Fundamentos de Seguridad – Análisis de la seguridad en los Sistemas de Información – CURSO 2015-2016

Práctica 1: Taller de OpenSSL. Cifrado (simétrico y asimétrico), resúmenes, certificados X.509, correo S/MIME y servidor seguro SHTTP.

PARTE 1 - Utilización de OpenSSL (resúmenes, cifrado simétrico y asimétrico de documentos)

2.1 Generación y comprobación de Resúmenes. Generación de claves asimétricas (pública-privada) y firmado de resúmenes

- Utilizando la **bibliografía acerca de OpenSSL de la página de la asignatura**, utilizar diferentes algoritmos de resumen (mínimo TRES) sobre un documento y comprobar dichos resúmenes ante modificaciones del fichero.
- Generar un par de claves asimétricas RSA de 2048 bits, de acuerdo con las indicaciones del apéndice A del manual básico (para RSA).
- Exportar dicho par de claves (pública y privada) en formato PEM (textual) y DER (binario). Utilizar los comandos de conversión de PEM a DER y viceversa.
- Con los dos pares de claves asimétricas creadas, **firmar y comprobar la firma** del resumen de un texto cualquiera.
- **Documentar** el trabajo realizado, **con ejemplos de los resultados obtenidos (en Base64 o en formato PEM) y profusión de volcados de pantalla**.
- **Opcional**: **Repetir** estas operaciones con claves **DSA**. Su generación exige búsqueda de documentación y el empleo de la utilidad “dsaparam”.

2.2 Cifrado Simétrico de documentos

Seguir los siguientes pasos para crear un documento de texto y cifrarlo con openssl.

- Estudiar en la documentación de openssl cómo se utiliza el comando enc para cifrar y descifrar. Explicar sus opciones más importantes, con especial atención a los métodos de cifrado (ecb, cbc, etc.).
- Crear un archivo de texto y otro binario (tamaño medio – entre 1 y 10 kbytes)
- Cifrarlos con diferentes algoritmos simétricos (mínimo cinco– AES y TDES obligatorios).
- Descifrarlos y comprobar el resultado
- Analizar el comportamiento para diferentes longitudes de mensaje y diferentes algoritmos de cifrado (mínimo cinco – AES y TDES obligatorios).
- **Explicar la gestión de contraseñas** detallada en el estándar PKCS #5 y su aplicación a las claves de cifrado simétrico, vectores de inicialización y “salt” (derivación de claves e “iv” a partir de contraseñas). Documentar las diferentes alternativas, empleando diferentes algoritmos de cifrado. **Demostrar que un fichero puede ser cifrado con contraseña y descifrado con su conjunto equivalente de clave (key), vector de inicialización (iv) y “sal” (salt)**.

- **Documentar** el trabajo realizado, **con ejemplos de los resultados obtenidos (en Base64 o en formato PEM) y profusión de volcados de pantalla**.
- **Opcional:** Se valorará muy positivamente la **demostración** de que el modo de operación **"ecb" es muy peligroso**, por ejemplo, con una **imagen de colores sólidos** (similar al ejemplo de "Tux" en la página de Wikipedia).

2.2 Cifrado Asimétrico de documentos

Seguir los siguientes pasos **para crear un documento de texto y cifrarlo con openssl, enviando a un compañero.el documento cifrado y la clave cifrada con su clave pública RSA** (que previamente ha de conocerse). Codificarlo todo en Base64 y enviar un correo electrónico con tres partes:

- Documento cifrado (indicando algoritmo utilizado)
- Clave simétrica empleada, cifrada con la clave pública del receptor
- Resumen del documento original (indicando algoritmo) cifrado con la clave privada del emisor
- El mensaje ha de ser de tipo textual, indicando las diferentes partes e instrucciones para su decodificación/comprobación (comandos OpenSSL necesarios para decodificar y verificar el documento).
- Se valorará positivamente el empleo de diferentes sistemas de cifrado, de generación de resúmenes, etc.
- **Documentar** el trabajo realizado, **con ejemplos de los resultados obtenidos (en Base64 o en formato PEM) y profusión de volcados de pantalla**.

