Seguridad de la Información para Periodistas

Protege tu notícia, a tu fuente y a ti mismo online

Por Silkie Carlo y Arjen Kanmhuis

Nota Importante Por favor, revisa las actualizaciones de las herramientas en www.tcij.org

El Centre for Investigative Journalism ha publicado esta serie de manuales con el generoso apoyo de la Rava and David Logan Foundation

La edición en español y su distribución se ha realizado con la colaboracón de Xnet

Seguridad de la Información para Periodistas

Protege tu noticia, a tu fuente y a ti mismo online.

Este manual es una herramienta práctica muy útil para los periodistas y especialmente para los periodistas de investigación. Por primera vez, los periodistas ahora son conscientes de que prácticamente cada comunicación electrónica que hacemos o recibimos está siendo grabada, guardada y sujeta a análisis y control. Como esta vigilancia se lleva en secreto, sin control, transparencia o cualquier posibilidad realista de exigir responsabilidades, nuestras fuentes, nuestras noticias y nuestro mismo trabajo profesional están bajo amenaza.

Después de que se conocieran las revelaciones de Snowden, sabemos que existen maneras para protegerse así como contra medidas. El último manual del CIJ, (The Center for Investigative Journalism, Centro de Periodismo de Investigación), ***Information Security For Journalists*** (Seguridad de la Información para Periodistas), presenta las formas más efectivas de mantener tu trabajo confidencial y a salvo del espionaje. Explica cómo escribir de forma segura, cómo pensar en la seguridad y cómo recibir, guardar y enviar de forma segura esa información que un gobierno o una corporación poderosa puedan querer que no conozcas, poseas o compartas. Para proteger tu privacidad y la seguridad de tus fuentes, ***Seguridad de la Información para Periodistas*** te ayudará a hacer que tus comunicaciones sean anónimas, indescifrables y no rastreables.

A pesar de que este manual es en gran parte sobre cómo usar tu ordenador, no necesitas tener un título en informática para utilizarlo. Sus autores y los expertos que los asesoraron en este proyecto trabajan con la tecnología más avanzada y se aseguran de que este manual sea preciso y práctico.

Gavin MacFadyen, Director del Centre for Investigative Journalism

Comisionado por el Centre for Investigative Journalism.

La edición en español y su distribución se ha realizado con la colaboracón de Xnet

Por Silkie Carlo

y

Arjen Kamphuis

Agradecimientos

Me gustaría expresar mi profunda gratitud a Arjen Kamphuis por su verdaderamente magnífica, paciente y generosa enseñanza, por su excelente trabajo y por su amistad.

Muchas gracias a Gavin MacFadyen y al CIJ por encargarnos y confiarnos la responsabilidad de escribir este manual cuyo objetivo es proteger a sus periodistas y sus fuentes, y por su defensa a la seguridad de la información en general.

Queremos darles conjuntamente las gracias a los denunciantes y a los hacktivistas, pero sobre todo a Edward Snowden, por democratizar la información de la que ahora nos valemos para defendernos y para proteger nuestras fuentes y la libertad de prensa.

Con solidaridad y gratitud hacia los periodistas que tengan la intención de usar este manual.

Silkie Carlo

Gracias a los héroes de la Free Software Foundation (Fundación de Software Libre) que hace 30 años anticiparon los problemas con los que ahora nos enfrentamos y tomaron las medidas necesarias para que tuviéramos alternativas.

Gracias a los programadores y a los hackers que comparten gratuitamente su trabajo con toda la humanidad.

Gracias a Gavin, Juliet y Minal del CIJ por su gran trabajo en apoyo al periodismo (lo que incluye su apoyo a la creación de este libro).

Gracias a los denunciantes por su coraje y sacrificio.
Y gracias a Silkie Carlo, co-autora de este trabajo, por su curiosidad, su motivación, su elegancia ante los ataques y su capacidad de dar siempre lo mejor de sí misma.

Les dedico este libro a mis padres, Ida & Andre Kamphuis, quienes me educaron a defender mis principios y nunca cedieron frente a aquellas autoridades que trataron de destruirlos.
Arjen Kamphuis

Arjen Kamphuis

Índice

Prefacio – Arjen

En los últimos 12 meses todos los miedos más extremadamente paranoicos de los activistas de la privacidad y los expertos en seguridad de la información han resultado ser problemitas inocentes en comparación con la realidad del espionaje industrializado en el planeta entero. Cualquier periodista que se haya mantenido al tanto de las continuas revelaciones y que desee proteger sus fuentes y sus historias de los husmeadores del gobierno puede haberse sentido desalentado. ¿Es que todo lo que tiene un chip y una batería nos está continuamente espiando? Si consideramos la mayoría de los aparatos portátiles como ordenadores móviles, tabletas y teléfonos inteligentes, la situación es realmente difícil. Pero hay medidas que puedes tomar y que no son caras ni requieren un doctorado en informática. Usar un sistema informático que ceda solo frente a los ataques más avanzados a nivel nacional, está al alcance de cualquiera.

Es decir, de cualquiera que esté dispuesto a pasar unos días aprendiendo a usar este software gratuito y el hardware que ya tengas a tu disposición, o que se puede comprar por menos de 270 euros. Este manual puede empezar a darte los conocimientos para brindarle seguridad a tu información y comunicación, y a la de tus fuentes; a usar herramientas y métodos que expertos de todo el mundo han demostrado que funcionan en algunas de las situaciones más extremas.

Dependiendo de las habilidades que ya tengas con los ordenadores, esta puede resultar una experiencia de aprendizaje algo difícil, pero ten por seguro que muchos otros antes que tú, y que tampoco se consideraban expertos, lograron sentirse cómodos con los conceptos y herramientas descritos en este libro.

Si eres un periodista del siglo XXI, necesitas estas herramientas. Después de todos, William Randolph Hearst dijo hace décadas: “periodismo es escribir lo que las personas poderosas y las instituciones no quieren que se escriba”.

Si no te consideras un periodista, pero quieres que se reconozca tu derecho a la privacidad garantizado por el Artículo 12 de la Declaración de los Derechos Humanos de la ONU, [1948], entonces este libro también es para ti.

Como casi todos los que han creado algo, solo podremos hacerlo apoyándonos en las mil generaciones que nos han precedido. Por eso, este libro siempre será accesible en varios formatos electrónicos sin restricciones, gratuitamente. Si falta el formato que te se sirve, háznoslo saber.

Si aprecias este trabajo, por favor trata de difundirlo lo más posible y ayúdanos a mejorar la próxima versión. Todo tipo de comentario constructivo es más que bienvenido. El problema continuará desarrollándose y nuestra respuesta también. Por favor contribuye compartiendo estos conocimientos y promoviendo estas herramientas en cualquier forma en que puedas hacerlo.

Arjen Kamphuis, Berlin 2014

Prefacio – Silkie

Cuatro semanas antes de que Edward Snowden denunciara las extraordinarias capacidades de vigilancia, yo era bastante analfabeta en informática, formada con Microsoft e incapaz de hacer tareas básicas en un Mac. Estaba a punto de embarcarme en una campaña y proyecto de investigación, y bastante paranoica, creé mi primera cuenta de correo electrónico encriptada gracias a una larga explicación que Arjen me dio por teléfono. Como en muchas curvas de aprendizaje, al principio la tecnología me parecía abrumadora. Peor aún, solo unas pocas personas con las que yo me comunicaba usaban encriptaciones.

Las cosas cambiaron muy rápidamente.

El 5 de Junio de 2013, el periódico the Guardian publicó las revelaciones de Snowden sobre el programa PRISM. Me di cuenta, junto con el resto del mundo, de que nuestra pesadilla orwelliana era ahora una realidad. Solo que la realidad era mucho más opaca, escalofriante y sombría que la pesadilla que leímos en la ficción. De hecho, la pesadilla se fue desarrollando en episodios aparentemente banales hasta convertirse en una realidad de la que ya no nos podemos despertar. Lo más importante de esta realidad es que realmente la capacidad y la responsabilidad de actuar. Gracias a Snowden sabemos ahora lo crítico que es este episodio, y estamos facultados con la información y la oportunidad de actuar.

Si periodismo es publicar lo que otros no quieren que sea divulgado, y para los periodistas de investigación sin duda es así, debes asumir que mientras produces tu mejor trabajo, tienes un adversario del que debes proteger tu reportaje, tus fuentes y a ti mismo.

Desde el 5 de junio de 2013, me pareció importante formarme en los métodos de seguridad de la información que protegen la libertad de expresión y la libertad de prensa, métodos simples que son absolutamente esenciales para preservar e impulsar la libertad y la democracia, y esenciales para proteger a los individuos que se encargan de hacerlo. Como completa novata en informática, sin ninguna habilidad natural, soy la prueba de que cualquiera capaz de entender la importancia de la seguridad de la información y que tenga la paciencia de aprender, se puede volver un usuario avanzado de los métodos de ‘InfoSec’ (Seguridad de Información) en cuestión de meses.

Este manual es el producto de un año de aprendizaje de una novata (yo misma) bajo la guía y las enseñanzas de un experto (Arjen), y está escrito en los términos más simples posibles, con instrucciones comprensibles, para compartir con ustedes un método rápido para este proceso de aprendizaje, que no comprometa el conocimiento, la enseñanza o la seguridad. La mejor forma de aprender es haciendo – así que sugiero firmemente que uses este manual mientras vas coleccionando las herramientas para InfoSec, y sigas las instrucciones conforme vayas avanzando.

Sobre todo espero que este manual le dé fuerza a una amplia gama de periodistas de

investigación y en especial a sus fuentes – inclusive a los que están expuestos al nivel más alto de riesgo. Por lo tanto, parte de la información aquí contenida es apta para un ‘escenario Snowden’, y estoy bastante segura de que hay muchas posibles fuentes allá afuera cuya información merece un grado similar de seguridad.
Si este manual consigue que una víctima de la injusticia o un testigo de actos criminales se alivien del peso de su historia; si consigue que un individuo pueda comunicar con el mundo y hacer oír su voz sin peligro, entonces este manual habrá servido muy bien a su propósito.

Silkie Carlo, Londres 2014

Introducción

Imagina que abres tu bandeja de entrada y te encuentras con un email anónimo de alguien que te ofrece compartir documentos sensibles y de importancia internacional. La fuente, y la información, requieren el nivel más alto de protección. ¿Qué haces?

Este manual está diseñado para instruir a periodistas y organizaciones de medios de comunicación sobre cómo ejercer la seguridad de información en la era digital y proteger tu trabajo, tus fuentes y tus comunicaciones en una variedad de niveles de riesgo.

Seguridad de información o “InfoSec”, es la práctica de proteger la información de accesos no autorizados. La información en riesgo puede incluir un reportaje en el que trabajas y los archivos relacionados, la identidad de tu fuente(s), tu comunicación con ellas y, a veces, tu propia identidad.
No necesitas ser un experto en informática para practicar InfoSec (¡Aunque sin duda vas a aprender mucho mientras vayas avanzando!). Usando este manual podrás aprender en cuestión de días a enviar correos y documentos encriptados desde tu segurísimo ordenador portátil.

Las Amenazas: ¿Quién plantea una amenaza?

Amenazas específicamente dirigidas
Las revelaciones de Snowden revelaron la extraordinaria capacidad de algunas agencias gubernamentales de inteligencia de interceptar comunicaciones, y de lograr acceso no autorizado a datos en casi todos los ordenadores personales o aparatos electrónicos de comunicación en el mundo. Esto podría suponer un riesgo en la seguridad de la información para un periodista de investigación, que trabaja en reportajes centrados en algún interés de estos gobiernos, sus agencias y sus contratistas privados en materia de inteligencia.

Muchos estados carecen de estas tecnologías sofisticadas de vigilancia – pero todos los estados poseen capacidades de vigilancia, algunas de las cuales pueden ser usadas, como ha sucedido algunas veces, en contra de periodistas, con consecuencias potencialmente graves. Se piensa que Etiopía, un estado menos avanzado tecnológicamente, haya lanzado ataques remotos contra periodistas en oficinas dentro de los Estados Unidos.

En la era globalizada, algunas corporaciones transnacionales tienen más riqueza y poder que muchos estados soberanos. De la misma manera, algunas corporaciones transnacionales poseen mayores capacidades de ‘seguridad’ o de vigilancia que muchas naciones soberanas.

Y no solo las corporaciones; también se sabe que sofisticadas organizaciones criminales

han usado tecnologías de vigilancia, y algunas organizaciones delictivas pueden superponerse con elementos criminales en el gobierno. El Ejército Mexicano gastó 350 millones de dólares en herramientas de vigilancia entre 2011-2012, y según informes ahora posee la tecnología para recoger mensajes de texto, llamadas telefónicas y correos; para activar de forma remota grabaciones de teléfonos móviles; y hasta para detectar movimientos a través de las paredes, usando tecnología radar. Asimismo, entre el 2011 y el 2012, nueve periodistas fueron asesinados en México por motivos relacionados con su trabajo.

El acceso no autorizado a tu información puede implicar su uso, divulgación, distorsión, modificación, inspección, grabación o destrucción. Tú y tu fuente podríais estar expuestos a riesgos jurídicos o físicos, y la información a la base de tu reportaje podría verse comprometida. En situaciones de alto riesgo, InfoSec puede tan importante como usar un chaleco antibalas y viajar con guardaespaldas; sin embargo, puesto que las amenazas digitales son invisibles, complejas y a menudo no detectables, es posible subestimarlas o pasarlas por alto.

Amenazas de emboscada
Puede que también quieras protegerte de los programas de vigilancia ‘por emboscada’, encabezados por la Agencia de Seguridad Nacional de EEUU (NSA) y el Cuartel General de Comunicaciones Gubernamentales del Reino Unido (GCHQ).

Se trata de programas que filtran y recogen en todo el mundo los datos de la red y las telecomunicaciones permitiendo, potencialmente, investigaciones retroactivas. Si, por ejemplo, por dar informaciones sobre actividades estatales secretas o controvertidas, te volvieras una persona de interés para el gobierno, sería posible recopilar un registro de tu actividad diaria yendo varios años atrás.

Practicar InfoSec

Como todo buen periodista, a lo largo de tu carrera vas a revolver algunos avisperos. Por lo tanto, una buena práctica de InfoSec equivale a normalizar varias estrategias de forma permanente, para que encajen fácilmente con tu trabajo diario. También quiere decir emplear diferentes estrategias de protección caso por caso, ya que cuando trabajes con casos sensibles y fuentes vulnerables tendrás que usar métodos de InfoSec más sólidos y que requieran más esfuerzos.

El primer paso hacia una buena práctica de InfoSec consiste en ser consciente de las amenazas; el segundo es ser consciente de la las vulnerabilidades de tu hardware y software. Entender cómo y por qué se verifica un acceso no autorizado es el primer paso para aprender a protegerte de él.

Cuestiones jurídicas
A pesar del hecho de que la continua vigilancia de ciudadanos respetuosos de la ley casi seguramente contraviene las leyes internacionales sobre los derechos humanos, el uso de algunos instrumentos para proteger la privacidad pueden ser ilegales.

Varios de los instrumentos de privacidad mencionados en este manual son instrumentos

criptográficos. La criptografía puede ser ilegal o requerir una licencia en diversos países, entre ellos China, Cuba, Irán, Libia, Malasia, Corea del Norte, Singapur, Sudán y Siria, puede ser ilegal o requerir una licencia Cuando entres a algunos de estos países, puede ser que tengas que declarar cualquier tecnología de encriptación que lleves en tu laptop. Deberías tener en cuenta las consecuencias legales de usar criptografía y tomar decisiones informadas sobre dónde y cuándo es seguro usarla. Puedes averiguar más sobre las leyes de criptografía en cada país aquí: http://www.cryptolaw.org

Modelar las amenazas

En este manual hay mucha información sobre varios tipos de amenazas posibles y sobre las medidas que se pueden tomar para defenderse de ellas. Sin embargo, como las tecnologías de ataque están en constante cambio y buena parte de su uso es totalmente secreto, raramente podemos decir con confianza cuáles son las amenazas exactas; cuándo y dónde se producen y a quién afectan; o la eficacia de nuestras defensas.

Por lo tanto, es tu responsabilidad evaluar personalmente los riesgos y diseñar, en el transcurso de la lectura de este libro, una respuesta defensiva apropiada . Quizás quieras también considerar los factores prácticos – algunos usuarios pueden comprometer su InfoSec, conscientes del riesgo, por otras exigencias prácticas de su trabajo, al tiempo que otros usuarios usan niveles de InfoSec sofisticados y superiores a sus necesidades sencillamente porque lo encuentran prácticamente factible.

Algunas preguntas básicas que quizás quieras preguntarte cuando modelas tus estrategias de InfoSec:

1. ¿Quiénes podrían ser tus adversarios o potenciales atacantes?
2. ¿Qué herramientas pueden poseer tus atacantes?
3. ¿Qué probabilidades hay de que tu atacante use las herramientas a su alcance en contra tuya?
4. ¿Qué riesgos podrían surgir, para ti y para aquellos con los que te comunicas/trabajas, en el caso de un ataque dirigido?
5. ¿Qué riesgos surgen de la vigilancia pasiva? ¿Hasta qué punto se extienden las herramientas usadas en la vigilancia pasiva?
6. ¿Qué estrategias de defensa son prácticas, seguras y eficaces a la luz del riesgo que calculas puedas tener?
7. ¿ Qué estrategias de defensa son prácticas, seguras y eficaces y pueden ser enseñadas a tus fuentes y a tus colegas, considerando el riesgo, evaluado u ocurrido, para ellos y para vuestras comunicaciones ?

Las amenazas cambiarán con el tiempo – pero también lo harán las tecnologías disponibles para proteger a los periodistas y a los ciudadanos. Así, es importante entender la teoría de InfoSec en la teoría, y estar siempre aprendiendo sobre su práctica.

Capítulo 1: Proteger el Sistema

Tu seguridad y/o métodos de encriptación serán eficaces si cada nivel de tu sistema es seguro. Puedes mandar tus correos con encriptación indescifrable o usar las contraseñas más fuertes que se puedan imaginar, pero si tu sistema es 'interceptado', 'hackeado' o vulnerable, tus esfuerzos pueden ser inútiles, ya que tu encriptación puede ser burlada sin necesidad de decodificarla.

