Universidad Politécnica de Cartagena

Escuela Técnica Superior de Ingeniería de Telecomunicación

SEGURIDAD EN REDES DE COMUNICACIONES

Práctica 3: Certificados Digitales para servidores web

María Dolores Cano Baños

Francisco López Ortiz

Objetivos

- Aprender a instalar un servidor web con facilidades criptográficas.
- Aprender a solicitar un certificado X.509 firmado por una autoridad certificadora.
- Aprender a instalar el certificado X.509.

Certificados Digitales

Para solucionar el problema de la Autentificación en las transacciones por Internet es necesario un sistema identificativo único de cada entidad o persona. Ya existen los sistemas criptográficos de clave asimétrica, mediante los cuales una persona dispone de dos claves, una pública, al alcance de todos, y otra privada, sólo conocida por el propietario. Cuando deseamos enviar un mensaje confidencial a otra persona, basta pués con cifrarlo con su clave pública, y así estaremos seguros de que sólo el destinatario correcto podrá leer el mensaje en claro.

El problema es cómo estar seguro de que efectivamente la clave pública que nos envían sea de la persona correcta, y no de un suplantador. De aquí surgió la idea de implementar una especie de documento de identidad electrónica que identificara sin dudas a su emisor.

La solución a este problema condujo a la aparición de los **Certificados Digitales** o **Certificados Electrónicos**, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales. La misión principal de un Certificado Digital es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

Un Certificado Digital es por tanto un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la clave pública de la misma, haciéndose otra persona o entidad de confianza responsable de la autenticidad de los datos que figuran en el certificado. A esta persona o entidad se la denomina **Autoridad Certificadora (Certification Authority)**. Las principales Autoridades Certificadoras actuales son Verisign (www.verisign.com), filial de RSA Data Security Inc., Thawte (www.thawte.com), y a nivel nacional la Fábrica Nacional de Moneda y Timbre (www.fnmt.es).

El sistema es análogo a otros de uso común, como el D.N.I. español, en el que una autoridad de confianza (el estado o la policía) atestigua que la persona portadora de dicho documento es quién dice ser.

El formato de los Certificados Digitales es estándar, siendo X.509 v3 el recomendado por la Unión Internacional de Telecomunicaciones (ITU) y el que está en vigor en la actualidad.

Servidor Apache

Apache es el servidor web más utilizado en la actualidad en Internet, ocupando un lugar clave en la infraestructura de esta red. La misión de un

servidor web es básicamente la de traducir una URL (Uniform Resource Locator) a un nombre de archivo y enviar este archivo a través de Internet , o traducir la URL por el nombre de un programa , correr ese programa y enviar la respuesta de vuelta.

Cuando se conecta a una URL, lo que hace es enviar un mensaje a la máquina que tiene esa dirección. Lógicamente todos esperamos que la máquina a la que enviamos ese mensaje esté activa y lista para recibir y actuar sobre el mensaje enviado. Una URL tiene tres partes:

`<scheme>://<host>/<path>`

Así, si`< scheme>` es `http`, significa que el navegador debe utilizar el protocolo HTTP (Hypertext Transfer Protocol). Si `<host>` es `www.upct.es` y `<path>` es `/`, significa normalmente ir a la página superior de la máquina. La parte `<host>` puede contener una dirección IP o un nombre, que el navegador convertirá a una dirección IP. Las peticiones llegan al puerto 80 (el puerto por defecto de HTTP) de la máquina `<host>`.

Los criterios a la hora de seleccionar un servidor web son los siguientes:

- Correr rápido, de manera que pueda atender muchas peticiones utilizando el mínimo hardware.
- Ser multitarea, pudiendo atender más de una petición a la vez. La manera de conseguir esta característica es correr el servidor sobre un sistema operativo multitarea.
- Autenticar peticiones: algunos usuarios pueden tener permiso para acceder a más servicios que otros.
- Responder a errores. Por ejemplo si se solitia una página no existente devolver un mensaje con Error 404 definido en el protocolo HTTP.
- Negociar el estilo y lenguaje de la respuesta con el emisor.
- Ofrecer variedad de formatos. A un nivel más técnico, un usuario puede querer imágenes JPEG en vez de GIF, o puede querer texto en formato vdi en vez de PostScript.
- Ser capaz de correr como servidor proxy. Un servidor proxy acepta peticiones de clientes y las reenvía a los servidores reales, y las respuestas de estos servidores las reenvía a los clientes. Hay dos razones por las cuales querer un servidor proxy:

1) El proxy puede correr en el extremo lejano de un corta fuegos, dando acceso a sus usuarios a Internet.
2) El proxy puede almacenar las páginas más visitadas en caché para hacer más rápido el acceso.