PARTE 2 - Envío, recepción y DECODIFICACIÓN MANUAL de mensajes S/MIME firmados y cifrados empleando certificados gratuítos de CAcert.org

En esta parte de la práctica se pretende que el estudiante domine el manejo y la estructura de correos electrónicos seguros con el estándar S/MIME, primero como usuario final (utilizando agentes de correo electrónico convencionales) y seguidamente el análisis y la generación de este tipo de mensajes de correo electrónico seguro desde línea de comandos.

1.- Se trata de registrarse en el sitio web http://www.cacert.org, crear una cuenta, solicitar y crear un certificado de cliente, instalarlo en un cliente de correo (Thunderbird, Outlook Express o Apple Mail) y enviar un mensaje firmado y cifrado a la dirección de un compañero de la asignatura, cuyo certificado ha de ser previamente importado en el cliente de correo, después de recibir un mensaje firmado de ese compañero.

2.- Una vez recibido el correo firmado y cifrado, hemos de DECODIFICAR MANUALMENTE, con la ayuda de la utilidad "OPENSSL SMIME" el texto del mensaje recibido, empleando nuestro certificado original (con la clave privada) y el certificado del compañero.

3.- Con la misma utilidad, hemos de generar otro mensaje cifrado y firmado con destino a nuestro compañero, que se intentará enviar por correo electrónico (en caso de que no se pueda, se estudiará la posibilidad de que el compañero lo copie en su programa de correo electrónico y lo pueda leer a través de dicho programa).

1. Acceder al sitio web http://www.cacert.org

2. Si se desea, seleccionar a la derecha **Translations / Español**

3. Seleccionar **Certificado Raiz** en el menú de la derecha, una vez en la página, instalarlo en el equipo (en formato PEM o DER si usa Firefox). Este mismo certificado ha de ser instalado en el programa gestor de correo electrónico (Mozilla Thunderbird, Microsoft Outlook Express, etc.)

4. Seleccionar **Darse de Alta** en el menú de la derecha

5. Rellenar **cuidosamente** el formulario. La **contraseña** ha de tener al menos una letra mayúscula y otra minúscula, un espacio y un signo de puntuación. Se aconseja que al menos tenga 15 caracteres. **NO LA OLVIDEN**.

6. Al pulsar el botón de **Siguiente**, nos informa de que nos envía a nuestra dirección de correo electrónico un mensaje de confirmación. Una vez recibido el mensaje, debemos **pulsar en el enlace que nos lleva de nuevo al sitio web para confirmar la creación de la cuenta**.

7. Una vez hayamos **accedido de nuevo** al sitio web y nos hayamos **registrado con nuestra dirección de correo y la contraseña**, pulsaremos a la derecha en **Certificado de Cliente**

8. Nos aparecerá una ventana similar a la de la **Figura 2**, seleccionaremos **Agregar**, a la izquierda de nuestra dirección de correo y pulsamos en **Siguiente**.

9. La ventana siguiente nos pregunta el **Nivel de Clave**. Dejaremos la opción seleccionada por defecto

10. Si utilizamos **Explorer**, puede que nos solicite permiso para ejecutar un control **Activex**, hay que autorizarlo, y después de mostrarnos el certificado, pulsando el botón **INSTALAR** podremos instalarlo. Con **Firefox** es más directo, y en ambos casos, el resultado final es que hemos instalado el certificado personal en la base de datos del navegador. Podremos acceder, en Opciones o en Herramientas, respectivamente, a los almacenes de certificados y comprobar que tenemos el certificado **personal** "CAcert WoT User" y en seleccionándolo, en **Ver/Detalles** comprobaremos que en el campo **Asunto**, contiene nuestra dirección de correo.
11. Llegados a este punto, es muy conveniente **guardar una copia del certificado (incluyendo la clave privad**a). El sistema nos **solicitará** una **contraseña** de protección. No es mala idea (sólo en este caso) **utilizar la misma contraseña** que creamos antes para el acceso a www.cacert.org.

