Tema 9

Seguridad del comercio electrónico

Antonio Sanz – ansanz@unizar.es

Comercio Electrónico

Índice

- Certificados digitales
- Protocolo SSL
- Seguridad web

Certificados digitales

Certificados digitales

- Elemento vital de la seguridad de las comunicaciones actuales → criptografía de clave pública
- Bases de la criptografía de clave pública: DOS CLAVES
  - Clave pública: La puede (y debe) tener todo el mundo
  - Clave privada: Sólo la podemos tener nosotros (es la prueba de nuestra identidad)

Certificados digitales

Lo que se cifra con una clave SÓLO se puede descifrar con su pareja

Certificados digitales

- Gracias a la criptografía de clave pública es posible que dos entidades se intercambien su clave pública y puedan tener seguridad en las comunicaciones

- Seguridad = Confidencialidad + Autenticidad + Integridad

Certificados digitales

- Firmas digitales: Forma de tener autenticidad e integridad en una comunicación
- Se basan en las funciones hash o resumen → reducen un documento a una cadena de bits:
  - Esa ristra cambia si se cambia una coma del documento
  - A partir de la cadena no se puede saber nada del original

Certificados digitales

- Funcionamiento de la firma digital:

1. El emisor genera el hash del fichero, y lo firma con SU clave privada
2. El emisor cifra el fichero con la clave pública del destino y lo envía
3. El receptor descifra con su clave privada, obtiene el documento y calcula el hash del fichero recibido
4. El receptor verifica la firma del hash con la clave pública del emisor
5. Si son iguales → Documento OK

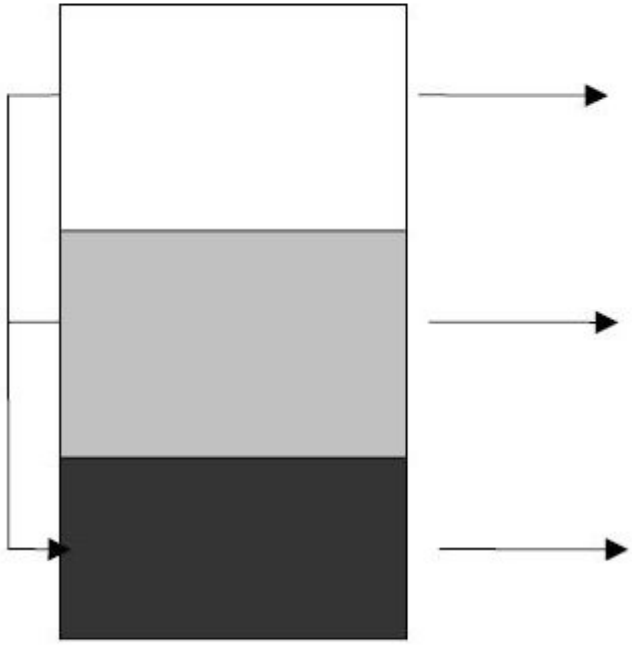
Certificados digitales

- Problemas de la criptografía de clave pública → Intercambio de claves
- ¿Qué sucede si yo me hago pasar por otra persona EN EL INTERCAMBIO DE CLAVES?
- Es necesario autenticar a las claves públicas de otras entidades → CERTIFICAR que son buenas

- Certificado digital

"Documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública"

Conceptos básicos



Información del usuario: Nombre, apellidos, email, DNI

Clave pública del usuario

Hash de los dos campos anteriores, cifrado con la clave privada K

Seguridad del comercio electrónico

Conceptos básicos

- Un certificado digital es un fichero que tiene el siguiente contenido:
  - Información del usuario → identificación unívoca
  - Información de la Autoridad de Certificación (AC)
  - Clave pública del usuario
- El certificado se crea haciendo un hash de la información y la clave pública, y firmándolo con la clave privada de la autoridad de certificación

