Seguridad y Competencias Profesionales
Tema 7: Seguridad en bases de datos
Curso 2012–2013

Ingeniería en Informática (2° ciclo)

Departamento de Ingeniería Informática
Universidad de Cádiz

Cádiz, 19 noviembre 2012

Índice

Objetivos

Conocimiento

- Reconocer la necesidad de tener una BD segura.
- Enumerar los aspectos fundamentales de la seguridad.
- Conocer los medios disponibles para tener una BD segura.

Comprensión

- Comparar las diferentes herramientas que tenemos para asegurar una BD.
- Explicar los riegos existentes en BD sin auditar.

Aplicación

- Formular métodos de seguridad para una BD.
- Utilizar las herramientas de las que dispone un DBA.

Bibliografía I

Abramson, I.; Abbey, M. & Corey, M.
Oracle Database 10g. Guía de aprendizaje
Osborne McGraw-Hill, 2005.

Castano, S.; Fugini, M.; Martella, G. & Samarati, P.
Database Security
Addison-Wesley, 1996.

Connolly, T. & Begg, C.
Sistema de Bases de Datos
Addison-Wesley, 4ª edición, 2005.

Date, C.J. & Darwen, H.
The SQL Standard
Addison-Wesley, 3ª ed., 1993.

Bibliografía II


Date, C.J.
Introducción a los Sistemas de Bases de Datos
Prentice Hall, 7ª edición, 2001.


Earp, R. & Bagui, S.
Learning SQL: A step by step guide using oracle
Addison Wesley, 2003.


Elmasri, R. & Navathe, S.B.
Fundamentos de sistemas de Bases de Datos
Addison-Wesley, 5ª edición, 2007.


Loney, K. & Bryla, B.
Oracle Database 10g. Manual del administrador
Osborne McGraw-Hill, 2005.

Bibliografía III


Piattini, M.G. & del Peso, E.
Auditoría Informática. Un enfoque práctico
Ra-Ma, 2ª edición, 2001.


Silberschatz, A.; Korth, H. & Sudarshan, S.
Fundamentos de Bases de Datos
McGraw-Hill, 5ª edición, 2006.

Otros recursos

Sobre Oracle

- http://www.oracle.es
- http://www.revista-ays.com

Sistemas de Bases de Datos (SBD)

Concepto

Un sistema de BD (SBD) es un sistema de mantenimiento de registros por ordenador, cuyo propósito general es registrar y mantener la información.

Elementos

- Datos
- *Software*: programas que mantienen y actualizan los datos (Sistema de Gestión de BD o SGBD)
- *Hardware*: componentes electrónicos sobre los que se ejecutan los programas y se almacenan los datos
- Usuarios del SBD
- Administradores del SBD

Catálogo o Diccionario de Datos (DD)

Concepto

- Base de datos que describe la estructura de los propios datos, y las diversas restricciones de integridad (RI) a imponer
- Su estructura viene impuesta por el SGBD escogido

Relación con seguridad

El DD contiene:

- Restricciones para evitar la revelación, alteración o destrucción no autorizada de información (seguridad en general)
- Propiedades que deben cumplirse en todo momento sobre dicha información (integridad en particular)

Consideraciones generales

- Aspectos legales, sociales y éticos: ¿el solicitante tiene derecho a conocer ese dato? ¿La BD cumple la legislación vigente?
- Política interna de la empresa: la empresa decide quién puede acceder a los datos
- Controles físicos: protección del cuarto de los ordenadores
- Protección de operación: uso y mantenimiento de contraseñas
- Controles de equipo: contraseñas para la protección de las áreas de almacenamiento y ficheros de datos
- Seguridad del SO: ¿borra el SO el contenido de las áreas de almacenamiento y ficheros cuando ya no se necesitan?

¿La seguridad del SO es suficiente?

Sistema operativo: primer bastión

Identifica y autentica a los usuarios *de la máquina*

Diferencias entre seguridad SO y BD

- Una BD tiene más objetos a proteger y son más complejos
- Los objetos de una BD viven más tiempo
- Se requiere control de acceso más fino a múltiples niveles (interno, conceptual, externo)

Conclusión

El SGBD implementa lo que el SO no tiene

Ventajas

- No hay necesidad de que todos los SO tengan los mecanismos que requiere cada SGBD.
- Conoce las características de los objetos a proteger.
- Lleva control del uso de objetos por parte de los usuarios.
- Son transportables.

