Seguridad en Bases de datos

Bases de datos II: Tema 6

Estructura

- Introducción
- Control de acceso discrecional.
- Control de acceso obligatorio.
- Cifrado de datos
- Bases de datos estadísticas
- Mecanismos de seguridad en Oracle.

Introducción

- Objetivo: analizar las técnicas empleadas por el SGBD para proteger la BD de personas no autorizadas a tener acceso a cierta información.
- Diferencia entre seguridad e integridad:
  - Seguridad: protección de los datos contra su alteración, o revelación no autorizada.

Proteger los datos ante usuarios No autorizados

  - Integridad: se refiere a la precisión o validad de esos datos.

Proteger los datos ante usuarios autorizados

- La seguridad abarca varios temas:

Cuestiones Éticas y legales

Política gubernamental

- La seguridad se debe imponer en varios niveles:
  - Físico: equipos protegidos
  - Sistema operativo
  - Red
  - Sistema de gestión de BD: posee un subsistema de seguridad y autorización que se encarga de garantizar la seguridad de los datos.

- Papel del Administrador de BD en la seguridad:
  - Creación de cuentas
  - Concesión y revocación de privilegios.
  - Asignación de niveles de seguridad según la organización.
- El sistema de BD debe llevar un control de las operaciones que cada usuario realiza (auditorías).
- Tipos de mecanismos:
  - Acceso discrecional
  - Acceso obligatorio

Control de acceso discrecional

- Es un modo de restringir el acceso a la información basado en privilegios.
- Debe asignarse privilegios adecuados a un usuario para que pueda acceder a un objeto determinado.
- Los usuarios con ciertos privilegios pueden conceder privilegios a otros usuarios a su discreción:
- Podemos hablar de dos niveles de asignación de privilegios en términos informales:
  - Nivel de cuenta: el administrador especifica los privilegios particualares que tiene cada usuario.
  - Nivel de relación: se controlan los privilegios para tener acceso a cada relación o vista. Cada tabla (relación) tiene asignada una cuenta propietario que tiene todos los privilegios sobre la tabla y se encarga de otorgarlos al resto de cuentas.

Control de acceso discrecional (2)

- Nivel de cuenta: privilegio para crear tablas, vistas, para realizar consultas, modificar tablas..
- Nivel de relación: privilegio para modificar, seleccionar ciertas columnas en una tabla, para crear claves ajenas….
- Las sentencias para asignar y quitar privilegios en SQL son: `GRANT` y `REVOKE`.
- Los privilegios se puede propagar con la opción `WITH GRANT OPTION`.
- Las vistas también pueden utilizarse como mecanismo de autorización discrecional:

```
CREATE VIEW [user.]nombrevista
AS CONSULTA
```


Control de acceso obligatorio

- En muchas organizaciones se necesita una política de seguridad adicional que clasifique los datos y los usuarios de acuerdo con ciertas clases de seguridad.
- Las clases de seguridad usuales son:
  - Máximo secreto (MS)
  - Secreto (S)
  - Confidencial (C)
  - No confidencial (NC)

MS> S > C > NC

- Modelo de seguridad multinivel: asigna a cada sujeto y objeto una de las clasificaciones de seguridad anteriores.
  - Acreditación: clasificación de un sujeto como clase(S)
  - Clasificación de un objeto como clase(O)

- Se asegura el cumplimiento de restricciones de acceso a datos de la siguiente forma:
  - Un sujeto S no puede tener acceso de lectura a un objeto (O) si la clase(O) > clase(S)
  - Un sujeto S no puede tener acceso de escritura a un objeto O si la clase clase(S)> clase(O)
- Para incorporar las nociones de seguridad multinivel en las BD relacionales se considera cada atributo y tupla como objetos de datos.
- Así, cada atributo A, está relacionado con un atributo de clasificación C:

`R(A1,C1,A2,C2,…An,Cn,CT)`

CT es el valor Más alto Ci

- La clave aparente de una relación multinivel es el conjunto de atributos que habrían formado la clave en una relación normal.
- A veces se puede utilizar un proceso llamado filtrado que produce varias vistas de la misma tupla según la clasificación de cada atributo.
- Concepto de poliinstanciación: varias tuplas pueden tener el mismo valor de clave aparente pero diferentes valores de atributos para usuarios con diferentes niveles de acreditación.

