Bases de Datos I

Facultad de Ciencias Exactas
UNIVERSIDAD NACIONAL DEL CENTRO DE LA PROVINCIA DE BUENOS AIRES

Seguridad y control de acceso

INGENIERÍA DE SISTEMAS

Cursada 2019

SEGURIDAD DE LA INFORMACIÓN

- La información es un activo esencial de las organizaciones
- Necesidad de proteger los datos contra accesos no autorizados, fraude/sabotaje, errores “accidentales”, etc.
- Aspectos relativos a la seguridad:
  - Cuestiones éticas y legales (de acceso a cierta información)
  - Políticas de la organización (decisiones sobre permisos de acceso)
  - Funciones del sistema (a nivel del hardware, del sistema operativo, ..)
  - Problemas operacionales (generación y resguardo de claves)
  - Necesidad de encriptación de ciertos datos confidenciales
  - Protección contra ataques directos o indirectos (mediante operaciones para “descubrir” información relevante a partir de información no confidencial, o por inyección de código SQL malicioso en la interfaz de aplicación para forzar a que se ejecute el código “malintencionado" sobre la BD)

SEGURIDAD EN BASES DE DATOS

- El SGBD provee un subsistema de seguridad y autorización de la BD
- Hoy en día hay múltiples formas de autentificación no solo cuenta de usuario y contraseña
- El Administrador de la BD (DBA) -que posee cuenta privilegiada- debe asegurar una política de acceso clara y consistente:
  - decidir quién entra a la BD y qué puede hacer sobre los objetos a los que puede acceder (limitado a lo que se tiene acceso)
  - garantizar la seguridad de partes de la BD contra accesos no autorizados (sin derecho de acceso)
  - no impedir el acceso a los datos por usuarios habilitados (disponibilidad)

¿Qué datos?
(restringir filas/columnas?)

¿Quiénes?
(cuáles usuarios?)

¿Qué operaciones?
(sólo consulta o modificación?)

CONTROL DE ACCESO A LA BD

Granularidad: La protección de los objetos depende de su tamaño o extensión (ej: atributo, tupla, relación, BD)

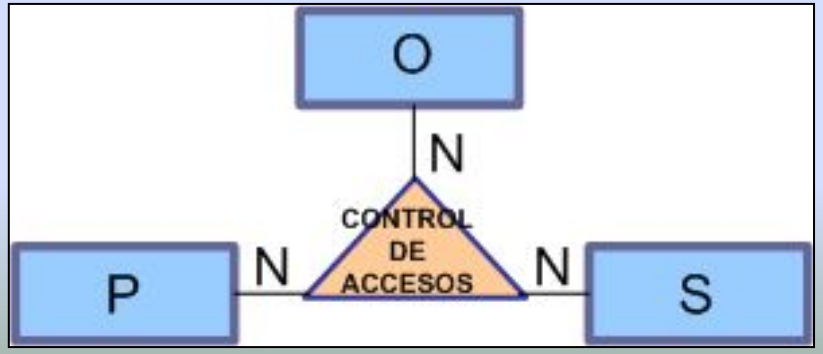
(S)ujeto: entidad que requiere acceso a un objeto

- (ej. usuario o programa)

(O)bjeto: entidad pasiva accedida por un sujeto

- (ej. registro, relación, índice, archivo)

(P)rivilegio o derecho de acceso: cómo un sujeto puede acceder a un objeto (consulta/modificación/borrado/inserción)



MÉTODOS DE CONTROL DE ACCESO

- **Control de Acceso Discrecional:**
  garantiza privilegios a usuarios: capacidad para acceder a datos específicos, registros o campos para operar de una manera determinada (read, insert, delete, update, otras…).

