MARTA PEIRANO

EL PEQUEÑO LIBRO ROJO DEL ACTIVISTA EN LA RED

Prólogo de EDWARD SNOWDEN

eldiario.es libros

rocaeditorial

eldiario.es libros

El pequeño Libro Rojo del activista en la Red

Introducción a la criptografía para redacciones, *whistleblowers*, activistas, disidentes y personas humanas en general

Marta Peirano

Rocaeditorial

Primera edición en este formato: enero de 2015

www.eldiario.es
ISBN: 978-84-9918-822-5

EL PEQUEÑO LIBRO ROJO DEL ACTIVISTA EN LA RED

Marta Peirano Prólogo de Edward Snowden

En tiempos de fascismo, todos somos disidentes. Y nuestras trincheras están en la Red.

Bradley Manning es un soldado raso que no quiso aceptar los crímenes de guerra como daños colaterales. Julian Assange es un informático que ha decidido hacer un trabajo al que los grandes periódicos han renunciado. Edward Snowden es un técnico informático que, ante la evidencia de un abuso contra los derechos de sus conciudadanos, decidió denunciar. Los tres son ciudadanos ordinarios que, enfrentados a circunstancias extraordinarias, decidieron cumplir con su deber civil. Las consecuencias para ellos no podrían ser más graves ni más reveladoras: son víctimas de una campaña internacional de descrédito personal cuya intención es convencer a los espectadores de que lo importante son las apariencias y no los hechos.

En cada oficina hay cientos de personas como ellos. Por sus manos pasan documentos secretos, algunos de los cuales necesitan salir a la luz. *El pequeño Libro Rojo del activista en la Red* es un manual para proteger sus comunicaciones, cifrar sus correos, borrar sus búsquedas y dispersar las células de datos que generan sus tarjetas de red, en el caso de que, al igual que ellos, usted decida arriesgarlo todo por el bien de su comunidad.

ACERCA DE LA AUTORA

Marta Peirano escribe sobre cultura, tecnología, arte digital y software libre para diarios y revistas. Fue jefa de cultura en el difunto *ADN.es* y sus blogs *La Petite Claudine* y *Elástico.net* han recibido múltiples premios y han figurado entre los más leídos e influyentes de la blogosfera española. Ha codirigido los festivales COPYFIGHT sobre modelos alternativos de propiedad intelectual y es la fundadora de la HackHackers Berlín y Cryptoparty Berlín. Ha publicado varios libros: *El rival de Prometeo*, una antología editada sobre autómatas e inteligencia artificial; dos ensayos colectivos (*Collaborative Futures* y *On Turtles & Dragons (& the dangerous quest for a media art notation system*), y *The Cryptoparty Handbook*, un manual para mantener la intimidad y proteger las comunicaciones en el ciberespacio. Desde septiembre de 2013 dirige la sección de cultura de *eldiario.es*

Índice

«Si estamos, como parece, en pleno proceso de convertirnos en una sociedad totalitaria donde el aparato de Estado es todopoderoso, entonces el código moral imprescindible para la supervivencia del individuo libre y verdadero será engañar, mentir, ocultar, aparentar, escapar, falsificar documentos, construir aparatos electrónicos en tu garaje capaces de superar los *gadgets* de las autoridades. Si la pantalla de tu televisor te vigila, invierte los cables por la noche, cuando te permitan tenerlo apagado. Y hazlo de manera que el perro policía que vigilaba la transmisión de tu casa acabe mirando el contenido de su propio salón.»

PHILIP K. DICK, *The Android and the Human,* 1972

«The internet is on principle a system that you reveal yourself to in order to fully enjoy, which differentiates it from, say, a music player. It is a TV that watches you. The majority of people in developed countries spend at least some time interacting with the Internet, and Governments are abusing that necessity in secret to extend their powers beyond what is necessary and appropriate.»

EDWARD SNOWDEN, 2013

Prólogo

por EDWARD SNOWDEN

*N*uestra habilidad para entender el mundo en que vivimos depende fundamentalmente de los intercambios no autorizados y no vigilados entre los periodistas de investigación y sus fuentes. La vigilancia persistente del periodismo de investigación debilita las libertades básicas que proporciona la libertad de prensa, socavando estructuras democráticas elementales.

Sin embargo, los periodistas no son expertos en seguridad. Las escuelas de periodismo no ofrecen cursos para aprender a usar herramientas de seguridad diseñadas para proteger la información y las comunicaciones. Y, cuando una fuente decide soltar la liebre y exponer el abuso de un gobierno, los periodistas ya no tienen tiempo de ponerse a aprender las medidas básicas de seguridad. La revelación de los programas indiscriminados de vigilancia de la NSA en Estados Unidos, la GCHQ en Inglaterra y otras agencias de seguridad gubernamentales a lo largo de los últimos años nos ha demostrado que la privacidad digital no es algo que se pueda dar por hecho, especialmente si eres un periodista de investigación.

Gracias a los avances de la tecnología, los sistemas de vigilancia masiva de hoy pueden registrar en tiempo real todos los metadatos de todas las comunicaciones que se estén dando en cualquier país, todo con un coste y un grado de complejidad tan accesible que está al alcance de literalmente cualquier gobierno del planeta. Esa acumulación de metadatos puede revelar una red completa de vínculos y asociaciones humanos, exponiendo cualquier interacción que pueda ser percibida como una amenaza para el régimen de poder establecido.

Como consecuencia, la vigilancia masiva representa un arma contra aquellos pocos que deciden convertirse en fuentes de información periodística, porque revela sus identidades, sus estructuras de apoyo y sus lugares de residencia o de refugio. Es información que los gobiernos pueden usar para eliminar el riesgo de futuras revelaciones por parte de esa fuente. Sus métodos pueden variar: una citación judicial en Estados Unidos puede hacer el mismo trabajo que una bala en Quetta o Chechenia. Pero el impacto sobre la fuente y el periodismo de investigación es el mismo.

Como profesionales, los periodistas tienen la responsabilidad de aplicar las mejores prácticas de seguridad antes de ponerse en contacto con un confidente por primera vez. Dicho de otra manera: nadie espera que un paciente que entra en una consulta médica le tenga que recordar a su médico que se cambie los guantes. Un periodista hoy en día necesita poseer un conocimiento funcional de las técnicas para anonimizar y de las herramientas de cifrado. También deben aprender a usarlas de manera efectiva.

A la luz de las revelaciones sobre las capacidades de los gobiernos, esta nueva responsabilidad puede resultar abrumadora. No basta con que los periodistas sepan establecer una clave pública PGP. Un periodista debe entender cómo funcionan las herramientas de seguridad y cómo no funcionan, y adaptar sus actividades a las limitaciones de esa tecnología. Por ejemplo, hay muchas herramientas de seguridad digital que protegen muy bien un contenido, pero dejan los metadatos al aire. Esto significa que el cifrado de un correo es tan seguro y efectivo como las palabras que elegimos para poner en el asunto o el nombre que le damos a un adjunto.

El periodista también debe conocer a su adversario. Debe saber cómo se interceptan las llamadas telefónicas, y que una línea segura tiene que estar protegida a ambos lados de la comunicación. Debe valorar las maneras en que la falta de tiempo, el margen de error y la reducción de recursos pueden devaluar el plan de seguridad más sensato y sus implementaciones. Deben tener siempre un plan B y prever circunvalaciones cuando el ordenador o el correo de una fuente ha sido comprometido. Deben conocer las técnicas para asegurar y corroborar la información pública que han acumulado.

Por este y otros motivos, *El pequeño Libro Rojo del activista en la Red* es un recurso esencial para asegurar que aquellos que recogen, analizan y transmiten información a la sociedad puedan proteger, no solo su trabajo, sino también —y por encima de todo— a sus fuentes.

La democracia depende de la existencia de una prensa valiente y con capacidad para realizar un periodismo de investigación, una que mide su éxito en su capacidad para exponer los abusos de la autoridad al gran público. Por eso, cada vez que un aparato de vigilancia masiva se pueda usar para monitorizar todos los encuentros «no autorizados» entre un reportero de investigación y su fuente, la prensa libre se tambaleará. Y sin la prensa libre, todas las instituciones de librepensamiento de la sociedad desaparecerán.

EDWARD SNOWDEN

Diciembre 2014

CÓMO COMBATIR LA VIGILANCIA ONLINE

Navegación

1. TOR BROWSER BUNDLE

Incluye todo lo que necesitas para acceder a la Tor Network. Hace que sea más difícil rastrear tu actividad en Internet: historial de navegación, *posts*, mensajes instantáneos y otros formatos de comunicación. No previene el tráfico de entrada y salida a la red. Mientras Tor te protege contra el análisis del tráfico, no puede prevenir la confirmación del mismo (también llamada *e2e*).

2. BLEACH BIT

Tiene varias herramientas con las que podrás limpiar, liberar espacio en tu ordenador y resguardar tu privacidad.

↳ www.torproject.org
↳ www.bleachbit.sourceforge.net

Seguridad portátil

3. TAILS

Un sistema operativo vivo. Puede instalarse en cualquier PC con un DVD o un pendrive. Protege tu privacidad y anonimato. Tiene incorporadas muchas aplicaciones preconfiguradas con el fin de preservar toda tu información sobre navegadores, mensajes instantáneos, e-mails, aplicaciones para oficina y más.

↳ https://tails.boum.org

Disco encriptado

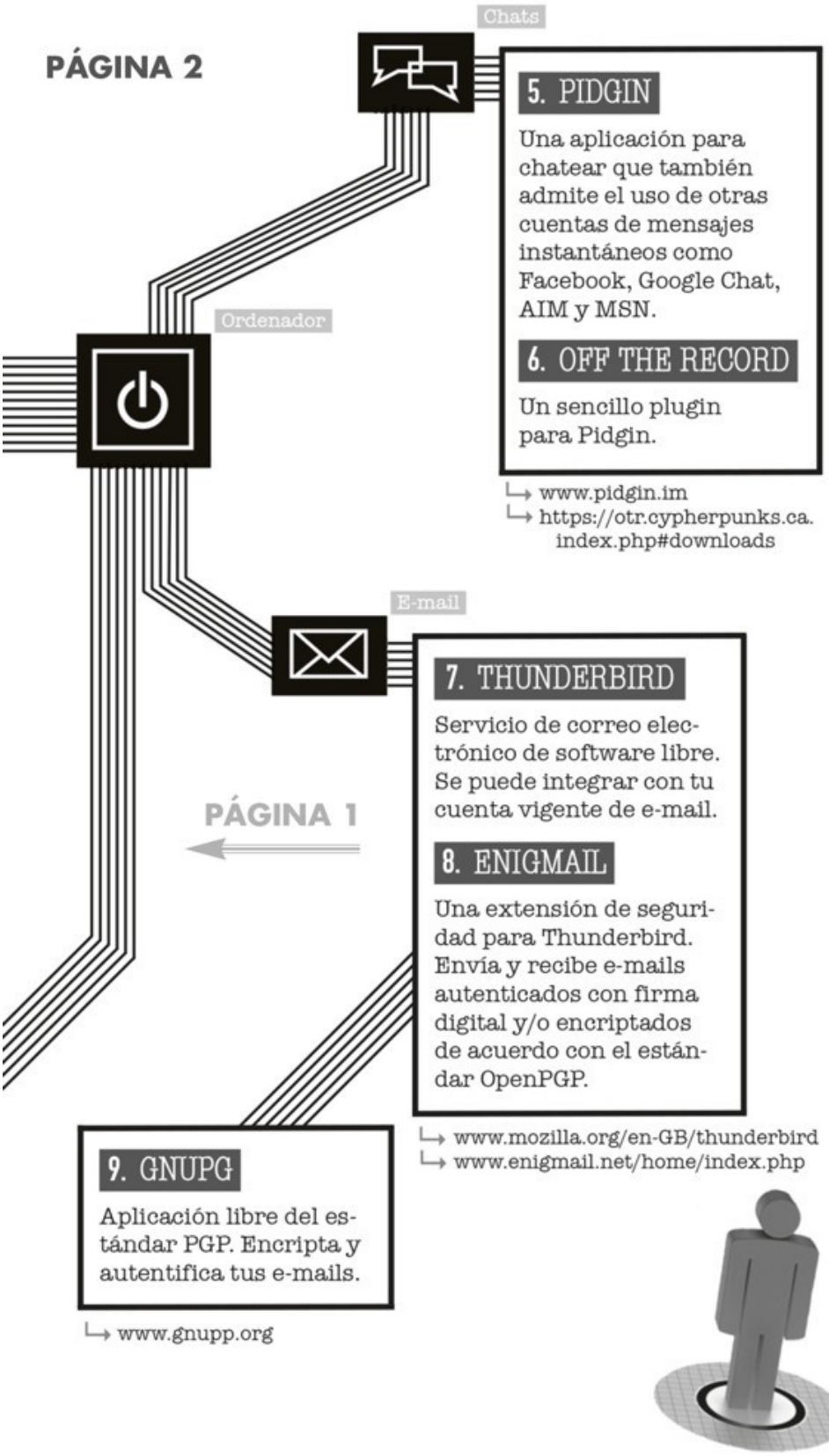
4. TRUECRYPT

Crea discos duros virtuales que encriptarán cualquier archivo que guardes en ellos. Usa varios tipos de encriptación.

↳ www.truecrypt.org

PÁGINA 2

PÁGINA 2



5. PIDGIN

Una aplicación para chatear que también admite el uso de otras cuentas de mensajes instantáneos como Facebook, Google Chat, AIM y MSN.

6. OFF THE RECORD

Un sencillo plugin para Pidgin.

↳ www.pidgin.im
↳ https://otr.cypherpunks.ca.index.php#downloads

7. THUNDERBIRD

Servicio de correo electrónico de software libre. Se puede integrar con tu cuenta vigente de e-mail.

8. ENIGMAIL

Una extensión de seguridad para Thunderbird. Envía y recibe e-mails autenticados con firma digital y/o encriptados de acuerdo con el estándar OpenPGP.

↳ www.mozilla.org/en-GB/thunderbird
↳ www.enigmail.net/home/index.php

9. GNUPG

Aplicación libre del estándar PGP. Encripta y autentifica tus e-mails.

↳ www.gnupp.org

PÁGINA 1

Glenn Greenwald, Edward Snowden y la importancia de saber cifrar

*L*a historia ya es leyenda: Glenn Greenwald estuvo a punto de perder el mayor bombazo periodístico de las últimas décadas solo porque no quiso instalarse la PGP. Él mismo la contaba con sana ironía cuando, seis meses más tarde, le invitaron a dar una conferencia como cabeza de cartel en el congreso del Chaos Computer Club, el mismo festival de *hackers* donde cinco años antes se presentó WikiLeaks. Todo empezó cuando el 1 de diciembre de 2012 Greenwald recibió una nota de un desconocido pidiéndole su clave pública para mandarle cierta información de suma importancia.

A pesar de tratar con fuentes delicadas y escribir sobre asuntos de seguridad nacional; a pesar de su apasionada defensa de WikiLeaks y de Chelsey (entonces Bradley) Manning, Glenn Greenwald no sabía entonces lo que era una clave pública. No sabía cómo instalarla ni cómo usarla y tenía dudas de que le hiciera falta, así que, cuando llegó un misterioso desconocido pidiendo que la utilizara, simplemente le ignoró. Poco después, el desconocido le mandó un tutorial sobre cómo encriptar correos. Cuando Greenwald ignoró el tutorial, le envió un vídeo de cifrado para *dummies*.

«Cuanto más cosas me mandaba más cuesta arriba se me hacía todo —confesó Greenwald más tarde a la revista *Rolling Stone*—. ¿Ahora tengo que mirar un estúpido vídeo?» La comunicación quedó atascada en un punto muerto, porque Greenwald no tenía tiempo de aprender a cifrar correos para hablar con un anónimo sin saber lo que le quería contar y su fuente no podía contarle lo que sabía sin asegurarse de que nadie escuchaba la conversación. Lo que hoy parece obvio entonces no lo era, porque ahora todos sabemos lo que la fuente sabía pero Greenwald ignoraba: que todos y cada uno de sus movimientos estaban siendo registrados por la Agencia de Seguridad Nacional norteamericana. La fuente lo sabía porque trabajaba allí.

Pero Greenwald recibía correos similares cada día. A medio camino entre el periodismo y el activismo, gracias a su trabajo en la revista *Salon*, su cuenta en Twitter y su columna en *The Guardian*, el periodista se había convertido en la bestia negra del abuso corporativo y gubernamental y su carpeta de correo estaba llena de anónimos prometiendo la noticia del siglo que luego quedaban en nada. Después de un mes, la fuente se dio por vencida. Seis meses más tarde, Greenwald recibió la llamada de alguien que sí sabía lo que era la PGP: la documentalista Laura Poitras.

Poitras no solo sabía encriptar correos; se había pasado los dos últimos años trabajando en un documental sobre la vigilancia y el anonimato. Había entrevistado a Julian Assange, a Jacob Appelbaum y a otros. No era un tema al que estaba naturalmente predispuesta, sino al que se vio empujada desde que la pararon por primera vez en el aeropuerto internacional de Newark, cuando la cineasta iba a Israel a presentar su último proyecto, *My Country, My Country*.

Se trataba de un documental sobre la vida del doctor Riyadh al-Adhadh y su familia en la Bagdad ocupada. Poitras había convivido con ellos mientras filmaba la película y un día estaba en el tejado de su casa con la cámara cuando tuvo lugar un ataque de la guerrilla local en el que murió un soldado norteamericano. Que Poitras estuviera por casualidad en el tejado y lo grabara todo generó rumores entre las tropas. Los soldados la acusaron de estar al tanto de la insurrección y de no haberles avisado para así asegurarse material dramático para su documental. Aunque nunca fue acusada formalmente, y nunca hubo pruebas, sus

billetes fueron marcados como «SSSS» (Secondary Security Screening Selection). Poitras ya no pudo coger un avión sin ser interrogada y sus pertenencias registradas.

Después de los ataques a las Torres Gemelas, el gobierno norteamericano empezó una lista negra de posibles terroristas que ha llegado a tener un millón de nombres. Un agente en el aeropuerto de Viena le explicó a Poitras que su pasaporte había sido marcado con la alerta máxima («400 en la escala Richter», le dijo) y que en ningún aeropuerto del mundo la dejarían volar sin antes registrarla. En su entrevista con el *Times*, Poitras dice que ya no recuerda cuántas veces la detuvieron en los siguientes seis años pero que fueron más de cuarenta. En muchos casos, los agentes del aeropuerto exigieron acceso a sus cuadernos y ordenadores para poder copiar su contenido y, en al menos una ocasión, requisaron todo su equipo durante varias semanas. Un día se le ocurrió que, si estaba en la lista negra y la paraban cada vez que viajaba, lo más probable era que su correo y su historial de navegación también estuvieran comprometidos.

«Supongo que hay cartas de seguridad nacional en todos mis correos», dice Poitras en la misma entrevista. La «carta de seguridad nacional» (National Security Letter o NSL) es una orden de registro que reciben los proveedores de servicios —las compañías telefónicas o los servidores de red— para que faciliten los datos de un usuario. Todas las comunicaciones electrónicas son susceptibles de recibir una sin que sea necesaria la intervención de un juez, y la proveedora tiene prohibido advertir el registro a su cliente. En 2011, Laura Poitras empezó a trabajar en su documental sobre la vigilancia gubernamental y, en el proceso, aprendió a proteger sus comunicaciones.

Empezó a dejar el móvil en casa, un dispositivo que no solo registra las conversaciones sino que funciona como localizador, incluso cuando todos los sistemas de localización y hasta el propio teléfono han sido desactivados. Dejó de tratar asuntos delicados por correo y empezó a usar un anonimizador para navegar por la Red. Aprendió a encriptar sus e-mails con una llave de clave pública. Empezó a usar diferentes ordenadores: uno para editar sus documentales, otro para mandar correos y un tercero sin tarjeta de red para almacenar material sensible. Por eso, cuando un anónimo le escribió para pedir su clave pública, Poitras se la dio inmediatamente. Una vez convencida de la seriedad de su contacto y la legitimidad de sus documentos, Poitras se puso en contacto con Greenwald, al que había entrevistado para su documental y, a cambio, había escrito sobre ella en *Salon* («U.S. Filmmaker Repeatedly Detained at Border», abril 2012). En junio de 2013 volaron juntos a Hong Kong para encontrarse con Edward Snowden y destapar el mayor caso de espionaje masivo de la historia.

Todos los periodistas a los que les cuento esta historia se ríen, pero es raro encontrar a uno que tenga software diseñado para proteger sus comunicaciones en su ordenador. «Me sorprendió darme cuenta de que había gente en los medios que no sabía que todo correo enviado sin cifrar a través de la red acaba en todas las agencias de inteligencia del planeta —dijo Snowden en una entrevista cuando se publicó esta historia—. A la vista de las revelaciones de este año, debería estar ya suficientemente claro que el intercambio no cifrado de información entre fuentes y periodistas es un descuido imperdonable.» Snowden es un experto en seguridad informática cuyo acceso a los numerosos programas de vigilancia total desarrollados por y para la *National Security Agency* (NSA, Agencia de Seguridad Nacional) fundamentaron su puntillosidad. Gracias a su cuidadosa estrategia ha sido capaz de controlar las circunstancias de sus extraordinarias revelaciones y escapar de Estados Unidos antes de ser encarcelado, como Bradley Manning. Si no hubiera sido tan paranoico, le habría pasado lo mismo que a las fuentes del cineasta Sean McAllister en el

país más peligroso del mundo para periodistas y disidentes: Siria.

Descuidar la seguridad es poner en peligro a tus fuentes

*S*ean McAllister es, según Michael Moore, uno de los cineastas más valientes y emocionantes del planeta. Sus documentales sobre la vida en zonas de conflicto como Yemen o Iraq han recibido múltiples premios y el reconocimiento de la prensa internacional. Se diría que su experiencia le ha enseñado a trabajar con extrema precaución («Es una ruleta ir por Siria filmando de encubierto —dijo en una entrevista—. Antes o después te pillan.»). Ese otoño de 2011 había viajado a Damasco para rodar un documental sobre la disidencia contra el régimen de Bashar al-Assad. Subvencionado por la cadena británica Channel 4, McAllister le pidió ayuda a Kardokh, un cyberdisidente de 25 años que procuraba herramientas de comunicación segura a la resistencia.

Kardokh (un pseudónimo) había logrado *hackear* el sistema de vigilancia electrónico que usaba el gobierno sirio para controlar las comunicaciones de sus ciudadanos, y hasta había conseguido convencer a la empresa italiana propietaria de dicho sistema de que cancelase su contrato con el gobierno sirio. Además, había creado junto con otros informáticos una página web llamada «Centro de Documentación de la Violencia» donde publicaban los nombres de los desaparecidos del régimen. Tenía buenas razones para mantenerse en el anonimato, pero no quiso perder la oportunidad de denunciar la represión criminal a la que estaban sometidos. «Cualquier periodista que hiciera el esfuerzo de contarle al mundo lo que nos estaba pasando era importante para nosotros», dijo en una entrevista. Por eso dejó que McAllister le entrevistara en cámara, bajo la promesa de que su rostro saldría pixelado y su voz sería modificada en la sala de edición.

El cineasta quería conocer a más miembros de la resistencia, pero Kardokh estaba preocupado por su despreocupación. Él y sus amigos encriptaban sus correos y tomaban medidas de todo tipo para mantener el anonimato en la Red; por el contrario, McAllister «usaba su teléfono y mandaba SMS sin ninguna protección». Poco después, el británico fue arrestado por los agentes de seguridad del régimen y todo su material fue requisado, incluyendo su ordenador, su móvil y la cámara con las entrevistas a cara descubierta que había rodado.

Cuando se enteró, Kardokh tiró su teléfono y huyó al Líbano (dice que su pasaje le costó 1.000 dólares, 235 por el billete y 765 por borrar su nombre de la lista negra). Otro activista llamado Omar al-Baroudi tuvo menos suerte. «Su cara estaba en esos vídeos.Y dijo que su número estaba en la agenda de Sean», explica un compañero. Cuando la operación se hizo pública, Channel 4 aseguró que el cineasta había tomado todas las precauciones posibles: «Es un cineasta experimentado y tomó medidas para proteger el material —dijo una portavoz de Channel 4—. Siria es un contexto extremadamente difícil para trabajar y por eso seguimos buscando maneras de minimizar el riesgo de contar esta importante historia».

«Me alegro de no haberle puesto en contacto con más gente», declaró Kardokh.

Muchos han culpado a McAllister por no tomar precauciones, pero pocos habrían actuado de manera diferente de haber estado en su lugar. La falta de recursos es intrínseca al medio: ¿cuántos periódicos invitan a sus empleados a talleres de seguridad informática?, ¿qué facultades incluyen clases de cyberseguridad y protección de las comunicaciones?, ¿cuántas cabeceras tienen a expertos en seguridad en plantilla para instalar software de seguridad en los equipos o asesorar a los corresponsales en apuros? Como recordaba el experto Christopher Soghoian en un editorial en *The New York Times* (*«When Secrets*

Aren't Safe With Journalists», 24 de enero de 2012), hasta el director del *NYT* discutió durante meses los detalles de los documentos que les había entregado Julian Assange, de WikiLeaks, en largas conversaciones telefónicas completamente desprotegidas. Las universidades incluyen programas para manejar comentarios y titular para Twitter, pero no nos enseñan a jugar a espías. La profesión mantiene prioridades que no reflejan el verdadero estado de cosas. Hasta las organizaciones más obsesionadas con el periodismo de investigación invierten más recursos en diseñadores web y en litigios que en expertos criptográficos.

Tanto es así que ni siquiera los portales creados por las grandes cabeceras para competir con WikiLeaks consiguen pasar el examen. Tanto la Safehouse de *The Wall Street Journal* como la Unidad de Transparencia de Al Jazeera fueron denunciadas por prometer una anonimidad falsa, exponiendo a las fuentes de manera innecesaria. El analista de seguridad y colaborador de WikiLeaks Jacob Appelbaum tardó menos de veinticuatro horas en encontrar un alarmante número de agujeros en su sistema. Y la Electronic Frontier Foundation señaló que sus Términos y condiciones de uso incluían el derecho de las cabeceras a revelar la identidad de su fuente si así se lo pedían terceras partes o agentes de la ley.

Más aún: quien subía documentos al sistema SafeHouse firmaba un documento en el que aseguraba «no infringir ninguna ley o los derechos de otra persona», que tenía el «derecho legal, poder y autoridad sobre esos documentos» y que el material no «interfería en la privacidad de o constituía un perjuicio para ninguna persona o entidad». En cualquiera de estos tres casos, tanto las denuncias de WikiLeaks como los vídeos de Bradley Manning o los documentos de Edward Snowden hubiesen quedado fuera de juego. Peor todavía: el periódico se reservaba el derecho a utilizar el material de la fuente sin responsabilizarse de su protección, acabando con uno de los principios más fundamentales del periodismo. Y para rematar la faena, el sistema plantaba una *cookie* en tu ordenador. Es difícil valorar si es una cuestión de astucia o estupidez; en todo caso no olvidemos que la más peligrosa de las dos es la segunda.

En ese sentido, los grandes medios se han distanciado del principio que sostiene WikiLeaks, donde la comunicación está diseñada para ser completamente opaca, incluso para el propio administrador. El sistema asegura por defecto que todas las comunicaciones estén protegidas; los documentos que viajan por el mismo están fuertemente cifrados y los servidores que los guardan permanecen escondidos en un laberinto de espejos llamado Tor. «Si aceptamos los documentos de manera anónima —explicaba Assange en un documental —, en lugar de guardar su identidad en secreto, simplemente no la sabemos.» El detalle es importante: Assange y los suyos no tienen que preocuparse por que el gobierno norteamericano, o cualquier otro, produzca una orden judicial que les obligue a revelar la identidad o procedencia de sus fuentes porque ellos mismos no las saben.

En el libro *Cypherpunks*, de Julian Assange, Jacob Appelbaum, Andy Muller-Maguhn y Jérémie Zimmermann, Appelbaum dice:

Si construyes un sistema que almacena datos sobre una persona y sabes que vives en un país con leyes que permiten al gobierno acceder a esa información, quizá no deberías construir ese tipo de sistema. Y esta es la diferencia entre la *privacidad-pordecreto* y la *privacidad-por-diseño*. (…) Si Facebook pusiera sus servidores en la Libia de Gadafi o la Siria de al-Assad nos parecería una negligencia absoluta. Y sin embargo, ninguna de las Cartas de Seguridad Nacional que se vieron el año pasado o el anterior tenían que ver con el terrorismo. Unas 250.000 fueron usadas para todo menos para terrorismo. Sabiendo eso,

estas compañías tienen un serio problema ético en el momento en que están construyendo ese tipo de sistemas y han tomado la decisión económica de vender a sus usuarios al mejor postor. No es un problema técnico: no tiene nada que ver con la tecnología, solo con la economía. Han decidido que es más importante colaborar con el Estado, vender a sus usuarios, violar su intimidad y ser parte de un sistema de control —cobrar por ser parte de una cultura de la vigilancia, la cultura del control— en lugar de resistirse a él. Así que son parte del problema. Son cómplices y responsables.

Además de Greenwald, Edward Snowden se puso en contacto con un periodista de *The Washington Post* llamado Barton Gellman. Fue este periódico el que tuvo la exclusiva de Prism, un programa de la NSA mediante el cual las grandes empresas de Internet habían dado acceso a sus servidores a la misma NSA y al FBI, incluyendo audio, vídeo, búsquedas, correos, fotos, mensajes y archivos. Entre los documentos publicados por el *Post* y el *Guardian* hay un powerpoint que explica los detalles del programa junto con una lista de las empresas que colaboraron con la Agencia: Microsoft (la primera vez, en septiembre de 2007), Yahoo (2008), Google y Facebook (2009) y Apple (2012). Ese mismo día se reveló también que Verizon y otras compañías telefónicas entregaban alegremente los registros de todas las conversaciones telefónicas al gobierno norteamericano.

