

APUNTES

de

AUTODEFENSA DIGITAL



Sumario

3 Introducción

4 Identificaciones

4 Las VPN

5 Navegar con Tor Browser Bundle

5 Los servidores autogestionados

5 Anonimizar los ficheros

6 Interceptaciones

6 Cifrar los correos con GPG

7 Thunderbird + Enigmail, GPG Suite y GPG4Win

7 HTTPS Everywhere

8 Chatear con Pidgin y OTR

9 Secuestros

9 Cifrar con Mac: FileVault y FileVault2

10 Cifrar con Linux: luks con Genome Disk Utility y VeraCrypt

10 Borrar ficheros

10 Borrar ficheros con Linux: secure-delete y wipe

11 Borrar ficheros con Windows: eraser

12 Intrusiones

12 Malware de estado

13 Soluciones especiales

13 Tails

13 Freepto

14 Contraseñas

15 Quiénes somos

16 Nuestros propósitos

17 Apuntes...

Introducción

Generalmente consideramos Internet como el lugar donde podemos exponer libremente nuestras ideas, compartir imágenes y vídeos, construir debates y relaciones políticas con otras personas sin tener miedo a la represión, porque “Internet por sí misma es una herramienta libre”. Pero esto no es cierto, porque en la mayoría de los casos hay alguien que “escucha” nuestras conversaciones, filtra nuestras búsquedas y censura las noticias.

En España, así como en otros estados considerados democráticos o dictatoriales, sobran los casos de represión digital. En estos apuntes vamos a presentar las herramientas básicas para poner nuestros datos a salvo y defendernos de posibles ataques.

Para entender cómo defendernos hay que tener en cuenta que la seguridad informática no es nada más que un termino medio entre riesgos de ataques y medidas de defensa que tomamos. Unos ataques pueden ser sencillos para unos y difíciles para otros.

Por ejemplo, una compañera de trabajo puede leer los correos y descubrir nuestros secretos mientras que nos alejamos del ordenador, pero difícilmente podrá secuestrar vuestro ordenador de casa. La policía usualmente elige la segunda posibilidad, siempre que no logre espiaros mientras vais al baño. Situaciones diferentes, según el tipo de ataque del cual somos objetivo.

Identificaciones

Cuando nos conectamos a Internet para chatear, enviar correos o para cualquiera otra cosa, el servicio que utilizamos (Facebook, Twitter, Google, etc..) almacena muchos de nuestros datos personales, como la dirección IP y el sistema operativo que utilizamos. Todos estos datos se quedan almacenados por mucho tiempo y pueden identificarnos de manera inequívoca.

Estos datos tienen valor legal y pueden ser utilizados para identificarnos delante de la ley. Para evitar de ser identificados se pueden tomar medidas técnicas que permiten ocultar los datos personales de la conexión, como la dirección IP y los programas que estamos utilizando.

Estas medidas técnicas tipicamente funcionan enviando los datos a un intermediario de confianza (proxy, vpn, etc..), que luego enviará otra vez los datos a su nombre hacia el destinatario final (Facebook, Google, etc..). Aquí presentamos las más comunes.

Las VPN

Las VPN (Redes Virtuales Privadas) son túneles que conectan tu ordenador a otra red, que puede estar situada en cualquier otro lugar del mundo. Utilizando esta conexión para enviar y recibir datos en Internet, tu identidad queda oculta a la persona con la que te estás comunicando o a los servicios que estás utilizando (como Facebook, Gmail, Twitter, ecc..).

Además la conexión de las VPN es cifrada, o sea que los datos no pueden ser leídos por los intermediarios de la red entre tu ordenador y la VPN. Es posible usar las VPN con la mayoría de ordenadores, smartphones y tabletas. Os aconsejamos el servicio de VPN de Riseup [1] y de Autistici/Inventati [2].

[1] <https://www.riseup.net/es/riseup-vpn/>

[2] <https://vpn.autistici.org/help/index-es.html>

Navegar con Tor Browser Bundle

Tor es un sistema que anonimiza tus comunicaciones, haciendo rebotar los datos de la comunicación entre diferentes nodos de la red Tor, que están distribuidos por todo el mundo.