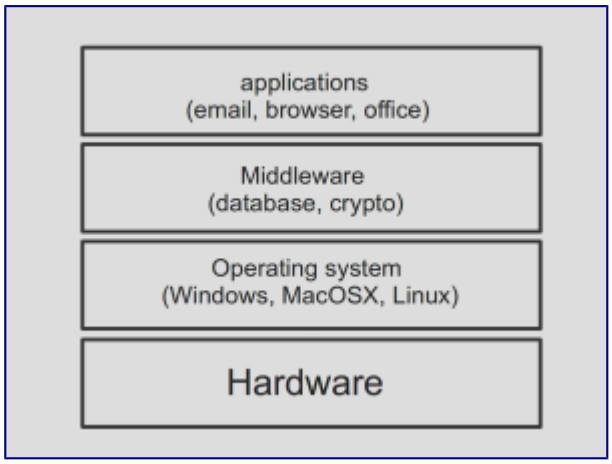
Según tu nivel de riesgo o la sofisticación de tu adversario, las estrategias de protección pueden variar desde tan solo tener tu teléfono u ordenador portátil contigo en todo momento, a usar ordenadores de segunda mano, comprados con dinero en efectivo y practicar medidas InfoSec más fuertes durante un proyecto específico.

Piensa en 'proteger tu sistema' como en construir un castillo de naipes: para que funcione, debes construir tu seguridad de abajo hacia arriba.
En este capítulo, aprenderás cómo poner los cimientos de un sistema seguro y gestionar la seguridad de tu hardware y firmware.

Este capítulo es el más importante del libro. También es bastante técnico y contiene la información más compleja de todo el libro. Las soluciones que se dan son muchas, pero la seguridad máxima es el resultado final de sólo una de ellas. Aquí, exponemos la horrible realidad de la enorme vulnerabilidad del hardware, y dejamos que tú decidas cuál es la medida de seguridad más apropiada para ti. Para varias de las soluciones descritas aquí (como las modificaciones especializadas del hardware y el reemplazo del firmware) necesitarás la ayuda de expertos.

Por más largo y técnico que sea este capítulo, ¡por favor sigue leyendo! Deberías de estar informado sobre las vulnerabilidades dentro de tu sistema, aún si en este momento no tienes la habilidad o la necesidad de resolverlas. Esta es información importante que fortalecerá tu confianza en tu sistema y en su uso, y que te preparará para las más simples futuras soluciones que esperamos sean desarrolladas pronto.

Arquitectura básica de un ordenador



Interfaz – pantalla
Aplicaciones – tu software/programas
Middleware – programación que conecta y permite el intercambio de información entre dos programas separados y a menudo, ya existentes: p.ej. permite que los programas acceder a las bases de datos
Sistema Operativo – Windows XP/7/8/10, Mac OS X, Linux, etc.
Firmware – software fundamental programado en el hardware que proporciona instrucciones para que un dispositivo comunique con el resto del hardware del ordenador
Hardware – los elementos físicos que componen un sistema informático

En este capítulo, vamos a considerar principalmente la seguridad al nivel básico: hardware y firmware.

Hardware y firmware
'Hardware' se refiere a tu máquina física. Los ordenadores de escritorio, 'desktop', no son recomendables para un trabajo periodístico importante, ya que son fijos y por lo tanto no sólo son poco prácticos, sino también vulnerables a ataques físicos cuando tú no estás allí. Aquí vamos a hablar de los laptops, u ordenadores portátiles.

Para nuestros fines, 'laptop' se refiere a todos los componentes físicos, incluyendo la batería, el disco duro, el lector de CD, la tarjeta Wi-Fi, el micrófono y la webcam. Consideramos también hardware adicional cualquier teclado, ratón, escáner/impresora, webcam, etc. que conectes a tu laptop.

Las amenazas al hardware pueden ser:

- Robo o daño
- Ataque físico
- Ataque virtual/remoto

Los riesgos principales a tu hardware son que este sea hurtado, dañado, físicamente interceptado o alterado; o que se acceda a él de manera virtual/remota para transmitir señales (esto es recoger y entregar información).

Hay cinco medidas claves que son importantes para la protección del hardware:
> Prevenir ataques virtuales y físicos en tu hardware:

1. Comprar el laptop correcto
2. Modificar tu hardware

   > Prevenir ataques físicos en tu hardware:

3. Comprar tu laptop anónimamente
4. Vigilar tu laptop
5. Medidas de detección (por si llegas a separarte de tu/s laptop/s)

Aunque estos cinco pasos al principio pueden sonar confusos y hasta abrumadores, todos ellos pueden ser practicados por periodistas novatos en informática y en InfoSec. Cómo conseguir tener un hardware seguro y cómo mantenerlo así se explicará en este capítulo, todo lo que tienes que hacer es escoger el nivel de riesgo para el que quieres prepararte y seguir los pasos apropiados.

1. Comprar el laptop correcto

Qué laptop compres va a determinar el nivel de seguridad que podrás lograr. Gracias a los documentos de Snowden, a medida que aprendemos más sobre las capacidades extensivas de vigilancia, también aprendemos cuáles máquinas pueden hacerse seguras y cuáles no. Esperamos que, con el tiempo, se puedan desarrollar soluciones más

seguras. Sin embargo, por el momento, muy pocos laptops se pueden convertir en completamente seguros contra las amenazas más grandes.

Esto tal vez no sea un problema para tí o para tu fuente, según quién sea tu adversario. Si defiendes tus comunicaciones y datos de gobiernos poderosos o de sus aliados (lo que en términos prácticos puede incluir bancos y corporaciones importantes), necesitarás una seguridad excelente para tu/s laptop/s. Por otro lado, si te defiendes de corporaciones, grupos políticos, militares, terroristas o rebeldes, agencias de seguridad privadas o individuos específicos, tendrás que estimar lo sofisticadas que son sus herramientas; lo fácil que sería usar esas herramientas en tu contra; lo importante que puedas ser como blanco; y por consiguiente, qué medidas deseas tomar.

Cuando compras un laptop, son cuatro los problemas a considerar que determinan si tu sistema se puede hacer seguro.

Mantenimiento del hardware

Podrías pensar en un laptop que te deje levantar la cubierta y entrar dentro de la máquina, para que puedas hacer 'mantenimiento' básico del hardware, y escoger qué componentes dejar o deshabilitar.

Muchos laptops IBM/Lenovo, HP, y Dell son aptos para esto, y proporcionan documentación extensiva del hardware en sus sitios web que ayudan en la modificación DIY (Hágalo Usted Mismo) del hardware[1].

No puedes fácilmente abrir la cubierta de los MacBooks – esto requiere cierta pericia y aun así, hacer tu propio mantenimiento de hardware en un MacBook puede invalidar la garantía.

[1] Esta flexibilidad de hardware y la documentación está disponible también para otras marcas – las sugerencias anteriores no son promociones de estas marcas o de sus productos.

Firmware

Firmware es el software programado en el hardware de tu laptop a un nivel profundo y básico. En términos elementales, el firmware imparte instrucciones a las partes de tu laptop sobre cómo comunicar entre sí. El firmware es otro posible blanco de ataque, ya que hackers muy sofisticados (probablemente a nivel de estado) pueden ser capaces de acceder remotamente y lograr control privilegiado sobre tu máquina. Por ejemplo, podrían implantar malware para eludir tu codificación.

En un MacBook puedes bloquear tu firmware, haciéndolo accesible solo por medio de una contraseña que tu estableces. La posibilidad de cerrar el firmware en un Mac proporciona una ventaja de seguridad concreta sobre otros laptops, de los cuales sólo un número limitado de modelos pueden ser asegurados mediante la tarea especializada y muy técnica de reemplazar el firmware de código cerrado (donde el código fuente es de propiedad privada e inaccesible al público o verificable) con firmware de código abierto (llamado 'coreboot', que es gratuito para todos y cuyo código fuente está disponible al

público y verificable). Por supuesto, la confianza en la seguridad que provee el bloqueo del MacBook depende de la confianza que se tenga en Apple. Sin embargo, no tiene vulnerabilidades conocidas hasta ahora, y usar el bloqueo debería por lo menos dificultar un hackeo sofisticado.

El bloqueo del firmware en Mac:

Esta es una función de Mac tan fácil de usar y que proporciona una defensa tan considerable contra hacks de firmware que los usuarios de Mac, expuestos a distintos niveles de riesgo, quizá deseen usarla.

Para establecer una cerradura en tu Mac (OS X), inicia la máquina, manteniendo pulsadas las teclas ‘cmd’ y ‘R’ mientras se inicia entrando en modo de Recuperación. En la barra de menú de arriba, ve a ‘Utilities’ (Utilidades) > ‘Firmware Password Utility’ (Utilidad de Contraseña para Firmware) > ‘Turn on Firmware Password’ (Activa la Contraseña de Firmware). Escoge una contraseña fuerte (ver capítulo 8) y haz click en ‘Establecer contraseña’. Es muy importante que recuerdes esta contraseña, o podrías no tener más acceso a tu Mac.

Chipsets

Hacia 2006, Intel empezó a poner componentes especiales en sus chipsets (combinaciones de chips que trabajan juntos en la placa base del laptop) para permitir la gestión automatizada del sistema por medio de una red. Esto se llama ‘Intel Active Management Technology’, y significa que un técnico de informática en una oficina grande o en la sección de informática en una universidad puede actualizar el software, o hacerle otras cosas a las máquinas, sin tener que estar físicamente cerca de ellas. El problema es que, por supuesto, la misma funcionalidad se puede utilizar para instalar spyware o manipular el sistema de otras maneras. Todos los laptops fabricados después del 2008 contienen estos chipsets, y son, por lo tanto, vulnerables a este tipo de ataques cuando están en una red.

El chipset ‘Intel 945’ es el más reciente sin esta función automatizable, y por esto se presta para hacer segura una placa base o un ordenador. Cuando vayas a escoger un laptop, en las especificaciones puedes ver cuál es el chipset.

Sistema operativo

También puede que desees comprar un laptop que te deje instalar el sistema operativo de tu elección (idealmente, open source, donde el código fuente esté disponible públicamente). Puedes hacer esto bastante fácilmente en la mayoría de los laptops, excepto los MacBooks.

Sistemas operativos propietarios (Windows, Mac) son de código cerrado y pueden tener varias puertas traseras de seguridad integradas (desde luego tienen control remoto de las funciones que permiten actualizaciones automáticas), por lo tanto no es posible saber cuánto seguro es ejecutar simultáneamente sistemas operativos alternativos. Mientras la

mayoría de laptops permiten al usuario borrar el sistema Windows, borrar el sistema operativo de un MacBook es desaconsejable ya que puede comprometer el funcionamiento general del sistema.

En Mac es posible ejecutar varios sistemas operativos, pero esto requiere conocimientos de cómo usar una ‘máquina virtual’, lo cual no vamos a tratar aquí (aparte de Tails, que obvia el uso del disco duro y se ejecuta desde una memoria USB.Ver capítulo 2).

¿Cómo puedes interpretar estos cuatro problemas de seguridad fundamentales para modelar tu nivel de riesgo? Es probable que el acceso remoto al Hardware, al firmware y al chipset solo puedan hacerlo agencias de inteligencia de naciones tecnológicamente avanzadas y ricas, pero con el paso del tiempo toda la tecnología tiende a democratizarse y llega a grupos menos poderosos. Por lo tanto, si potencialmente puedes incluir a una agencia de inteligencia de este tipo entre tus adversarios, quizá quieras evaluar esos tres factores de vulnerabilidad. Aún si no enfrentas este nivel de riesgo, quizá quieras, de todos modos, tomar algunas precauciones de seguridad como medida de cautela (en particular aquellas que requieren poco esfuerzo, como cerrar el firmware de un Mac).

Es probable que agencias de inteligencia con tecnología avanzada tengan acceso a puertas traseras en sistemas operativos. Puede también darse el caso, sin embargo, de que corporaciones especialmente grandes o poderosas puedan obtener este conocimiento o acceso, así que si tu adversario es un gigante corporativo, deberías de considerar los aspectos de seguridad de tu sistema operativo.

Escoger qué laptop usar no es fácil, deberías de tomarte tu tiempo para procesar esta información, evaluar tu nivel de riesgo, y decidir cuánto esfuerzo y disciplina invertirás en la seguridad de tu información.

He aquí algunas sugerencias sobre qué laptops podrías comprar según varios niveles de riesgo generalizados:

Riesgo bajo: vigilancia de emboscada, hacking individual de bajo nivel o hurto.

Puedes empezar con cualquier laptop. ¡Un buen periodista de investigación sobrepasará esta categoría pronto! La seguridad de la mayoría de los sistemas se puede reforzar de manera aceptable contra amenazas poco sofisticadas a nivel de software. Manteniendo tu máquina contigo todo el tiempo, puedes defenderte contra hurtos o intervenciones físicas. También puedes evitar las emboscadas mediante la selección que hagas del software y de las aplicaciones.

Riesgo mediano: vigilancia dirigida por un adversario que está preparado, o le es posible invertir recursos relativamente limitados.

Usa un laptop en el que puedas borrar el sistema operativo actual e instalar el tuyo (idealmente, un sistema operativo Linux de código abierto); o el sistema operativo Tails para trabajar en el proyecto desde cualquier ordenador. Ver capítulo 2 para más información sobre sistemas operativos.

Riesgo alto: vigilancia dirigida por una agencia de inteligencia.

Solo hay unas cuantas máquinas que pueden ser aseguradas con confianza contra el acceso remoto a hardware, firmware y chipset. Por ahora, el modelo que se protege más frecuentemente de esta manera es el IBM ThinkPad X60 (y X60s). Tiene un chipset Intel 945 (esto es pre-AMT), y se puede realizar en él un trabajo especializado para asegurar el hardware y el firmware (el firmware propietario se puede reemplazar por firmware de fuente abierta, 'coreboot'). Después se debería usar el sistema operativo Tails (ver capítulo 2) en este ordenador seguro, para mantener un sistema fiable.

Si necesitas uno de estos ordenadores fiables, por favor, contáctanos de manera segura en el Centre for Investigative Journalism. Puedes mandar un correo encriptado a infosec@tcij.org o contactar a la oficina (ver http://www.tcij.org/about-cij/contact-us).

Si quieres hacerlo tú mismo, podrías comprar un laptop con chipset pre-AMT que te deja abrir la cubierta, y usar la documentación en línea del laptop para guiarte a través de un mantenimiento de hardware básico. Por ejemplo, podrías remover la memoria de disco duro del laptop, y remover/deshabilitar el micrófono, webcam, tarjeta Wi-Fi, tarjeta Bluetooth, o modem 3G, y puerto Ethernet de tu laptop (ver punto 2 en este capítulo). Sin embargo, a menos que cuentes con una formación específica, serás incapaz de hacer las modificaciones de más pequeña escala del hardware para su máxima seguridad o reemplazar el firmware.

Máximo riesgo: vigilancia dirigida y orientada por una agencia de inteligencia, posiblemente con vistas a comprometer la seguridad y libertad del blanco/s, y la integridad de su información.

En situaciones de muy alto riesgo deberías de tener al menos dos laptops con todas las medidas de seguridad implementadas, uno de los cuales no debe nunca por bajo ningún concepto conectarse a internet. Esta será tu máquina con seguridad de tipo 'air gap', un laptop que nunca, jamás, entra en línea. Esta puede ser una máquina muy útil para guardar o acceder archivos (por ejemplo, que quizá tengas en una memoria USB), escribir artículos, y producir tus reportajes. Tú, o el especialista que te ayude, tendrías que remover o deshabilitar todos los aparatos de conectividad en el laptop, para asegurar que verdaderamente esté desconectada de la línea en todo momento (ver punto 2). Idealmente ambas, tu máquina 'air gapped' y tu máquina en línea, deberían de ser dos IBM ThinkPad X60s especialmente protegidas.

Hecho: Glenn Greenwald usa un laptop airgapped [N.d.t: aislado de conexiones de red inseguras] para trabajar en los documentos Snowden.

Esto agrega un nivel extra de seguridad para tu información y la de tu fuente, porque tus documentos importantes están, no sólo guardados en una máquina segura sino también enteramente desconectados de la red. Hasta la máquina más segura puede exponerse a cierto grado de riesgo cuando está en red, particularmente si el usuario es objeto de un ataque dirigido.

2. Modificar tu hardware

Démosle un vistazo a todos los componentes internos modificables que potencialmente podrían ser usados para vigilarte a ti, tu fuente y tu trabajo.

- Webcam
- Micrófono
- Memoria de disco duro
- Tarjeta de Wi-Fi
- Tarjeta de Bluetooth
- Modem 3G
- Puerto Ethernet

Webcam:
Las webcams no solo pueden ser activadas remotamente y de forma encubierta, sino que imágenes de la webcam también han sido interceptadas como parte de programas de vigilancia por emboscada (ver las revelaciones de Snowden sobre el programa OPTIC NERVE del GCHQ). Una solución simple es poner un adhesivo sobre tu webcam.

Micrófono:
El micrófono de tu laptop también puede ser activado de forma remota y encubierta, para capturar audio. Podrías probar a poner pegamento caliente sobre la entrada del micrófono en la cubierta de tu laptop para amortiguar el sonido. Mejor aún, abre la cubierta y corta el cable del micrófono.

Memoria de disco duro:
Se han encontrado algunos discos duros que contienen firmware ‘malo’, es decir, que podrían activarse para comprometer tu seguridad, si te convirtieras en el blanco de una agencia dotada de herramientas muy sofisticadas.

En niveles de alto riesgo, es aconsejable extraer el disco duro y trabajar desde una memoria USB. Las memorias USB también son ideales para guardar el sistema operativo seguro, Tails (ver capítulo 2); es decir, pueden sostener un sistema anónimo pequeño desde el cual trabajar. Los USB son muy transportables y fáciles de replicar (para compartir con colegas/fuentes), y son fácilmente protegibles con encriptación de alto grado (ver capítulo 4). Esto también quiere decir que si tu laptop es dañado o hurtado, la información guardada en tu USB todavía está segura. Aun así, puede que desees usar el disco duro para tu uso general del día a día, y trabajar desde memorias USB o Tails para proyectos específicos.