Irónicamente, el gobierno quiso proteger la identidad de sus fuentes y presionó al *Post* para que los nombres de las compañías fueran borrados del informe. Cuando finalmente el documento salió sin censurar, el presidente Obama habló pero no para negar los hechos ni disculparse, sino para condenar el soplo y decir que él y los suyos podían estar tranquilos: «Con respecto a Internet y los correos, esto no se aplica a los ciudadanos estadounidenses ni a las personas que viven en los Estados Unidos». Aun en el caso de que eso fuera cierto —y sabemos que no lo es—, sería un consuelo muy pequeño: el 80 por ciento de esos usuarios están fuera de Estados Unidos.

Estas son las empresas de las que habla Appelbaum, cuyos servidores están sometidos a leyes que no respetan la privacidad de los usuarios. Aunque la mayor parte de estas empresas aceptaron el escrutinio y la recolección de las Agencias de inteligencia, daría igual que se hubiesen negado heroicamente. De hecho, Yahoo hizo un conato de resistencia que perdió en los tribunales en agosto de 2008, su fecha de incorporación, según el famoso documento que publicó el *Post*. La única manera de proteger los datos de los usuarios es no tenerlos. Lamentablemente, estas son empresas cuyo modelo económico depende de esos datos.

Por qué software libre

*L*a lucha por la libertad tiene efectos secundarios: Jacob Appelbaum está en la lista de terroristas internacionales, Julian Assange está atrapado en la embajada de Ecuador en Londres, Edward Snowden vive exiliado en Rusia hasta nueva orden y Bradley Manning pasará los próximos 35 años de su vida como un traidor encerrado en una prisión militar. Los tres primeros prefirieron trabajar por el bien común que colaborar con la cadena de abusos a cara descubierta; Manning se confesó con alguien que traicionó su confianza y lo denunció a la NSA: el *hacker* y analista de sistemas Adrian Lamo.

Es interesante recordar que, aunque sus perfiles no podrían ser más diferentes, todos son analistas de sistemas y ninguno de ellos ha sido «atrapado» por culpa de la tecnología. Tampoco es casual que todos sean usuarios de Linux. Cuando nuestra vida y nuestra libertad dependen de un software, Linux es la única opción posible.

Hay quien piensa que la insistencia en el software libre es cosa de fanáticos o de elitistas. Desde la explosión de noticias sobre los abusos persistentes a nuestra intimidad por parte de empresas y gobiernos, muchas compañías de software han orientado sus esfuerzos a desarrollar aplicaciones y protocolos para proteger las comunicaciones. Si se comprometen a implementar el anonimato del usuario y a no recopilar datos, si aseguran haber patentado una manera de cifrar las conversaciones telefónicas, si presentan una alternativa a WhatsApp, ¿por qué no usarlas? La respuesta es simple: porque aunque lo que prometen sea cierto, aunque sean la mejor aplicación del mundo mundial, no podemos saberlo.

Imaginemos una empresa que asegura producir verduras orgánicas completamente libres de pesticidas, no modificadas genéticamente, que se cultivan siguiendo las pautas naturales de la madre naturaleza y con extremo respeto al medio ambiente y a la salud de sus consumidores. Imaginemos que el presidente de dicha empresa es un emprendedor que cree firmemente en la necesidad de cambiar nuestros métodos de producción agrícola y nuestros hábitos de consumo. Su coche es eléctrico, su casa funciona con paneles solares, su web está llena de fotos de bellos prados llenos de ovejas felices pastando al sol y campos de trigo y manantiales. Su discurso es razonable, su producto parece excepcional. Pero, cuando vamos a visitar su maravillosa finca, encontramos sus tierras rodeadas por varias capas de alambre de púas y un muro donde pone No pasar.

Técnicamente es su finca, y probablemente tiene buenas razones para protegerla. Y es posible que al otro lado del muro esté todo lo que dice nuestro emprendedor imaginario. El problema es que no podemos saberlo. Si fuera como dice y tuviéramos acceso a la finca, probablemente encontraríamos cosas que no funcionan bien, pero al menos tendríamos la oportunidad de valorar los compromisos que estamos dispuestos a hacer y señalar los errores que se deben corregir para contribuir a sus mejoras. Nadie dice que el software libre sea perfecto, pero al menos podemos saber hasta qué punto no es perfecto y ayudar a que lo sea.

Ahora el ejemplo contrario. «Cryptocat» es una aplicación de software libre que sirve para cifrar conversaciones por chat. El verano pasado le pasó lo peor que le puede pasar a un proyecto de sus características: el experto en seguridad Steve Thomas descubrió un agujero en el sistema y lo publicó. Al parecer, las llaves criptográficas generadas por la aplicación podían ser descifradas con un ataque llamado *Meet-in-the-middle* (no confundir con el más popular *Man-in-the-Middle)*, que reduce significativamente el número de

intentos que debe hacer un ordenador para adivinar una clave usando la fuerza bruta.

Además de señalar el fallo y demostrarlo, Thomas creó una aplicación, un software llamado DecryptoCat, que explotaba automáticamente esta vulnerabilidad y era capaz de descifrar un chat en dos horas desde cualquier ordenador. «Todas las conversaciones que hayan tenido lugar durante los siete meses entre la versión 2.0 y la actualización 2.1 han sido comprometidas», admitió el programador en su página.

El error de Cryptocat era que, aunque utilizaba tres capas de cifrado convencionales —RSA, Diffie-Hellman y ECC— lo hacía generando claves demasiado pequeñas, y en criptografía el tamaño es clave. «Cryptocat tiene una misión, y es ofrecer comunicación segura o, lo que es lo mismo, encriptar datos —explicaba el experto en seguridad Adam Caudill—. La parte más importante de cualquier sistema criptográfico es la generación de claves; si esto te sale mal, todo lo demás no importa.»

Hay quien ve aquí la prueba de que las aplicaciones de software libre no son dignas de confianza. En realidad es la demostración perfecta de lo contrario. Gracias a que Cryptocat es un programa de código abierto, Steve Thomas y cualquier otro experto en seguridad informática, programador o aficionado puede mirar cómo funciona e ingeniar maneras de franquearlo. Gracias a que se han establecido los canales apropiados, las vulnerabilidades son denunciadas y el código puede ser actualizado.

«Cada vez que ha habido un problema de seguridad con Cryptocat hemos sido completamente transparentes, absolutamente responsables y hemos corregido nuestros errores —declaró el programador—. Fallaremos docenas de veces, si no centenares en los próximos años. Os pedimos que continuéis vigilantes y que seáis cuidadosos. Así es como funciona la seguridad de código abierto.»

Es un modelo de evolución completamente darwinista: cada vez que alguien descubre un agujero nuevo, su programador actualiza el software para proteger su programa de nuevos ataques, haciéndolo cada vez más seguro. O pierde su mercado en favor de una aplicación mejor.

La Red te vigila

*N*avegar es una actividad promiscua. Cada vez que introduces una dirección en el navegador, pinchas en un enlace o buscas una palabra en Google, tu navegador intercambia fluidos digitales con otros ordenadores desconocidos, una jungla de servidores y proveedores de servicios que pueden estar en cualquier parte del mundo y que obedecen a otra legislación.

Son peajes en el universo de la Red, donde dejamos parte de nosotros mismos. En cada uno de ellos revelamos por defecto la composición de nuestro equipo informático, el nombre y versión de nuestro sistema operativo, el nombre y versión del navegador y nuestra localización geográfica, gracias a nuestra dirección IP. Esto pasa docenas de veces con un solo enlace, sin que nosotros tengamos que hacer nada y sin saber quién está escuchando. Y hay mucha gente escuchando. Después de un año de visitas, la incansable maquinaria de registrar metadata ha acumulado miles de páginas sobre nosotros en un archivo que incluye nuestro nombre, dirección, estado civil, financiero y emocional; compras, viajes, amigos, inclinaciones políticas y predicciones acerca de nuestras vidas basadas en todo lo anterior. Esto, sin que nadie nos «vigile» especialmente.

La mayor parte de los datos que se registran son de tipo comercial y funcionan cruzando inmensas bases de datos para saber cosas de ti que ni tú mismo sabes. Target, por ejemplo, es capaz de determinar si una adolescente está embarazada antes de que lo sepa ella misma solo mirando lo que compra. Las recién embarazadas compran miniaturas, cosas de plástico y ropa en colores pastel. Si están de tres meses compran loción sin perfume y suplementos de calcio, magnesio y zinc. Si están de más de seis meses compran bolas de algodón extragrandes y una cantidad anormal de toallitas sanitarias y desinfectantes en gel. Pero mucho más específico: «Si Jenny Ward, que tiene 23 años y vive en Atlanta —explicaba Charles Duhigg en su famoso artículo en *The New York Times*— compra un frasco hidratante de manteca de coco, un bolso lo suficientemente grande para que quepa un pañal, suplementos de zinc y magnesio y una alfombra de color azul pastel, hay un 87 por ciento de probabilidades de que esté embarazada y dé a luz a finales de agosto».

Es verdad que mucha gente compra crema hidratante sin perfume y que, contra lo que pudiera pensarse, hay personas que prefieren los colores pastel sin que su juicio esté fuertemente condicionado por una explosión de hormonas. Pero no es la preferencia por cada uno de esos productos por separado sino una combinación específica de todos ellos lo que nos indica con exactitud la situación de un cliente para poder mandarle cupones que se anticipan a su siguiente necesidad. Y no merece la pena discutir la validez de estas reglas, porque no son las conclusiones de un sociólogo o de un psicólogo sino las de un programador. Por primera vez en la historia somos capaces de cruzar cantidades absurdas de detalles insignificantes para sacar conclusiones estadísticas sobre el comportamiento humano. Bienvenidos a la era del Big Data.

Parece una conspiración, pero en este caso es solo capitalismo aplicado a la Era Digital. Hace unos años, la mayor base de datos personales del mundo no la tenía la CIA ni el FBI sino Wallmart, gracias a un ingenioso sistema por el cual los clientes renunciaban a su privacidad a cambio de un minúsculo descuento en sus compras al final de mes: la tarjeta de puntos. Hoy las entrañas de la Red esconden una máquina despersonalizada y sistemática que registra, procesa, filtra y analiza todos nuestros movimientos con la misma sencilla intención de vendernos cosas. Los Data Centers de Amazon, Facebook, Twitter o

Google no son grandes solo porque guardan todos nuestros correos, ni son ricos solo por vender publicidad.

Si estas cosas pasaran a pie de calle, nos parecerían un ataque ultrajante a nuestra intimidad, pero la mayor parte del tiempo no lo vemos así porque el sistema nos hace creer que su trabajo es hacernos felices. A cambio de nuestra intimidad, la máquina recompone el mundo a la medida de nuestras compras, preferencias, pagos, amigos y recomendaciones. Gracias a nuestra indiscreción, Amazon solo nos ofrece libros que nos gustan, Spotify pincha nuestros grupos favoritos y Facebook sabe quién cumple años esta semana para que compremos el regalo con tiempo y reservemos mesa en el restaurante adecuado. La Red se ha convertido en la más eficiente de las secretarias porque *sabe* quiénes somos mejor que nosotros mismos, pero no trabaja para nosotros. Nosotros somos la carne que está siendo masticada por un mercado tentacular que no está sujeto a una regulación efectiva.

Análisis de Conducta, Análisis de Redes Sociales, Sentiment Analysis, Minería de datos, Escucha activa, Big Data... los nombres no son neutros ni descriptivos, sino todo lo contrario. Cada vez que escribimos algo en un buscador, creamos un usuario en una red social o mandamos un correo por Gmail, aceptamos que la empresa responsable venderá nuestros datos a terceros para hacer cosas con ellos que no sabemos ni nos imaginamos, sin necesidad de autorización, a menudo en lugares donde la ley no nos protege. Nuestros datos cambian de manos a gran velocidad, casi siempre por dinero, a veces por descuido y, en el peor de los casos, por la fuerza. Porque nuestra secretaria es eficiente pero no siempre discreta y hay un número creciente de criminales que se interesan por nuestros números de tarjeta, transacciones bancarias y cartillas médicas.

Todo esto es capitalismo, pero ahora sabemos que también hay conspiración. Desde los atentados del 11 de septiembre de 2001, gobiernos propios y ajenos pinchan nuestros teléfonos, leen nuestros correos y registran nuestras vidas de manera sistemática con intenciones que no son estadísticas ni comerciales. Las nuevas leyes de retención de datos, cuya responsabilidad fue protegernos de la invasión de las empresas, obligan hoy a los proveedores de servicios —Internet, telefonía, transportes— a mantener un diario con las actividades de todos sus usuarios en tiempo real, a veces hasta siete años, para ponerlo a disposición de las autoridades si así lo requieren.

Más aún, la sección 215 de la Patriot Act americana prohíbe a cualquier empresa u organización revelar que ha cedido datos sobre sus clientes al gobierno federal. Eso significa que si el gobierno de Estados Unidos quiere leer tu historial —desde tus cartas de amor a tus chats con disidentes—, las grandes empresas que lo guardan —Google, Facebook o Twitter— están obligadas a facilitar los datos sin poder advertir al usuario de que el registro ha tenido lugar. Ni siquiera pueden poner un papelito que diga que tus pertenencias han sido registradas, como hacen en los aeropuertos con las maletas que facturas.

¿Cómo hemos llegado a esto?

*L*os límites del poder son los que impone la tecnología, y el espionaje de masas es tan viejo como la comunicación de masas. Ya en la década de 1970 se descubrió que la NSA (entonces AFSA o Armed Forces Security Agency) y la CIA habían estado espiando a los ciudadanos norteamericanos desde agosto de 1945, con la generosa colaboración de las tres principales compañías de telégrafos del país: Western Union, RCA e ITT.

La NSA operaba sin orden de registro y sin que existiera información previa que justificara la vigilancia. En su momento de mayor actividad, el PROYECTO SHAMROCK (así se llamó), era capaz de recoger, imprimir y analizar hasta 150.000 mensajes al mes. Cuando el comité del Senado cerró la operación en 1975, la NSA tenía guardada información de más de 75.000 ciudadanos; a esto se lo llamó «el mayor programa de interpretación del gobierno americano sobre los americanos jamás realizado». Hoy el centro que ha construido la NSA en Utah tendrá capacidad para recoger, procesar y almacenar «todo tipo de comunicaciones, incluyendo el contenido de correos privados, llamadas telefónicas y búsquedas en Internet, así como toda clase de huellas digitales: recibos del párking, itinerarios de viaje, compras de libros y otra "calderilla digital"».

Además de la NSA, la CIA tenía sus propios programas de espionaje doméstico. La notable Operación Chaos estaba destinada a vigilar y desacreditar a los líderes del movimiento estudiantil y alimentar la batalla contra Fidel Castro. El proyecto Cointelpro (un acrónimo mal resuelto de Counter Intelligence Program) también era parte de un programa para vigilar y desacreditar organizaciones y líderes de movimientos políticos, de los Panteras Negras a Mujeres por la Paz, incluyendo miembros del Senado y cualquier figura que rechazara públicamente la Guerra de Vietnam, sin olvidar al doctor Martin Luther King. Los programas empezaron con Lyndon B. Johnson y fueron heredados por Richard Nixon, que perdió la presidencia precisamente por un escándalo de espionaje. Cuando estalló el Watergate, el entonces director de la NSA, Lew Allen, archivó los proyectos. Pero no cerró el chiringuito, porque un país como Estados Unidos no puede vivir sin sus agencias de inteligencia. Para controlarlas, el mismo comité del Senado que había ordenado la desaparición de los programas de espionaje doméstico se inventó un freno de mano legislativo al que llamó la Foreign Intelligence Surveillance Act (FISA). Su trabajo era vigilar a las agencias de inteligencia para que no volvieran a las andadas, y eran responsables de producir o denegar órdenes de registro y asegurarse de que no se mancillaban los derechos constitucionales de los ciudadanos.

El otro freno de mano fue la famosa Directiva 18, el manual de procedimiento interno donde se regula el uso de las «señales de inteligencia» (*sigint*), que es como llamaron a la captura «accidental» de señales ciudadanas sin previa orden de registro. Ha sido precisamente esta directiva, y su interpretación por parte de FISA, lo que ha hecho posible por ejemplo que la NSA capture «accidentalmente» todas las llamadas telefónicas que han hecho los ciudadanos norteamericanos desde 2006, lea sus correos o ponga escuchas en los servidores de Google, Facebook o Yahoo.

En treinta años, los dos frenos de mano que impuso el Congreso para protegerse de los abusos de su propia agencia de seguridad se han transformado en embrague y acelerador. Peor aún es que dichas operaciones han tenido el apoyo de todos los poderes políticos; George W. Bush lo puso en marcha, Obama lo mantuvo y quince jueces de FISA

lo han declarado constitucional.

Hay quien se pregunta por qué nos importa tanto lo que pasa en Estados Unidos. La pregunta es legítima pero ingenua. El escándalo no es que la NSA haya espiado sino que *ha espiado a ciudadanos norteamericanos*. Espiar a ciudadanos de otros países es perfectamente legítimo bajo la legislación norteamericana, incluso si esos extranjeros son la canciller alemana Angela Merkel o el primer ministro israelí Ehud Olmert.

La mayoría piensa que, si no tiene nada que ocultar, no tiene nada que temer. Es una mentira que por mucho que se repita no deja de serlo. Para empezar, sabemos que las Agencias de inteligencia de Estados Unidos y del Reino Unido nos espían, pero no sabemos lo que están haciendo las de Corea, Venezuela, Bielorrusia o Brasil. La Red no estaba diseñada para convertirse en el circo de miles de pistas en el que se ha convertido y las empresas que la han rediseñado no han invertido en infraestructura para proteger a los usuarios, porque hasta hace poco nadie se lo había pedido. Internet se ha llenado de sofisticados software espía que son usados por cientos de miles de adolescentes aburridos en sus dormitorios, solo porque están a mano. Por cada informe escandaloso que se publica sobre los programas de la NSA hay cientos, probablemente miles de organizaciones desconocidas y peligrosas acumulando e intercambiando datos. Deberíamos protegernos porque la Red se ha convertido en un lugar peligroso, pero nos seguimos comportando como si fuera Tiffany's, *el lugar donde no te puede pasar nada malo.*

Pero aunque no lo fuera, deberíamos protegernos. La ley que protege nuestro derecho a hacerlo ha costado muchas guerras y muchas vidas. No siempre es conveniente vivir a cara descubierta. Gracias a WikiLeaks sabemos que Gadafi contrató servicios de empresas europeas para espiar a sus propios ciudadanos y «neutralizar» a los disidentes antes de que salieran a la calle, y que no es el único. En nuestro país se proponen reformas del Código Penal donde se plantea encarcelar a ciudadanos por apoyar una manifestación en Twitter. Cuando nuestros representantes no pelean por defender nuestros derechos sino contra nuestro derecho a ejercerlos, la única respuesta es la desobediencia. Puede que no tengamos nada que ocultar, pero sí tenemos mucho que temer. En una sociedad ultravigilada, todo el mundo es antisistema.

Estructuras de Red: quién controla Internet

*L*awrence Lessig dice que tres cosas regulan la red: los mercados, la ley y el código. Las herramientas usadas para la circunvalación de comunicaciones no son necesariamente las mismas que protegen la identidad de sus protagonistas. Cuando un intercambio de información delicada tiene lugar entre dos partes, no basta con que el contenido esté encriptado; también es esencial proteger la ruta de transmisión. Las infraestructuras de Red no son libres, están en manos de compañías y agencias gubernamentales que tienen acceso directo a los canales de transmisión de datos.

La información querrá ser libre pero su capacidad de movimiento es realmente muy limitada. Esto es porque, como explicaba Neal Stephenson en su formidable ensayo *Mother Earth Mother Board* (*Wired,* 1996), la información solo tiene tres maneras de moverse: en brazos (libros, disco duro, vecinas), por ondas de radio (satélites, antenas) y por cable electrificado. Gracias a la popularidad del wifi, la mayor parte de los usuarios de la Red piensan que Internet es algo que flota libremente en el aire, como el oxígeno, un recurso natural. Pero ese complejo entramado de telecomunicaciones que llamamos Internet es un consorcio de más de 40.000 redes enlazadas a través de antenas, satélites, grandes centros de procesamiento de datos y, sobre todo, dos millones y medio de kilómetros de fibra óptica, que no son estructuras públicas ni funcionan de acuerdo con la regulación de los países a los que sirve, incluyendo las leyes de protección de datos.

En EE.UU., el 95% de las comunicaciones viene por cable. Como se puede ver en la web submarinecablemap.com, las autopistas de la información tienen todavía menos dueños que los grandes tubos de petróleo que nos proporcionan agua caliente y calefacción. Son infraestructuras fuertemente centralizadas, cuyo valor geopolítico es cada día mayor —la mano que sujeta el cable es la mano que domina el mundo—. Y, a pesar de esto, son estructuras frágiles, como quedó patente el día que la guardia costera egipcia descubrió a tres buceadores cortando cables cerca de la costa de Alejandría en marzo de 2013.

La red de autopistas submarinas que conecta artificialmente lo que ha separado el mar tiene doscientos cables que tienden a uno y otro lado de los continentes, concentrándose necesariamente en puntos estratégicos. Egipto es uno de esos puntos y la línea atacada (SEA-ME-WE 4) es uno de los cuatro cables que conectan Europa, Oriente Medio y el continente asiático. Evidentemente, este cordón umbilical es de extrema importancia para todos los países implicados y los saboteadores no eran aficionados, ni gamberros ni acababan de llegar. Antes de ser capturados, ya habían causado graves daños en otros nodos importantes (I-ME-WE, TE-North, EIG y SEA-ME-WE-3), ralentizando las comunicaciones en Pakistán hasta un 60% y las globales un 30%. Curiosamente, nadie les estaba buscando; la patrulla que les descubrió lo hizo por casualidad. No hay nadie vigilando las arterias de la Información.

Lo cierto es que los cables submarinos llevan una existencia llena de callados peligros en la oscuridad del suelo oceánico. Cuando no hay desastres naturales, la infraestructura sufre accidentes constantes con anclas de buques, submarinos, barcos de pesca, marañas de redes abandonadas llenas de basura. Cuando las redes se ralentizan, se asume que ha habido un problema y que la teleco correspondiente irá a solucionarlo. «Ha habido un fallo en la línea submarina de cable a Pakistán a través de Alejandría, Egipto —declaró Wateen Telecom—. El cable de fibra óptica ha sido dañado por motivos desconocidos.»

El sabotaje coincidió además con el famoso ataque a Spamhaus, cuyo responsable fue detenido hace unas semanas en Barcelona. Los expertos dijeron entonces que el bombardeo de 300.000 millones de bits por segundo que habían sufrido los servidores de la compañía suiza podría haber congestionado la Red a nivel global. Pero lo más probable es que fuera el cable dañado, cuyo mal funcionamiento no solo limita el tráfico de la zona sino que sobrecarga el de las demás, generando una situación de colapso internacional.

Pero no siempre se trata de un ataque. En 2007, un barco pirata robó unos trozos de cable en la costa de Vietnam pensando que contenían cobre (los piratas son gente muy anticuada). El 28 de marzo de 2013, una campesina de 75 años natural de Georgia dejó a tres millones de armenios desconectados del resto del planeta durante la friolera de doce horas. Cuando le preguntaron por qué lo había hecho, la pobre anciana explicó que andaba cortando leña para su chimenea y que se llevó el cable con la hoz sin darse cuenta. Ni siquiera sabía lo que era Internet.

El bonito mapa de TeleGeography (telegeography.com) muestra nuestras comunicaciones intercontinentales combinando cartografía victoriana con las estructuras de los mapas de metro y ferrocarril. Está lleno de datos interesantes, como quién consume más ancho de banda (EE.UU.), un histórico de la capacidad y consumo creciente de las redes y una media del tiempo que tarda la información en llegar de un lado a otro (el ping).

Pero lo más importante se entiende sin explicaciones: hay países cuya conexión a la Red cuelga literalmente de un hilo, cuya destrucción sería un apagón o una nueva clase de embargo. En submarinecablemap.com, menos bonito, vemos que la conexión de millones de personas depende de una sola compañía que a menudo opera a miles de kilómetros de su país. Esto significa que la supervivencia de un país depende de un gobierno que no ha sido votado democráticamente, un consorcio de multinacionales que opera según las leyes de mercado, no la regulación local.

Además de la contingencia del fondo marino, nuestra infraestructura global es vulnerable a los problemas derivados de la relación entre vecinos que están conectados tecnológicamente, pero no social, política y económicamente. Israel, que está rodeado de enemigos pero apadrinado por una superpotencia lejana, debe conectarse por un cable que pasa por Chipre, Sicilia y Grecia. Palestina depende en parte de la conexión a Israel (!) y en parte de los operadores europeos que tienen un pie en Jordania y que se enganchan al cable que cruza Arabia Saudí y la línea FLAG, protagonista del ensayo de Stephenson.

La red de cables submarinos está regulada desde 1982 por la Convención de las Naciones Unidas sobre el Derecho del Mar y esta prescribe que, en aguas internacionales, «todos los estados tienen derecho a tirar cable submarino y a mantenerlo y repararlo como sea conveniente». Los estados costeros, sin embargo, pueden ejercer su soberanía en un cinturón náutico de doce millas en la costa adyacente a su territorio nacional.

Teóricamente, para denegar el desembarco de cables cerca de su costa, un país debe alegar un motivo razonable, normalmente relacionado con la protección medioambiental (bancos de pesca, corales, etc), pero la soberanía es problemática cuando está en juego una infraestructura que nos afecta a todos. El cable que enlaza Singapur con Australia SEA-ME-WE-3 ha estado caído durante meses, porque el operador no consigue permiso del Gobierno de Indonesia para meter máquinas en sus aguas. Y, aunque el presidente sirio Bashar al-Assad asegura que los «apagones» en su país son ataques terroristas, las organizaciones de internautas y medios aseguran que él mismo ha «apagado» la Red para tener controlada la «insurrección», igual que el gobierno de Egipto apagó la Red el 28 de enero de 2011 para silenciar y disolver la protesta.

Tener dos cables tampoco garantiza nada: en 2008, dos cables de dos compañías distintas fallaron a la vez, dejando completamente incomunicados a Egipto, Pakistán, Kuwait y la India, y parcialmente incomunicados a Líbano y Argelia. El hilo que seguía Neil Stephenson en su ensayo para *Wired* se colapsó durante el terremoto de Taiwán en 2006, cortando todas las comunicaciones en Hong Kong, China y el sudeste asiático.

El origen del monopolio: la Gran Red Victoriana

Parece poca cosa pero, antes de que Samuel Morse lanzara el primer cable entre Washington y Baltimore en 1844, la información iba siempre en brazos. El primer cable submarino internacional unió la Gran Bretaña con Francia a través del estrecho de Dover con gran esfuerzo y dinero de los hermanos John Watkins y Jacob Brett en 1850. Era un largo cable de cobre que fue a morir inmediatamente en el ancla de un solo pescador. Pero no fue en vano, porque el experimento les valió para afianzar la licencia y el futuro control de las telecomunicaciones. Tras una instalación accidentada, el primer cable transatlántico submarino consiguió conectar Irlanda con Terranova (agosto de 1858). Duró solo tres semanas, antes de que los cables cedieran a las inclemencias del suelo marino y la mayor parte de los inversores huyeran, pero el gran proyecto de conectividad global consiguió estabilizarse diez años más tarde gracias al apoyo gubernamental y a una fabulosa resina de las colonias asiáticas llamada gutapercha. Fue el principio de un desarrollo que se extendió por todo el planeta, gracias a las muchas colonias del Imperio británico y a su superioridad naval.

Entonces Internet era la Atlantic Telegraph Company, la misma AT&T Corp. que llevó el primer cable transoceánico de fibra óptica de Nueva Jersey a Inglaterra en 1988. La leyenda asegura que podía soportar hasta 40.000 conversaciones telefónicas al mismo tiempo.

La alianza de cinco ojos: NSA, GCHQ y todos sus amiguitos

Más de cien años más tarde, en lo más duro de la guerra fría, el gobierno norteamericano descubrió un cable en la costa este de Rusia que conectaba las dos principales bases navales soviéticas. Nixon quería saber cómo llevaban los rusos el desarrollo de sus misiles balísticos intercontinentales y el programa nuclear, así que la NSA empezó una operación —nombre en clave Ivy Bells— para intervenir sus comunicaciones.

Se enviaron dos submarinos de ataque con un equipo especial de buceadores para plantar micros en la línea. Los buceadores entraban cada dos semanas en agua enemiga, fuertemente vigilada por submarinos rusos, para recoger las cintas y llevarlas a la base norteamericana (la tecnología de almacenamiento no había entrado en su era dorada) donde el servicio de inteligencia transcribía rápidamente el material. Y así estuvieron escuchando a la armada naval rusa durante casi una década, hasta que un especialista en análisis y transcripción de voz de la agencia llamado Ronald Pelton, acosado por las deudas, le vendió la exclusiva a la embajada soviética por 35.000 dólares.

Pelton fue juzgado y condenado a tres cadenas perpetuas consecutivas en 1986, que seguirá cumpliendo en el correccional de Allenwood, Pensilvania, hasta noviembre del año que viene. Teóricamente, la operación Ivy Bells también había quedado enterrada, pero un artículo de *The Guardian*, basado en documentos de Edward Snowden, demostró que hay al

menos dos programas de espionaje masivo en funcionamiento usando la misma táctica: «Mastering the Internet» y «Global Telecoms Exploitation», a cargo de la mejor amiga de la NSA, la agencia de espionaje británico GCHQ.

El programa incluye la recolección de llamadas telefónicas, contenido de correos, conversaciones del Facebook y todo el historial de movimientos de los internautas y, con permiso del bienintencionado Lawrence Lessig, es perfectamente legal. El truco es el mismo que usó Hitchcock en *Extraños en un tren* (1951): las leyes de ambos países prohíben explícitamente el espionaje de sus propios ciudadanos, así que la NSA y la GCHQ han hecho un intercambio de ciudadanos: EE.UU. espía los cables británicos (programas OAKSTAR, STORMBREW, BLARNEY Y FAIRVIEW) y la Gran Bretaña espía los norteamericanos, para luego intercambiar archivos. Ni siquiera tienen que mandar submarinos porque los cables son *suyos*.

