



Técnicas de control de acceso en servidores web

Gonzalo Álvarez Marañón

CSIC



Agenda

- ◆ Qué es el control de acceso
- ◆ Acceso anónimo
- ◆ Autenticación básica
- ◆ Autenticación de Windows integrada
- ◆ Autenticación a nivel de aplicación
- ◆ Autenticación mediante certificados digitales



Qué es el control de acceso

- ◆ Proteger la entrada a un web completo o sólo a parte:
 - *Autenticación*: identifica al usuario o a la máquina que trata de acceder a los recursos
 - *Autorización*: dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos



Métodos de autenticación

- ◆ Algo que tú sabes
 - Nombre de usuario y contraseña
- ◆ Algo que tú tienes
 - Certificados X.509 en el ordenador o en tarjetas inteligentes
- ◆ Algo que tú eres
 - Escáner de huellas o de retina



Algo que tú sabes

◆ Ventajas

- Almacenamiento barato
- Fácil de gestionar y desplegar
- Implantado en la mayoría de sistemas

◆ Inconvenientes

- Secreto de tamaño reducido
- Debe introducirse manualmente
- Inseguro, malas contraseñas, etc.



Algo que tú tienes

◆ Ventajas

- Prueban la identidad
- Aseguran transacciones
- Windows 2000 soporta tarjetas

◆ Inconvenientes

- Almacenados en el ordenador carecen de valor
- Apenas hay lectores de tarjetas y son incompatibles



Algo que tú eres

◆ Ventajas

- Identificación del usuario

◆ Inconvenientes

- Si se comprometen, hay que cambiarlos todos
- No suelen ser muy fiables
- Uso en LAN, no en WWW



Autenticación anónima

- ◆ Forma de acceso por defecto
- ◆ El usuario anónimo pertenece al grupo *Invitados* y tiene asignada la cuenta *IUSR_nombremáquina*
- ◆ IIS suplantarán esta cuenta antes de ejecutar cualquier código o acceder a cualquiera de los archivos
- ◆ Pueden crearse otras cuentas anónimas



Control por dirección IP, nombre de host o dominio

- ◆ Recursos accesibles exclusivamente por ordenadores que posean determinada dirección IP, cierto nombre de host o pertenezcan a un dominio dado
- ◆ Se aplican una serie de reglas sencillas
 - Permitir a todos menos a unos cuantos
 - Denegar a todos menos a unos cuantos



Cuándo usarla

- ◆ Siempre que se piense utilizar otro ordenador desde el cual realizar tareas de administración remotamente
- ◆ Sólo como medida adicional de seguridad, combinándolo con alguno de los otros métodos



Ventajas de este método

- ◆ Resulta muy fácil de configurar y de mantener
- ◆ No necesita participación activa de los usuarios



Desventajas de este método

- ◆ Resulta poco flexible, ya que no permite acceso a usuarios con direcciones IP distintas
- ◆ No comprueba la identidad de un individuo, sino de una máquina
- ◆ Puede entrarse a una máquina y desde ella acceder al servicio protegido



Control por nombre y contraseña

- ◆ La forma más extendida
- ◆ Los tipos más comunes:
 - Autenticación básica
 - Autenticación mediante resúmenes
 - Autenticación de Windows integrada



Autenticación básica

- ◆ El navegador presenta al usuario la ventana de autenticación
- ◆ El navegador intenta establecer una conexión con el servidor
- ◆ Si el servidor rechaza la información de autenticación, el navegador le presenta nuevamente la ventana al usuario
- ◆ Se establece la conexión de acceso al recurso protegido



Desventajas de este método

- ◆ Las contraseñas se transmiten en claro
- ◆ Los usuarios pueden revelar sus contraseñas a otras personas
- ◆ Los usuarios suelen perder u olvidar sus contraseñas
- ◆ Los usuarios no suelen elegir contraseñas especialmente robustas
- ◆ Los usuarios tienen la fea costumbre de apuntarlas en cualquier sitio



Autenticación mediante resúmenes

- ◆ Enviar un resumen criptográfico de la contraseña (un *hash*) en vez de la propia contraseña:
 1. El servidor envía al navegador cierta información que será utilizada en el proceso de autenticación
 2. El navegador añade esta información a su nombre de usuario y contraseña, junto con otra información adicional, y crea un resumen del conjunto



