Seguretat en BD

Gestió i Administració de Bases de Dades.
Grau en Enginyeria Informàtica

Oriol Ramos Terrades

Carles Sánchez Ramos

Departament de Ciències de la Computació

Continguts

- Introducció. Conceptes bàsics i mesures de control
- Control d'accés discrecional (DAC)
- Control d'accés obligatori (MAC)
- Control de flux
- Xifrat
- Manteniment de la privacitat
- Reptes en la seguretat de BD

Conceptes bàsics: Tipus de seguretat

- Aspectes legals i ètics. Drets d'accés a les dades. Llei de protecció de dades.
- Polítiques governamentals, institucions, empresa, en quant a la disposició de la informació pública.
- Nivells de sistema. Decidir si la tècnica de seguretat ha de ser implementada en HW o en SGBD.
- Nivells de seguretat. Identificar diferents nivells dins institució (*TS-Top Secret, S-Secret, C-Confidencial*, etc.)

Conceptes bàsics: Amenaces a la BD

- **Pèrdua d'integritat** per canvis no autoritzats.
- **Pèrdua de disponibilitat**. Objectes no disponibles a usuaris o programes.
- **Pèrdua confidencialitat**. Pèrdua de la protecció de dades davant l'accés no autoritzat. Pèrdua de confiança en l'organització.

Conceptes bàsics: mecanismes de seguretat

- **Mecanismes discrecionals:** Concedir permisos d'accés a determinada informació (inserció, esborrat, etc.) a usuaris.
- **Mecanismes obligatoris:** Classificació d'objectes (dades) i subjectes (usuaris) en nivells de seguretat. Ex: Usuari nivell n sols pot veure dades de nivell n o inferior.

Mesures de control

- **Control d'accessos:** Evitar que persones autoritzades accedeixin a la informació. Gestionar comptes d'usuaris i passwords.
- **Control d'inferències:** No permetre l'accés a dades individuals confidencials si l'accés és a dades globals (BD estadístiques, *data mining*).
- **Control de flux:** Prevenir que la informació llegida per l'usuari vagi a altres no autoritzats. Canals ocults.
- **Xifrat de dades:** Codificar dades amb algorisme de xifrat, i descodificar per llegir. Xifrat de clau pública.

Seguretat i DBA

DBA: Responsable de seguretat. Té compte d'usuari *admin* per a definir polítiques de seguretat. Fa les accions:

- Creació de comptes d'usuari.
- Concessió i retirada de privilegis a les comptes (mecanismes discrecionals).
- Assignació de nivells de seguretat a dades i usuaris (mecanismes obligatoris).

Comptes d'usuari

- DBA gestiona els comptes d'usuari amb les que els usuaris inicien sessió amb la BD.

- El SGBD valida que el nom del compte i el password coincideixin amb un dels usuaris que tingui guardats en una taula d'usuaris xifrada.

- El SGBD registra les transaccions que un usuari realitza durant la sessió. Cal afegir al registre de sistema l'usuari i el terminal que fan cada transacció.

- **Auditoria de BD:** Revisar el registre de sistema per examinar transaccions fetes pels usuaris.

Control d'accés discrecional (DAC)

Control d'accés basat en privilegis. La majoria dels SGBD l'implementen.

Dos nivells de privilegis:

- **Nivell de compte:** DBA especifica privilegis d'usuari, independentment de la BD.
- **Nivell de relació o taula:** Control d'accés a cada relació o vista de la BD.

Nivell de compte, privilegis:

`CREATE SCHEMA, CREATE TABLE, CREATE VIEW,`
`ALTER TABLE, DROP, SELECT,` etc.

Control d'accés discrecional (DAC)

Nivell de relació: Especificar les transaccions a aplicar a cada relació o vista.

Matriu d'accés, M_{ij}: permisos del subjecte i sobre objecte j.

Per a cada relació, l'usuari propietari té tots els privilegis, que pot concedir a altres usuaris (`GRANT`).

Per a una relació, es poden concedir 3 privilegis:

- **Selecció:** Permís d'accés (`SELECT`).
- **Modificació:** Permís de `UPDATE, DELETE, INSERT`.
- **Referència:** Permís d'utilitzar la relació com a referència en regles d'integritat.

Control d'accés discrecional (DAC): aspectes

1. Especificació de privilegis per vistes
2. Revocació de privilegis
3. Propagació de privilegis (`GRANT OPTION`)

Especificació de privilegis per vistes

Vista: Mecanisme d'autorització discrecional.