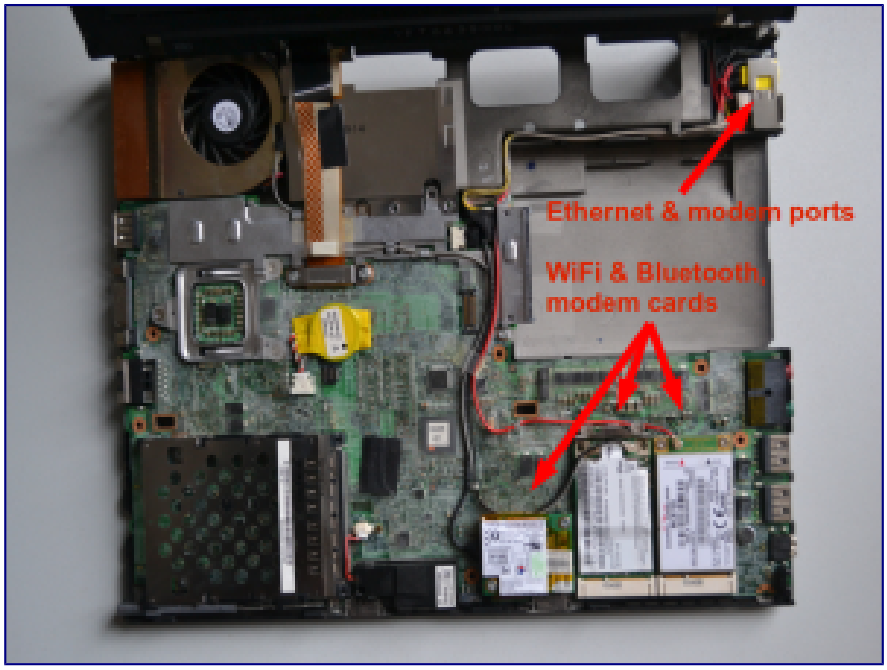
Tarjeta Wi-Fi, tarjeta Bluetooth, modem 3G:
En alto nivel de riesgo, cualquier elemento que permita una conexión podría ser activado remotamente y encubierto para instalar herramientas de vigilancia, o de hecho para pasarle tu información a un adversario. Por ende, deberías aspirar a tener el mayor control posible sobre la conectividad de tu laptop.

La mejor manera de hacer esto es extrar físicamente los componentes de conectividad.

Esto significa abrir la cubierta del laptop, desmontar la tarjeta Wi-Fi, al igual que cualquier tarjeta Bluetooth y modem 3G, si tu laptop los tiene (consulta el manual de tu laptop si no estás seguro, a menudo se pueden encontrar ejemplares en la red). Al principio esto puede parecer una tarea abrumadora, pero cualquiera con mano firme y con la formación correcta puede hacerlo a la primera
De esta manera puedes controlar cuándo estás en línea o no. Podrías comprar un adaptador USB de Wi-Fi USB, que funciona igual que tu tarjeta Wi-Fi, y te permite conectarte a internet. La diferencia es que puedes fácilmente conectar y desconectar el adaptador del puerto USB y así tú decides cuándo estás en red y cuándo no. En la que es otra opción, puedes escoger cuándo estar conectado por medio de un cable Ethernet.

Puerto Ethernet:
El puerto Ethernet es lo que usas para conectarte físicamente a una 'red de área local' (LAN), que puede ser desde la red de una oficina grande o el enrutador de tu casa proporcionado por tu proveedor de internet. Por supuesto, ahora el Wi-Fi es de uso más común que las conexiones cableadas de Ethernet.

Se sabe que los puertos Ethernet tienen vulnerabilidades de seguridad específicas, que pueden ser explotadas contra blancos de riesgo especialmente alto. Si deseas proteger tu máquina de la explotación del Ethernet (p.ej. para una máquina airgapped), podrías llenar el puerto con pegamento caliente. Otra opción, consiste en desconectar los cables del puerto del interior del laptop.



3. Comprar tu laptop de forma anónima

A medida que aprendes sobre InfoSec, puede que quieras comprar uno o dos laptops nuevos. Esta no es solo una sabia decisión, cuando trabajas con una fuente nueva de alto riesgo, o en un proyecto sensible, sino también cuando se trata de prepararte ante la posibilidad de estas eventualidades y para implementar tu nuevo aprendizaje de InfoSec.

El proceso de comprar un laptop seguro debería de ser lo más anónimo posible en situaciones de alto riesgo, con el fin de prevenir que un adversario introduzca previamente herramientas de vigilancia en tu hardware; esté al corriente de tu nuevo hardware y así se vea motivado a invadir tu máquina física o virtualmente después de la compra; o rastree tu laptop o tus datos y de este modo dé contigo y/o tu fuente.

Si trabajas con una fuente de alto riesgo, como un informador de datos de inteligencia, esa persona puede estar ya bajo vigilancia. Debes dar por hecho que el riesgo de vigilancia que corre tu fuente también lo corres tú.

Los documentos de Snowden revelaron que agencias de inteligencia interceptaban dispositivos como laptops, teléfonos y otros aparatos electrónicos para implantar herramientas de vigilancia, antes de que la fábrica los sellase y los pusiera en tránsito – así que deberías evitar comprar cualquier hardware (incluso cargadores) en internet. La mayoría de los elementos de hardware pueden ser modificados para actuar como herramientas de vigilancia.

Primero deberías decidir qué modelo de laptop quieres comprar (después de leer este capítulo) y asegurarte de que antes de comprarlo haces tu búsqueda sobre laptops utilizando el navegador anónimo Tor (ver capítulo 3). Para estar seguro, puedes comprar tu/s laptop/s en persona, con dinero en efectivo. Si compras un modelo más viejo quizá quieras encontrar un área, preferiblemente lejos de donde normalmente compras, donde haya varias tiendas de electrónica de segunda mano. A niveles más altos de riesgo quizá quieras usar varias tiendas diferentes para comprar cada laptop y accesorios (p.ej. memorias USB), y mientras compras, poner cualquier aparato que te pudiera rastrear (p.ej. tu teléfono) en una jaula Faraday (un recinto metálico que impide la transmisión de señales) o dejarlo en un lugar seguro en casa.

Para organizaciones de comunicación o campañas, es una buena idea, como prevención, preparar equipos con herramientas y configuración de seguridad (que deberían de estar guardados en caja fuerte hasta su uso) y formar en su uso a varios empleados. Para consejos sobre kit de herramientas ya confeccionados y formación, contactar con infosec@tcij.org.

4. Vigilar tu laptop

Evitar el robo, daño (intencionado o no) y ataques físicos a tu hardware, especialmente si consideras que estás en riesgo de vigilancia dirigida, significa adoptar un comportamiento nuevo importante: mantener tu laptop en todo momento contigo, cerca de ti, o bajo tu vista. Adoptar este tipo de comportamiento se llama a veces ‘OpSec’, o ‘Seguridad Operacional’. Si en algún momento tu laptop queda desatendido (por ejemplo en casa, en un café o en la oficina) o en manos de otra persona (por ejemplo equipaje facturado en un vuelo; o al ser retenido por la policía/autoridades), deberías considerar, dependiendo de tu nivel de riesgo, la posibilidad de que quizá el sistema ya no sea seguro.

Haz que tu sistema seguro sea lo más simple, pequeño y liviano que te sea posible, evita conectar el laptop a un ratón, teclado, impresora, estación de conexión u otros aparatos

(que, por su alto riesgo, podrían estar ‘interferidos’) para limitar el hardware que debas llevar contigo o del que debas responsabilizarte.

Tienes que considerar la seguridad física de tu hardware no sólo en el momento presente y en el futuro, sino de forma retrospectiva. ¿Pudo haber sido atacado físicamente antes? ¿Cómo fue fabricado? ¿Podría el hardware estar ya comprometido?

Como sabemos que el envío puede ser arriesgado, tratamos el tema de comprar hardware nuevo en persona, en efectivo (punto 3). Ésta no solo es una manera más anónima de comprar un laptop, sino que también puedes responsabilizarte físicamente de forma inmediata.

5. Medidas de detectabilidad

Detectar posibles intervenciones físicas en tu laptop es extremamente difícil. Si necesitas guardar tu laptop de forma segura por cualquier razón (por ejemplo, si deseas cruzar la frontera de un país sin tu laptop) deberías tratar de hacerlo de manera que si hay cualquier transgresión de la seguridad fuera detectable. Sé creativo/a – pero será un reto ser más astuto que un adversario sofisticado. Idealmente, lo dejarás bajo la estrecha protección de alguien en quien confíes, si no puedes protegerlo tú mismo.

Para defensa tecnológica contra riesgos de bajo nivel y como una medida de seguridad general, podrías descargar la aplicación de código abierto llamada Prey: ver https://preyproject.com. Se trata de un software de rastreo que ayuda a los usuarios a encontrar, bloquear y recuperar sus ordenadores. También te permite capturar imágenes de la pantalla del laptop robado, y activar la webcam para tomar una foto del nuevo dueño. ¡Descargar software de rastreo puede parecer un contrasentido para un periodista que quiere proteger estrictamente su privacidad! Puesto que es de código abierto, la aplicación está pensada para ser bastante fiable. Sin embargo, un adversario sofisticado no se verá dificultado por esta aplicación. Sólo se recomienda usar esta aplicación como defensa contra adversarios menos avanzados.

Si deseas continuar usando hardware que no puedes hacer fiable, hay medidas que puedes tomar para proteger tu información y comunicaciones de ataques de adversarios no gubernamentales/menos poderosos, así que por favor sigue leyendo. Sólo sé consciente de que, si te conviertes en el blanco de vigilancia de alguien con los recursos, habilidad y motivación para obtener tu información, se trata de un hecho consumado.

Capítulo 2: Sistema Operativo

Si tu hardware es ya seguro contra vigilancia automatizada y preinstalada, es vital que impidas la introducción de software que pueda hacer vulnerable otra vez al sistema. Aun si operas a bajo nivel de riesgo, usar el software correcto puede ayudar a proteger la seguridad de tu información y tus comunicaciones de cualquier vigilancia automática y de emboscada (dragnet).

El software más importante en un ordenador, además del firmware (Ver 'Firmware' en Capítulo 1) es el sistema operativo. Este es el software que toma el control cuando se enciende el ordenador, y es la interfaz por la que usas el ordenador. En resumen, el sistema operativo le dice al ordenador qué hacer y cómo hacerlo. Entre los sistemas operativos más conocidos están versiones de Windows (p.ej. XP, Vista, 8, 10), OS X (para Mac), y distribuciones de Linux.

Ahora sabemos que agencias de inteligencia tienen acceso a 'puertas traseras' en sistemas operativos populares, que permiten el acceso encubierto a información de los usuarios.

Amenazas asociadas con sistemas operativos:

- Malware, virus
- Vigilancia de 'puerta trasera' en el sistema operativo, accesible para la comunidad de inteligencia

Dos medidas claves son importantes para la protección contra amenazas del sistema operativo:

Usa un sistema operativo de código abierto (para riesgo mediano)
Usa Tails, un sistema operativo amnésico, de incógnito (para alto – máximo riesgo)

Para estar relativamente seguro/a de que tu sistema operativo no tiene potenciales 'puertas traseras' de vigilancia (es decir que no pude ser explotado con propósitos de vigilancia), es necesario que sea 'open source' (de código abierto). El Software 'Open source' es software distribuido libremente, cuyo código fuente, el tejido mismo del sistema operativo, es 'abierto' y disponible públicamente. Esto permite que los expertos independientes puedan ver la fuente del código en cualquier momento, y verifiquen que no hayan defectos de seguridad en la constitución del sistema operativo. Una definición completa de diez puntos está disponible (en inglés) en www.opensource.org/osd.

Además, los sistemas operativos de código abierto son menos susceptibles a malware (software malicioso, típicamente spyware) y virus. Esto es porque son usados mucho menos frecuentemente que los sistemas operativos propietarios y tienen proporcionalmente una baja participación en el mercado.

El software de código abierto también es conocido como ‘software libre’ no sólo por el libre acceso a su fuente de código, sino también porque es distribuido gratuitamente o sólo a cambio de donaciones.

Debemos mencionar que el software de código abierto, es tan fiable como la confianza que se tenga en la experiencia y frecuencia con la que la fuente de código es creada y examinada. Sin embargo, el software de código abierto, que se usa ampliamente, es más probable que se controle con frecuencia, y es preferible (al menos para los propósitos de InfoSec) al software de fuente cerrada.

Sistemas operativos de Microsoft y Apple (p.ej. Windows, OS X) son de código cerrado, y cabe pensar que contengan puertas traseras de vigilancia accesibles a la NSA e intereses aliados. Los sistemas operativos de Microsoft son particularmente inadecuados, ya que su código fuente está más cerrado que el código de Apple y sus sistemas son más susceptibles a malware y virus. Si piensas que tú, o alguien con quien te comunicas, podría ser (o convertirse en) un blanco de vigilancia, este tipo de sistemas operativos con código fuente cerrado son inadecuados para información y comunicaciones importantes.

Nota: sistemas operativos de código cerrado para telefonía, como iOS y Android, son omnipresentes en teléfonos inteligentes, que son por ende indefensibles contra ataques dirigidos – ver capítulo 7 para más InfoSec de telefonía.

Linux
Linux es el sistema operativo líder de código abierto, desarrollado por la comunidad. Hay muchas versiones del sistema operativo Linux que puedes usar.

Ubuntu
Ubuntu.com

Ubuntu es el sistema operativo Linux más ampliamente usado. Es fácil de instalar, altamente funcional, y amigable para el usuario.

Puedes remplazar tu sistema operativo Windows con Ubuntu, o puedes utilizar ambos, Windows y Ubuntu, en el mismo laptop (lo que puede ayudar a familiarizar al usuario con el nuevo sistema antes de ponerse de lleno con él). Ubuntu es muy amigable para el usuario y no demasiado diferente a otros sistemas operativos, así que nosotros recomendamos lo anterior, que remplaces tu sistema operativo Windows con Ubuntu. Esto elimina el sistema operativo Windows totalmente, lo cual es esencial para los propósitos de InfoSec (de otra manera, las ‘puertas traseras’ pueden permanecer). Ten en cuenta que la eliminación de tu sistema operativo antiguo, también eliminará todos los archivos asociados con este, así que asegúrate de hacer un backup (copia) de todos los archivos de ese laptop que desees conservar.

No es recomendable que usuarios inexpertos limpien el sistema operativo de un MacBook para instalar Ubuntu, ya que esto puede causar problemas con la funcionalidad de un Mac. Podrías usar Ubuntu por medio de una ‘máquina virtual’ en Mac, pero no trataremos

esto aquí – no está claro qué ventajas de seguridad se pueden lograr al ejecutar ambos sistemas operativos simultáneamente.

Debemos comentar que algunos elementos de Ubuntu son, de hecho, de fuente cerrada, pero se piensa (aunque no se sabe con certeza) que estos no suponen un riesgo para la seguridad. Aun así, otras variaciones populares de Linux, entre las que están 'Debian' y 'Trisquel', son enteramente de código abierto. Ten en cuenta que estos pueden ser ligeramente menos intuitivos para usar y mantener para quienes empiezan a usar Linux.

Tails
tails.boum.org
Utiliza un sistema operativo amnésico, incógnito para obtener el mayor grado de seguridad: Tails. Tails significa 'The Amnesic Incognito Live System' (El Sistema Amnésico Incognito En Vivo). Es un sistema operativo de código abierto, basado en Linux que protege la privacidad y el anonimato del usuario.

Amnésico: porque después de apagarlo no queda ningún rastro en el sistema de su uso en el ordenador.
Incógnito: porque está orientado hacia la privacidad y la seguridad, accediendo a internet de manera anónima por defecto, y esquivando así cualquier censura.

Tails está diseñado expresamente como un sistema anti-vigilancia, y viene con varias aplicaciones incorporadas (enteramente de código abierto) orientadas a la seguridad:

Anonimato en la red incorporado
El navegador integrado, Iceweasel, usa tecnología de navegación anónima en la red por medio de Tor (ver capítulo 3). El navegador también incluye extensiones de seguridad populares como HTTP

Encryption y HTTPS Everywhere que encriptan tu información de navegación; Adblock Plus para bloquear anuncios; y NoScript para bloquear Java y Flash (ya que pueden comprometer el anonimato). Esto quiere decir que algunas aplicaciones en la red no funcionarán por medio de Tails, pero es un compromiso que vale la pena por la incomparable privacidad obtenida cuando se trabaja en proyectos sensibles.
Nota: si intentas entrar a una cuenta en línea que está claramente conectada a tu identidad real, comprometerás tu anonimato durante toda esa sesión en la que estés usando el ordenador. Apaga y reinicia Tails cada vez que uses una nueva identidad contextual. Archivos y documentos también pueden poseer metadatos que pueden indicar tu ubicación mediante GPS. Ver capítulo 4 para consejos sobre cómo borrar dichos metadatos.

Correo y chat encriptado incorporado
Tails ofrece mensajería encriptada incorporada. Tails incluye el correo electrónico Claws con OpenPGP para la encriptación del correo (ver capítulo 5) y el sistema de mensajería instantánea Pidgin (ver capítulo 6) que mantiene la privacidad y el anonimato de tus mensajes.

Encriptación de archivos incorporada
Tails viene con LUKS, que puede encriptar archivos. Si quieres guardar archivos en la misma memoria USB en la que estás ejecutando Tails, puedes crear un espacio de almacenamiento permanente o un 'volumen' persistente en el dispositivo USB. Tails encriptará el volumen persistente por defecto, solicitando tu contraseña para ver o acceder a cualquier archivo guardado.

Información del experto: Si bien este volumen persistente es útil para guardar información y documentos relativamente poco importantes, no deberías usarlo para guardar o transportar los documentos más sensibles. Esto se debe a que el volumen persistente no está 'oculto'. Esto es, si un adversario llegara a obtener tu USB, podría ver que existe un volumen encriptado en el aparato, y podría forzarte o engañarte para que le des la contraseña. Deberías crear un volumen 'oculto' para los documentos más sensibles, quizá en un USB diferente, que aparenta no ocupar espacio: sólo tú sabes que está ahí. Esto puede hacerse fácilmente con una aplicación llamada TrueCrypt (ver capítulo 4).

Protección de contraseña incorporada
Tails viene con KeePassX precargado, un gestor de contraseñas que almacena usuarios y contraseñas en una base de datos local, encriptada y protegida por tu contraseña maestra. También viene con PWGen, un generador de contraseñas aleatorias fuertes.

Tails está diseñado para ser usado desde un USB, independientemente del sistema operativo original del ordenador. Esto quiere decir que puedes quitar el disco duro de tu laptop (recomendado para trabajo de alto riesgo), y aun así iniciar el laptop desde el USB con Tails. Otra opción, consiste en poner un USB con Tails en un ordenador con el disco duro intacto, e iniciar por medio de Tails – la máquina ignorará el disco duro y el sistema operativo original y, en su lugar, funcionará desde la memoria USB con Tails.

La existencia de un 'mini sistema' en un USB con Tails lo hace ideal para proyectos periodísticos sensibles. Tu máquina puede esencialmente estar 'limpia' sin ningún trazo de tu trabajo en ella, y tus documentos pueden estar guardados en una memoria portátil USB muy transportable y barata.. Tails hasta viene ya precargado con software de código abierto cómo OpenOffice para crear, leer y editar documentos, Gimp para editar fotos, y Audacity para editar sonido.

