Envío y recepción de datos de forma segura Paper

Matías Lugo

Víctor Zanardi

Darío Gutiérrez

Universidad Nacional de Quilmes
Buenos Aires, Argentina
victorh.zanardi@gmail.com
matilugo04@gmail.com
dariofg93@gmail.com

En el presente informe, daremos una breve explicación sobre el problema planteado, los riesgos al compartir archivos en internet, maneras en las que estos archivos pueden cifrarse y descifrarse (simétrica y asimétricamente) y también se mostrara como aplicar estos conceptos a través de una tecnología (PGP).

In this report, we will give a brief explanation of the problem posed, the risks of sharing files on the Internet, ways in which these files can be encrypted and decrypted (symmetrically and asymmetrically) and also show how to apply these concepts through technology (PGP).

I. Cual es el problema?

Hoy en día, gran parte de la comunicación en Internet se lleva a cabo a través de la difusión de mensajes en las redes sociales y en los servicios de mensajería instantánea, sin olvidar que el correo electrónico también forma parte de la comunicación interactiva. Sobre todo cuando se trata de la transmisión de **información confidencial** como contratos, datos bancarios, etc., el correo electrónico es el medio más utilizado, e incluso muchas empresas hacen de este servicio su medio de comunicación interno. Por ello, lo que interesa es proteger la información sensible e impedir que se lea el contenido de los correos enviados. Los criminales que quieren acceder a los datos privados de los usuarios o los servicios secretos que buscan información se benefician de los mensajes que se envían sin codificar. El cifrado de la información se convierte, de esta manera, en un proceso necesario para evitar que personas no autorizadas puedan leer correos electrónicos ajenos.

A. Algunos robos informáticos

"El único sistema verdaderamente protegido es aquel que está apagado, encerrado en un bloque de hormigón y sellado en una habitación forrada de plomo con guardias armados – y aun así tengo mis dudas". Corría el año 1989 cuando el profesor y reputado experto en seguridad informática Gene Spafford realizo esta llamativa reflexión.

Se trata de una exageración, con la que probablemente pretendía lanzar un toque de atención a la sociedad en general sobre la escalada imparable de los delitos informáticos. ¿Pero somos realmente conscientes de los peligros a los que estamos expuestos en la era del todo conectado e informatizado?

La mejor forma de responder esta pregunta es repasar algunos de los robos informáticos más importantes de la historia:

- En 2005 un joven Cameron Lacroix accedió a la cuenta de Paris Hilton en los servidores de T-Mobile asociados a sus terminales Sidekick en los que se guardaban desde la agenda de contactos, hasta los videos pasando por las fotos de los usuarios, incluidas las de la *celebrity*. Una vez que tuvo acceso, Lacroix sustrajo varias imágenes subidos de tono de Hilton, su directorio telefónico y publico todo en Internet. Si bien la información robada no es muy relevante, el hackeo en si lo es porque sentó las bases para los muchos parecidos que vendrían después.
- En 2010 se hicieron públicas varias incursiones más dignas de consideración que terminaron con el robo de información protegida. De lo más sonado fue la sustracción cometida por Aaron Swartz de unos cuatro millones de documentos y aplicaciones bajo copyright del repositorio digital de publicaciones académicas JSTOR a través de las redes del MIT.
- También fue conocida el hurto de certificados digitales a la empresa Realtek, de no mucho volumen pero "bastante serio" porque "utilizando este certificado robado misteriosamente a Realtek se consigue llevar a cabo el ataque de Stuxnet contra las centrales de centrifugación de uranio de Natanz".

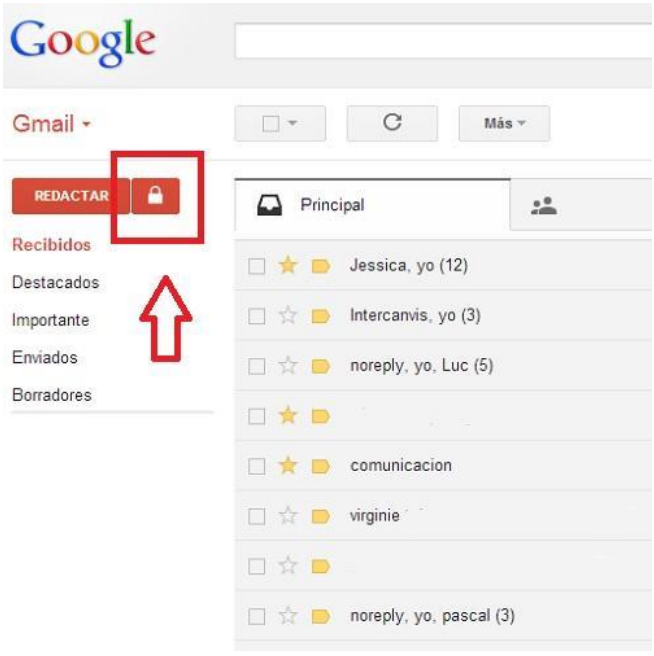
II. Protocolo pgp: Protege tu privacidad mediante el uso de claves

