aumenta il costo.



PROTEZIONE ASSOLUTA NON ESISTE

RUBUSTEZZA DI UN SISTEMA

La rapida rilevazione degli errori ed il loro confinamento in un sistema è detta robustezza del sistema.

Per ottenere un'elevata robustezza occorre applicare intesivi controlli della legittimità di operazioni sugli oggetti del sistema come salvaguardia:

1) sia da utenti malintenzionati;
2) che da errori commessi dai sistemi stessi in seguito a guasti.

RUBUSTEZZA DI UN SISTEMA: ALCUNE DEFINIZIONI

Guasto (fault): è un difetto, strutturale o algoritmico, di un componente del sistema.

Errore (error): è una transizione i uno stato non conforme alle specifiche.

Fallimento o insuccesso (failure): è un evento per cui il sistema viola definitivamente le specifiche di funzionamento.

RUBUSTEZZA DI UN SISTEMA

Un Guasto (fault) dopo un intervallo di tempo non predicibile può portare a uno o più errori.

Un Errore (error) può manifestarsi dopo un tempo non predicibile in uno o più fallimenti.

RUBUSTEZZA DI UN SISTEMA

L'affidabilità di un sistema è data da un parametro:

MTBF = Mean Time between failures

Supponendo che tutti i guasti portino a fallimento sta ad indicare il tempo medio tra due fallimenti consecutivi.

ROBUSTEZZA DI UN SISTEMA

TOLLERANZA AI GUASTI (FAULT TOLERANT)

Si intende la capacità di un sistema di non subire fallimenti anche in presenza di errori.

Trattamento del guasto	
Rilevazione e diagnosi	Rilevare gli errori
	Diagnosi • localizzare il guasto • valutare il danno (propagazione V/H)
Recovery	Riconfigurare il sistema;
	Ripristinare lo stato consistente da cui riprendere l'elaborazione (backward/forward recovery)

SISTEMI CON ELEVATA PROTEZIONE

Le metodologie di progettazione dei sistemi caratterizzati da elevata robustezza possono essere derivate da quattro principi generali detti

principi di Denning

1. ambiente chiuso;
2. privilegio minimo;
3. **controllo delle risorse in assenza di effetti collaterali;**
4. verifica delle decisioni indipendente da errori.

PRINCIPI DI DENNING

Una macchina virtuale o "sistema" è caratterizzato da:

- Soggetti;
- oggetti;

PRINCIPI DI DENNING

Oggetti	Soggetti
Implementa un insieme di operazioni	Invoca le operazioni implementate dagli oggetti

Una componente può essere oggetto in un determinato istante, soggetto in un istante diverso.

PRINCIPI DI DENNING

Oggetti	Soggetti
Implementa un insieme di operazioni	Invoca le operazioni implementate dagli oggetti
Pagine di memoria; file dispositivi canali di comunicazione	Programma Utente

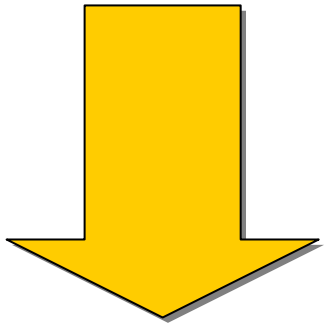
PRINCIPI DI DENNING
MATRICE DI PROTEZIONE

soggetti \ oggetti	A	B	C	D	X	Z	Y
X	op1, op2	op2	Ø	op1	Ø	op1	op5
Y	op2, op4	Ø	op3	op6	Ø	op2	Ø
Z							
K							
H							

PRINCIPI DI DENNING
MATRICE DI PROTEZIONE

Definisce in ogni istante

lo stato di protezione del sistema

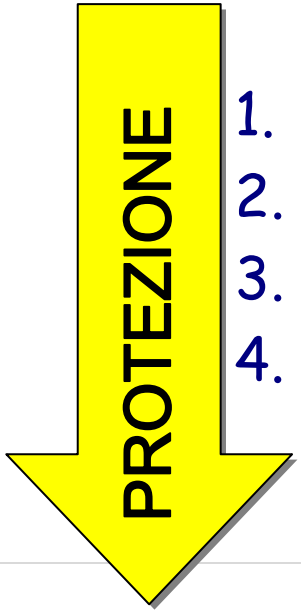


quali operazioni possono essere eseguite da un soggetto del sistema

PRINCIPI DI DENNING
MATRICE DI PROTEZIONE

Ogni sistema che ha tra i suoi obiettivi la protezione deve avere una rappresentazione di questa matrice.

