

Curso: (30227) Seguridad Informática

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas
Universidad de Zaragoza

<http://webdiis.unizar.es/~ftricas/>

<http://moodle.unizar.es/>

ftricas@unizar.es

Tema Seguridad y bases de datos

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas
Universidad de Zaragoza

<http://webdiis.unizar.es/~ftricas/>

<http://moodle.unizar.es/>
ftricas@unizar.es



Seguridad en bases de datos

- ▶ Los propios gestores no tienen en cuenta estos aspectos
- ▶ Las medidas adoptadas no son estándar entre distintos sistemas
- ▶ ¡Leer la documentación!
- ▶ Daremos algunas ideas



Los objetivos de un atacante

- ▶ Los propios datos (claro)



Los objetivos de un atacante

- ▶ Los propios datos (claro)
Pero también ...
- ▶ Cotas. Valores máximos o mínimos pueden proporcionar información interesante
- ▶ Existencia. Si existe un dato o no
- ▶ Resultados negativos. Cuando alguien (o algo) no tiene 'algo' también es información interesante.
- ▶ Valor probable

Hay que defenderse contra todas las posibilidades...

Tampoco se trata (como casi siempre) de cerrar toda la información para que no pase nada malo.



Nuestros objetivos

- ▶ Consistencia interna.
 - ▶ Los datos cumplen con las reglas establecidas (no hay precios negativos, ...)
- ▶ Consistencia externa
 - ▶ Los datos reflejan la realidad.



Reglas de integridad

Además de la integridad referencial y las tradicionales

- ▶ Comprobación de los valores de los campos: contienen valores 'razonables' y/o válidos
- ▶ Comprobación de ámbito adecuado (devolver valores sólo cuando el rango es suficientemente amplio).
- ▶ Comprobaciones de consistencia.
Ej.: en la factura algo vale X, y en la tarifa vale Y...

Puede haber conflictos entre estas comprobaciones y la confidencialidad (para comprobar algún valor hay que acceder a valores privados)



Empezando por lo básico

- ▶ La conexión con la base de datos no suele ser cifrada
 - ▶ En algunos casos como producto aparte
 - ▶ Podríamos usar SSL
 - ▶ ¿Otros?

Siempre se puede habilitar una red privada virtual (VPN)



Empezando por lo básico

Nuestra principal preocupación debería ser el daño que pueda realizar una entrada de datos maliciosa

- ▶ Todas (o casi todas) proporcionan autenticación mediante clave, y control de acceso a las tablas
- ▶ Sólo ofrecen protección contra el resto de usuarios de la base de datos



Control de acceso

En el DBMS

- ▶ Niveles de acceso
 - ▶ Manipulación de datos de las tablas básicas
 - ▶ Operaciones compuestas
- ▶ Podemos:
 - ▶ Restringir las operaciones basándonos en cada usuario
 - ▶ Definir los niveles de protección para cada tipo de dato
- ▶ En todo caso ...
 - ▶ Completitud (todos los campos están protegidos)
 - ▶ Consistencia (no hay incoherencias en las reglas)



Control de acceso

En el DBMS

- ▶ El objetivo es proteger a unos usuarios de los otros
- ▶ Cada usuario tiene sus tablas, y gestiona quién puede acceder a ellas.
- ▶ No es una solución escalable



Control de acceso

En el DBMS

- ▶ Generalmente:

- ▶ Usuarios

- Se autentifica con un proceso de entrada. A veces es suficiente con que el usuario se haya autenticado en el sistema operativo.

- ▶ Acciones (SELECT, INSERT, ...),

- ▶ Objetos (Tablas, otros...),

Los usuarios invocan acciones sobre los objetos. El DBMS decide si la acción está permitida o no.



Control de acceso

En el DBMS

- ▶ Privilegios (quién, qué, herencia, ... GRANT)
- ▶ Vistas (sólo puedes ver ...)
 - ▶ Tablas virtuales como filtro de las reales
 - ▶ Se podría crear una por cada tipo de usuario del sistema

```
CREATE VIEW          empleado_sencillo AS  
SELECT nombre, despacho, telefono,  
correo, fechaIngreso  
FROM info_empleado;
```

Tambien se pueden hacer cosas mas sofisticadas...



Control de acceso

En el programa

- ▶ Esto no ayuda con aplicaciones que tengan su propio sistema de usuarios
- ▶ En la práctica, los propios programas deben ocuparse del control de acceso a la base de datos
- ▶ Hay que ser muy cuidadosos con la información que se pueda deducir

¿Compartimentalizar?

Por ejemplo: varios perfiles de usuarios para la base de datos.



Control de acceso

Las vistas

- ▶ Son flexibles y permiten políticas de control de acceso definidas a un nivel próximo al de la aplicación
- ▶ Pueden servir para políticas de seguridad basadas en contexto o en los datos
- ▶ Invocación controlada
 - ▶ Las lecturas sin problemas
 - ▶ Las actualizaciones pueden tener problemas
- ▶ Los datos pueden ser reclasificados fácilmente



Control de acceso

Vistas. Desventajas

- ▶ La comprobación de acceso puede ser complicada y lenta
- ▶ Las vistas tienen que comprobarse desde el punto de vista de la corrección: ¿respetan la política de seguridad?
- ▶ Completitud y consistencia no se obtienen automáticamente.
- ▶ La parte relativa a la seguridad del DBMS se puede complicar mucho.