12. **Una vez obtenido** el certificado digital, deberemos **configurar un cliente de correo electrónico** para que pueda firmar y cifrar mensajes con dicho certificado. Los correos a través de web (como el de la ULPGC) no permiten el uso de certificados., así que si no lo tenemos instalado, **habrá que configurar uno de los clientes de correo más usuales** (Mozilla Thunderbird, Microsoft Outlook Express o Apple Mail) con la misma cuenta de correo. **Consultar la ayuda del programa para instalar el certificado** (Microsoft Outlook Express puede que ya lo tenga instalado, ya que comparte la base de datos de certificados del Explorer).

13. En este cliente de correo electrónico **hemos de instalar tanto el certificado raíz de cacert.org, como nuestro certificado personal**. Verificar que el certificado raíz tiene asignada la confianza y se encuentra en el almacén de autoridades de confianza. Nuestro certificado personal ha de estar en el almacén de "mis certificados" o similar.

14. Una vez **configurado** e **instalado** el certificado, podremos **FIRMAR** los mensajes que envíemos, pero para **CIFRAR** correo para un destinatario, es necesario **disponer previamente de SU certificado** (obviamente, sólo con la clave pública)

15. **Recibir un mensaje firmado de un compañero** e **instalar su certificado** en **nuestro** cliente de correo. Como comprobación, debemos **acceder al almacén de certificados del programa de correo y verificar que en la pestaña de "Otras personas" o "Personas" aparece dicho certificado, antes de continuar**.

16. Enviar un mensaje con Asunto: (nombre y apellidos) a dicha dirección de correo (**la del compañero**) con un breve texto de salutación y sobre todo, **con las opciones de FIRMADO Y CIFRADO activadas.**

17. Una vez recibida la respuesta del compañero en otro mensaje cifrado y firmado, se trata de **DECODIFICAR** ese mensaje desde la utilidad "**openssl smime**". Para ello, hemos de guardar el mensaje completo como texto, exportar nuestro certificado completo (con clave privada) y el certificado del compañero y **procesar estos tres ficheros** (mensaje de texto y los dos certificados) a través de la citada utilidad. Obsérvese que el descifrado y la verificación de firma han de hacerse por separado. Documentar exhaustivamente el proceso.

18. **Opcional:** De manera similar, se utilizará la utilidad "openssl smime" **para generar un nuevo mensaje de correo electrónico cifrado y firmado con destino al compañero**, de forma que según se reciba directamente o se tenga que importar en nuestro sistema, comprobemos que un mensaje creado desde línea de comandos puede ser leído directamente en el programa de correo electrónico.

19. **Documentar** el trabajo realizado, **con ejemplos de los resultados obtenidos (en Base64 o en formato PEM) y profusión de volcados de pantalla**

PARTE 3 - Configuración de un SERVIDOR WEB SEGURO (SHTTP) utilizando un certificado AUTOFIRMADO, con privilegios de Administrador en un servidor web – Apache, ISS, etc.

Esta última parte de la práctica 1 consiste en la **creación de un certificado AUTOFIRMADO de servidor Web, utilizando** las herramientas de la utilidad openssl; y en la **instalación de dicho certificado en un servidor apache seguro,** que responda a la dirección web **https://www.ejemplo.com.** Una vez configurado el servidor seguro, se preparará una página HTML y se colocará como **"index.html**" en el directorio raíz del servidor, de forma que esta página **será accedida de forma segura desde un navegador web.** Todo el proceso ha de ser **documentado** con profusión de ejemplos de **comandos en línea, de ficheros de configuración (resumidos) y de volcados de pantalla.**

A diferencia de las anteriores, esta parte de la práctica **requiere privilegios de administrador** en la máquina en la que se pretenda configurar el servidor seguro. **Podrá realizarse en una máquina Windows, Linux o Mac, virtual ó real, pero el servidor ha de ser un APACHE**.