El protocolo PGP ofrece la posibilidad de proteger y cifrar la información transmitida a través del correo electrónico. PGP son las siglas en ingles de Pretty Good Privacy, o lo que en español podría definirse como "privacidad bastante buena" y originalmente se usó para denominar un programa desarrollado por Phil Zimmermann en 1991 y que a lo largo de los años se ha generalizado para describir el método de encriptado que utiliza este software.

El cifrado más importante es el asincrónico, el cual tiene un funcionamiento que consta de la asignación de un par de claves: una privada y otra pública. La clave pública se pone a disposición de los contactos de correo potenciales bien comunicándosela o cargándola en un key server externo. Con esta clave estos contactos pueden cifrar los mensajes electrónicos que quieran enviarte. La clave privada, en cambio, es de tu propiedad y está protegida por una contraseña. Con ella podrás descifrar los correos electrónicos entrantes previamente cifrados con la clave pública. Para establecer una comunicación segura siguiente este proceso, será necesario que tu interlocutor también haga uso del protocolo PGP y te informe acerca de su clave pública. El sistema de cifrado asimétrico, ya que ambos interlocutores usan una clave diferente. Con la ayuda de la firma electrónica se garantiza, de manera adicional, la autenticidad de los mensajes que se envían.

La cantidad de pasos necesarios para llevar a cabo la configuración ha hecho que solo unos pocos usuarios instruidos en la materia se hayan decidido a usar dicho software. Sin embargo, para que un mayor número de personas pueda dotar de seguridad a sus correos electrónico, estas tienen a su disposición algunos plugins como OutlookPrivacyPlugin, Mailvelope o Secure Gmail.

.



III. El contexto

A. *GnuPG*

Tenemos que saber que es GnuPG (GNU Privacy Guard) es un derivado libre de PGP y su utilidad es la de cifrar y firmar digitalmente, siendo además multiplataforma.

Usaremos el que ya viene incorporado en muchos sistemas Linux.

B. *Anillo de claves*

GPG tiene un repositorio de claves(anillo de claves) donde guarda todas las que tenemos almacenadas en nuestro sistema, ya sean privadas o públicas, con la clave pública ciframos un mensaje que solo podrá descifrar el que posee la clave privada.

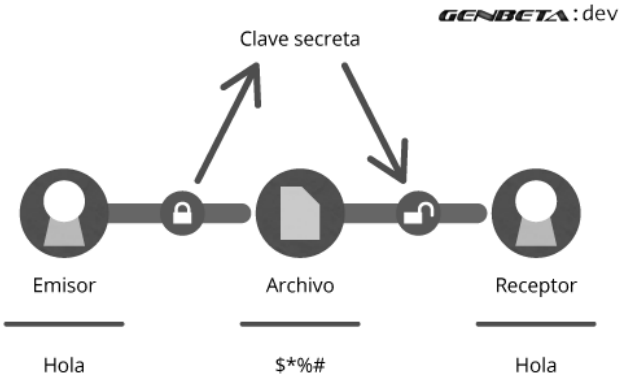
Más adelante cuando veamos un anillo de claves debemos de recordar que pub hace referencia a la clave pública y sub hace referencia a la privada.

C. *Servidores de claves*

Para que nos cifren un mensaje tenemos que compartir la clave pública de nuestro para de claves para cifrar, y como es un poco engorroso difundir una clave a muchas personas existen servidores de claves PGP (compatibles con GPG), donde subiré una clave pública para el que quiera probar los ejemplos. Unos ejemplos de servidores son: pgp.rediris.es ó pgp.mit.edu.

IV. Cifrar y descifrar archivos

A. *Cifrado Simétrico*



Como es conocido el cifrado simétrico es el tipo de cifrado más sencillo que hay, es más rápido de procesar y por desgracia menos seguro que el cifrado asimétrico.

