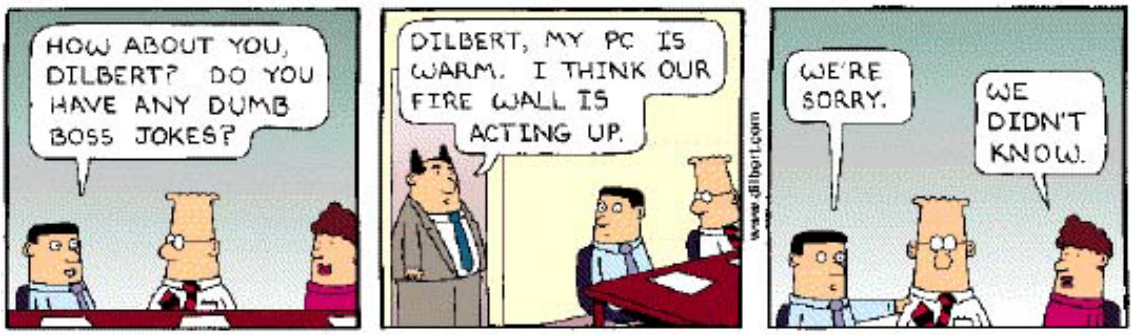
Comercio Electrónico

Práctica 7: Seguridad en las comunicaciones



José Luis Salazar
jsalazar@unizar.es

Antonio Sanz
ansanz@unizar.es

Rafael del Hoyo
rdelhoyo@ita.es

Objetivo de la práctica

Poner en práctica algunos de los conceptos vistos en la teoría relativos a la seguridad de nuestra infraestructura de comercio electrónico. Se instalará un certificado digital para poder activar el protocolo SSL en nuestro servidor, y se verán de forma práctica varios aspectos de la programación segura de aplicaciones web.

¿Qué hay preparar de forma previa a la práctica?

Será necesario el revisar y tener frescos todos los conocimientos adquiridos en la teoría, así como haber repasado los conceptos relacionados con la firma digital.

¿Cuál es el resultado de la práctica?

Se obtiene como resultado de la práctica una infraestructura de clave pública necesaria para establecer confianza entre los usuarios de comunicaciones digitales.

¿Qué se aprende con esta práctica?

Se aprende a realizar todo el proceso de adquisición e instalación de un certificado digital para poder activar SSL en nuestro servidor web.

Introducción

Una vez realizado por completo el despliegue de los servicios existentes en nuestro proyecto de comercio electrónico, se procede a añadir la capa de seguridad al conjunto (por motivos de duración de la práctica se hace de forma separada, pero es muy importante tener en cuenta que la seguridad es un requisito de desarrollo, que tiene que ser tenido en cuenta en la fase de diseño como parte vital del todo).

La capa de seguridad va a ser añadida mediante SSL (Secure Socket Layer), un protocolo que aprovecha las ventajas de la criptografía de clave pública para ofrecer confidencialidad, integridad y autenticidad en entornos web.

Configuración de SSL en el servidor web

Para poder activar el protocolo SSL dentro de nuestro servidor web es necesario seguir estos pasos:

- Escoger un PSC (Proveedor de Servicios de Certificación).
- Generar una petición de firma de certificado (Certificate Signing Request) en el formato requerido por el PSC.
- Enviar tanto la CSR como los documentos acreditativos necesarios al PSC.
- Recibir e instalar el certificado definitivo.

Nosotros no vamos a proceder de tal manera, pero vamos a simular el proceso. Para ello necesitamos:

- Descargar la interfaz de creación de certificados XCA (http://criptosec.unizar.es/soft/setup_xca-0.6.4.exe). La instalación no ofrecerá ningún problema.
- Siempre que tratemos de conectarnos con un navegador al servidor web y nos dé un error, haremos la corrección correspondiente, cerraremos el navegador y si es necesario, reiniciaremos el servidor.

Generación de PSC

Dado que la práctica la realizaremos en Windows y generaremos certificados compatibles tanto con Firefox como con Explorer debemos configurar la aplicación XCA para que utilice por defecto la función Hash SHA-1, desde el menú FILE.

A continuación procederemos a generar una CA que será usada para emitir certificados empleados en la práctica. Para ello emplearemos la aplicación XCA. Empezaremos creando una base de datos de claves tanto secretas como públicas, protegiéndola con un password.

Después, procederemos a la creación de un certificado raíz, donde el firmante y el suscriptor sean la misma entidad en la pestaña Certificates, no olvidando seleccionar CA como plantilla de certificado.