Snowden le dijo al *Guardian* que «la GCHQ es peor que la NSA», posiblemente su primer comentario ocioso. En lo que respecta al resto del mundo, son perfectamente indistinguibles. De acuerdo con sus documentos, en 2010 las dos agencias se palmeaban la espalda para celebrar la «alianza de los cinco ojos», un entramado de vigilancia de doscientos cables de fibra óptica que incluye las infraestructuras de los EE.UU., Reino Unido, Canadá, Australia y Nueva Zelanda. O sea, la mayor parte del tráfico de las comunicaciones.

Si el primer cable de telecomunicaciones transoceánico era capaz de soportar hasta 40.000 conversaciones telefónicas al mismo tiempo, la agencia británica es capaz de «procesar» hasta seiscientos millones de llamadas al día. Un equipo de analistas —trescientos de GCHQ y 250 de la NSA— dedican todo su tiempo a transcribir las señales y cruzarlas con el resto de datos que capturan por otras vías. Todo ese contenido es almacenado en sus Data Centers. Si los cables submarinos son las arterias de la Red, los Data Centers son sus neuronas, el lugar donde van a parar las vidas privadas de todos nosotros. Los gobiernos y compañías que dominan la Red guardan más documentación sobre cada uno de nosotros que la Stasi sobre los disidentes de Alemania Oriental, y los archivos no están tan descentralizados como nos gusta imaginar.

Data Centers: la Nube con forma de Stasi

Si una noche de invierno un viajero se encontrara de pronto con un gran complejo industrial protegido por varias capas de hombres, armas, perros y alambre de espino, lo más probable es que fuera a) un Centro de Internamiento de Extranjeros, b) una granja de producción intensiva o c) un Data Center. Las tres construcciones guardan prisioneros que han perdido todos sus derechos: animales, detenidos sin cargos y datos personales, privados e intransferibles.

Además de la protección militar, diseñada para contener lo que hay dentro y para frustrar la curiosidad de los que están fuera, las tres instituciones disfrutan de una última capa de invisibilidad legal que protege sus secretos de vecinos, abogados, activistas, espías o reporteros. Pero hay diferencias: si el hedor y el sonido de los animales hacinados revelan rápidamente la granja, para descubrir al Data Center nos basta una factura de la luz. Según Google, los suyos consumen unos 260 millones de vatios, la cuarta parte del consumo energético de una central nuclear. Pero esos son sus números y nos los tenemos que creer.

Mientras las paguen, ninguna empresa está obligada a enseñar sus facturas y ninguna lo hace. Irónicamente, estas largas catedrales de servidores, cables, unidades de almacenamiento masivo y circuitos de refrigeración disfrutan el mismo grado de protección de datos que el Pentágono.

El almacenamiento se ha devaluado medio millón de veces desde que IBM presentó el primer disco de un giga en 1980, pero Internet crece a una velocidad de un exabyte al día, más de un millón de terabytes. Cisco augura que en tres años los grandes Data Centers estarán manejando 1.3 zettabytes, que son 1300 exabytes, que es como enviar todas las películas jamás producidas cada tres minutos. El centro que ha construido la Agencia Nacional de Seguridad norteamericana en el desierto de Utah será capaz de contener un yottabyte de información, el equivalente a 1.000 zettabytes o 500.000.000.000.000.000.000 páginas de texto. Qué modesto parece en comparación el Ministerium für Staatssicherheit, con sus 111 kilómetros de archivos, 47 de películas y 90.000 sacos de papel que los funcionarios hicieron trizas en diciembre de 1989.

Contra todo pronóstico, Utah es solo el segundo más grande del mundo. Le supera en metros el Range International Information Hub de Langfang, el faraónico Silicon Valley de China, que tiene 620.000m2. Con tecnología y mano de obra de IBM, en 2016 China sigue con su plan de transformar la antigua provincia ganadera del Hebei en el gran centro neurálgico de las telecomunicaciones asiáticas y de paso el mayor Centro de Datos del planeta. El nudo del proyecto es un conglomerado de telecos que incluye China Telecom, China Unicom, China Mobile, Beijing University of Posts and Telecommunications, Beijing Telecommunications Planning Design Institute, CORGAN, Gehua Cable o plataformas de servicios online como Qzone, el Facebook asiático.

Solo en servidores, el Utah Data Center ocupa 100.000 m2. La nueva planta de la NSA está en el desierto de Utah, pero hay muchas más en Colorado, Georgia o Maryland y plantas secretas fuera de EE.UU. Su misión es procesar «toda forma de comunicación, incluyendo los contenidos de correos privados, conversaciones telefónicas, búsquedas en Internet y todo tipo de datos personales: tickets de párking, itinerarios de viaje, compras con tarjeta y otras menudencias virtuales». O, como diría la Gestapo más concretamente, investigar y combatir «todas las tendencias peligrosas para el Estado» bajo el amparo de la Patriot Act y criptografía de vanguardia. Antes de su inauguración oficial en septiembre ya había sido rebautizada como la Estrella Negra de la minería de datos.

Qué diferencia con el Pionen Data Center de Suecia, al que los vecinos lo llaman cariñosamente el Centro de Datos de Malo de James Bond. Estos grandes archivadores están enterrados en un antiguo refugio nuclear que palpita bajo las Montañas Blancas de Estocolmo que fue recuperado por la teleco sueca Bahnhof. Dispone de 8.000 servidores capaces de sobrevivir a desastres nucleares, terremotos y apagones, gracias a dos motores submarinos alemanes que funcionan con diésel. Dicen que Julian Assange guarda sus secretos más valiosos aquí, pero todos sabemos que el fundador de WikiLeaks esconde sus tesoros a plena vista y solo se queda la llave. Moraleja: no importa dónde estén tus datos siempre que nadie los pueda leer.

Fuera de las grandes agencias de espionaje, la liga de campeones se la reparten Google, Facebook, Apple y Microsoft. Cada vez que alguien usa el buscador, mira un video

de Youtube, recibe un correo de Gmail o comparte una canción en Spotify; cada palabra en el muro de Facebook, cada llamada por Skype pasa por al menos uno de los centros multimillonarios que han sustituido a las grandes fábricas de la segunda revolución industrial en regiones de las que nadie se acordaba. Google tiene diecinueve centros en EE.UU., doce en Europa, tres en Asia, uno en Rusia y otro en Sudamérica pero su caballo de batalla está en Council Bluffs, Iowa, y este año empieza lo que algunos llaman con cierta histeria la mayor expansión de la historia. La compañía ofrece una visita guiada en YouTube, un mapa en Street View de su centro en Carolina del Norte y una serie de bucólicas fotos para los amantes de la ingeniería.

Apple tiene plantas en Newark, Santa Clara y Cupertino pero el gordo —cinco veces más gordo que cualquiera de los demás— está en Maiden, Carolina del Norte, y en 2013 empezó otros dos en Oregón y Reno. La gran nube de Microsoft está en Boydton, Virginia, en un pueblo de 431 habitantes. Facebook ha plantado la suya en Prineville, Oregón, del que también hay fotos. Todas esas compañías —y sus colaboradores, asociados, clientes y gobiernos— lo saben todo de nosotros. Y así seguirá siendo mientras los mercados, la ley y el código hagan equipo para protegerse unos a otros a expensas de nuestra privacidad.

Curiosidad: descubre cuánto sabe Facebook sobre ti

Si alguna vez han pensado en lo fácil que resultará en el futuro escribir su biografía, estarán encantados de saber que Facebook ya se ha puesto a trabajar, aunque de momento se parezca más a *La vida de los otros* que a *El escritor fantasma* de Polanski. Un *hacker* australiano llamado Nik Cubrilovic descubrió que el sistema toma nota de todas las actividades de los usuarios incluso fuera de casa, aprovechando un camino de miguitas al que todos hemos contribuido: el botón de «Me gusta». Donde esté ese pequeño trozo de código con el que decoramos nuestros posts, compras, comentarios, ahí está Facebook tomando nota.

La buena noticia es que no hará falta esperar a que caiga el muro para exigir esos expedientes, como hicieron los alemanes en junio de 1990 a las puertas de la Stasi. La empresa tiene residencia legal en Irlanda, lo que significa que está sujeta a la Directiva europea de Protección de Datos y que, por lo tanto, cualquier interesado que solicite datos personales tiene derecho a obtenerlos «sin restricciones a intervalos razonables y sin excesiva demora o gasto». Para ejercitar dicho derecho, el grupo austríaco Europe versus Facebook ha preparado esta receta.

Facebook tiene escondido en su servidor un documento para solicitar datos personales, que ahora mismo está escondido bajo «Privacidad. Preguntas sobre nuestra política de privacidad. Solicitud de datos personales» pero cambia todo el rato de lugar. El formulario pide todos los datos personales y una copia del DNI, que hay que escanear (o hacerle una foto) y subir al sistema desde nuestro disco duro. Un detalle: si nuestros datos de usuario no coinciden con la documentación oficial, hay que cambiarlos para que lo hagan. No solo validará el proceso; he notado que después se siente uno mejor cuando «al enviar este formulario declaras bajo pena de perjurio que toda la información enviada es correcta y verdadera».

Curiosamente, el formulario también pide que citemos la ley que ampara la petición. El nombre oficial de la Directiva europea es 95/46/EC y la ley que nos interesa pertenece a la sección V, artículo 12. En el formulario pondremos «Section 5 DPA Art. 12 Directive 95/46/EG». El formulario es sencillo; lo difícil es recibir confirmación de que vamos a recibir un CD con todo el material. Según la regulación irlandesa, la empresa tiene cuarenta días para mandarlo. El verdadero viaje es enfrentarse al PDF monumental que viene dentro. Pensarás que caminas en sueños y que solo Facebook sabe a dónde vas.

El manual

«El enemigo conoce el sistema.»

CLAUDE SHANNON

Contraseñas: buenas, malas y peores

*H*ay tres maneras de proteger un mensaje. La más elemental es no mandarlo, aunque entonces no podemos hablar de comunicación sino de secretos. La segunda es convertir el mensaje en algo ilegible; eso es criptografía. La tercera se llama estenografía y consiste en camuflar el mensaje, haciéndolo desaparecer dentro de otro mensaje. En Internet, la criptografía se ha convertido en la única herramienta efectiva para protegerse de la vigilancia corporativa y gubernamental, pero es una carrera constante. Como dice Claude Shannon, el enemigo conoce el sistema. Tenemos que conocerlo mejor que él.

En un mundo fuertemente digitalizado, la contraseña es el único obstáculo que se interpone entre nuestra intimidad, nuestras comunicaciones, nuestro dinero y nuestros sistemas de seguridad y el resto del mundo. Y sin embargo, las empresas de seguridad publican cada año informes que dicen que el 98 por ciento de la gente sigue utilizando 1234, admin o admin123.

Es absurdo, pero invertimos más tiempo en elegir la clase de azúcar que le ponemos a los cereales o el color de las cortinas del baño que en proteger las cosas que más nos importan en esta vida. Y cuando las pensamos durante más de cinco segundos, casi siempre producimos contraseñas fácilmente identificables para cualquiera que nos conozca un poco, aunque sea por Facebook.

Si tu contraseña es la combinación de los nombres de tus hijos, la fecha de nacimiento de tu madre o el pueblo al que fuiste de luna de miel, necesitas cambiar de estrategia. Estas son las cinco reglas de oro para proteger tu identidad.

1. Aprende a hacer contraseñas seguras

El estándar de seguridad en una contraseña es que debe tener ocho caracteres o más, y que debe incluir una mezcla no significativa de letras y otros caracteres, que pueden ser números pero también, cuando el sistema lo permite, símbolos. Por ejemplo:

XXTHEENEMYKNOWSTHESYSTEM=45

Efectivamente, podemos cumplir los requisitos utilizando el nombre de nuestro primer perro y la fecha de su cumpleaños. A eso me refería cuando dije «no significativa». Cuanto más información contenga la contraseña, por remota que parezca, más posibilidades hay de que la descubra alguien. Recuerda que no eres el único aireando las historias de la familia en el Facebook, el resto de tu familia —padres, hermanos, primos, tíos— también están allí.

Evidentemente, el impulso autodestructivo que nos lleva a elegir contraseñas fáciles es que queremos recordarlas luego. De nada nos sirve tener la contraseña más compleja del mundo si somos incapaces de recordarla o tenemos que llevarla escrita en la cartera.

Los expertos aconsejan utilizar uno de los muchos generadores de contraseñas que hay disponibles en la Red, que cumplen todos los requisitos de seguridad sin que tengamos que pensar. Son combinaciones poco agraciadas pero, si generamos muchas contraseñas, antes o después aparecerá una que podremos recordar más fácilmente que las otras, quizá porque nos recuerda a algo en concreto o porque la combinación de teclas nos resulta particularmente agradable a la vista. Incluso hay generadores que ya cuentan con esa

necesidad, como onlinepasswordgenerator.com.

2. Aprende a memorizar contraseñas seguras

Si somos incapaces de recordar una clave autogenerada, la otra opción es usar una frase que conozcamos bien y modificarla, sustituyendo unas cuantas letras por unos cuantos números o añadiendo algún símbolo aquí y allí. Mejor que no sea parte del cancionero popular, el estribillo de la canción de verano o «Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura». Cualquier secuencia de caracteres que genere al menos una respuesta en Google debería quedar descartada de antemano porque en todos los bares hay alguien que conoce *La Divina Comedia*. Los *crackers* —que es como se llama a los *hackers* que se dedican a destripar contraseñas— usan bases de datos con millones de combinaciones conocidas y, si eliges un estribillo de Bob Dylan, lo más probable es que esté en el *top ten*.

Mejor que sea la primera estrofa del poema que le escribiste a la primera chica de la que te enamoraste. Pongamos que te lo aprendiste de memoria antes de quemarlo junto con todas sus fotos y los restos de tu corazón destrozado y que nunca lo volviste a ver. Cambias rosa por cardo y espinas por garfios y lo aliñas con unos cuantos números. Ya tienes una contraseña difícil de la que nunca te vas a olvidar.

Tampoco lo sustituyas siguiendo un patrón reconocible. Hasta hace unos años, estaba de moda entre los programadores usar un lenguaje que llamaron *133t*, un derivado de «elite» donde se sustituye la letra «e» por un 3, la «a» por un 4, la «l» por un 1 y la «o» por un 0. Este es, posiblemente, el «lenguaje secreto» más popular de Internet y hasta las bases de datos de contraseñas más anticuadas del mundo han asimilado el 133t como parte de su vocabulario. Eso incluye el esperanto, el volapük y cualquier idioma que hablen los elfos, los dragones, los ewoks y todas las colonias intergalácticas. Cuanto más idiosincrática y menos lógica sea la secuencia, más segura es. Cuanto más de moda esté y en más libros y películas aparezca, más vulnerable.

3. Usa contraseñas distintas para cada cosa

¿Tienes la misma contraseña en Facebook, Twitter, Instagram y Pinterest? La estadística revela que la mayor parte de los usuarios repite la misma contraseña para todos los servicios que usan o han usado en los últimos siete años, el equivalente digital a tener una sola llave para la casa, el coche, el buzón y la oficina y dejarla bajo el felpudo. ¿Es la misma que usabas en MySpace, Flickr y Second Life? Entonces es seguro que tu contraseña ha sido comprada y vendida muchas veces.

Ciertamente, es difícil acordarse de una contraseña, más aún acordarse de varias. Los principales navegadores ofrecen como solución una llave maestra: nosotros elegimos una contraseña (pongamos, el poema modificado del punto anterior) y el navegador genera una clave distinta para cada servicio. Este sistema tiene un fallo evidente: si alguien tiene acceso a la llave maestra tiene acceso a todo; si perdemos el portátil o el navegador, nos quedamos fuera de todo.

En principio, es mejor solución que usar la misma contraseña para todo y peor solución que tener una buena contraseña para cada cosa. Un saludable punto intermedio es lo que se llama un llavero o Keychain, como *Keepass*, que guarda todas las contraseñas

protegidas por una contraseña maestra pero en una web remota, bien lejos de nuestro ordenador. Si alguien descubre la contraseña principal todavía tenemos un problema, pero, para poder usarla, primero tiene que adivinar el lugar donde hemos guardado el resto.

4. Cambia de contraseñas con frecuencia

El otro día descubrí que un exnovio al que no veía desde hace doce años sigue usando la misma contraseña que el día que nos conocimos. Y como además la usa para todo, si yo fuera mala persona —o peor, una exnovia despechada— podría dedicarme a enviar tweets en su nombre, insultar a sus amigos desde su muro de Facebook, comprar perfumes caros con su cuenta de Amazon y subastar sus pertenencias en eBay usando sus fotos privadas de Flickr y cobrarlo todo en su PayPal, antes de desviarlo a mi cuenta. ¿Y si fuera un enemigo de verdad?

Hasta las tarjetas electrón caducan a partir de cierto tiempo. La clave privada se autodestruye cada cinco años, pero nuestras contraseñas deberían cambiar mucho más a menudo, dependiendo de nuestras circunstancias y del grado de peligrosidad de nuestras actividades.

Evidentemente, algunas contraseñas son más importantes que otras. No vale igual la contraseña de la BIOS o tu clave *root* de administración que la contraseña del Flickr, pero cada ventana, por pequeña que sea, es un punto de vulnerabilidad. No olvidemos que las redes sociales guardan mucha más información sobre nosotros de la que se refleja en nuestros perfiles, incluyendo localización geográfica, horas de actividad y contactos más frecuentes dentro y fuera de sus fronteras.

5. No compartas tus contraseñas

Lo dice el refrán: dos pueden compartir un secreto siempre y cuando uno de los dos esté muerto. El amor es un gran invento y hasta es posible que tu pareja sea tu alma gemela y que nunca tengas que arrepentirte. Pero, si le has dado tu contraseña, debes cambiarla lo más rápidamente posible. Si usas la misma contraseña para todo, debes cambiarlas todas. Y si se enfada porque ya no tiene acceso a tus correos, documentos o plataformas de administración privadas, debes cambiar de pareja.

Lo mismo pasa con colaboradores, colegas, madres, jefes, empresas, servicios y redes. Una contraseña que conoce otra persona es una contraseña muerta. Hay que saber dejarla.

Correos

Tipos de correos, tipos de conexiones, elegir un correo para cada cosa, cómo encriptar el correo con PGP

*E*l correo electrónico es, junto con el teléfono, la manera más popular de comunicarse, pero también la más misteriosa. Hasta un niño puede explicar cómo llega una carta desde el remitente a su destinatario pero, cuando se trata de explicar cómo llega el e-mail a su carpeta de entrada, hasta los adultos más escépticos despliegan narrativas de gran valor surrealista, más inspiradas por el realismo mágico de *Matrix* que por la realidad. Lo cierto es que los correos que enviamos pasan por muchas manos antes de llegar a su destinatario; solo entre las de proveedores de telecomunicaciones y las proveedoras de servicio pueden llegar a cien.

Cuando enviamos un correo sin haberlo protegido primero, tanto la contraseña como el contenido del correo salen a la Red como texto limpio, perfectamente legible. Cualquiera que tenga las herramientas adecuadas —y no hace falta ser un *hacker*, hoy los GUIs del software espía son más fáciles de usar que Photoshop— puede capturar la información y leerla sin esfuerzo.

Siempre que sea posible hay que mandar los correos a través de protocolos de transferencia de datos seguros, como SSL o TSL. La mayoría de los clientes de correo incluyen la opción, pero en muchos casos hay que seleccionarla porque no se usa por defecto. Pero cuidado: cuando enviamos un e-mail, la conexión que establecemos solo es de nuestro ordenador al servidor de correo y nuestro túnel SSL nada más los protegerá hasta allí. La mejor manera de asegurar la integridad de nuestros mensajes es combinar SSL con un programa de cifrado para el propio mensaje. Para eso existe la PGP.

Pero antes de adentrarnos en el maravilloso mundo del encriptado de clave pública, debemos considerar otro tipo de correos que pueden resultar útiles para momentos concretos.

Para gargantas profundas: correos de usar y tirar, identidades con fecha de caducidad

Un pequeño *disclaimer*: el único correo cien por cien seguro es el que no ha sido enviado. Todos los correos contienen información útil sobre la persona que lo envía, lo único que podemos hacer es limitar esa información al mínimo, o adulterarla hasta que no sirva para nada. Si queremos transmitir información delicada y no queremos que nadie la intercepte, lo mejor es hacerlo sin conectarse a la Red. Ahora bien, si no nos queda más remedio que comunicarnos a través del correo electrónico, nuestras opciones dependerán de la clase de problema al que nos enfrentamos o, más concretamente, de quién queremos proteger nuestra identidad.

Los correos de usar y tirar son cuentas de vida muy corta, al final de la cual no solo desaparece su contenido sino la cuenta de correo desde la que se envió. El servicio suele funcionar a través de un servidor que hace de proxy entre nosotros y nuestro destinatario, recogiendo el mensaje y la dirección a la que debe llegar y enviándolo desde otro lugar, con una dirección genérica. Es el formato apropiado si queremos enviar un soplo, unos

documentos o dar un chivatazo sin que nadie sepa nunca quién lo hizo, ni siquiera (o especialmente) nuestro interlocutor. También es perfecto si queremos abrir una cuenta de correo (o de Twitter, o un blog) anónima, donde el proceso normalmente requiere de una dirección de correo alternativa para usar de referencia y enviar la confirmación. Y, por qué no, para esquivar el spam.

Es esencial escoger bien el servicio. Antes de mandar un correo de este tipo, es importante recordar que nuestro nombre es solo uno de los muchos elementos que traicionan nuestra identidad y que, aunque el receptor no sepa que somos nosotros, la compañía sí lo sabe. Hasta los servicios de correos anónimos están obligados a mantener los logs de los usuarios, un registro de movimientos que incluye fechas e IPs, susceptibles de ser reclamados por las autoridades. Y, en muchas ocasiones, sus propias licencias incluyen la posibilidad de compartir nuestros datos con terceros.

Lo mejor es escoger un servicio que no registre nuestros datos porque ha implementado la tecnología para no recibirlos. El problema es que, aunque prometan que ese es el caso, no podemos saber si es verdad. Es nuestra responsabilidad tomar las precauciones adecuadas para que el contacto sea lo más inofensivo posible. Esto incluye crear una cuenta de correo anónima, enviar los datos y borrar todas las huellas antes de poner pies en polvorosa.

No todos son técnicos, algunos son de sentido común. Para que un correo sea lo más anónimo posible, no podemos mandarlo desde nuestra casa, el trabajo o un café donde seamos habituales, ni a través de un ordenador que hayamos usado o vayamos a usar para otros propósitos. Esto descarta apps como Gliph, que, aunque graciosa para chatear con los amigos, es más bien cosmética. La distancia que recorramos para mandarlo debería ser proporcional al peligro que corremos. Y, evidentemente, no deberíamos buscar la dirección del lugar a donde vamos desde casa o el móvil, como si fuese un restaurante.

Mandar correos en lugares públicos: concentración, precisión y discreción

Una vez allí, y pasando lo más desapercibido posible, ya puedes crear tu correo temporal en un servicio de correo de usar y tirar. Las de Mintemail.com y Filzmail.com desaparecen en tres y veinticuatro horas respectivamente, pero hay muchas otras: Airmail, Guerrillamail, etc.

Asegúrate de que el equipo no tiene una cámara web apuntándote. Algunos cibercafés habilitan las webcams de las estaciones para que vigilen sin ser vistas, como medida de precaución. Evita esos o transforma tu imagen lo mejor que sepas sin hacer el ridículo. No te pongas la capucha de *hacker* con unas gafas de sol porque todo el mundo se acordará de ti, aunque sea por payaso. Pero es increíble lo mucho que podemos cambiar de aspecto sin esfuerzo, peinándonos con el pelo hacia atrás o con unas gafas no graduadas.

También es importante que, mientras estés allí, no hagas nada que no sea lo que has ido a hacer. No te pongas a mirar el correo, no navegues por la red, no escuches música en Spotify, no abras el Facebook. No aproveches que hay dos por uno para echar una partidita. Antes de marcharte, asegúrate de que limpias bien el caché del navegador, y que eliminas cookies y el historial. La manera más limpia de hacerlo es usar tu propio sistema operativo desde un pincho USB, pero mira siempre que no queda nada almacenado en el disco duro y, por el amor de dios, no te dejes el pincho USB clavado en la torre. Pasa más de lo que te

imaginas.

Atención, gargantas profundas: este modelo solo es efectivo cuando la información que enviamos no depende del prestigio de la fuente. Las comunicaciones serán siempre unidireccionales, así que deben ser documentos que hablan por sí solos, todas las historias deben ir acompañadas de todos los datos necesarios para corroborar su veracidad e intenciones.

Si lo que queremos es una cuenta de correo temporal, como quien queda para hablar por teléfono desde una cabina pública, entonces los MintEmail o Mailinator son el equivalente digital a «esta carta se autodestruirá en 4 horas». Las medidas higiénicas son las mismas que con los correos de usar y tirar.

Gmail, Yahoo y otros servicios de correo cómodos, convenientes y gratuitos

Técnicamente, hay dos tipos de e-mail: el que escribimos, recibimos y almacenamos a través del navegador —como Gmail, Hotmail o Yahoo Mail— y el que procesamos usando un cliente de correo, como Outlook Express, Thunderbird Mail o Mail.App.

El tipo webmail (Gmail, etc) es cómodo y conveniente porque permite leer el correo desde cualquier parte del mundo y desde cualquier ordenador. Además, permite centralizar todas las cuentas de correo en una sola, pudiendo gestionar nuestras comunicaciones personales, laborales y extracurriculares en una sola pestaña.

¿Cómodo, fácil, conveniente y gratis? Si algo parece demasiado bueno para ser cierto, es porque lo es. ¿Qué pensaríamos de un desconocido que nos ofrece recibir todo nuestro correo en su casa sin cobrarnos nada, por la simple satisfacción de hacernos la vida más fácil? ¿Sospecharíamos de sus intenciones o le entregaríamos alegremente nuestros datos fiscales y una autorización para tirar sin preguntarnos todo lo que parezca propaganda? A todos los servicios online, y especialmente a todo lo que tiene que ver con la red social, se aplica sin excepción el famoso proverbio: Si no lo pagas, no eres el cliente, eres el producto.

Los servicios como Yahoo o Gmail están basados en la Nube, lo que significa que nuestro buzón está guardado junto con otros millones de buzones en un edificio seguro, secreto y remoto llamado Data Center. El Data Center es como un banco en el que tenemos servicio de banca online; tenemos acceso a nuestros documentos mediante una conexión virtual, a través de un nombre de usuario y una clave y podemos realizar ciertas gestiones.

Es más seguro que tener el dinero en casa (es más fácil *hackear* el ordenador del vecino que franquear los muros de un Data Center, aunque ocurre de vez en cuando) y podemos ver el correo desde cualquier parte, como quien saca dinero de los cajeros en un viaje. Pero, como en un banco, solo vemos una parte infinitesimal de lo que hace nuestro dinero cuando no lo tenemos en el bolsillo y cualquier empleado tiene más derechos sobre nuestro buzón que nosotros mismos. Y la fortaleza está tan bien guardada que, si quisiéramos hacerle una visita de cortesía y recoger el correo en mano, acabaríamos en la cárcel antes de tocar el timbre.

Es poco habitual que los empleados se aprovechen, pero ocurre. Fue lo que hizo David Barksdale, un ingeniero de 27 años, que aprovechó su trabajo en Google para acosar a cuatro menores durante meses, leyendo sus correos, escuchando sus conversaciones y manipulando sus datos. Estas son las cosas que pasan cuando pones tu correspondencia

privada en manos de extraños. Pero todo esto, aunque preocupante, es anecdótico en comparación con el problema principal: que el banco no es una ONG y sus servicios no son altruistas. Su verdadero negocio eres tú.

Solo para empezar, Google procesa e indexa todos los correos que pasan por sus manos para vendernos publicidad personalizada. Indexar significa que nuestro nombre o nuestros temas de conversación pueden aparecer en los resultados de búsquedas, no solo en Google sino en otros lugares y contextos como, por ejemplo, un aeropuerto. Los acuerdos de usuario que nunca leemos (llamados EULA: *End User Licence Agreement*) y que siempre firmamos como precondición para acceder al servicio deseado, no solo garantizan a la empresa de servicios el acceso indiscriminado a nuestros correos y conversaciones, también se reservan el derecho a compartirlo con terceros y venderlo al mejor postor. Esto incluye otras empresas que estudian tu comportamiento para formular patrones de todo tipo, principalmente de consumo pero también de tipo político y socioeconómico. ¿Sabemos qué amigos tienen Google o AOL?

Además, son la primera puerta a la que llaman las autoridades, incluyendo los servicios secretos de países a los que no pertenecemos, cuyas leyes no nos protegen y cuyos gobernantes no tenemos derecho a elegir por los cauces democráticos. Y, como la mayor parte de los servicios que utilizamos tienen su sede en Estados Unidos, la ley los protege a ellos pero no a nosotros. La Patriot Act, parte de la legislación antiterrorismo nacida del 11-S, establece que el gobierno estadounidense y sus aliados pueden exigir acceso ilimitado a cualquiera que no sea ciudadano estadounidense sin que su proveedor pueda decirle nada. El 98 por ciento del planeta no es ciudadano norteamericano.

La ley establece también que las empresas están obligadas a facilitar esos datos y que no pueden, bajo ningún concepto, advertir al usuario de que está siendo o ha sido objeto de una investigación.

Es como si la policía de un país extranjero pudiera entrar en tu casa con una llave maestra y hacer copia de todas tus cartas, pinchar tus teléfonos y hacer fotos del contenido de los armarios y cajones. En España, la ley de protección de datos protege nuestro buzón de miradas inquisitivas, pero no puede proteger el buzón que guarda Google en un complejo industrial de Utah.

El falso anonimato de la multitud

Algunos activistas piensan que Gmail tiene la ventaja de esconderles en la multitud. Es muy fácil hacerse usuario y, cuando lo hacemos, no estamos obligados a dar nuestro nombre verdadero, ni a dejar más señas personales que otro correo. Pero la multitud no existe en la era de los superordenadores. Hubo un tiempo en que era imposible almacenar los millones de datos que producimos a diario, pero los tiempos han cambiado.

