Módulo 2.1

Redes y Seguridad

Gr. Ing. Informática

J.L. Vázquez Poletti

Objetivo

En este módulo usaremos varios algoritmos de cifrado históricos, para luego aprender el manejo de diversas herramientas de encriptación y esteganografía.

Punto de partida

El cifrado de las comunicaciones es un aspecto vital, clave del éxito de las operaciones de Third Echelon. Por ello, vamos a dedicarle una sesión al manejo de diversas herramientas relacionadas, no sin antes entender desde un punto de vista práctico la evolución de ciertos algoritmos.

Cifrado histórico: Máquina Enigma

En el servidor web de Third Echelon se dispone de un simulador de la célebre máquina de cifrado Enigma. El mismo se encuentra en la siguiente dirección: http://thirdechelon/enigma/.

1. Intercambiar 4 mensajes con el compañero del segundo puesto a la derecha o izquierda (2 mensajes cada uno), escribiéndolos en papel. Cada mensaje debe tener una posición de partida en los rotores diferente y al menos 3 conexiones en el panel distintas.

¿Qué dificultades se han encontrado en la (de)codificación de los mensajes y transmisión de los mismos así como de las claves?
¿Qué método se podría implantar para la difusión segura de las claves?

Herramientas de hashing

Para verificar la integridad de los datos, se dispone de un par de herramientas de hashing (MD5 y SHA1) accesibles en la siguiente dirección: http://thirdechelon/hash/.

- Generar hashes a partir de diferentes textos.

¿Aumenta el tamaño del mismo con un texto más grande?

En **/home/ubuntu/Isolation/** se han aislado dos programas llamados **subject1** y **subject2** respectivamente.

1. Calcular el hash MD5 de ambos con el comando **md5sum**.
2. Calcular el hash SHA1 de ambos con el comando **sha1sum**.

¿Qué se puede deducir de ambos programas tras ejecutar los comandos?
Ejecutar los dos programas. ¿A qué podría deberse este fenómeno?
Echar un vistazo a esta página: http://www.mscs.dal.ca/~selinger/md5collision/

Máquinas Virtuales

- RyS-ThirdEchelon (ubuntu:reverse)

Más información

Máquina Enigma: http://www.cryptomuseum.com/crypto/enigma/

MD5: http://www.ietf.org/rfc/rfc1321.txt

SHA1: http://www.ietf.org/rfc/rfc3174.txt

Steghide: http://steghide.sourceforge.net/

TrueCrypt: http://www.truecrypt.org/

Cifrado Simétrico

En http://thirdechelon/symmetric/ se dispone de un servicio de cifrado de mensajes con clave simétrica.

- Cifrar y descifrar varios mensajes.

¿Cuál es la regla que sigue el tamaño del texto cifrado en función del texto plano y la clave?

Steganografía

Vamos a trabajar con los archivos contenidos en los siguientes directorios:

- **/home/ubuntu/Documents/SamFisher/** (texto)
- **/home/ubuntu/Pictures/OmegaMission/** (imágenes)

El comando que usaremos es **steghide**:

- **steghide embed -cf ARCHIVO1 -ef ARCHIVO2**. Oculta **ARCHIVO2** en **ARCHIVO1**.
- **steghide info ARCHIVO**. Obtiene información de **ARCHIVO**.
- **steghide extract -sf ARCHIVO**. Extrae el archivo oculto en **ARCHIVO**.

Vamos a probar algo sencillo:

1. Averiguar cuántos bytes útiles para ocultar archivos tienen las imágenes.
2. Hacer una copia de **SpyCam.jpg**. Ocultar el archivo **background.txt** en **SpyCam.jpg**. ¿En qué otras imágenes se puede ocultar?
3. Verificar que la ocultación se ha realizado con éxito. Comparar visualmente la imagen con la copia realizada antes de la ocultación.
4. Extraer el archivo (**background.txt**) y borrarlo del directorio de las imágenes.

Ahora vamos a complicar las cosas algo más:

1. Crear un fichero de texto llamado **mensaje.txt** en el que introduzcamos una palabra. Ocultar **mensaje.txt** en **Madrid.jpg**. Después ocultar **abilities.txt** en **Madrid.jpg** con una clave diferente.
2. Extraer el fichero oculto en **Madrid.jpg**. ¿Qué fichero se obtiene?
3. Ocultar **mensaje.txt** en **SamFisher.jpg**. Ocultar **SamFisher.jpg** en **Madrid.jpg** con una clave distinta. Copiar **Madrid.jpg** a **/home/ubuntu/**.
4. En **/home/ubuntu/** extraeremos el fichero contenido en **Madrid.jpg** (**SamFisher.jpg**). De éste extraeremos **mensaje.txt**.

Cifrado del Sistema de Ficheros

El servidor dispone de un encriptador de sistemas de ficheros llamado **TrueCrypt**, que puede ser arrancado al pinchar en el icono con forma de llave de la barra de aplicaciones.

1. Crear un nuevo volumen con las siguientes características:
   - Disco cifrado en un fichero (**/home/ubuntu/vault1**) con formato **Linux ext4**
   - Volumen estándar (no oculto) de **50 MB** que **no** se permitirá montar en otras plataformas
   - Cifrado con una combinación de **3 algoritmos en cascada**
2. Montar el volumen en **TrueCrypt**, copiar las imágenes que hemos empleado en la parte de steganografía y desmontarlo
3. Crear un nuevo volumen (**/home/ubuntu/vault2/**) con las mismas características del anterior pero con las siguientes excepciones:
   - Volumen **oculto**
   - Usando dos ficheros de contraseña (**keyfiles**) en vez de un texto (las imágenes con las que se ha trabajado antes servirán)