El nombre **del servidor seguro será "www.ejemplo.com"**. Dado que no disponemos de control, desde el punto de vista del "Domain Name Service" o DNS, sobre el dominio de Internet "ejemplo.com", **tendremos que asegurarnos de que tanto el servidor como el programa cliente que utilicemos para realizar una conexión de prueba** (que podrá ser en la misma máquina o en otra conectada en red**) tienen definido el nombre www.ejemplo.com en su fichero de HOSTS**. En una máquina Linux, este fichero se encuentra en /etc/hosts, mientras que en un Windows XP su localización es "\windows\system32\drivers\etc\hosts".

El objetivo de esta parte es conseguir que el estudiante resuelva un problema real, haciendo uso de los recursos de Internet. Por tanto, **no se detallan las instrucciones**. Precisamente lo que se pretende es que el estudiante **redacte una breve pero clara y concisa descripción de los pasos a ser realizados y la incorpore en la memoria de la práctica**.

Existen multitud de páginas en Internet con descripciones, para diferentes versiones de sistema operativo y servidor. Por ejemplo, una **búsqueda** en Google del texto **"openssl create install autosigned server certificate apache"** lleva a páginas que ilustran el proceso. Un posterior **refinamiento**, añadiendo palabras clave como **"openssl", "windows" o "linux" permitirá escoger los ejemplos** idóneos en nuestro caso particular.

No olvidemos que **la memoria de esta parte debe ser en sí misma un buen ejemplo de documento explicativo**, por tanto, la lectura de la **documentación** que utilicemos para aprender a realizar esta parte de la práctica nos servirá de ayuda para realizar la memoria, y por tanto, **deberá ser incluida en la bibliorafía**.

Necesariamente, **se describirán detalladamente los pasos realizados para generar el certificado de servidor y los ficheros modificados para configurar el servidor apache. También se habrán de mostrar copias de pantalla de la página web obtenida de forma segura, con indicación de las características de la conexión (equivalente a "Herramientas/Información de la página/Seguridad" en un Mozilla Firefox), mostrando el tipo de cifrado obtenido en la conexión.**

4 Realización de un documento con el trabajo efectuado

Preparar un **DOCUMENTO DE TEXTO** (en formato RTF o mejor aún, PDF) **documentando exhaustivamente los pasos realizados en cada una de las TRES PARTES de esta práctica**. El número de páginas no será inferior a 15, y se incluirán listados de todos los ficheros obtenidos (textos de ejemplo, ficheros cifrados, resúmenes, firmas, etc.) en formato texto, Base64, PEM o similar, según cada caso. **El documento ha de estar formado por TRES capítulos**, correspondientes a los tres ejercicios propuestos en esta práctica, en los que se describa con detalle las operaciones realizadas.

Se aconseja incluir una **portada** con los datos del estudiante, título del trabajo (Practica 1 de la asignatura ....) un **índice** de los capítulos, una **bibliografía** con los recursos utilizados (libros, páginas web, etc.) y en general, todo aquello que estimemos debe incorporar un **trabajo de calidad profesional**.

Se valorará tanto la **calidad técnica del trabajo como la claridad de la redacción**, el empleo de fuentes específicas para distinguir el texto escrito de los comandos utilizados (se aconseja una fuente del tipo Courier de paso fijo para comandos y ficheros de texto), la **inserción de volcados de pantalla** para mostrar textos, páginas web o resultados de opciones del navegador, la ausencia de faltas ortográficas y la profesionalidad del trabajo en general. **En este sentido, se aconseja muy encarecidamente personalizar en la medida de lo posible el "prompt" del sistema operativo,** de forma que los volcados de pantalla sean lo más personales posible.

El documento final, de nombre ***PRACTICA1.PDF*** o ***PRACTICA1.RTF***, será entregado en el contenedor denominado ***ENTREGA DE LA PRÁCTICA 1***, en la página principal de la asignatura, en el Campus Virtual de la ULPGC.

Se valorará muy positivamente la revisión del trabajo en entrevista personal con el profesor. Por ello, **desde que esté entregado, se intentará una entrevista** breve con el profesor para su **defensa y calificación**.