Ahora la NSA está construyendo un Data Center con capacidad, según estimaciones, de entre 3 y 12 exabytes. Para ponerlo en contexto, está diseñado para guardar todo el tráfico de la Red, que en un año se estima entre 5 y 9 exabytes. Esta capacidad de monitorizar y almacenar todas las comunicaciones funciona en combinación con su software de procesamiento de datos, que incluye programas que reconocen el «estilo» de un usuario cuando escribe o la cara de una persona específica en un vídeo de seguridad. La realidad de esos programas, que vamos conociendo gracias a las filtraciones de Edward Snowden, supera con creces las pesadillas distópicas de George Orwell y

Aldous Huxley.

Además, Gmail no es huérfana. Todos sus servicios están fuertemente integrados junto con el resto de servicios en el gran entramado de su empresa y, hoy por hoy, es casi imposible conectarse a la Red sin pisar al menos una de las baldosas amarillas de Google. Cada vez que usamos uno de esos servicios, su base de datos recoge nuestra localización, sistema operativo y actividades.

Total, que podemos tener cien cuentas de correo distintas con cien nombres diferentes pero, salvo que usemos un ordenador diferente para cada una, nos conectemos desde redes distintas y usemos Tor, lo natural es que todas y cada una de ellas apunten directamente a nuestra casa.

Finalmente, si usamos Gmail (o cualquier servicio de correo gratuito) en combinación con un cliente de correo, como Thunderbird, Outlook o Mail. App, podemos escoger la opción de «descargar» el correo sin que quede nada en el servidor. Aparentemente, nuestro historial de correo queda borrado de los servidores de la empresa, dejando como única copia la que está en nuestro disco duro. Y digo aparentemente porque la realidad no podría ser más distinta. Google guarda (es más, tiene la obligación legal de guardarlo) al menos una copia de todos y cada uno de los correos que envían, reciben, rebotan y borran cada uno de sus usuarios en un momento dado. Esta regla vale para muchas otras cosas: cuando borras algo en un servicio online, lo único que haces es ponerlo fuera de tu alcance. En la Nube, nada se pierde ni desaparece, solo cambia de carpeta.

La solución a (casi) todos esos problemas es cifrar el correo antes de que salga de nuestro ordenador. Si no nos queda más remedio que usar webmail para comunicarnos, existe una extensión llamada Lock the Text (http://lockthetext.sourceforge.net), pero es técnicamente complicado y no del todo efectivo. Lo más limpio, eficaz y sostenible es instalar un cliente de correo apropiado (en este libro recomendamos Thunderbird, de la Fundación Mozilla) y configurarlo para que utilice SSL/TLS junto con un protocolo de criptografía de clave pública.

De este modo la amenaza local —cualquier persona que tenga acceso a tu ordenador, desde una novia celosa hasta la policía que lo requisa— queda neutralizada. Y la amenaza global —la NSA, tu jefe o Google— todavía tendrán tus datos almacenados en un Data Center bajo una jurisdicción que no contempla tus derechos pero, si quieren hacer algo de provecho con ellos, al menos tendrán que llamar para pedir la llave.

La PGP

Cómo mandar correos armados hasta los dientes

*C*orre el rumor de que encriptar correos es difícil y hay algo de verdad: es más difícil hacerlo que no hacerlo. Y sin embargo, cuando necesitamos proteger nuestras comunicaciones para no perder el trabajo, la libertad o la vida, esa dificultad parece muy pequeña. Lo cierto es que, hoy en día, las aplicaciones que permiten encriptar correos son gratuitas y fáciles de instalar. La manera más popular de proteger nuestra correspondencia es usar criptografía de clave pública.

Este tipo de criptografía se llama de clave pública para diferenciarse de la de clave privada o simultánea, donde los usuarios comparten una clave secreta con las limitaciones que eso supone. En la de clave pública cada usuario tiene dos claves, una privada y una pública. Las dos son personales e intransferibles pero la pública sirve para encriptar mensajes y la privada, para descifrarlos. Para poder escribir correos cifrados, la persona que envía utiliza la clave pública de su interlocutor, mientras que este utiliza su propia clave privada para descifrarlos. Esta última es secreta, está protegida por una contraseña y garantiza que nadie más que la persona a la que están dirigidos pueda leer los correos, aunque los capture en tránsito.

Por ejemplo, cuando le mando un correo cifrado a mi amigo Patricio, lo encripto usando su clave pública y no la mía. Una vez se entiende cómo funciona este proceso, veremos que mucha gente tiene su clave pública en su web, o en sus páginas de Facebook y Twitter, para que podamos mandarles mensajes cifrados sin tener que preguntar primero. Una vez en su disco duro, Patricio usa su clave privada para descifrarlo. De esta manera, cualquiera puede mandarle un mensaje cifrado a Patricio usando su clave pública, pero nadie (ni siquiera yo misma) puede desencriptar un mensaje que va dirigido a él.

Cuando ciframos un mensaje, su contenido es ilegible desde que sale de mi cliente de correo hasta que llega al de su destino. Lo único legible de nuestro correo serán las cabeceras de Subject y las direcciones que aparezcan en el From y To. Si quieres que tus comunicaciones sean anónimas, además de seguras, puedes usar un correo de usar y tirar o un Remailer. Aquí enseñamos un protocolo llamado PGP (Pretty Good Privacy) con Thunderbird, el cliente de correo de la fundación Mozilla. Los hemos elegido porque son populares, relativamente sencillos de instalar y están disponible para Windows, OS X y Linux.

Los punks de verdad usan PGP

Como ya hemos dicho, la criptografía de clave pública utiliza dos claves, una pública y otra privada. Estas dos se llaman *Keypair* y son dos párrafos de código que se pueden guardar en el disco duro, pero es más seguro y más práctico guardarlos en un pincho USB que llevaremos siempre con nosotros. Mucha gente lo lleva en el llavero —válganos la redundancia— para no perderlo ni olvidarlo. No está de más hacer una copia de seguridad, por si la primera se pierde o se corrompe (más adelante hablaremos de lo que pasa cuando perdemos nuestra clave).

Como ya hemos visto, para enviar un correo cifrado a una o varias personas

necesitamos tener la clave pública de cada una de ellas y cada una de ellas necesita tener nuestra clave pública para responder. En otras palabras: ¡que fluya esa clave pública! ¡Promiscuidad! ¡Alegría! Cuando ponemos nuestra clave pública en un lugar prominente de nuestro blog o nuestras cuentas de Twitter estamos haciendo algo más que distribuir nuestra clave. Poner nuestra clave pública en un sitio bien visible —¿tazas, camisetas, diademas?— es una manera de animar a otros a que protejan sus relaciones digitales, estableciendo nuevos parámetros de conducta que nos protegen de los ataques, de las empresas y de los gobiernos que nos vigilan. Es una llamada de atención en un espacio donde todo el mundo se indigna de que la NSA nos lea el correo pero sigue escribiéndose con cualquiera sin usar protección. Usar criptografía no es solo para *hackers* y espías internacionales. Compartir nuestra clave con el mayor número de gente posible es ser parte de la solución. Y es lo más punk que se puede hacer online sin acabar en la cárcel (al menos de momento).

Como periodista, tener una clave pública indica que te tomas en serio a tus fuentes. En la introducción de este libro ya contamos cómo Glen Greenwald estuvo a punto de perder la exclusiva más importante de su vida por no saber usar la PGP, o cómo un documentalista puso en peligro la vida de sus informadores en Siria por no proteger sus comunicaciones y su material. Los expertos en seguridad ponen su clave pública en su perfil de Twitter, en la firma de su correo y en todos los lugares donde aparece su contacto. Los periodistas deberían hacerlo con más razón. Uno no sabe cuántas exclusivas pierde cada día solo por no haber establecido canales lo suficientemente seguros.

Una vez tenemos las claves públicas de nuestros interlocutores y ellos tienen la nuestra, el resto es tan simple como usar una dirección de correo. Una vez obtiene las claves, el sistema las añade a nuestro *keyring*, una especie de agenda telefónica de claves públicas que usa cada vez que mandamos un correo a esas personas.

Instalar PGP en Windows, OS X y Linux (y bola extra: Android)

Hay muchas maneras de hacerlo pero en este libro te enseñamos a utilizar PGP —un protocolo de software libre para encriptar mensajes de correo— con Thunderbird, un cliente de correo de la fundación Mozilla, también basado en el software libre.

Usamos aplicaciones de software libre por una razón muy concreta: es imposible saber si un programa es lo que dice ser sin mirarle las tripas. Hay muchas aplicaciones en el mercado que ofrecen proteger la identidad del usuario pero, si no tenemos acceso a su código, no sabemos si la protección es real hasta que es demasiado tarde. Cuando nuestra seguridad o la de otros depende de un trozo de código, no tiene sentido correr riesgos.

En cualquier caso, independientemente de nuestro sistema operativo, para instalar PGP en Thunderbird necesitamos tres cosas antes: Thunderbird, una implementación de la PGP llamada Gnu Privacy Guard (GPG) y una extensión de Thunderbird llamada Enigmail.

Thunderbird, el cliente de correo integral

Instalar Thunderbird es fácil. La mayor parte de las distribuciones de Linux lo traen por defecto, igual que Firefox. Los usuarios de otros sistemas operativos pueden encontrar su versión, en el idioma que más les convenga, en el subdirectorio de Mozilla: http://www.mozilla.org/es-ES/thunderbird

La configuración no difiere mucho de la de cualquier otro cliente de correo: hay que

introducir nombre de usuario y contraseña de todas las cuentas de correo que queramos administrar y las señas del servidor que maneja nuestras cuentas. Si se trata de un servicio web popular como Yahoo o Gmail, es probable que el programa adivine todo lo demás. Si no es el caso, el sistema nos pedirá las coordenadas del servidor.

Normalmente están publicadas en el FAQ de la página del servicio o podemos pedírselas al administrador, pero conviene entender qué significan esos parámetros.

El Incoming Mail Server (POP3, IMAP, HTTP) es el servidor asociado a nuestra cuenta, una especie de oficina postal donde nuestros correos llegan y esperan a que los leamos, bien entrando directamente desde el navegador, o mandando a nuestro cliente de correo para que se encargue de recogerlos y almacenarlos siguiendo los parámetros que hayamos configurado. Una vez en nuestro disco duro, podemos leer, responder, borrar y rebotar cualquier correo sin necesidad de estar conectados a la Red. Para eso, el cliente de correo debe saber la dirección y el protocolo. Los más populares son tres: IMAP, POP3, HTTP. El de Gmail, por ejemplo, es: pop.googlemail.com pero, para usar con Thunderbird, es mejor cambiarlo a IMAP. Esto se puede hacer en la página de administración de nuestro webmail, bajo la pestaña «Forwarding POP/IMAP».

El Outgoing Mail Server (SMTP) es el servidor que envía los correos y su protocolo habitual es SMTP (Simple Mail Transfer Protocol). Aunque nos podemos suscribir a uno dedicado (como smtp.com), lo normal es que lo haga la misma empresa que da el servicio de correo o nuestro proveedor de Internet.

Ojo; cuando enviamos un correo a alguien, los datos no van directamente a nuestro interlocutor sino que pasan por muchas manos antes de llegar al servidor de la empresa que nos gestiona el correo. Debemos configurarlo para que use SSL/TSL, que nos garantiza que el correo irá cifrado hasta el servidor general, pero no que llegará cifrado a su destino. No hace falta que cambiemos el tipo de contraseña en la configuración, porque vamos a usar PGP. Tampoco hace falta cambiar el puerto.

Si una vez configurado Thunderbird el uso de SSL/TSL nos genera un error, lo más probable es que el servidor que aloja nuestro correo no esté configurado para usar ese tipo de protocolo de transferencia segura. En estos casos podemos cambiar la configuración a STARTTLS. Si esto también falla, quedan dos opciones: llamar al administrador para pedirle que implementen un protocolo de seguridad o cambiar de servicio a uno más seguro.

Thunderbird trae su propio sistema anti-spam, pero lo único que hace es moverlo a la carpeta de spam y despejar la bandeja de entrada. Para habilitar el antivirus, hay que ir al menú de Preferencias y entrar en la pestaña de Seguridad para habilitar el software. Los más avanzados podrán encontrar una lista de posibilidades en el repositorio: http://kb.mozillazine.org/Antivirus_software

Y ya que estamos en este menú, tampoco está de más restringir las cookies. Todas estas preferencias se pueden configurar en los menús de herramientas del sistema. En Windows y Macs están bajo Herramientas > Opciones; en Linux bajo Preferencias > Preferencias.

Instalar la PGP en Windows (el menos seguro de los sistemas operativos)

Entra en la página del proyecto Gpgwin (http://gpgwin.org) y encuentra la página de

descargas. Una vez allí, descarga la versión estable más reciente (con todos los respetos, si eres usuario de Windows deberías olvidarte de las betas). Abre el archivo, que será un ejecutable con el nombre de la versión acabado en xe. Cuando el sistema te pregunte si estás seguro de querer instalar el programa, dile que sí.

El proceso de instalación consiste en aceptar la licencia, elegir el idioma y, salvo que sepas exactamente lo que te está preguntando, aceptar todas las opciones por defecto hasta que te pregunte dónde quieres poner el programa. Tanto si aceptas la opción por defecto como si eliges otra, asegúrate de apuntarlo. Te hará falta más tarde.

Para instalar Enigmail hay que entrar en Thunderbird porque es la extensión que te permite generar y manejar claves, cifrar y descifrar correos dentro de la aplicación. Las extensiones de Thunderbird (ahora se llaman Add-ons) se encuentran en el menú principal, que se abre pinchando en el icono de tres rayitas que está en la parte superior derecha, junto al buscador.

Thundermail es prima de Firefox, el navegador, y su manera de añadir extensiones es idéntica: ponemos el nombre de la extensión que buscamos (Enigmail) y pinchamos en Añadir para instalarlo. Cuando el sistema te pregunte si estás seguro de que quieres instalar el programa, le dices que sí. Cuando esté completamente instalado, reinicia la aplicación.

Instalar la PGP en OS X (que tampoco es gran cosa)

Antes de empezar, el lector debe saber que es posible usar PGP con el cliente de correo de OS X, pero usando un parche que no es de software libre, con lo que me remito a la explicación anterior.

Los usuarios de OS X pueden ir directamente a github o descargar el instalador de la GPG desde gpgtools.org. Al pinchar en el Downloader, el sistema preguntará si queremos guardar el archivo (queremos), que debería llevar el nombre de la aplicación y acabar en .dmg. Una vez guardado buscamos la aplicación (si no está en el escritorio, probablemente estará en la carpeta de descargas) y la abrimos haciendo doble clic.

Dentro hay un archivo llamado GPGTools.pkg. Al ejecutarlo, el programa comprobará que el sistema tiene lo que hace falta para que funcione la aplicación (si es un Mac muy antiguo es posible que no cumpla los requerimientos mínimos). Una vez en marcha, el instalador nos lleva por la licencia y otras opciones. Podemos aceptar las que vienen por defecto hasta llegar al Tipo de Instalación o Installation Type, donde queremos customizar.

La ventana que se abre ofrece una lista de programas. Si ya tienes instalado Thunderbird, el sistema debería permitir que seleccionemos Enigmail (si no lo hace, podemos instalarlo luego desde el menú de extensiones de Thunderbird, como hicimos unos párrafos más arriba con Windows). Entre las preseleccionadas está el parche que mencionamos arriba, GPGMail. Puesto que no vamos a usarlo, es mejor sacarlo de la instalación. Cuando pinchamos Instalar, el sistema nos pedirá la contraseña de administración y ¡voilà! Ya tenemos el horno preparado para encriptar correos.

Instalar la PGP en Linux (la solución natural)

Por norma general, los usuarios de Linux no necesitan instalar la GPG ni, ya que nos ponemos exquisitos, explicaciones sobre cómo instalar un software en su ordenador.

Los usuarios de Ubuntu pueden instalar PGP desde el Centro de administración de software (Ubuntu Software Center), y tanto Ubuntu como Mint Debian traen Thunderbird como cliente de correo por defecto. En principio solo necesitamos instalar Enigmail como si fuera una extensión, desde el menú de la aplicación, como hacemos con los Add-ons de Firefox.

Enigmail es, en efecto, una extensión que permite mandar mensajes con una firma digital que garantiza la autenticidad y legitimidad del mensaje y su procedencia.

Bola extra: ¡Android!

Es verdad, cada vez más gente lee su correo desde el móvil. Si ese móvil tiene Android —que contrariamente a lo que se suele pensar es un sistema operativo y no una marca, como iPhone o Nokia— el proceso es complicado pero se puede hacer. Lo primero es ir a Google Play Store e instalar APG (Android Privacy Guard) y K-9 Mail. APG es un manager para gestionar las claves públicas y privadas; K-9 es una versión del cliente de correo de Android, pero con algunos añadidos necesarios. Una vez instalados, necesitaremos generar una nueva clave privada, usando el protocolo DSA-Elgamal. Lamentablemente, Android no tiene capacidad para generar claves realmente grandes (en criptografía, el tamaño sí importa), así que tenemos que generar una en nuestro ordenador y copiarla en un archivo de texto para importarla en el teléfono.

Atención: esta es nuestra clave privada y, cuando la copiamos en modo texto, queda completamente desprotegida. La manera de asegurar su virginidad es importarla manualmente, con el móvil desconectado de la Red. Una vez copiada, la importamos rápidamente a APG y la borramos de inmediato.

Una vez tenemos la clave, hay que configurar K-9. En general, todo es igual que en cualquier cliente de correo pero, en la opción de Cryptography, debemos asegurarnos de que utiliza APG. Y todo funcionará mejor si cambiamos la opción de generar HTML por una de texto plano. Esta regla también se aplica a cualquier tipo de correo, encriptado o no.

Importar las claves públicas de nuestros contactos es más fácil y cómodo usando una tarjeta de memoria SD. La buena noticia es que, una vez importadas tus dos claves, todas las aplicaciones que tengan integrado PGP podrán usarlas sin problemas.

Cómo generar tus dos claves PGP

En este manual hemos elegido usar Thunderbird y su extensión Enigmail. Podemos configurar Enigmail en cualquier momento abriendo el menú principal y seleccionando OpenPGP – Setup Wizard.

Es importante que prestemos atención y escojamos las opciones que más nos convengan. Enigmail permite poner una firma digital en todos los correos, que sirve para que nuestros interlocutores sepan a ciencia cierta que el mensaje es nuestro y no de un impostor cualquiera usando su clave y nuestra dirección de correo (sí, eso puede pasar). También querrá saber si queremos que todos los correos salgan encriptados. Salvo que se trate de un cliente de correo que usamos única y exclusivamente para enviar material delicado, lo mejor es que no.

Por último, nos preguntará si puede cambiar las opciones de formato de nuestros correos para que el cifrado funcione mejor, como cambiar de HTML a texto plano. Esta es una buena cosa tanto si usamos criptografía como si no, porque en cuanto a seguridad los

correos en HTML son un nido de cucarachas, por no hablar de lo mucho que pesan. Finalmente, y esto es de vital importancia, nos pedirá una contraseña.

Esta contraseña protegerá nuestra clave privada y es importante que la recordemos porque sin ella nos será imposible leer los correos que lleguen cifrados con nuestra clave pública. Pero también es importante que sea una buena contraseña. Esto es: muy larga, compuesta de cifras, letras y símbolos, difícil de adivinar. Si no se te ocurre nada, hay un capítulo dedicado a la creación de contraseñas seguras. Léelo antes de continuar.

Una vez introducida la contraseña, el asistente de configuración nos enseñará la lista de opciones que hemos escogido. Si es todo correcto, el siguiente paso es la creación de las claves.

El tamaño sí importa, pero dentro de un orden

Nuestra clave criptográfica puede llegar a ser bastante grande y, en teoría, cuanto más grande, más segura. PGP ofrece varias opciones de tamaño, de los 384 a los 4096 bits. Pero generar una clave requiere un gran esfuerzo por parte del ordenador y, cuanto más grande sea, más tardará en producirla. Una clave de 1024 tarda ocho veces más en hacerse que una de 384 bits. La buena noticia es que, si guardamos bien nuestras claves, solo tenemos que hacer este proceso cada cinco años. La menos buena es que da más o menos igual.

Según cálculos de Arjen Lenstra y Eric R. Verheul, padres de un algoritmo de cifrado para PGP llamado XTR, una llave de 2048 bits aguantaría el tipo contra los más poderosos (digamos, la NSA) durante al menos seis años. Contra el resto del mundo (los que no son la NSA ni su prima inglesa GCHQ) podemos estar tranquilos con una de 1024 bits.

Subir a 4096 es como conducir un Ferrari para cruzar la calle, se puede hacer pero es una tontería. Por otra parte tampoco conviene bajar mucho; las llaves de 384 y 512 bits han sido ya destripadas con ordenadores normales de última generación y se espera que las de 768 podrán serlo dentro de poco. Los expertos recomiendan 2048 y las opciones por defecto del programa, también.

Certificado de anulación: el seguro contra imprevistos

Tener una clave privada es un poco como llevar una pistola de descargas en el bolsillo: te puede salvar de muchos peligros, salvo que llueva o que te la quiten. Si nos quedamos sin llave, es como salir de casa y dejar la puerta cerrada por dentro, sin ningún documento que pruebe que la casa es nuestra. Será imposible demostrar a tu círculo de contactos que tu nueva clave es legítima o que la vieja ya no lo es. Peor aún, si alguien se hace con las claves y empieza a enviar correos usando nuestra firma digital, será virtualmente imposible demostrar que no hemos sido nosotros, especialmente delante de un juez. Para eso está el certificado de anulación.

Ocurre más a menudo de lo que te imaginas: te roban el ordenador, pierdes el pincho, se corrompe la memoria. Más típicamente *nerd*: insistes en aprenderte la clave de memoria y en una visita a México se te olvida para siempre. Hay quien se hace un tatuaje en un lugar donde no le da el sol, pero no es aconsejable. No solo estará expuesta cada vez que nos quitemos la ropa (por poco frecuente que sea), además la llave está diseñada para

caducar a los cinco años.

El certificado es la única manera de anular la clave y hacerte una nueva *antes* de que hayan pasado cinco años. Acuérdate de guardarlo en un lugar seguro (fuera de tu ordenador, lejos de la humedad, el fuego y tu futura expareja) y ponerle un nombre que tú sepas reconocer dentro de dos o tres años, pero que no grite su contenido a los demás.

Si todo ha salido bien, el asistente habrá generado tus dos claves y el certificado de anulación. ¡Enhorabuena! Ya puedes empezar a enviar mensajes cifrados y descifrar los que te manden a ti.

Cómo usar la PGP

Domina el arte de encriptar correos, descifrarlos y administrar tu *keyring*

*U*na vez instalados los programas y generadas las claves, tendremos un archivo con el certificado de anulación en el disco duro que acaba en rev.asc. Tus claves están escondidas en el sistema como un archivo normal, pero puedes hacer una copia de seguridad en el menú de herramientas de OpenPGP. Para acceder a ese menú abre un correo nuevo, pinchando en OpenPGP y escogiendo OpenPGP Management. Al lado de la caja de búsqueda hay una opción para ver todas las claves. Cuando actives esa opción, aparecerá tu correo.

Pinchando en ese correo con el botón derecho aparece un nuevo menú de opciones que incluye «Export Keys to File». Esta opción nos permite guardar las claves en cualquier sitio, desde el escritorio (no recomendable) hasta una memoria USB que llevaremos siempre con nosotros para descifrar nuestro correo dondequiera que vayamos (más recomendable). También es importante guardar una copia del certificado de anulación. Evidentemente, es más seguro guardar ambas cosas en sitios separados. Si se corrompe el sistema y lo perdemos todo, la copia de las claves nos permite seguir descifrando correos. Si nos requisan el ordenador o lo roban, el certificado nos permite avisar a nuestros contactos de que nuestra clave ya no es segura y generar otra nueva.

Una vez instalados los programas, Thunderbird tendrá una nueva opción en el menú cuando abramos un nuevo correo, llamada OpenPGP, con las opciones de firmar y cifrar el correo. Lamentablemente, para mandar e-mails cifrados a otras personas, ¡necesitamos sus claves públicas! Si queremos mandar un correo cifrado a las cinco personas de nuestro equipo, necesitamos tener las claves públicas de las cinco. Mientras practicamos, podemos mandarle correos a Adele, «the Friendly OpenPGP Email Robot». Escribiendo a su dirección de correo [adeleen@gnupp.de] podrás comprobar si todas las funciones de tu sistema de cifrado funcionan correctamente.

Antes que nada tendrás que enviarle tu clave. Para hacerlo, basta con escribir un correo (sin cifrar) y, antes de mandarlo, pinchar en el icono de OpenPGP Adjuntar mi clave pública. Adele te contestará enviando su propia clave. Para guardarnos una clave que nos ha mandado alguien, debemos abrir el adjunto que acaba en .asc (el otro, que acaba en .asc.sig es la firma digital de nuestro interlocutor). Su firma será un desatino de símbolos y números y el sistema nos dirá que no le conoce, lo que es correcto porque todavía no tenemos el contacto en nuestro *keyring*. Una vez importemos el contacto, sus correos vendrán encabezados por una banda de color verde. Fíjate bien en lo que pone en esa banda, sobre todo si cambia de verde a amarillo o rojo. Los contactos se pueden administrar en el menú OpenPGP Key Management.

Para mandar correos cifrados a un desconocido nos hace falta su clave pública, pero él no necesita tener la nuestra. Nuestra clave pública es la que usan los demás para cifrar mensajes que solo nosotros podemos descifrar con nuestra clave privada. Por eso es importante que los periodistas tengan su clave pública bien a la vista. Cuando una fuente se quiere comunicar con nosotros de manera segura, es mucho pedir que llamen para preguntar por ella. Una opción es subir nuestra clave a un servidor de claves o *keyserver*, una especie de listín telefónico de claves públicas. En el menú podrás comprobar si alguno de tus contactos de correo tiene clave pública, y añadirla a tu *keyring* con un OK. También

tendrás que validar sus firmas.

Para añadir tu propia clave al *keyserver* basta con ir al menú de Key Management y habilitar «Display All keys». Selecciona la tuya, pincha con el botón derecho para desplegar un menú de opciones donde aparecerá la opción «Upload Public Key to keyserver» y selecciona una lista de servidores. Elige el más popular en tu entorno. A partir de aquí, podrás dar tu ID a todo aquel que quiera comunicarse contigo. La ID es tu matrícula en el mundo de la criptografía de clave pública, una secuencia alfanumérica de ocho cifras con el prefijo 0x (por ejemplo: 0x940BB7D4). Es más fácil de recordar que nuestra clave pública.

Hay varias otras cosas a tener en cuenta. La primera es que tenemos que especificar el uso de cifrado para mandar un correo cifrado, igual que especificamos el receptor cada vez que escribimos un e-mail. Más importante aún, nuestra configuración no nos protege cuando leemos y contestamos correo desde el navegador, usando el servidor de Gmail o Yahoo.

De la misma manera, cualquier correo cifrado que recibamos y abramos en la página de Gmail o en otro cliente de correo que no sea el que hemos habilitado (por ejemplo, en el trabajo) será completamente ilegible salvo que tengas a mano tus dos claves. El juego de llaves que necesitas para cifrar y descifrar correos se llama *Key-pair*. Podemos generar uno nuevo en el menú OpenPGP Key Management Generate.

Cómo manejar identidades

Además de cifrar los correos, OpenPGP nos da la oportunidad de firmarlos. Esto sirve para que cualquier contacto que tenga nuestra clave pública guardada en su *keyring* sepa que nuestra identidad es legítima. La manera más fácil de legitimar una cuenta es entregarla en persona, por eso mucha gente se pasa las claves en mano, con pinchos USB y hasta —si son muy peliculeros— escrita en un papel. Cuando guardamos los datos de alguien, registramos también su firma y en el menú podemos valorar hasta qué punto confirmamos que la persona que está en nuestro *keyring* es quien dice ser. Las opciones van desde «No lo sé» hasta «Estoy segurísimo» (*I trust ultimately*).

La valoración que hagamos afectará a la fiabilidad de ese usuario, así que no hay que elegir con ligereza. Es bueno firmar siempre los mensajes porque, aunque se puede forzar una clave y falsear una huella digital, es muy difícil hacer las dos cosas a la vez. La criptografía es un juego de estadísticas que funciona por capas. Cuantas más capas de dificultad interponemos entre nuestros datos y el exterior, más seguros están.

Cada vez que mandamos un correo cifrado, necesitamos la clave de nuestro destinatario y nuestra contraseña, que el sistema no debe guardar por motivos de seguridad. No es la contraseña del correo sino la que introdujimos cuando generamos las claves. Si mandamos un adjunto, una ventana nos preguntará si queremos cifrar el mensaje pero ignorar el adjunto, cifrar el mensaje y cada adjunto por separado o cifrarlo todo en un paquete. La mejor opción es la segunda, así que podemos seleccionarla y hacerlo de manera definitiva marcando la cajita final.

Al recibir un correo cifrado, Enigmail se encargará de descifrarlo, no sin antes pedirte la contraseña de nuevo. Si parece un aburrimiento tener que escribir la contraseña una y otra vez, consideremos lo fácil que es ir al baño y dejarse el ordenador abierto y logueado al alcance de cualquiera. Al cabo de un tiempo escribir la contraseña se convierte

en un acto natural, como cepillarse los dientes después de comer o secarse después de la ducha.

Con Thunderbird podemos usar varias cuentas de correo. Por motivos de conveniencia, se puede tener una cuenta que usaremos exclusivamente para mantener correspondencia protegida o desactivar el cifrado por defecto y seleccionar a grupos de personas —fuentes, colegas, activistas— con los que la comunicación debería estar siempre protegida. Las dos son soluciones que nos evitan riesgos innecesarios.

¡Mi clave privada ha sido descubierta!

Nos han robado el ordenador o requisado nuestras pertenencias. Si aún no ha ocurrido pero estamos en una situación en la que podría pasar (por ejemplo, cruzando la frontera siria con entrevistas a disidentes), entonces lo más recomendable es eliminar nuestra *key-pair* de antemano y guardarla en un lugar seguro. Si la policía requisa nuestro ordenador con todos los correos dentro, tendrán los correos pero no los podrán leer sin las claves.