Tor Browser Bundle es un navegador (basado en Firefox) que te permite utilizar Tor sin tener que instalar o configurar nada. Puedes bajar la última versión desde su página web oficial [1].

[1] <https://www.torproject.org/projects/torbrowser.html.en>

Los servidores autogestionados

Además de los millones de servicios ofrecidos por empresas que existen en Internet, hay otros que son ofrecidos por colectivos que se empeñan técnicamente y políticamente en ofrecer servicios libres. Estos colectivos ponen la privacidad y el anonimato de los usuarios por encima de todo, tomando medidas técnicas para que las autoridades no puedan sacar informaciones de los servidores y de los ficheros de logs. Entre los colectivos más conocidos, aconsejamos Riseup [1] y Autistici/Inventati [2].

[1] <https://riseup.net/>

[2] <https://www.autistici.org/es/index.html>

Anonimizar los ficheros

La mayoría de los ficheros multimedia (ficheros audio, vídeo, pdf, documentos, ...) contienen muchos datos “escondidos” que podrían ayudar a identificar a quién creó, modificó o utilizó el fichero. Por ejemplo, las fotos y los vídeos suelen contener la información del modelo de cámara utilizado y la posición GPS. Para eliminar estas informaciones existen diferentes herramientas que limpian los ficheros de manera muy sencilla. En sistemas GNU/Linux aconsejamos Metadata Anonymisation Toolkit [1].

[1] <https://mat.boum.org/>

Interceptaciones

Todos los datos que enviamos y recibimos por Internet pasan por muchos nodos de la red, que si quisieran podrían leer el contenido de estos datos. No hay manera de evitar que lean nuestros datos, pero es posible cifrar el contenido para que sólo lo pueda entender la persona con la que estamos hablando en Internet.

La medida de cifrar los datos, es una técnica que puede ser utilizadas para la navegación, el envío de correos, los chats y otros servicios. Aquí vamos a presentar herramientas sencillas para cifrar la información de los servicios más comunes.

Cifrar los correos con GPG

Cuando hablamos de cifrar los correos, nos referimos a transformar un texto que puede ser leído o "robado" por cualquier persona, en otro del que estamos seguros que sólo va a poder ser leído por el destinatario.

¿Cómo se hace eso? Pues para explicarlo de forma sencilla con un símil, podríamos decir que la persona que quiere recibir el correo tiene muchos candados y una sola llave que los abre todos, los candados se los da a todos los que quieren enviarle el correo (clave pública) y la llave se la queda él y no se la puede dar a nadie. Cuando alguien le envía un correo, lo "cierra" con ese candado que le ha dado el destinatario (lo cifra con su clave pública). De esta manera, nadie lo puede leer, sólo el destinatario de dicho correo, que lo puede abrir con su llave (clave privada).

Todo este proceso de generación de las llaves (claves) se llevan a cabo mediante los programas que enumeramos en este capítulo, que permiten almacenar tanto las claves públicas de tus contactos como tu clave privada.

De todas formas, existen directorios en internet en los que se puede encontrar las claves públicas de personas que las han dejado allí para que los que quieran cifrar los correos que les envían, lo puedan hacer sin problemas.

Thunderbird + Enigmail, GPG Suite y GPG4Win

Thunderbird [1] es una aplicación de correo libre, fácil de configurar y personalizar, y hay versiones para Linux, Windows y Mac OS X. Instalando el plugin Enigmail [2] es posible recibir y enviar correos cifrados de manera automática, además de disponer de un panel para gestionar las llaves de cifradura GPG.

En sistemas Mac OS X aconsejamos GPG Suite para cifrar, descifrar, firmar y verificar correos y ficheros [3]. Si buscas algo similar para los sistemas Windows puedes probar GPG4Win [4].

Cifrar los correos con las llaves GPG es una de las maneras más seguras de comunicar en Internet.

[1] <http://www.mozilla.org/es-ES/thunderbird/>

[2] <https://addons.mozilla.org/es/thunderbird/addon/enigmail/>

[3] <https://pgptools.org/>

[4] <http://www.gpg4win.org/>

HTTPS Everywhere

HTTPS Everywhere es un plugin para los navegadores Firefox y Chrome que se encarga de utilizar comunicaciones cifradas con las paginas web que visitas, dejándote un alto nivel de defensa contra posibles interceptaciones.