Seguridad del comercio electrónico

Conceptos básicos


```
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBADANBgkqhkiG9w0BAQQFADBzMQswCQYDVQQGEwJFUzER
MA8GA1UECBMIWmFyYWdvemExETAPBgNVBAcTCFphcmFnb3phMQ0wCwYDVQQKEwRN
RUJBMRkwFwYDVQQLExBNRUJBIC0gU2VndXJpZGFkMRQwEgYDVQQDEwtDQSBkZWwg
TUVCQTAeFw0wNDA5MDcxNTE1MDVaFw0wNDEwMDcxNTE1MDVaMHMxCzAJBgNVBAYT
AkVTMREwDwYDVQQIEwhaYXJhZ296YTERMA8GA1UEBxMIWmFyYWdvemExDTALBgNV
BAoTBE1FQkExGTAXBgNVBAsTEE1FQkEgLSBTZWd1cmlkYWQxFDASBgNVBAMTC0NB
IGRlbCBNRUJBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPAjqamg
Q8TWK4gCBLLZouM0SlyVwf3iX/5YeteHJRBMOuYjiSUgj0apWcz4KPxbRvFOKgWK
ARfqgit2+RgjmNW4/IIQJZ3uSFPJcEP23h43GTGGhrX27mE5Vsgu5kilTemkjBS/
vz5w3ZhPgSkm/4I65AiKX3K8k2cIMmAWh0aYZlVZTUx61NipXC0VR6/dvkKVPTG/
yMC5V0DtxQmtb0/DLhOBbzdDOUCpZHUiw0Wyxu8KX4+Q7Zk7LIr+Cff1NRy7BCRR
6u8F+db+oXSY8aW1Tjj6ARZjvs7Awcv01i8ey01kYc67c+tpe892/vcTrj8Vc16V
PTQqR25tZ88jHQIDAQABo4HQMIHNMB0GA1UdDgQWBBRsCX0mv8n6SkM1AHLHJngf
AS2tizCBnQYDVR0jBIGVMIGSgBRsCX0mv8n6SkM1AHLHJngfAS2ti6F3pHUwczEL
MAkGA1UEBhMCRVMxETAPBgNVBAgTCFphcmFnb3phMREwDwYDVQQHEwhaYXJhZ296
YTENMAsGA1UEChMETUVCQTEZMBcGA1UECxMQTUVCQSAtIFNlZ3VyaWRhZDEUMBIG
A1UEAxMLQ0EgZGVsIE1FQkGCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQF
AAOCAQEATuPi612ubGPoYpM5gDIstXWEAc6b/mgYZciIb+8NpMThtBgiPsj8T/r/
EHevSeIUTWiDhJ1v7l0aIBNshUJd5E6LsLbrTkNEH01XGahtmso4zic/uAAASzfX
VKgPYF/NnWtulgCw5JKBSTGAJMlQ5/9xbn8bs53pTzUYxyYMkIow1JyyXecdES4v
+LJuHy1msGjyDg5c4q0xolWrmQrLFociqD/zQY7Sqn7lWNZ3aXDH6+say4Wudpac
EWPxkwb67QrIM73cCA5rxB/jFCmj5V5A4ynrLm83g7TQNrFqcDO/TOiZjnf3+aCb
zn4lvpXeRaQZj3tlsghrctBKZRzpLA==
-----END CERTIFICATE-----
```


Certificados digitales

- Los certificados digitales se pueden aplicar a personas y a entidades → Servidores web

- Es perfectamente factible generar un certificado digital para un servidor web → Poder autenticar al servidor y establecer comunicaciones seguras

Certificados digitales

- Ciclo de vida de un certificado digital:
  - Solicitud
  - Generación
  - Uso
  - Expiración/Revocación

Certificados digitales

- Solicitud:
  - Se genera una petición de certificado (Certificate Signing Request)
  - Esta CSR tiene la información del servidor y la clave pública (NUNCA la privada)
  - Tiene que tener información que lo identifique UNÍVOCAMENTE → Nombre DNS
  - Se envía a la Autoridad de Certificación (AC)

Certificados digitales

- Generación:
  - La AC autentica a los dueños del servidor (documentación acreditativa)
  - Se genera el hash firmado y se suma a los datos enviados = Certificado
  - Se envía al cliente (los certificados tipo DNI electrónico tienen su propio medio)

Certificados digitales

Uso:

- Se instala el certificado en el servidor
- Se usa para dar seguridad en las comunicaciones mediante SSL
- Todos los certificados se expiden por una duración (de 1 a 5 años)
- Importante: 1 certificado = 1 nombre de dominio (misitio.com NO es www.misitio.com)