Si en un descuido nos roban el ordenador y sí tenemos las claves dentro, o pensamos que han sido comprometidas por el motivo que sea, es el momento de usar nuestro certificado de anulación. Para hacerlo, enviamos rápidamente un correo a todos nuestros contactos con el certificado adjunto, igual que hicimos con la clave pública, para que no nos manden más información hasta que el agujero haya sido tapado. Los recipientes podrán aceptar la anulación y esperar una nueva clave.

Perder la clave privada no significa solo que nuestros nuevos correos están expuestos; toda la correspondencia que haya sido cifrada hasta entonces estará comprometida, como una casa de la que han robado la llave. Lo más seguro es cambiar el cerrojo y reencriptar toda la correspondencia con la nueva clave. Y asumir que algo se ha filtrado y actuar en consecuencia.

Thunderbird de bolsillo

Es cómodo tener el correo centralizado pero un corresponsal no puede siempre llevar su ordenador a todos lados. Si estamos de viaje y dependemos de ordenadores ajenos —ya sean cibercafés, salas de prensa o préstamos temporales— lo más práctico es llevar en el bolsillo lo imprescindible para nuestras comunicaciones.

Hoy en día los pinchos USB tienen gran capacidad y pequeño tamaño, algunos incluso están ingeniosamente camuflados en sortijas, tarjetas de crédito, pulseras y cinturones. Personalmente, creo que lo mejor es llevar una versión actualizada y personalizada de Tails con todos los programas necesarios para comunicarse de manera segura. Si solo queremos llevar el correo, hay una versión portátil de Thunderbird que se puede usar con la PGP. La otra ventaja de llevar el paquete de correo en el bolsillo es que podemos cifrar todo el pincho USB (ver capítulo sobre discos duros).

Para descargarlo hace falta un disco duro USB, un ordenador y el software, que encontraremos fácilmente si buscamos Portable Thunderbird en la página del repositorio: http://portableapps.com/apps/internet/Thunderbird_portable

Los pasos son sencillos: pincha en el botón del programa y descarga el código en tu ordenador (no en el pincho). Una vez descargado, abre el instalador pinchando dos veces y,

cuando pregunte dónde quiere guardar el programa, indica tu disco duro USB. Espera a que termine de guardar y *¡voilà!* Ya tienes Thunderbird portátil.

El programa está diseñado para trabajar con GPG pero, como ocurre con la versión normal de Thunderbird, tenemos que instalar GPG y Enigmail. Para hacerlo, basta con descargar GPG for Thunderbird Portable de Portable Apps (la última versión a la hora de escribir esto es 1.4.15 Rev 2) y la extensión Enigmail de la página de Mozilla. Cuando reiniciemos el pincho USB estará todo preparado para la configuración del cliente de correo. Es exactamente igual que en la versión normal.

Advertencia: por la boca muere el pez

Es importante reiterar que, en los capítulos anteriores, ofrecemos soluciones técnicas para problemas técnicos, diseñadas para controlar la información que mandamos junto con nuestros correos. Ningún programa ni medida extraordinaria nos ayudará si el contenido mismo de nuestro mensaje nos pone en evidencia.

Hay muchas maneras de destapar nuestra identidad que no tienen que ver con la tecnología. Muchas son de sentido común: todas las referencias a noticias locales o detalles geográficos nos exponen con facilidad, así como los comentarios sobre personas conocidas de nuestro entorno directo, las referencias familiares, las anécdotas personales.

Ningún cifrado puede protegernos si usamos el mismo *nick* o apodo que hemos usado para otras cosas. Tampoco podemos usar un nombre con el que nos sentimos identificados, ni el de nuestro personaje favorito ni el de nuestra amada mascota ni nuestra marca de aftershave. No debemos hacer chistes ni contar una historia que ya hemos contado antes a alguien que sabe quiénes somos, aunque no le veamos desde hace veinte años. Hay que ser neutro y riguroso, y a veces hasta eso no basta. La pista más peligrosa es el estilo, una de esas cosas que son visibles para todo el mundo menos para uno mismo.

Todos tenemos uno, aunque pensemos lo contrario. El estilo es una preferencia por ciertas palabras y no otras, por ciertos tiempos verbales, o la costumbre de encadenar una palabra específica seguida de un tiempo verbal específico. También es una manera especial de puntuar, usando el punto y coma como si fueran dos puntos o evitándolo por completo, o la manía de poner siempre tres elementos en una descripción y nunca dos, ni cuatro.

Cuando un estilo se populariza en una región o entorno, lo llamamos acento, cuando alguno de sus elementos se cuela en la cultura popular, lo llamamos *cliché*. Los estilos colectivos siguen siendo estilos, y a menudo basta leer un texto para adivinar a qué generación pertenece el autor, que los adopta precisamente para diferenciarse de las anteriores. Los llamamos estilos porque son parte del romance de nuestra personalidad, de nuestro genio individual, pero los ingenieros los llaman patrones, que es el idioma favorito de las máquinas.

Dicho de otra manera, el estilo no es más que un uso característico y reiterativo del lenguaje, y hay software específico capaz de peinar la Red en busca de esos patrones y volver con nuestro nombre y apellidos en menos de lo que tardamos en comprar un billete a Moscú.

¿Hemos comentado en periódicos o participado en foros? ¿Hemos escrito blogs o conversado en el #IRC? ¿Tenemos cuentas de Twitter, Facebook, MySpace, Twenty, Yahoo Groups o cualquier rincón de la Red donde lleguen los largos dedos de Google? ¿Has publicado tu tesis en la web de la universidad? Si la respuesta a una o varias de estas

preguntas es afirmativa, nuestro estilo es de dominio público. Como los programas de reconocimiento de caracteres o los reconocimientos de voz, este tipo de software necesita muchas muestras para ser concluyente y todos los textos que hemos repartido por la Red serán testigos en nuestra contra, como fragmentos de una huella digital única e incriminatoria. En la era post 11-S, el misterioso Unabomber hubiese durado exactamente media hora; lo que tardó un simple análisis de texto en relacionar su Manifiesto con los *papers* que publicó en la Universidad de XXXX antes de fugarse a las montañas.

Incluso si hemos sido ermitaños digitales y lo único que hemos hecho ha sido enviar correos, si no estaban cifrados, las posibilidades de que nos pillen corren parejas al tamaño del enemigo. Si es un individuo o una empresa pequeña, hay poco que temer. Pero si nos enfrentamos a gobiernos, grandes corporaciones o personas con amigos en altos cargos, lo normal es que tengan fácil acceso a esos correos. Cuanto mayor sea una empresa, más susceptible es de ser o haber sido uno de esos «terceros» que tanto aparecen en los EULA.

Para estar seguros, lo mejor es usar las armas del enemigo y pasar nuestros textos por un sistema de reconocimiento. ¡Que no sea el que queremos mandar de manera anónima! Si el programa vale algo, señalará todos nuestros lugares comunes y podremos cambiarlos por expresiones ajenas, patrones que no nos pertenecen, despistando a los sabuesos digitales.

Probablemente el texto resultante nos parecerá feo, falto de ritmo o rimbombante y pretencioso. Hay que resistir el impulso de mejorarlo: si nos pillan, que no sea por vanidad.

Navegar

Cómo dar esquinazo a los cotillas, vendedores de seguros y tratantes de contraseñas ajenas con SSL, VPN y Tor

*Y*a lo hemos dicho antes: conectarse a la Red es una actividad muy, muy sociable. Visitar una página, mandar un correo o pinchar «Me gusta» en un blog es empezar una conversación en la que enviamos y recibimos paquetes de datos del servidor de la Red donde está alojada la página, con la intervención de muchos y variados intermediarios. Esto es porque, aunque parezca instantánea, la comunicación no es directa; entre el servidor de esa web y nuestro ordenador hay al menos diez ordenadores involucrados, normalmente muchísimos más. Cada uno de ellos es una parada en las que —como ocurre en los aeropuertos— nos registran y toman las huellas, aunque no nos demos cuenta. En algunos casos hasta nos cambian la maleta y no lo sabemos hasta que es demasiado tarde.

¿A quién pueden encontrarse nuestros paquetes de datos en un simple clic? Aquí va la lista más pequeña posible de sospechosos habituales:

–**Cualquiera que esté usando la misma conexión que tú**. Cuando nos conectamos a una red wifi pública, nuestra tarjeta de red habla con el router y este manda los mensajes a la Red. En otras palabras, nosotros estamos a un lado del router y la Red está del otro. Cuando no estamos solos en ese lado, como ocurre en cibercafés, universidades y salas de prensa, los datos pueden ser capturados fácilmente por un sniffer o alguien familiarizado con el popular ataque Man-in-the-Middle (ver nota sobre redes Wifi).

–**Tu proveedor de banda ancha**. Lo natural es que registre todos tus movimientos, solo porque puede, pero en algunos países hasta tiene la obligación legal de hacerlo. No lo dudes: tu empresa telefónica registra todos tus movimientos y los guarda en una carpeta con tu nombre y dirección. Si quieres saber por cuántos de sus ordenadores pasas cada vez que pinchas en un enlace, vete a www.dnsleaktest.com y pincha en «Extended test».

–**Los puntos neutros** (Internet Exchange Point, Network Access Point o Punto de Acceso a la Red). Son las articulaciones del sistema, el conmutador donde las distintas proveedoras intercambian tráfico y usuarios.

–**Su proveedor de banda ancha**. El servidor que aloja la página deseada también tiene telefónica. Y la suya también lo registra todo.

–**Todos los administradores que trabajan para ellos.** Los servidores no son inteligencias independientes que funcionan por sí mismas, detrás de cada uno hay un equipo de gente trabajando. Todos o cualquiera de ellos podrían estar leyendo tu correo ahora mismo.

Antes enviábamos cartas y paquetes postales y teníamos que fiarnos de que el cartero no las abriera. Ahora las cartas pasan por demasiadas manos, son procesadas demasiadas veces. La pregunta correcta ya no es quién podría abrir nuestras cartas —aunque sabemos que mucha gente las abre y se guarda la información que hay en ellas para usarla y venderla más adelante—. Ahora el otro problema es el análisis de tráfico: gente que registra quién las manda, quién las recibe, con qué frecuencia se mandan, en qué momento del día, cuánto pesan, de qué color son los sobres, etc. Eso es *tracking*.

Esa gente no necesita leer el contenido de tus cartas para saber quiénes son tus mejores amigos, colaboradores, amantes o familiares, de la misma manera que Target no necesita leer tu informe médico para saber que estás embarazada, porque ya tiene tu ticket

de compra. Y la única manera de protegernos de ellos es ir camuflados desde que salimos de casa hasta que volvemos a casa. O sea, usar criptografía de puerta a puerta.

Para hacerlo, hay tres herramientas de criptografía con distintos niveles de protección y perfectamente combinables: SSL/TLS, VPN y Tor. En este capítulo vamos a verlas una a una.

Redes públicas

Tan inocuas y respetables como un fumadero de opio medieval

*L*as redes wifi de los aeropuertos, cafés, universidades y periódicos son más venéreas que un fumadero de opio regentado por periodistas de Tómbola. Esto es porque, cuando un ordenador se conecta a la Red, no lo hace directamente sino a través de un router, que canaliza el flujo de información y nos hace de ventana a Internet. Y cuando nos conectamos desde una wifi pública en una cafetería o estación de trenes, respiramos el mismo aire íntimo y transparente que los demás clientes del establecimiento, un aire donde flotan desprotegidas sus cuentas de Twitter, chats en Facebook y los números de las tarjetas de crédito con las que están comprando sus billetes de avión o pagando habitaciones de hotel.

Tan desnudos están esos datos que cualquiera podría, armado de un software perfectamente vulgar y un poco de mala leche, sentarse a escuchar todo lo que hacen y dicen esos usuarios desprevenidos que chatean alegremente, en la seguridad ilusoria de que sus nombres y contraseñas de usuario les protegen de todo mal. Basta con sentarse entre los usuarios y el router a interceptar mensajes haciéndose pasar alternativamente por los dos.

Por eso se llama ataque Man-in-the-middle (hombre-en-elmedio): el usuario piensa que se está comunicando con el router y el router piensa que comunica con el usuario, pero se les ha colado un intermediario sin que se den cuenta que no solo es capaz de interceptar todos sus paquetes —incluyendo contraseñas y números de tarjeta de crédito— sino que es capaz de cambiar esos paquetes con la misma facilidad del que abre una carta, cambia el contenido y la mete en otro sobre a la misma dirección. Gracias a las últimas tecnologías, el intermediario ni siquiera tiene que estar en la sala, le basta con dejar un Caballo de Troya, un dispositivo de aspecto inocuo que se enchufa discretamente a la pared y le envía todos los paquetes por control remoto.

Una vez plantada esa oreja, el infiltrado puede controlar todo el tráfico de esa red wifi —café, aeropuerto, universidad, estación de trenes, oficina o periódico— desde la comodidad de su casa. Y esta es solo una de las muchas razones por las que resulta absolutamente imprescindible que esos paquetes de datos salgan cifrados de nuestro sistema y permanezcan cifrados hasta llegar a su destino. Un ataque como este será capaz de interceptarlos pero no podrá hacer nada con ellos a no ser que le demos las claves.

1. SSL/TLS

El Secure Socket Layers o SSL es un protocolo de seguridad entre ordenadores, una especie de túnel que se genera entre el ordenador que pincha en el enlace y el servidor de la página enlazada. Los paquetes de datos que circulan entre la entrada y la salida del túnel quedan cifrados de principio a fin. La SSL fue creada por Netscape en 1994 y no solo ofrece un nivel alto de confidencialidad sino que protege la integridad de la información —nadie puede infectar los paquetes o inyectar en ellos información no deseada sin que nos demos cuenta—. También garantiza la identidad de las partes implicadas gracias a un sistema de certificados. Treinta años después de su nacimiento, SSL sigue vigente pero como parte de un combo de seguridad más complejo junto con Transport Layer Security

(TLS).

Aunque no nos suene, todos usamos TLS. Es el estándar de seguridad para todas aquellas transacciones en las que se intercambia información delicada, como números de tarjeta de crédito o direcciones postales. Para saber si estás usando TLS, basta con mirar en la URL del navegador. Los servidores que tienen implementado este protocolo empiezan su dirección con https://, que es el protocolo de transferencia tradicional http pero con una «s» de seguro al final.

Además de las letras, los navegadores modernos cambian el color a verde y muestran un icono con forma de candado para demostrar que estás usando un formato de navegación seguro. Para comprobarlo en directo, abre la página de tu banco o la de Paypal. El candado que sale a la izquierda de la URL es el signo de que tu comunicación con esa página está protegida.

Antes hemos visto qué ocurre cuando navegamos. Cuando usamos SSL/TLS, nuestro navegador debe comprobar que la página solicitada tiene un certificado en regla. Esto es: que procede de una fuente oficial, que no está caducado y que viene de donde dice venir. En otras palabras, nos aseguramos de que la página que visitamos es quien dice ser. Una vez comprobada la identidad, el navegador genera una clave criptográfica aleatoria para cifrar la comunicación.

El cifrado de clave pública es un proceso exigente y requiere muchos recursos del ordenador, por eso este protocolo usa también un cifrado de clave simétrica, donde la clave es generada de manera aleatoria y es compartida por las dos partes. Cada sesión genera su propia clave que, una vez terminada la conversación, se descarta para siempre. Otros nombres para este tipo de cifrado son: de clave secreta, de clave única, de clave compartida y de clave privada. En el cifrado de clave pública, cada usuario tiene una clave privada y una pública, que puede usar para cifrar datos pero no para descifrarlos.

Sobre los certificados

Para navegar usando el protocolo SSL/TLS no hace falta nada más que un navegador actualizado. Para ofrecer SSL/TLS desde el servidor, hace falta adquirir un certificado de una Autoridad de certificación. Las Autoridades tienen la responsabilidad de confirmar que el portador del certificado es quien dice ser, pero no todas tienen la misma reputación. Como ocurre con las burocracias de todo el mundo, algunas Autoridades venden sus certificados solo después de comprobar los nombres del registro de dominio, cosa que cualquier ratero puede falsear.

Los certificados de alta garantía (*high assurance certificates*) incluyen la comprobación del dominio y del registro de negocio, que añade un nivel de dificultad a los chorizos. Los segundos son más recomendables y suelen tener un seguro de garantía, que paga el servidor pero que sirve para compensar al usuario en caso de haber sido estafado. Pero el tipo de certificado no indica en ninguno de los casos el nivel de seguridad de la sesión, solo el grado de «fiabilidad» del servidor de destino.

Si queremos que nuestros usuarios se sientan seguros visitando nuestra web o enviando información delicada, entonces deberíamos implementar el protocolo SSL/TLS en nuestro servidor. Para eso hay que pedir un certificado.

A la hora de elegir una Autoridad, es bueno buscar una que ofrezca certificados compatibles con los principales navegadores. No nos vale de nada tener un esquema de

seguridad si los usuarios se quedan fuera. También es importante que tengan su propio Root Certificate Authority (CA), porque quiénes son ellos para garantizar tu identidad cuando su identidad no está garantizada como dios manda.

También deben tener el sello de garantía de WebTrust, demostrando que cumplen los estándares adecuados para entregar y manejar certificados. Y cuidado con los oportunistas. Si sus ofertas parecen sospechosas o anuncian certificados premium con el argumento de que son más seguros, sabemos que no son de fiar.

Noticias de última hora

En el momento de escribir este libro se ha hecho público un agujero de seguridad en las conexiones SSL/TLS que afecta a los sistemas Apple iOS 6, iOS 7 y Apple TV. El problema era una línea que se coló en el bloque de código responsable de validar la identidad de un servidor y afectará a cualquier sistema que utilice el SecureTransport API de Apple para conexiones SSL/TLS. Eso incluye Safari y un número indeterminado de aplicaciones diseñadas dentro y fuera de la empresa.

Apple ya ha publicado una actualización que corrige el error y, para cuando hayamos publicado estas páginas, el problema se habrá olvidado. Pero ilustra perfectamente uno de los principios básicos y más infravalorados de la seguridad en Red: actualizar el software. Todos los usuarios de Apple que no apliquen las actualizaciones pertinentes o que tengan versiones más antiguas estarán expuestos aunque naveguen a través de SSL/TSL. Para comprobar si la conexión es segura visita gotofail.com con Safari. Hasta entonces, es más seguro utilizar Firefox o Chrome. O, si realmente te tomas la seguridad en serio, mudarse a Linux. No hace falta cambiar de ordenador.

2. VPN: VIRTUAL PRIVATE NETWORK

Una Red Privada Virtual (VPN) es una red de ordenadores que se crea por encima de la que ya existe. Por usar una metáfora habitual, es similar al envío de un paquete en el que el emisor mete el contenido en una caja y lo manda en un camión a un gran almacén de reparto. Los paquetes van por la carretera (Internet) como todos los demás, pero nadie puede ver lo que llevan dentro. Una vez en el almacén, el paquete cambia la dirección del remitente por una genérica y aleatoria (IP) y es recogido por otro repartidor, que se lo entrega al destinatario final para que lo abra con su llave. De esta manera, los paquetes llegan a su destino sin que nadie sepa quién los manda salvo el emisor, el receptor y el servicio de reparto.

Hay muchas razones para usar VPN y, aunque no son incompatibles, tiene dos ventajas inmediatas sobre TOR. La primera es que no es una práctica especialmente relacionada con el crimen o el anonimato. La segunda es que la conexión es mucho más rápida. La desventaja es que nos tenemos que fiar de que la empresa de reparto no lleve un registro de nuestras operaciones que pueda ser reclamado más adelante por las autoridades o robado por *hackers*.

La VPN no solo protege la identidad de los usuarios, también sirve para proteger espacios de trabajo del resto de la Red. Muchas universidades y centros de investigación la utilizan para ofrecer acceso a los estudiantes e investigadores a su biblioteca local sin tener que estar físicamente en el edificio. Administraciones y empresas de todo el mundo la usan

para que sus empleados puedan entrar en la base de datos o colaborar desde puntos remotos sin comprometer el sistema. En todos esos casos, la VPN es como un club de campo que facilita el acceso a personas seleccionadas (estudiantes, empleados), y mantiene al resto de los usuarios de la Red fuera de sus instalaciones. De este modo quedan a salvo, no solo de mirones y polizontes sino también de virus y otras enfermedades de transmisión virtual.

La VPN también funciona como proxy, porque las conexiones siempre proceden del servidor VPN y nunca del usuario. Por eso muchos la aprovechan para visitar páginas prohibidas desde países donde existe algún tipo de censura, como China, Cuba o Irán, o para usar la wifi pública de cafés y aeropuertos sin exponerse. Dicen que es la única manera segura de bajarse torrents sin arriesgarse a una denuncia y más de uno la usa para abonarse a servicios de televisión en otros países (por ejemplo, conectarse a Netflix desde España).

Una VPN tiene muchos usos para un periódico. Para empezar, no es tontería proteger a la redacción de virus, malware y otras bacterias indeseables en un trabajo donde navegar y mandar correos se ha convertido en el 80 por ciento de la actividad. Los corresponsales y colaboradores pueden usar redes ajenas sin preocuparse de la seguridad, encontrarse con otros usuarios sin que nadie lo sepa, mantener conversaciones sin que nadie las oiga, intercambiar archivos en un contexto seguro sin que nadie lo intercepte. También pueden trabajar desde cualquier parte del mundo como si estuvieran en su propia mesa, usando su ordenador de la redacción o colaborar con el resto de su equipo.

Un investigador que trate temas delicados puede fingir que escribe desde otros países o hacer llamadas desde su mesa cuando en verdad está en Hong Kong sin que lo sepa su interlocutor. Un blogger anónimo puede participar en las redes sociales sin que le sigan el rastro hasta casa. En resumen, la VPN funciona como una red local pero ofrece protección internacional, multiplataforma, anónima, segura y cifrada. Y también funciona como una Darknet: lo que pasa dentro se queda dentro. O mejor dicho, si el servicio es legítimo, lo que pasa dentro no ha pasado jamás.

Medidas de emergencia cuando nos conectamos desde una wifi pública

Si compramos por ejemplo un billete de avión a través de un hostpot en un café, en esos paquetes van nuestras contraseñas, correo, datos personales, número de la tarjeta de crédito, todo ordenadito y sin encriptar. Si no nos queda más remedio que usar una, estas son nuestras sugerencias para evitarlo.

1. No lo hagas. Si viajas con frecuencia, invierte en un router de viaje protegido por WPA2. Si te gusta trabajar en cafés, compra un pincho USB de 3G.

2. Usa protección. Asegúrate de que tu antivirus está actualizado y que hay un firewall activado que te advierte de cualquier contacto que tenga lugar entre tu ordenador y el resto del mundo. No son 100% seguros pero al menos dificultan el ataque.

3. Desactiva la tarjeta wireless cuando no necesites la conexión. Hay portátiles, como los Thinkpad, que permiten bloquearla físicamente con un pequeño interruptor. Si el tuyo no lo tiene, debes desactivar la tarjeta desde el menú del sistema operativo, y lo mismo por triplicado para teléfonos y tabletas. Las configuraciones de conexión automática tienen más peligro que el cuarto oscuro del Martin’s un domingo al mediodía.

4. Evita las redes abiertas. Toda red que se llame «Red Abierta», «Internet gratis» o «Pincharme aquí» debe despertar el mismo grado de aprensión que una billetera tirada en la calle con billetes de 500. En un café, aeropuerto o biblioteca, utiliza siempre la Red que

corresponde al local. Si tienes dudas, pregunta al responsable.

5. Ante la duda, WPA2. Si tienes que elegir entre varias redes, elige la que tenga el mejor protocolo de seguridad. De más a menos segura, esto es: WPA2, WPA y WEP.

6. Cuidado con lo que compartes. Podría ser la impresora, los grandes éxitos de Estopa o todas las carpetas de un proyecto que desarrollas con siete personas más. En un ordenador corporativo lo natural sería que las opciones compartidas solo funcionen en la Intranet de la empresa, pero es mejor no arriesgar. Busca las opciones de Red y comprueba que todas tus ventanas están cerradas. Si tienes que compartir directorios en una Red pública, aprende a crear una Red Privada Virtual.

7. Controla los DNS. Hay estafadores que aprovechan la resolución de DNS (en español: sistema de nombres de dominio) para redirigirnos a una página de Phishing cuando intentamos navegar. Los expertos aconsejan utilizar servicios seguros de resolución de DNS (como OpenDNS) o extensiones de seguridad (DNSSEC).

8. Encríptalo todo. El HTTPS es el canal seguro del HTTP, un protocolo que encripta las comunicaciones de manera que, aunque alguien pueda interceptar tus paquetes de datos, al menos no los podrá leer. Lo utilizan por defecto las entidades bancarias, tiendas online y todos los servicios que incluyan flujo de datos personales y contraseñas. Para ver si lo estás usando, fíjate en el campo de la direccón URL. Cuando no haya HTTPS, tira de SSL. Casi todos los sitemas incluyen hoy una implementación de SSL (Secure Sockets Layer o capa de conexión segura) o de su sucesor TLS (Transport Layer Security o seguridad de la capa de transporte), en el control de administración o como extensión para el navegador.

9. Escucha a tu navegador. Las páginas deben tener un certificado digital que confirma la identidad del servidor. Cuando ese certificado caduca o es revocado, el Protocolo de Estado de Certificado Online del navegador nos avisa de que la url podría no ser de fiar. Si no conocemos al responsable de la web, lo más sensato es cerrar la pestaña.

10. Cásate con Tor. El proxy más sencillo y efectivo del mundo está disponible para todos los sistemas y navegadores, como programa o como extensión. Aunque intercepten tus datos, no sabrán de quién son.

Cómo establecer una VPN

Para usar una Red Privada Virtual hacen falta tres cosas: un cliente, un servidor y una llave o certificado. El cliente VPN es el programa que se instala el usuario en su ordenador para comunicarse con el servidor remoto, y la llave es su certificado de autentificación. En cada contacto, el cliente enseña sus credenciales al servidor y espera a que el servidor demuestre que es quien dice ser. Si hay un tercero interceptando tu tráfico y haciéndose pasar por el servidor VPN (como en un ataque *Man-in-the-middle*) no podrá resolver esta parte del proceso y la comunicación será imposible.

Por su parte, el usuario debe usar sus propias claves para acceder al servicio (si no, cualquiera con acceso a su ordenador sería capaz de entrar). Una vez el intercambio es validado, todas las comunicaciones entre usuario y servidor serán cifradas y toda su actividad online será anónima para todos menos para la empresa contratada. Todo lo que hagamos dentro del servidor VPN (visitar páginas web, tener reuniones, intercambiar archivos, conducir entrevistas) será completamente opaco para el mundo exterior. Desde el punto de vista de la Red, todo sucede en la oscuridad de un túnel cifrado. Un buen servicio

rebautiza a los usuarios con IPs aleatorias y genéricas para que no se sepa de dónde vienen ni quiénes son.

El primer paso es elegir un servidor VPN. Salvo que nos inviten a uno o seamos capaces de montar uno a distancia —una habilidad que por desgracia no ha sido incluida aún en los cursos de periodismo de ninguna universidad española—, la manera más sencilla de hacerlo es contratar el servicio. Como nuestra prioridad es la seguridad no nos vale cualquiera o el más barato. El procedimiento más adecuado es preguntar en los foros de seguridad, donde todavía se reúnen los *geeks* para hablar de cosas importantes. En estos círculos, la reputación es lo más importante, porque no nos queda más remedio que fiarnos de que los responsables no tienen dispositivos ocultos que registren nuestras actividades. O que tengan su sede en un país que no imponga censura ni sea especialmente propenso a requisar o registrar servidores. Esto ya deja muchos países fuera.

Siguiendo con la metáfora del club de campo, los administradores deberían dejarnos ver las instalaciones antes de hacernos firmar el contrato. ¿Cómo saber si es el lugar adecuado para nosotros?

Cómo reconocer un buen servicio VPN

–No quieren saber quién eres. Los servicios más comprometidos con la seguridad prefieren saber lo menos posible de ti. Si el proceso de contrato exige mucho más que una dirección de correo, sácalo de la lista.

–No quieren saber lo que haces. Si sus términos incluyen el mantenimiento de registros (logs) por «motivos de seguridad» o como seguro contra actividades ilícitas, no nos vale para nada. Su protocolo debería incluir un cambio automático de dirección IP y, si cabe, la destrucción periódica de metadata cada poco tiempo (dos días). Si no sabes cómo debería ser la declaración de intenciones apropiada de un servicio VPN, fíjate en la de Private Internet Access, un favorito entre los expertos en seguridad corporativa con sede en Estados Unidos y servidores de salida en Canadá, Reino Unido, Suiza y Holanda:

No mantenemos absolutamente ningún registro de ninguna clase. Utilizamos direcciones IP compartidas en lugar de direcciones IP dinámicas o estáticas para que sea imposible conectar al usuario con su IP externa. Estas son algunas de las soluciones que hemos implementado con los años para ofrecer el más alto grado de anonimato entre nuestros usuarios. Pero nos gustaría animar a nuestros clientes a usar e-mail anónimo y pagar con Bitcoin para asegurar todavía más los niveles de anonimato.

Nuestros tres principios son: privacidad, calidad de servicio y atención al cliente inmediata. No compartiremos ningún tipo de información con terceras personas sin una orden de registro válida. Y aunque eso ocurriera, sería imposible conectar a ningún usuario con ninguna actividad que haya tenido lugar en nuestro sistema porque usamos IPs compartidas y no mantenemos registros de nada.

Así tiene que sonar un servicio de red privada: directo, informado, específico y cien por cien comprometido con la privacidad de sus clientes. Y todo eso por cuarenta dólares al año.

–Pasa el test de derrame de DNS. El DNS es el servicio de nombre de dominio que convierte nuestra dirección IP en un dominio (Dominio.com). Para comprobar que somos invisibles dentro de la VPN, podemos ir a dnsleaktest.com dos veces, una antes y otra después de conectarnos a la red privada. La dirección IP debería pasar de ser la nuestra,

con su dirección asociada en el mapa, para convertirse en una IP genérica y apuntar a la localización geográfica del servidor contratado.

–Tiene opciones discretas de pago. Como entrar en un banco y pagar o usar una divisa criptográfica vigente. Cualquier pago con tarjeta, transferencia o Paypal compromete seriamente tu identidad.