En el caso que la página web no soporte comunicaciones cifradas o las soporte sólo en parte, el plugin no podrá cifrar la comunicación y el envío y la recepción de datos será vulnerables a interceptaciones.

Puedes instalar este plugin con mucha facilidad visitando su página web [1].

[1] <https://www.eff.org/https-everywhere>

Chatear con Pidgin y OTR

La mayoría de las mensajerías instantáneas (Skype, GTalk, Facebook Chat, Yahoo! Messenger, etc..) protegen las conversaciones con el cifrado SSL (o TLS) poniendo más difícil a los compañeros de piso o a un colega leer tus conversaciones.

En estos tipos de mensajerías tu privacidad se queda en mano de las empresas, que con toda probabilidad colaborarán con las autoridades para poderte interceptar y identificarte.

En alternativa a estos servicios comerciales, aconsejamos los servidores autogestionados de A/I [1] y Riseup [2] ofrecen a sus usuarios el servicio de mensajería instantánea Jabber (XMPP) que, combinado con el sistema de cifrado OTR [3], nos proporciona un alto nivel de seguridad contra las interceptaciones.

[1] http://www.autistici.org/es/stuff/man_jabber/index.html

[2] <https://help.riseup.net/en/otr>

[3] <http://www.cypherpunks.ca/otr/>

Secuestros

Los datos de todos los dispositivos electrónicos (ordenadores, móviles, tabletas, disco duros, etc...) no están a salvo de posibles secuestros. La contraseña de Windows, el código pin de los móviles y todas las medidas de autenticación, no te protegen de posibles lecturas de tus datos cuando el villano de turno (que sea un ladrón de ficheros o un policía forense) tiene en su mano el dispositivo.

La manera más segura para evitar que estos villanos puedan ver tus datos es la criptografía asimétrica, o sea un sistema que protege tus datos con una contraseña. Esta técnica de defensa se puede usar con los ordenadores, y sólo en parte con los smartphones y las tabletas.

Es posible cifrar todo el disco duro, la carpeta de los usuarios, una carpeta cualquiera o un fichero solo. La medida más segura es cifrar todo el disco duro de manera que los datos no puedan ser leídos y el sistema no pueda ser comprometido.

Cifrar con Mac: FileVault y FileVault2

Con el sistema operativo ya instalado se puede cifrar todo el disco duro o sólo la carpeta de los usuarios, respectivamente con FileVault2 y FileVault.

Para utilizar FileVault2 se necesita Mac OS X Lion 10.7 o superiores, y se puede elegir entre cifrar las carpetas de los usuarios y cifrar todo el disco, que se desbloqueará insertando la contraseña al encender el ordenador. Para más información visita la página oficial de apple [1] y esta otra página en castellano [2].

Con Mac OS X Panther 10.3 o superiores se puede utilizar FileVault y sólo se puede cifrar las carpetas de todos los usuarios.

[1] <https://support.apple.com/kb/HT4790>

[2] <http://www.mimac.es/area/Programas+Mac/Encriptar+tu+disco+duro>

Cifrar con Linux: luks con Gnome Disk Utility y VeraCrypt

Con los sistemas GNU/Linux al momento de instalación es posible cifrar todo el disco duro o solo la carpeta de los usuarios. Si tienes un sistema ya instalado, solo será posible cifrar de manera sencilla las carpetas de los usuarios. La solución mejor es cifrar todo el disco, si instalamos un sistema desde cero el procedimiento es sencillo. Consulte la guía de instalación de Ubuntu [1].

Para poder crear y manipular discos duros externos existen diferentes herramientas incorporadas en las diferentes distribuciones de GNU/Linux. Para las que utilizan Gnome (como Ubuntu, Xubuntu, Debian, ecc...) aconsejamos Gnome Disk Utility [2] y también VeraCrypt [3], la cual es considerada una solución más robusta y multiplataforma.