Autenticación mediante resúmenes

3. Se envía en claro al servidor tanto el resumen como la información adicional
4. El servidor añade esta información adicional a una copia en claro de la contraseña del cliente y crea el resumen del conjunto
5. El servidor compara el resumen que ha creado con el que le ha llegado
6. Si ambos números coinciden, se le concede acceso al usuario



Ventajas de este método

- ◆ Incorporado al estándar HTTP 1.1
- ◆ No transmite las contraseñas a través de Internet, ni siquiera cifradas



Desventajas de este método

- ◆ Sólo está soportado en IE
- ◆ El servidor debe estar en un dominio de directorio activo
- ◆ En NT, las contraseñas en claro son un blanco fácil de ataques, por lo que deberían extremarse las medidas de seguridad para proteger al controlador de ataques físicos y de red



Autenticación de Windows integrada

- ◆ Nuevo nombre para la anterior “desafío/respuesta”
- ◆ Variante de la autenticación mediante resúmenes criptográficos, pero negociando NTLM o Kerberos
- ◆ El navegador tiene que demostrarle al servidor que conoce la clave por medio de un corto intercambio de datos



Proceso de la autenticación

- ◆ No se le presenta al usuario una ventana de autenticación, sino que se utiliza la información de la sesión abierta por el ordenador del cliente
- ◆ Si falla, entonces se le presenta al usuario la ventana de identificación
- ◆ Si falla, se le presenta esta ventana repetidamente



Ventajas de este método

- ◆ No transmite las contraseñas en claro a través de Internet



Desventajas de este método

- ◆ Sólo está soportado por IE, versión 2.0 o posterior y servidores NT
- ◆ No funciona para conexiones con proxy



Permisos web

- ◆ Lectura
- ◆ Escritura
- ◆ Acceso al código fuente
- ◆ Examinar directorios
- ◆ Registrar visitas
- ◆ Indizar este recurso



Permisos de ejecución

- ◆ Ninguno
- ◆ Sólo secuencias de comandos
- ◆ Secuencias de comandos y ejecutables



Permisos NTFS

- ◆ Control total
- ◆ Modificar
- ◆ Lectura y ejecución
- ◆ Leer
- ◆ Escribir



Autenticación a nivel de aplicación

- ◆ Tabla con los nombres de usuario y sus contraseñas
- ◆ `strSQL = "SELECT IdUsuario " _ &"FROM Users " _ &"WHERE login ="&login&" AND password = "&password&""`
- ◆ Si las credenciales son válidas, se recupera el ID del usuario y se le permite acceder al recurso/servicio



Limitaciones

- ◆ Ataques de SQL
- ◆ Contraseñas en claro en la BD
- ◆ Ataques de diccionario
- ◆ Credenciales sólo en la página de entrada:
¿y el resto?



Variables de sesión

- ◆ Utilizar una variable de sesión de ASP
- ◆ Ventajas:
 - ASP gestiona el mantenimiento de la variable
 - Se puede hacer caducar al cabo de un tiempo variable
 - Ámbito de sesión: caducan al cerrar el navegador



Tickets de sesión

- ◆ Incluyen la siguiente información:
 - Número aleatorio
 - Estampilla de tiempo
 - Nombre de usuario
 - Contraseña de usuario
 - ¿IP?

Nonce : Estampilla : Hex (Hash (Nonce
: Estampilla : Usr : Pwd))



Canales seguros con SSL

- ◆ SSL: protocolo para dotar de seguridad a las sesiones de navegación a través de Internet
- ◆ Creado en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator
- ◆ Con SSL v3.0 alcanzó su madurez



Servicios de seguridad de SSL

- ◆ Confidencialidad: cifrado de datos
- ◆ Integridad de mensajes
- ◆ Autenticación de servidores
- ◆ Autenticación de cliente (opcional)