I principi di Denning permettono di stabilire se la rappresentazione scelta permette di ottenere opportuni gradi di protezione.



1. ambiente chiuso;
2. privilegio minimo;
3. controllo delle risorse in assenza di effetti collaterali;
4. verifica delle decisioni indipendente da errori.

PRINCIPI DI DENNING

Le operazioni che possono essere invocate da un soggetto **X** all'istante **t** definiscono i diritti di **X** a quell'istante = dominio di protezione di **X**

La matrice di protezione viene utilizzata per garantire che la computazione evolva senza violare i diritti.

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

L'ambiente di cooperazione è chiuso:

non esistono privilegi per default: un soggetto ha nei confronti di un oggetto solo i diritti che gli sono stati esplicitamente concessi;

mediazione completa: ogni accesso ad un oggetto è completamente mediato dai meccanismi di protezione;

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

non esistono privilegi per default

ogni soggetto deve avere, quindi, solo i diritti che gli sono stati esplicitamente concessi e che sono necessari per la sua computazione.

Questo (mezzo principio) proibisce:

1) gerarchia;
2) la rappresentazione dei divieti.

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

I meccanismi di protezione ad ambiente chiuso comportano una implementazione della matrice di protezione flessibile per poter assegnare/revocare dinamicamente i diritti sugli oggetti. Esistono due implementazioni:

1) per righe: **capability**;
2) per colonne: **Access Control List (ACL)**.

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

Lista di Capabilities

- Se il soggetto X può invocare l'operazione Op su Y allora X ha una capability (Y,Op);
- La lista di capability è associato a ciascun soggetto;
- ad ogni invocazione di un operazione si controlla che esista una capability che la permetta;
- il controllo si svolge nell'ambiente del soggetto e non coinvolge l'oggetto.

PRINCIPI DI DENNING

PRIMO PRINCIPIO:AMBIENTE CHIUSO

Mediazione completa

Lista di Capabilities

ESEMPI

Capability = ticket cifrato con chiave nota solo all'OS

Il protocollo Kerberos adottato da Windows NT Server: il servizio KDC (Kerberos Key Distribution Center) viene automaticamente eseguito su qualsiasi server Active Directory e su tutti i client windows che supportano il protocollo.

PRINCIPI DI DENNING

PRIMO PRINCIPIO:AMBIENTE CHIUSO

Mediazione completa

Lista di Capabilities

ESEMPI

Capability = ticket cifrato con chiave nota solo all'OS

protocollo Kerberos

L'autenticazione Kerberos è basata appunto sull'utilizzo di un ticket interamente crittografato e contenente informazioni sufficienti per identificare l'utente e controllarne l'autenticazione.

PRINCIPI DI DENNING

PRIMO PRINCIPIO:AMBIENTE CHIUSO

Mediazione completa

Lista di Capabilities

ESEMPI

Capability = ticket cifrato con chiave nota solo all'OS

protocollo Kerberos

Si tratta di un procedimento analogo all'acquisto di un biglietto per un parco di divertimenti. Dopo aver acquistato il biglietto, è possibile utilizzarlo per tutti i giochi del parco quante volte lo si desidera fino al momento dell'uscita.

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

Lista di Capabilities

ESEMPI

Capability = puntatore ad un oggetto;

Linguaggi con tipi = ogni tipi di dato ha diverse capabilities ed attua regole rigide sul suo uso.

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

Lista di Controllo degli Accessi

- I diritti dei soggetti sono associati al singolo oggetto;
- quando un oggetto riceve un'invocazione controlla se esiste il diritto corrispondente;
- il *controllo viene spostato nell'ambiente dell'oggetto*.

PRINCIPI DI DENNING

PRIMO PRINCIPIO:AMBIENTE CHIUSO

Mediazione completa

Lista di Controllo degli Accessi

ESEMPI

Controllo su aree di memoria mediante chiave;

