TP OpenPGP / GnuPG - Cifrado y firma digital

Fecha de Entrega: Chivilcoy 14/11/2022 - Luján 21/11/2022.

Objetivo: Conocer la utilización y las implicancias del cifrado simétrico y asimétrico de mensajes, la generación de claves y firmado digital de archivos mediante experiencias con herramientas de cifrado de código abierto utilizadas en el ámbito profesional. Categorías ISO: FCAP**S**.

Bibliografía

- STALLINGS, W. 2011. *Cryptography and Network Security: Principles and Practice.* (5th ed). Prentice Hall
  - Capítulo 1: “Overview”
  - Capítulo 2: “Classical Encryption Techniques”
  - Capítulo 3. Sección 1: “Block Cipher Principles”
  - Capítulo 9. Sección 1: “Principles of Public-Key Cryptosystems”
  - Capítulo 11: “Cryptographic Hash Functions”
  - Capítulo 13. Sección 1: “Digital Signatures”
  - Capítulo 18. Sección 1: “Pretty Good Privacy (PGP)”
- KESSLER, G. 2019. *An Overview of Cryptography*. https://www.garykessler.net/library/crypto.html (bib. de consulta)
- ASHLEY, M. 1999. Capítulo 1: “Primeros Pasos”. En *Guía de “GNU Privacy Guard”.* The Free Software Foundation. https://gnupg.org/gph/es/manual.html#INTRO (bib. de consulta)

Experiencia de laboratorio

ACLARACIÓN: La operatoria con criptografía de clave pública en GnuPG requiere que la fecha y hora de los equipos esté adecuadamente establecida por lo que, como primer requisito, ajuste la fecha y hora de su equipo utilizando el comando `date -s "YYYY-MM-DD HH:mm:ss"` o mediante protocolo NTP (paquete ntpdate).

1. Determine qué servicios de seguridad se proveen **en cada uno** de los siguientes escenarios.
   a. Alicia cifra un mensaje con su clave privada y comparte el mensaje cifrado en Internet.
   b. Alicia cifra un mensaje con su clave pública y comparte el mensaje cifrado en Internet.
   c. Alicia cifra un mensaje con la clave pública de Beto y envía el mensaje cifrado a Beto.
   d. Alicia cifra un mensaje con la clave privada de Beto y envía el mensaje cifrado a Beto.
2. Se le solicita que comparta un archivo con “información confidencial” a un compañero. El medio utilizado para compartir el fichero será el servidor web provisto por el equipo docente (utilice scp para subir el archivo al servidor en cuestion). ¿Se puede impedir que otras personas con acceso al servidor web puedan obtener la información del archivo? ¿Que se requiere? ¿Hay forma alternativa?

Trabajo práctico

1. Determine qué servicios de seguridad se proveen **en cada uno** de los siguientes escenarios. Para ello confeccione una tabla donde las columnas sean: integridad, confidencialidad, autenticidad, no repudio.

   a. Alicia cifra un mensaje con su clave privada y comparte el mensaje cifrado en Internet.
   b. Alicia cifra un mensaje con su clave pública y comparte el mensaje cifrado en Internet.
   c. Alicia cifra un mensaje con la clave pública de Beto y envía el mensaje cifrado a Beto.
   d. Alicia cifra un mensaje con la clave privada de Beto y envía el mensaje cifrado a Beto.
   e. Beto genera un mensaje, obtiene un resumen criptográfico del mismo, cifra el resumen con su clave pública y publica el mensaje y el resumen cifrado en Internet.
   f. Beto genera un mensaje, obtiene un resumen criptográfico del mismo, cifra el resumen con su clave privada y publica el mensaje y el resumen cifrado en Internet.
   g. Alicia cifra un mensaje con su clave privada y luego con la clave pública de Beto, y lo envía a Beto.
   h. Alicia cifra un mensaje con la clave pública de Beto y luego con su clave privada, y lo envía a Beto.

   Para finalizar responda: ¿Son equivalentes los últimos dos casos? Justifique su respuesta.

2. Repita las acciones realizadas en el punto 2 de la experiencia de laboratorio con un archivo de su equipo y verifique que la salida generada en *ARCHIVO.EXT.gpg* es inintelegible. Puede utilizar los comandos `cat` para mostrar el contenido en texto plano o `hd` para obtener el volcado en hexadecimal.

3. Compare el tamaño del archivo original versus el tamaño del archivo cifrado ¿Cuál es mayor? ¿A qué puede deberse la diferencia?

4. Obtenga el listado de algoritmos de digestos soportados por `openssl` ejecutando

   ```
   openssl list --digest-commands
   ```

   Utilizando el comando `openssl NOMBREHASH` , calcule los hashes MD5, SHA256 y SHA512 de un archivo o grupo de archivos. Almacene los resultados en un nuevo archivo de texto.

   Modifique un byte de cualquiera de los archivos como entrada y vuelva a calcular el hash.

5. Descargue y valide la autenticidad de un mensaje de correo:

   1. Descargue el mensaje de correo indicado en el enlace siguiente:

      w3m -dump https://lists.debian.org/debian-security-announce/2022/msg00223.html > mensaje.txt

   2. Abra el archivo con un editor de texto e interprete qué parte del archivo corresponde al mensaje y qué parte corresponde a la firma.