Nota

Nos centraremos en Oracle (versión 10).

Seguridad en un SGBD

Subsistemas presentes

Control	Previene fallos
Detección	Detecta fallos cuando se producen
Recuperación	Corrige fallos tras detectarse

Aspectos a proteger

Confidencialidad	Evitar fugas de información y asegurar la privacidad
Disponibilidad	Mantener la información accesible
Integridad	Datos no falseados y consistentes entre sí

Mecanismos disponibles

Prevención: privilegios

- A distinta granularidad: BD, tablas, columnas, tuplas, etc.
- Según tipo de operación (DDL, DCL, DML)
- Según horario
- Según situación (permisos manuales impuestos por DBA)
- Combinables de diversas formas

Detección

Auditoría a varios niveles de granularidad y de detalle.

Recuperación

- Copias de seguridad
- Integrados en el SGBD

Seguridad de los datos

Objetivo en una BD

Datos sólo accesibles de la forma autorizada por personas autorizadas.

Conceptos relacionados

Seguridad Protección de los datos contra acceso accidental o intencionado por parte de personas no autorizadas y contra su destrucción o alteración.

Reserva Derecho a determinar cuándo, cómo y en qué medida y circunstancia se permitirá la comunicación de la información a terceras personas.

Principios generales

Asignación mínima de privilegios

Cada usuario sólo tendrá los permisos estrictamente necesarios.

Tareas del DBA

- Limitar vías de acceso a las permitidas.
- Controlar el acceso a ellos según acción y usuario.

Problemas

Conflicto de intereses

- Queremos un SGBD cómodo, potente, flexible y rápido
- Pero esto dificulta el control de los accesos

Otros problemas

- Extracción de datos personales por inferencias en BD estadísticas
- Definir los niveles de seguridad en BD muy grandes

Autenticación del usuario

Antes de limitar al usuario, hemos de saber quién es

Acceso en línea

- Autenticamos a un humano
- Lo identificamos:
  - Algo que sabe (contraseñas)
  - Algo que tiene (tarjetas magnéticas, p.ej.)
  - Algo que es (biometría)

Acceso en segundo plano

- Autenticamos a un programa, no a un humano
- Identificación no personal

Sistemas de gestión de privilegios

Tipos de SBD según permisos por omisión

Abiertos Permiten todo, y el DBA ha de quitar lo innecesario

Cerrados No permiten nada, y el DBA ha de dar lo necesario

Tipos de usuarios

- Hacen programas: el usuario sólo debe poder acceder a datos permitidos, a través de esquemas externos
- Usan programas: el usuario sólo debe poder ejecutar los programas que necesita

Operaciones a controlar

- Conectarse a la BD
- Consultar ciertos datos
- Actualizar ciertos datos
- Crear o actualizar objetos (DDL)
- Ejecutar procedimientos almacenados
- Crear estructuras adicionales:
  - Índices
  - Agrupamientos
  - Funciones de dispersión
- Conceder privilegios sobre objetos o el sistema

Concesión de privilegios

Posibles acciones

- Un usuario puede dar privilegios (**GRANT**) y revocarlos (**REVOKE**) a otro usuario o a un rol
- Puede permitirse también administrar dicho privilegio (**WITH ADMIN OPTION**)
- Estos últimos privilegios pueden revocarse en cascada si son concedidos sobre objetos de algún esquema, y no sobre el sistema
- Si un privilegio viene de varias cadenas de **GRANT**, sólo se pierde cuando se revocan todas

Roles

- Reúnen una serie de privilegios en un solo sitio
- Pueden activarse y desactivarse a voluntad

Restricción de acceso a una parte de una tabla

Permitimos que el usuario acceda a una vista o "ventana" de la tabla original

Uso del nivel externo

- Nivel superior de la arquitectura ANSI/SPARC
- Contiene subesquemas para usuarios y aplicaciones
- Cada subesquema contiene vistas, consultas con nombre que pueden tratarse como tablas, con ciertas condiciones

Utilidad

- Podemos permitir únicamente acceder a una vista, y no a la tabla original
- Esto nos permite, por ejemplo, limitar las filas visibles según los valores de sus campos
- En un futuro podremos cambiar la tabla original con mayor facilidad (independencia lógica)

Conceptos importantes en recuperación de fallos

Ficheros de recuperación (*redo logs*)

