El software criptográfico GnuPG

Jacobo Tarrío Barreiro
<jtarrio@alfa21.com>

Historia de GnuPG

- Basado en PGP (de Philip Zimmermann, 1990)
- Zimmermann tiene problemas con el gobierno USA
  - Artefactos criptográficos clasificados como armas
    - Exportación limitada
  - Se "exportan" copias de PGP
- La solución pasa por vender PGP a una empresa
- Se crea GnuPG (1999) para tener un programa criptográfico libre

Cómo es una clave GnuPG

- Formada por una clave DSA (para firmar) y una ElGamal (para cifrar)
- La clave tiene asociados unos ID de usuario
- Los ID de usuario van firmados por la propia clave y, tal vez, otras claves
- Físicamente se divide en dos ficheros: clave secreta (cifrado) y clave pública

Generación de claves

- Generación de un par:
  - gpg --gen-key
- Generación de un certificado de revocación:
  - gpg --gen-revoke UID
  - Útil por si se pierde la clave secreta o la contraseña de la clave

Cómo cifra GnuPG

- GnuPG calcula una clave aleatoria
- Cifra el mensaje utilizando un método de clave secreta, con esa clave
  - AES, 3DES, Blowfish, CAST5, Twofish
- Cifra esa clave usando un método de clave pú blica
  - DSA, RSA
- Une la clave cifrada, el mensaje cifrado, y los empaqueta

Cifrado de mensajes

- Cifrado:
  - gpg --encrypt FICHERO
- Cifrado con armadura ASCII:
  - gpg --encrypt --armor FICHERO
- Descifrado (salida por pantalla):
  - gpg --decrypt FICHERO
- Descifrado (salida en fichero):
  - gpg FICHERO

Cómo firma GnuPG los mensajes

(o los ficheros)

- Calcula un hash del mensaje a firmar
  - MD5, RIPEMD/160, SHA-1, SHA-256, SHA-384, SHA-512
- Cifra el hash con la clave secreta del usuario que firma
- Añade el hash cifrado al mensaje

Firma de mensajes

- Firma de un texto:
  - gpg --sign [--armor] FICHERO
- Firma de texto claro:
  - gpg --clearsign [--armor] FICHERO
- Firma en un fichero separado:
  - gpg --detach-sign [--armor] FICHERO
- Comprobación de una firma:
  - gpg FICHERO

Intercambio de claves

- Se necesita tener la clave pública de alguien para enviarle un mensaje cifrado o para verificar un mensaje firmado
- Existen diversos métodos para obtenerla:
  - Grabándola en un fichero
  - A través de un servidor de claves
- Problema: ¿seguro que la clave es de quien dice ser?

Importación/exportación de claves

- Importar una clave pública:
  - gpg --import FICHERO
- Exportar una clave pública:
  - gpg --export [--armor] UID > FICHERO
- Listar claves disponibles:
  - gpg --list-keys [UID]
- Recibir una clave de un servidor de claves:
  - gpg --keyserver SERVIDOR --recv-keys UID
- Enviar una clave a un servidor de claves:
  - gpg --keyserver SERVIDOR --send-keys UID
- Buscar una clave en un servidor:
  - gpg --keyserver SERVIDOR --search-keys UID

Validez de una clave pública

- GnuPG establece una red de confianza
- Los usuarios firman los ID de usuario asociados a una clave
- Cada usuario indica cuánto confía en las firmas de otras personas
  - Esto aumenta la extensión de la red de confianza

Firma de claves

- Obtener "fingerprint":
  - gpg --fingerprint UID
- (Comparar fingerprint)
- Firmar clave:
  - gpg --sign-key UID
- (Exportar clave o enviar a servidor de claves)
- Ver firmas de una o varias claves:
  - gpg --list-sigs [UID]
- Editar confianza:
  - gpg --edit-key UID
  - (comando trust)

Uso de GnuPG en Debian

- Voto en línea
  - Mensajes firmados y cifrados
- Autenticidad de paquetes
  - Ficheros firmados
- Avisos de seguridad
  - Mensajes firmados
- Red de firmas "Debian"
  - Excusa para ir a "botellones Linux" ;-)

Datos útiles

- Sitio web de GnuPG
  - http://www.gnupg.org/
- Compatible con OpenPGP
- Servidores de claves
  - keys.gpul.org
  - pgpkeys.mit.edu
  - keyring.debian.org
- Mi ID de clave
  - 0x149cddb2
  - (para fingerprint, preguntar personalmente)