- **Control de Acceso basado en Roles:**
  establece grupos de privilegios encapsulados en un rol que se otorgan a usuarios

- **Control de Acceso Mandatorio:**
  clasifica usuarios y datos en múltiples niveles de seguridad y luego fuerza determinadas reglas acordes a cada nivel

CONTROL DE ACCESO DISCRECIONAL

El acceso a la BD se basa en otorgar (y revocar) privilegios sobre los objetos de la BD, selectivamente a usuarios:

GRANT privilegio/s ON objeto/s TO usuario/s
[WITH GRANT OPTION]

- **privilegio/s:** derecho/s para acceder a datos o ejecutar operación/es en la BD
- **objeto/s:** tablas, vistas, índices, etc.
- **usuario/s:** nombre de usuario que la BD reconoce como autorizado para acceder a la BD (uno o varios) o PUBLIC (=todos los usuarios, aún los futuros)
- **WITH GRANT OPTION:** permite que el usuario poseedor de privilegios pueda transmitirlos a otros usuarios
  - → Se puede propagar un mismo privilegio a más de un usuario
  - → Se puede recibir un mismo privilegio de más de un usuario

CONTROL DE ACCESO DISCRECIONAL

Niveles de ASIGNACIÓN DE PRIVILEGIOS:

- **Nivel de cuenta: capacidades particulares conferidas que tiene cada usuario, independientemente de las relaciones de la BD** (CREATE SCHEMA, CREATE TABLE, CREATE VIEW, ALTER, DROP, …)

- **Nivel de relación: privilegios de acceso a relaciones particulares**
  - **SELECT** – leer todas las columnas (incluyendo las que se añadan con ALTER TABLE)
  - **DELETE** – remover datos
  - **INSERT** (columna/s) – incorporar nuevas tuplas con valores no-nulos o no-default en esa/s columna/s. Sin ( )– ídem para todas las columnas
  - **UPDATE**– análogo a INSERT para modificar datos existentes
  - **REFERENCES** (columna/s) – definir FK referidas a esa/s columna/s. Sin ( )– ídem para todas las columnas

CONTROL DE ACCESO DISCRECIONAL

- El propietario de un esquema puede ejecutar CREATE, ALTER, DROP de objetos en su esquema
- El propietario de un objeto posee todos los privilegios sobre el objeto, y también la capacidad de concederlos (mediante GRANT) y además WITH GRANT OPTION (WGO)
- El **DBA** tiene una cuenta especial con privilegios de superusuario y es responsable de la seguridad de la BD (entre otras cosas!)
- Para poder llevar registro de la concesión de privilegios otorgados el SGBD lleva una **matriz de acceso**

	Objetos O_j (relaciones, columnas, ...)		
Sujetos S_i	...	**...**	**...**
(usuarios)	...	**A[S_i, O_j]**	...
	...	**...**	**...**

CONTROL DE ACCESO DISCRECIONAL

Un usuario puede REVOCAR un privilegio que otorgó previamente a otro usuario (o la opción de propagarlo):

REVOKE [GRANT OPTION FOR] privilegio/s ON objeto/s
FROM usuario/s {CASCADE | RESTRICT}

- Si se especifica **GRANT OPTION FOR** se quita la posibilidad de propagar el privilegio (pero no cancela el privilegio sobre el objeto), sino se revoca el privilegio sobre el objeto en sí
- opción **CASCADE**: revoca el privilegio al usuario y a todos los que lo recibieron a través de él (no quedan privilegios *colgados*)
  → alguien puede seguir conservándolo si lo recibió de otro usuario
  → el SGBD debe llevar rastro de la *concesión de privilegios*
- opción **RESTRICT**: se rechaza si quedan privilegios colgados

CONTROL DE ACCESO DISCRECIONAL

VISTAS → mecanismo para forzar seguridad sobre los datos

GRANT/REVOKE en VISTAS:

- Para crear una Vista, se debe tener permiso SELECT para todas las relaciones base (tablas/vistas) que definen la Vista
- El creador de una vista tendrá privilegio SELECT WGO sólo si posee privilegios SELECT WGO sobre cada relación base
- Si una vista es actualizable y su creador tiene privilegios de INSERT, DELETE o UPDATE sobre la/s relación/es base, tendrá esos mismos privilegios en la vista
- Si se pierde el privilegio SELECT sobre alguna de las relaciones base → la vista es removida
- Si el creador de una vista pierde un privilegio obtenido con WGO sobre una relación base → pierde el privilegio sobre la vista (también los demás usuarios que hayan obtenido el privilegio sobre la vista)

CONTROL DE ACCESO DISCRECIONAL

Ejemplo

A es propietario del esquema y crea las tablas T1 y T2

A: **GRANT SELECT ON T1, T2 TO B;**
→ B puede seleccionar tuplas de T1 y T2 (sin posibilidad de propagarlo)