Si usuari A té una relació R que vol compartir només en una part amb l'usuari B, A crea una vista V incloent els atributs i tuples a compartir, autoritzant a B l'accés a la vista V.

Revocació de privilegis

Si volem concedir privilegis a altres usuaris de forma temporal, cal revocar privilegis.

`REVOKE`: Comanda per a retirar privilegis.

```
REVOKE <operacio> [,<operacio>] ON <taula> [,<taula>]
FROM <usuari> [,<usuari>];
```

On:

`<operacio>` → `SELECT | UPDATE | INSERT | DELETE`

Exemple:

```
REVOKE SELECT,DELETE ON Espectacles FROM enric;
```

Propagació de privilegis: `GRANT OPTION`

Quan el propietari d'una relació dona privilegis a un altra, pot donar-li a més la capacitat de propagar el privilegi a un tercer usuari.

Amb `GRANT OPTION`:

- Qui rep el privilegi pot donar-lo a altres usuaris.
- Propagar privilegis sense saber-ho el propietari

$$A \xrightarrow{R} B \xrightarrow{R} C \xrightarrow{R} .. \xrightarrow{R} Z \qquad (A..Z), \text{ usuaris}$$

- Si $A \rightarrow B$ i $B \rightarrow C$, en cas de que A revoqui B, C perd també els privilegis.
- Cas de que $A1 \rightarrow A4$, i $A2 \rightarrow A4$. Si $A1 \rightarrow A4$ es revoca, $A4$ mantindrà privilegis fins que $A2$ els revoqui.

Propagació de privilegis: GRANT OPTION

GRANT: Comanda per a propagar privilegis.

```
GRANT <operació> [,<operació>] ON <taula> [,<taula>]
TO <usuari> [,<usuari>] [GRANT OPTION]
```

On:

<operació> → SELECT | UPDATE | INSERT | DELETE

Exemple:

```
GRANT SELECT,UPDATE On Espectadors TO enric GRANT
OPTION;
```

Propagació de privilegis: `GRANT OPTION`

Exemple: DBA crea 4 comptes *A1, A2, A3, A4*. *A1* pot crear relacions base.

Privilegi per a crear relacions base:

```
GRANT CREATE TABLE TO A1;
```

A1 crea relacions:

```
EMPLEAT(DNI,Nom,Data_Neix,Adreça,Sexe,SOU,Num_Dept
DEPARTAMENT(Num_Dept,Nom_Dept,DNI_Director)
```

A1 dona privilegis d'inserció i esborrat de les 2 relacions sense propagar privilegis:

```
GRANT INSERT,DELETE ON EMPLEAT,DEPARTAMENT TO A2;
```

Propagació de privilegis: `GRANT OPTION`

A1 dóna privilegis d'accés de les dues relacions a *A3* amb propagació:

```
GRANT SELECT ON EMPLEAT, DEPARTAMENT TO A3 WITH GRANT
OPTION;
```

A3 dona privilegis d'accés sobre la relació `EMPLEAT` a *A4*:

```
GRANT SELECT ON EMPLEAT TO A4;
```

A1 revoca privilegis d'*A3*, revocant també els privilegis d'*A4* que havia concedit *A3*:

```
REVOKE SELECT ON EMPLEAT FROM A3;
```

Propagació de privilegis: GRANT OPTION

A1 vol donar privilegis d'accés sobre alguns atributs i tuples de la relació EMPLEAT a *A3*:

```
CREATE VIEW A3EMPLEAT AS
SELECT Nom, Data_Neix, Adreça
FROM    EMPLEAT
WHERE   Num_Dept=5;
GRANT SELECT ON A3EMPLEAT TO A3 GRANT OPTION;
```

A1 permet actualitzar un atribut de la relació EMPLEAT(Sou) a *A4*:

```
GRANT UPDATE ON EMPLEAT(Sou) TO A4;
```

Per a privilegis UPDATE, INSERT els noms de les relacions es poden especificar amb atributs.

Per a privilegis SELECT, DELETE els noms de les relacions no especifiquen atributs.

Control d'accés obligatori (MAC)

Política de seguretat addicional al discrecional, classificant dades i usuaris segons el nivell de seguretat.

Especialment utilitzat en aplicacions governamentals, militars, industrials.