- Oracle va registrando los cambios en estos ficheros antes de llevarlos a los ficheros de datos de la BD
- Pueden llenarse, por lo que suelen rotarse varios juegos
- Pueden multiplexarse a varios soportes de almacenamiento
- Pueden archivarse, para tener mayor alcance

Puntos de comprobación (*checkpoints*)

Marcan un momento en que todos los cambios anteriores a él confirmados se han guardado en los ficheros de datos

Fallos de soportes de almacenamiento

Requisitos del mecanismo

- Tener una copia de seguridad reciente
- Disponer de registros de recuperación en un soporte distinto al que falló (se recomienda *multiplexar*)

Pasos a ejecutar

1. Recuperar la base de datos a partir de la copia de seguridad
2. Repetir lo hecho desde la copia de seguridad:
   - Se hacen los cambios de las transacciones completadas y sin completar
   - Se deshacen los cambios de las transacciones sin completar

Fallo del usuario

Casos

- **DROP TABLE** o **DROP TABLESPACE** lanzado por error
- Fallo en un programa que manipulaba automáticamente una tabla

Técnica: *tablespace point-in-time recovery*

1. Retirar los espacios de tablas afectados
2. Recuperar en una BD aparte los espacios en un instante específico de tiempo a partir de copias de seguridad
3. Mover los espacios recuperados a la BD original

Fallo de una instancia

Casos

- Pérdida de fluido eléctrico
- Cierre de la instancia no limpio

Acciones

1. A partir del último punto de comprobación, se repiten todos los cambios que había en el registro de recuperación
2. Se cancelan todas las transacciones que hubiera abiertas

Otros fallos

Sentencia SQL

- Ejemplo: **INSERT** con el disco lleno
- Se informa del fallo y se cancelan sus cambios
- Posiblemente se cancela la transacción

Proceso de la instancia

Un proceso monitor se ocupa de lanzarlos de nuevo.

Integridad

Recordatorio del concepto

Protección de los datos contra operaciones que introduzcan inconsistencia en los datos, manteniendo su corrección, validez y precisión.

Riesgos contra la integridad

- Operaciones semánticamente inconsistentes
- Interferencias debido a accesos concurrentes

Restricciones semánticas o de integridad

Tipo

Estáticas	Violación sobre definición de dominio de un dato
Dinámicas	El sueldo de un empleado no puede disminuir

Formas de describirlas en el SGBD

- Descritas dentro de los objetos del esquema (DD): tipos de los atributos, valor nulo aceptado/rechazado, longitudes máximas, claves foráneas, etc.
- Descritas utilizando disparadores y procedimientos almacenados

¿Restricciones en el DD o con código?

Ventajas

- Las RI son más sencillas de entender y de cambiar, facilitando su mantenimiento.
- Se detectan mejor las inconsistencias.
- Se protege mejor la integridad. No se puede escribir un programa que las viole llevando a la BD a un estado inconsistente.

Desventaja principal

Son mucho menos expresivas.

Problemas por concurrencia

Situación

- Múltiples usuarios escriben y leen en una BD concurrentemente, posiblemente sobre los mismos objetos
- Cada usuario debe poder llevar sus transacciones (secuencias de operaciones ejecutadas de forma atómica) sobre un estado consistente de la BD

Protecciones contra concurrencia

- Un acceso de A a X puede requerir un cerrojo:
  - Exclusivo: hay que esperar a que todos los demás suelten sus cerrojos sobre X
  - Compartido: hay que esperar a que todos los demás tengan como mucho cerrojos compartidos sobre X
- Al actualizar filas, las transacciones echan cerrojos exclusivos sobre ellas, forzando un orden sobre las escrituras

Problemas al aislar transacciones

Tipos de lecturas problemáticas

Sucias	Hay datos modificados por una transacción no confirmada
No repetibles	Al volver a ejecutar una consulta, hay datos cambiados o borrados por una transacción confirmada
Fantasma	Al volver a ejecutar una consulta con una condición, hay datos añadidos por una transacción confirmada

Tipos de niveles de aislamiento

Lectura de datos confirmados

Las sentencias (*no* las transacciones) sólo leen datos que estaban confirmados en el momento de su inicio. Es el nivel por omisión.

Serializable

La transacción sólo ve los datos que estaban confirmados a su inicio, y puede operar sobre ellos. Puede tener que ser reintentada por el cliente varias veces.