   3. Busque y descargue de la base de claves de Debian la clave pública del desarrollador que redactó el mensaje. Utilice el formulario disponible en https://db.debian.org/

      ```
      wget "https://db.debian.org/fetchkey.cgi?fingerprint=B6E62F3D12AC38495
      C0DA90510C293B6C37C4E36" --output-document moritz.key
      ```

   4. Importe dicha clave pública en GnuPG utilizando el comando

      ```
      gpg --import ARCHIVO_CLAVE.KEY
      ```

5. Valide la autenticidad del mensaje e indique si sufrió alguna alteración.

   ```
   gpg --verify mensaje.txt
   ```

6. Genere un par de claves pública y privada asociadas a su dirección de correo electrónico.
7. Exporte su clave pública y presentela a los docentes personalmente en el próximo encuentro. ¿Por qué es necesario esto?
8. Resuelva las consignas planteadas en los puntos precedentes y realice los pasos necesarios para **firmar** con su clave privada la resolución de este trabajo. Envíe el archivo firmado por correo electrónico a las cuentas de correo de los docentes.

Guia de lectura

1) ¿Cuales son los servicios de seguridad definidos por la recomendación ITU-T X.800?
2) Según el modelo OSI ¿Cuáles son los tres elementos de la arquitectura de la seguridad?
3) ¿Qué mecanismos de seguridad se encuentran definidos en la recomendación X.800 y en que consisten?
4) ¿A grandes rasgos, cuáles son las cuatro distintas políticas de seguridad que se pueden adoptar en un firewall?
5) ¿Cuales son los dispositivos o roles que se pueden definir para proveer mecanismos de seguridad de red y cuales son sus funciones?
6) ¿En qué consiste el concepto de “Seguridad como un Servicio” (Security as a Service)?
7) ¿Cuales son los elementos de la arquitectura de un sistema de cifrado simétrico ?
8) ¿Que ventajas y desventajas tienen los algoritmos de cifrado simétricos vs los algoritmos asimétricos?
9) ¿Porqué no se recomienda la seguridad por oscuridad?
10) ¿Cuales son los dos tipos de ataques se pueden pueden realizar a un algritmo de encriptación?
11) ¿Qué mecanismos existen para asegurar la integridad de los datos?

Referencias adicionales

- RFC 4880 OpenGPG Message Format. Section 2: General functions. Nov 2007.
  https://tools.ietf.org/html/rfc4880#section-2
- X.800 : Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT
  https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.800-199103-I!!PDF-S&type=items
  https://www.itu.int/rec/T-REC-X.800-199103-I/es

Anexo OpenPGP

Cifrar un archivo simétricamente

```
gpg --symmetric --cipher-algo ALGORITMO ARCHIVO.EXT
```

ALGORITMO es alguno de los algoritmos simétricos soportados por la aplicación, y *ARCHIVO.EXT* es el nombre que usted dio al archivo elegido.

El archivo resultande se almacena en el directorio de trabajo con el nombre ARCHIVO.EXT.gpg

Descifrar un archivo cifrado (simétrica o asimétricamente)

```
gpg ARCHIVO.EXT.gpg
```

Si en el paso de cifrado se utilizó la opción `-a` debe volver a utilizarse al momento de descifrar.

Generar par de claves asimétricas

```
gpg --gen-key
```

Complete los datos con su nombre y dirección de correo electrónico. Por ejemplo:

```
Nombre y apellidos: SU NOMBRE
Dirección de correo electrónico: SU-EMAIL@DOMINIO.COM
Frase de contraseña: escriba una frase
(esta clave protege la clave privada y será requerida para firmar o cifrar un documento)
```

Las claves de GnuPG se almacenan en el directorio `.gnupg` dentro del directorio del usuario. El archivo `pubring.gpg` (o `pubring.kbx`) contiene la clave pública propia y las de terceros. Las claves secretas se almacenan en el directorio `private-keys-v1.d` .

Exportar claves públicas propias

```
gpg --export -a SU-EMAIL@DOMINIO.COM
```

Importar claves públicas de un tercero

```
gpg --import ARCHIVO.DE.CLAVE
```

Listar claves conocidas

```
gpg --list-keys
```

Cifrar un archivo asimétricas

```
gpg --encrypt --recipient DESTINATARIO@DOMINIO.COM ARCHIVO.EXT
```

Fimar digitalmente un archivo de texto plano

```
gpg -u SUEMAIL@DOMINIO.COM --clearsign ARCHIVO.TXT
```

El archivo resultande se almacena en el directorio de trabajo con el nombre ARCHIVO.EXT.ASC

Fimar digitalmente un archivo binario (imagen, pdf, etc)

```
gpg -u SUEMAIL@DOMINIO.COM --sign ARCHIVO.EXT  (-sa para utilizar ASCII de 7 bit)
```

Cifrar y firmar digitalmente un archivo

```
gpg -es -u SUEMAIL@DOMINIO.COM --recipient DESTINATARIO@DOMINIO.COM ARCHIVO.EXT
```