Certificados digitales

- Expiración/Revocación :
  - Expiración: El certificado deja de poder ser usado → Hay que renovarlo
  - Revocación: La clave privada ha sido comprometida → Hay que REVOCAR (quitar validez) el certificado para que nadie pueda usarlo en nuestra contra

Certificados digitales

- Usos prácticos de los certificados digitales:
  - SSL → Seguridad en las comunicaciones
  - Firma electrónica → Autenticidad e integridad de documentos
  - DNI Electrónico, Factura Electrónica, Receta Electrónica → Pieza clave de la Administración Electrónica

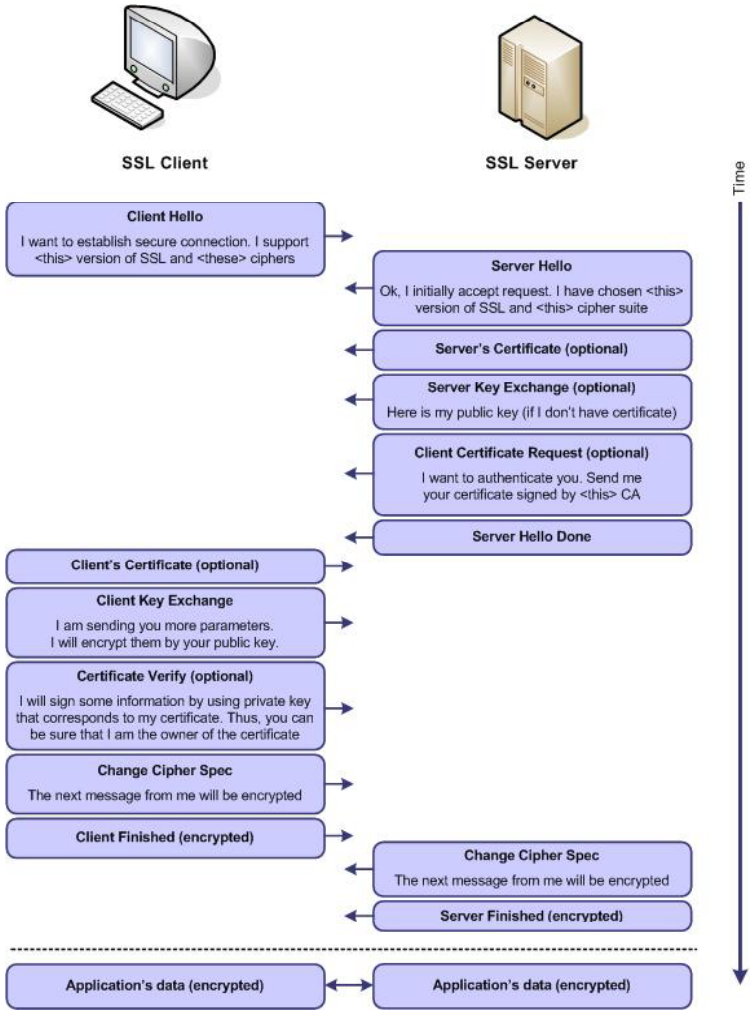
SSL/TLS

SSL/TLS

- Secure Socket Layer o Transport Layer Security
- Proporciona a una comunicación:
  - Confidencialidad
  - Integridad
  - Autenticidad de servidor (y en algunos casos, de cliente)
- Protocolo base de la seguridad en el comercio electrónico
- Desventaja: Costoso en recursos

Seguridad del comercio electrónico

SSL/TLS



Ejemplo: Comunicación mediante SSL

SSL/TLS

- Ejemplo de una conexión:
  - Se inicia la conexión segura
  - El cliente exige al servidor el certificado digital, que este envía junto con un identificador (ID) de sesión
  - El cliente verifica el certificado y envía sus preferencias de cifrado (y su certificado, en caso de que lo exija el servidor), junto con una clave de sesión cifrada con la claves públicas del servidor

SSL/TLS

- El servidor verifica el certificado del cliente (si procede), y comprueba las peticiones de cifrado. Descifra la clave de sesión y acepta las preferencias del cliente.
- Se establece la conexión cifrada con la clave de sesión.

