SEGURIDAD Y ENCRIPTACION DE BASES DE DATOS

INTRODUCCIÓN

En la actualidad la mayor parte de bases de datos contienen la información sensible. Esto puede incluir la información de cliente, salarios de empleado, registros pacientes, números de la tarjeta de crédito, etc. La llave al mantenimiento de esta información en una manera segura es la confidencialidad.

La seguridad de los datos implica protegerlos de operaciones indebidas que pongan en peligro su definición, existencia, consistencia e integridad independientemente de la persona que los accede. Esto se logra mediante mecanismos que permiten estructurar y controlar el acceso y actualización de los mismos sin necesidad de modificar o alterar el diseño del modelo de datos; definido de acuerdo a los requisitos del sistema o aplicación software.

El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección. Los sistemas operativos proveen algunos mecanismos de protección para poder implementar políticas de seguridad. Las políticas definen qué hay que hacer (qué datos y recursos deben protegerse de quién; es un problema de administración), y los mecanismos determinan cómo hay que hacerlo. Esta separación es importante en términos de flexibilidad, puesto que las políticas pueden variar en el tiempo y de una organización a otra. Los mismos mecanismos, si son flexibles, pueden usarse para implementar distintas políticas.

Los siguientes siete requisitos son esenciales para la seguridad de la base de datos:

* La base de datos debe ser protegida contra el fuego, el robo y otras formas de destrucción.
* Los datos deben ser reconstruibles, porque por muchas precauciones que se tomen, siempre ocurren accidentes.
* Los datos deben poder ser sometidos a procesos de auditoria. La falta de auditoria en los sistemas de computación ha permitido la comisión de grandes delitos.
* El sistema debe diseñarse a prueba de intromisiones. Los programadores, por ingeniosos que sean, no deben poder pasar por alto los controles.
* Ningún sistema puede evitar de manera absoluta las intromisiones malintencionadas, pero es posible hacer que resulte muy difícil eludir los controles. El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.

Principios básicos para la seguridad

* Suponer que el diseño del sistema es público.
* El defecto de acceso debe ser: sin acceso.
* Chequear permanentemente, no confiar en que la seguridad sea inmutable.
* Los mecanismos de protección deben ser simples, uniformes y construidos en las capas más básicas del sistema.
* Los mecanismos deben ser aceptados sicológicamente por los usuarios.

MEDIDAS DE SEGURIDAD

* Físicas: Controlar el acceso físico al equipo. Ojo con backups!!!. Tarjetas de acceso, etc
* Personal: Acceso sólo del personal autorizado. Evitar sobornos, etc.
* SO: Seguridad a nivel de SO. Mejor servidor dedicado. Deshabilitar resto servicios.
* SGBD: Uso herramientas de seguridad que proporcione el SGBD. Perfiles de usuario, vistas, restricciones de uso de vistas, etc.
* Un SGBD cuenta con un subsistema de seguridad y autorización que se encarga de garantizar la seguridad de porciones de la BD contra el acceso no autorizado.
* Identificar y autorizar a los usuarios: uso de códigos de acceso y palabras claves, exámenes, impresiones digitales, reconocimiento de voz, barrido de la retina, etc
* Autorización: usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día.
* Uso de técnicas de cifrado: para proteger datos en Base de Datos distribuidas o con acceso por red o internet.
* Diferentes tipos de cuentas: en especial del ABD con permisos para: creación de cuentas, concesión y revocación de privilegios y asignación de los niveles de seguridad.
* Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoría de la Base de Datos.

En relación al SGBD, debe mantener información de los usuarios, su tipo y los accesos y operaciones permitidas a éstos.

Tipos de usuarios:

* DBA, están permitidas todas las operaciones, conceder privilegios y establecer usuarios
* Usuario con derecho a crear, borrar y modificar objetos y que además puede conceder privilegios a otros usuarios sobre los objetos que ha creado.
* Usuario con derecho a consultar, o actualizar, y sin derecho a crear o borrar objetos.