El USB es ideal para viajar y lo puedes conectar a cualquier ordenador, si haces que el ordenador se inicie desde el USB (se explica en las instrucciones más adelante). Es prudente tener memorias USB con Tails separadas para distintos proyectos, para difundir el trazo de tu identidad y minimizar el riesgo en el caso de que llegaras a perder un USB. Si es apropiado, también podrías darle un USB con Tails ya preparado a tu fuente, con unas cuantas instrucciones, para que tenga una forma segura de comunicarse contigo. En escenarios de alto riesgo, puede que desees usar Tails en una máquina enteramente separada de tu laptop habitual.

Usar Ubuntu es una buena opción para el trabajo del día a día. Pero es sabio crear también un USB con Tails y cambiar a Tails cuando se trabaja en proyectos sensibles,

particularmente cuando se trabaja con documentos importantes, comunicándose con individuos de alto riesgo, o investigando en la red para proyectos sensibles. Más allá, tomar serias medidas preventivas de InfoSec , puede prolongar tu anonimato y por lo tanto el tiempo del que tú y, lo que es más importante, tu fuente, dispongáis antes de convertiros en blancos de vigilancia.

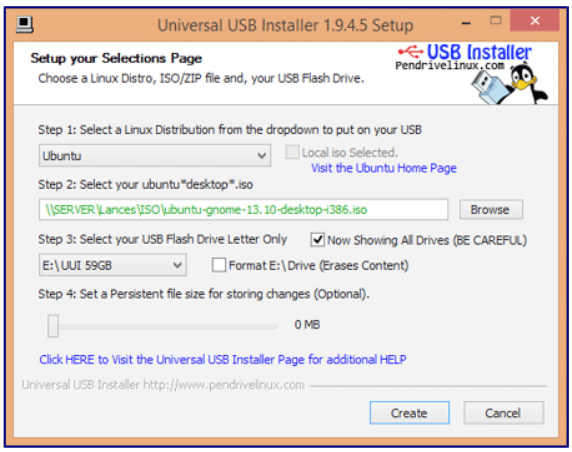
Ahora has aprendido cómo proteger sólidamente tu sistema. En los siguientes capítulos aprenderás cómo proteger tus comunicaciones, convertir en anónima tu información de navegación, y encriptar y transportar documentos sensibles.

Instrucciones paso a paso

Ubuntu

Nota: todos los documentos, programas, archivos, etc. de Windows serán borrados si reemplazas Windows con Ubuntu (recomendado).

1. ***Descarga Ubuntu***
   Descarga Ubuntu en
   http://www.ubuntu.com/download/desktop
   Necesitarás saber cuánta RAM tiene tu laptop y descargar ya sea el de 32-bit (para máquinas más antiguas, como los ThinkPads recomendados, con 2GB o menos de RAM) o el de 64-bit (para máquinas más nuevas con 4GB o más de RAM). La descarga puede llevar unos 20-60 minutos.
2. ***Descarga el instalador de USB Linux (Linux's USB Installer)***
   Ve a http://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows, haz clic en 'Download Pen Drive Linux's USB Installer ›', y desplaza hacia abajo para hacer clic en el botón grande 'Download UUI' (Descargar UUI). Esto descargará el instalador de USB, dejándote guardar Ubuntu en una memoria USB, que usarás para instalar Ubuntu.
   Información del experto: Durante la instalación, el disco duro no puede ejecutar ningún otro software, por lo que necesitas de otra fuente, en este caso el USB, para ejecutar el programa de instalación.
3. ***Coloca Ubuntu en el instalador de USB***
   Cuando ambas descargas estén completas, inserta un USB limpio y abre el instalador USB.
   Selecciona Distribución de Linux en el menú desplegable (Ubuntu); usa el botón 'Browse' (Buscar) para localizar la descarga de Ubuntu; y selecciona Letra del Lector USB (donde el ordenador ha localizado tu USB). Haz clic en 'Create' (Crear).



Cuando esto esté completo, retira el USB de forma segura, y apaga el ordenador.

4. ***Instalar Ubuntu***
   Arranque desde un USB

   Es necesario configurar el equipo para arrancar desde un dispositivo USB – una configuración que se encuentra en el menú de la BIOS de tu portátil. Puedes acceder al menú de la BIOS al arrancar tu ordenador. Antes de intentar esto, es posible que quieras buscar en línea para saber qué tecla pulsar para poder acceder al menú de la BIOS de tu ordenador portátil. En muchos ordenadores, en el momento del arranque (encendido) , aparece un mensaje ‘ingresar en configuración’, informándote de que puedes pulsar [tecla] para entrar en la BIOS de configuración del sistema, en cuyo caso puedes seguir esa instrucción. A menudo son teclas como F1, F2, F3, F12 o DEL.

   También es posible que desees investigar cómo, a través del menú propio de la BIOS de tu ordenador, puedes arrancar el equipo desde la unidad USB. Inserta la memoria USB en el portátil mientras está apagado, luego arráncalo y entra en el menú de la BIOS. Este ajuste puede estar en un elemento del menú, tal como Inicio > Arranque; o fichas de menú tales como ‘arranque’, ‘opciones de arranque’ u ‘opciones de selección de arranque’. Selecciona tu unidad USB o asegúrate que tu unidad USB es la opción prioritaria de arranque (si un elemento de la lista tiene una ‘+’, significa que tiene un submenú, ¡donde tu listado USB puede estar escondido!). A menudo, puedes cambiar el orden con las teclas + y -. Ve al menú ‘Salir’ o a ‘Guardar y salir’, y selecciona la opción (o similar) ‘Salir Guardando Cambios’ para asegurarte la opción de arranque.

   Después de guardar y salir del menú BIOS, la máquina debería de iniciarse desde el USB y por lo tanto se debería de cargar el menú de inicio del instalador de Ubuntu.

   Selecciona ‘Install Ubuntu on a Hard Disk’ (‘Instalar Ubuntu en un disco duro’). Ahora el instalador automático te guiará a través de la configuración de Ubuntu.

   Puede que te pida configurar el Wi-Fi, pero no tienes que preocuparte en configurar el Wi-Fi ahora, especialmente si has quitado tu tarjeta de Wi-Fi.

Bajo ‘Installation type’ (Tipo de instalación):

- Selecciona: Replace Windows with Ubuntu (Reemplaza Windows con Ubuntu) (si quieres borrar Windows)
- Selecciona: Encrypt the new Ubuntu installation for security (Encriptar la nueva instalación de Ubuntu para seguridad)
- Selecciona: Use LVM with the new Ubuntu installation (Usa LVM con la nueva instalación de Ubuntu)

Escoge una contraseña fuerte (ver capítulo 8 para orientación).

El software te pedirá que registres tu nombre (pero no tienes que introducir nada aquí). Escoge un nombre para tu ordenador y un nombre de usuario para el inicio de sesiones. Escoge una contraseña fuerte y marca las opciones ‘require my password to log in’ (solicita mi contraseña para iniciar sesión) y ‘encrypt my home folder’ (encripta mi carpeta personal).

Ahora Ubuntu completará la instalación. Una vez instalado, apaga el laptop y retira el USB. ¡Enciende el laptop y Ubuntu debería lanzarse!

Cuando te conectes a internet, ve al icono de Ubuntu que está en la parte superior izquierda en tu ‘Desktop’ (escritorio) y busca ‘updates’ (actualizaciones). Haz clic para aceptar cualquier actualización.

Ajustes de privacidad en Ubuntu

- Selecciona ‘System Settings’ (Configuraciones del Sistema) en tu desktop (escritorio) > Security and Privacy (Seguridad y Privacidad)
- Bajo ‘Files and Applications’ (Archivos y Aplicaciones) puedes controlar si queda registrado el uso de tus archivos y aplicaciones
- Bajo ‘Search’ (Búsqueda) puedes deshabilitar los resultados de búsqueda en la red por Dash. Esto detiene la integración de Amazon en Ubuntu y previene que tus búsquedas en Dash sean enviadas de vuelta a los servidores de Ubuntu y Amazon. Puedes hacer un clic con el botón derecho en el ícono de Amazon en tu desktop (escritorio) y seleccionar ‘Unlock from Launcher’ (liberar del lanzador) para eliminarlo del desktop
- Bajo ‘Diagnostics’ (Diagnósticos) puedes optar por evitar enviar ‘error reports’ (informes de error) y ‘occasional system information’ (información ocasional del sistema) a Canonical

Tails

Hay tres formas de instalar Tails que recomendamos:

1. Por medio de un USB clonado con Tails de una fuente fiable, permite la creación de un volumen persistente. (Contactar con infosec@tcij.org para ayuda en encontrar un USB clonado con Tails)
2. Manualmente por medio de UNetbootin (que no te permite crear un volumen

persistente en el USB, pero puedes crear un volumen persistente en el USB con Tails que clones de este)

3. Manualmente por medio de tu sistema Linux (que tampoco te permite crear un volumen persistente en el USB).
    - Una vez que tengas un USB con Tails, deberías de reiniciar tu ordenador desde el USB cuando quieras usar Tails. Ver el recuadro de ‘Iniciar desde USB’ en la página 32

¿Qué método de instalación debería usar?

Recomendamos especialmente empezar con Tails desde un USB clonado. La instalación manual no es sencilla y por esto no tiene un porcentaje de éxito perfecto.
Las instalaciones manuales no se actualizan automáticamente a la versión más reciente de Tails. Para tu seguridad, debes asegurarte de usar la última versión de Tails y actualizar regularmente (ver ‘Actualizar Tails’).

Sin embargo, los sistemas Tails hechos con el ‘Instalador de Tails (esto es copias de Tails que han sido clonadas de un sistema Tails ya existente) se actualizan automáticamente y le permiten al usuario crear un volumen persistente.

Por lo tanto, recomendamos el uso de un sistema Tails clonado de una fuente fiable. Otra opción consiste en probar una instalación manual de Tails y usar esa copia para clonar un sistema Tails nuevo (en una segunda memoria USB). Ver ‘Clonar Memorias USB con Tails’.

A continuación damos las instrucciones para la instalación desde el sistema operativo **Linux**. Para opciones de instalación en **Windows** y **Mac**, ver la documentación de Tails (puede que quieras abrir este tipo de páginas, y la página de descarga para Tails, por medio del navegador Tor, el cuál explicamos en el capítulo 3) https://tails.boum.org/doc/first_steps/index.en.html.

Nota: Si bien son muchos más los usuarios que utilizan con éxito desde ordenadores Mac la última *versión de Tails; los desarrolladores de Tails tienen menos experiencia usando Mac y han sido reportados problemas (como la imposibilidad de acceder al WiFi).*

Necesitarás:
1. Un USB limpio (explicado a continuación) que sea de 4GB o más grande (idealmente 16GB si tienes intención de guardar documentos en este también)

2. La descarga de la versión disponible más reciente de Tails
a) Abre el navegador Tor. Ve a https://tails.boum.org/download/, desplaza abajo a ‘2. Download the ISO image’ (descargar la imagen ISO), y haz clic en el botón inferior Direct Download (Descarga Directa) y Latest Release (Última Edición) (‘Tails [versión] ISO image’). Guarda el archivo.

Limpiar y preparar la memoria USB

Tal vez hayas usado esta memoria USB anteriormente, o tal vez venía con un software preinstalado. De cualquier manera, abrir el lector USB en un ordenador y trasladar los

archivos a la papelera, sólo evita que aparezcan en un listado visible, pero no los ‘borra’ realmente. Para tu nueva memoria USB con Tails, lo que quieres es empezar con un dispositivo completamente limpio.

También necesitamos cambiar algunas configuraciones en el USB, para que esté preparado para iniciar el ordenador y hospedar Tails.

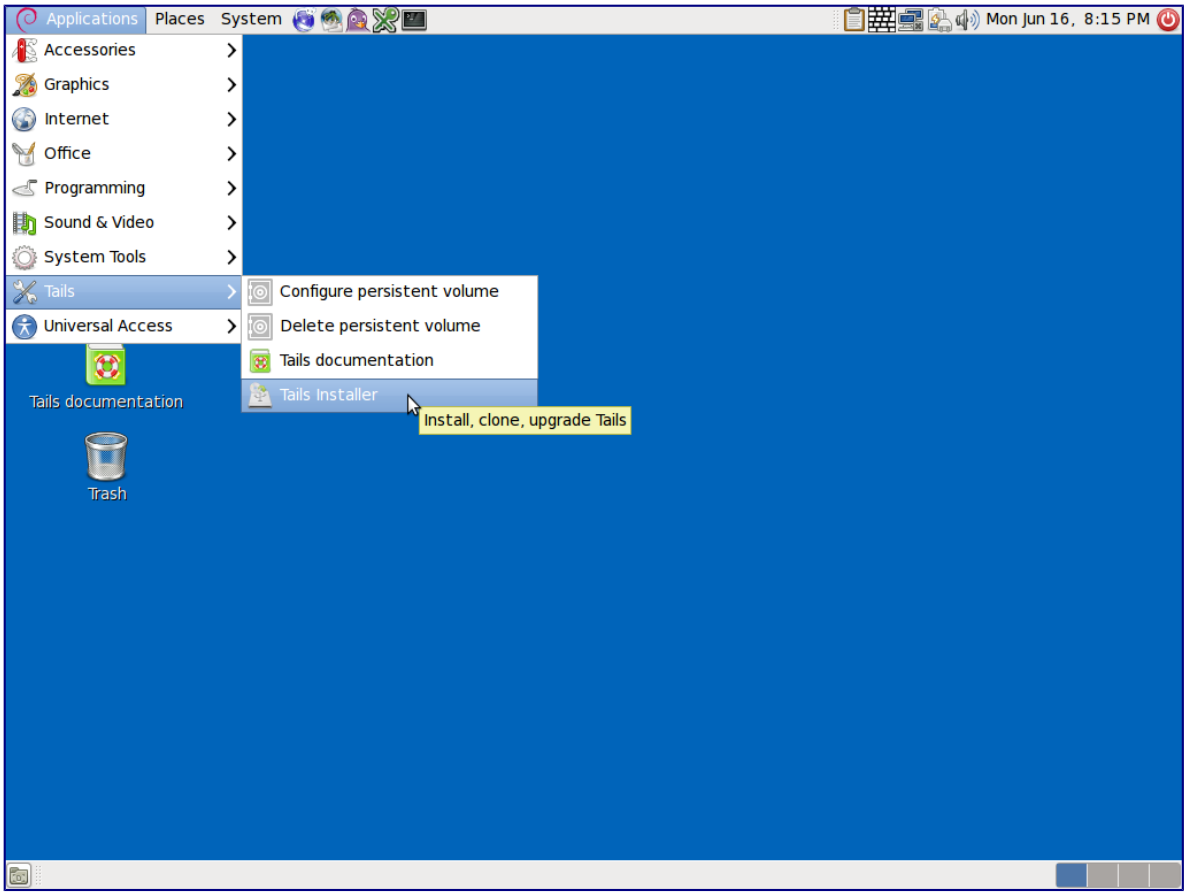
1. Instala Gparted
   Ve al Ubuntu Software Centre (Centro de Software de Ubuntu) en tu ordenador, y busc
2. Inserta tu USB en el laptop
3. Abre GParted. Ve a GParted > Refresh Devices (Refresca Dispositivos)
4. Tu USB debería aparecer como dispositivo en el menú desplegable en la parte superior derecha (p.ej. listado como /dev/sdb o dev/sdc) y mostrará el espacio disponible en la memoria USB. Selecciona este dispositivo
5. Ahora hay un rectángulo alargado en la parte superior de la ventana, perfilado de verde, posiblemente con un espacio a la derecha del rectángulo sombreado de amarillo. Haz clic con el botón derecho, selecciona ‘unmount’ (desmontar); haz clic con el botón derecho otra vez y selecciona ‘delete’ (borrar)
6. Todos los colores del rectángulo han desaparecido y han sido reemplazados por gris. Haz clic con el botón derecho en el rectángulo, y selecciona ‘New’ (Nuevo)
7. Aparece una pantalla llamada ‘Create new Partition’ (Crear nueva Partición). Bajo ‘File System’ (Archivo de Sistema) selecciona ‘fat32’, y bajo ‘Label’ (Etiqueta) escribe ‘TAILS’. Haz clic en ‘Add’ (Agregar).
   fat32 = File Allocation Table 32 bits (Tabla de Asignación del Archivo 32 bits)
8. Haz clic en el ‘tick’ verde (justo abajo de la opción ‘Partition’ (Partición) en la barra de herramientas en la parte superior de la ventana)
9. En la caja emergente, selecciona ‘Apply’ (Aplicar) para aplicar todas las operaciones al dispositivo, y ‘Close’ (Cerrar) cuando el mensaje aparezca: “All operations successfully completed” (Todas las operaciones completadas con éxito)
10. Ahora, haz clic con el botón derecho en el rectángulo largo verde y haz clic en ‘Manage Flags’ (Gestionar Opciones)> selecciona ‘boot’ (iniciar), y cierra
    Esto le dirá al ordenador que este lector puede ser usado para iniciar el sistema desde él

Puedes retirar el USB de forma segura. ¡Está listo para Tails!

1. Clonar Tails en memoria USB

Si has recibido un USB con Tails clonado, todo lo que tienes que hacer es programar tu ordenador para iniciar desde el lector USB (ver página 32), e insertar tu USB con Tails para empezar.
Podrás entonces usar tu memoria USB con Tails para crear una memoria USB con Tails nueva, esto puede ser particularmente útil para proporcionárselo a fuentes y colegas.

1. Prepara un nuevo USB limpio, arrancable con GParted, como antes (página 34), al que clonar Tails. Este lector tiene que ser como mínimo de 4GB para contener una instalación de Tails, pero idealmente 8GB o más
2. Inicia el sistema Tails con tu memoria USB actual
3. Introduce el dispositivo USB limpio e arrancable en uno de los puertos USB libres en el ordenador
4. En el escritorio o desktop de Tails ve a Applications > Tails > Tails Installer (Aplicaciones > Tails > Instalador de Tails).



5. Se abrirá una ventana nueva. Selecciona: Clone & Install (Clona & Instala)
6. La ventana del Instalador de Tails debería de listar tu memoria USB limpia. Haz clic en ‘Install Tails’ (Instala Tails) en la base de la ventana y haz clic en ‘Yes’ (Sí) en la ventana emergente para confirmar la selección del dispositivo. Ahora se hará un clon de tu instalación de Tails en la otra memoria USB.
   Cuando haya terminado el Instalador de Tails te dirá: Installation complete! (¡Instalación completa!)
7. Cuando esté completado, apaga el sistema y trata de iniciar desde el nuevo lector creado para asegurarte de que funciona correctamente.

2. Instalar Tails manualmente vía UNetbootin

1. *Descarga Unetbootin*
   Descarga UNetbootin 494 para Linux (unetbootin-linux-494) aquí:
   https://sourceforge.net/projects/unetbootin/files/UNetbootin/494/
   N.B. La página a la que lleva el enlace de arriba también te ofrecerá la versión más actual de UNetbootin, sin duda un número más alto que 494. Sin embargo, asegúrate de bajar la versión 494 para Linux para que la instalación de Tails funcione.