Se nos pedirá una serie de datos para generar el certificado, que pueden ser los siguientes:

CN (Country Name): ES
State or Province: Zaragoza
Locality Name: Zaragoza
Organization Name: Universidad de Zaragoza //(Nombre de la propietaria de la CA)
Organizational Name: Dep.. Tecnico
Common Name: El nombre por el que se va a conocer al CA.
Email Address: Mail para contacto con los dueños de la CA

Generación del certificado de servidor

Para generar un certificado digital para nuestro servidor, en primer lugar será necesario crear una petición de firma de certificado (CSR o Certificate Signing Request) que luego firmaremos con el certificado de la CA que creamos en el apartado anterior. No nos olvidemos de seleccionar correctamente la plantilla de certificado de servidor.

CN (Country Name): ES
State or Province: Zaragoza
Locality Name: Zaragoza
Organization Name: XXX //(Nombre de la entidad)
Organizational Unit: YYY
Common Name: www.www.es (URL de la entidad)
Email Address: Mail para contacto de la entidad

Common Name: El nombre del dominio de nuestra página (es VITAL ponerlo de forma correcta o de lo contrario nuestro certificado no funcionará de forma correcta). Los campos que aparecen como "Extras" o "Empresas adicionales" no nos interesan.

Instalación del certificado de servidor

La instalación del certificado de servidor seguro requiere de la modificación del fichero de configuración de SSL. Dicho fichero puede o bien estar incluido dentro del *httpd.conf* o conformar un fichero propio denominado *httpd-ssl.conf* (ambos dentro del directorio %XAMPP%\apache\conf\extra).

Se deberán cambiar las siguientes opciones de configuración:

SSLCertificateFile conf/ssl.crt/Cert_Server.crt
SSLCertificateKeyFile conf/ssl.key/Clave_Server.pem

Desde XCA se exportarán el certificado de servidor y las claves asociadas al mismo a los directorios recién especificados en los fichero de configuración (muy importante el respetar los *path* adecuados).

Si se para y se vuelve a iniciar el servidor web se recogerán los cambios y, al acceder por SSL (https://localhost), se podrá ver los detalles del servidor.

En el caso de que la interface gráfica del XAMPP no nos arranque el Apache (señal obvia de que existe un error), podemos arrancarlo desde línea de comandos abriendo un shell y accediendo a D:\xamppN\xampp\ y tecleando "apache_start" (de esta forma si tenemos un error de sintaxis en la configuración aparecerá indicado). Si este comando no nos da información, la otra fuente donde obtener más datos es el fichero de errores de Apache, situado en D:\xamppN\xampp\apache\logs\error.txt.

Se podrá observar que nos informa de dos irregularidades: En primer lugar, no se puede verificar el certificado porque el navegador no tiene instalado el certificado de la CA, y en segundo lugar porque el nombre escrito en el navegador no coincide con el del certificado. El segundo problema tiene difícil solución en este momento (tendríamos que tener un servidor de DNS para poder incluir nuestra correlación IP / nombre de dominio), pero el primero puede solucionarse instalando el certificado de la CA en el navegador.

Instalación del certificado de la CA en el navegador

Para instalar el certificado de la CA en el navegador, será necesario exportar el certificado de la CA (con el nombre Cert_CA.crt al fichero de trabajo y seguir los pasos que se detallan a continuación:

Internet Explorer

Acceder a *Herramientas → Opciones de Internet → Contenido → Certificados*. Seleccionar la pestaña de "Entidades emisoras de certificados de raíz de confianza",

y pulsar sobre "Importar". Seleccionar el fichero Cert_CA.crt (será necesario indicar que muestre todos los ficheros) e importarlo.

Acto seguido aparecerá en la lista junto con las otras CA de las que se tiene reconocimiento automático por parte del navegador.

Mozilla Firefox

Acceder a *Herramientas → Opciones → Avanzado → Certificados → Ver certificados → Autoridades*, y pulsar sobre la pestaña de "Importar", e importar el certificado directamente

Acto seguido aparecerá en la lista junto con las otras CA de las que se tiene reconocimiento automático por parte del navegador.

Trabajo a realizar durante la práctica

Se entregarán como resultado de la práctica los siguientes ficheros que serán enviados como adjuntos a la dirección de correo 512961@unizar.es:

- Los dos certificados generados en la sesión.
- Copia de los ficheros modificados sobre la configuración de Apache para su correcto funcionamiento.