

PGP y GPG

I Jornadas Seguridad GNU/Linux

Jose Miguel Garrido (AugCyL)

Problema:

EL CORREO ELECTRONICO NO ES SEGURO

- Administradores
 - Sniffers
- Echelon, Carnivore e Infopol
- ... y miles de problemas mas

Problema:

El correo electronico no garantiza:

Privacidad

○ ¿Quien ha leído el mensaje?

Autenticidad

○ ¿Quien me envia el mensaje?

Integridad

○ ¿Esta el mensaje manipulado?

Soluciones

S/Mime

- Basado en X 509

- Ventajas

- Integrado con Explorer y Netscape

- Desventajas

- Integrado con Explorer y Netscape

- Necesario certificado

- Posible uso de 40 bits

- No hay implementaciones libres, ni siquiera código fuente

Soluciones

OpenPGP (RFC 2440)

□ PGP o GPG

¿Que es PGP?

Aplicacion para usuarios

Garantiza

- Privacidad
- Autenticidad e integridad

Cifrado hibrido

Historia de PGP

PGP Pretty Good Privacy

Creado por Phil Zimmermann en 1991

- Version 1 -> Totalmente insegura

- Version 2.6 -> RSA e IDEA

- Version 5 -> DH, DSA y CAST

- Version 7.03

PGP y NAI

1997: PGP fue comprado por Network Associates

- Orientacion a Windows
- Codigo fuente restringido
- Ni siquiera Zimmermann puede revisarlo

2001: Phil Zimmernmann se centra en OpenPGP

GPG

Gnu Privacy Guard

Implementacion libre de OpenPGP

Proyecto oficial de GNU

Instalado por defecto en muchas distribuciones.

Necesaria version > 1.06

Creacion de claves

Creacion de la clave

- `gpg --gen-key`

Certificado de revocacion

- `gpg --output XX.rev --gen-revoke XX`

Intercambio de claves

Exportacion

- `gpg --armor --output XX.gpg.asc --export XX`

Importacion

- `gpg --import XX.gpg.asc`

Verificar huella dactilar

- `gpg --fingerprint XX`

Cifrar documentos

□ Cifrar

- `gpg --armour --output doc.asc --encrypt --recipient XX@ doc.txt`

□ Descifrar

- `gpg --output doc --decrypt doc.asc`

Firmar documentos

Firma normal

- `gpg --output doc.firm --sing doc`

Resultado como texto

- `gpg --output doc.asc --clearsign doc`

Firma acompañante

- `gpg --output doc.sig --detach-sing doc`

Comprobar firma

- `gpg --verify doc.asc`

Cifrar y firmar

□ `gpg --armor --output XX.pgp --encrypt --recipient XX@
--sig doc`

Gestion de claves

Anillo de confianza

- "Los amigos de mis amigos pueden ser mis amigos"
- Mecanismo alternativo a la certificacion
- No requiere autoridad de certificacion

Niveles de confianza

unkown (-) Por defecto

none (q) Se sabe que lo hace mal

marginal (m) El otro sabe firmar

full (f) Es como si fuera yo mismo

Algoritmo de clave valida

1 Si viene firmada por suficientes claves validas

- o la hemos firmado nosotros
- o firmada por algien con "full"
- o por varios con "marginal"

2 Y el camino es de 5 pasos o menos

Key sign party

Reunion en la que los participantes comprueban mutuamente su identidad y se firman las claves.

Servidores de claves

Enviar clave

- `gpg --keyserver servidor.net --send-key XX`

Recibir

- `gpg --keyserver servidor.net --recv-key XX`

Referencias

Pagina oficial GPG: www.gnupg.org

Kriptopolis: www.kriptopolis.com

PGP internacional: www.pgpi.com

Phil Zimmermann: web.mit.edu/~prz