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

Lista di Controllo degli Accessi

ESEMPI

Protezione su file Unix/Linux

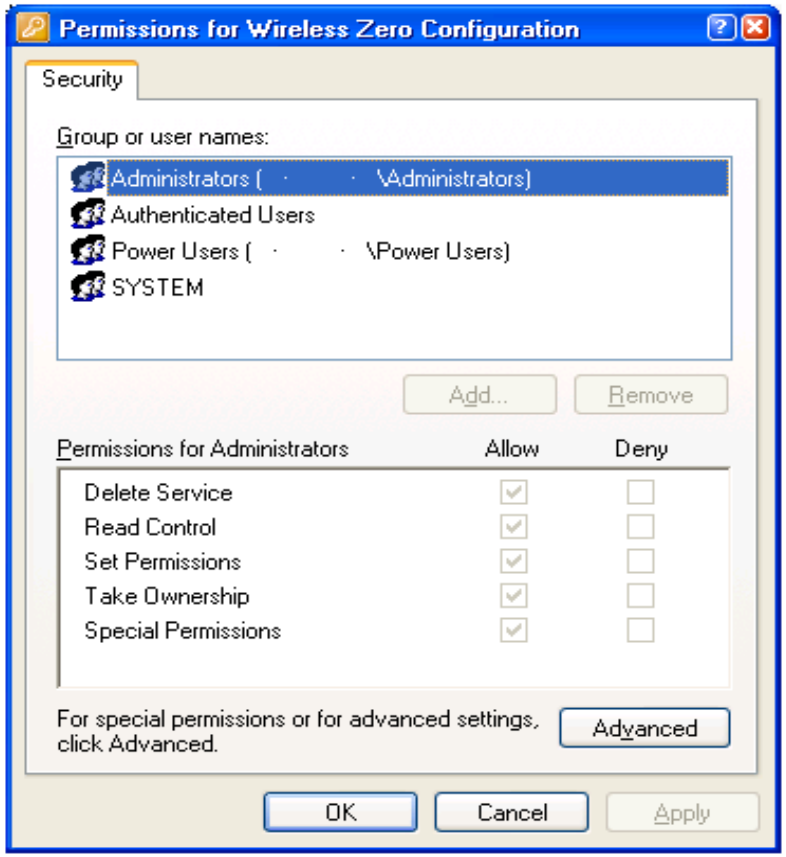
Possessore/Gruppo	Diritti di Accesso
Proprietario (owner) **U**	**R**ead, **W**rite, e**X**ecute
Gruppo a cui l'utente appartine **G**	**R**ead, **W**rite, e**X**ecute
Tutti gli altri **A**	**R**ead, **W**rite, e**X**ecute

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

Lista di Controllo degli Accessi – ESEMPI: Windows



PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

Confronto ACL - Lista di Capabilities

	Decisioni di Controllo	Trasferimento di privilegi	Revoca
ACL	Effettuata a ciascun accesso (late binding)	Di solito non è possibile	Immediata basta modificare ACL
Capability	Effettuata quando viene assegnata la capability (early binding)	È possibile.	Complicata (capability con scadenza)

PRINCIPI DI DENNING

PRIMO PRINCIPIO: AMBIENTE CHIUSO

Mediazione completa

E' possibile un uso combinato dei due meccanismi.
Ad esempio:

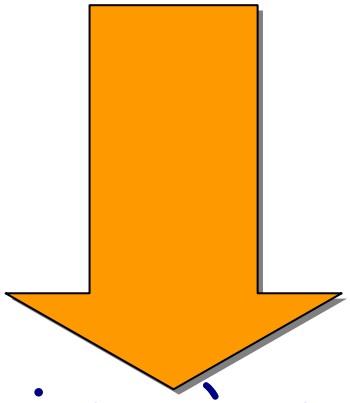
La Virtual Memory Map in Hardware = capability di accesso a memoria fisica.

OS kernel attua una ACL sulle pagine di memoria fisica.

PRINCIPI DI DENNING

SECONDO PRINCIPIO: PRIVILEGIO MINIMO

A ogni istante un utente deve avere tutti e soli i diritti necessari per proseguire la computazione.



La matrice di protezione è una struttura dati dinamica che evolve nel tempo

PRINCIPI DI DENNING

TERZO PRINCIPIO: GESTIONE DELLE RISORSE IN ASSENZA DI EFFETTI COLLATERALI

Un soggetto non può modificare lo stato di un oggetto in modo diverso da quello specificato.

PRINCIPI DI DENNING

QUARTO PRINCIPIO: VERIFICA DELLE DECISIONI INDIPENDENTE DA ERRORI

Affronta il problema dell'affidabilità dei controlli.

I controlli di protezione sono anch'essi soggetti ad errori o a violazioni.

Ogni controllo deve essere sempre eseguito più volte in ambienti diversi.

