Comunicaciones Seguras

Correo Electrónico Encriptado

Rafael Bonifaz: rafael@bonifaz.ec

Correo electrónico

- Es uno de los sistemas de comunicación más antiguos de Internet
- Ampliamente utilizado
- Existen protocolos como Pop3, Imap y SMTP
- La mayoría de gente usa Webmail

Problemas de Privacidad

- Cuando se usa webmail o Imap, el correo se almacena en el servidor
- El administrador del servidor podría leer el correo
- Si se compromete la cuenta, se comprometen TODOS los correos en el servidor
- El correo viaja como texto plano y podría ser interceptado en el camino
- Con cifrado

PGP y GPG

- PGP: Pretty Good Privacy
- Diseñado por Phil Zimmermann en 1991
- OpenPGP se convirtió en un estándar IETF
- GNU PG es la implementación libre de PGP creado por la FSF

Llave pública y llave privada

- Llave pública
  - Se la publica en Internet
  - Se utiliza para encriptar mensajes
  - Se utiliza para validar la firma electrónica para autenticar el mensaje
- Llave privada
  - Es una clave que no se debe compartir
  - Se utiliza para desencriptar mensajes
  - Se utiliza para firmar un correo de forma digital

Correo electrónico de forma local

“Si quien controla el pasado, controla el futuro, ¿Quien controla el presente, controla el pasado”

George Orwell

- Cuando se usa un correo electrónico se suele almacenar el correo en Internet
- ¿Quién puede leer ese correo?
- ¿Qué pasaría si mi cuenta es comprometida?
- Se pueden descargar las cuentas de correo electrónico incluso con proveedores tipo PRISM

Thunderbird/Icedove y Enigmail

- Thunderbird es un cliente ampliamente utilizado de correo electrónico para protocolos POP3, IMAP y SMTP
  - IMAP → sincroniza servidor y cliente
  - POP3 → descarga correos y los borra del servidor
  - SMTP → envía correos
- Enigmail es un complemento que permite utilizar PGP en Thunderbird
- Permite crear y administrar las llaves públicas y privadas
- Se puede instalar desde repositorio o como complemento de Thunderbird/Icedove
- http://rafael.bonifaz.ec/blog/2013/10/encriptar-correos-con-pgp/

Tor y Torbirdy

- Torbirdy mejora la seguridad al utilizar Tor y algunas otras personalizaciones
- Si se va a probar Torbirdy se recomienda arrancar Thunderbird/Icedove desde la línea de comando con la opción –**P**
- También se puede usar Thunderbird/Icedoce con **torify**
- Se puede instalar desde repositorio o como complemento de Thunderbird/Icedove

```
$ torify icedove
```

¿Cómo compartir la llave pública?

- La llave pública es un archivo de texto que se debe compartir con quién nos queremos comunicar
- Se puede hacer por correo con ciertos riesgos
- Se puede subir a servidores públicos con otros riesgos
  - Cuando se sube a un servidor público se utiliza el certificado de revocación
- Se utiliza una “huella digital” de 40 caracteres para validar la llave pública
  - El identificador de la clave son los últimos 8 caracteres, pero no se debe usar
  - https://evil32.com/

Firma de llaves y red de confianza

- Las llaves públicas pueden ser firmadas por llaves privadas de otras personas
- Si Alicia firma la llave de Bob esta diciendo que conoce Bob y verificó su llave
- Juan conoce a Alicia, pero no a Bob y quiere comunicarse con Bob
- Si Juan confía en Alicia, puede verificar la clave pública de Bob porque esta fue firmada por Alicia
- Mientras más conocidos han firmado la clave de Bob mayor seguridad tendrá Juan de que se comunica con quien se quiere comunicar