Control de acceso

Protección de campos

- ▶ Ni siquiera los que tienen acceso a la BD son siempre gente de confianza
 - ▶ Mejor proteger los datos delicados de su vista (criptografía)
 - ▶ Opciones propias
 - ▶ Campos PASSWORD
 - ▶ Mejor no fiarse: cifrar, codificar, almacenar, decodificar, descifrar ...
- Problemas: ¿y para buscar? ¿y las prestaciones? ¿y el espacio?



Ataques mediante análisis estadísticos

- ▶ Cuidado con el acceso que damos a nuestra base de datos
- ▶ Eliminar el acceso a datos delicados
- ▶ Por ejemplo, datos únicos

Ejemplo:

Si conozco a un cliente de Alfamén, de 72 años, y sólo hay uno con esas características, no importa que el nombre y la dirección no aparezcan.



Ataques mediante análisis estadísticos

- ▶ Una solución sería permitir sólo funciones agregadas (AVG, COUNT, MAX, MIN, SUM, ...)
- ▶ Pero se puede inferir información



Ataques mediante análisis estadísticos

Ejemplo

```
SELECT COUNT(*)  
  FROM clientes  
 WHERE ciudad = "Alfamen"  
    AND edad   = 72;
```

Si da 1 ...

```
SELECT AVG(sueldo)  
  FROM clientes  
 WHERE ciudad = "Alfamen"  
    AND edad   = 72;
```



Ataques mediante análisis estadísticos

- ▶ Restringir las peticiones por debajo de determinados números
- ▶ Cuidado (claro) con sus complementarias

```
SELECT AVG(sueldo)
  FROM clientes
 WHERE NOT (ciudad = "Alfamen"
           AND edad = 72);
```

Pero siempre se puede conseguir algo ...



Ataques mediante análisis estadísticos

```
SELECT COUNT(*)  
FROM clientes  
WHERE ciudad = "Calatayud"  
AND edad = 72:
```

Devuelve 100

```
SELECT AVG(sueldo)  
FROM clientes  
WHERE ciudad = "Calatayud"  
OR (ciudad = "Alfamen"  
AND edad = 72);
```

Y ya esta!

Como?



Ataques mediante análisis estadísticos

- ▶ Ataque directo. Si hay pocos datos, se calcula el agregado y se deducen datos.
- ▶ Ataque indirecto. Combinación de datos de diferentes agregaciones.
- ▶ Ataque mediante predicados trazadores

$$\begin{aligned}q &= \text{count}(a \text{ and } b \text{ and } c) = \\ &= \text{count}(a) - \text{count}(a \text{ and not}(b \text{ and } c)) = \\ &= \text{count}(a) - \text{count}(a \text{ and } (\text{not } b \text{ or not } c))\end{aligned}$$

- ▶ Fallos mediante sistemas lineales



Algunas defensas

- ▶ Los datos sensibles no deberían estar disponibles
- ▶ Auditar las preguntas de vez en cuando
- ▶ Modificar la base de datos de forma que no afecte al análisis estadístico
- ▶ Añadir ruido estadístico (no sistemáticamente)
- ▶ No hay soluciones suficientemente buenas
- ▶ Disparadores (*'Triggers'*)
- ▶ ¿El futuro?

'Information Commissioner's Office. Anonymisation'

<https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/>



Privacidad

“OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”

<http://www.oecd.org/sti/ieconomy/privacy.htm>

- ▶ Colección de datos limitada. Sólo los datos necesarios, con consentimiento, obtenidos legalmente...
- ▶ Datos de calidad. Relevantes, ajustados a la realidad, completos y al día
- ▶ Claramente especificado el uso de los datos
- ▶ Uso limitado. No se proporcionan a terceros sin permiso del usuario o de la ley
- ▶ Salvaguardado: niveles adecuados de protección y seguridad
- ▶ Principio de apertura. Debería ser fácil conocer qué datos se tienen de alguien, para qué se usan...
- ▶ Participación individual. La consecuencia del anterior: fácil eliminar los datos, corregirlos, ...
- ▶ Responsabilidad. El que tiene los datos es responsable del uso que se haga de ellos.

Cryptographic Storage Cheat Sheet

1 Introduction

1.1 Architectural Decision

2 Providing Cryptographic Functionality

2.1 Secure Cryptographic Storage Design

2.1.1 Rule - Only store sensitive data that you need

2.1.2 Rule - Use strong approved Authenticated Encryption

2.1.2.1 Rule - Use strong approved cryptographic algorithms

2.1.2.2 Rule - Use approved cryptographic modes

2.1.2.3 Rule - Use strong random numbers

2.1.2.4 Rule - Use Authenticated Encryption of data

2.1.3 Rule - Store the hashed and salted value of passwords

2.1.4 Rule - Ensure that the cryptographic protection remains secure even if access controls fail

2.1.5 Rule - Ensure that any secret key is protected from unauthorized access

2.1.5.1 Rule - Define a key lifecycle

2.1.5.2 Rule - Store unencrypted keys away from the encrypted data

2.1.5.3 Rule - Use independent keys when multiple keys are required

2.1.5.4 Rule - Protect keys in a key vault

2.1.5.5 Rule - Document concrete procedures for managing keys through the lifecycle

2.1.5.6 Rule - Build support for changing keys periodically

2.1.5.7 Rule - Document concrete procedures to handle a key compromise

2.1.5.8 Rule - Rekey data at least every one to three years

2.1.6 Rule - Follow applicable regulations on use of cryptography

2.1.6.1 Rule - Under PCI DSS requirement 3, you must protect cardholder data

3 Related Articles

4 Authors and Primary Editors

4.1 Other Cheatsheets

'OWASP Cryptographic Storage Cheat Sheet'

http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet



Departamento de
Informática e Ingeniería
de Sistemas

Universidad Zaragoza