   Cuando la descarga esté completa, haz clic con el botón derecho en el archivo de UNetbootin y selecciona 'Properties' > Permissions tab (Propiedades > Pestaña de Permisos) > Marca la caja de al lado de 'Execute' (Ejecuta) para 'Allow executing file as program' (Permitir la ejecución de archivo como programa)

2. *Lanzar Unetbootin*
   Abre la 'Terminal' (usa la herramienta de búsqueda en Ubuntu, el icono en la parte superior derecha de la pantalla, si no puedes encontrar la Terminal). Es una caja negra con una entrada de comando que dice: user@

   > Escribe:
   cd Downloads
   (o cd Descargas si el idioma del sistema operativo es castellano)

   (Asumiendo que Tails y UNetbootin están dentro de la carpeta Downloads) y presiona Enter.
   Nota: las instrucciones son sensibles a mayúsculas y minúsculas: asegúrate de dejar un espacio después de 'cd' y que la D en Downloads sea mayúscula.

   > Escribe sudo ./ seguido por el nombre del archivo de tu descarga de UNetbootin. Que será probablemente así:

   sudo ./unetbootin-linux-494

   y presiona Enter (asegúrate de dejar un espacio después de 'sudo'). Puede que te pida tu contraseña, introdúcela (tu tecleado de la contraseña no va a ser visible en el Terminal, pero escríbela de todas maneras y presiona Enter).

   UNetbootin debería lanzarse.

3. *Haz la copia*
   Inserta el USB preparado. En UNetbootin, selecciona el botón redondo al lado de 'Diskimage' (Imagen de disco). Selecciona el archivo de imagen del disco presionando en el paréntesis (…) a la derecha de la ventana. Abre Downloads (Descargas) (dando por hecho que allí es donde está guardada tu descarga de Tails), y selecciona el archivo .iso de Tails. Bajo 'Type' (Tipo) selecciona 'USB drive' (Memoria USB), y bajo 'Drive' (Dispositivo), selecciona la ubicación del USB (probablemente es /dev/sdc, o similar, pero es muy importante que tengas esta ubicación correcta – en GParted, habrás visto la ubicación de tu lector bajo

‘partition’ (partición)). Si no muestra nada bajo ‘Drive’, espera un momento, o prueba a marcar o desmarcar la casilla de ‘show all drives’ (enseña todos los lectores).

Haz clic en OK.

Cuando la copia esté completa, sal de UNetbootin en vez de reiniciar, y cierra la Terminal también. Retira el USB de manera segura y apaga el sistema.

¡Has terminado! Una vez hayas dispongas tu ordenador para iniciarse desde el USB (ver página 32), puedes empezar con Tails desde tu memoria USB.

3. Instalar Tails manualmente vía Linux

Ver también:
https://tails.boum.org/doc/first_steps/installation/manual/linux/index.en.html

1. Averigua el nombre del dispositivo para la memoria USB

   El ‘nombre del dispositivo’ se refiere a la forma en que tu ordenador ha identificado la memoria y debería de ser algo como /dev/sdb, /dev/sdc1, etc. Si no estás seguro/a del nombre exacto del dispositivo, haz lo siguiente:

   1. Asegúrate de que el USB al que quieres copiar Tails esté desenchufado.
   2. Abre GNOME Disk Utility (Utilidad del Disco) desde el menú Applications ▸ System Tools ▸ Disk Utility (Aplicaciones ▸ Herramientas del Sistema ▸ Utilidad del Disco) (si no puedes encontrarlo, usa la función de búsqueda de Ubuntu, el icono en la parte superior izquierda, para localizarlo con la búsqueda ‘GNOME’).
   3. ‘Disk Utility’ lista todos los dispositivos de almacenamiento actuales en la sección izquierda de la ventana.
   4. Inserta el USB al que quieres copiar Tails. Un dispositivo nuevo aparecerá en la lista de dispositivos de almacenamiento. Haz clic en él.
   5. En la sección derecha de la ventana, verifica que el dispositivo corresponda con el tuyo, la marca, tamaño, etc.

      En esta captura de pantalla, el USB es un Kingston DataTraveler de 2.0 GB y su nombre de dispositivo (Device) es /dev/sdc. El tuyo será diferente.

      Si aún no estás seguro/a del nombre del dispositivo, deberías de detenerte o te arriesgas a sobrescribir tu disco duro interno.

2. Localiza Tails

   Encuentra la descarga de Tails, haz clic con el botón derecho, y selecciona ‘properties’ (propiedades). Deberías de ver la ubicación del archivo (p.ej. /home/amnesia/Desktop/tails-0.6.2.iso) – guarda una nota de esta.

3. Enchufa el USB
4. Instala isohybrid

   Si usas Ubuntu, la utilidad ‘isohybrid” debería estar incluida en tus paquetes de software. Para comprobarlo, o en efecto instalarlo, abre ‘Terminal’ (si no puedes encontrar Terminal, usa la función de búsqueda de Ubuntu, el icono en la izquierda superior). Es una caja negra con una entrada de comando que dice: usuario@

   Escribe lo siguiente cuidadosamente en la Terminal, antes de presionar Enter:

   sudo apt-get install syslinux
   Nota: las instrucciones de Terminal, como de más arriba, son sensibles a las mayúsculas y se deben escribir exactamente.

5. Haz la copia
   En la Terminal, escribe el siguiente comando, reemplazando [tails.iso] con la ubicación de Tails que encontraste en el paso 2, y reemplazando [device] con el nombre del dispositivo que encontraste en el paso 1.

   sudo dd if=[tails.iso] of=[device] bs=16M && sync

   He aquí un ejemplo de mando a ejecutar (el texto en negrita significa la sección que será diferente en tu caso).

   sudo dd if=/home/amnesia/Downloads of=/dev/sdb bs=16M && sync

   Puede que te solicite tu contraseña, introdúcela (es posible que tu tecleado de la contraseña no sea visible en la terminal, pero escríbelo de todas maneras y presiona Enter).

   A menos que veas un mensaje de error, Tails se estará copiando al dispositivo. Todo el proceso puede llevar algo de tiempo, generalmente unos minutos. Recibirás un mensaje en la terminal diciéndote que la instalación se ha completado, o puede que la entrada de comando simplemente reaparezca cuando esté completa. Puedes apagar tu ordenador y empezar Tails desde el dispositivo nuevo.

Troubleshooting (Solución de problemas)

dd: /dev/sdx: No such file or directory (No existe el fichero o el directorio)
Revisa el nombre del dispositivo que encontraste en el paso 1. Si no estás seguro de la ruta a tu descarga de Tails o si te da el mensaje de error (No such file or directory), puedes escribir primero dd, seguido por un espacio y después arrastrar el icono de tu descarga de Tails desde el navegador de archivos y dejarlo caer en la Terminal. Esto debería de inserir la ruta correcta a tu descarga de Tails en Terminal. Después completa el

comando y ejecútalo.

dd: /dev/sdx: Permission denied (Permiso negado)
Puede que hayas cometido un error con el nombre del dispositivo, por favor, revísalo. Si estás seguro/a del nombre del dispositivo, este podría ser un problema de permiso denegado y podrías necesitar lograr privilegios administrativos antes de poder ejecutar los comandos en la terminal (esto se resuelve, generalmente, incluyendo 'sudo' en la instrucción, como se ha indicado anteriormente).

dd: tails.iso: No such file or directory (No existe el fichero o el o el directorio)
Puede que hayas cometido un error con el nombre de la ruta hacía el archivo de tu descarga de Tails en el paso 2.

Actualizar Tails
Tails (si se ha hecho con el instalador de Tails, es decir un sistema de Tails clonado) debería buscar y descargar actualizaciones automáticamente. Después de iniciar Tails y conectarte a Tor, si hay una actualización disponible, aparece una caja de dialogo y propone que actualices tu sistema.
Sin embargo, a menudo puede llevar un poco de tiempo hasta que Tails se conecte a internet después de iniciarse, en cuyo caso puede que no sea capaz de buscar actualizaciones al principio. Puedes revisar si hay actualizaciones en cualquier momento abriendo el Terminal (icono de caja negra en la barra de herramientas superior en el escritorio de Tails) y tecleando el siguiente comando:

tails-upgrade-frontend-wrapper

Y presiona Enter. Tails revisará si hay actualizaciones, o te informará si tu sistema está al día.
Nota: si tu versión de Tails se hizo manualmente usando UNetbootin o tu sistema Linux, en lugar de clonar otro sistema Tails, no se actualizará. En este caso, deberías consultar la página web de Tails para las actualizaciones y, si hay una versión nueva disponible, crear un nuevo USB de Tails . Cada vez que haces una instalación manual de Tails, deberías de clonarlo a una memoria USB nueva y usar esa copia, ya que ésta se actualizará automáticamente y te permitirá crear un volumen permanente.

Usar Tails
Primero, debes hacer que tu laptop se inicie desde el lector USB. Ver página 31 de las instrucciones.
Cuando inicies en Tails, verás una pantalla con las opciones 'Live' (En Vivo) y 'Live failsafe' (En Vivo a prueba de fallos). Usa las teclas con flechas para escoger 'Live' y presiona le tecla de Enter.

Después te ofrecerá, 'More options?'(¿Más opciones?). No es esencial que entres en este menú a menos que necesites configurar Tails para evitar la censura a Tor. De otra manera puedes seleccionar no y 'Login' (Ingreso).

Si seleccionas sí para más opciones, verás:

‘Administrative password’ (Contraseña administrativa). Es improbable que necesites crear una, a no ser que quieras acceder al disco duro interno del ordenador (que no está recomendado y puede dar lugar a riesgos de seguridad innecesarios).

‘Windows camouflage’ (Camuflaje Windows). Si activas el camuflaje ‘Activate Microsoft Windows (version) camouflage’, Tails se verá más similar al sistema operativo de Windows. Esto puede ser útil en lugares públicos si crees que el SO Tails puede ser reconocido o generar sospechas.

‘Spoof all MAC addresses’(Burla todas las direcciones MAC), debería seleccionarse automáticamente. Esta es una buena opción para esconder todos los números de serie en tus tarjetas de red, y por lo tanto es otra función que ayuda a esconder tu ubicación.

‘Network configuration’ (Configuración de red), bajo la cual tienes dos opciones: connect directly to the Tor network (conectar directamente a la red de Tor), o ‘This computer’s internet connection is censored, filtered or proxied. I need to configure bridge, firewall or proxy settings’(La conexión a internet de este ordenador está censurada, filtrada o con proxy. Necesitas configurar un puente, contrafuegos o detalles de de proxy). Si tu red no permite la conexión a Tor, selecciona la segunda opción.

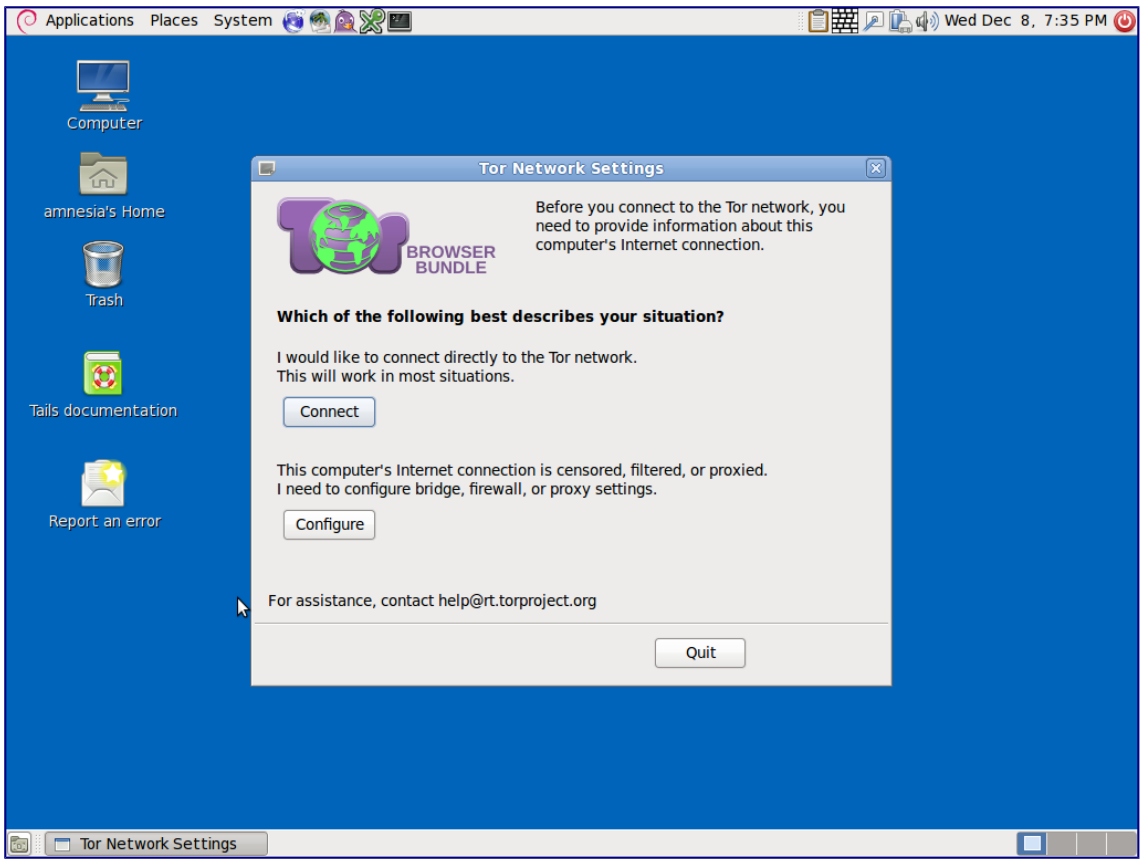
Usar Tails vía puentes/eludir la censura

Esto ayuda a la gente a conectarse a la red de Tor en situaciones donde su conexión no permite conexiones a Tor. Puentes son transmisores de Tor (nodos o ordenadores que reciben tráfico en la red de Tor y lo transmiten) que ayudan a eludir la censura.

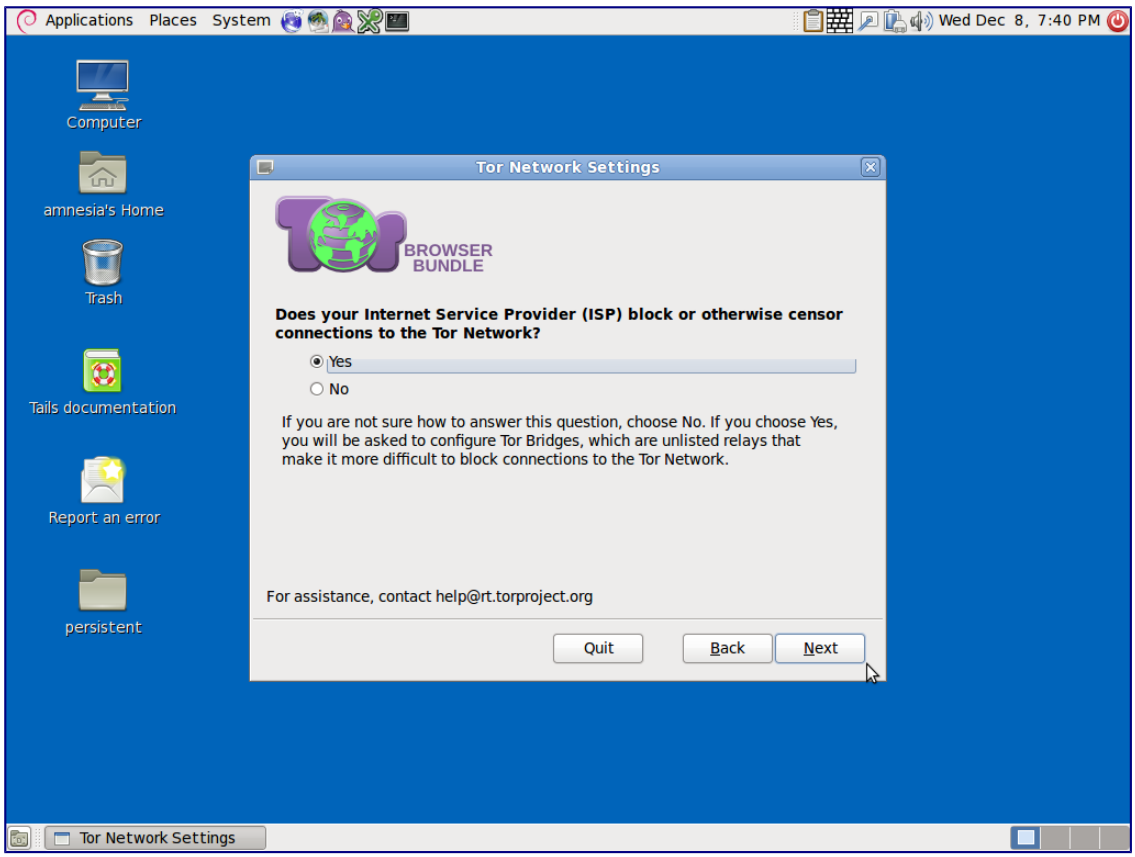
Cuando inicias usando el USB con Tails y te ofrece ‘More options?’(¿Más opciones?), selecciona ‘Yes’ (Sí) y continúa.

Bajo *‘Network configuration’* (Configuración de red), selecciona *‘This computer’s internet connection is censored, filtered of proxied. I need to configure bridge, firewall or proxy settings’* (La conexión a internet de este ordenador está censurada, filtrada o con proxy. Necesitas configurar un puente, cortafuegos o detalles de proxy).

Después, cuando te conectes a Internet, aparecerá la ventana de tu navegador Tor haciéndote la misma pregunta.



Si la segunda opción es relevante, haz clic en *'Configure'* (Configurar). Te preguntará si necesitas (usar un proxy para acceder a internet) use a proxy to access the internet, selecciona *'No'*; después, si tu ordenador (tiene la conexión a internet por medio de un cortafuego que solo permite conexiones a ciertos puertos) internet connection goes through a firewall that only allows connections to certain ports – selecciona *'No'*; a continuación, si tu (ISP obstruye / censura conexiones a la red Tor) ISP blocks / censors connections to the Tor network. Si necesitas configurar puentes, selecciona 'Yes' (Sí) aquí y presiona 'Next' (Próximo).