Funcionamiento de SSL

- ◆ Algoritmos de cifrado simétrico:
 - DES, 3DES, RC2, RC4, IDEA
- ◆ Algoritmos de clave pública:
 - RSA
- ◆ Algoritmos de resumen
 - MD5, SHA
- ◆ Certificados
 - DSS, RSA
- ◆ Clave de sesión distinta en cada transacción



Fases del protocolo SSL

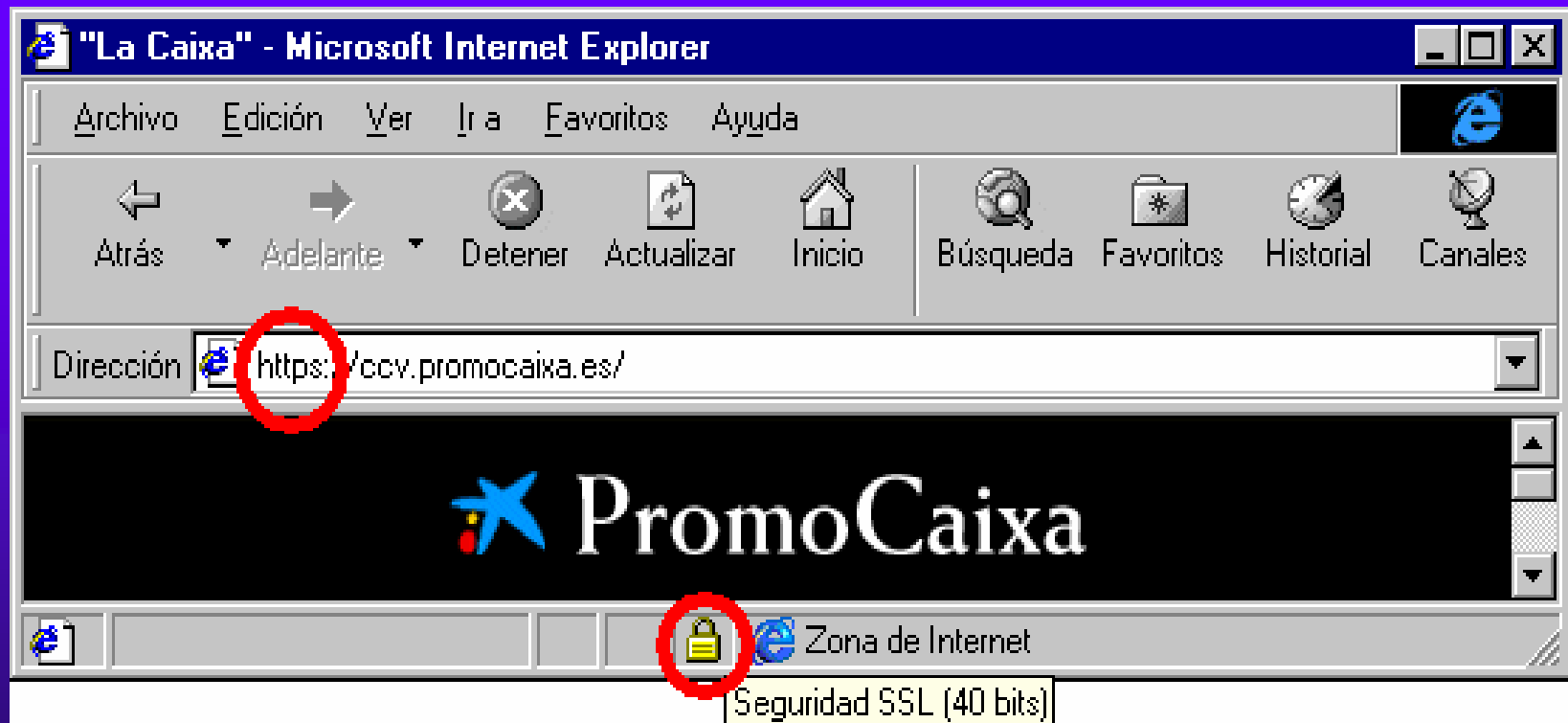
- ◆ **Fase hola:** acordar los algoritmos a usar
- ◆ **Fase autenticación:** intercambio de certificados X.509v3
- ◆ **Fase clave sesión:** se crea la clave de sesión para cifrar la comunicación
- ◆ **Fase fin:** verificación del canal seguro
- ◆ A partir de ahí, comunicación segura



Cómo utilizar SSL con el navegador

- ◆ Ninguna acción especial para invocarlo
- ◆ Asegurarse de que está habilitado:
 - Internet Explorer: Herramientas • Opciones de Internet • Opciones avanzadas • Seguridad

Cómo saber si una página es segura



Alerta de seguridad



Alerta de seguridad



La información que intercambie con este sitio no puede ser vista o cambiada por otros. No obstante, existe un problema con el certificado de seguridad del sitio.