–No te obliga a instalar su propio software. Como ya aseguramos en el *Manual de la Cryptoparty* (Berlín, 2012) hay una solución de software libre para cada problema. Si instalas un software propietario nunca sabrás si tu actividad está siendo protegida o todo lo contrario.

–No usa el protocolo PPTP (Point-to-Point Tunneling Protocol) diseñado por Microsoft sino OpenVPN (basado en SSL) o IPSec (ver nota sobre PPTP). Hay servicios como WiTopia que ofrecen un plan sencillo que solo usa PPTP y otro más caro (como el doble de caro) que incluye OpenVPN/IPSec.

–Es multiplataforma. Si no puedes usarlo desde tu móvil o tu tableta, es como ponerse la coraza y olvidarse el casco o los zapatos. Si no puedes usarlo desde cualquier ordenador (tenga Linux, Windows o OS X), no sirve para trabajar desde ordenadores prestados ni para colaborar con otras personas.

–Es rápido. De nada te sirve estar protegido si no puedes navegar.

–No es nuevo. La reputación lo es todo. No te fíes de nadie que todavía no se haya labrado la suya.

–No es gratuito. Sospecha de todo lo que sea gratis porque lo que dicen es completamente cierto: Si no lo pagas, no eres el cliente, eres el producto. El modelo de negocio de los servicios gratuitos suele ser la publicidad, y lo natural es que registren tus actividades aunque solo sea para colocarte anuncios más ajustados a tus inquietudes.

Como en todo, se pueden hacer excepciones. Si estamos atascados en un aeropuerto y necesitamos usar la Red para algo no especialmente sensible pero nos da repelús usar el wifi sin protección, es mejor una VPN gratuita que ir a pelo; de la misma manera que es mejor usar spray espermicida a no usar nada, pero lo más seguro es ponerse un condón. Las redes de los aeropuertos son particularmente populares entre los husmeadores (*sniffers*) porque están completamente desprotegidas y abundan usuarios histéricos y descuidados tratando de comprar billetes o reservar habitaciones en hoteles marcando una y otra vez su tarjeta de crédito. Si solo queremos abonarnos a Netflix o ver vídeos que no están disponibles en nuestro país también es una opción razonable. Al menos mientras abonarse a Netflix desde países que no lo tienen todavía sea legal (nunca se sabe).

–Ten varios servidores distribuidos por los países seguros. O, dependiendo de las necesidades específicas de cada caso, los países apropiados. StrongVPN tiene un plan de 7 dólares al mes que ofrece solo servidores con protocolo PPTP (mal) y salidas a cuatro ciudades pero, por 30 euros al mes, tienes servidores con OpenVPN y salida a 15 ciudades.

¿Por qué es importante esto? Porque la ley que protegerá la intimidad de nuestros paquetes de datos será la del país del servidor de salida, que es de donde los datos aparentarán haber venido. La opción habitual es escoger un país con una ley fuerte de protección de datos, como Holanda o Suiza. Otra tendencia es la de buscar países con burocracias incompatibles a la nuestra, aplicando el principio de que los enemigos de mis enemigos son mis amigos.

Eso significa que los disidentes norteamericanos tendrían que elegir Rusia, los chinos, Suecia y así elegir un servidor cuyo gobierno ha sido históricamente incapaz de colaborar con el tuyo. Esta tendencia tiene un peligro claro: que un país no quiera

entregarte gratis no significa que no quiera negociar tu entrega.

–No hay quejas de ningún usuario ni acusaciones fundadas de filtraciones contra el servicio en cuestión.

Cuando contratamos el servicio, lo normal es que nos den al cliente el software adecuado para nuestro sistema operativo. Pero también hemos dicho que no debemos instalar un software propietario de la empresa y que el estándar de seguridad para los expertos en la materia es OpenVPN.

Cuidado con el PPTP

En realidad PPTP no tiene uno sino dos problemas bastante gordos. El primero es que se trata de un protocolo poco seguro, hasta el punto de que sus propios desarrolladores en Microsoft recomiendan no usarlo. El segundo es que sus vulnerabilidades son bien conocidas y tienen poco o ningún arreglo, porque no son agujeros en el sistema que se pueden eliminar o parchear, sino errores estructurales de diseño que no pueden ser corregidos sin desarmar la herramienta y acabar con su flexibilidad.

La misma gente que lo diseñó para Microsoft asegura que no pueden cambiar el diseño de Linux PPTP sin que deje de funcionar con Microsoft PPTP y viceversa. «La única solución es eliminar el producto y promocionar otro —concluyen en su revisión—. Nuestra elección para sistemas Open Source es OpenVPN o IPsec.»

La pregunta evidente es: si es frágil y todo el mundo lo sabe, ¿por qué no lo eliminan del mercado? La respuesta es que PPTP es muy fácil de usar: está disponible en casi todos los servidores, es sencillo de instalar y tiene buena documentación. Como hemos apuntado antes en la lista de virtudes del buen servidor VPN, el servicio, empresa o individuo que se toma la seguridad en serio utiliza estándares abiertos como OpenVPN.

3. YA TENGO CLIENTE, SERVIDOR Y CLAVE

En este manual instalaremos OpenVPN, que usa el mismo tipo de cifrado del que hemos hablado antes (SSL/TLS) y funciona en los tres sistemas operativos principales: Linux, Windows y OS X. Si ya estamos en este momento del proceso es porque ya hemos contratado el servidor VPN. Al terminar, la empresa nos habrá mandado un nombre de usuario y contraseña y unas instrucciones de instalación. Aunque suele haber un instalador automático, aquí veremos cómo hacerlo manualmente para entender la alineación de jugadores.

La configuración manual empieza por descargarse un .zip con archivos para configurar el cliente en nuestro ordenador. Una vez descomprimidos, el directorio puede incluir:

Nuestras claves criptográficas
Un archivo de configuración con la extensión .conf o .ovpn
El certificado llamado ca.crt
El cliente, con la extensión client.crt
La llave, con la extensión .key
Una lista con los servidores disponibles

A veces el archivo de configuración acabado en .conf/.ovpn contiene toda la información necesaria y solo ese archivo para instalar todo lo necesario. Otras veces parte

de esa información se guarda en un directorio del sistema, lejos de la carpeta de usuario. Cada casa tiene sus particularidades.

4. CONFIGURAR EL CLIENTE OPENVPN EN LINUX

Todas las distribuciones modernas de Linux tienen un Network Manager o Administrador de Redes. Si usamos un entorno gráfico, podremos encontrarlo en el panel de herramientas permanentemente visible donde también vemos la fecha, el estado de la batería, etc. Es el mismo programa que usamos para configurar nuestra conexión wifi. Al pinchar, seleccionamos la opción VPN Connections y Configure VPN (si la opción no aparece es porque tenemos que instalar un paquete llamado network-manager-openvpn). Veremos una lista con nuestras conexiones por cable (Ethernet) e inalámbrica (wifi). Añadimos una (Add) y escogemos el tipo de conexión OpenVPN. Al crearla se abrirá un menú de configuración que vamos a rellenar con los datos que nos han dado. Tiene tres pestañas: General, VPN y IPv4.

1. General: no tocamos nada.
2. VPN: rellenamos Gateway con la información del servidor contratado, algo como vpn.servidorvpn.nl. Cambiamos la seguridad a contraseña (password) e introducimos nuestro usuario y contraseña. El certificado de la casilla siguiente debería aparecer automáticamente o estar en la carpeta que hemos descomprimido. Si no está ahí, es probable que la hayan colocado en una carpeta del sistema tipo /etc/ssl/ca.crt. Si no lo encontramos, el FAQ del servicio o los administradores podrán aclararnos dónde está.
3. Pinchamos en Avanzado. Marcamos el tipo de compresión LZO (salvo que las instrucciones indiquen otra cosa) y, en Seguridad, metemos el tipo de cifrado y autentificación. Aunque tengamos opiniones muy encendidas acerca de cuál debería ser el estándar mínimo, lo más seguro es confiar en las especificaciones del servicio que hemos contratado, porque son las que están optimizadas para su configuración específica. Si pensamos que la capa de cifrado AES-256-CBC es una combinación muy pobre, siempre podemos hablar con el administrador y preguntarle si podemos subir a 512. Pero, salvo que sepamos a ciencia cierta que nos vigilan las tres agencias de inteligencia más poderosas del planeta, es como ir a comprar el pan en tanque. Es más seguro pero no especialmente productivo.
4. Después de guardar todas las indicaciones del servidor, el sistema nos pedirá una contraseña para generar una clave. Como ocurre con el resto de tecnologías de cifrado, nuestra protección es tan fuerte como nuestra contraseña: es importante elegir una apropiada, que sea lo bastante larga, errática y mestiza para que no pueda aparecer en una de las miles de millones de bases de datos de contraseñas que circulan por los foros de *hackers*, ni ocurrírsele a nuestra hermana en un momento de lucidez fraternal. Si no sabes de qué se trata todo esto, vete al capítulo de contraseñas.
5. Una vez acabado todo volvemos al asistente de configuración de redes y pinchamos en la nueva red VPN que hemos creado. Para comprobar que nos conectamos a través del servidor VPN, podemos volver a dnsleaktest.com y ver que nuestra IP corresponde ahora al servidor remoto y pinchar en Extended Test, solo por diversión.
6. Para desconectar, volvemos a pinchar en el Network manager y en Desconectar.

5. CONFIGURAR EL CLIENTE OPENVPN EN OS X

Lo primero es descargar un cliente de OpenVPN llamado Tunnelblick del repositorio de Google Code: code.google.com/p/ tunnelblick. Ni pensar en la versión en Beta salvo que sepa uno lo que estás haciendo.

1. Lo instalamos haciendo doble clic en el icono y, cuando termine, lo empezamos y lo volvemos a cerrar. Es importante hacerlo en ese orden porque, aunque parezca que no hemos hecho nada, Tunnelblick ha creado el nido donde instalaremos el paquete de configuración que nos manda el servicio de servidores VPN.
2. Descomprimimos el paquete de instalación y pinchamos en el archivo de configuración.
3. Una vez acabado el proceso podemos volver a abrir Tunnelblick con nuestro nombre de usuario y contraseña y guardarlo en nuestra Keychain. El icono de conexión con el server debería aparecer por defecto. Para conectarnos solo tenemos que pinchar en él.

6. BOLA EXTRA: CONFIGURAR L2TP EN OS X

Podría pasar que no tengamos acceso o no queramos instalar Tunnelblick porque todo esto parece muy raro. Si es así, también podemos configurar una conexión L2TP. Para eso no hace falta descargar nada más que el directorio del servidor. Vamos a Preferencias del sistema y abrimos el Administrador de Redes (Network). Para realizar cambios es necesario desbloquear la ventana pinchando en el candado de la esquina inferior izquierda e introducir nuestra contraseña de administración. Una vez aceptada:

1. Añadimos una nueva red pinchando en +. Nos ofrecerá varias opciones y tenemos que elegir interfaz VPN, tipo L2TP sobre IPSec y el nombre del servicio que hayamos contratado.
2. En Conexión introducimos el servidor y nuestro nombre de usuario.
3. Pinchamos en la configuración de autentificación y elegimos el formato apropiado. En la de usuario suele ser una contraseña (la escribimos) o un certificado que tenemos que buscar en el directorio que hemos descomprimido. En el de máquina, lo mismo. Clicamos OK.
4. Una vez acabado este paso podemos ir a Opciones avanzadas y elegir que todo el tráfico pase por nuestra conexión VPN. Pinchamos en Conectar y nos pregunta si queremos aplicar los cambios. Decimos que sí y esperamos a que el color de la red VPN cambie a verde.
5. Para comprobar que estamos bien conectados visitamos dnsleaktest.com, a ver si nos reconoce. La dirección IP que salga ya no debería ser la nuestra sino la del servidor.

7. CONFIGURAR EL CLIENTE OPENVPN EN WINDOWS

Lo primero es bajarse el directorio con el instalador del servidor que hemos contratado y la última versión estable del cliente de la página de openVPN: http://openvpn.net/index.php/opensource/downloads.html

OpenVPN solo funcionará en versiones superiores a Windows 2000. Los que tengan versiones más antiguas tienen cosas más importantes de las que preocuparse (o pueden instalar Linux, que es perfecto para rejuvenecer ordenadores de mediana edad).

1. Cuando abramos el programa, podemos aceptar las opciones por defecto del asistente de configuración, incluyendo licencia y componentes de instalación. Una vez acabado, tendremos un directorio C:\Program File\openVPN\config\ (salvo que la hayamos instalado en otro lado a propósito).

2. Abrimos el directorio del servidor VPN y volcamos su contenido en la nueva carpeta de configuración C:\Program File\openVPN\config\. El más importante se llama client.ovpn, si no está en ese directorio no podremos abrir el programa.

3. Si lo hemos movido todo bien, deberíamos encontrar OpenVPN en el menú de programas y en la barra de iconos del escritorio.

4. Desplegamos el menú del programa y seleccionamos Abrir como administrador y después el icono de OpenVPN. En el menú de iconos donde normalmente están el reloj y los avisos de configuración aparecerá una flecha, que podemos pinchar para desplegar la lista de redes VPN posibles. ¡De momento será muy corta! Elegimos nuestra conexión VPN.

5. Introducimos el nombre de usuario y contraseña que nos ha dado el administrador del servidor. El resto de la configuración —autentificación, llaves, etc— será gestionado por el archivo de configuración que descargamos al principio. Al final de este proceso, si todo ha salido bien, el icono se volverá verde para indicar que la conexión está activa.

Tor

Nadar envuelto en capas de cebolla

*L*a World Wide Web es solo la punta del iceberg. Bajo la superficie está la llamada Deep Web, llamada también Web invisible porque sus contenidos no salen en los buscadores comerciales. Dicen que es varias veces más grande que la capa visible (visible significa que está en el listín de Google y, por tanto, sale en las búsquedas). También dicen que esconde una masa de cuentas bancarias, registros académicos y administrativos, archivos históricos y, en general, datos en crudo que no se quiere o puede indexar. En ese continente subterráneo está Tor (The Onion Router), una infraestructura de túneles subterráneos recontracifrados donde la identidad de cada nodo se pierde en un inteligente juego de espejos.

Tor es la herramienta preferida de los *cypherpunks* porque no requiere que depositemos nuestra confianza en los administradores de un servidor lejano, como pasa cuando usamos VPN. También la usan disidentes en China, Irán y Siria, especialmente desde que descubrimos, gracias a uno de los muchos documentos que «liberó» Edward Snowden, que la NSA lleva años intentando romper la protección del sistema sin éxito. De momento, los espías mejor pagados y equipados del mundo solo pueden desenmascarar a un usuario de Tor cuando esconde otras vulnerabilidades en sus ordenadores. Como, por ejemplo, un plugin para escuchar música.

La NSA ha podido intervenir el navegador de Tor cuando el usuario ha modificado su configuración para instalar algún software que no debía. Gracias a esos pequeños agujeros, la agencia pudo instalar su propio código en el disco duro del usuario, garantizándose el acceso a todo su tráfico y hasta registrando todo lo que escribe con un programa que registra las pulsaciones sobre el teclado y las transforma en texto. Una vez el sistema está comprometido hasta este punto, no hay criptografía capaz de salvarnos.

En esos casos el uso de Tor no ha sido suficiente, pero solo porque el usuario ha descuidado otro aspecto de su sistema. Es importante ser exquisitos, y evitar blindar la puerta para dejarse abierta la terraza. En otros casos, la NSA y la GCHQ (la mayor agencia de espionaje británico) han llegado a colocar escuchas en las arterias de la World Wide Web, unos cables trasatlánticos que conectan unos continentes con otros y que, en algunos países, se limitan a una sola línea por donde pasa el tráfico centralizado de todo el país. La idea es capturar la señal que emiten esos cables e identificar la que corresponde a Tor para después cruzar la información con el mayor número posible de nodos de salida.

Son medidas desesperadas que solo tienen sentido si se pudiera tener acceso a todos los cables en todo momento y si los nodos no cambiaran de persona o de lugar. Los documentos de la Agencia dejan bien claro que Tor sigue siendo impermeable a sus ataques: «Nunca seremos capaces de desanonimizar a todos los usuarios de Tor de manera continua —se puede leer en uno llamado *Tor Stinks* (Tor apesta)—. Con análisis manual podríamos desanonimizar a una fracción muy pequeña». De momento no han podido desanonimizar a ningún objetivo directo. Otro documento de inteligencia llama a Tor «el rey del anonimato superseguro», lo que no deja de tener su gracia porque todo empezó en su propia casa.

Tor es un proyecto militar desarrollado en el Laboratorio de Investigación Naval de Estados Unidos por un encargo del DARPA. Aunque sigue recibiendo becas del gobierno y

del ejército norteamericano, sus responsables lo desvincularon de las fuerzas armadas en 2005 gracias al apoyo de la Electronic Frontier Foundation. Hoy el proyecto se llama The Tor Project y es el software que usan Snowden, Julian Assange y todos los activistas de perfil superior para sus comunicaciones.

También es el sistema que utiliza la famosa Dark Web, un «barrio chino» de webs subterráneas donde uno puede contratar sicarios, encargar documentación falsa, hacerse o deshacerse de coches robados, armas de fuego, pornografía ilegal, animales protegidos, etc. Los que acceden a través de Tor (y se esconden dentro) se llaman *hidden services* (servicios ocultos). Entre las millones de páginas que ha habido enterradas entre sus capas de amorosa cebolla ha habido grandes estrellas. La reina es sin duda WikiLeaks, cuyos servidores están físicamente repartidos por todo el planeta pero sus branquias digitales respiran en los servicios ocultos de Tor. Y uno de los grandes fenómenos ha sido Silk Road, una especie de eBay de compraventa de drogas que solo admitía pagos con Bitcoin. La plataforma funcionó durante dos años con un margen de beneficios de 1.200 millones de dólares sin que la policía supiera cómo desmantelarla.

Ustedes dirán: ¡pero Silk Road fue cerrado! ¡El dueño está en la cárcel! Y tendrán razón, pero solo en parte. Cuando por fin arrestaron al capo —un exestudiante de física de 29 años que compartía casa en San Francisco y se hacía llamar Temible Pirata Roberts— no fue porque consiguieran quitarle las capas a la cebolla. Lo pillaron porque, en una inspección de rutina, la aduana canadiense encontró un paquete postal que viajaba en dirección a su casa con nada menos que nueve pasaportes falsos. Lo más triste de todo es que no los quería para viajar sino para alquilar más servidores en otros países y expandir su imperio sin salir de su habitación.

Cómo funciona Tor

Como ya hemos visto antes, cada vez que nos conectamos a la Red para navegar, chatear o enviar correos nuestro sistema envía paquetes de datos con información sobre nosotros. Cuando navegamos a través de Tor, los paquetes quedan reducidos a lo imprescindible y viajan protegidos por varias capas de criptografía de clave pública. Además, cada vez que se abre un canal de comunicación en el sistema, Tor genera un circuito virtual para que el tráfico circule por él.

En otras palabras, los paquetes no van directamente a su destino sino que realizan un recorrido disperso, impredecible y aparentemente anárquico, saltando de nodo en nodo hasta llegar a su destino, de modo que ninguno sabe de dónde viene el paquete ni a dónde va. Cada nodo recibe el paquete junto a la dirección del siguiente nodo y lo envía sin poder abrirlo, modificarlo, reconducirlo o conocer su destino final.

Los usuarios de Tor forman una comunidad, una especie de sociedad secreta cuyo único requisito es llevar máscara (usar Tor). Como es de esperar, la oscuridad ofrece un lugar de encuentro para disidentes, activistas y *leakers*, pero hay muchas y variadas especies nocturnas, no todas recomendables. Pero, en comunión con la filosofía *cypherpunk*, su discreción ha sido implementada de manera tecnológica, no ideológica ni moral. Los miembros del club no necesitan fiarse unos de otros ni vigilarse unos a otros para que todo funcione.

Así se pela una cebolla

Pongamos, por ejemplo, que queremos leer un artículo de eldiario.es. Cuando escribo la url en el navegador y accedo a la página, el servidor de eldiario.es registra que un lector ha entrado de 22:36 a 23:58 desde un ordenador con Linux Mint, usando Mozilla Firefox como navegador y ha pinchado en este enlace y este otro antes de despistarse y acabar viendo vídeos musicales en YouTube. Pero ojo: entre el servidor de eldiario.es y nosotros hay muchas más paradas y esa información, junto con otras muchas, pasarán a formar parte de nuestro historial en el Data Center de numerosas agencias, compañías o grupos interesados dentro y fuera de nuestro país. Por no hablar de las *cookies*. Navegando sin protección se cogen cosas por ahí.

Ahora bien, si usamos Tor —que incluye una versión modificada de Mozilla Firefox— nuestra petición sale de casa tapada de pies a cabeza y pasa por un mínimo de tres nodos (llamados relays) que también están protegidos. Cuando por fin sale de Tor y llama a la puerta del servidor de eldiario.es, la información que revela es la del último nodo, llamado de salida o exit relay.

Los nodos de salida están en la muralla de Tor, al borde del reino, y tienen una gran responsabilidad. Son los intermediarios entre la red secreta y el exterior, como Caronte entre el mundo de los vivos y el de los muertos, y canalizan todo el tráfico porque el sistema está configurado para que ninguno de todos los nodos parezca ser el origen del paquete de datos salvo el último. Es por eso que la EFF aconseja que los nodos de salida sean siempre un servidor dedicado en un servicio comercial y no un ordenador personal en una casa u oficina.

Tener un nodo de salida en Tor no es ilegal, pero significa hacerse responsable de todos los paquetes que salen de la cebolla, sin tener control sobre su contenido o la naturaleza de sus remitentes. El blog de Tor incluye un manual pormenorizado con todas las medidas que se pueden tomar para tener un nodo de salida en Tor sin comprometer su integridad personal. Pero como este manual quiere servir como guía para aquellos que necesitan esconderse y no exponerse, mi consejo es que se conviertan en un puente, que es igual de necesario pero mucho más discreto.

En la cebolla existen tres tipos de nodos: los normales (o nodos medios), los de salida y los puentes. Estos últimos son nodos invisibles, en el sentido de que funcionan como un nodo normal (no de salida) pero no están listados y, por lo tanto, no pueden ser bloqueados por las proveedoras de banda ancha. No se sabe cuántos hay ni quiénes son ni dónde están, pero se usan cuando pensamos que nuestra conexión a Tor ha sido bloqueada activamente por la compañía telefónica o por el gobierno, como ocurre en China.

Tor no sirve solo para anonimizar usuarios. Si configuramos nuestros servidores para que solo acepten tráfico dentro de la red de Tor, lo hacemos invisible. Es el caso de todos los servidores que operan en la Darknet y de todo el entramado de servidores de WikiLeaks, que no tienen una dirección IP como las webs convencionales sino una dirección Onion, una combinación alfanumérica de 16 caracteres que se genera de manera automática cuando se configura el servidor. Tor es por definición un sistema descentralizado: si desaparece un nodo de su red, otro ocupa su lugar como si nada hubiera ocurrido.

Para los que nunca salen a la superficie, la vida dentro de la Deep Web se parece mucho a la que hay fuera, pero de la misma manera en que un asentamiento Amish se parece a una pequeña ciudad. Tienen sus buscadores (Torch), su mensajería (TorPM,

PrivacyBox), su correo (Tor Mail). También hay un Twitter (TorStatusNet), una red de libros (TorBook) y hasta algo como Yahoo! Answers llamado Tor Answers. Es todo igual, pero completamente distinto. Y no hace falta participar para ser parte del sistema. Con instalar Tor y usarlo ya estás haciendo un servicio a la comunidad.

Instalar Tor

Hace un tiempo, instalar un proxy tan sofisticado como Tor era complicado y usarlo también era difícil. Hoy solo hay que instalarse un paquete llamado Tor Bundle. Hay uno para cada sistema operativo y, la mayor parte de las veces, la plataforma nos ofrece el apropiado sin que tengamos que pensar, porque nuestro navegador se lo ha chivado.

Algunos usuarios de Linux podrían tener dudas razonables acerca de si su sistema es de 32 o 64 bits. Lo más probable es que sea de 64 pero, para estar seguros, lo mejor es abrir un terminal y escribir *uname -m*) y después apretar Enter. Los usuarios de Windows encontrarán la información navegando por el menú, bajo Propiedades del sistema.

Bundle significa hatillo. El de Tor consiste en una combinación de aplicaciones que, juntas y bien usadas, son lo más cerca que hay de trabajar con máxima seguridad. En el momento de escribir este libro (Version 3.5.2.1), el paquete incluye el cliente de Tor (Vidalia), una interfaz gráfica, un proxy llamado Polipo y una versión comisariada de Firefox. Es importante que no la toquemos mucho.

Tener Tor instalado y funcionando no nos hace invisibles, tenemos que configurar las aplicaciones con acceso a Internet y que no son el navegador para que usen Tor como proxy. Y es imprescindible usar el navegador que viene en el paquete y no desafiar sus limitaciones. Salvo que se tengan habilidades especiales o sepamos exactamente lo que tenemos que hacer, lo mejor al principio es aceptar las opciones de configuración que vienen por defecto. Una de ellas es que no tiene instalado ningún *plugin* (add-on, extensión, Skin, App) externo ni *drivers* propietarios y chismosos como Javascript, RealPlayer, Quicktime, Flash, etc. Cualquier página que requiera de esos *plugins* quedará fuera de nuestro alcance pero, si los instalamos, será como abrir una ventana en la fortaleza. El resto de las precauciones no habrán valido para nada.

Eso significa, por ejemplo, que no podemos ver vídeos en Youtube o admirar algunos de los diseños más vanguardistas de la Red. Hay quien lo considera un fastidio. Yo prefiero entenderlo como una medida de presión para que los webmasters y diseñadores dejen de usar tecnologías que exponen a los usuarios y consumen más recursos de los que les corresponde. En tiempos de HTML5, usar Flash es un desatino. Renunciar a las páginas que lo hacen es la manera más efectiva de acabar con él.

También hay limitaciones de seguridad. Tor encripta los paquetes desde que salen de nuestro sistema hasta que llegan a su destino, pero lo que pasa una vez allí depende de la configuración del servidor final. El paquete de Tor incluye HTTPS Everywhere, un pequeño código que fuerza al servidor final a utilizar HTTPS, si es que lo tiene. Se trata de una extensión del protocolo normal de transferencia de hipertexto (http) que dirige el tráfico por un puerto distinto al habitual (puerto 443, en lugar de 80) y lo encripta usando el protocolo Secure Sockets Layer (SSL).

Es como un túnel que se abre entre nosotros y la página solicitada, pero el nivel de protección es relativo, porque se puede ver el túnel desde fuera. Si solo usamos HTTPS, nuestras comunicaciones quedan expuestas, aunque protejan su contenido. Cuando

navegamos sobre HTTP —cosa que, lamentablemente, hace casi todo el mundo— tanto nuestros datos como nuestras conexiones quedan desnudas a la vista de todos. Cualquier niño con un móvil del año pasado puede interceptarlos y leerlos. Muchos ya lo hacen.

Aunque ya es el protocolo estándar para bancos, comercios y otros servidores donde tienen lugar transacciones, no todas las webs tienen implementado ese tipo de protocolo y, cuando lo tienen, lo utilizan solo cuando hay dinero cambiando de manos. Hacer que todas las páginas de un servidor usen HTTPS ralentiza la navegación, por eso muchos servidores lo tienen pero no lo usan por defecto. HTTPS Everywhere sirve para forzar la transmisión segura sin tener que hacerlo a mano cada vez.

Hay muchas maneras de utilizar Tor. En un mundo perfecto, podríamos usarlo en todo momento sin tener que pensar en ello. Lamentablemente, los recursos son limitados y no siempre podemos trabajar donde queremos, con el ancho de banda necesario y el sistema apropiado. Lo mejor es llevar una versión de Tails en un pincho USB y usarla siempre que sea necesario.

Algunas reglas a observar por recomendación de The Tor Project:

No uses Torrent. Los sistemas de intercambio de archivos tienen la mala costumbre de ignorar las órdenes del proxy, aun cuando tengan la opción configurada. No es conspiración sino tecnología: la estructura del torrent requiere conexiones directas y, aun cuando nos conectemos a través de Tor, el *tracker* revelará nuestra dirección IP. Esto no solo nos expone a nosotros sino a todos los que haya a nuestro alrededor.

Renuncia a los plugins. Ya lo hemos dicho antes: Flash, RealPlayer, Quicktime, Realtime y en general toda esa familia de software propietario son vulnerabilidades en tu sistema. Puede que algunos de los plugins que ofrece el repositorio de Mozilla estén diseñados para reforzar la protección de Tor, pero no hay prisa. Si son software libre y son seguros, acabarán siendo parte del paquete.

Usa siempre HTTPS. HTTPS Everywhere elegirá usar HTTPS siempre que sea una opción pero, cuando no lo es, no puede hacer nada. Hay que fijarse siempre en la dirección y evitar todos aquellos servidores que no hayan implementado el protocolo de seguridad. ¡Sobre todo cuando hacemos transacciones o compramos billetes!

No abras adjuntos mientras estás en Tor. Es más, la regla debería decir: no abras adjuntos de desconocidos y mucho menos cuando estás conectado a la Red. Es la manera más popular de hacerse con un sistema. Cuídate especialmente de descargar y abrir archivos de texto o PDF porque pueden esconder programas que revelen tu identidad. En casos de necesidad, lo más seguro es abrir el documento en un ordenador desconectado de la Red.

Usa los puentes. Tor no deja que otras personas sepan qué webs visitas o qué tráfico generas, pero no les impide saber que estás usando Tor. En algunos países, el uso de herramientas de anonimización es suficiente para ponerte en una lista negra. Si todavía no estás siendo vigilado pero crees que podrías estarlo, configura el sistema para conectarte usando puentes. Si te sientes especialmente paranoico o tienes razones para pensar que te buscan, conéctate desde diferentes ordenadores y utiliza siempre un pincho USB con TAILS para protegerte con discreción y no dejar huella.