Ahora tienes un recuadro para rellenar uno o más 'bridges' (puentes) –secuencias de números que identifican un Tor relay (repetidor puente). Para conseguir puentes, ve a https://bridges.torproject.org o, si no puedes acceder a la página web, escribe un correo a bridges@torproject.org desde una cuenta gmail.com o yahoo.com, con la línea *'get bridges'* (obtener puentes) en el cuerpo del mensaje y te deberían enviar algunos. Usar un puente puede ser una forma sumamente lenta de conectarse a internet, pero si necesitas sortear censuras, funciona muy bien.

Crear un volumen persistente en Tails

Crear un espacio de almacenamiento persistente en tu memoria USB con Tails.

Para crear un volumen persistente en Tails, ve a Applications > Tails > Configure persistent volume (Aplicaciones > Tails > Configurar volumen persistente. Una vez que hayas introducido una contraseña muy fuerte (ver capítulo 8), puedes escoger qué tipo de archivos guardarás en el volumen persistente. Podrías seleccionar todos los tipos para mantener tus opciones abiertas.

Ahora, cada vez que arranques el USB con Tails, se te harán dos preguntas: 'Use persistence?' (¿Usar persistencia?) y 'More options?' (¿Más opciones?) (Como antes). Si haces clic en 'Yes' (Sí) para 'usar persistencia' y introduces la contraseña, puedes acceder a cualquier tipo de dato (p.ej. cliente de correo configurado, cliente de mensajería instantánea, gestor de contraseñas, o a archivos) que hayas guardado en el volumen persistente en sesiones previas.

Usar KeePassX
KeePassX es un gestor de contraseñas que guarda usuarios y contraseñas en una base de datos local encriptada, protegida por una contraseña maestra. También viene con PWGen, un generador de contraseñas aleatorias fuertes. Encontrarás el KeePassX en Applications > Accessories > KeyPassX (Aplicaciones > Accesorios> KeyPassX).

Para crear un nuevo banco de datos para contraseñas:
File > New database (Archivo > Nuevo banco de datos). Crea una contraseña maestra fuerte que protegerá tu banco de datos. Después puedes nombrar tu archivo de datos y elegir la ubicación en la que se guardará.

Groups > New groups (Grupos > Grupos nuevos) (p.ej. grupo 'Jabber', para tus usuarios y contraseñas de Jabber – más sobre Jabber en el capítulo 6).

Para agregar una contraseña nueva:
Haz clic en un grupo > Entries > Add new entry (Inscripciones > Agregar nueva inscripción). Aquí tienes la opción de introducir una contraseña, o generar una al azar (haz clic en 'Gen'). Si haces clic en el icono del ojo, podrás ver los caracteres de la contraseña, si no permanecerá oculto.

Para extraer una contraseña:
Cuando has agregado una contraseña a un grupo, puedes hacer un clic con el botón derecho sobre la contraseña deseada y seleccionar 'copy password to clipboard' (copiar contraseña al portapapeles). Después puedes pegarla en un formulario de inicio de sesión.

Correo electrónico en Tails
Deberías de leer el capítulo 5 sobre encriptación de correo antes de continuar leyendo el resto del capítulo.

Importar tu clave de otro laptop/sistema operativo
Mucha gente usa una memoria Tails, dirección de correo, clave, etc. separada, para proyectos diferentes, que es una manera genial de trabajar con seguridad y compartimentar tus actividades. Sin embargo, quizá quieras agregar una clave generada en otro laptop a tu gestor de claves en Tails (pero ten en cuenta si esto podría comprometer tu anonimato en Tails). Para esto, necesitaras un USB extra.

Inserta un USB en el laptop que tiene la clave que deseas mover. Abre Thunderbird, y ve a Enigmail > Key management (Gestión de claves). Encuentra tu dirección de correo/llave en tu lista de contactos y haz clic con el botón derecho en ella para seleccionarla > Export keys to file > Export secret keys (Exportar llaves a archivo> Exportar claves secretas). Encuentra tu dispositivo USB y selecciónalo como la locación en donde guardar tu llave. Remueve la memoria USB de forma segura.

Inicia tu sistema Tails. Una vez que Tails haya iniciado y se haya conectado a Internet, inserta el dispositivo USB con tu llave guardada en él. Haz clic en el applet de encriptación OpenPGP de Tails (el icono de portapapeles a la derecha superior de la barra de menú) > File > Import (Archivo > Importar). Abre los archivos de tu USB para encontrar

la llave a importar y selecciona Import (Importar).

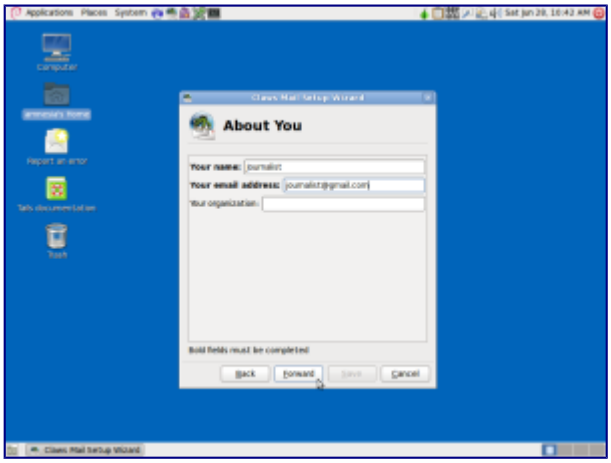
Cuando hayas importado tu clave a Tails, puede que desees borrar de forma segura la llave del USB que has usado para transportarla, ya que no es prudente tener tu llave secreta guardada en un USB desprotegido. Con la función ‘Wipe’ (Limpiar) en Tails (haz clic con el botón derecho sobre el archivo en el dispositivo USB) se borrará el archivo de forma segura.

> Claws

Tails viene con un cliente de correo para escritorio pre instalado, Claws. Puedes usarlo para configurar tu cuenta de correo con un plug-in GPG para mandar correos encriptados, de manera muy similar a como puedes configurar Thunderbird en tu sistema operativo regular (ver capítulo 5).

Configurar tu cuenta de correo con Claws

1. Usa el set up wizard (asistente de instalación) de Claws, introduce tu nombre (si lo deseas) y tu dirección de correo.
   Por favor toma nota de que muchos servidores de correo no funcionan bien con la red Tor, en cuyo caso la configuración de Claws podría no funcionar. Puedes utilizar o probar un proveedor de correo diferente, o ver ‘Otras formas de encriptar en Tails’ abajo.

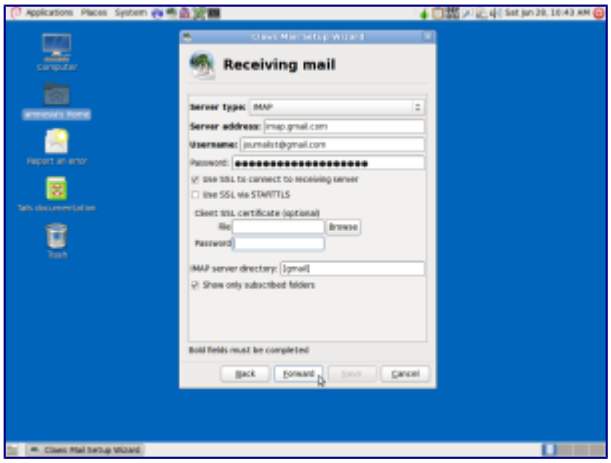


2. Recibir correo
   Para recibir correo, tienes las opciones de tipo de servidor POP3 o IMAP.
   Información del Experto: A diferencia de POP, IMAP ofrece comunicación de dos vías entre tu cuenta de correo online y tu cliente de correo en el escritorio, de manera que cualquier cambio que haces en el cliente de correo se aplica a tu cuenta online (p.ej. si marcas un correo como ‘leído’ en Claws Mail con IMAP, aparecerá como ‘leído en tu correo web también).

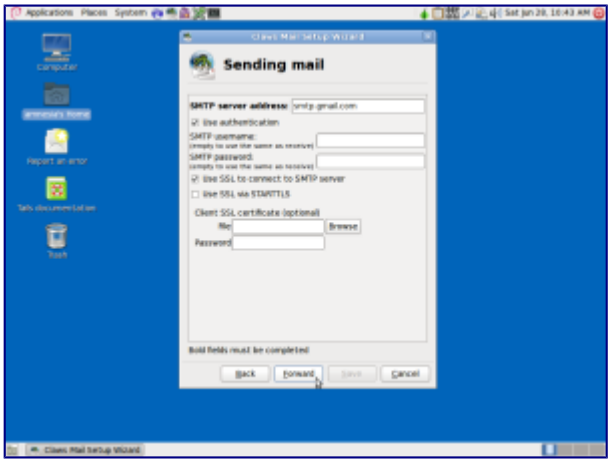
   ADVERTENCIA: Desarrolladores de Tails han descubierto recientemente que Claws Mail filtra la versión de texto simple de correos encriptados al servidor IMAP, haciendo que tu correo ‘encriptado’ sea potencialmente legible si es interceptado. Por esto, recomendamos que encriptes tus mensajes manualmente en un editor de

texto y después lo pegues en Claws Mail (ver ‘Otras formas de encriptar correos en Tails – Applet de encriptación OpenPGP). Otra opción, configurar tu correo en POP3.
En función de si has escogido IMAP o POP3, deberás buscar en la red la correcta dirección IMAP o POP3 del servidor de correo de tu proveedor. Bajo ‘username’ (nombre de usuario) teclea tu dirección de correo entera.

Puedes introducir la contraseña o dejarla en blanco (en cuyo caso la solicitará cada vez que la contraseña es necesaria).
El ‘IMAP server directory’ (directorio de servidor IMAP) es opcional y se puede dejar en blanco.



3. Enviar correos
   También necesitarás buscar online la dirección del servidor SMTP de tu proveedor de correo, e introducirlo aquí.



4. ¡Configuración terminada!
   Ahora ya puedes abrir Claws, configurar una encriptación, fabricar un par de llaves y cambiar tus configuraciones.

Configurar Claws para encriptación
Claws debería ya tener instalados los plug-ins para encriptación, pero para verificar:
En Claws, ve a Configuration > Plugins > PGPcore > Load (Configuración > Plug-ins > PGPnúcleo > Cargar)

Aparece una ventana nueva, ‘Select the plugins to load’ (Selecciona los complementos a cargar): selecciona ambos PGPcore y PGPinline (mantiene presionado ‘Ctrl’ para poder seleccionar múltiples opciones), y haz clic en Open (Abrir).

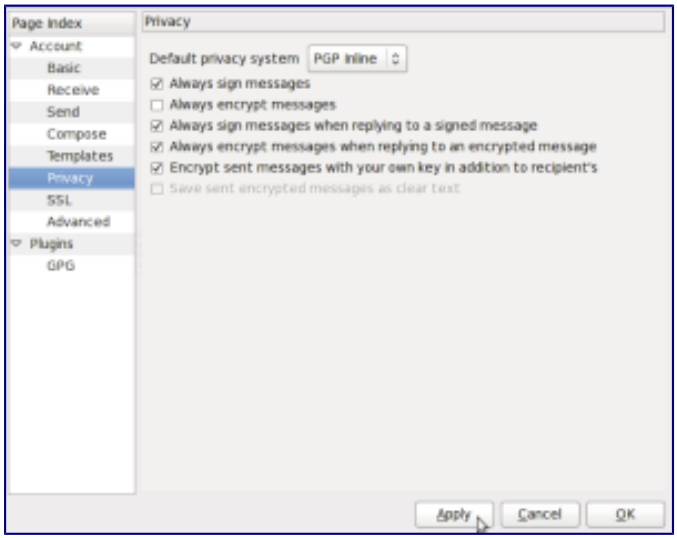
Fabricar un par de llaves
En Claws, ve a Configuration > Preferences for current account > GPG (Configuración > Preferencias de cuenta corriente > GPG) (bajo Plug-ins).

– Escoge ‘Select key by your email address’ (Selecciona llave por medio de tu dirección de correo).
– Si todavía no has creado un par de llaves para la dirección de correo, haz clic en ‘Generate a new key pair’ (Generar un par de claves nuevas).

- Te pedirá que introduzcas la frase de contraseña para esa dirección de correo (dos veces) y después la llave se empezará a generar.
- Mueve tu ratón alrededor de la pantalla mientras se genera la llave para aumentar la aleatoriedad.
- Una vez completado, una ventana aparecerá con el mensaje ‘Key generated’ (clave generada) y preguntando ‘Do you want to export it to a key server?’ (¿Deseas exportarlo a un servidor de llaves?). Si deseas que la llave sea públicamente accesible (es como listar tu número en una guía telefónica), para que las personas puedan encontrar tu llave y mandarte correos encriptados, selecciona ‘Yes’ (Sí).

Verificar tu encriptación y opciones de firma
En Claws, ve a Configuration > Preferences for current account > Privacy (Configuración > Preferencias de cuenta corriente > Privacidad) (en el menú a mano izquierda).

– Pon el ‘privacy system’ (Sistema de privacidad por defecto) en ‘PGP Inline’.
– Puede que quieras marcar ‘Always sign messages’ (Siempre firma mensajes).
– También deberías de marcar ‘Encrypt sent messages with your own key in addition to recipient’s’ (Encripta mensajes enviados con tu propia llave además de la del destinatario) para que puedas decriptar y leer tus mensajes enviados.
– Cuando hayas hecho tu selección, haz clic en ‘Apply’ (Aplica).



Todas las otras configuraciones por defecto en Claws deberían de estar bien. Quizá quieras cambiar la frecuencia con que Claws busca nuevos mensajes. Hazlo aquí por medio de:
Configuration > Preferences > Mail handling > Receiving (Configuración > Preferencias > Gestión de correo > Recibir).

> Otras formas de encriptar correos en Tails – applet de encriptación OpenPGP

Ya que *todas* las conexiones a internet en Tails van por medio de la red Tor, las conexiones a tu proveedor de correo desde tu cliente también irán por medio de Tor. Los usuarios de algunos proveedores de correo a veces tienen problemas al configurar sus cuentas de correo con Claws por medio de Tails, porque la conexión es re-dirigida por medio de la red Tor para esconder su ubicación.

Tails ofrece un método alternativo que puedes usar para encriptar correos y archivos adjuntos del correo. En vez de usar un cliente de correo para encriptar el mail entero, puedes seleccionar un texto y encriptarlo con la clave del destinatario deseado, para luego pegarlo en el cuerpo de un mail (p.ej. al redactar un correo desde un interfaz web en el navegador).

Importar la llave pública del contacto

Ve al applet de encriptación OpenPGP (el icono de portapapeles en la derecha superior de la barra de menú) > Manage keys (Gestionar llaves) > después o bien:

Remote > Find remote keys (Remoto > Encuentra claves remotas) (si no conoces la llave de la persona). Introduce el nombre del contacto y haz clic en ‘Search’ (Búsqueda).
O
File > Import (Archivo > Importar) (si ya tienes la llave guardada en un archivo).

Encriptación del texto

Applications (‘Aplicaciones’ a la izquierda superior del menú de herramientas) > Accessories > gedit Text Editor (Accesorios > gedit Editor de Texto). Escribe tu mensaje. Después selecciónalo todo (Ctrl + A) y copia (Ctrl + C, o clic con el botón derecho > ‘copy’) el mensaje en el portapapeles. Ve al applet de encriptación OpenPGP > Sign/encrypt Clipboard with Public Keys (Firma/encripta portapapeles con Llaves Públicas) > selecciona el destinatario de tu correo (necesitas ya haber importado su llave), firma el mensaje con la dirección de correo que usarás para mandar tu correo y haz clic en OK. Después pega el mensaje (Ctrl + V) en la ventana de redacción de tu cuenta de correo y envíalo.

Ten en cuenta que has encriptado el mensaje, para que sólo el destinatario deseado pueda deshacer la encriptación. Esto quiere decir que una vez encriptado, no lo puedes desencriptar para leerlo tú. Por lo tanto, si usas este método, es una buena idea seleccionar tu propia llave pública, además de la del destinatario cuando encriptes el mensaje. Entonces podrás desencriptarlo si deseas leer tus mensajes enviados.

Desencriptar el texto

Selecciona el texto encriptado que deseas desencriptar. Incluye las líneas“—–BEGIN PGP MESSAGE—–“ (INICIO MENSAJE PGP) y “—–END PGP MESSAGE—–” (FIN MENSAJE PGP). Copia el texto al portapapeles (Ctrl + C, o clic derecho > ‘copy’). El applet OpenPGP (icono del portapapeles) muestra un candado, lo que significa que contiene texto encriptado. Si el texto que has seleccionado está sólo firmado pero no encriptado, el applet OpenPGP enseña un sello, lo que significa que el portapapeles contiene texto firmado.

Haz clic en el applet OpenPGP (icono portapapeles) y selecciona ‘Decrypt/Verify Clipboard’ (Decripta/Verifica Portapapeles) en el menú. El texto desencriptado aparece en el ‘Output’ (Producto) de la caja de texto GnuPG.

Encriptación de adjuntos del correo

Es fácil encriptar archivos usando llaves públicas y mandarlas por correo con Tails. Haz clic con el botón derecho en el archivo deseado > Encrypt (Encriptar) > marca la dirección de correo del destinatario (firma el mensaje como la dirección de la que mandarás el correo) > OK. Ahora verás una copia del archivo seleccionado, con la extensión ‘.pgp’, esto quiere decir que es un archivo encriptado. Adjunta el archivo .pgp en tu correo, que sólo puede ser desencriptado y abierto por el destinatario seleccionado.

Capítulo 3: Navegación Segura

Navegar por internet conlleva los siguientes riesgos:

- Que se obtengan tus datos personales.
- Que se recojan datos sobre tu comportamiento de navegación, entre ellos las páginas web que has visitado y cuándo.
- Que se obtengan tus contraseñas e información de auto-relleno.
- Que se obtengan datos sobre tu ubicación (o ubicaciones previas).
- Que se introduzca malware en tu ordenador (software malicioso, a veces spyware).
- Que se te bloquee el acceso a ciertos sitios.
- Que se te impida el uso de navegadores anónimos.

Acción de InfoSec:

- Usa un navegador de uso general con extensiones que refuercen la privacidad en tu actividad diaria.
- Usa el navegador Tor para navegar de forma anónima, evitar la censura y esconder tu ubicación real.

Un navegador es el software que usas para acceder a la World Wide Web (Red Informática Mundial). Para muchos de nosotros, navegar es 'Internet' y, en muchos sentidos, es una ventana al mundo.

Dadas las enormes oportunidades de navegación en internet, algunos estados imponen restricciones de acceso a ciertos sitios, lo cual coarta la libertad de las personas y por supuesto, supone un problema a los periodistas locales, investigadores y corresponsales extranjeros. Mientras el acceso a la red en Occidente no está propiamente restringido, tenemos serios problemas de privacidad con nuestra navegación en internet. La mayoría de proveedores y páginas web siguen recogiendo gran cantidad de información sobre sus usuarios.