Seguridad web

Seguridad web

- Arquitecturas web
- Ataques al servidor web
- Ataques a las aplicaciones
- Medidas de seguridad

Seguridad del comercio electrónico

Seguridad web

- Arquitecturas web: El cliente se conecta a un servidor para realizar su trabajo
- Programación web muy sencilla
- Independiza el tipo de cliente que empleemos
- Permite escalabilidad y centralización de la aplicación
- Problema: Seguridad

Seguridad web

- Aplicaciones web → Cliente/Servidor

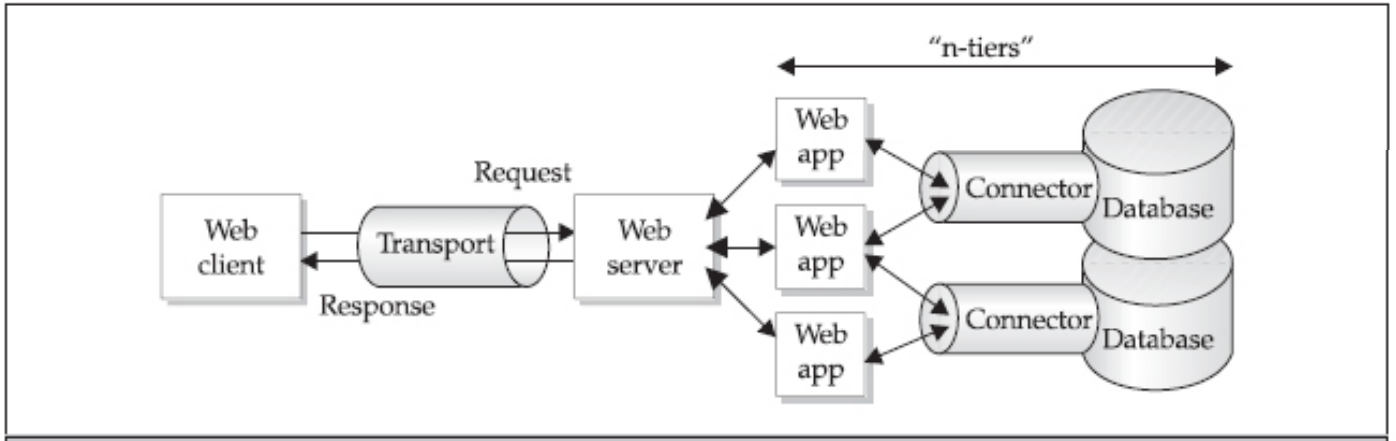


Figure 1-1. The end-to-end components of a typical Web application architecture

Seguridad web

- Puntos de ataque:
  - Cliente
  - Conexión
  - Servidor web
  - Aplicación web
  - Base de datos

Seguridad del comercio electrónico

Seguridad web

- Todos aquellos que puedan realizarse sobre un sistema operativo
- Troyanización → Más común en entorno web (conseguir autenticación del usuario mediante un keylogger)
- Robo de cookies (autenticación)
- DNS spoofing & Man in the middle también muy frecuentes

Seguridad del comercio electrónico

Seguridad web

- Securizar los equipos cliente (actualizaciones, antivirus, cortafuegos personal)
- Emplear certificados digitales para autenticar el servidor
- Poner tiempos de expiración de cookies agresivos (5 minutos máximo)
- Problema grave (poco se puede hacer desde nuestro lado)

Seguridad del comercio electrónico

Seguridad web

- Ataques de sniffing contra la autenticación, o de manipulación de la misma (cambiar las fotos de un producto)
- Ataques de DoS
- Solución: Emplear SSL para asegurar la comunicación y escalar el sitio web para hacerlo robusto frente a ataques DoS

Seguridad web

- Ataques a la versión del servidor (falta de parches/actualizaciones)
- Configuración incorrecta del servidor
- Fallos de otros servicios del equipo (o del propio sistema operativo)
- Ataque a los sistemas de administración del servidor (son otra aplicación web ¡¡contraseñas por defecto!!)
- Herramientas automatizadas: Whisker & Nikto