Empleado

a

Nombre	Salario	Productividad	CT
Smith U	4000 C	Regular S	S
Brown C	8000 S	Bueno C	S

b

Nombre	Salario	Productividad	CT
Smith U	4000 C	NULL	C
Brown C	NULL	Bueno C	c

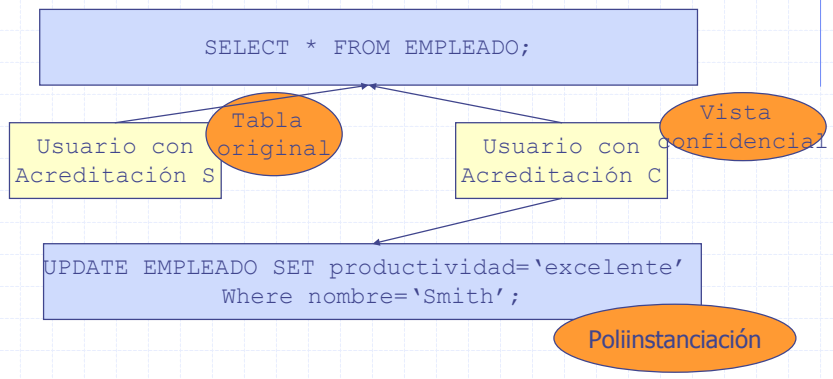
c

Nombre	Salario	Productividad	CT
Smith U	NULL	NULL	U

d

Nombre	Salario	Productividad	CT
Smith U	4000 C	Regular S	S
Smith U	4000 C	Excelente S	C
Brown C	8000 S	Bueno C	S

- Supongamos la siguiente consulta:



Base de datos estadística

- Una base de datos estadística es aquella que permite consultas que proporcionen información general (sumas, promedios) pero no consultas que proporcionen información individual.
- Problema: es posible hacer inferencias a partir de consultas válidas para deducir las respuestas a consultas no válidas: deducción de información confidencial por inferencia.

- Ejemplo: tabla `persona`

NOMBRE	DNI	INGRESOS	DIRECCION	CIUDAD	ESTADO	CP	SEXO	GRADO

Consultas estadísticas

```
c1: select count(*) from persona
      where 'condicion';
C2: select average(ingreso) from persona
      where 'condicion'
```

Consulta: "*obtener el salario de 'Jane Smith' si sabemos que tiene un doctorado y que vive en la ciudad de Valencia*"

```
condicion= grado= 'doctor' and sexo ='M'
and ciudad ='Valencia' and pais ='España'
```

Si el nº de tuplas es pequeño Se puede deducir El salario

Cifrado de datos

- Otra forma de proteger los datos es el cifrado o encriptación de los datos (guardado y transmisión de los datos de forma cifrada).
- Se utiliza un algoritmo de encriptación: los detalles del algoritmo son conocidos pero no la clave utilizada
- Los datos sólo son legibles cuando se proporcionan al usuario.

Mecanismos de seguridad en Oracle

- Control de acceso discrecional
- Facilidades que ofrece Oracle:
  - Usuarios y esquemas de la BD.
  - Privilegios
  - Papeles
  - Opciones de almacenamiento y cuotas
  - Limitación de recursos
  - Auditorías

Usuarios

- Cada BD Oracle tiene una lista de nombres de usuarios con una clave asociada para su autentificación (se guardan en el catálogo del sistema).
- Existe un esquema asociado a cada usuario que corresponde a los objetos que son de su propiedad.
- Por defecto se crean dos usuarios: `SYS y SYSTEM.`
- Sentencia para crear nuevos usuarios:

```
CREATE USER userIDENTIFIED {BY password| EXTERNALLY}
DEFAULT TABLESPACE tablespace
TEMPORARY TABLESPACE tablespace
QUOTA {integer [K|M] UNLIMITED } ON tablespace
[PASSWORD EXPIRE]
[ACCOUNT LOCK |UNLOCK]
[PROFILE {profile| DEFAULT }]
```


