ADMINISTRACIÓN DE REDES Y SEGURIDAD

TRABAJO PRÁCTICO 3

November 30, 2018

Cátedra:
Lic: Zappellini, Bruno Damian

Integrantes:
Toledo Margalef, Pablo Adrian
UNPSJB - Trelew

CRIPTOGRAFÍA Y SUS APLICACIONES

Conceptos Básicos

1. (a) Encriptación simétrica, pero intercambio de claves a través de algún medio seguro
   (b) Encriptación simétrica
   (c) Encriptación asimétrica
2. (a) Verdadero.
   (b) Falso. EL encriptado asimétrico hace crecer el payload considerablemente.
   (c) Falso. El mecanismo seguro de intercambio de claves es necesario para encriptación simétrica.

Aplicaciones de Criptografía

PKI

Para poder verificar la firma en un mail recibido es necesario conocer la información de la autoridad certificante, que figura en la información del correo electrónico envíado. CUando el cliente de corre recibe el mensaje con su firma, busca en la autoridad la información necesaria para verificar el mensaje y realiza el camino para obtener una nueva firma. Si la firma obtenida es igual a la que figura en el mensaje, quiere decir que la firma es auténtica y el mensaje no fue alterado en su camino de origen a destino.

Para poder enviar un mail encriptado es necesario tener generado mi par de claves pública y privada, para poder realizar la encriptación y decriptación de los mensajes. También es necesario que el otro extremo de la conversación reciba mi clave pública para poder descifrar el mensaje recibido.

Para poder recibir un mail encriptado y poder abrirlo es necesario poseer la clave pública del remitente.

Se ingresa al sitio www.cacert.org y el navegador, en mi caso firefox 54, nos avisa que estamos por ingresar a un sitio no seguro. Agregamos la excepción al navegador y logramos entrar.

Instalamos el certificado (PEM Format) y observamos las siguientes peculiaridades:

1. El algoritmo de encriptación es: MD5 con RSA.
2. La cantidad de bits de cifrado es de 512 bytes

3. Como dato curioso podemos señalar que el certificado expira en 2033, con su comienzo de funcionamiento en 2003

Ya instalado el certificado verificamos que en la página figura el símbolo del candado verde indicando que el navegador confía y posee certificados para el sitio en el cual está entrando.

Creamos nuestro usuario dentro de cacert y en le opción "Client certificate" creamos un certificado para utilizar personalmente. Este certificado es instalado en el navegador.

Luego cerramos sesión y al ingresar de nuevo, seleccionamos la opción para autenticarse utilizando un certificado. Firefox, en mi caso, abre un diálogo listando los certificados disponibles. Seleccionamos el certificado y luego logramos iniciar sesión en cacert.

Creado nuestro certificado, lo exportamos para poder utilizarlo en nuestro cliente de correo. Una vez importado, ya podemos utilizarlo para firmar y encriptar mensajes.

Situaciones posibles

Al firmar un mensaje, lo que llega es el documento junto con la información de la firma. Esta firma se verifica con el algoritmo habitual, utilizando la clave pública del emisor, el algoritmo de encriptación que indica el certificado. También verifica el certificado al recibirlo.

En los clientes habituales, en mi caso Android, al recibir un mail encriptado me pide que revise las opciones de encriptación de mi cuenta de GMAIL, luego de setear correctamente las claves e importar los certificados. El contenido del mail es desencriptado con total normalidad.

Al momento de recibir un mail encriptado, en el cliente de correo de Thunderbird lo recibo con total normalidad. Pero es porque posee la clave pública junto con el certificado avalando la autenticidad de la clave.

Escenarios

a. Su clave privada fue robada: Se debe reportar el incidente a la autoridad de registración. Para que en la autoridad certificante pueda marcar nuestra clave pública actual como inválidad. Y generar un nuevo par de claves para operar.

b. Su clave privada fue robada y además usted perdió acceso a la misma, puesto que la misma fue borrada de su sistema:

1. Si se pierde acceso a la clave privada y además fue robada. Una salida a esta situación es, al momento de generar las claves, también generar el certificado de revocación, para ser usado en caso de ser necesario. Este certificado se lleva a la Autoridad de Registro.

2. Con respecto a la información encriptada, ya quedó al descubierto. Pero, sin embargo, queda dicho que el certificado está revocado, cuando esa información llegue a destino, al verificar el certificado quedará en evidencia que está encriptada con una clave privada inválida.

3. La información firmada pierde validez. En caso de querer re-verificar la autenticidad, se puede pedir una re-firma del mensaje.

PGP

Al instalar y poner en funcionamiento Enigmail, utilizando el wizard de instalación provisto por el complemento, podemos en un simple paso encriptar y firmar nuestros mails enviados.

Para que en el otro extremo de la comunicación puedan leer el mensaje y/o verificar la autenticidad del mismo, no hace falta más que utilizar el certificado enviado con el correo, generado de mi lado de la comunicación y la clave pública que proviene del repositorio.

Para poder firmar un mail es necesario el algoritmo de hashing para el mensaje, provisto en el certificado generado, y la clave privada propia, para la encriptación y generación del mensaje firmado.

Si, en cambio, es el otro extremo el que nos envía un correo encriptado, necesitamos que se nos envíe el certificado, validando la identidad del emisor. Luego necesitamos obtener la clave pública del emisor desde el repositorio y desenciptar el mensaje.

En todo caso, este procedimiento depende fuertemente de la confianza que se le imprima a la clave desde el cliente de correo. En nuestro caso para otorgar confianza en necesario haber obtenido el certificado del emisor y haberle dado el nivel de confianza deseado. De esta forma se nos advertirá sobre las consecuencias del uso de esta clave.

Escenarios

a. Alguien le ha robado la clave privada. Usted no habıa generado un certificado de revocación para su clave. Sin embargo, usted dispone de la clave privada actualmente, del mismo modo que la persona que se la robó

b. Alguien le ha robado la clave privada y además borró la misma de su almacén de claves. Usted no habıa generado una revocación de su clave.

A considerar:

1. ¿Qué consecuencias sufro respecto de la información que se firma con esa clave?

2. ¿Qué consecuencias sufro respecto de la información encriptada para que solo esa clave pueda abrir?

3. ¿Qué acciones se pueden llevar a cabo en cada caso? y ¿cómo debo proceder?

1.a. La información firmada con esa clave seguirá siendo poder accedida con el uso de la clave pública actual, hasta que se genere el certificado de revocación. A partir de ese momento perderá validez.

2.a. La información quedará al descubierto, por lo que se debe generar el certificado de revocación lo antes posibles, de esta manera, la futura información quedará al resguardo y, la información queda al descubierto, se sabe que está encriptada con una clave pública obsoleta.

3.a. Como se dijo, se debe generar el certificado de revocación

1, 2 y 3, b. En el caso de haber perdido la clave y no tener certificado de revocación es necesario crear un nuevo par de claves. Esto tomará el trabajo de realizar todo el procedimiento que se realizó para obtener el par original de claves.

GPG - GNU

Se crea el mensaje secreto con

```
$ echo "Mensaje secreto para Bruno" > archivo.txt
$ gpg -c archivo.txt
```

Introducimos la clave para encriptar (dos veces), en nuestro caso 1234, y obtenemos el archivo encriptado. Luego desencriptamos utilizando la clave con:

```
$ gpg -d archivo.txt
```

Esteganografía

Al esconder el texto seleccionado, en nuestro caso un par de párrafos de la novela El Hobbit, la imagen no parece, a simple vista haber sufrido cambios.

Al momento de extraer el texto obtenemos aquello que insertamos dentro.