GnuPG

Una introducción

Unai Zalakain

http://unaizalakain.info/talks/gpg.pdf

Jornadas de Tecnología y Cultura Libre,
Junio 2016

Índice

Qué es

- software criptográfico
- software libre
- permite cifrar [confidencialidad]
- permite firmar [autenticación, integridad, no repudio]
- permite crear redes de confianza
- interfaz de línea de comandos
- multitud de interfaces gráficas
- integración con clientes de correo
- integración con gestores de contraseñas

Cifrado simétrico

- texto plano $\leftarrow$ clave $\rightarrow$ texto cifrado
- quien puede cifrar, puede descifrar
- todas las partes necesitan conocer la clave común

Cifrado asimétrico

- texto plano — clave pública destinatario → texto cifrado
- texto cifrado — clave privada destinatario → texto plano
- cualquiera que posea la clave pública puede cifrar
- solo quien posea la clave privada puede descifrar
- se puede cifrar para múltiples claves privadas

Firmas digitales

- texto plano — clave privada emisor → texto firmado
- texto firmado — clave pública emisor → texto plano
- solo quien posea la clave privada puede firmar
- cualquiera que posea la clave pública puede comprobar

Redes de confianza

- firma digital de una clave con otra
- certificación de que la clave firmada pertenece a la persona mencionada
- la confianza puede ser transitiva: red de confianza
- *firmar solamente aquellas identidades de las que se esté absolutamente segura*
- confianza inversamente proporcional a la longitud de la cadena de firmas entre dos claves
- confianza proporcional al número de caminos sin escalafones comunes entre dos claves
- *strong set*: la mayor red de confianza interconectada pública

Keysigning Parties

- antes:
  1. enviar clave pública propia a la coordinadora
- durante:
  1. verificar información sobre la clave pública propia
  2. verificar información sobre las claves públicas de las demás
  3. verificar identidad de las demás
- después:
  1. firmar digitalmente las claves públicas verificadas
  2. enviar las claves públicas firmadas digitalmente a sus dueñas
  3. recibir la clave pública propia firmada digitalmente por las demás
  4. subir la clave pública propia firmada digitalmente por las demás a los servidores

Subclaves

- clave maestra representa identidad
- firmas digitales, cifrado y autenticación delegadas a subclaves
- subclaves firmadas digitalmente por clave maestra
- clave maestra puede mantenerse separada y segura
- clave maestra solo necesaria para operaciones inusuales:
  - modificación de claves
  - firmas digitales de claves de otras
  - generación de certificados de revocación
- subclaves pueden ser revocadas sin afectar identidad principal

Creando una clave

```
gpg2 --full-gen-key
```

1. seleccionar `RSA and RSA`
2. seleccionar 4096 como tamaño
3. fijar fecha de expiración
4. proteger con una frase de paso fuerte
5. certificado de revocación generado automáticamente

Añadiendo una subclave para firmas digitales

```
gpg2 --edit-key sixto.rodriguez@riseup.net
```

```
addkey
```

```
save
```

1. seleccionar `RSA (sign only)`
2. seleccionar 4096 como tamaño
3. fijar fecha de expiración

Añadiendo una identidad

```
gpg2 --edit-key sixto.rodriguez@riseup.net
```

```
adduid
```

```
save
```

1. seleccionar `RSA (sign only)`
2. seleccionar 4096 como tamaño
3. fijar fecha de expiración

Listando claves

- públicas

  `gpg2 -k`

- privadas

  `gpg2 -K`

Creando un certificado de revocación

```
gpg2 --gen-revoke sixto.rodriguez@riseup.net
```

Guardando una copia de seguridad

```
umask 077
gpg2 --export-secret-keys --armor > secret.gpg
gpg2 --export-keys --armor > public.gpg
```

Transfiriendo la clave maestra

- GPG2 guarda cada clave secreta en un fichero distinto
- pueden obtenerse los nombres de los fichero con:

```
gpg2 -K --with-keygrip
```

- los ficheros se encuentran en

```
${GNUPGHOME}/private-keys-v1.d/<keygrip>.key
```

- añadir/quitar fichero con clave secreta

Cifrando y descifrando

```
echo "Ping" | \
gpg2 -e -a -r sixto@rodriguez@riseup.net | \
gpg2 -d
```

Firmando y comprobando

```
echo "Ping" | gpg2 -s -a | gpg2 -v
```

Servidores de claves

```
echo "keyserver hkps://hkps.pool.sks-keyservers.net" >> \
    ${GNUPGHOME}/gpg.conf
gpg2 --send-keys 0BAA856A317CD58B302BFAAD8A5015B1CCB5CBDE
gpg2 --search-key unai@gisa-elkartea.org
gpg2 --recv-keys 4B3F515D76ADA88FA8B5247BF1DB723A779DD1F7
```

Verificando una clave

```
gpg2 --sign-key unai@gisa-elkartea.org
gpg2 -a --export unai@gisa-elkartea.org > signed.key
# Enviar signed.key al correo mencionado en la clave
```

Consejos útiles I

- firmar públicamente solamente aquellas claves a las que no nos importe estar públicamente relacionadas
- mantener la clave maestra privada separada y segura
- comunicarse con los servidores de claves sobre HKPS (HKP sobre TLS)
- comunicarse con un pool de servidores
- evitar descargar una clave de un servidor especificado por dicha clave

Consejos útiles II

- asegurarse del fingerprint de las claves descargadas
- generar certificados de revocación
- especificar fecha de expiración
- especificar preferencias de algoritmos de cifrado fuertes
- enviar claves firmadas por correo a su dueño en vez de subirlas a los servidores

Software de interés I

gnupg2	más completo y con una mejor interfaz
gnupg-agent	gestor de claves privadas
gnupg-curl	soporte para HKPS
guncat	descifra texto parcialmente cifrado
pius	firma y envía por correo un grupo de claves
kgpg	GUI para GPG

Software de interés II

pass	gestor de contraseñas cifradas con GPG
qtpass	GUI para pass
PassFF	rellenado de formularios en Firefox a través de pass

Software de interés III

icedove	cliente de correo
enigmail	addon para cifrado con GPG para icedove
claws-mail	cliente de correo
claws-mail-smime-plugin	addon para cifrado con GPG para claws-mail

Referencias I

- *Creating the perfect GPG keypair*. URL: https://alexcabal.com/creating-the-perfect-gpg-keypair/.
- *GnuPG Keysigning Party HOWTO*. URL: https://www.rubin.ch/pgp/kspa/gpg-party.en.html.
- *OpenPGP Best Practices*. URL: https://help.riseup.net/en/gpg-best-practices.
- *PGP Web of Trust: Core Concepts Behind Trusted Communication*. URL: https://www.linux.com/learn/pgp-web-trust-core-concepts-behind-trusted-communication.
- *Subkeys*. URL: https://wiki.debian.org/Subkeys.

Referencias II

- *The GNU Privacy Handbook*. URL: https://www.gnupg.org/gph/en/manual.html.

Reforcemos la red de confianza!

1. exportar la clave pública

   ```
   gpg2 -a --export > public.key
   ```

2. subir la clave pública a `http://biglumber.com/x/web?keyring=891`
3. acudir a la keysigning party

Esta presentación se puede encontrar en:

`http://unaizalakain.info/talks/gpg.pdf`