[1] <http://planetubuntu.es/post/como-instalar-ubuntu-12-10>

[2] https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.es.html

[3] <https://veracrypt.codeplex.com/>

Borrar ficheros

Cuando borramos un fichero en realidad su contenido no se pierde, sino que el sistema borra la dirección donde está almacenado. Existen diferentes maneras para recuperar la dirección del fichero, que sólo funcionan si el sector donde están guardados los datos no ha sido utilizado para otro fichero.

Para estar seguros de que el contenido no podrá ser leído en futuro, podemos utilizar unas herramientas que antes de borrar la dirección del fichero, escriben encima de ello datos casuales más de una vez.

Borrar ficheros con Linux: secure-delete y wipe

Las herramientas Secure-Delete [1] y wipe [2], son un conjunto de herramientas muy útiles que usan avanzadas técnicas para borrar de forma permanente archivos.

En este paquete encontrarás la herramienta para eliminar ficheros existentes en el disco duro y en la partición de swap, limpiar el espacio libre y la memoria RAM [2].

[1] <http://sourceforge.net/projects/securededelete/>

[2] <http://www.peatonet.com/informatica-forense-borrado-seguro-de-archivos-con-wipe-e-integracion-en-el-explorador-nautilus/>

[3] <http://www.atareao.es/ubuntu/borrado-seguro-o-como-triturar-archivos/>

Borrar ficheros con Windows: eraser

Eraser es una herramienta para Windows que permite borrar con seguridad los ficheros guardados en Windows y en otros dispositivos, rescribiendo encima de ellos más veces. Para más información puedes visitar su página oficial [1] o este artículo en castellano [2].

[1] <http://eraser.heidi.ie>

[2] https://securityinabox.org/es/eraser_principal

Intrusiones

Las intrusiones en los ordenadores, móviles y tabletas, son prácticas utilizadas para espiar a una o más personas en remoto. Con estas medidas el atacante logra obtener el control de los dispositivos con la instalación de un malware, o sea programas que se instalan engañando al usuario o aprovechando de fallos del sistema. Un Malware es algo parecido a un virus: es un programa que se esconde en el ordenador con finalidades malévolas. Quien produce estos malware y los difunde puede hacerlo por diferentes razones, como vender tus datos a empresas que trabajan en publicidad o utilizar tu correo para enviar spam.

Malware de Estado

En los últimos años la policía de diferentes Estados está empezando a utilizar los malware para espiar personas y buscar pruebas de un supuesto crimen. Por norma general estos malware se encargan de:

- Registrar todo lo que aparece en la pantalla (screenshot)
- Registrar todas las teclas que pulsas (keylogger)
- Permitir desde remoto la navegación en los ficheros del ordenador y copiarlos

En España ha sido redactado un borrador (el Borrador del Código Procesal Penal [1]) en el cual se autoriza a la policía a utilizar malware bajo autorización de la magistratura. En el texto se evidencia que las intrusiones telemáticas por parte de la policía se podrán autorizar sólo para:

- Los casos de supuestos crímenes penales con penas máximas mayores de tres años
- Los casos de terrorismo
- Los casos crimen organizado y crimen informático

Soluciones especiales

Además de la herramienta que podemos instalar en nuestros sistemas, existen unos sistemas operativos que llevan ya instalado y configurado todo lo necesario.

Estas distribuciones se suelen instalar dentro de una memoria USB y se pueden arrancar en casi todos los ordenadores, sin modificar el sistema y los datos que están en el disco duro del ordenador.

Tails

Tails se focaliza en preservar la privacidad y el anonimato, con todas las conexiones salientes forzadas a salir a través de Tor. El sistema está diseñado para ser arrancado sin dejar ningún rastro en el almacenamiento local a menos que se indique explícitamente. Hay instaladas muchas herramientas para poder navegar con Tor, manejar ficheros y correos criptados, y otras herramienta que hemos mencionado en las páginas anteriores.

Se instala en una memoria USB y es posible guardar con seguridad datos y instalar nuevos programas como si fuera un sistema operativo, porque la memoria USB está totalmente cifrada. [1]

<https://tails.boum.org/index.es.html>

Contraseñas

Contraseñas robustas

Algo fundamental para asegurar nuestra privacidad es la creación de contraseñas seguras, esto es sencillo simplemente cumpliendo estas normas:

- Usa al menos 8 caracteres, cuantos más mejor.
- Usa mayúsculas, minúsculas, números y signos de puntuación.
- No uses repeticiones de caracteres como 12345 o abcdef.
- No uses información personal que pueda relacionarse contigo.
- No uses palabras de ningún idioma.
- No utilices la misma contraseña para varios servicios.
- No la escribas en lugares que puedan ser descubiertos o estén a la vista (móvil, cuaderno, post-it...)
- No uses las "Opciones de Recuperación de la Contraseña" de algunos servicios.