Privilegios sobre los objetos, añadir nuevos campos, indexar, alterar la estructura de los objetos, etc.

El ABD asigna el propietario de un esquema, quien puede otorgar o revocar privilegios a otros usuarios en la forma de consulta (select), modificación o referencias. A través del uso de la instrucción grant option se pueden propagar los privilegios en forma horizontal o vertical.

Los SGBD tienen opciones que permiten manejar la seguridad, tal como GRANT, REVOKE, etc. También tienen un archivo de auditoria en donde se registran las operaciones que realizan los usuarios.

Ejemplo: grant select on Empleado to códigoUsuario

revoke select on Empleado from códigoUsuario

Otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos, como:

* Lectura y copia de datos no autorizados
* Modificación o alteración de datos
* Destrucción de datos

Matriz de Autorización

La seguridad se logra si se cuenta con un mecanismo que limite a los usuarios a su vista o vistas personales. La norma es que la base de datos relacionales cuente con dos niveles de seguridad:

* Relación. Puede permitírsele o impedírsele que el usuario tenga acceso directo a una relación.
* Vista. Puede permitírsele o impedírsele que el usuario tenga acceso a la información que aparece en un vista.

Aunque es imposible impedir que un usuario tenga acceso directo a una información puede permitírsele acceso a una parte de esta relación por medio de una vista. De tal manera que es posible utilizar una combinación de seguridad al nivel relacional y al nivel de vistas para limitar el acceso del usuario exclusivamente a los datos que necesita.

Un usuario puede tener varias formas de autorización sobre partes de la base de datos. Entre ellas se encuentran las siguientes:

* Autorización de lectura, que permite leer, pero no modificar la base de datos.
* Autorización de inserción, permite insertar datos nuevos pero no modificar lo ya existente.
* Autorización de actualización, que permite insertar modificar la información pero no permite la eliminación de datos.
* Autorización de borrado, que permite la eliminación de datos.

Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores. Además de las formas de autorización de acceso de datos antes mencionados, es posible autorizar al usuario para que modifique el esquema de la base de datos.

* Autorización de índice, que permite la creación y eliminación de índices.
* Autorización de recursos, que permite la creación de relaciones nuevas.
* Autorización de alteración, que permite agregar o eliminar atributos de una relación.
* Autorización de eliminación, que permite eliminar relaciones.

Las autorizaciones de eliminación y borrado difieren en cuanto a que la autorización de borrado solo permite la eliminación de tuplas. La habilidad para crear nuevas relaciones viene regulada por la autorización de recursos de tal forma que la utilización del espacio del almacenamiento puede ser controlada. La autorización de índice puede aparecer innecesariamente puesto que la creación o eliminación de un índice no altera los datos en las relaciones. Más bien los índices son una estructura para realizar mejoras.

La forma fundamental de autoridad es la que se le da al administrador de la base de datos. El administrador de la base de datos puede entre otras cosas autorizar nuevos usuarios, reestructurar la base de datos, etc.

CIFRADO DE LA BASE DE DATOS

Los ataques a la seguridad pueden consistir en la escucha de los mensajes que se transmiten por la red, la inyección de mensajes en la red, la retransmisión de mensajes escuchados anteriormente, la suplantación del cliente o del servidor, etc. La solución a estos problemas se basa generalmente en utilizar criptografía tanto para proteger los datos como para autentificación. En la transmisión se aplica un algoritmo de cifrado al mensaje M usando una clave Kc y en la recepción se aplica el algoritmo de descifrado usando Kd. La función de cifrado es muy difícil de invertir sin conocer la clave. Existen dos esquemas:

Sistemas de clave secreta

En estos sistemas Kc es igual Kd. El algoritmo más usado es el Data Encryption Standard (DES) basado en 16 niveles de sustituciones y permutaciones. Es la más común por sencillez y velocidad. Este esquema sufre el problema de la distribución de la clave. Un ejemplo de sistema de autentificación basado en este esquema es Kerberos.