Sobre I2P, la Internet Invisible

Mucha gente me pregunta por la otra gran red del inframundo digital, llamada The

Invisible Internet Project (I2P). Se trata de una red similar a Tor pero solo en apariencia. Diseñada desde el principio como una darknet para descargar archivos sin temor a las autoridades, los usuarios se conectan mediante túneles cifrados pero la estructura está basada en el sistema P2P de intercambio de archivos y por tanto es completamente descentralizada. En ese sentido, Tor tiene un directorio central interno, no tan diferente al de la Red convencional.

Tor funciona como un «router cebolla» donde el cifrado se realiza en capas interconectadas, pero I2P es un «router ajo», con un protocolo que pega los paquetes de datos y los encripta juntos para que el tráfico sea lo más confuso posible para los mirones y las herramientas de análisis de tráfico. Los canales de ida y de venida son diferentes y, como es la costumbre en los sistemas de pares, todos los nodos participan en la entrega y tiene nodos de salida llamados Outproxies.

Pero corre sobre Java y tiene sensiblemente menos servidores de salida que Tor, gracias al sistema de pares. Por antigüedad, envergadura, número de usuarios y cantidad de personas capaces involucradas, Tor es la opción más segura para navegar y guardar la ropa, pero es verdad que el hosting de páginas ocultas funciona y es más rápido en I2P que bajo los Hidden services. Y es la mejor para su propósito primigenio: descargar con P2P.

Móviles

Navegar, llamar y hasta chatear (casi) seguro en el móvil con Orbot, Orweb y CsipSimple

*L*os móviles son chivatos naturales, la única manera real de proteger nuestras comunicaciones con un móvil es no llevarlo encima. Incluso antes de las revelaciones de Snowden sabíamos que un móvil revela el paradero de su portador aun apagado y fuera de cobertura. Después de las revelaciones sabemos que además también puede escuchar y grabar todo lo que ocurre a su alrededor. Pero el mundo del periodista gira en torno a su móvil, su primera ventana en tiempo real a los acontecimientos que le interesan. No podemos renunciar a él.

En circunstancias especiales y siempre que no se sospeche la intervención directa y específica de las agencias de inteligencia mejor equipadas de la historia, uno podría seguir el ejemplo clásico del *dealer* profesional y usar tarjetas de prepago en móviles de primera generación (cuanto menos inteligentes, mejor) para desecharlos cada pocos meses. Aunque —y en esto consiste el análisis de tráfico— si nuestros patrones de llamada y contactos se repiten, la estrategia se desarma. Solo sirve cuando viajamos de incógnito por un tiempo limitado. Para el día a día, la única salida es cifrar.

Pero lo primero es lo primero: proteger el teléfono por si lo roban, se pierde o nos lo dejamos en algún bar. La mayor parte de los teléfonos hoy en día tienen dos tipos de protección por defecto: un pin para desbloquear la tarjeta SIM que hay que introducir cada vez que se enciende el teléfono y un bloqueo de pantalla que se resuelve con una contraseña o dibujando un patrón. Todo esto está muy bien, siempre y cuando no lo hayamos desactivado porque es un desgaste tener que desbloquear el móvil todo el rato. Y otra cosa: es más segura la contraseña que el patrón, aunque satisface sensiblemente menos, y además es necesaria para el paso siguiente, que es cifrar el terminal.

El cifrado de todo el teléfono es una de las opciones de Android 4.0. Esto se encuentra en Ajustes Seguridad Cifrar teléfono. Es una buena idea, sobre todo si guardamos todas las contraseñas a nuestro correo y servicios, nuestras notas, la agenda de números, entrevistas, fotos y todas las cosas que los periodistas tenemos ahora en el móvil. Para hacerlo necesitamos tener activado el bloqueo de pantalla con protección por contraseña. También debemos asegurarnos de que el teléfono está enchufado o bien cargado porque tardará al menos una hora en hacer el proceso y, si se apaga y se interrumpe el cifrado, podemos perder archivos. Una vez cifrado, será imposible acceder a su contenido sin la contraseña de desbloqueo de pantalla.

Las opciones de GPS y localización por *wireless* deberían estar apagadas aunque, para ser honestos, la única manera segura de que no sepan dónde estamos llevando un teléfono encima es que le quitemos la batería, y ni siquiera eso es cien por cien seguro. Pero es bueno dejarlas apagadas porque consumen una gran cantidad de energía y ancho de banda. Todas las aplicaciones que requieren actualización de datos en tiempo real, desde el correo o Twitter hasta el GPS consumen muchos recursos. Si podemos vivir sin estar conectados todo el tiempo, es mejor (para el anonimato) tener el *wireless* y el resto de conexiones apagadas mientras no las usamos.

Tor en el móvil

Orbot es un proxy creado por el fantástico proyecto Guardian para llevar la cebolla a Android. Es gratis, libre y vale para lo mismo que en el escritorio pero con añadidos «de bolsillo». Ojo: usar Tor en el móvil nos protegerá de muchos y variados males —no todo el mundo es la NSA— pero, mientras tengamos uno en el bolsillo, estaremos siempre localizados para bien y para mal. Pero podemos controlar el tráfico. Está diseñado para que se pueda tuitear de manera anónima (cambiando el Proxy Host: localhost y Proxy Port: 8118) y chatear por túnel cifrado en combinación con Gibberbot.

También sirve para visitar páginas bloqueadas en redes institucionales o censuradas y puede ser configurado para proteger todas las comunicaciones (modo Universal) o funcionar de manera automática con otras aplicaciones seleccionadas. Como ocurre con Tor en el escritorio, el proceso ralentiza un poco las comunicaciones pero más vale lento y seguro que rápido y desnudo.

Orbot es una App para Android y se instala como cualquier otra: vamos a Google Play, buscamos la aplicación y la instalamos, desde el escritorio o el mismo móvil. El proceso de instalación advierte de antemano de que, para disfrutar de todas sus ventajas, debemos instalar también otras aplicaciones como el navegador Orweb o Gibberbot, para tener conversaciones cifradas. Una vez terminada, apretamos la cebolla verde y *¡voilà!*: estamos conectados a Tor.

Para cambiar la configuración de lenguaje podemos acceder en el asistente del menú, donde también hay opciones para detener o salir de la aplicación. Para cambiar de identidad (IP) basta con arrastrar el dedo por encima de la cebolla, como si pasáramos página. Pero para navegar, como nos han avisado, tenemos que instalar Orweb, también disponible en Google Play o la página de The Guardian Project: guardianproject.info/apps/.

Una vez instalado, el Orweb nos dirá si estamos o no estamos usando Tor. Si la cebolla está verde y la pantalla nos felicita, es que lo estamos, aunque siempre podemos comprobarlo visitando una web que nos muestre nuestra IP. En el menú de configuración (Settings) podremos encontrar opciones de Proxy, puertos y limpieza de cache, cookies y otras cosas que se pegan cuando uno navega. Lamentablemente no hay versión para iPhone pero, si la seguridad es una prioridad, el iPhone no es una opción. Es una caja negra inexpugnable, pero solo para el usuario.

Hablar sin testigos: OSTN + CsipSimple

Contra todo pronóstico, hubo un tiempo en que Skype parecía una de las plataformas más seguras para mantener una conversación, con un uso pionero de canales cifrados y tecnología P2P para resguardar las conversaciones de oídos hambrientos de la Red. Sin embargo, muchos descartaron la plataforma cuando Microsoft la compró en otoño de 2011 por miedo a que sus conversaciones acabaran en la nevera de Bill Gates. El tiempo les ha dado rápidamente la razón: los papeles de Snowden revelaron que el tecnócrata había dejado la puerta amorosamente abierta a la NSA y el FBI para monitorizar el tráfico de Skype de manera masiva e injustificada.

Hoy hay muchas plataformas de VoIP (Voz sobre IP) que pelean por ocupar su sitio, pero no todas están cifradas y muchas menos son de fiar. El proyecto Open Secure Telephony Network (OSTN) pretende sentar las bases para un estándar de comunicación VoIP segura a través del protocolo SIP (Session Iniciation Protocol) para la conexión, el

protocolo de transmisión seguro SRTP (Secure Real-Time Transport Protocol) y el protocolo de cifrado ZRTP, encargado de negociar el intercambio de llaves criptográficas entre los dos interlocutores.

OSTN es un servicio que combina estas tecnologías para ofrecer una experiencia de llamada sencilla, ininterrumpida y abierta. Para abonarse hay que ir a la página del proyecto Ostel.co (nótese la falta de m al final de ese .co) y pedirlo (es completamente gratuito). Nos pedirá un usuario y una contraseña y, a riesgo de ser pesada, recordemos que la contraseña debe ser poderosa (ver capítulo sobre contraseñas). De nada nos sirve el cifrado si usamos la misma combinación en el correo, el Twitter y el cerrojo del gimnasio. Una vez generada la cuenta recibiremos un correo de confirmación con instrucciones.

Con esto nos abonamos al servicio pero, para que funcione en nuestro móvil, tenemos que descargar la aplicación, que se llama CsipSimple y está en Google Play. Cuando la hayamos descargado debemos abrirla y añadir una cuenta. Buscamos OSTN e introducimos el nombre de usuario y contraseña que hemos creado antes (si no nos acordamos, al menos el nombre y el servidor están en el correo de confirmación). El servidor es ostel.co. Una vez registrados, podemos comprobar que todo funciona llamando al número de prueba 9196. Oiremos nuestra propia voz (con retardo) y saltará una ventana de comprobación preguntando si el SAS es correcto.

ZRTP usa un sistema de autentificación de cuatro letras llamado *Short Authentication String* (SAS) que se genera cada vez que añadimos un nuevo interlocutor a la lista. El SAS se muestra a ambos lados de la comunicación y tiene que ser el mismo en ambos teléfonos. Para comprobarlo, lo leemos en voz alta. Si los dos interlocutores tienen el mismo, pueden validar la autentificación y seguir hablando tranquilamente. Si no lo es, significa que la conversación ha sido interceptada con un ataque Man-in-middle y ya no están seguros.

En circunstancias normales, cuando todo es correcto, la barra amarilla en la pantalla dirá que ZRTP está verificado y que todo funciona correctamente. En la barra negra hay una «i» de información donde se pueden ver los detalles de la llamada. A partir de aquí, ya podemos hacer llamadas seguras y videoconferencias.

Los usuarios de iPhone tienen un apaño, pero pagando. Se trata de una aplicación llamada Acrobits Softphone que cuesta 6,99 dólares y una extensión de ZRTP que cuesta 24,99 dólares. Una vez instaladas en el iPhone, añadimos una cuenta genérica SIP con el nombre de usuario y contraseña que usamos para darnos de alta en OSTN y, en la configuración avanzada, cambiamos el proxy a ostel.co, el protocolo de transporte a tls (sip), expires: 1800 y llamadas seguras a ZRTP. El resto es igual que en Android.

Para los que prefieren la mensajería, ChatSecure (antes conocido como Giggerbot) ofrece un cliente de mensajería instantánea cifrado con OTR (Off-The-Record) y compatible con Facebook Chat, Google Talk, Hangouts, Jabber, etc. Tiene versiones para Android y iPhone, además de versión de escritorio para Mac, Linux y Windows. En combinación con Orbot es perfecto para la circunvalación de firewalls. Pero atención: hacen falta dos para tener conversaciones secretas. Nuestros interlocutores tienen que usar un cliente que también use cifrado OTR. Hay muchos: ChatSecure, Adium, Jitsi, Gajim, Pidgin.

Archivos y correos cifrados en el móvil

En el capítulo dedicado a proteger el correo y las claves de llave pública ya hay una pequeña nota sobre cómo fortificar nuestros e-mails en Android con un cliente llamado K-9 y un gestor de claves llamado APG (Android Privacy Guard).

APG se puede usar también por su cuenta para cifrar correos y para cifrar documentos y otros archivos antes de mandarlos usando cualquier otra aplicación. Para esto bajamos la aplicación (es la de Thialfihar), la lanzamos y pinchamos en Encriptar. Después seleccionamos el archivo a cifrar pinchando en el icono de archivo. Si tenemos una clave pública podemos seleccionar ese modo de cifrado. Si no, tenemos que conformarnos con usar una contraseña y guardar el nuevo archivo con la extensión .gpg.

El programa tiene la opción de eliminar el archivo original una vez ha sido cifrado, para que no haya copias abiertas en la memoria. Si por algún motivo queremos conservar las dos copias, hay que deshabilitar esa opción. Si no encontramos los archivos cifrados es porque se guardan por defecto en la carpeta APG.

Para usar APG en el correo debemos descargar K-9 (y hacerlo en ese orden) que es un clon del cliente de correo de Android al que se le han quitado algunas cosas y añadido otras, todo en nombre de la seguridad. También necesitamos tener una cuenta de correo previa y nuestras claves pública y privada. Si no sabemos cómo generarlas, debemos leer el capítulo dedicado a la PGP. Android no tiene capacidad para generar claves del tamaño apropiado; tenemos que generarlas en el escritorio y después importar el archivo a APG desde el menú Manage Secret Keys. Si estamos usando la misma cuenta de correo en los dos lados, nada nos impide usar la misma clave. Una vez importadas, las claves aparecerán en todas las aplicaciones que tengan integrado PGP.

La configuración de K-9 es igual a la del cliente de correo oficial de Android y no supone un gran desafío salvo porque debemos asegurarnos de que el Tipo de seguridad es SSL (always) o TLS (always) y que en la caja de Criptografía o cifrado utiliza APG. Como en Thunderbird y todo en general, el mundo será un lugar mejor si usamos texto plano en lugar de HTML. Para todo lo demás —servidores, etc— debemos copiar la configuración de nuestro cliente de correo en el escritorio. En las opciones de frecuencia de actualización debemos dejarlo en ninguna, para bajar el correo manualmente cuando estamos en una red segura.

El cliente querrá verificar el certificado del servidor de correo antes de conectarse a él. Debemos comprobar que la huella SHA-1 que nos muestra coincide con el de tu servidor. Si no estás seguro de cómo hacerlo, para eso está el servicio de atención al cliente. Por último, si tienes más de un cliente de correo (como por ejemplo Thunderbird en el escritorio y K-9 en el móvil usando la cuenta del periódico) querrás cambiar la configuración del servidor de correo para que los mensajes no se borren al ser descargados por una u otra aplicación. Si no lo hacemos así, en lugar de tener una copia de todo nuestro correo en cada dispositivo los tendremos repartidos entre uno y otro, lo que genera una gran desesperación.

Una vez configurado todo, cada vez que escribamos un correo tendremos la opción de autentificarlo y de cifrarlo. Importar las claves públicas de nuestros contactos es más fácil y cómodo usando una tarjeta de memoria SD. También podemos instalar KeePassDroid.

Disco duro

Cómo proteger documentos, carpetas y hasta el contenido entero de tu ordenador o memoria USB

*E*n un mundo lleno de peligros, proteger nuestros datos mientras viajan es la manera responsable de navegar. Pero también hay muchos y buenos motivos para proteger esos documentos mientras están aparentemente seguros en el disco duro de nuestro ordenador. Un ordenador permanentemente conectado a la Red es una ventana abierta, no solo en casa. Si alguien tiene acceso a la red a la que estamos conectados —por ejemplo, en el periódico —, todos los ordenadores que se conectan a través de ella pueden estar comprometidos. Por no hablar de la amenaza física: si alguien entra en nuestra casa, oficina, redacción u hotel y consigue tener acceso físico a nuestro ordenador, de nada nos sirve cifrar el correo y guardar todos los documentos en una carpeta abierta que pone Importante.

Puede que seamos superprofesionales y extremadamente cuidadosos: nada evitará que una patrulla nos detenga en el aeropuerto y requise todas nuestras pertenencias. Pongamos que viajamos con la lista de nuestras fuentes en una memoria flash, como hizo Sean McAllister saliendo de Siria. Si no está protegida, todas nuestras fuentes están expuestas y hasta puede que nuestro descuido les cueste la vida. Si está protegida, también es posible que nos obliguen a facilitar la clave pero al menos habremos ganado tiempo para activar otros recursos, como el periódico o el consulado, antes de poner en peligro a nadie más.

Si tenemos dudas sobre qué documentos cifrar y en qué circunstancias, antes hay que tener en cuenta el principio de que ningún ordenador conectado a ninguna Red es seguro.

Si tenemos material que debemos proteger a toda costa, en casa, en el periódico o en el bolsillo, hay que pensar en esos datos como si fueran joyas de valor incalculable que no pueden quedar expuestas nunca más de lo estrictamente necesario. Lo natural sería guardarlas en una caja fuerte que solo abrimos cuando es imprescindible y que nunca dejamos abierta. En términos de tecnología digital doméstica, nuestra caja fuerte es un disco duro externo con protección criptográfica que solo montamos en nuestro ordenador cuando es estrictamente necesario y cuando dicho ordenador no está conectado a la Red.

En principio podemos encriptar lo que queramos, desde una carpeta específica dentro de nuestro disco duro hasta todo el contenido de nuestro ordenador, de manera que no llegue ni a encenderse sin la contraseña adecuada. También podemos hacer lo mismo con nuestras memorias USB y el contenido de nuestros teléfonos. Un software que ofrece seguridad, sencillez, flexibilidad y goza de una cierta reputación es TrueCrypt. Su licencia no ha sido aprobada aún por la Open Source Initiative y las principales distribuciones de Linux —incluyendo Debian, Ubuntu, Fedora, openSUSE y Gentoo— ofrecen en su lugar una implementación llamada tcplay.

Lamentablemente, tcplay no ofrece un Interfaz gráfico para los no iniciados. Como la consola todavía no es todo lo popular que debería (para iniciarse recomiendo apasionadamente la introducción a la línea de comandos de Flossmanuals), de momento nos conformaremos con TrueCrypt. La buena noticia es que, aunque su licencia no sea la deseable, su estándar de seguridad ha sido demostrado una y otra vez contra enemigos notables como la NSA y el FBI.

Cómo instalar TrueCrypt en nuestro equipo

Lo primero es ir a la página oficial de TrueCrypt [http://www. truecrypt.org] y descargar el software para nuestro sistema operativo. Una vez más, si somos linuxeros recién estrenados y no sabemos si nos corresponde el paquete de 32 bit o de 64, lo mejor es abrir un terminal y escribir *uname -m* y después apretar Enter.

Cuando pinchamos dos veces en programa, el instalador nos da dos opciones: instalar el programa y extraer los directorios. La primera opción es para instalar el programa en el ordenador; la segunda, para guardarlo en nuestro teléfono o memoria USB y usarlo discretamente. Aunque se puede usar el programa sin instalar, hay habilidades que no están cuando trabajamos directamente con el .exe, como el cifrado de todo el disco duro.

El asistente de instalación es sencillo e incluye todas las opciones deseables, incluyendo una versión traducida al castellano (Settings Language Español). Salvo que prefiramos guardar el programa en algún lugar específico, podemos pinchar Next hasta que esté cómodamente instalado en nuestro disco duro.

Tu nueva caja fuerte

Si la instalación se ha hecho correctamente, TrueCrypt ya debería formar parte del menú de programas. Cuando lo abramos, nos pedirá que creemos un volumen. Al aceptar, lanzaremos un nuevo asistente de configuración para la creación de nuestra primera caja fuerte.

El asistente nos ofrecerá tres opciones: a) crear un contenedor de archivos cifrados, b) cifrar una partición externa o USB y cifrar todo el disco duro. La segunda opción está diseñada para la portabilidad, discos duros externos y memorias USB. La tercera protege el sistema entero; cualquiera que quiera usar nuestro ordenador estará obligado a introducir una contraseña antes de que se inicie el sistema operativo. De momento, vamos a trabajar con la primera opción.

Crear un contenedor protegido es como instalar una pequeña caja de seguridad en la pared de casa. El asistente de instalación nos ofrece dos opciones: una caja estándar y una oculta. De momento, vamos a elegir la primera. Más adelante explicaremos para qué sirve la caja misteriosa.

Es extremadamente importante recordar que este proceso no sirve para cifrar contenidos sino para construir una caja de seguridad donde meter esos documentos, una carpeta protegida que podemos mover, renombrar y borrar. Cuando seleccionemos una caja estándar, el sistema querrá saber cómo queremos llamarla y dónde queremos ponerla. Hay que acordarse bien de dónde la ponemos porque nos hará falta encontrarla más tarde. La decisión es de importancia relativa porque, a diferencia de una caja de seguridad real, esta podemos relocalizarla más adelante donde nos resulte más conveniente, incluyendo una memoria USB o un servidor. Pero mucho cuidado con seleccionar directorios que ya existen porque, en lugar de encriptarlos, los borrará. Cuando hayamos creado y colocado nuestra pequeña caja negra, volveremos al menú principal.

En esta parte del proceso, el sistema nos ofrece diferentes algoritmos de cifrado (concretamente ocho en el momento de escribir este libro). AES es el estándar, pero Twofish y Serpent también tienen buena reputación. Las opciones combinadas como AES-

Twofish-Serpent ofrecen usar tres capas de cifrado en orden descendente. Esto es, que los datos son cifrados por un algoritmo y el resultado es cifrado por el siguiente algoritmo y el resultado de eso es cifrado por un tercer algoritmo. Cada uno de esos procesos tiene una clave diferente, siempre basada en tu contraseña original. La idea es que, si uno de los algoritmos es destripado, todavía nos protegen otros dos. También significa que el proceso será más largo y lento que un día sin pan. Encriptar es un trabajo muy duro.

Es más, hay quien dice que las capas de triple cifrado usando el mismo algoritmo (triple AES, por ejemplo) ofrecen más vulnerabilidades que una sola, lo que tendría más sentido si el valor inicial fuese el mismo las tres veces. En cualquier caso, no se puede fallar. Todas son tan extraordinariamente seguras que importa más crear una buena contraseña que haber elegido cualquiera de ellas. En cuanto al algoritmo hash, los expertos recomiendan usar de SHA-256 hacia arriba. SHA-512 fue diseñado por la NSA.

Lo siguiente es decidir el tamaño de nuestra caja fuerte. Si tenemos todos nuestros archivos sensibles en una carpeta, podemos mirar qué tamaño tiene y hacer un cálculo aproximado de cuánto espacio necesitaremos más adelante. Mejor holgada que justa, pero un volumen muy grande llamará más la atención. Si pensamos que el directorio protegido deberá «viajar» de nuestro disco duro a una memoria externa o un CD, el tamaño no debe superar la capacidad del dispositivo que vayamos a usar.

Si ya hemos elegido el nombre, la ubicación y el tamaño, solo queda introducir la contraseña. Como siempre, debe ser larga e incluir letras, números y símbolos en combinaciones que no salgan en el diccionario (ver capítulo sobre contraseñas seguras). En este caso no hay seguro contra olvidos, perder esa contraseña es literalmente como meter los documentos en la caja fuerte, cerrarla y perder las coordenadas. No podremos volverla a abrir.

Una vez tengamos contraseña (hay que escribirla dos veces y las dos veces tiene que coincidir para seguir con el proceso), el sistema procederá a generar la clave que cerrará nuestra caja fuerte. Cualquier cosa que hagamos mientras se genera salvo cerrar la ventana (mover el ratón, cambiar de escritorios, cambiar carpetas de sitio, crear caos y desconcierto en general) hará que la clave sea más compleja y, por tanto, más difícil de romper. Una vez generada, pasaremos a crear el directorio pinchando en *Format*. Tendrá el nombre que le dimos antes y se alojará donde nosotros establecimos unos pasos atrás. Ya podemos cerrar la ventana de enhorabuena (OK) y la aplicación (Exit) y ya tenemos caja fuerte.

Abrir, cerrar y modificar los contenidos de tu caja fuerte

Ya tenemos caja fuerte, pero ¡no podemos abrirla! Eso es porque no está montada, lo que significa que está en el sistema, pero cerrada con llave, lejos de miradas indeseables como tiene que ser. Para acceder a sus contenidos debemos montar el volumen, igual que montamos nuestros teléfonos, reproductores de música y cámaras de fotos en el sistema cuando las conectamos al ordenador. Pero montar este volumen equivale a abrir la puerta de nuestra caja fuerte, algo que solo debe ocurrir cuando y mientras necesitamos leer, crear, mover o borrar los documentos que hay dentro.

Si no estamos haciendo ninguna de esas cosas, nuestro directorio cifrado deberá permanecer desmontado del sistema, como una memoria USB que desconectamos del ordenador. Incluso cuando nuestro sistema está suspendido o hibernando, incluso si es de noche o no estamos conectados a la Red. Uno no se lleva a casa una caja fuerte para luego

dejársela abierta por la noche. En otras palabras: el directorio cifrado debería estar desmontado la mayor parte del tiempo.

Para montar el directorio y acceder a él, debemos volver a la ventana principal de TrueCrypt —si la hemos cerrado, podemos volver a abrirla pinchando en el icono del programa— y seleccionar cualquier número (o letra, dependiendo del sistema operativo) de la lista de unidades posibles. Da igual cuál sea, son como plazas de aparcamiento libres esperando a ser ocupadas. Una vez seleccionado, pinchamos en Seleccionar Archivo y buscamos nuestra caja fuerte, el volumen TrueCrypt que hemos creado antes. Después debemos Abrir, Montar e introducir la contraseña que hemos creado anteriormente.

El sistema pedirá la contraseña dos veces. No podrás seguir si la contraseña no es correcta las dos veces. Si tienes muchas cajas fuertes, recuerda que cada una tiene su propia contraseña. Si todo está correcto, podrás ver el directorio en la lista y en el directorio de unidades de tu disco duro. Si has elegido la letra T, entonces se mostrará como Disco local (T:).

Ahora puedes meter documentos, películas, música, fotos y cualquier dato que se te ocurra en la caja y quedará cifrado de manera automática. De la misma manera, cuando sacas un documento del directorio protegido, será descifrado automáticamente.

Es así de fácil. El programa tiene varios mecanismos de seguridad, entre ellos que, si el ordenador se apaga de pronto o el sistema falla, la caja se cerrará como una almeja y hará falta la contraseña para volver a abrirla. Pero no se cerrará si entramos en suspensión o nos quedamos viendo *Juego de Tronos* con la caja abierta. Para cerrarla, basta con volver a la ventana de inicio de TrueCrypt, donde están listados todos los volúmenes montados, seleccionar el nuestro y pinchar en Desmontar. Nadie podrá acceder a él sin tener la contraseña, incluyendo tú mismo.

Doble nudo: crear una caja de seguridad fantasma

Saber blindar nuestros documentos es cada vez más importante, pero también puede suponer un peligro en sí mismo. El uso de claves criptográficas es ilegal en muchos de los países que a los periodistas nos gusta visitar. Eso significa que, si te detienen con un disco duro encriptado y te niegas a facilitar la clave, pueden pasar muchas cosas desagradables.

Es más, un chequeo de rutina que revela material encriptado en un aeropuerto puede despertar la curiosidad de las autoridades y ponernos en alguna lista de sospechosos. La mayoría de las personas que se han hecho famosas en los últimos años por abanderar la criptografía como herramienta de resistencia a los abusos institucionales están en esas listas —a veces como terroristas internacionales— y sufren de manera cotidiana registros, detenciones e interrogatorios, solo por el simple hecho de defender su derecho a tener una caja fuerte en el disco duro de su ordenador.

Salvo que nuestro propósito sea, precisamente, que nos detengan por usar herramientas criptográficas y así demostrar que el sistema está corrupto y hemos perdido nuestro derecho a la intimidad antes de que la ley lo haya borrado de sus libros, la manera más productiva de usar estas herramientas es hacerlo sin que se note. Hay maneras de camuflar directorios protegidos para que no despierten sospechas.

La manera más fácil y rápida de hacerlo es cambiarle el nombre a los archivos. Pero hay que elegir bien el archivo del que lo vamos a disfrazar. Por ejemplo, parecería buena idea cambiarlo por una imagen —renombrar el archivo .tr como archivo .png o archivo .jpg

— y guardarlo en una carpeta con fotos turísticas de nuestro viaje. Lamentablemente, si a alguien se le ocurre abrirnos el disco duro y navegar por las carpetas, todas las fotos mostrarán una *preview* menos la falsa. También hay que mirar el tamaño de los archivos. Si es un archivo pequeño, podemos camuflarlo como documento de texto o PDF. Si es verdaderamente grande, tendrá que ser otra cosa, como un .iso, para que el tamaño tenga sentido. No demos por sentada la falta de habilidades informáticas de las autoridades aeroportuarias. Si nos equivocamos, no hay segunda oportunidad.

La técnica de camuflar una información dentro de otra se llama Estenografía. Es una estrategia fascinante que se practica desde hace milenios, desde los generales que tatuaban instrucciones en la cabeza de sus esclavos hasta las cartas de amor que solo revelan su verdadero contenido en contacto con el fuego, el humo o el agua. Hoy hay muchas herramientas de estenografía digital, algunas formidablemente complejas, que sirven para esconder todo tipo de datos dentro de otros datos.

Uno podría, por ejemplo, camuflar las obras completas de Tolstoi en un *gif* animado del pato Lucas, la Declaración Universal de los Derechos Humanos de 1948 o la tercera sinfonía de Brahms, sin que ninguna de sus tapaderas cambie de aspecto o de tamaño. También se pueden camuflar datos —imágenes, documentos, audio— en mensajes de correo. Si el mensaje o el documento es interceptado, las autoridades no ven un documento sospechosamente blindado sino otro vídeo de gatitos.

La solución que ofrece TrueCrypt es una mezcla de las dos tácticas, y es la opción que hemos descartado antes, llamada «Esconder volumen TrueCrypt». La manera más sencilla de explicarlo es que crea un fondo falso dentro de la caja fuerte. Si nos detienen con un volumen de material cifrado y nos obligan a abrirla, podemos dar la contraseña de la caja fuerte. El documento que realmente queremos proteger estará camuflado dentro, sin que nadie lo pueda ver. Mejor aún, TrueCrypt está diseñado de tal manera que es imposible saber si hay o no hay un compartimento secreto dentro, salvo que el contenido digamos «oficial» que hemos expuesto parezca demasiado banal para merecer protección y despierte sospechas. Si ponemos las recetas de cocina de la abuela ya pueden ser buenas. Deberíamos poner ahí documentos que justifiquen el cifrado, como cartas de amor ilícitas o literatura indecente. A todo el mundo le gustan las cartas de amor.