Para asegurarte una creación de contraseña segura y poder recordarla en un futuro existen varios trucos mnemotécnicos, como por ejemplo, utilizar las primeras letras de una frase larga o de una canción añadiendo números y algún símbolo de puntuación.

¿Quiénes somos?

Un poco de historia...

Tras varios años como Sección dentro del Sindicato de Oficios Varios de la Federación Local de Madrid CNT-AIT, en Enero de 2014 se constituye el Sindicato de Telecomunicaciones y Servicios Informáticos.

En Septiembre de 2015, tras más de un año y medio en la CNT, nuestra asamblea resolvió desfederarse de la Federación Local de Madrid y de la Confederación, debido a cuestiones que hemos expuesto en un comunicado público.

Durante todo este tiempo nos hemos enfrentado, con mayor o menor acierto, a corporaciones como Capgemini, Indra, Banco Santander (ISBAN), Ydilo o Panel Sistemas, brindando solidaridad a los/as compañeros/as y extendiendo la autoorganización. Por otro lado, hemos estado desarrollando labores referidas a la privacidad en las redes, la represión digital y la autodefensa, habiendo lanzado un itinerario con otros colectivos e individualidades para continuar desarrollando estos aspectos. En este mismo sentido, en la medida de nuestras posibilidades, nos dedicamos a realizar talleres de autodefensa digital en distintas ciudades del Estado español.

Nuestros propósitos

Somos una organización de trabajadores/as que parte del ramo de las telecomunicaciones y los servicios informáticos y que reúne también a trabajadores/as de otros sectores laborales, cuestión que alentamos enérgicamente.

Reivindicamos el asociacionismo obrero como una forma genuina de llevar adelante el vínculo entre personas explotadas, que diariamente nos vemos forzadas a vender nuestro tiempo y energía a la burguesía, a cambio de un salario que nos permite subsistir para reproducir la misma actividad todos los días. Vemos en esta asociación la posibilidad de potenciar nuestros deseos y necesidades, generando una comunidad de lucha sin representantes ni intermediarios, en oposición al reformismo y a la democracia imperantes.

A raíz de esto, el medio que utilizamos y promovemos en la conflictividad social es la acción directa, esto es, la lucha sin mediadores, rechazando la intromisión de elementos extraños entre los/as trabajadores/as y el Capital.

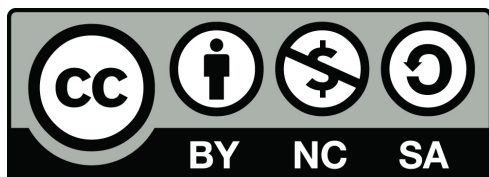
Consideramos importante recomponer el tejido solidario que siempre ha existido entre los/as proletarios/as, que la burguesía ha ido desmembrando tras años de imposición ideológica, represión, nacionalismo, etc. Por esto, no nos interesa aglutinar gente bajo unas siglas, sino promover y alentar la autoorganización y la autonomía de clase.

Queremos, con nuestro esfuerzo, continuar aportando a las experiencias históricas y actuales de lucha anticapitalista e internacionalista, hacia la supresión de esta sociedad de clases, el trabajo asalariado y el Estado, por una verdadera comunidad humana donde las personas nos podamos relacionar libremente, “a cada una según sus necesidades, de cada una según sus capacidades”. Y afirmamos que esto sólo será posible mediante una revolución proletaria mundial.

[illegible]

[illegible]

This image shows a single sheet of white paper with horizontal blue or grey ruling lines, typical of notebook paper. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



Este obra está bajo una licencia de Creative Commons
Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional.

Versión 1.6 - Impreso en Marzo 2016

¡Descarga, copia, comparte y difunde!

<httpS://www.stsi-madrid.org/>