- Ser seguro.

El servidor web Apache cubre más de la mitad del mercado que su competidor directo Microsoft. Esto no se debe sólo a que sea de libre distribución y por tanto gratuito. Su código es abierto, lo que significa que puede ser examinado por cualquiera, si hay errores miles de personas los detectan. Este hecho lo hace más fiable que cualquier software comercial. En particular, Apache es extensible a través de una tecnología establecida

para escribir nuevos módulos (Tomcat, mod_ssl, etc.), que permiten añadir nuevas características. El módulo ssl que utilizaremos en esta práctica añade capacidades criptográficas al servidor web Apache. En la página http://www.modssl.org/docs/2.8/ encontrará un manual completo sobre el módulo ssl para servidores web Apache.

Desarrollo de la práctica

En esta práctica aprenderá a instalar un servidor web, crear una pareja de claves pública y privada, y obtener un certificado para el servidor. Describiremos el proceso en detalle para darle un idea de cómo es, pero es importante referirse a la documentación del software que utilice en caso de ser diferente del utilizado en esta práctica.

Para instalar y configurar un servidor web con facilidades criptográficas debe seguir estos pasos:

- Obtener un servidor web (descargándolo de Internet o comprando el software o una computadora que lo incluya).
- Instalarlo.
- Crear una pareja de claves pública y privada para el servidor.
- Opcionalmente, crear un certificado autofirmado para poner en operación el servidor web de inmediato.
- Enviar la clave pública a una autoridad certificadora (CA).
- Enviar otros documentos de soporte a la autoridad certificadora.
- Recibir de la autoridad certificadora el certificado público X.509 v3 firmado.
- Instalar el certificado en el servidor web.

Esta práctica le muestra el proceso utilizando el servidor Apache+mod_SSL y VeriSign como ejemplos.

Desgarga e instalación del servidor web Apache+mod_SSL

El servidor web Apache fue escrito por un grupo de programadores llamado *The Apache Group*. Éstos integraron el paquete mod_SSL al servidor Apache. Detallaremos en este apartado cómo obtener e instalar Apache_modSSL, incluyendo la creación de la identificación y la firma de VeriSign.

Será necesario descargar de Internet el servidor Apache, mod_ssl y openssl. Desde la página web de Apache se puede descargar este servidor web de modo gratuito. Para hacerlo, debe contar con una conexión a Internet y un navegador como el Netscape.

1. Los siguientes archivos que va a descargar debe guardarlos en la cuenta de root. Si ha entrado con su login de usuario pase a superusuario y haga una copia de todos estos archivos a /root.

2. Para iniciar el proceso de descarga vaya a la URL indicada abajo y descargue la versión 1.3.29.

   http://www.apache.org

3. Vaya a la página http://www.modssl.org/ y descargue el paquete mod_ssl compatible con la versión de Apache que acaba de descargar. Observe que estos ficheros (por ejemplo, mod_ssl-2.6.4-1.3.12.tar.gz) traen dos números de serie. El primero (2.6.4) indica la versión de mod_ssl, el segundo muestra la versión de Apache a la que corresponde (1.3.12).