Seguridad del comercio electrónico

Seguridad web

- Actualización del servidor y de todos los servicios asociados (sistema operativo incluido)
- Leer la documentación y configurarlo de forma óptima
- Emplear cortafuegos para controlar el acceso al servidor
- Usar Nikto & Whisker antes que otros lo hagan…

Seguridad web

- Desarrollo de aplicaciones web → Mantener una metodología de programación segura
- Application web → Muy expuesta al exterior (cuidar las medidas de seguridad)

Seguridad del comercio electrónico

Seguridad web

- Usar JavaScript para validar datos (Ejemplo: comprobar que el campo e-mail está completo)
- Problema: El intruso puede descargar el código, modificarlo y lanzar el ataque evitando esa validación
- Solución: Realizar la validación SIEMPRE en el lado del servidor

Seguridad del comercio electrónico

Seguridad web

- Modificación de campos “hidden” → Usados en formularios para guardar información
- Problema: Un intruso puede cambiar un campo “role” de “user” a “admin”
- Solución: Validar también los campos ocultos (en realidad … ¡¡TODO!!)

Seguridad del comercio electrónico

Seguridad web

- Ataques de fuerza bruta a la autenticación → Similares al sistema operativo
- No hace falta tener los hashes... pero son mucho más lentos
- Ejemplo: Emplear Brutus para web-cracking
- Solución: Contraseñas robustas + mecanismos de detección de acceso reiterativo

Seguridad del comercio electrónico

Seguridad web

- Sesiones web: Identificadores que marcan en cada web el estado de una aplicación (estado de compra, permisos disponibles, etc ...)
- Si un intruso puede “adivinarlos”, puede “secuestrar” una conexión
- Solución: Usar SSL, generarlos de forma aleatoria, darles tiempos de expiración cortos

Seguridad del comercio electrónico

Seguridad web

- Cross Site Scripting: Un intruso puede introducir código malicioso en un foro, correo... que sea ejecutado cuando el cliente lo abra
- Problema: Captura de cookies, otra info
- Solución: Validación de las entradas (filtrado de HTML “peligroso”)

Seguridad web

- Inyección SQL: Ataque a la base de datos a través de la aplicación web (manipulando los datos de entrada y “concatenando” consultas)

- Problema: Permite a un intruso ejecutar SQL en nuestra BD → Falsear la autenticación, obtener información ...

Seguridad web

Ejemplo: Código que ejecuta esta consulta:

```
SELECT * FROM Users WHERE Username=
  '$username' AND Password='$password'
```

El intruso hace que :

```
$username = 1' or '1' = '1
$password = 1' or '1' = '1
```

Por lo que la consulta final es:

```
SELECT * FROM Users WHERE Username= '1'
  OR '1' = '1' AND Password= '1' OR '1' = '1'
```

Resultado: ¡¡¡Acceso libre a la aplicación!!!!

Seguridad web

Ejemplo: Código que ejecuta esta consulta:

SELECT *fieldlist* FROM *table* WHERE *field* = '$EMAIL';

El intruso hace que :

$email = x'; DROP TABLE members; --

Por lo que la consulta final es:

SELECT email, passwd, login_id, full_name
FROM members WHERE email = 'x'; DROP
TABLE members; --';

Resultado: ¡¡¡¡Una tabla menos!!!!

Seguridad web

- Solución: Validación inicial de todos los datos que entran al servidor
- Solución dos: Emplear funciones que “escapen” los caracteres extraños
- Extras: Usar “stored procedures” y separación de privilegios

Seguridad del comercio electrónico

Seguridad web

- Intercepción/manipulación de la comunicación
- Ataques desde IP ajenas al servidor web
- Ataques para obtener información de otras bases de datos (information leaks)

Seguridad del comercio electrónico

Seguridad web

- Usar SSL para comunicación entre los servidores web y los de bases de datos (cuidado con el rendimiento)
- Restringir el acceso a la bases de datos
- Separar roles de usuarios y permisos por bases de datos
- Emplear cifrado

Seguridad del comercio electrónico

Conclusiones

- Entornos web → Cada día más empleados
- Importante garantizar la seguridad de la comunicación (cliente, red y servidor)
- Programación segura de aplicaciones web → Aspecto vital

Seguridad del comercio electrónico

SEGURO que hay alguna duda...