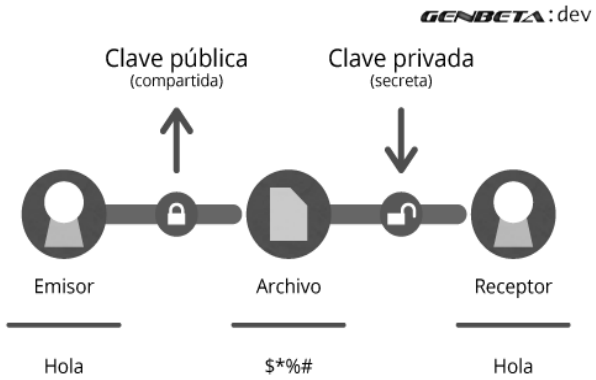
Para empezar la prueba tenemos que tener un archivo de cualquier tipo e introducir en la termina de Linux el comando con gpg con el parámetro –c para cifrar y –d para descifrar.

```
losDelFondo@ubuntu:~/gpg$ echo "Genbeta
Dev" > texto.txt

losDelFondo@ubuntu:~/gpg$ gpg -c
texto.txt
```

Tras crear un archive de texto usamos el comando gpg –c [archivo], nos aparecerá un cuadro que nos pide la contraseña y se generara un archivo .gpg. Después lo descifraremos con el comando gpg –d [archivo] (e introduciendo la clave de alta seguridad).

```
losDelFondo@ubuntu:~/gpg$ gpg -d
texto.txt.gpg

gpg: datos cifrados CAST5

gpg: cifrado con 1 frase contraseña

Genbeta Dev

gpg: AVISO: la integridad del mensaje no
está protegida
```

B. *Cifrado Asimétrico*



Generar las claves: Para poder cifrar asimétricamente primero tenemos que crear la pareja de claves (pública y privada) con el comando gpg --gen-key.

```
losDelFondo@ubuntu:~/gpg$ gpg --gen-key

gpg (GnuPG) 1.4.11; Copyright (C) 2010
Free Software Foundation, Inc.

This is free software: you are free to
change and redistribute it.

There is NO WARRANTY, to the extent
permitted by law.

Por favor seleccione tipo de clave
deseado:

   (1) RSA y RSA (predeterminado)

   (2) DSA y Elgamal

   (3) DSA (sólo firmar)

   (4) RSA (sólo firmar)

¿Su selección?:
```

GPG nos permite elegir el tipo de clave que queremos usar, hay opciones que solo permiten firmar y otras que permiten firmar y cifrar, en este caso usaremos DSA y Elgamal.

```
las claves DSA pueden tener entre 1024
y 3072 bits de longitud.

¿De qué tamaño quiere la clave? (2048)
```

Nos pide el tamaño de la clave que puede variar entre 1024 bits y 3072, la fecha en la que expirara, información del emisor de la clave (nombre, mail y datos extra que queramos dar) y finalmente la contraseña que salvaguarda la clave.
Tras generar las claves podemos verlas con el comando gpg -k.

```
losDelFondo@ubuntu:~/gpg$ gpg -k

/home/losDelFondo/.gnupg/pubring.gpg

------------------------------

pub   2048D/18384645 2013-01-23

uid      Pedro Gutiérrez (Manual GPG -
Genbeta Dev) <info@xitrus.es>

sub   2048g/C4A9EA7A 2013-01-23
```

Exportar y enviar la clave privada: El objetivo de esta pareja de claves es que cualquiera pueda mandar un archivo cifrado que solo veremos nosotros y esto se hace difundiendo la clave pública que acabamos de crear (la pública, **nunca** la privada), para exportarla en un archivo usaremos el comando gpg --output [archivo destino] --export [ID de la clave pública] (la clave pública generada antes tiene la ID 18384645).

```
losDelFondo@ubuntu:~/gpg$ gpg --output
CPub.gpg --export 18384645

losDelFondo@ubuntu:~/gpg$ ls

CPub.gpg
```

Este archive ahora se puede difundir por el medio que queramos, el único problema que tendremos en cuenta es que alguien se hiciese pasar por otro al mandarnos un mensaje, para eso el que nos envíe algo lo debería firmar (si fuese pertinente).