4. Descargue el paquete openSSL para Linux de http://www.openssl.org.

5. Lo primero que haremos, y puesto que otros pasos así lo requieren, será descomprimir nuestro servidor apache y configurarlo indicando en qué directorio lo queremos instalar:

```
#gunzip apache_1.3.29.tar.gz
#tar –xvf apache_1.3.29.tar
#cd apache_1.3.29
#./configure --prefix=/usr/local/apache
#cd ..
```

6. A continuación instalaremos OpenSSL con los siguientes comandos. Tras descomprimir el archivo lo configuramos indicando dónde lo queremos instalar (opción prefix del script *config*), lo compilamos y lo instalamos, como cualquier programa Linux que viene en forma de código fuente.

```
#gunzip openssl-0.9.7d.tar.gz
#tar –xvf openssl-0.9.7d.tar
#cd openssl-0.9.7d
#./config --prefix=/usr/local/ssl
#make
#make install
```

7. Descomprimimos el mod_ssl que hemos descargado de Internet, y lo configuramos indicándole donde tenemos el código fuente del Servidor Apache (que aún no hemos instalado).

```
#gunzip mod_ssl-2.8.16-1.3.29.tar.gz
#tar –xvf mod_ssl-2.8.16-1.3.29.tar
#cd mod_ssl-2.8.16-1.3.29/
#./configure -–with-apache=../apache_1.3.29
#cd ..
```

8. En este punto es donde podremos añadir a nuestro servidor apache todos los módulos que queramos (Perl, PHP, Tomcat, ssl, etc.), de la misma forma que se indica en sus respectivas guías de instalación. En este caso, el único módulo a añadir es mod_ssl. Primero le indicamos dónde hemos descomprimido OpenSSL y después le indicamos los distintos módulos que queremos usar:

```
#cd apache-1.3.29/
#SSL_BASE=../openssl-0.9.7d   ./configure
--prefix=/usr/local/apache   --enable-module=ssl   --enable-
shared=ssl
```

NOTA: Todo sobre la misma línea de comando

9. Ya tenemos Apache preparado para instalarlo. Así que compilamos:

```
#make
```

Ahora es el momento de crear nuestro certificado y clave, proceso realizado por la facilidad *mkcert.sh*. Será necesario contestar a diversas preguntas sobre nuestra "empresa". A toda esta información se la conoce como *Distinguished Name*. Algunas preguntas son opcionales (no llevan respuesta por defecto entre corchetes []). El Distinguised Name es requisito para crear una solicitud de certificado a cualquier Autoridad Certificadora como Verisign.

10. Para crear el certificado y clave debemos usar el comando

```
#make certificate
```

seguido de las correspondientes opciones.

11. Según la información que se muestra en pantalla después de compilar, ¿cuántas opciones tenemos para crear el certificado? ¿Qué significa cada una de ellas?
12. En nuestro caso, debemos crear un certificado de prueba (test). Ejecute el comando para tal fin.
13. Seleccione el algoritmo de cifrado RSA. ¿Cuál es la longitud de la clave?
14. Cuando se le soliciten los datos de la empresa introduzca los siguientes (sustituya xx por el valor que corresponda a su equipo):

```
1. Country Name        (2 letter code) [XY]:ES
2. State or Province Name (full name)  [Snake Desert]:Murcia
3. Locality Name       (eg, city)      [Snake Town]:Cartagena
4. Organization Name (eg, company) [Snake Oil, Ltd]:IT4-PCxx
5.  Organizational  Unit  Name  (eg,  section)  [Webserver
Team]:src
6.  Common  Name  (eg,  FQDN)   [www.snakeoil.dom]:  www.IT4-
PCxx.upct.es
7. Email Address (eg, name@FQDN) [www@snakeoil.dom]:src@IT4-
PCxx.upct.es
8. Certificate Validity (days) [365]:[ENTER]
```

15. Introduzca la siguiente contraseña de cifrado para la clave privada:

    mysuperpassword

    ¿Qué método de cifrado se emplea? ¿Para qué se emplea esta contraseña *mysuperpassword*?
16. ¿En qué directorio se guarda el archivo con la clave privada? ¿Cuál es el nombre de ese archivo?
17. ¿En qué directorio se guarda el archivo con el certificado? ¿Cuál es el nombre de ese archivo?
18. ¿En qué directorio se guarda la solicitud de certificado? ¿Cuál es el nombre de ese archivo?

19. Por último sólo resta instalar los archivos en su lugar correspondiente:

```
#make install
```

20. Si todo ha ido bien, tendremos al final de la instalación un cuadro indicándonoslo, y mostrando lo que tenemos que escribir para ejecutar el servidor apache en modo “normal” y en modo “seguro”. ¿Cuál es el comando para arrancar el servidor en modo normal? ¿Y en modo seguro?