El certificado de seguridad fue emitido por una organización en la que usted no ha depositado su confianza. Vea el certificado para determinar si desea confiar en la entidad.



El certificado de seguridad es válido.



El certificado de seguridad coincide con la página que desea ver.

¿Desea continuar?

Sí

No

Ver certificado



Servidores seguros

- ◆ SSL no es sinónimo de seguridad:
 - Agujeros en guiones CGI, ASP, ISAPI, etc.
 - Páginas mal diseñadas que permiten acceder a cuentas de otros usuarios
 - Ficheros confidenciales accesibles a través de web
 - Servidor con muchos agujeros de seguridad



SSL y comercio electrónico

- ◆ Servidor web con catálogo de productos
- ◆ Junto a los artículos, botón de carrito
- ◆ Se paga todo al final
- ◆ Se rellena un formulario con datos personales e información de pago
- ◆ El comerciante gestiona manualmente las compras



Limitaciones comerciales de SSL

- ◆ SSL ofrece canal seguro, pero carece de proceso financiero
- ◆ SSL garantiza confidencialidad en tránsito, no en el servidor
- ◆ SSL permite ataques para averiguar números de tarjeta reales
- ◆ Debilidad criptográfica: 40 bits de clave (excepto aplicaciones financieras)



Control por certificados

- ◆ Los clientes se identifican mediante la presentación de un certificado
- ◆ Contienen información como su nombre, empresa, departamento, dirección de correo, ciudad, país, etc.
- ◆ Permite sofisticados esquemas de control de acceso basándose en uno de estos atributos o en una combinación de varios o en el conjunto del certificado



Cómo funcionan

- ◆ El usuario instala el certificado en su navegador
- ◆ Sólo tiene que presentarlo para que se produzca la autenticación
- ◆ Pueden almacenarse localmente en el disco duro o en una tarjeta inteligente
- ◆ Están además protegidos por una contraseña



Correspondencias de certificados y cuentas

- ◆ Uno a uno: se puede hacer corresponder uno o varios certificados individuales a cada cuenta
- ◆ Muchos a uno: utilizan reglas de ajuste basándose en la información contenida en los distintos atributos de los certificados, aceptándose todos los certificados de cliente que verifiquen ciertas reglas



Ventajas de este método

- ◆ Permiten autenticarse en muchos servidores distintos
- ◆ Son fáciles de escalar
- ◆ Permiten descentralizar la verificación de permisos de acceso



Desventajas de este método (I)

- ◆ ¿Quién emite los certificados?
 - ¿Entidad externa o la propia empresa?
- ◆ ¿Qué confianza proporciona un certificado?
 - Robustez de los algoritmos criptográficos
 - Procedimientos de certificación fiables
 - Seguridad de la clave privada del usuario
 - Seguridad de la clave privada de la CA



Desventajas de este método (II)

- ◆ TALÓN DE AQUILES: Es fácil emitir certificados, pero difícil revocarlos: CRL
- ◆ Pueden resultar una pesadilla por su complejidad:
 - Olvido de la clave que protege el certificado
 - Borrado involuntario
 - Robo del ordenador
 - Compartido con otros usuarios



Conclusiones

- ◆ Existen distintas formas de autenticación según las necesidades
- ◆ La más segura y flexible es la autenticación mediante certificados
- ◆ La más utilizada es la autenticación a nivel de aplicación
- ◆ Ninguna es la mejor, cualquiera es buena si está bien implantada, depende de la situación



Contacto

- ◆ Email:

- gonzalo@iec.csic.es

- ◆ Web:

- www.iec.csic.es/cryptonomicon