Subir una clave pública a un servidor de claves: Los servidores de claves suelen ser de acceso público (al no haber mucho problema por difundir una clave pública) y en este caso subiremos una clave a los servidores del **MIT (**gpg.mit.edu**)** usando el comando gpg --send-keys --keyserver [Dirección del servidor] [ID de la clave pública]

```
losDelFondo@ubuntu:~/gpg$ gpg --send-
keys --keyserver pgp.mit.edu 18384645

gpg: enviando clave 18384645 a hkp
servidor pgp.mit.edu
```

Importar la clave desde el archivo o servidor de claves: Para poder usar la clave pública para cifrar o comprobar la identidad del remitente tenemos que importar previamente la clave, desde un archivo debemos de usar el comando gpg –import [Archivo de la clave pública] (el que hemos descargado anteriormente).

```
losDelFondo@ubuntu:~/gpg$ gpg --import
CPub.gpg

gpg: clave 18384645: «Pedro Gutiérrez
(Manual GPG - Genbeta Dev)
<info@xitrus.es>» sin cambios

gpg: Cantidad total procesada: 1
```

Para realizar la importación desde el servidor tenemos que usar el comando gpg –keyserver [Dirección del servidor] –recv-keys [ID de la clave].

```
losDelFondo@ubuntu:~/gpg$ gpg --
keyserver pgp.mit.edu --recv-keys
18384645

gpg: solicitando clave 18384645 de hkp
servidor pgp.mit.edu

gpg: clave 18384645: «Pedro Gutiérrez
(Manual GPG - Genbeta Dev)
<info@xitrus.es>» sin cambios

gpg: Cantidad total procesada: 1
```

Cifrar con la clave pública: Finalmente, para cifrar el documento usaremos el comando gpg --encrypt –recipient [ID de la clave] [Archivo].

```
losDelFondo@ubuntu:~/gpg$ echo "Genbeta
Dev" > documento.txt

losDelFondo@ubuntu:~/gpg$ gpg --encrypt
--recipient 18384645 documento.txt

losDelFondo@ubuntu:~/gpg$ ls

documento.txt documento.txt.gpg
```

Descifrar un archivo con la clave privada: Y ahora es el momento de descifrar con nuestra clave privada el documento tras recibirlo, con el comando gpg –d [Archivo] e introduciendo la contraseña que creamos para salvaguardar la clave privada.

```
losDelFondo@ubuntu:~/gpg$ gpg -d
documento.txt.gpg

Necesita una frase contraseña para
desbloquear la clave secreta

del usuario: "Pedro Gutiérrez (Manual
GPG - Genbeta Dev) <info@xitrus.es>"

clave ELG-E de 2048 bits, ID C4A9EA7A,
creada el 2013-01-23 (ID de clave
primaria 18384645)

gpg: cifrado con clave ELG-E de 2048
bits, ID C4A9EA7A, creada el 2013-01-23

      «Pedro Gutiérrez (Manual GPG -
Genbeta Dev) <info@xitrus.es>»

Genbeta Dev
```

Y el resultado lo muestra a continuación, aunque si queremos especificar una salida podemos usar el parámetro –o [Archivo de salida].

Links and Bookmarks

Toda la información fue obtenida de distintos websites [1], [2], [3], [4].

V. Conclusion

Muchos usuarios piensan que ya intercambian email cifrados con sus contactos únicamente con protocolos SSL y TSL, pero no es del todo cierto. A través del uso de dichos certificados solo **se cifra el trayecto de transmisión de los mensajes electrónicos**, lo que tiene el inconveniente de permitirle a terceros a acceder a ellos y leerlos. Lo bueno es que posibilitan el cifrado de los componentes de correo electrónico que PGP no ha cifrado. La solución ideal, en la práctica, es la protección de cifrado de ambas tecnologías.

Pero si crees que con esto puedes dormir tranquilo, estas equivocado. Los robos informáticos expuestos al principio del Paper no conforman ni el 1% de todos los delitos informáticos de la historia. Lo mejor que se puede hacer para estar seguros es contar con las medidas básicas.

Acknowledgment

A toda la comunidad que investiga y comparte sus conocimientos y a los servicios de internet que se ocupan de hacer llegar la información.

References

[1] https://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura Post de Usuario Pedro Gutiérrez, website: GenvetaDev, Ene. 2013.

[2] https://www.1and1.es/digitalguide/correo-electronico/seguridad-correo-electronico/pgp-o-como-cifrar-correos-electronicos/ Artículo, website: 1&1 España, Oct. 2016.

[3] https://tecnologia.uncomo.com/articulo/como-cifrar-un-correo-electronico-en-gmail-19941.html Post de Judith Tirado, website: uncomo.

[4] http://www.eldiario.es/turing/Grandes-robos-informaticos-historia_0_132986921.html Artículo publicado por Elías Notario, website: elDiario, Mayo. 2013.