PRINCIPI DI DENNING

QUARTO PRINCIPIO: VERIFICA DELLE DECISIONI INDIPENDENTE DA ERRORI

L'implementazione dei meccanismi di protezione:

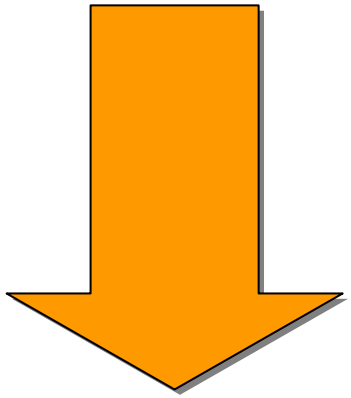
- non deve introdurre una relazione gerarchica tra entità di elaborazione (master-slave)
- né assumere che alcune entità sono più affidabili di altre (hard core).

Occorre introdurre una cooperazione tra "entità pari" mediante la quale raggiungere un consenso sulle decisioni.

PRINCIPI DI DENNING

QUARTO PRINCIPIO: VERIFICA DELLE DECISIONI INDIPENDENTE DA ERRORI

Evitare il complesso della "LINEA MAGINOT".



Un sistema che abbia un unico meccanismo di protezione è indifeso quando questo meccanismo viene in qualche modo scavalcato.

PROTEZIONE DELLE BASI DI DATI

PROTEZIONE DELLE BASI DI DATI

La sicurezza delle basi di dati e delle applicazioni che utilizzano tali dati dipende da:

1) dal grado di protezione offerto dal sistema operativo
2) dalle procedure di autorizzazione e dal software di gestione della base di dati
3) dalle procedure di sicurezza attuate per le reti di trasmissione

PROTEZIONE DELLE BASI DI DATI

Per le basi di dati, il termine "sicurezza" viene spesso sostituito dal termine autorizzazione

Si trattano solo misure di sicurezza logica per i dati, ossia le procedure che assicurano che l'accesso ai dati avvenga solo da parte di soggetti autorizzati secondo le modalità (*lettura, scrittura, ecc.*) autorizzate.

PROTEZIONE DELLE BASI DI DATI

TERMINOLOGIA

Si fornisce un breve elenco di termini usati in ambito di sicurezza delle basi di dati

Segretezza	si intende la protezione dei dati dalla lettura o dal rilascio non autorizzato.
Privacy	fa parte della segretezza, ma comprende anche gli aspetti legislativi legati alla tutela della confidenzialità dei dati degli individui e delle organizzazioni.
Integrità	si intende la protezione dei dati dalla modifica non autorizzata.
Disponibilità	questo termine indica che un sistema non deve solo essere protetto da agenti ostili, ma anche essere pienamente disponibile agli utenti autorizzati.

PROTEZIONE DELLE BASI DI DATI

ATTACCHI

Un elenco dei principali tipi di attacchi alle basi di dati è il seguente:

Segretezza	Rilascio improprio di informazioni.
Integrità	Modifica impropria dei dati
Disponibilità	Negazione del servizio

PROTEZIONE DELLE BASI DI DATI

CAUSE CHE CREANO PROBLEMI ALLA SICUREZZA

Accidentali	Disastri naturali
	Errori o bug HW/SW
	Errori umani
Fraudolente	Perpetrate da utenti autorizzati
	Perpetrate da agenti ostili

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE

Protezione da accessi impropri
Protezione da inferenza
Integrità fisica
Integrità logica/semantica
Auditing
Autenticazione degli utenti
Identificazione, protezione e gestione dei dati sensibili

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:
PROTEZIONE DA ACCESSI IMPROPRI

CONTROLLI DI FLUSSO

si tratta di controllare le sequenze di operazioni (read, write, ecc) che avvengono da un soggetto autorizzato verso un oggetto non autorizzato

Lo scheduler di un DBMS oltre a serializzare le operazioni elementari delle transazioni concorrenti deve controllare che questo non facciano accessi impropri.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:

PROTEZIONE DA ACCESSI IMPROPRI

CONTROLLI DI FLUSSO

SOGGETTO: autorizzato su X ma non su Y non può eseguire questo flusso di operazioni elementari:

ACCESSO a X
READ X
WRITE X on Y

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:

PROTEZIONE DA INFERENZA

INFERENZA

Con operazioni di assegnamento tipo :

$$Y = f(X)$$

In cui l'insieme di dati Y (non autorizzato) è ricavato applicando la funzione f all'insieme X (autorizzato).

PROTEZIONE DELLE BASI DI DATI
REQUISITI DI PROTEZIONE:
PROTEZIONE DA INFERENZA
INFERENZA

Accesso diretto

SELECT X from R WHERE Y = valore.