Sólo lectura

La transacción sólo ve los datos que estaban confirmados a su inicio, y *no* puede operar sobre ellos.

Auditoría

Tipos

- A nivel de área de un departamento
- A nivel de aplicación informática

Metodología de auditoría de BD

Tradicional con una lista de control

Por riesgos evaluados, en base a los cuales se fija un objetivo de control y se indica cómo van a reducirse dichos riesgos.

Riesgos

Debidos a dependencia en la BD

- Reunir más datos en la BD implica más poder para el DBA
- Personal más difícil de reemplazar en caso de que se vaya
- Fallos de diseño y de implementación pueden causar gran impacto (p.ej. disparadores mal escritos o maliciosos)

Debidos a complejidad

- Más errores en datos y programas que en un Sistema de Gestión de Ficheros
- Posible incompatibilidad entre sistemas de seguridad del SGBD y del SO

Uso de un objetivo de control

Ejemplo

SGBD deberá preservar la confidencialidad de la BD.

Técnicas de control

- Tipos de usuarios
- Perfiles
- Privilegios

Mecanismos asociados

- Preventivas: controlar el acceso.
- Detectivas: monitorizar los accesos.
- Correctivas: copias de seguridad.

Si existen controles se diseñan *pruebas de cumplimiento*.

Pruebas sobre los mecanismos

De cumplimiento

Listar los privilegios y perfiles existentes en el SGBD. Si hay inconsistencias en los controles o no existen, diseñar *pruebas sustantivas*.

Sustantivas

Se analiza si dicho riesgo podría usarse para atacar la integridad del sistema, a través de una serie de transacciones. Los resultados se recogerán en un informe, con:

- Situación.
- Riesgo existente.
- Deficiencia a solucionar y posibles soluciones

Amenazas a la seguridad

Elementos a proteger

- Metadatos:
  - Estructura general de la BD guardada en el DD
  - Su borrado afecta a la disponibilidad de los datos
- Datos o información:
  - Almacenada en los ficheros base
  - Confidenciales

Tipos de amenazas

Las amenazas pueden ser:

- Accidentales: fallos de software y/o hardware, o errores humanos
- Intencionadas

Amenazas intencionadas

Ataques directos

- Inciden sobre la confidencialidad, integridad y disponibilidad de la BD:
  - Revelación,
  - Alteración y
  - Destrucción de datos

  Prevenimos controlando los medios de acceso a la BD y aplicando políticas administrativas oportunas.
- Inferencias estadísticas: tratan de descubrir datos individuales de los datos estadísticos.

Ataques indirectos

Caballos de Troya, rootkits, o cualquier otro *malware*

Definición de la política

Aspectos administrativos

- Control centralizado o descentralizado.
- Distinción entre propietario y administrador.

Mecanismos de control de acceso

- De menor privilegio.
- Según objeto, parte del objeto y contexto.
- Según la historia del objeto, del usuario, etc.
- Sistemas abiertos o cerrados.
- Derechos de acceso.

Control de flujo de información

Aplicación del reserva, respeto de la LOPD, etc.

Conclusiones

- La seguridad de la BD está formada por mecanismos que protegen a la BD frente a amenazas intencionadas o accidentales.
- Los controles de seguridad incluye:
  - mecanismos de autorización,
  - controles de acceso,
  - esquemas externos,
  - copias de seguridad y de recuperación,
  - mecanismos de integridad,
  - sistemas de cifrado y tecnología RAID.
- La carencia, la deficiencia o el mal diseño de medidas de seguridad en una BD puede no cumplir las leyes.

Tareas

1. Podemos decir que un SBD está compuesto por:
   - Software
   - Hardware
   - Datos
   - Usuario

   indicar las medidas de seguridad que se deben tomar para proteger cada uno de estos tipos de elementos.
2. Cada grupo buscará información sobre una de las siguientes BD NoSQL (Not SQL): Cassandra, Hadoop/HBase, CouchDB o MongoDB.
   - Introducción a NoSQL: características y comparativa con SQL (resaltar aspectos sobre seguridad).
   - Descripción de BD NoSQL escogida.
   - Enumerar algún proyecto/empresa que la utilice.
   - Referencias bibliográficas (para más información consúltese: `http://nosql-database.org/`).
3. Realizar los ejercicios propuestos bajo Oracle 10g.