Nivells o classes de seguretat (de + a -):

- TS: Top Secret
- S: Secret
- C: Confidencial
- U: No classificat

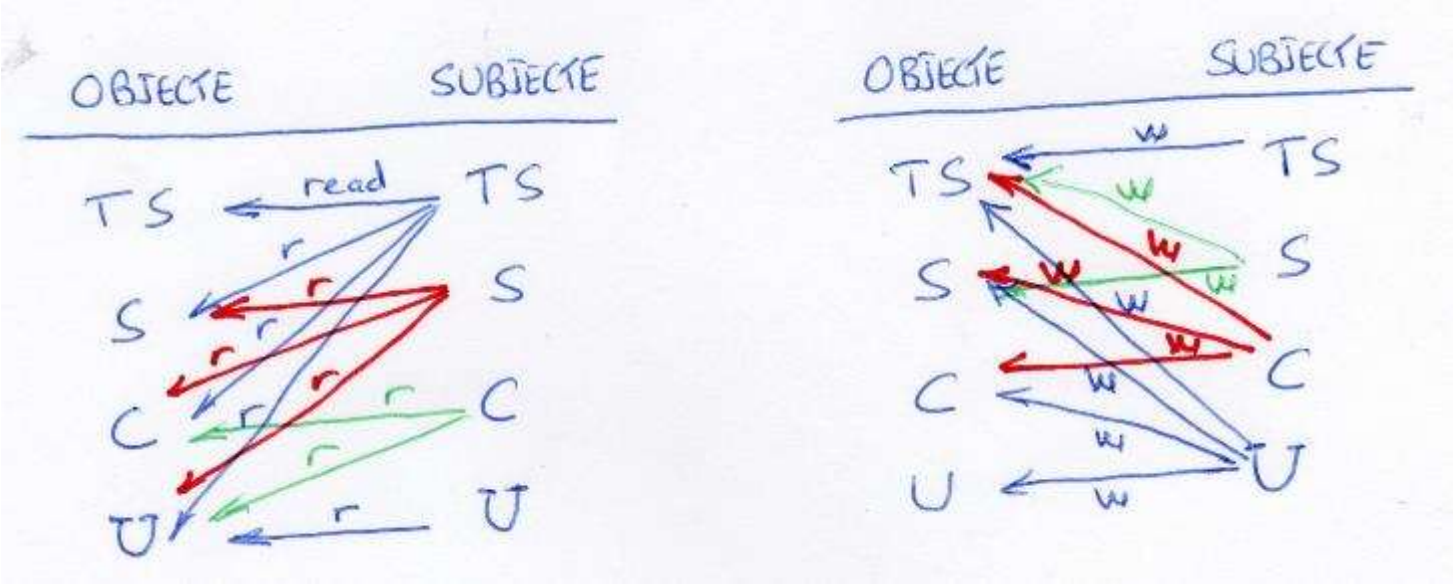
Control d'accés obligatori (MAC)

Model Bell-Lapadula: Model de seguretat multinivell, que classifica per nivells:

- **Nivell d'autorització:** Assignat a subjectes (Usuari, Compte, Programa) – *Clase(S).*
- **Classificació d'un objecte:** Assignat a objectes (relació, tupla, atribut, vista, operació) – *Classe(O).*

Control d'accés obligatori (MAC): regles

- **Propietat de seguretat simple:** A un subjecte S no se li permet **lectura** a un objecte O si $Classe(S) < Classe(O)$.
- **Propietat *:** A un subjecte S no se li permet **escriure** un objecte O si $Classe(S) > Classe(O)$. Violació de la regla faria que la informació arribés a nivells més baixos.



Control d'accés obligatori (MAC)

Relació multinivell R: Definició de nivells de seguretat sobre atributs, valors en atributs o tuples en R:

$$R(A_1:C_1, A_2:C_2, \ldots, A_n:C_n, TC)$$

- A_i: Atributs
- C_i : Classificació de l'atribut A_i
- TC : Classificació de la tupla $TC = \max(C_i),\ i=1..n$

Control d'accés obligatori (MAC)

Exemple de visualització de tuples tenint en compte nivells de seguretat ($S > C > U$):

EMPLEADO

Nombre	Sueldo	RendimientoTrabajo	TC
Gómez U	40000 C	Normal S	S
Campos C	80000 S	Bueno C	S

Tuples originals

EMPLEADO

Nombre	Sueldo	RendimientoTrabajo	TC
Gómez U	40000 C	NULL C	C
Campos C	NULL C	Bueno C	C

Tuples per usuaris C

EMPLEADO

Nombre	Sueldo	RendimientoTrabajo	TC
Gómez U	NULL U	NULL U	U

Tuples per usuaris U

DAC vs MAC

Control accés discrecional (DAC):

- Més utilitzat en DBMS.
- Major flexibilitat per a definir els controls.
- Vulnerabilitat en atacs maliciosos (troians) si no es controla la propagació.