Este capítulo explica algunas opciones para minimizar las restricciones sobre la libertad y privacidad en la navegación en determinadas circunstancias.

¿Qué navegadores usar?

Mucha gente no es consciente de los problemas de privacidad que tienen los navegadores y usa cualquier navegador que ya esté instalado en su sistema. Sin embargo, hay alternativas que son más seguras en general y que pueden mejorarse mucho añadiendo 'extensiones', software adicional que mejora la funcionalidad de tu navegador.

Aunque existen decenas de navegadores con fines especializados, aquí recomendaremos tres navegadores de código abierto:

1. Firefox, como navegador de uso general para Linux y Windows.

2. Chromium, como navegador de uso general para Mac.
3. Tor, como navegador seguro que hace que oculta tu ubicación e identidad (apto para Linux, Windows y Mac).

Información del experto: La razón por la que recomendamos Firefox para Linux y Windows, pero no para Mac, es que Firefox a veces da problemas con Tor en un Mac (porque Firefox y Tor están basados en el mismo código).

Navegador de uso general

El uso de internet en el día a día se centra generalmente en páginas web no restringidas y en páginas en las que tienes que iniciar sesión, como las plataformas de redes sociales, LinkedIn, periódicos, YouTube, tiendas, etc. No tiene sentido usar Tor en páginas en las que has iniciado sesión con tu identidad real, a menos que tu mayor preocupación sea ocultar tu ubicación real (en cuyo caso deberías usar el sistema operativo Tails).

Firefox
Un conocido navegador de código abierto.

En Windows, descarga Firefox para tu sistema operativo y en tu idioma en www.getfirefox.com.
En distribuciones Linux /Ubuntu, Firefox debería ya estar instalado.

Chromium
Un clon Google Chrome de código abierto sin los servicios adicionales de Google.
Descarga Chromium para Mac en
http://www.macupdate.com/app/mac/36244/chromium
(Otra opción: ve a www.macupdate.com y busca Chromium)

Extensiones
Por supuesto, un navegador de uso general mostrará tu identidad y ubicación. Sin embargo, podemos usar algunas extensiones para evitar:

– Que rastree tu comportamiento de navegación.
– Que se guarden y filtren tus contraseñas e información de auto-relleno.
– Que se permitan ataques por intermediario o se introduzca malware.

En https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/, puedes encontrar extensiones variadas para aumentar tu privacidad que deberían ser aptas tanto para Firefox, como para Chromium.

Nosotros recomendamos en especial las siguientes extensiones de código abierto:
HTTPS Everywhere: fuerza la encriptación de todas las conexiones entre tu navegador y el servidor web que estás visitando.
https://www.eff.org/https-everywhere

NoScript: bloquea JavaScript. JavaScript es un elemento esencial de muchas páginas web, pero puede usarse para rastrear tu comportamiento de navegación, filtrar tus contraseñas e introducir malware. NoScript es muy efectivo, pero tendrás que concederle

o negarle privilegios según qué página sea, dependiendo de si son de confianza o no.
https://noscript.net/

Ghostery: bloquea una amplia gama de rastreadores que se encuentran su base de datos y que vigilan tu comportamiento de navegación. Asegúrate de desactivar 'GhostRank' en Settings > Options (Configuración > Opciones), ya que envía información con fines comerciales.
https://ghostery.com

Web Of Trust: es una base de datos de clasificaciones de páginas web. Te dirá si otros usuarios consideran o no de confianza una página.
https://www.mywot.com/

LastPass: es un generador y gestor de contraseñas para Firefox.
https://lastpass.com/

Tor
https://www.torproject.org/

Sobre Tor
El navegador Tor se diseñó especialmente para mantener el anonimato, pues redirige todo su tráfico a través de la red de Tor ('The Onion Router').

Se trata de una red mundial de ordenadores llamados nodos Tor, que mantienen entre sí conexiones encriptadas. Cuando se inicie el navegador Tor, se conectará a uno de estos nodos. Este nodo se conectará con un segundo nodo que a su vez se conectará con un tercer nodo. Estos nodos podrían estar en cualquier lugar del mundo, y el primer y tercer nodo no conocen la existencia el uno del otro. El tercer nodo se conectará a internet en general y mostrará las páginas web de los portales que visitas. Esos portales no podrán ver quién eres ni dónde estás (siempre y cuando no te identifiques iniciando una sesión con servicios asociados a tu identidad real).

Puesto que el navegador Tor gestiona su tráfico en diferentes lugares de todo el mundo, es más lento que un navegador normal, pero este es un precio que vale la pena pagar por estar en la red de manera anónima.

Con el fin de afianzar la seguridad del navegador, Tor activa automáticamente HTTPS-Everywhere y evita automáticamente extensiones como Flash, RealPlayer y QuickTime. Debido a esto, y a las limitaciones de velocidad, servicios como YouTube no funcionarán en el navegador Tor, tendrás que utilizar tu navegador habitual.

Superar las restricciones
Si el proveedor de red que usas (puede ser en todo el país o sólo en una red Universitaria) bloquea el acceso a la red de Tor, puedes usar 'bridges' (puentes) para acceder.
Los puentes son transmisiones 'privadas' de Tor (nodos u ordenadores que reciben tráfico en la red Tor y lo trasmiten) que tienen menos probabilidades de ser bloqueados y por lo tanto ayudan a evitar la censura.

Inicia el Tor Browser Bundle (Paquete de aplicación del Navegador Tor). En el Vidalia Control Panel, ve a Settings > Network > (Configuraciones > Red) activa ‘My ISP blocks connections to the Tor network’ (Mi ISP bloquea conexiones a la red Tor).

Ahora tienes una caja para insertar uno o más ‘bridges’ (puentes), secuencias de números que identifican una transmisión de Tor. Para conseguir ‘bridges’, ve a https://bridges.torproject.org o si no puedes acceder a esta página, envía un correo a bridges@torproject.org desde una cuenta con dirección de correo gmail.com o yahoo.com, escribe solamente ‘get bridges’ (recibir puentes) en el cuerpo del mensaje y recibirás algunos. El uso de puentes quizá sea una forma muy lenta de conectarte a internet, pero si lo necesitas para evitar censura, funciona muy bien.

Advertencias
La versión más reciente del navegador Tor incluye un control con una barra deslizante para determinar las opciones de seguridad. Dentro del navegador Tor, haz clic en la cebolla verde (a la izquierda de la barra de dirección) y selecciona ‘Privacy and Security Settings’ (Configuraciones de Privacidad y Seguridad) para ver la barra deslizante y varias opciones. La **barra deslizante está por defecto en el mínimo**, lo que aumenta su facilidad de uso. Para beneficiarte del alto nivel de privacidad que Tor ofrece, o si necesitas navegar de forma anónima, deberías arrastrar la barra al nivel máximo.

No abras documentos (como .doc y .pdf) descargados con Tor mientras estás en la red. Estos formatos de documento contienen elementos que pueden conectarse a internet de forma independiente, revelando así tu dirección IP real. Asegúrate de estar desconectado de internet primero o usa un ordenador diferente para trabajar con este tipo de documentos.

No uses bittorrent con Tor ya que este puede desvelar tu dirección IP real y consume cantidades desproporcionadas de la capacidad de la red Tor.

Asegúrate de que usas la versión más reciente del navegador Tor. La página inicial de Tor mostrará una alerta cuando haya actualizaciones disponibles, o puedes hacer clic en la cebolla verde en la ventana del navegador (a la izquierda de la barra de dirección) sobre ‘Check for Tor Browser update’ (Buscar actualizaciones para Tor).

Instalar Tor

Mac, Windows:
Descarga e instala el navegador Tor para tu sistema operativo en https://www.torproject.org/ siguiendo las instrucciones de instalación de la página.

Linux/Ubuntu:

1. Descarga el navegador Tor para Linux en https://www.torproject.org/ y selecciona ‘Guardar archivo’. Espera a que la descarga se haya completado.
2. En tu directorio de archivos, ve a Descargas (o donde hayas guardado tu descarga), haz clic con el botón derecho en la descarga de Tor y selecciona ‘Extraer aquí’. Abre el archivo extraído (p. ej. tor-browser_en-US), y haz clic en ‘Tor

browser setup’.

3. Ahora tienes la opción a ‘Connect’(Conectar) o ‘Configure’(Configurar). A menos que tu proveedor de red bloquee el acceso a la red de Tor (en cuyo caso, consulta nuestra sección previa ‘Superar restricciones’), selecciona ‘Connect’.
4. El navegador Tor debería iniciarse ahora. El icono de ‘Tor browser setup’ en tu directorio de archivos, debería ser ahora ‘Tor browser’, este es tu icono para iniciar Tor. Puedes arrastrar este icono al escritorio o fijarlo a la barra de programas para hacer el acceso a Tor más fácil.

Capítulo 4: Data

Riesgos:

- Pérdida
- Corrupción
- Interceptación
- Robo
- Recuperación de información ‘borrada’
- Metadatos desanonimizadores/comprometedores

Acciones de InfoSec:

- Copia de seguridad de información
- Encriptación de información
- Compartir información de forma segura
- Borrar información de forma segura
- Borrar metadatos

Cuando se guarda o transporta información, hay varios riesgos que requieren atención: interceptación/robo, pérdida, corrupción e incriminación. La diferencia entre intercepción y robo es la capacidad del dueño de detectarlo. Intercepción normalmente significa que se ha hecho una copia de la información de manera encubierta, mientras que robo sugiere que se ha hurtado el aparato de almacenamiento (ordenador portátil, USB o disco duro) que contenía esta información o datos originales. El segundo caso sería detectable, pero el primero puede que no lo sea.

Si la información delicada cae en manos de adversarios, las consecuencias para las fuentes del periodista pueden ser graves.

Hay varias opciones para proteger archivos digitales. Guardar el material en un aparato pequeño (USB, tarjeta de memoria o disco duro externo) y esconderlo puede ser efectivo en ciertos casos. En esta situación, la seguridad entera del material depende de que no se encuentre el aparato escondido.
Para proteger tu información en caso de que alguien acceda a ella de modo no autorizado, también es importante encriptarla. TrueCrypt es una herramienta fácil de usar encriptar archivos y discos enteros, y puede incluso ocultar su existencia.

TrueCrypt
TrueCrypt es software de encriptación de código abierto.
Descarga: https://truecrypt.ch/downloads/

En junio de 2014, la página web de TrueCrypt cambió de forma repentina: declaró que ya no era seguro usar el producto y aconsejó a los usuarios que cambiaran a BitLocker de Microsoft (que solo se puede usar en Windows, una plataforma cuya inseguridad es bien conocida). Se retiraron todas las versiones previas del software y se reemplazaron con una nueva versión, la 7. 2, que sólo puede desencriptar archivos de TrueCrypt ya

existentes.

Todavía se discute sobre qué pasó realmente, quién hizo los cambios en la web y por qué, pero hay consenso entre los expertos sobre la fiabilidad de la versión previa de TrueCrypt (ahora en la red en la nueva página web https://truecrypt.ch/).

Con TrueCrypt se puede crear un 'contenedor' encriptado que actúa como una caja fuerte para los archivos, cerrado por una contraseña. Una vez se ha creado esta caja fuerte y se han introducido los archivos, se puede mover a un dispositivo de almacenamiento externo como un USB, o enviar a otras personas en internet. Incluso si el archivo es interceptado, la caja fuerte no revela los contenidos a quien no tenga la contraseña (para escoger una buena contraseña, véase capítulo 8).

* *¡Importante! No olvides tu contraseña, no hay ninguna otra manera de acceder a tu información una vez se ha encriptado. ¡Perder la contraseña significa perder la información!**

Resolución de problemas al instalar TrueCrypt

TrueCrypt ya no se mantiene y actualiza. Por lo tanto, la última versión disponible del software quizá no es fácil de instalar en sistemas operativos posteriores a junio de 2014. Por ejemplo, algunos usuarios han informado de que les sale un mensaje de error cuando tratan de instalar TrueCrypt en Mac OS X Yosemite indicando que el sistema operativo es demasiado viejo (a pesar de ser el más nuevo). Si te encuentras con este problema, puedes probar lo siguiente:

1. Abre el archivo .dmg descargado de TrueCrypt.
2. Copia el paquete 'TrueCrypt 7.1a.mpkg' y pégalo en un directorio diferente. Podrás editar la versión nueva copiada.
3. Haz clic con el botón derecho en . mpkg copiado y selecciona 'Show Package Contents' (Mostrar los contenidos del paquete).
4. Edita el archivo Contents/distribution.dist (Contenidos/distribución. dist) en el editor de texto, como se muestra abajo:
   Antes, se veía esto:
   1 function pm_install_check() {
   2 if(!(system. version. ProductVersion >= '10. 4. 0')) {
   3 my. result. title = 'Error';
   4 my. result. message = 'TrueCrypt requires Mac OS X 10. 4 or later. ';
   5 my. result. type = 'Fatal';
   6 return false;
   7 }
   8 return true;
   9 }

   Borra todo el código 'if', para que quede así:

   1. function pm_install_check() {
   2. return true;

3. }

Guarda la copia nueva del .mpkg, y utiliza esta versión para instalar TrueCrypt.

Encriptar un archivo con TrueCrypt

1. **Descarga**
   Descarga TrueCrypt de truecrypt. ch e instálalo en tu sistema como cualquier otra aplicación.
   TrueCrypt funciona igual en los sistemas Windows, Mac y Linux y los contenedores encriptados son compatibles entre estos tres sistemas. Esto te permite trabajar de forma segura con otras personas sin tener que saber qué sistema están usando.
2. **Crear un volumen encriptado**
   Para crear un 'volumen' encriptado (como una carpeta), inicia el programa y haz clic en:

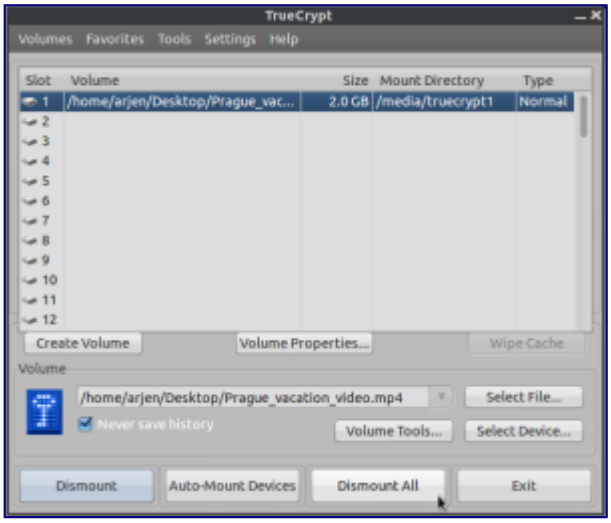
   - 'Create Volume' (Crear volumen) > 'Create an encrypted container' (Crear un contenedor encriptado) > selecciona 'Standard TrueCrypt volume' (Volumen TrueCrypt estándar) > selecciona la ubicación de tu ordenador en la que el contenedor se guardará (se podrá mover después) y dale un nombre (inocuo) al contenedor.
     Para encriptar un disco duro externo completo, como un USB, selecciona 'Create Volume' (Crear volumen) > Create a volume within a partition/drive' (Crear un volumen dentro de una partición/dispositivo)
   - La próxima pantalla se llama 'Encryption Options' (Opciones de rncriptación). Las opciones por defecto están bien. Para encriptar de la forma más segura (encripta múltiples veces), ve a 'Encryption Algorithm' (Algoritmos de encriptación), selecciona 'AES twoFish-Serpent'), y en 'Hash Algorithm' (Algoritmo de resumen criptográfico), selecciona SHA-512.
   - La próxima pantalla se llama 'Volume size' (Tamaño del volumen). Selecciona el tamaño del contenedor (esto determinará la máxima cantidad de información que puede guardarse en él).
   - Introduce la contraseña del volumen en la siguiente pantalla. Crea una que sea buena (ver capítulo 8) y ¡que no se te olvide!
   - La próxima pantalla se titula 'Format Options' (Opciones de Formato). Selecciona FAT.
     Información del Experto: FAT es compatible con todos los sistemas pero tiene limitaciones respecto al tamaño máximo de los archivos que puede contener (los archivos individuales no pueden ser mayores a 4 GB). Normalmente, no debería suponer ningún problema. Si necesitas poder guardar archivos mayores y estás seguro de que escoger algo diferente a FAT no creará problemas al compartir los archivos, escoge una de las otras opciones.
   - El programa generará un conjunto de información al azar para encriptar el

volumen. Mueve el ratón aleatoriamente un instante antes de hacer clic en ‘Format’. Ahora, el programa creará el volumen. En función del tamaño del algoritmo de encriptación escogido y la velocidad de tu ordenador, llevará desde unos segundos hasta unas horas (para volúmenes muy grandes).

- Cuando el sistema haya terminado, presiona ‘Exit’ (Salir) para regresar a la pantalla principal del programa. ¡Felicidades, has creado tu volumen seguro!

3. ***Poner los archivos que quieres encriptar en tu nuevo volumen encriptado***
   Ahora el volumen puede ‘montarse’ (activarse). Haz clic en ‘Select File’ (‘Seleccionar Archivo’ > localiza y selecciona el volumen que acabas de crear > Haz clic en ‘Mount’ (Montar).
   Ahora introduce la contraseña y haz clic en ‘OK’.

   El contenedor de TrueCrypt aparecerá como un lector separado en tu sistema (igual que un USB o disco duro externo), y puedes añadir archivos como lo harías en un USB (ve a ‘My Computer’ o ‘Finder’ y selecciona y arrastra los archivos al interior del contenedor).
   Cuando hayas metido los archivos deseados dentro del contenedor, ‘cierra’ el contenedor haciendo clic en ‘Dismount’ (Desmontar) en TrueCrypt. Parecerá que el contenedor es solo un archivo en tu ordenador.



Volúmenes encriptados escondidos

Los volúmenes ocultos son volúmenes encriptados que están de forma indetectable dentro de un volumen TrueCrypt normal. El fin de esto es poder alegar denegación plausible y que haya una capa más de protección si llegaran a obligarte a dar tu contraseña.

Crea una contraseña para el volumen TrueCrypt ‘externo’ normal, el contenedor que es visible en tu directorio. Pon dentro de este contenedor archivos sensibles que podrías, de manera plausible, querer encriptar y mantener secretos (a menos que sea un señuelo convincente, un adversario podría seguir insistiendo para que le des la contraseña ‘real’) , pero que, en el peor de los casos, podrías compartir si se te presiona.