- Formas de autentificar un usuario:
  - A través del usuario y password:

```
create user yo identified by miclave
```

  - A través del sistema operativo:

```
Create user OPS$esther identified EXTERNALLY
```

- Modificación de usuarios:

```
ALTER USER usuario [mismas opciones]
```

```
DROP USER usuario [CASCADE]
```

- Vistas para controlar usuarios: **`dba_users`**

Profiles (perfiles)

- Cada usuario tiene asignado un perfil que especifica las limitaciones sobre los distintos recursos del sistema:
  - Número de sesiones concurrentes
  - Tiempo de procesamiento de CPU
  - Cantidad de entradas y salidas lógicas
  - Cantidad permitida de tiempo sin trabajar
  - Cantidad de tiempo por conexión.
- Se pueden crear varios perfiles y asignarlos individualmente a cada usuario de la BD. Existe un perfil por defecto

- Sentencia de creación de *profile:*

```
Create profile nombreperfile LIMIT
[SESSIONS_PER_USER numero]
[CPU_PER_SESSION numero]
[CPU_PER_CALL numero]
[CONNECT_TIME numero]
[IDLE_TIME numero]
[LOGICAL_READS_PER_SESSION numero]
[LOGICAL_READS_PER_CALL numero]
[COMPOSITE LIMIT numero]
[PRIVATE_SGA numero]
[PASSWORD_LOGIN_ATTEMPS maximo]
[PASSWORD_LIFE_TIME maximo]
[PASSWORD_REUSE TIME maximo]
 PASSWORD_REUSE_MAX maximo]
[ACCOUNT_LOCK_TIME maximo]
[PASSWORD_GRACE_TIME maximo]
```

recursos

Parámetros de passwords

- Asignación de perfiles a los usuarios:

```
ALTER USER usuario PROFILE el_perfil
```

- Borrar un perfil:

```
DROP PROFILE miperfil
```

- Es necesario habilitar los límites de recursos:

```
Parámetro de inicialización:
        RESOURCE_LIMIT = TRUE
Habilitar el parámetro:
       alter system set RESOURCE_LIMIT = TRUE
```

- Los parámetros relacionados con los passwords están activos aunque `RESOURCE_LIMIT = FALSE`

Privilegios

- Derecho a ejecutar un tipo particular de sentencia SQL.
- Existen dos tipos de privilegios
  - Privilegios del sistema: permite a los usuarios realizar acciones particulares en la BD.
  - Privilegios de objetos: permite a los usuarios acceder y manipular un objeto particular.
- Un usuario puede recibir privilegios de forma directa o a través de papeles (grupo de privilegios con nombre). Normalmente los privilegios se asignan a papeles.

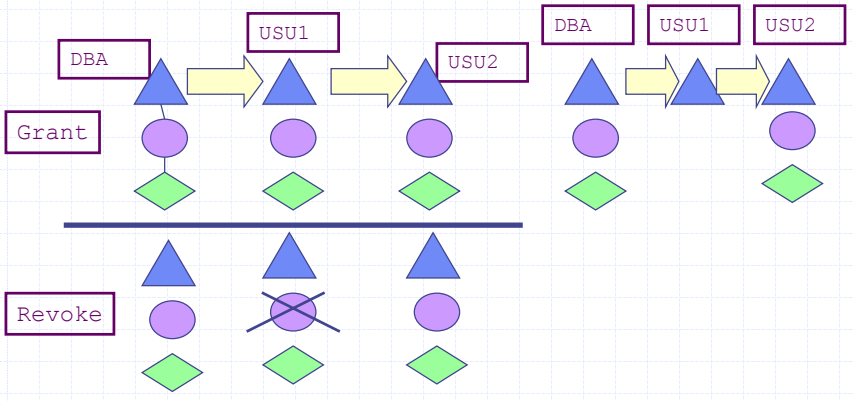
Ejemplos de privilegios de sistema:

Categoría	Ejemplos
INDEX	create any index alter any index drop any index
TABLE	create table crate any table alter any table select any table upadate any table delete any table
TABLESPACE	create tablespace alter tablespace drop tablespace

Otorgar y quitar privilegios del sistema:

```
GRANT privilegio_sis TO user [WITH ADMIN OPTION];
```

```
REVOKE privilegio_sis FROM user;
```



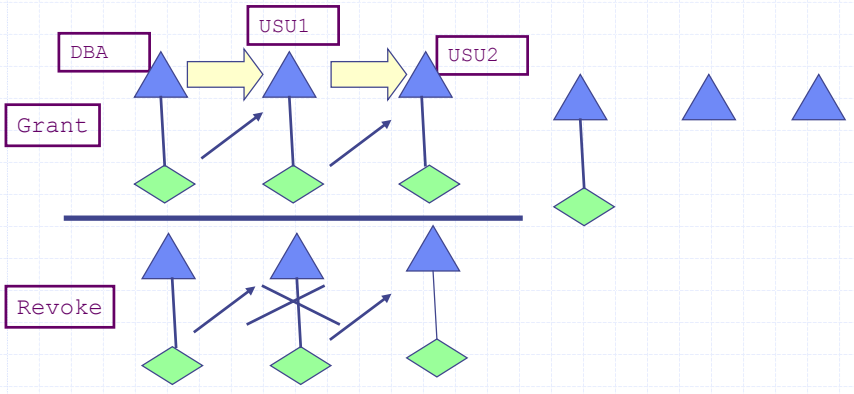
Resumen de privilegios de objetos:

priv.	table	view	sequence	procedure
ALTER	X		X	
DELETE	X	X		
EXECUTE				X
INDEX	X			
INSERT	X	x		
REFERENCES	X			
SELECT	X	X	x	
UPDATE	X	X		

Conceder y quitar privilegios de objetos:

```
GRANT privilegio_obj [lista_col] ON [esquema.]obj
TO {user |role|PUBLIC [WITH GRANT OPTION];
```

```
REVOKE privilegio_obj ON [esquema.]obj
 FROM user;
```



Papeles

- Los papeles proporcionan una forma más sencilla de gestionar los privilegios.
- Son un grupo de privilegios a los que se le da un nombre (se conceden a usuarios o a otros papeles).
- Propiedades de los papeles:
  - Reducen las concesiones de privilegios.
  - Gestión dinámica de los privilegios: cuando se deben cambiar los privilegios de un grupo, basta con modificar los privilegios del papel que representa el grupo.
- Creación de papeles:

```
CREATE ROLE role;
DROP role;
```


- Papeles predefinidos:

Nombre del papel	Descripción
connect resource	por compatibilidad con versiones anteriores
DBA	Todos los privilegios del sistema WITH ADMIN OPTION
EXP_FULL_DATABASE	Para exportar la BD
IMP_FULL_DATABASE	Para importar la BD
DELETE_CATALOG_ROLE	Privilegios de borrado de tablas del catálogo
SELECT_CATALOG_ROLE	Privilegios de consultar catálogo del sistema

Auditorías

- Oracle permite auditorías selectivas de las acciones de los usuarios para ayudar en la investigación de uso dudoso de la BD.
- Se pueden realizar a tres niveles:
  - Auditorías de sentencias: auditan sentencias SQL especificas sin importarles ningún objeto determinado.
  - Auditorías de privilegios: audian el uso de privilegios potentes del sistema sin importarles ningún objetos determnado.
  - Auditorías de objetos: auditan el acceso a un objeto de un esquema específico sin importar el usuario.
- El resultado de la auditoría se almacen en una tabla denominada rastro de la auditoría.

- Para auditar operaciones del sistema o privilegios del sistema se debe poseer el privilegio `AUDIT SYSTEM` y para auditar objetos `AUDIT ANY`.

```
AUDIT {operación|privilegio} [by usuario]
[By {sesion|access}] [WHENEVER [NOT] SUCCESSFUL]

AUDIT {operación_obj} on [esquema.]objeto
[By {sesion|access}] [WHENEVER [NOT] SUCCESSFUL]
```