Control accés obligatori (MAC):

- Alt grau de protecció, preveu fluxos il·legals d'informació.
- Polítiques excessivament rígides.

ALTERNATIVA: **Control d'accés basat en rols (RBAC)**

Altres mètodes de control d'accés:

1. Control d'accés basat en rols (RBAC)
2. Control d'accés en comerç electrònic
3. Seguretat en BD estadístiques

Control d'accés basat en rols (RBAC)

- Apareix els anys 90 per a reforçar la seguretat en grans empreses.
- Permisos associats a rols i rols s'assignen a usuaris o sessions. Usuari o sessió pot tenir assignat varis rols.
- Creació, destrucció de rols: `CREATE ROLE, DESTROY ROLE.`
- Comandes `GRANT, REVOKE` per a concedir o revocar rols a usuaris.
- Control per rols garanteix que sols els usuaris autoritzats tenen accés a determinades dades.

Control d'accés basat en rols (RBAC)

Jerarquia de rols:

- Jerarquia d'autoritat.
- Rols de menor autoritat connectats amb els de major.

Assignació temporal de rols, definint temps d'assignació o activació d'un rol mitjançant l'activació d'un altra.

RBAC utilitzat en seguretat d'aplicacions web i Internet; Assignar rols a tasques de flux de treball.

Característiques RBAC:

- Flexible, neutralitat en les polítiques.
- Millor suport per a la gestió de seguretat.
- Poden modelar polítiques de seguretat DAC i MAC.
- Mecanisme natural de seguretat en execució de tasques i fluxos de treball.
- Facilitat pel desenvolupament en Internet.

Seguretat en BD estadístiques

BD estadístiques contenen informació individualitzada, sobre la que es pot treure informació general (població, dades gestió acadèmica, etc.).

Es volen obtenir estadístiques (mitges, desviacions, etc.), prohibint l'obtenció de dades individuals.

Mecanismes de protecció:

1. Forçar que sentències continguin funcions d'agregat (SUM, COUNT, etc.).
2. Prohibir consultes amb un nombre de tuples menor que un llindar.
3. Prohibir seqüència de consultes que obtinguin les mateixes tuples.
4. Agrupar tuples en grups, prohibint accessos únicament a tuples d'un subgrup.

Control de flux

Flux entre objectes X, Y: Programa llegeix X i el grava a Y.

Control de flux evita que informació d'un objecte no vagi a objectes menys protegits. Es permet flux sempre que objecte receptor tingui tants o més privilegis que l'objecte llegit.

- **Política de flux:** canals en els que es permet moure la informació.
- **Política de flux simple:** Donades dues classes (Confidencial – C, No Confidencial – N), permetre tots els fluxos excepte els que van de C → N.

Mecanismes de control d'accés: Comprovar autoritzacions d'usuaris quan hi ha fluxos.

Control de flux

Mecanisme control de flux: Assignar classe (autorització) de seguretat a programa en execució, que li dona els permisos:

- Programa P pot llegir un objecte si el seu nivell d'autorització és igual o superior a la classificació de l'objecte O [Classe(O) <= Classe(P)].
- Programa P pot escriure en un objecte si el seu nivell d'autorització és igual o inferior a la classificació de l'objecte O [Classe(O) >= Classe(P)].

Exemple: Programa amb autorització *Secret*:

- Pot **llegir** objectes *No Classificats, Confidencials* i *Secrets*.
- Pot escriure **objectes** de tipus *Secret* i *Alt Secret*.

Control de flux

Dos tipus de flux:

- **Fluxos explícits:** Fets amb instruccions d'assignació.
- **Fluxos implícits:** Fets per instruccions condicionals.

Garantir seguretat en flux: Definir regles mitjançant relacions entre autoritzacions, declarant fluxos autoritzats ($A \rightarrow B$, quan informació d'A afecta a B) i operacions que permetin aquests fluxos.

Assignar etiquetes d'autorització a usuaris, programes i objectes.

Canals ocults

Permet transferències d'informació que violen política de seguretat, que informació de nivell alt vagi a nivell baix.

