Fundamentos de la Seguridad Informática
Criptografía Aplicada

Grupo de Seguridad Informática
Facultad de Ingeniería
Universidad de la República

Propósito

Las prácticas descritas en este documento introducen a los participantes en los problemas de seguridad asociados a la criptografía. El objetivo es ilustrar los problemas asociados al tráfico de datos sin cifrar y mostrar diferentes formas de criptografía aplicada. Pondremos en práctica los conceptos de criptografía simétrica y asimétrica, junto a la noción de firma digital.

Formato de trabajo

Cada práctica consta de una guía que explica las cosas que deben realizarse para resolverla y una serie de entregables que deben enviarnos para aprobar el laboratorio. Estos entregables son generalmente archivos generados, información obtenida del laboratorio, o documentación sobre los pasos realizados. Esto está detallado en cada una de las prácticas.

Por otro lado, en cada una de las prácticas se listan ciertos *objetivos de aprendizaje*. Estos son los conceptos que esperamos que los participantes estudien y entiendan para realizar la práctica, y que los reafirmen en el desarrollo de la misma.

1. Man in the Middle

El objetivo principal de esta práctica es concientizar sobre la importancia de cifrar la información sensible.

Herramientas

Para realizar esta práctica se dispondrá de la herramienta *ettercap* [2].

Objetivos de aprendizaje

En esta práctica se deberán comprender lo siguientes puntos

- Diferencias entre codificar y cifrar

- Mecanismos de mitigación del ataque analizado
- Campos de aplicación del mecanismo de codificación utilizado

1.1. Presentación

En criptografía, man-in-the-middle (MitM) es un ataque en el que el adversario adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes sin que ninguna de ellas conozca que la comunicación entre ellos ha sido intervenida. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. A continuación establecemos el escenario en el que se realizará esta práctica.

1.2. Escenario

- Un servidor `S` que brinda cierto servicio.
- Un cliente de dicho servicio (la máquina víctima `V`).
- Una máquina Linux `A` equipada con herramientas de ataque.

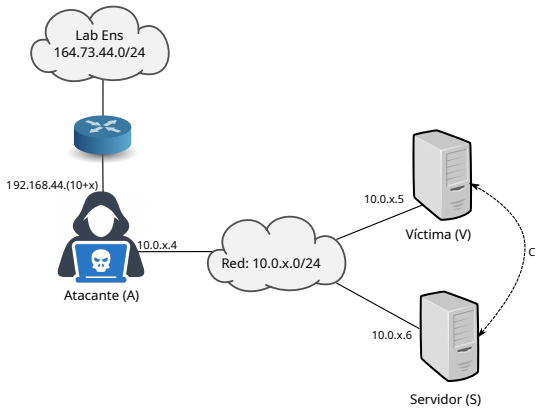

Figura 1: Descripción del Escenario

Existe un escenario como este para cada grupo `x`. El acceso al escenario es utilizando el protocolo SSH, y se realiza a través de la red de enseñanza de facultad, como indica la figura.

Para conectarse a la red de enseñanza desde afuera de la facultad, hay que conectarse por SSH a lulu.fing.edu.uy, con su usuario estudiantil de fing (de la forma nombre.apellido):

```
ssh -l nombre.apellido lulu.fing.edu.uy
```

Luego es necesario entrar a la máquina atacante (identificada por su dirección IP), utilizando el usuario `fsiXX` (donde XX es el número de grupo) y el par de claves SSH que en su momento registraron en el EVA:

```
ssh -l fsiXX 192.168.44.(10+x)
```

Donde `10+x` indica que el último octeto de la IP se obtiene de sumar diez al número de grupo correspondiente. Por ejemplo, la máquina atacante del grupo 32 es la `192.168.44.42`.

Observar que para esto, el par de claves SSH debe estar disponible en el *homedir* del usuario estudiantil en `~/.ssh/id_rsa`.

Otra posibilidad es usar la opción `-J` de SSH para conectarse directamente al atacante:

```
ssh -J <nombre.apellido>@lulu.fing.edu.uy fsiXX@192.168.44.(10+x)
```

La máquina atacante está conectada a la red objetivo (`10.0.x.0/24`), que es donde deben realizar el ataque descripto en la guía de la práctica.

1.3. Guía de la práctica

```
* KWVNQOCZIZ TI PMZZIUQMVBI MBBMZKIX XIZI KIXBCZIZ MT BZINQKW MVBZM
TI UIYCQVI AMZDQLWZ G TI DQKBQUI.

* MT BZINQKW BZIVAUQBQLW KWVBQMVM CVI NZIAM WKCTBI. AM WKCTBW
CBQTQHIVLW CV ITOWZQBUW LM KWLQNQKIKQWV KWVWKQLW (MZZM MNM KM
BZMQVBI G KQVKW KCIZMVBI G WKPW).

* MVBZMOIJTMA: LMVBZW LM CV LQZMKBWZQW XZIKBQKI1, ITUIKMVIZ CV
IZKPQDW, AQV NWZUIBW (BMFBW XTIVW), YCM KWVBMVOI:

* VCUMZW LM XCMZBW BKX LMABQVW LMT UMVAIRM G VWUJZM LMT AMZDQKQW
XWZ LMNMKBW MV MAM XCMZBW.

* MT BMFBW XTIVW BZIVAUQBQLW.
```

(entender el texto de la guía es parte del laboratorio).

2. GPG - OpenSSL

El objetivo principal de esta práctica es utilizar los conocimientos adquiridos en las clases teóricas sobre criptografía asimétrica.