Evidentemente, para esconder un compartimento dentro de una caja fuerte, necesitamos tener la caja. Si volvemos atrás en el proceso de creación de nuestro volumen cifrado y escogemos «Esconder un volumen TrueCrypt» en lugar de crear un volumen normal, nos encontraremos dos opciones: modo directo y modo normal. El modo directo es para meter nuestro directorio invisible dentro de un directorio que ya existe (por ejemplo, el que creamos en la sección anterior). El modo normal es para crear una caja nueva y después crear el compartimiento secreto dentro.

El proceso de creación de un nuevo volumen es idéntico al que ya hemos descrito, así que elegiremos la primera opción. El asistente de configuración nos dará una lista con los volúmenes protegidos que ya hay en nuestro disco duro. Debemos elegir uno y abrirlo. Como está sin montar —o, al menos, *debería* estarlo— tendremos que introducir la contraseña. Un mensaje nos informará de que el recipiente ha sido escaneado para determinar el tamaño máximo de nuestro directorio invisible. En los siguientes pasos tendremos que elegir un tamaño y debería ser lo más pequeño posible para dejar sitio en el directorio original. Un fondo falso que ocupa todo el volumen de la caja fuerte desafía su propósito. Y aquí debemos estar muy vigilantes, porque la caja fantasma tiene una extraña particularidad.

Digamos que nuestro directorio cifrado original tiene 20 megas y que nuestro directorio oculto 6. Eso quiere decir que quedan 14 megas libres en el directorio original. Es de extrema importancia que no excedamos ese límite o perderemos archivos. La explicación es que esta táctica está diseñada para que no se pueda saber si hay o no hay un volumen oculto. El sistema no nos avisará si el directorio original empieza a devorar el directorio fantasma porque, técnicamente, no sabe que existe. El directorio secreto es secreto hasta para el sistema, y por eso nos dejará llenar la caja hasta los 20 megas sin tenerlo en cuenta. Si nos excedemos de los 14 megas empezará a borrar cosas dentro del directorio oculto.

De hecho hay un seguro contra este tipo de riesgo. Cuando estamos montando los directorios cifrados, el menú ofrece la posibilidad de «Proteger el volumen oculto de daños causados por escribir en el volumen externo». Si usamos esa opción, el peligro de sobreescribir y borrar documentos valiosos desaparece, pero nuestro directorio invisible deja de ser invisible. Es mejor usarla solo cuando estamos actualizando los documentos del directorio cifrado normal en un entorno completamente seguro y desconectados de la Red.

Después de elegir el tamaño, el asistente nos pedirá que pongamos otra contraseña. Esta contraseña debe ser nueva y diferente de las anteriores, pero igual de compleja. Si nos encontramos en la obligación de desvelar una contraseña, daremos la de la caja original, que se abrirá sin nunca revelar la existencia del directorio fantasma. El resto del asistente es igual que el anterior (deja las opciones de tipo de archivo y nodo que aparecen por defecto) y, después de varios OK y de que el sistema te recuerde no meter más cosas de las que caben en el directorio, tendrás tu directorio cifrado invisible, camuflado dentro de una caja de seguridad.

Para montar el directorio invisible hay que seguir los mismos pasos que para montar un directorio cifrado normal: seleccionamos la unidad donde queremos montarlo (por ejemplo: F) y después seleccionamos el directorio donde lo hemos escondido. Cuando intentemos abrirlo nos pedirá la contraseña. Si ponemos la del directorio cifrado normal, abrirá ese directorio. Si ponemos la del directorio cifrado secreto, abrirá el secreto. Dos contraseñas, una sola puerta.

Opción C: TrueCrypt de bolsillo

Otra manera de disimular nuestra habilidad para encriptar documentos es no tener el programa instalado en el ordenador sino en una memoria USB o un disco duro extraíble. Esto tiene sus propias ventajas e inconvenientes: podemos usarlo para cifrar documentos cuando viajamos sin ordenador o usamos distintos ordenadores. Lo malo es que lo usaremos en ordenadores sobre los que no tenemos ningún control y podrían esconder virus, *malware* y escuchas de todo tipo, como un software de reconocimiento de teclado que registre todo lo que escribimos. Además, un pincho USB es más susceptible de ser interceptado y destripado que un archivo escondido en las tripas de nuestro disco duro.

Hay quien prefiere llevar los archivos cifrados en el ordenador y el programa en el bolsillo o la maleta para que el abrelatas esté lo más lejos posible de la lata. Otros prefieren hacerlo al revés; llevar los documentos en el bolsillo y el programa instalado en el ordenador con algún directorio cifrado lleno de bobadas para despistar. En cualquier caso, la versión portátil de TrueCrypt tiene varias limitaciones. Entre otras, no permite cifrar particiones ni el disco duro entero.

Antes de descargar el programa en una memoria USB tenemos que comprobar que es lo bastante grande (normalmente basta con pasarle el ratón por encima) y abrir un directorio o carpeta nueva en la que podremos después colocar el programa. Es mejor no llamarla TrueCrypt o Caja fuerte sino algo más discreto como fotos-vacaciones o facturas; algo que nadie querrá mirar sin que le obliguen. Después vamos a la página de descargas de Truecrypt.org y pinchamos en la última versión. En lugar de elegir Instalar, elegimos Extraer y descargamos el programa en la carpeta que hemos creado en la memoria USB.

Cuando terminamos de descargar el software, nos vamos a la carpeta y extraemos el contenido, que incluye entre otras cosas una Licencia, un manual en PDF y dos ejecutables. Para hacer funcionar el programa, debemos pinchar dos veces en TrueCrypt.exe. El resto del proceso —salvo por las limitaciones ya mencionadas— es exactamente igual que en la versión instalada normal. Podremos crear directorios protegidos, directorios fantasma y abrir los que ya teníamos con las contraseñas correspondientes.

Para dejarlo todo bien puesto, solo nos queda borrar el instalador (que se llamará TrueCrypt Setup junto con la versión y acabado en .exe) y desmontar el pincho USB. Que nadie note que nos instalamos programas «antisistema».

Full Data Detox

Limpiar nuestro sistema de información comprometedora

A estas alturas ya lo sabe todo el mundo: borrar es el nuevo guardar. Al igual que ocurre con los perfiles del Facebook, borrar documentos y ficheros en el ordenador no significa que los datos pasan a mejor vida o se evaporan en éter, como un holograma desconectado. Solo significa que desaparecen de nuestra vista y ya no los podemos ver, o encontrar.

También hay información que no vemos, como datos temporales que hemos acumulado en nuestro historial de navegación o archivos fantasma que se generan cuando escribimos un documento, extensiones invisibles, logs de correos y otras huellas digitales que viven camufladas en el sistema sin que las tengamos en cuenta. Tanto unos como otros pueden ser fácilmente recuperados con software forense de recuperación de datos.

La razón por la que pasa esto es que nuestros programas almacenan datos sin pedirnos permiso, y porque los datos que almacenamos en el disco duro —a propósito o sin querer— no son ni se comportan como los datos que almacenamos en el mundo real. Cuando borramos un archivo, este deja de aparecer en el escritorio o la carpeta donde estuviera almacenado. Su nombre ya no aparece en las listas ni en las búsquedas, pero eso es porque ya no está indexado, no porque ya no esté. Es como si una página dejara de estar indexada en Google; no podemos encontrarla sin saber lo que buscamos pero sigue colgada en la Red. Los datos son como un tatuaje; solo se pueden borrar tatuando otra cosa encima. Que es exactamente lo que vamos a hacer.

Limpieza de datos en Windows

Lo primero es descargar una pequeña herramienta llamada CCleaner que limpiará los archivos temporales y otros datos fantasma que viven en nuestro ordenador. Una vez la descargamos de su repositorio (poniendo CCleaner en Google o, mejor dicho, en DuckDuckGo) pinchamos dos veces para lanzar el asistente de configuración. Mientras se instala podemos elegir un idioma, instalar el programa para un usuario solo o para todo el sistema y, extrañamente, instalar Google Chrome y establecerlo como navegador predeterminado. De momento, vamos a quedarnos con Firefox (deshabilitando la casilla en cuestión) e instalar el programa. Cuando acaba el proceso, una ventanita nos preguntará si puede escanear el disco duro en busca de cookies. Si quieres mantener las tuyas, para que el navegador recuerde tus contraseñas y configuraciones, dirás que sí. Para limpiar todas las cookies dirás que no. A estas alturas ya sabemos todos cuál es la opción más segura.

Antes de lanzarnos a limpiar archivos, debemos pasar por la Configuración y cambiar un par de cosas. Aquí podemos salvar unas cookies (las más importantes) y debemos cambiar la opción de Borrado normal (Rápido) a Borrado seguro de archivo (lento). Podemos elegir entre varias opciones, de la menos intensa (1 pase) a la más intensa (35 pasadas). Si podemos dejar el ordenador haciendo su tarea mientras nos vamos a la cama o hacemos otras cosas, la más segura es la de 35 reescrituras pero, si vamos a dejar que la herramienta funcione por defecto, nos podemos conformar con la de 3.

De vuelta en el limpiador, el sistema nos ofrecerá varias opciones de programas y

de datos temporales para eliminar. Para hacer una limpieza de verdad, picaremos en todas las cajas. Por si no queda claro, esto no significa que vayamos a eliminar los programas sino solo los archivos ocultos que guardan esos programas por defecto. Antes de eliminar los archivos, el programa ofrece una lista de lo que va a desaparecer por si se cuela alguna cosa.

Al final de la lista, CCleaner nos da la opción de limpiar el espacio libre que queda en el disco duro. El proceso será más largo pero, si es la primera vez que hacemos una desintoxicación, lo mejor es decir que sí y relajarse. Cierra todos los programas que tengas abiertos y deja que empiece la diversión.

Otra opción para borrar archivos de manera permanente en Windows —aunque sin las habilidades del mayordomo de la tele— es File Shredder, en Fileshredder.org. Se instala como cualquier otro programa y empieza automáticamente cuando la abrimos. Una vez instalada, aparecerá como una de las opciones del sistema sin que tengamos que buscarla.

El procedimiento es rápido e indoloro (menos para el archivo a desaparecer). Seleccionamos el documento y pinchamos con el botón derecho del ratón para desplegar el menú. Allí elegimos Borrar de forma segura (*Secure delete files*). Después de pedirnos la confirmación, podemos decirle adiós al documento, que será borrado bit por bit hasta que solo quede un agujero humeante de tachones irreconocibles. La función Pro sobreescribe los archivos borrados hasta cincuenta veces.

Limpieza de datos en OS X

La táctica para deshacerse de datos en OS X es diferente y un poco más entretenida. Lo primero que tenemos que hacer es borrar los archivos de los que nos queremos librar. Después debemos borrar el espacio que tenemos libre, como si pasáramos la fregona por el suelo después de sacar la basura. Parece limpio pero, si viniera el mayordomo a hacernos la prueba del algodón, veríamos que no lo está. Para eso hay una aplicación especial que encontraremos en Aplicaciones > Utilidades > Disk Utility (utilidad del disco). Una vez abierta, seleccionamos nuestro disco duro y aplicamos Borrar espacio libre.

El programa nos dará tres opciones de borrado pero son bastante explícitas. La primera es *Todos los datos a cero*, que sobreescribe ceros sobre toda la superficie no indexada del disco. Es la opción menos segura pero la más rápida. Si estamos en un apuro y no tenemos tiempo, esta opción es mejor que nada.

Las siguientes dos opciones, *Borrado en siete pasos* y *Borrado en 35 pasos* sobreescriben siete y 35 veces el contenido del disco, pero no con ceros sino siguiendo patrones aleatorios diseñados para ofrecer el mayor número de combinaciones posibles, como el algoritmo de Gutmann. Si tenemos tiempo podemos elegir la más segura (35 pasos) y dejarla funcionando toda la noche.

Limpieza de datos en Linux

Extrañamente, casi no hay programas con interfaz gráfica de usuario (iconos y ventanitas) para eliminar archivos de manera segura en Linux salvo una especie de CCleaner para Linux llamado BleachBit. Si se me permite un pequeño inciso, la línea de comandos no es difícil. Para algunas personas es más fácil de manejar que los entornos gráficos (gente orientada a la escritura como yo) y ofrece un entorno más seguro y estable

que los pesados escritorios de ventanas con sus feos iconos y sus menús desplegables.

Para los que se atrevan con la consola, hay un potente programa llamado Wipe. Se puede instalar desde el administrador de software de nuestra distro favorita (yo uso y recomiendo LMDE) o directamente desde la consola, con el comando más simple del mundo: *sudo apt-get install wipe*. Pero como este es un libro para todos los públicos, vamos a buscar el camino fácil e instalar BleachBit.

Se instala como cualquier programa, descargando el software desde la página oficial, desde el Manager. Una vez instalado y abrimos BleachBit, podemos ir a Preferencias y marcar las dos primeras opciones: Ocultar limpiadores irrelevantes y Sobreescribir archivos para ocultar su contenido. La primera elimina información irrelevante, la segunda permite el proceso de sobreescritura que hemos descrito antes. En la siguiente pestaña (Unidades) seleccionamos los directorios que queremos sobreescribir.

La opción por defecto es la home y la carpeta de archivos temporales, pero podemos cambiarla a otra más localizada. En Idiomas debemos seleccionar los que nos sean pertinentes (por ejemplo: español, inglés y alemán) para que todos los documentos en otros idiomas sean eliminados por irrelevantes. Si no estamos seguros, es mejor no marcar nada antes que perder todas las extensiones de un idioma por accidente. La última pestaña es la Lista blanca, un lugar seguro donde debemos seleccionar aquellas carpetas que el programa no debe tocar. Todo lo que esté dentro de esas carpetas permanecerá como estaba.

Ya hemos configurado el programa. Antes de continuar, un pequeño detalle: el proceso de eliminación es irreversible. Por eso —y porque errar es humano— es buena idea guardar todos nuestros directorios importantes en un volumen cifrado antes de empezar, al menos hasta dominar el arte de limpiar sistemas, incluso si están en la Lista blanca.

BleachBit tiene muchas opciones. Si queremos limpiar todo el disco duro de restos indeseables, la ventana de inicio ofrece una lista con todos los programas que guardan datos, logs o historiales desde el caché, *cookies* e historial de Firefox a los logs de Skype o los documentos «rotos» que deja LibreOffice. Algunas opciones dan más miedo que otras, pero el programa explica cuál va a ser el procedimiento al seleccionar cualquiera de ellas.

Una vez seleccionados todos los archivos a eliminar, debemos pinchar en la lupa para obtener la lista de lo que va a desaparecer. Hay que mirarse bien esa lista, que no se nos escape nada verdaderamente importante por error. Cuando los hayamos borrado —y puede pasar un buen rato, sobre todo si era la primera vez— el programa nos presentará un informe con todo lo que ha eliminado. Veremos que algunas cosas de la lista están en rojo; esas no han sido borradas porque se necesita contraseña de administrador (superusuario) para hacerlo, bien porque están en directorios del sistema, bien porque están protegidas contra escritura. Para eliminar esas tendremos que repetir el proceso, pero abriendo el programa como administradores.

Una vez terminado este proceso haremos dos cosas. La primera es que tenemos una cantidad insospechada de espacio libre en el disco duro, que siempre es bueno. La segunda es que todas las cosas que nos hacían la vida más cómoda —recordar las contraseñas, adivinar las direcciones web, cargar las páginas rápidamente desde el caché— se han acabado. La vida del superagente secreto es dura, pero si hemos llegado hasta aquí es porque preferimos la seguridad a las comodidades mundanas del Panopticon.

Esto es como una limpieza en profundidad de la casa para asegurarse de que no hay agujeros bajo el sofá. Para eliminar uno o varios archivos de manera permanente, el proceso es Archivos Triturar archivos, seleccionar el archivo a eliminar y *bang!* Para eliminar directorios o carpetas enteros, seleccionamos Triturar carpetas y las carpetas a eliminar. En

ambos casos, el programa querrá saber si estamos seguros *seguros*. Si le decimos que sí, no volveremos a ver nunca al archivo comprometedor.

Problema: unidades de estado sólido (SSD)

Los usuarios de unidades de estado sólido SSD (en lugar de discos convencionales HDD) no encontrarán las opciones de borrado seguro de datos que acabamos de describir. Esto es porque se trata de tecnologías distintas. Los discos duros HDD funcionan un poco como un vinilo: la información se imprime sobre la superficie magnética del disco con ayuda de un cabezal. El almacenamiento de datos es sólido y por eso podemos eliminarlos escribiendo muchas veces encima de la misma superficie.

El sistema de memoria SSD es un entramado de semiconductores que almacenan los datos de forma completamente distinta, y la única manera de borrarlos es pasar la unidad por un pasapuré. Lo mismo pasa con los iPhones, iPads y memorias USB. Lo mejor es no meter datos comprometedores en esos dispositivos y limitarse a los discos convencionales.

Publicar sin ser visto

Los diez mandamientos del blogger anónimo

*E*l diablo está en los detalles: aunque la tecnología no es infalible, la mayor parte de los arrestos que se producen son resultado de un descuido y no de una operación de estrategia informática. Es por eso que los mandamientos que siguen no son solo una lista de soluciones técnicas para proteger nuestra identidad, sino sobre todo un código de conducta que debe convertirse en una segunda naturaleza si queremos mantenernos fuera del radar el mayor tiempo posible. Como es natural, cuanto más tiempo escribamos en el mismo blog, más probabilidades tenemos de que nos pillen.

1. Elegirás una plataforma de publicación apropiada: En los últimos años han surgido varias plataformas específicas para el usuario que busca anonimato, como Invisiblog, BlogACause o Anonyme.com. Lamentablemente, todos estos servicios han demostrado ser menos anónimos de lo que prometían (y menos duraderos; Invisiblog ya ha desaparecido). Además, sus Términos de usuario imponen conductas que no son especialmente compatibles con el ejercicio de la discreción, especialmente si están sujetos a la legislación norteamericana. De momento, los expertos aconsejan la fórmula WordPress + Tor + todas las precauciones que siguen.

2. Usarás el navegador apropiado: Esto es, uno que te permita anular el caché, eliminar el historial y deshabilitar el Java. No añadas extensiones que aumenten las posibles contingencias.

3. Abrirás una cuenta de correo anónima para registrar tu weblog. Y será una cuenta exclusiva, que no usarás para ninguna otra cosa. Tanto si usas Hushmail o RiseUp como si te haces una de usar y tirar como MintEmail o FilzMail, elegirás un nombre completamente ajeno, a ser posible realista, y una contraseña nueva.

4. Usarás Tor por encima de todas las cosas. Hay otros anonimizadores, pero solo Tor está aprobado —de hecho, diseñado— por la Electronic Frontier Foundation. Si eso no te convence, considera que si es lo bastante bueno para los servicios de inteligencia chinos y los narcotraficantes internacionales es bueno para ti. Si escribes desde ordenadores ajenos, como bibliotecas o cibercafés, lleva una copia del Tor Bundle Browser en un pincho USB y nunca te olvides de usarlo.

5. No registrarás nombres de dominio. O, si no queda más remedio, lo harás de manera anónima. Cada vez hay más servicios de registro de dominio que aceptan Bitcoin pero primero tienes que conseguir la divisa sin comprometer tu identidad. Por muy abanderados de la libertad que suenen, toma las mismas precauciones para registrarte —nombre, e-mail, contraseña nuevos, Tor, etc.

6. Elegirás un nombre apropiado. Ni el apodo que tenías de pequeña ni la combinación de las iniciales de tus hijos ni el nombre de tu personaje favorito. Si no se te ocurre un nombre lo suficientemente neutro, un generador de nombres como

fakenamegenerator.com te proporcionará una identidad completa, incluyendo grupo sanguíneo y profesión. No olvides usar Tor para generar tu próximo álter ego; estos servicios también guardan sus logs.

7. No usarás Google Analytics para contar tus visitas. Si has seguido nuestro primer consejo, no hace falta preocuparte porque no es compatible con Word Press, pero si estás usando Tumblr, Typepad o Blogger, debes saber que el contador de Google los pondrá todos juntos en su registro administrativo. Si tienes más de un blog, una búsqueda revelará que tu blog secreto y tu blog público están escritos por la misma persona.

8. No te delatarás. Contra todo pronóstico, cuando se identifica a un blogger anónimo es el propio blogger el que revela su identidad, con detalles sobre su localización, comentarios acerca de sus allegados o pequeñas píldoras sobre su vida privada, etc. Y sobre todo, no presumas ni te metas en peleas ni aceptes entrevistas ni mandes a amigos a recoger premios. Aunque ganes el juicio como hizo el policía bloguero británico NightJack contra el *Times*, tu tapadera habrá volado para siempre.

9. No serás tú mismo. En la era del Big Data, el estilo es un rasgo igual de distintivo que las huellas digitales. Si has dejado el tuyo diseminado por la Red en forma de blogs, comentarios, discusiones en foros y monólogos en el muro del Facebook, tienes que tomar medidas.

10. Conocerás la legislación. Si insultas a una modelo (*Skanks of NYC*), robas dinero a los ricos para dar a los «pobres» (Jeremy Hammond) o consigues que una empresa, individuo o institución te lleven a juicio, los grandes poderes fácticos de la Red estarán obligados a desvelar todo lo que saben de ti. No te metas en líos que no sean estrictamente necesarios para tu proyecto.

Una solución de bolsillo: Tails

*C*omo hemos visto, la vida online implica muchas vulnerabilidades pero también ofrece muchas soluciones. Hasta ahora hemos hablado de proteger nuestras cuentas con mejores contraseñas, de combinar estrategias de conexión para que no se intercepten nuestros paquetes de datos, se registren nuestros movimientos ni se conozca nuestra identidad (SSL, VPN, Tor). Hemos aprendido a mandar correos cifrados con criptografía de clave pública (PGP) y a proteger documentos y directorios en una caja de seguridad virtual (TrueCrypt). Todas esas tecnologías están sujetas a los principios del software libre y están disponibles en la Red para ser descargadas, compartidas, distribuidas y modificadas a placer. Pero, aquellos que buscan una solución completa para asegurarse de que no queda ningún agujero por donde se filtren sus actividades, pueden concentrar todas las tecnologías en un sistema operativo diseñado específicamente para eso, una adaptación de Debian GNU/Linux llamado Tails.

Tails (The Amnesic Incognito Life System) es lo que se llama una distribución *live*, también llamada Live CD. Esto significa que está hecho para funcionar desde un medio de almacenamiento externo (DVD, memoria USB o tarjeta SD) y que funciona independientemente del sistema operativo del ordenador en el que lo queramos usar. En otras palabras: cuando conectamos la memoria USB al equipo o metemos el DVD en la disquetera y reiniciamos el ordenador, el ordenador ejecutará la distribución Live —en este caso, Tails— en lugar del sistema operativo original que tenga instalado en el disco duro, pero ofreciendo acceso al contenido de sus directorios.

Este sistema operativo de bolsillo resulta extraordinariamente conveniente para conectarse a ordenadores extraños sin tener que preocuparse por nada, o para convertir nuestro ordenador habitual en una fortaleza inexpugnable para gestionar actividades específicas (por ejemplo, para publicar un blog anónimo o comunicarnos con una fuente delicada). Es polifacético y multipropósito, cabe en un dispositivo del tamaño de un dedal y permite usar cualquier terminal del mundo como si estuviéramos en casa. Solo necesitamos una memoria USB con un mínimo de 4GB y un ordenador con un mínimo de 1GB de memoria RAM.

El sistema trae todos los programas habituales en una distro moderna, incluyendo navegador (Firefox), procesador de textos (Libreoffice), cliente de correo (Claws), mensajería (Pidgin), editores de imagen y sonido, etc. Pero, como está diseñado con la seguridad como principio integral del sistema, todas las aplicaciones que ofrecen vulnerabilidades han sido eliminadas, y todas las herramientas que ofrecen protección al usuario han sido instaladas por defecto.

Todavía más importante: en Tails, todas las comunicaciones en todos los programas están cifradas con HTTPS y solo pueden tener lugar a través de Tor. Si una aplicación trata de conectarse a la Red sin pasar por Tor, el sistema está diseñado para bloquear el acceso. Utiliza un sistema de cifrado llamado Luks para cifrar otros discos duros externos o memorias USB, trae OpenPGP para cifrar nuestros correos y un cliente de correo llamado Claws (garras). También incluye OTR para proteger las conversaciones de mensajería instantánea y hasta una trituradora de documentos llamada Nautilus Wipe.

Como todo funciona desde la tarjeta de memoria flash o el pincho USB, Tails solo usa memoria de proceso durante su actividad (esto es, no toca el disco duro del ordenador ni su memoria Swap). Es como si el ordenador tuviera un sueño del que solo puede ser

consciente mientras está ocurriendo, pero del que lo olvida todo al despertar. Una vez desmontamos la memoria del ordenador y lo reiniciamos de nuevo, el equipo volverá a su sistema operativo habitual como si nada hubiera sucedido, sin que quede rastro de la operación anterior. Por eso lo llaman «amnésico».

Descargar e instalar Tails

La manera más fácil de instalar Tails es usando otro Tails. El sistema tiene su propio instalador, de modo que, si tenemos una copia del sistema en un DVD o memoria USB, solo necesitamos otra memoria USB con 4GB. Cuando abrimos Tails, el menú de Aplicaciones > Tails > Tails installer y ofrece la opción de Clonar e Instalar. Conectamos la memoria USB que queremos usar como lanzadera del nuevo Tails y esperamos a que aparezca en la lista de receptores posibles (Target Device). Si no aparece o no estamos seguros, es mejor empezar de nuevo que arriesgarse. Una vez localizada, pinchamos en Instalar Tails y confirmamos la operación. Y ¡ya hemos duplicado el sistema en una nueva llave! Instalar Tails a mano es bastante más complejo y pesado, aunque no imposible.

Si ya tenemos la memoria USB y el ordenador preparados, lo primero es ir a la página de Tails: Tails.boum.org y pinchar en el enlace de descarga. Lamentablemente, todavía no hay una página en castellano (si quieres y puedes traducirla, ¡pincha en Contribute! El mundo será un lugar mejor gracias a ti) pero la página tiene instrucciones detalladas para principiantes.

1. Descarga la imagen ISO: La imagen ISO es una imagen exacta de un sistema de ficheros que se rige por el estándar ISO 9660, y la fórmula más corriente de almacenamiento para sistemas operativos GNU/Linux. Bajársela no tiene pérdida: pinchamos en el icono verde y elegimos —esto es al gusto— descarga directa o torrent. Nos descargará un archivo .iso (la última versión de Tails a la hora de cerrar el libro es Tails-i386-0.23.iso) que depositaremos en el escritorio.

2. Comprobar la firma digital: Como en el caso de las claves, este proceso no es estrictamente necesario para tener Tails (nos lo podemos saltar) pero es la única manera de comprobar que nos estamos descargando la imagen ISO genuina y no nos han dado el cambiazo. Para eso debemos descargar la firma digital de Tails, que esta justo debajo del botón para descargar la iso.

Para importar la clave a nuestro sistema hay que usar el terminal y el siguiente comando:

cat Tails-signing.key | gpg —keyid-format long –import

Y, para verificarla, este (usando el nombre de nuestra versión, que puede no ser la del ejemplo)

gpg —keyid-format long —verify Tails-i386-0.23.iso.pgp Tails-i3860.23.iso

Si el resultado no incluye la frase «Firma Correcta de Tails Developers (signing key)» puede ser porque a) no hemos escrito bien los comandos, b) no hemos descargado la clave apropiada (están una encima de otra, la imagen ISO y la firma) o c) nos han dado gato por liebre. El 98% de las veces será una de las dos primeras. Si está todo correcto y persiste

el error, es mejor copiar la imagen de alguien de confianza.

3. Instala Tails: Hay muchas maneras de hacerlo. La página oficial de Tails ofrece varias opciones, incluyendo la instalación sobre DVD, memorias USB y tarjetas de memoria SD. También hay numerosos tutoriales en la Red, incluyendo varios en YouTube que podemos seguir paso a paso para los principales sistemas operativos.

Si no conocemos a nadie que tenga ya el sistema (no importa si es algo más antiguo, una vez tenemos la instalación hecha es fácil actualizar), la segunda mejor opción es descargar un programa específico para crear un Live USB, un instalador universal USB que nos haga el trabajo sucio. Cada uno tiene sus instrucciones y hay varios que incluso traen Tails entre sus opciones preconfiguradas. Siempre que podamos, debemos usar la más fresca del repositorio oficial.

La opción manual es la más complicada y, salvo que sepamos bien lo que hacemos, también es la más peligrosa. Cualquiera que sea el camino que decidamos seguir, hay que prestar MUCHA atención a los pasos, ir MUY despacio y tener MUCHO cuidado. En un descuido podemos perder todo el contenido del disco duro.

4. ¡Empezar a usar Tails!: Antes que nada: para que funcione, nuestro ordenador tiene que tener activada desde la BIOS la opción de cargar el sistema desde una memoria externa. Si nuestro Live USB no funciona —pero hemos comprobado que sí funciona en otros ordenadores— entonces tenemos que entrar en la BIOS y modificar sus opciones de arranque.

Una vez esté en marcha, es importante recordar que Tails está basado en Tor y que hereda todas sus limitaciones: tus «espías» sabrán que estás usando Tor y el último nodo escupirá los paquetes de datos sin protección. Más vale que estén cifrados. Tor tampoco mejora la calidad de nuestras contraseñas ni nos protege de los ataques Man-in-the-middle. Lo mejor es usarlo en combinación con una VPN o Red Privada Virtual. El tráfico será lento pero mucho más seguro.

El sistema ofrece la opción de crear un directorio para almacenar documentos dentro de la misma memoria USB. Aunque apetitosa, no es una opción aconsejable: es mejor llevar los documentos por separado, siempre protegidos con un abrigo cifrado y, a ser posible, un fondo falso. Si no saben de qué estoy hablando es que no se han leído el capítulo correspondiente al cifrado de documentos.

Finalmente, lo más importante: la carrera contra los bugs es constante y acelerada, y cada nueva versión de Tails es más segura que la anterior. Es importante mantener nuestros programas actualizados y no instalar aplicaciones que no sean innatas al sistema. No sabemos dónde han estado ni quién puede estar detrás.