Dos tipus:

- **Canal de temporització:** Informació es transmet després d'una temporització d'esdeveniments.
- **Canal d'emmagatzemament:** Sense sincronització temporal, es transmet accedint a informació de sistema, en zona protegida (semàfors).

Canals ocults

Exemple: BD distribuïda amb un node amb seguretat Secret (S) i un altra No Classificat (U).

- Si els nodes es posen d'acord en quina informació es pot enviar, s'estableix un canal ocult i una transacció amb dades secretes es podrà executar en node U.

Canals ocults no són problema si la implementació de BD està ben construïda i és robusta. Si no, els usuaris se'n poden aprofitar.

Utilitat: Programa fa càlculs amb informació sensible pot necessitar accés individual per a validar càlculs. Un cop el programa és en producció, es tanca l'accés.

Xifrat

Xifrat: Valor afegit per a mantenir seguretat de les dades en entorns segurs o no.

Aplicar algorisme de xifrat utilitzant una clau de xifrat pre-definida. Receptor necessita la clau per a desxifrat per obtenir dades originals.

Tipus de xifrat:

- Estàndard de xifrat (DES)
- Xifrat de clau pública
- Firmes digitals

Estàndard de xifrat (DES)

- Desenvolupat pel govern USA per ús públic.
- Sistema de xifrat entre un emissor (A) i un receptor (B).
- Algorisme combina dos operadors: substitució i permutació, que aplica fins a 16 vegades.
- Missatge original es xifra en blocs de 64 bits, sobre una clau de 64 bits.
- NIST (*National Institute of Standards*) introdueix algorisme AES (*Advanced Encryption Standard*) amb blocs de 128 bits i claus de 128, 192 o 256 bits.

Xifrat de clau pública

1976, Diffie i Hellman.

Algorisme basat en funcions matemàtiques, no en patrons de bits.

Dos claus independents:

- Clau pública
- Clau privada.

Xifrat de clau pública: components

1. Text pla original
2. Algorisme de xifrat.
3. **Clau pública:** Associada a un receptor, que la fa pública.
4. **Clau privada:** Associada a un receptor, que la guarda.
5. Text xifrat
6. Algorisme desxifrat. Aplicat a text xifrat s'obté text original.

Xifrat de clau pública: passos

1. Un usuari (U) genera un parell de claus, una de xifrat i una altra de desxifrat.
2. L'usuari U col·loca la clau pública en lloc públic.
3. Per enviar missatge a U, un emissor (E) xifra el text original amb la clau pública del receptor.
4. Emissor E envia missatge a receptor U.
5. Receptor U utilitza clau privada en el missatge rebut.

Manteniment privacitat

Desafiament actual. Mesures:

- Evitar grans nodes de dades centralitzats
- Modificar i distorsionar dades intencionadament.

Dades sensibles: dades mèdiques, econòmiques, etc.

Nou repte: Control d'accés i privacitat dispositius mòbils.

Problema: On i com guardar informació sensible (comptes NIU UAB).

Reptes en la seguretat de BD

L'augment dels sistemes de BD i el creixement d'amenaces potencials planteja reptes en la seguretat en sistemes de BD:

1. **Qualitat de les dades:** Cercar tècniques per avaluar i demostrar la qualitat de les dades.
   - Regles d'integritat efectives
   - Tècniques de recuperació de dades incorrectes
2. **Drets de propietat intel·lectual:** Protegir propietat intel·lectual davant Internet i Intranet.
3. **Marca d'aigua per a BD:** Protegir contingut davant duplicació i distribució no autoritzada. Prova de propietat del contingut.

Reptes en la seguretat de BD

4. **Supervivència BD:** BD s'han de mantenir operatius davant atacs de seguretat. El SGBD preparat per a un atac. Al detectar-lo, caldria fer:
   - **Aïllament:** Eliminar accés atacant.
   - **Avaluació danys:** Rastrejar funcions i dades afectades.
   - **Reconfiguració:** Reconfigurar-se per a mantenir-se operatiu.
   - **Reparació:** Reparar dades i funcions.
   - **Tractament errades:** Identificar febleses que han permès els atacs. Estudiar i planificar atacs produïts, per estudiar mesures preventives.

En resum...

Diferents nivells de seguretat

Amenaces:

- Pèrdua integritat
- Disponibilitat
- Confidencialitat

Mesures de control:

- Control d'accés: DAC, MAC, RBAC
- Control d'inferència
- Control de flux
- Xifrat: Estàndards, Clau pública, Firma electrònica