Herramientas

- *GPG*
- *OpenSSL*

Objetivos de aprendizaje

- las diferencias entre criptografía asimétrica y simétrica
- los distintos modelos de confianza en criptografía asimétrica

- comprender el Web of Trust Model utilizado por GPG
- las diferencias entre firmar y cifrar
- identificar ejemplos prácticos en los que podría utilizar las herramientas estudiadas en esta práctica

2.1. Presentación

GPG [3] es un programa de criptografía de clave pública compatible con el estándar OPENPGP RFC 4880 [1]. Sirve para firmar y cifrar datos. Se genera un par de claves (pública/privada) para el usuario. La clave privada debe ser protegida con una *passphrase* y almacenada en un lugar seguro. Será empleada para firmar documentos que podrán ser verificados por terceros utilizando la clave pública. La clave pública tiene como objetivo su distribución, y es la que usarán otros usuarios para enviar información cifrada que se descifrará con la clave privada.

OpenSSL [5] es un conjunto de herramientas criptográficas, en el marco de un proyecto destinado a desarrollar herramientas que implementan los protocolos (Secure Sockets Layer) (SSL v3 *deprecado*) y Transport Layer Security (TLS v1 y superior), así como también una librería criptográfica de propósito general.

2.2. Guía de la práctica

- Descomprimir el archivo `.tar.gz` resultado del procesamiento del archivo `apendice.txt` que se encuentra en el EVA, que contiene los archivos necesarios para realizar la práctica. (Pista: “No es criptografía, es un mecanismo de codificación popular”).
- Usando la herramienta GPG:
  - Generar un par de claves (pública/privada) para el grupo, poniendo el string “fsiXX” en el campo comment. XX son dos dígitos con el número de grupo.
  - Cifrar el archivo `paracifrar.txt` utilizando la clave pública de los docentes contenida en el archivo `fsi-pub.asc`.
  - Exportar la clave pública del grupo generada.
  - Firmar la clave pública de los docentes y asignarle un nivel de confianza adecuado para la situación (justifique)[4].
- Utilizando la herramienta OpenSSL:
  - Generar un par de claves RSA (pública/privada) para el grupo.
  - Generar un Certificate Signing Request (CSR)

Esta práctica puede realizarse en las PCs linux de de facultad (`pcunix`), o en cualquier PC linux que dispongan. No es necesario hacerlo en la máquina atacante de la practica 1.

Entregables:

Crear un directorio `practica2`, con los siguientes archivos:

- el archivo cifrado con la clave pública de los docentes: `paracifrar.gpg`
- la clave pública del grupo generada y exportada con GPG: `fsiXX-pub.asc`
- la clave pública de los docentes firmada por el grupo: `fsi-pub-signed.asc`
- la clave pública del grupo generada con OpenSSL: `fsiXX-pub.pem`
- el CSR: `fsiXX.csr`
- un archivo de texto plano (fsiXX.txt) indicando los comandos utilizados para obtener cada resultado

3. Ataques a Hash MD5

El objetivo de esta práctica es mostrar las vulnerabilidades asociadas a MD5.

Objetivos de Aprendizaje

- entender los diferentes tipos de colisiones existentes en las funciones de hash
- identificar posibles escenarios de ataque utilizando esta vulnerabilidad
- comprender la estructura del código Postscript que permite que el ataque sea efectivo (alto nivel, no se necesita ser programador postscript)

3.1. Guía de la práctica

- Descargar del EVA el archivo comprimido `practica3.tar.gz`, que contiene los siguientes archivos:
  - carta.ps
  - hack.ps
- Comparar los dos archivos según los siguientes criterios:
  - Calculando sus valores de hash MD5 y SHA-1.
  - Utilizando un visor de postscript.
  - Utilizando un editor de texto (aquí se verá el código PS).
  - Utilizando el comando diff.

  Reafirmando lo dicho en los objetivos de aprendizaje: esta práctica no pretende que sean expertos en programación postscript, sino que puedan leer el código y comentar qué se vé como diferencia

  Esta práctica puede realizarse en las PCs linux de de facultad (`pcunix`), o en cualquier PC linux que dispongan. No es necesario hacerlo en la máquina atacante de la practica 1.

Entregables

Almacenar en el directorio `practica3` un archivo de texto sin formato, conteniendo los resultados obtenidos en las comparaciones.

Intente comentar el resultado de los comandos en la comparación. ¿Son distintos? ¿Por qué? ¿Es esperable?

4. Desafío

El desafío se pondrá en la página de EVA. Algunos puntos a tener en cuenta:

- el desafío es **opcional**
- si se desea realizar, es recomendable terminar con la parte obligatoria primero
- no altera el resultado final con respecto a la parte obligatoria. Si no se realiza una parte, por más que se haga el desafío no compensa
- no se contesta ninguna duda sobre el desafío, por ningún medio.

Entregables:

Crear un directorio `desafio` que contenga un archivo explicando los pasos del análisis que se llevaron adelante para resolver el desafío.

En caso que desarrolle herramientas, incluir el código fuente.

Forma de Entrega

Se debe entregar el archivo `entrega1.tar.gz` conteniendo lo solicitado en cada práctica.

La entrega se realizará a través del EVA. Se deberá entregar el archivo solicitado en la actividad `Laboratorio 1`.

Referencias

[1] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. OpenPGP message format. `http://www.rfc-archive.org/getrfc.php?rfc=4880`.

[2] Ettercap. Suite for man in the middle attacks on LAN. `http://ettercap.sf.net`.

[3] GNU Project. Gnu Privacy Guard. `http://www.gnupg.org`.

[4] GNU Project. GNU privacy handbook - key management. `http://www.gnupg.org/gph/en/manual/c235.html`.

[5] The OpenSSL Project. Openssl, secure sockets layer and transport layer security. `http://www.openssl.org`.