PROTEZIONE DELLE BASI DI DATI
REQUISITI DI PROTEZIONE:
PROTEZIONE DA INFERENZA
INFERENZA

Dati correlati

$$Y=X1*X2$$

Con X1 e X2 variabili visibili e Y non visibile, Y e inferito tramite la relazione aritmetica *.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:
PROTEZIONE DA INFERENZA

INFERENZA

Dati mancanti

Riuscire a vedere una tabella con istanze di elementi vuoti (perché sensitivi e quindi non mostrati nel risultato della query).

Conoscere il nome di una tabella senza poterne vedere il contenuto. Ciò costituisce inferenza in quanto rivela l'esistenza di dati sensitivi.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:

PROTEZIONE DA INFERENZA

CONTROLLI DI INFERENZA

I modi per prevenire attacchi di inferenza (statistica) si basano sulle seguenti tecniche:

perturbazione dei dati: vengono inseriti nella base di dati informazioni spurie che perturbano i risultati della query.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:

PROTEZIONE DA INFERENZA

CONTROLLI DI INFERENZA

Controllo sulle query: in particolare sulle dimensioni del query set. Se il numero di record ritornati da una query è inferiore a un certo valore K prestabilito la query non ottiene risposta.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:

PROTEZIONE DA INFERENZA

CONTROLLI DI INFERENZA

Questi controlli vengono messi in atto in :

- basi di dati altamente sensitive;
- basi di dati statistiche (censimenti, dati statistici su fenomeni e popolazioni).

Il fondamentale requisito di queste basi di dati è quello di dover essere accedute solo mediante query statistiche (contenenti operatori AVG, COUNT(), SUM …) per non poter risalire ai dati di un singolo individuo.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: INTEGRITA' FISICA

L'integrità fisica dei dati è minacciata in generale da malfunzionamenti HW e da fault del Sistema Operativo.

L'unico modo per garantire l'integrità fisica è la ridondanza dei dati mediante tecniche di back-up e recovery.

Si parla in questo caso di AFFIDABILITA'.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: INTEGRITA' LOGICA/SEMANTICA

L'integrità logica è garantita se i dati inseriti, o modificati, sono conformi alle definizioni e soddisfano i vincoli dichiarati nello schema logico.

Questo infatti deve prevedere oltre la struttura dei dati anche le condizioni che devono soddisfare per essere significativi.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: INTEGRITA' LOGICA/SEMANTICA

VINCOLI STATICI

- un attributo non può assumere valore nullo NOT NULL;
- gli attributi che costituiscono chiave primaria con l'opzione UNIQUE nella definizione degli indici;
- tipi ristretti cioè valori che un attributo può assumere restringendo il tipo base:

POSINT = FROM INTEGER WHERE INTEGER > 0;

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:
INTEGRITA' LOGICA/SEMANTICA

VINCOLI STATICI

- tipi non comparabili: attributi che semanticamente non sono confrontabili: ad es. anzianità ed ammontare;
- meccanismo delle asserzioni: queste sono predicati che specificano le condizioni che i dati devono soddisfare:

ASSERT a1 ON dipendenti:
Anzianità BETWEEN 18 AND 67

PROTEZIONE DELLE BASI DI DATI
REQUISITI DI PROTEZIONE:
INTEGRITA' LOGICA/SEMANTICA
VINCOLI DINAMICI

Sono vincoli che impongono delle condizioni sul modo in cui possono variare i valori di certi attributi, e quindi coinvolgono stati successivi della base di dati:

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:

INTEGRITA' LOGICA/SEMANTICA

VINCOLI DINAMICI

ASSERT a2 ON UPDATE OF dipendenti (anzianità)
NEW Anzianità > OLD Anzianità;

NEW e OLD denotano i valori degli attributi di un ennupla prima e dopo una modifica.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE:
INTEGRITA' LOGICA/SEMANTICA

VINCOLI DINAMICI

Attivazione di TRIGGER in seguito all'esecuzione di alcuni comandi per garantire l'integrità e la consistenza dei dati:

```
DEFINE TRIGGER t1
ON DELETION OF Dipendenti
(   DELETE Carriera
    WHERE Carriera.Matricola = Dipendenti.matricola )
```

PROTEZIONE DELLE BASI DI DATI
REQUISITI DI PROTEZIONE: AUDITING

Le tecniche di auditing tracciano le operazioni utente;

Il rendere pubblico che esistono misure di sicurezza nel sistema sono le contromisure più efficaci per prevenire questi attacchi.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUDITING

Senza considerare la specifica architettura del Data Base l'auditing devono catturare le seguenti informazioni:

WHO	A full identification of the person viewing or modifying the data
WHERE	A log showing the specific application procedure and method used to access the data
WHEN	A reliable date-time-stamp, globalized to Greenwich Mean Time (GMT)
WHAT	A full listing of all data entities that were viewed or modified
WHY	Context-based information describing how the data was disclosed

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUDITING

Il Data Base Security può riguardare i seguenti aspetti:

Server Security	Occorre limitare l'accesso al Server su cui è presente il Data Base
Database Connections	Il Data Base Administrator non deve permettere aggiornamento da parte di utenti non autenticati del Data Base né dare ad altri utenti il profilo di SA.
Table Access Control	E' frutto della collaborazione del Data Base Administrator e del System Administrator (SA) in quando mediante un Access Control List occorre limitare l'accesso ad un system object.
Restricting Database Access	Ciò è relativo in special modo ai Data Base Internet. E' molto semplice fare un "port scan" e trovare le porte che vengono usate dai vari Data Base.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUDITING

Restricting Database Access

Occorre considerare misure addizionali per prevenire accessi da Internet:

Trusted IP Address	Occorre limitare l'accesso al Server su cui è presente il Data Base
Server account disabling	The server ID can be suspended after three password attempts.
Special tools	Products can be used to send an alert when an external server is attempting to breach the system's security.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUDITING

Failed log-on attempts

Per controllare accessi non autorizzati al database: (ORACLE)

Query:

```
SQL> select count(*),username,terminal,to_char(timestamp,'DD-MON-YYYY')
  2  from dba_audit_session
  3  where returncode<>0
  4  group by username,terminal,to_char(timestamp,'DD-MON-YYYY');
```

Result:

```
COUNT(*) USERNAME        TERMIN TO_CHAR(TIM
---------- --------------- ------ -----------
         1 BILL            pts/3  09-APR-2003
         3 FRED            pts/3  09-APR-2003
         4 ZULIA           pts/1  09-APR-2003
```

ZULIA ha tentato di accedere per ben 4 volte con insuccesso.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUDITING

Attempts to access the database with non-existent users

```
SQL> select username,terminal,to_char(timestamp,'DD-MON-YYYY HH24:MI:SS')
  2  from dba_audit_session
  3  where returncode<>0
  4  and not exists (select 'x'
  5     from dba_users
  6     where dba_users.username=dba_audit_session.username)
SQL> /

USERNAME          TERMIN TO_CHAR(TIMESTAMP,'D
----------------- ------ --------------------
FRED              pts/3  09-APR-2013 17:31:47
FRED              pts/3  09-APR-2013 17:32:02
FRED              pts/3  09-APR-2013 17:32:15
BILL              pts/3  09-APR-2013 17:33:01
```

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUDITING

Attempts to access the database at unusual hours

```
QL> select     username,
  2     terminal,
  3     action_name,
  4     returncode,
  5     to_char(timestamp,'DD-MON-YYYY HH24:MI:SS'),
  6     to_char(logoff_time,'DD-MON-YYYY HH24:MI:SS')
  7  from dba_audit_session
  8  where to_date(to_char(timestamp,'HH24:MI:SS'),'HH24:MI:SS') <
to_date('08:00:00','HH24:MI:SS')
  9 or to_date(to_char(timestamp,'HH24:MI:SS'),'HH24:MI:SS') >
to_date('19:30:00','HH24:MI:SS')
SQL> /

USERNAME   TERMIN ACTION_N RETURNCODE TO_CHAR(TIMESTAMP,'D TO_CHAR(LOGOFF_TIME,
---------- ------ -------- ---------- -------------------- --------------------
SYS        pts/1  LOGOFF            0 09-APR-2003 20:10:46 09-APR-2003 20:16:41
SYSTEM     pts/5  LOGOFF            0 09-APR-2003 21:49:20 09-APR-2003 21:49:50
ZULIA      pts/5  LOGON             0 09-APR-2003 21:49:50
EMIL       APOLLO LOGON             0 09-APR-2003 22:49:12
```

PROTEZIONE DELLE BASI DI DATI
REQUISITI DI PROTEZIONE: AUDITING

Occorre proteggere il Data Base contro questi abusi:

- l'utilizzo dei sistemi di audit deve far parte della politica dell'organizzazione riguardo alla sicurezza e protezione;

- Il database di audit deve essere monitorato regolarmente come prevenzione contro eventuali attacchi e usi impropri.