21. Si arrancamos la versión segura nos pedirá el password que hallamos dado a nuestra clave SSL, y a partir de este momento ya podemos acceder a nuestro servidor seguro desde nuestro navegador, ¿con qúe dirección IP?

Para comprobar que funciona correctamente dirigimos nuestro navegador a la dirección IP de la máquina donde estamos (192.168.4.x) con el `[scheme]` *https* y recibiremos una ventana informándonos del acceso a “zona segura” y de que el certificado no está aprobado por ningún organismo oficial, por lo que podría no ser válido.

22. ¿Quién firma el certificado actual?¿Qué información adicional contiene el certificado?

Tras aceptar el certificado (**sólo para esta sesión**) nos sale la página de presentación de Apache con la información de SSL.

Instalación del certificado de VeriSign

Para solicitar un certificado firmado por una autoridad certificadora diríjase a la URL https://www.verisign.com/products/srv/trial/intro.html de VeriSign. Verisign es una empresa fundada en 1995 por RSA Data Security Systems y otros socios. Desde esta URL solicitaremos un certificado temporal y lo instalaremos en el servidor Apache.

23. Tras entrar en la URL pulse “Continue”.

24. Introduzca la solicitud de certificado que ha creado durante la instalación del Apache (punto 18). Debe introducir unas líneas de texto de aspecto similar al siguiente:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2DCCAUECAQAwgZcxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZNdXJjaWExEjAQ
BgNVBAcTCUNhcnRhZ2VuYTERMA8GA1UEChMISVQ0LVBDMDYxDDAKBgNVBAsTA3Ny
YzEdMBsGA1UEAxMUd3d3LklUNC1QQzA2LnVwY3QuZXMxIzAhBgkqhkiG9w0BCQEW
FHNyY0BJVDQtUEMwNi51cGN0LmVzMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDPcNbMDO1v7gjgHWGAQCytJPwGtcZkkU0xSpmNIOiUd6cHyaJ2jM3q78zDTy1r
QEXpUscJGUU6QySdM8f5qyrP3+39lBr6kVC6ZFS+ClPrYlw4D5Jv7J1ok2INWdV7
CGC7r0WBZtiCuoOtOq+hnzLuEM0zgCkEI4vzrTilQpAtLwIDAQABoAAwDQYJKoZI
hvcNAQEEBQADgYEAcx8oA9rQJBmfg7TdabWm4R52wYyFcvG7FmYJ6yzhnkTRuZEH
IsNhB7RgVgdlWXlYGS1OU7TgXXeFUiyAY024BHsFuzQc7NB7mPVfgjtI0TByystx
bq3421uHDi2csYPB/Vby0jvb6SfdKfHwobnXV8KQiwMKYEHGLCv76UlX4ro=
-----END CERTIFICATE REQUEST-----
```

25. Rellene la información que se le solicite: país, provincia, empresa, etc., al igual que hizo anteriormente. Es muy importante que la dirección de correo electrónico que escriba sea correcta, pues el

certificado de prueba le será enviado automáticamente a esa dirección.

26. Acepte el acuerdo. En breves momentos le llegará el certificado temporal.

27. El correo electrónico que recibirá llevará incorporado el certificado temporal. El aspecto es el siguiente:

```
-----BEGIN CERTIFICATE-----

MIIDMjCCAtygAwIBAgIQCIccTVPMFKUXvu8hiZM0GzANBgkqhkiG9w0BAQUFADCB
qTEWMBQGA1UEChMNVmVyaVNpZ24sIEluYzFHMEUGA1UECxM+d3d3LnZlcmlzaWdu
LmNvbS9yZXBvc2l0b3J5L1Rlc3RDUFMgSW5jb3JwLiBCeSBSZWYuIExpYWIuIExU
RC4xRjBEBgNVBAsTPUZvciBWZXJpU2lnbiBhdXRob3JpemVkIHRlc3Rpbmcgb25s
eS4gTm8gYXNzdXJhbmNlcyAoQylWUzE5OTcwHhcNMDQwNDIzMDAwMDAwWhcNMDQw
NTA3MjM1OTU5WjByMQswCQYDVQQGEwJFUzEPMA0GA1UECBMGTXVyY2lhMRIwEAYD
VQQHFAlDYXJ0YWdlbmExETAPBgNVBAoUCElUNC1QQzA2MQwwCgYDVQQLFANzcmMx
HTAbBgNVBAMUFHd3dy5JVDQtUEMwNi51cGN0LmVzMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPcNbMDO1v7gjgHWGAQCytJPwGtcZkkU0xSpmNIOiUd6cHyaJ2
jM3q78zDTy1rQEXpUscJGUU6QySdM8f5qyrP3+39lBr6kVC6ZFS+ClPrYlw4D5Jv
7J1ok2INWdV7CGC7r0WBZtiCuoOtOq+hnzLuEM0zgCkEI4vzrTilQpAtLwIDAQAB
o4HRMIHOMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEIGA1UdHwQ7MDkwN6A1oDOG
MWh0dHA6Ly9jcmwudmVyaXNpZ24uY29tL1NlY3VyZVNlcnZlclRlc3RpbmdDQS5j
cmwwUQYDVR0gBEowSDBGBgpghkgBhvhFAQcVMDgwNgYIKwYBBQUHAgEWKmh0dHA6
Ly93d3cudmVyaXNpZ24uY29tL3JlcG9zaXRvcnkvVGVzdENQUzAdBgNVHSUEFjAU
BggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEFBQADQQC6xVKKcgqjJpyd
EgzD9iA7avOBALG4QzoTN1ZG2Z6q93vwHyi+T9rO1i5gLazF73ayIkgWmTJLhehf
fIztFKM7
-----END CERTIFICATE-----
```

28. Guarde el certificado en un archivo dentro del directorio */root/apache_1.3.29/conf/ssl.crt* con el nombre *verisign.crt*.

29. Modifique el archivo de configuracion */usr/local/apache/conf/httpd.conf* e indique la ruta del nuevo archivo que contiene el certificado firmado por la autoridad y la clave privada:

```
SSLCertificateFile    /usr/local/apache/conf/ssl.crt/verisign.crt
```

30. Reinicie el servidor Apache.

31. ¿Qué diferencias observa al arrancar el servidor seguro?

32. Imagine que reinstala el servidor web Apache y sigue empleando el certificado que le llegó anteriormente de Verisign. A la hora de arrancar el servidor web seguro no funciona. Visualice ambos, certificado y clave, con los comandos abajo indicados. ¿Qué campos deben coincidir?

```
openssl x509 –noout –text –in [RUTA DEL CERTIFICADO]
openssl rsa –noout –text –in [RUTA DE LA CLAVE PRIVADA]
```

CUESTIONARIO

NOMBRE _____

NOMBRE _____

FECHA _____

2 y 3. ¿Qué diferencia hay entre ApacheSSL y Apache con mod_ssl?

11. ¿Cuántas opciones tenemos para crear el certificado? ¿Qué significa cada una de ellas?

13. Seleccione el algoritmo de cifrado RSA. ¿Cuál es la longitud de la clave?

15. ¿Qué método de cifrado se emplea? ¿Para qué se emplea esta contraseña *mysuperpassword*?

16. ¿En qué directorio se guarda el archivo con la clave privada? ¿Cuál es el nombre de ese archivo?

17. ¿En qué directorio se guarda el archivo con el certificado? ¿Cuál es el nombre de ese archivo?

18. ¿En qué directorio se guarda la solicitud de certificado? ¿Cuál es el nombre de ese archivo?

20. ¿Cuál es el comando para arrancar el servidor en modo normal? ¿Y en modo seguro?

21. Si arrancamos la versión segura nos pedirá el password que hallamos dado a nuestra clave SSL, y a partir de este momento ya podemos acceder a nuestro servidor seguro desde nuestro browser, ¿con qúe dirección IP?

31. ¿Qué diferencias observa al arrancar el servidor seguro?

34. Imagine que reinstala el servidor web Apache y sigue empleando el certificado que le llegó anteriormente de Verisign. Ala hora de arrancar el servidor web seguro no funciona. Visualice ambos certificado y clave con los comandos abajo indicados. ¿Qué campos deben coincidir?