Unidad 3: Seguridad, Transacciones, Concurrencia y Recuperación

Bases de Datos Avanzadas, Sesión 11 : Seguridad y Autorización.

Iván González Diego
Dept. Ciencias de la Computación
Universidad de Alcalá

INDICE

- *Seguridad.*
- *Autorización.*
- *Cifrado y Autentificación.*

Referencias: Silberschatz 4ª Ed. Pp 343 - 364
Elmasri, 3ª Ed. Pp 553 - 595

Seguridad y Autorización

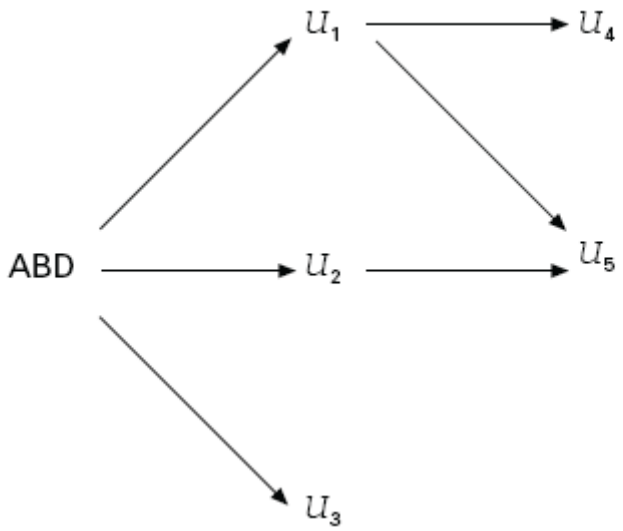
- Los datos deben estar protegidos contra accesos no autorizados que pueden producir :
  - Destrucción
  - Alteraciones malintencionadas
  - Inconsistencias de los datos
- Violaciones de seguridad
  - Lectura no autorizada
  - Modificación no autorizada
  - Destrucción no autorizada
- Protección frente a usuarios no autorizados:
  - Sistema Gestor de Base de Datos
  - Sistema Operativo
  - Conexiones de Red
  - Sitios protegidos
  - Personas con autorizaciones

Seguridad y Autorización

- Autorizaciones
- Varios tipos sobre datos:
  - Lectura
  - Inserción
  - Actualización
  - Borrado
- Varios tipos sobre el esquema:
  - Indices
  - Recursos: nuevas relaciones
  - Alteración: nuevos atributos a las relaciones
  - Eliminación de las relaciones
  - Vistas: como una forma de ocultar detalles de la base de datos a ciertos usuarios.

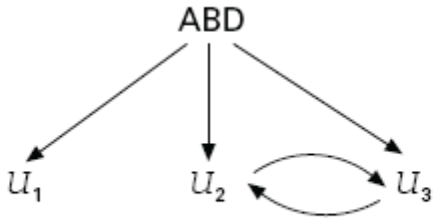
Seguridad y Autorización

- Concesión de privilegios
- Un usuario que tiene concedido autorizaciones puede transmitir esas autorizaciones a otros usuarios.
- Grafo de autorización:

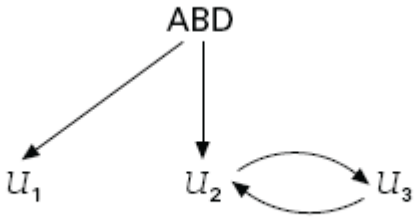


Seguridad y Autorización

- Intento de eludir autorización

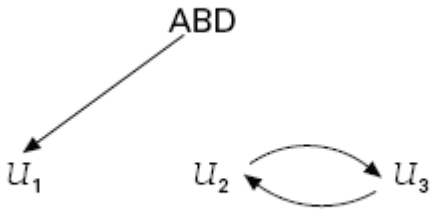


(*a*)



(*b*)

U_3



(*c*)

Seguridad y Autorización

- Concepto de papel (Role)
- Hay usuarios que tienen los mismos privilegios y autorizaciones.
- En vez de asignarlo a cada usuario que se crea del mismo tipo $\Rightarrow$ mejor crear un esquema de autorización para conjuntos de usuarios del mismo tipo $\Rightarrow$ papel
- Asignar el papel de ese usuario en la base de datos.
- Asignar un identificador propio para cada usuario
- Trazas de auditorías
- Registro histórico donde se guarda todos los cambios que se han producido junto con el usuario que lo ha realizado y cuando.

Autorización en SQL

- Privilegios en SQL
- Delete, insert, update y select
- Grant ⇒ conceder privilegios

grant <lista de privilegios> **on** <nombre de relación o de lista> **to** <lista de usuarios/papeles>

grant select on *sucursal* **to** U_1, U_2, U_3

- Con update y insert se pueden establecer a campos concretos

grant update (*importe*) **on** *préstamo* **to** U_1, U_2, U_3

- También references ⇒ declarar claves externas en relaciones

grant references (*nombre-sucursal*) **on** *sucursal* **to** U_1

- All privileges ⇒ todos los privilegios son concedidos
- Nombre usuario public ⇒ referencia a todos los usuarios y los que puedan venir.

Autorización en SQL

- Papeles
- Crear: **create role** *cajero*
- Conceder privilegios: **grant select on** *cuenta* **to** *cajero*
- Asignar papeles a otros usuarios o papeles:

grant *cajero* **to** juan
create role *gestor*
grant *cajero* **to** *gestor*
grant *gestor* **to** maría

- Privilegios de un usuario o papel constan:
  - Privilegios concedidos al usuario o papel
  - Privilegios concedidos a papeles que se hayan concedido al papel o usuario

Autorización en SQL

- Privilegio de conceder privilegios
- Un usuario no está predeterminado a conceder un privilegio que se le ha concedido a otro usuario.
- Si se desea ⇒ with grant option

grant select on *sucursal* **to** U_1 **with grant option**

- Retirar autorización ⇒ revoke

revoke <lista de privilegios> **on** <nombre de relación o de vista>
from <lista de usuarios o papeles> [**restrict** | **cascade**]

revoke select on *sucursal* **from** U_1, U_2, U_3
revoke update (*importe*) **on** *préstamo* **from** U_1, U_2, U_3
revoke references (*nombre-sucursal*) **on** *sucursal* **from** U_1

revoke grant option for select on *sucursal* **from** U_1

Autorización en SQL

- El creador de un objeto $\Rightarrow$ obtiene los privilegios de ese objeto y además puede concederlos a otros.
- Sólo el propietario del esquema puede ejecutar cualquier modificación del mismo

Cifrado y Autenticación.

- Proteger datos extremadamente delicados ⇒ cifrado
- Técnicas de cifrado:
  - Sencillas
  - Complicadas:
    - DES: Data Encription Standard: Sustitución y ordenación de los caracteres en base a una clave de cifrado
    - AES: Advanced Encription Stantdard
    - Cifrado de clave asimétrica: clave pública y clave privada
- Autenticación ⇒ tarea de verificar la identidad de una persona o software que se conecte a la base de datos.
  - Usuario – contraseña
  - Sistemas desafío-respuesta + cifrado con clave pública
  - Firmas digitales