L'overhead dovuto all'introduzione di sistemi di auditing è ampiamente ricompensato dall'aumento del livello di protezione del Data Base soprattutto se i dati sono altamente sensibili.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

Autenticazione: identifica una persona che effettua una richiesta basata su:

- Qualcosa che si sa: password, chiave crittata;
- Qualcosa che si possiede: hardware (chiave, smartcard);
- Qualcosa che si è: biometrica (impronta digitale, vocale, iride);

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

I Sistemi di Gestione delle Basi di Dati (SGDB) prevedono meccanismi:

- sia per controllare che ai dati accedano solo persone autorizzate;
- sia per restringere i dati accessibili e le operazioni che si possono fare su di essi.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

SQL Server

SQL Server consente di utilizzare 2 metodi per l'autenticazione e l'accesso alle proprie risorse:

- l'autenticazione integrata con il sistema operativo:
- oppure l'accesso per mezzo di un nome utente e una password che vengono verificati da SQL Server (autenticazione standard).

l'obiettivo da perseguire è quello di assegnare a ciascun utente i permessi minimi di cui necessita per eseguire le proprie attività.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

SQL Server

Per creare un nuovo utente di SQL Server, o per concedere l'accesso ad un login a livello di sistema operativo sono da seguire i seguenti passi logici:

1) creare un login in grado di accedere a SQL Server
2) concedere al login l'accesso ad uno o più database
3) assegnare i permessi sulle risorse

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

SQL Server

```
EXEC sp_addlogin 'Simone', 'Verdi';
```

Adesso l'utente Simone potrà accedere all'istanza di SQL Server, ma non ha ancora il permesso di utilizzare i database presenti nel server (salvo quelli in cui sia definito l'account guest).

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

SQL Server

Per consentire ad un login l'accesso ad uno dei database è indispensabile renderlo User di un database. Con il seguente comando

```
USE MyDatabase
GO
EXEC sp_grantdbaccess 'Simone', 'Simus'
```

viene indicato a SQL Server che il Login Simone può avere accesso al database MyDatabase all'interno del quale sarà identificata come Simus.
Giunti a questo punto il login Simone può accedere a SQL Server, può accedere anche al database MyDatabase ma non ha la possibilità di compiere alcuna operazione su di esso in quanto non sono stati ancora concessi permessi sulle risorse.

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

SQL Server

È possibile concedere permessi sulle risorse in maniera esplicita ad un utente utilizzando l'istruzione GRANT.

```
GRANT SELECT, UPDATE ON dbo.MyTable TO Simus
```

affinché l'utente Simus sia in grado di interrogare e aggiornare la tabella dbo.MyTable. In alternativa possiamo rendere Simus membro di un database role (predefinito o personalizzato) che abbia già dei permessi.

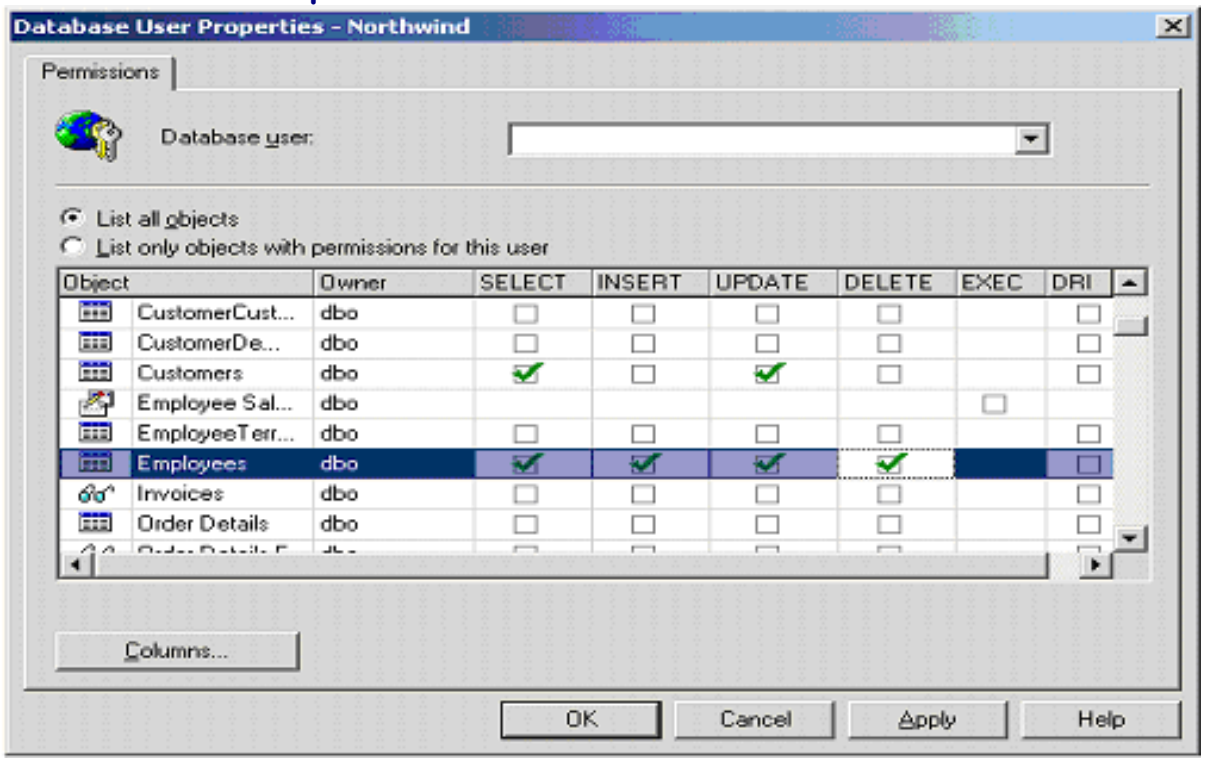
```
EXEC sp_addrolemember 'db_datareader', 'Simus'
```

PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: AUTENTICAZIONE DEGLI UTENTI

SQL Server

Se volessimo concedere ad uno user dei permessi espliciti sugli oggetti dovremmo accedere alle proprietà dell'utente facendo doppio click su di esso e, scegliendo il pulsante "Permissions...", si aprirà la finestra mostrata nell'illustrazione che segue:



PROTEZIONE DELLE BASI DI DATI

REQUISITI DI PROTEZIONE: **identificazione, protezione e gestione dei dati sensitivi**

Oltre ai metodi esposti sopra è possibile proteggere i dati da utenti non autorizzati anche mediante crittografia.

PROTEZIONE DEI DOCUMENTI

PROTEZIONE DEI DOCUMENTI

IL MODELLO BELL-LAPADULA

E' un modello di controllo degli accessi usato da molti governi ed organizzazioni militari.

Il modello e' costituito da:

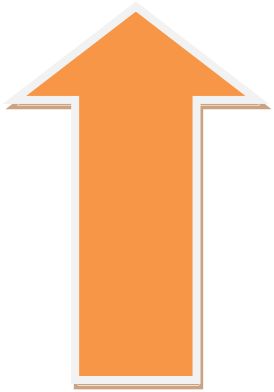
a) un sistema di classificazione;
b) utenti;
c) risorse (documenti, dati,...)
d) un insieme di proprieta' che devono essere rispettate: *simple property, star property e tranquillity property.*

PROTEZIONE DEI DOCUMENTI

IL MODELLO BELL-LAPADULA

SISTEMA DI CLASSIFICAZIONE

E' costituito da quattro livelli:



MAX	Top Secret
...	Secret
	Confidential
MIN	Unclassified

PROTEZIONE DEI DOCUMENTI

IL MODELLO BELL-LAPADULA

UTENTI E RISORSE

Ogni utente che puo' accedere al sistema di gestione delle informazioni regolato dal modello Bell LaPadula ha associato un livello di classificazione.

Ogno risorsa ha associata un livello di classificazione.

PROTEZIONE DEI DOCUMENTI

IL MODELLO BELL-LAPADULA

SIMPLE PROPERTY

Spesso chiamata **NO READ UP** stabilisce che un utente che ha una particolare classificazione NON puo' leggere risorse con un livello di classificazione piu' alta.

PROTEZIONE DEI DOCUMENTI

IL MODELLO BELL-LAPADULA

STAR PROPERTY

Spesso chiamata **CONFINEMENT PROPERTY** o **NO WRITE DOWN** stabilisce che ad un utente NON e' permesso creare risorse con un livello di classificazione piu' basso.

PROTEZIONE DEI DOCUMENTI

IL MODELLO BELL-LAPADULA

TRANQUILLITY PROPERTY

Stabilisce che il livello di classificazione di una risorsa non puo' essere cambiato fintantoche' e' in uso da un utente.

Sistemi di protezione del software, dei dati/documenti

FINE

GRAZIE PER L'ATTENZIONE !!!