Índice general

Enunciado

Se trata de configurar el servidor Apache para trabajar con el protocolo https (http seguro), que proporciona comunicaciones cifradas e identificación segura de los servidores de páginas web. Se utiliza en entidades que requieran el envío de datos personales o sensibles como contraseñas.

https no es un protocolo propiamente dicho, sino que es la conjunción de http en el nivel de aplicación sobre una capa de transporte segura (protocolo TLS), heredero de SSL.

La solución es obtener un certificado digital de sitio y servir las peticiones desde un puerto seguro (443 es el número de puerto por defecto en https) en vez de hacerlo en el puerto 80 (número de puerto por defecto en http). El tráfico a través de dicho puerto seguirá el estándar TLS (Transport Layer Security).

Para ello hay que configurar el Servidor de páginas web. Si queremos que nuestro servidor web acepte conexiones HTTPS, debemos disponer de un Certificado de clave pública para el sitio (servidor) web. Todos los certificados están firmados por una Autoridad de certificación. La autoridad certifica una clave pública a quien tiene los derechos de uso del sitio. En la instalación por defecto de los navegadores web incorporan en el almacén que usen los certificados raíz de buena parte de las Autoridades de Certificación comerciales. Por eso se pueden usar para verificar certificados firmados por dichas autoridades.

Adquirir un certificado de una autoridad puede ser gratuito (si la autoridad es una institución de titularidad pública como la FMNT), o tener un coste si es emitido por empresas como Verisign.

La tercera alternativa es que una organización tenga su propia autoridad de certificación. La organización puede distribuir copias del certificado raíz autofirmado, para que los usuarios los añadan a los almacenes de certificados de Autoridades de confianza que use el navegador.

Ese sistema también puede ser usado para la Autenticación de usuarios que accedan al sitio con el objetivo de limitar el acceso a un servidor web a usuarios autorizados. Para ello, el administrador del sitio crea un certificado personal de usuario, que éste deberá tener incorporado al almacén de su navegador. Ese certificado contiene la identificación del usuario (habitualmente en el campo CN o E) junto con otros datos que son usados en el protocolo de conexión al sitio

para verificar la identidad del usuario, como mecanismo alternativo al uso de nombres de usuario y contraseña.

La práctica consistirá en que el alumno cree una Autoridad de Certificación, certificado(s) de sitio y personales haciendo uso de la herramienta openssl. Y posteriormente configure el tanto el servidor de páginas como el navegador para que soporten el protocolo https sin que aparezcan mensajes de alerta de seguridad. Para ello tendrá que:

- Autoridad de Certificación. Generar un par de claves RSA (pública y privada) de longitud 2048 y un certificado X.509 de clave pública para la Autoridad de Certificación. Será un certificado autofirmado.
- En el campo CN debe aparecer el valor "AP1.1_AP1.2 AC", donde AP1.1 y AP1.2 son los primeros apellidos de los componentes del grupo de prácticas. En O debe aparecer "SEGURIDAD DE SISTEMAS INFORMÁTICOS" y en OU debe aparecer "Practica 3 2020-2021".
- Generar un par de claves RSA (pública y privada) de longitud 1024 y un certificado X.509 de clave pública de sitio firmado por la autoridad creada en el punto anterior.
- En el campo CN debe aparecer el valor que identifique al sitio. Puede ser el Nombre de Dominio o la dirección IP del sitio. Si se trabaja en local sería "localhost" o "127.0.0.1".
- Generar certificados personales X.509 de usuario, firmados por la AC creada en el punto primero. Crear uno para cada uno de los componentes de grupo de prácticas. En el campo CN debe aparecer el DNI del estudiante y en E el buzón email de la Usal. Dos Certificados por estudiante, uno de clave pública, en formato pem (crt) y el otro que contenga la clave privada, en formato pkcs12.
- Configurar el servidor de páginas para servir páginas seguras. Se usará el certificado generado en el segundo punto. Opcionalmente configurarlo para validar los usuarios que se conectan a través de certificados.

Acceder a alguna página validando la identidad personal con un mecanismo basado en certificado digital. Si no dispones de un certificado de la FNMT y/o DNIe, lo haremos con el certificado CaCert accediendo a la página segura de CAcert. ¿Cómo crees que se realiza esta autenticación?

Trabajando con curvas elípticas

Repetir el apartado 2 pero usando cifrado de curvas elípticas (ecc). Generar un par de claves ecc (pública y privada) de longitud 160 y un certificado X.509 de clave pública de sitio firmado por la autoridad creada en el punto anterior.

Fuentes para este apartado

- https://www.keycdn.com/support/elliptic-curve-cryptography
- https://support.globalsign.com/customer/portal/articles/1994347-ecc
- https://support.globalsign.com/customer/en/portal/articles/1995283-ecc-compatibility
- https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Se entregará un informe que documente la actividad realizada para las tareas encomendadas.