A: **GRANT SELECT ON T1, T2 TO C WITH GRANT OPTION;**
→ C puede seleccionar tuplas de T1 y T2 (y puede propagar el privilegio)

C: **GRANT SELECT ON T1 TO B, D;**
→ B y D pueden seleccionar tuplas de T1 (pero no propagar el privilegio)

A: **REVOKE SELECT ON T1 FROM C CASCADE;**
→ C pierde el privilegio de selección sobre T1
y esto se propaga en cascada a B y D
pero B había recibido también el privilegio directamente de A

¿Qué privilegios conserva cada usuario entonces? (*analizar grafo*)

ANÁLISIS EN CLASE

CONTROL DE ACCESO BASADO EN ROLES

- Se puede tornar complejo el manejo de concesión y revocación de privilegios cuando hay muchos usuarios en una BD
- **Rol** → Conjunto de privilegios o derechos de acceso

CREATE ROLE <nom_rol>;

GRANT nom_rol [{,<nom_rol> }] TO <a-quien> [{,<a-quien>}]
[WITH ADMIN OPTION] ;

  - a_quien→ usuarios/ otros roles/ PUBLIC (todos)
  - un usuario puede tener asignado a uno o más roles
  - Rol especial: ADMIN (tiene privilegios como: *create role* y *drop role*)
  - WITH ADMIN OPTION → se puede conceder (y luego revocar) el rol a otros

Ej: CREATE ROL RR; GRANT CREATE TABLE TO RR; GRANT RR TO user1;

- Si se cambian los privilegios encapsulados en un rol → los privilegios de todos los usuarios que tienen ese rol también cambian
- SQL:1999 incluye soporte para roles (muchos SGBD adhieren a este enfoque)

CONTROL DE ACCESO BASADO EN ROLES

Para revocar un Rol o la posibilidad de conceder el Rol:

REVOKE [ADMIN OPTION FOR] nom_rol [{, nom_rol}]
FROM <*a_quien*> [{,<*a_quien*>}] [CASCADE | RESTRICT] ;

a_quien= usuario | otro rol |PUBLIC

→ No se pueden revocar los privilegios del propietario de un objeto

Ej: REVOKE CREATE TABLE FROM RR;

→ RR pierde el rol

REVOKE ADMIN OPTION FOR manager FROM RR;

→ RR pierde la posibilidad de ceder el rol

CONTROL DE ACCESO MANDATORIO

- Cada objeto de la BD (tabla, vista, tupla, columna,…) tiene asignada una **clase de seguridad** → ***seguridad multinivel***
- Cada sujeto (usuario, cuenta, programa) tiene asignado un permiso para una clase de seguridad
- Las clases de seguridad usuales son: **Top secret** (TS), **Secret** (S), **Confidential** (C), **Unclassified** (U)
- Se basan en estrategias de la organización, no pueden ser modificados por los usuarios individualmente
- Existen reglas que habilitan -o no- las lecturas/escrituras en la BD, según combinaciones de clases de seguridad y permisos
- La mayoría de los SGBD actuales no soportan este control - algunos lo hacen para aplicaciones específicas (*ej. Defensa, Espionaje, …*)

CONTROL DE ACCESO MANDATORIO

Modelo Bell-LaPadula (BLP): **asigna a cada sujeto S y objeto O un nivel de Seguridad:** Top secret (TS), secret (S), confidential (C), unclassified (U) → con TS > S > C > U

Derecho de acceso → si se satisface la regla de control de acceso:

- S puede leer O sólo si nivel(S) >= nivel(O)
- S puede escribir O sólo si nivel(S) <= nivel(O)

→ "no read up, no write down"

- un sujeto no puede leer un objeto con nivel más alto que el que él posee
- un sujeto no puede escribir un objeto que tenga clasificación menor que la que él posee (impide que la información fluya a niveles de seguridad más bajos)

BIBLIOGRAFÍA

Date, C., "An Introd
uction to Database Systems". 8º ed., Addison Wesley, 2004 (Cap. 17)

Elmasri, R., Navathe, S., "Fundamentals of Database Systems", Addison Wesley, 6th. Ed, 2011 (Cap. 24) – Pearson, 7th. Ed (Cap.30)

Ramakrishnan R., Gehrke J., "Database Management Systems", 3° ed. , McGraw-Hill, 2003 (Cap. 21)