Sistemas de clave publica

En estos sistemas Kc es distinto a Kd. Kd es la clave secreta del servidor. El algoritmo más usado es el RSA basado en la factorización de números muy grandes que tengan pocos factores. Este esquema elimina el problema de la distribución de la clave pero no el de la suplantación de servidores.

La encriptación la podemos realizar mediante:

* El propio sistema operativo. Usando herramientas que trae el sistema operativo, pero entonces no se realiza de extremo a extremo. Es útil sólo si se combina con un sistema de canal de comunicaciones seguro.
* Incorporar herramientas de encriptación. Suelen trabajar en el sistema de ficheros. Como el anterior, es útil sólo combinándolo con un canal seguro.
* Usando las funciones que me proporciona la Base de datos. Hace más complejo el tratamiento de la base de datos, pero es la más segura ya que los datos se desencriptan en el momento del tratamiento, quedando por tanto el transporte y el almacenamiento, incluso temporales, completamente encriptados.
* Usando muestras propias funciones, incorporando funciones de encriptación ajenas a la Base de datos. Es el que añade la complejidad más alta al programador, pues este debe gestionar las funciones, claves, etc.

Encriptación de datos en transito

La mayoría de los ambientes de base de datos utilizan TCP/IP y el servidor de base de datos escucha algunos puertos y acepta las conexiones iniciadas por los clientes de la base de datos. Mientras que los puertos son configurables, la mayoría de la gente utiliza los puertos por defecto del servidor que está usando, por ejemplo: puerto 1433 para el servidor de Microsoft SQL, puerto 1521 para Oracle, puerto 4100 para Sybase, puerto 50000 para DB2, y puerto 3306 para MySQL.

Los clientes de la base de datos se conectan con el servidor sobre estos puertos predefinidos para iniciar una comunicación, dependiendo del tipo de la base de datos y la configuración del servidor, redireccionando a otro puerto o terminando la comunicación entera sobre el mismo puerto del servidor.

Meterse en tu base de datos de comunicaciones es relativamente fácil, porque la base de datos de comunicaciones son en su mayoría en texto plano. La manera de evitar que esto suceda es encriptar las comunicaciones entre la base de datos de clientes y servidores de bases de datos. Este tipo de cifrado es llamado cifrado de los datos en tránsito. La encriptación se produce en los extremos.

Anatomía de la Vulnerabilidad de datos en tránsito: Sniffing De Datos

Si un hacker va a espiar y robar datos, debe de suceder dos cosas:

1. El hacker debe ser capaz de colgarse físicamente en las comunicaciones entre los clientes de la base de datos y el Servidor de bases de datos.
2. El hacker debe ser capaz de entender el flujo de comunicación a un nivel que le permita la extracción de los datos sensibles.

De los dos, el conseguir la llave física es seguramente la tarea más difícil, sobre todo en redes bien diseñadas. Con el fin de aprovechar el flujo de comunicación TCP/IP, un hacker debe ejecutar sus herramientas en una máquina que sea capaz de ver los paquetes transmitidos desde el cliente al servidor y viceversa. Una opción es ejecutar estas herramientas en la máquina cliente, y otra es ejecutar las herramientas en el Servidor de Base de Datos – en ambos casos las maquinas puede ver todo el flujo de la comunicación.

Implementar Opciones para Encriptación de Datos en Tránsito.

Puede elegir entre un buen número de opciones cuando se desea cifrar los datos en tránsito. En concreto las siguientes opciones que ofrecen una muestra de la amplia gama de técnicas:

* Características específicas de cifrado de la Base de datos (ejemplo, Oracle Advanced Security).
* Métodos de conexión de base (ejemplo, usar protocolo Secure Sockets Layer [SSL]).
* Garantizar los túneles (ejemplo, mediante el sistema Secure Shell [SSH] túneles o VPN).
* Basándose en paquetes seguros (ejemplo, el cifrado IPSec).