Sin embargo, dentro de ese volumen hay otro volumen escondido. Nadie lo puede ver y

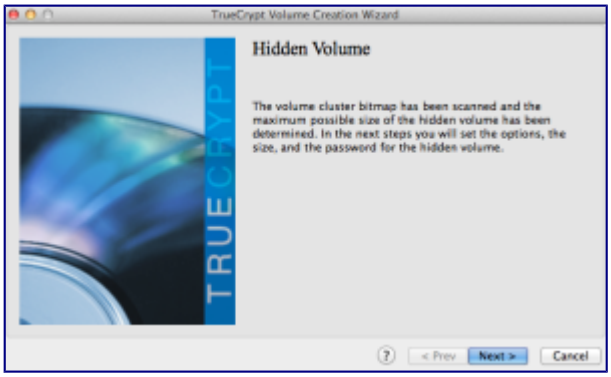
hasta donde sabemos, incluso las pruebas más sofisticadas no pueden revelar la existencia de un volumen TrueCrypt escondido. Sólo el creador sabe que está allí. Accede a él introduciendo una contraseña alternativa que has creado específicamente para acceder a ese volumen escondido. Esta es una contraseña que estarías dispuesto a mantener en secreto durante mucho más tiempo que la contraseña del volumen exterior.

1. **Crear el volumen exterior**
   Inicia TrueCrypt y haz clic en:
   - 'Create Volume' (Crear Volumen) > 'Create an encrypted container' (Crear un contenedor encriptado) > selecciona 'Hidden TrueCrypt volume' (Volumen TrueCrypt escondido) > selecciona la ubicación donde el contenedor se guardará en tu ordenador (se podrá mover después) y dale un nombre (inocuo) al contenedor.
     Para encriptar todo un disco duro externo como un USB, selecciona 'Create Volume' (Crear volumen) > Create a volume within a partition/drive' (Crear un volumen dentro de una partición/dispositivo)
   - La siguiente pantalla se llama 'Encryption Options' (Opciones de encriptación). Las opciones por defecto están bien. Para encriptar de forma más segura (encripta múltiples veces), ve a 'Encryption Algorithm' (Algoritmos de encriptacion), selecciona 'AES twoFish-Serpent', y en 'Hash Algorithm' (Algoritmo de resumen criptográfico), selecciona SHA-512.
   - La próxima pantalla se llama 'Volume size' (Tamaño del volumen). Selecciona el tamaño del contenedor (esto determinará la cantidad máxima de información que puede almacenar).
   - Introduce la contraseña del volumen en la próxima pantalla. Crea una buena contraseña (ver capítulo 8) y ¡que no se te olvide!
   - La próxima pantalla Se llama 'Format Options' (Opciones de Formato). Selecciona FAT.
     Información del Experto: FAT es compatible con todos los sistemas pero tiene limitaciones respecto al tamaño máximo de los archivos que puede contener (los archivos individuales no pueden ser mayores de 4 GB). Normalmente, no debería suponer ningún problema. Si necesitas poder guardar archivos mayores y estás seguro de que escoger algo diferente a FAT no creará problemas al compartir los archivos, puedes escoger una de las otras opciones.
   - El programa ahora generará un conjunto de datos al azar para encriptar el volumen. Mueve tu ratón aleatoriamente durante un instante antes de hacer clic en 'Format'. El programa creará el volumen. En función del tamaño del algoritmo de encriptación escogido y de la velocidad de tu ordenador, esto llevará entre unos segundos y unas horas (para volúmenes muy grandes).
   - La siguiente pantalla se llama 'Outer volume' (Volumen exterior), léela con atención. Ahora debes copiar algunos archivos que parezcan importantes dentro del volumen (es decir copiar y pegar algunos archivos dentro del

lector con el contenedor TrueCrypt que ahora aparece en ‘My Computer’/‘Finder’). Después haz clic en ‘Next’ (Siguiente).

- La siguiente pantalla se llama ‘Hidden Volume’ (Volumen escondido). Léela, y haz clic en ‘Next’ (Siguiente).

2. **Crear el volumen oculto**



Ahora que se ha creado el volumen exterior, se te guiará para crear el volumen escondido. Esto te llevará por el mismo proceso que en el paso previo, pero para un volumen oculto. Pasarás por las pantallas de ‘Encryption Options’ (Opciones de encriptación), ‘Hidden Volume Size’ (Tamaño del volumen escondido) [la disponibilidad de espacio depende del tamaño de los archivos que hayas usado como señuelo en tu volumen exterior], ‘Hidden Volume Password’ (Contraseña del volumen escondido) y ‘Format Options’ (Opciones de formato).

Importante: para el volumen escondido debes escoger una contraseña diferente a la del volumen exterior. Estas dos contraseñas sirven para acceder al volumen exterior o al escondido.

3. **Pon los archivos que quieras encriptar en tu volumen escondido**
Ahora el volumen ‘montarse’ (activarse). Haz clic en ‘Select File’ (Seleccionar archivo) > localiza y selecciona el archivo que acabas de hacer > haz clic en ‘Mount’ (Montar).

Ahora, introduce una de las dos contraseñas para el volumen exterior o escondido, dependiendo de a cuál quieras acceder (debería de ser al volumen escondido) y haz clic en ‘OK’.
Ten en cuenta que si añades más información al volumen exterior, ésta puede

sobrescribirse en el espacio/información del volumen escondido. Lo ideal es que no tengas que añadir o modificar más información del volumen exterior después de crear el volumen escondido.

El contenedor TrueCrypt de ese volumen aparecerá ahora como un lector separado en tu sistema (igual que un USB o disco duro externo) y puedes meter archivos en él como en un USB (ve a 'My Computer' o 'Finder' y selecciona y arrastra los archivos al interior del contenedor).
Una vez hayas metido los archivos deseados dentro del contenedor, 'cierra' el contenedor haciendo clic en 'Dismount' (Desmontar) en TrueCrypt. Ahora parecerá que el contenedor sólo es un archivo más en tu ordenador.

Encriptar discos duros

Los sistemas Mac y Linux tienen una opción incorporada para encriptar un disco duro entero.

Linux/Ubuntu:
Te habrás dado cuenta de que en nuestra guía de instalación de Ubuntu (capítulo 2), te recomendamos optar por 'encriptar la instalación de Ubuntu' y 'encriptar la carpeta raíz'. Estas opciones encriptan el disco duro entero y el directorio de inicio con contraseñas separadas.

Mac:
Ve a System Preferencias del Sistema > Seguridad y Privacidad > FileVault > Enciende 'FileVault'.

Windows:
La forma más segura de encriptar un disco duro en un sistema Windows es usando TrueCrypt.
El método es casi igual a los descritos arriba, excepto en el inicio del proceso: haz clic en 'Create Volume' (Crear volumen) > selecciona 'Encrypt a non-system partition/drive (Encriptar una partición/dispositivo externo al sistema) > 'Standard TrueCrypt volume' (Volumen TrueCrypt estándar) > Selecciona el dispositivo del disco duro.

Puedes encontrar instrucciones completas aquí:
http://webapps.lsa.umich.edu/lsait/admin/HowTos/Encrypt-w-TrueCrypt-Win-FDE.pdf

Compartir información de forma segura

Riesgos:

- Interceptación
- Intervención
- Destrucción de documentos de origen
- Identificación de la fuente
- Identificación del periodista

Acciones de InfoSec:

- Intercambiar USB o discos duros encriptados (en persona, si es posible)
- Intercambiar volúmenes pequeños de información por medio de adjuntos encriptados en correos electrónicos encriptados
- Intercambiar volúmenes grandes de información encriptada por medio de servicios para compartir archivos

Intercambio físico

La forma más segura de compartir volúmenes grandes de información es intercambiar físicamente un dispositivo de almacenamiento (lo ideal, un USB o disco duro) con los datos en forma encriptada.

Puede estar encriptado el dispositivo entero o varias carpetas guardadas en el equipo, encriptadas con diferentes contraseñas, de modo que la fuente puede permitir que se acceda a ella de manera controlada (la fuente puede facilitar las contraseñas a lo largo de un período de tiempo mediante canales seguros tales, como correos encriptados o chat OTR. Ver capítulos 5 y 6).

Así pues, todo lo que necesitas para intercambiar información en persona es software de encriptación (como TrueCrypt) y una memoria USB. Hoy día puedes comprar memorias USB con una gran capacidad de almacenamiento (256GB) por poco más de 20 €.

Intercambio digital

Si no puedes verte cara a cara con tu fuente para recoger los documentos, tendrás que intercambiarlos en línea de manera segura.

Se pueden compartir pequeños volúmenes de información como adjuntos encriptados, si ambos usáis correo electrónico encriptado (ver capítulo 5).

Es posible encriptar volúmenes grandes de información usando TrueCrypt, por ejemplo, y dar al archivo un nombre inocuo que no se relacione de ninguna manera con la naturaleza de los datos o aspectos específicos del contenido. Puedes después intercambiar este archivo mediante un servicio recomendado de intercambio de archivos y enviar un enlace al archivo online al destinatario y la contraseña para desencriptarlo por un canal separado y seguro.

Una vez más, para que esta sea una opción segura, necesitas un sistema seguro. Si tu hardware o sistema operativo son inseguros, los archivos que intercambies y las contraseñas que compartas pueden también no ser seguros, un adversario podría potencialmente acceder de forma remota a tu ordenador, o incluso controlarlo. Idealmente, tu fuente y y tú intercambiaréis documentos por medio de sistemas seguros y ambos usando Tails. Para hacerlo con la máxima seguridad, solo accederás a estos archivos desde un dispositivo aislado de conexiones de red inseguras.

Mega

'Mega' (https://mega.co.nz/) es una alternativa a plataformas conocidas de intercambio de archivos como Dropbox y Google Drive. Mega usa algunas encriptaciones dentro del navegador antes de que el archivo se suba, para proteger al usuario frente a amenazas de bajo nivel y para proteger a Mega legalmente frente a acusaciones de facilitar que se vulneren los derechos de autor (ya que ellos no pueden saber los contenidos del archivo compartido). Aunque esta encriptación no debería considerarse 'a prueba de gobiernos', añade una fina capa de protección frente a cotillas, mientras los datos se transmiten a través de una conexión Wi-Fi abierta del café/biblioteca anónimos que hayas elegido. Como la mayoría de proveedores de almacenamiento en línea, Mega provee 50GB por cada dirección de correo distinta que tengas. Como con cualquier otro aspecto de InfoSec, se aconseja compartimentar la información en varias cuentas que no se puedan relacionar entre sí.

SecureDrop

Algunas organizaciones periodísticas con considerables recursos y capacidad informáticos han puesto en marcha su propio sistema para facilitar el intercambio seguro de archivos, entre los que destaca SecureDrop. SecureDrop es un sistema de envío de código abierto para informantes y es una excelente noticia que haya organizaciones que lo utilicen. Sin embargo, establecer de forma adecuada un sistema así y mantenerlo seguro no es algo trivial y no debería hacerse sin involucrar a especialistas con amplia experiencia y que puedan acreditar. No es una solución viable para un periodista independiente.

Para preguntas sobre este tema, ponte en contacto con el proveedor de servicios de informática de tu organización (pero pregunta si han hecho algo así antes, en caso contrario, busca ayuda en otro lugar). El CIJ puede ayudar y proporcionar algunos contactos fiables para empezar.

OnionShare
https://onionshare.org
OnionShare es una herramienta de código abierto que te permite compartir (mediante la red de Tor) archivos de cualquier tamaño de forma segura y anónima.

OnionShare ofrece un método seguro para intercambiar archivos porque permite a los usuarios compartir directamente de un ordenador a otro, a través de conexiones Tor, sin subir los archivos a servidores de terceros. En su lugar, a efectos de la transmisión, el ordenador del remitente se convierte en el servidor.

OnionShare es fácil de instalar y usar en Windows, Mac, Ubuntu y Tails. La instalación de Ubuntu requiere uso mínimo de la línea de comando. Puedes descargar OnionShare y encontrar las instrucciones para instalar aquí: https://onionshare.org

Usar OnionShare:
Para enviar archivos usando OnionShare, debes tener en funcionamiento el navegador Tor. También debes usar el navegador Tor para descargar archivos compartidos en

OnionShare.

El remitente escoge los archivos que desea compartir, y OnionShare permite que los archivos puedan descargarse mediante una URL, accesible por medio de Tor. Mientras el destinatario descarga el archivo, el remitente puede ver el progreso y fin de la descarga.

Si te preocupa que la vigilancia se intensifique o que se intente interceptar tus archivos compartidos, deberías poner especial cuidado en compartir de forma segura la URL con tu contacto (por ejemplo, por medio de OTR encriptado o correo encriptado) y de manera anónima (por ejemplo, usando una cuenta de correo desechable anónima creada en el navegador Tor).

Cuando la descarga se haya completado, o cuando el remitente cierre OnionShare, los archivos se eliminan por completo de internet (a menos que deselecciones 'Stop sharing automatically' (Dejar de compartir automáticamente) en OnionShare, lo que permite que los archivos se descarguen múltiples veces).

Puedes encontrar más instrucciones de uso aquí:
https://github.com/micahflee/onionshare

Borrar archivos de forma segura

En la mayoría de sistemas, borrar un archivo no elimina realmente los datos del disco duro del ordenador (o de la memoria USB, si están ubicados allí). El archivo todavía existe, pero el espacio que ocupa se marca simplemente como 'no usado', en algún momento volverá a usarse y será desplazado por otros archivos. Pero, hasta entonces, el archivo 'borrado' todavía se puede recuperar con las herramientas forenses adecuadas y experiencia.

Para borrar archivos de forma segura, puedes usar herramientas específicas que sobreescriben archivos varias veces con información al azar. Este método es muy seguro, pero puede llevar un tiempo considerable en el caso de volúmenes grandes de datos (p. ej. varias horas para un USB de múltiples gigabytes).

Mac
Borrar archivos individuales de forma segura:
Después de mover un archivo a la papelera, abre la carpeta de que la contiene, ve a Finder (a la izquierda en la barra superior de herramientas) y selecciona 'Vaciar la Papelera de manera segura'. Todos los archivos de la papelera se eliminarán del directorio del Mac y el espacio del disco duro que ocupaban se sobreescribirá con datos aleatorios.

Para limpiar de forma segura una memoria USB (o cualquier disco duro externo):
Introduce el USB. Inicia 'Utilidad de discos' > selecciona el disco que quieras borrar (ver menú a la izquierda) > selecciona la pestaña 'Borrar'. Selecciona 'Opciones de seguridad' y desplaza la barra deslizante hacia 'Más seguro'* > 'OK' > 'Borrar'.

Para limpiar todo el espacio 'libre' en el disco duro del Mac:
Esto busca cualquier área del disco duro marcada como disponible para información

nueva y la sobreescribe con datos nuevos.

Inicia ‘Utilidad de discos’ > selecciona el disco que quieras borrar (ver menú a la izquierda) > selecciona la pestaña ‘Borrar’ > haz clic en ‘Borrar espacio libre’. Aparecerá una ventana con ‘Opciones para borrar el espacio libre’. Arrastra la barra deslizante hacia ‘Más seguro’* y haz clic en ‘Borrar espacio libre’.
*(En algunas versiones de Mac OS, hay un botón en vez de una barra deslizante, llamada ’Borrado en 35 pasos’).

Windows, Linux/Ubuntu
En los sistemas Linux y Windows, BleachBit (http://bleachbit.sourceforge.net/) es la mejor herramienta de limpieza de código abierto y se considera muy fiable.

Tails
En el sistema Tails hay una aplicación para borrar de forma segura, a la que se accede fácilmente haciendo clic con el botón derecho sobre un archivo y seleccionando ‘Wipe’ (Limpiar). Puedes borrar de forma segura todo el espacio ‘libre’ en una carpeta haciendo clic en el espacio de la carpeta con el botón derecho y seleccionando ‘Wipe available diskspace’ (Limpiar espacio disponible del disco).

Borrar físicamente
Si hay que limpiar todo un disco también existe la opción de destruir físicamente el dispositivo de almacenamiento. Para estar seguros de que ningún dato puede recuperarse, el dispositivo tiene que triturarse en pedazos muy pequeños, de no más de 1mm. No des por sentado puedes burlar técnicas forenses especializadas simplemente rompiendo el disco con un martillo o sumergiendo el aparato en agua. Aunque casi con total seguridad impedirá que el aparato vuelva a funcionar, la información se puede recuperar si el contrario tiene los recursos y el tiempo para usar métodos avanzados de recuperación de datos.

Opta por memorias USB
Ya que guardar información en el disco interno de un ordenador portátil conlleva riesgos adicionales y posiblemente hace más difícil que la información pueda borrarse de forma segura, guardar material delicado en un medio de almacenamiento externo como un USB o disco duro externo (para volúmenes grandes), es muy recomendable. Es importante encriptar también estos aparatos o archivos, para protegerlos en caso de pérdida o robo.

Metadatos
Los metadados son datos acerca de datos. Los metadatos pueden ser el autor de un documento en Microsoft Word, o las coordenadas GPS en las que se sacó una foto. Archivos de audio, video, y PDF también contienen metadatos y datos escondidos (como cambios o comentarios, nombres de archivos, etc.). La mayoría de impresoras láser a color imprimen su tipo y número de serie en pequeños puntos invisibles en cada centímetro cuadrado de papel, por lo que esos pedazos de papel son rastreables si el número de serie de la impresora está conectado a ti de alguna forma (p. ej. si compraste la impresora en internet).

Cada programa que usas puede tener configuraciones específicas de metadatos, así que deberías investigar en internet (o consultar a un experto) sobre el programa y archivo que te planteas usar para estar al corriente de qué información se guarda, cómo la puedes eliminar y cómo puedes asegurarte de que es inofensiva.

LibreOffice
LibreOffice es un paquete Office gratuito de código abierto.
https://www.libreoffice.org/

En LibreOffice, la información del usuario se puede ver, y borrar yendo a:
‘Archivo’ > ‘Propiedades’ > ‘General’.

-> Haz clic en ‘Reiniciar’ para reiniciar la información general del usuario (p. ej. tiempo total de edición, número de revisión)
-> Desactiva ‘Apply user data’ (Aplica data de usuario)

Después revisa las pestaña de descripción ‘Description’ y ‘Custom Properties’ (Propiedades Personalizables) y borra cualquier información que no quieras difundir. Bajo la pestaña de ‘Security’ (Seguridad), desactiva ‘Record changes’ (Grabar cambios) si no está ya deshabilitada.
Bajo Edit (Editar) > Changes (Cambios) > Accept or Reject (Aceptar o Rechazar): puedes borrarlos si el destinatario no los necesita.

Si usas la característica de Versions (Versiones), ve a File (Archivo) > Versions (Versiones) y borra cualquier versión antigua del documento que esté guardada allí.

(Sólo para Writer – editor de texto) View (Ver) > Hidden Paragraphs (Párrafos Escondidos), revisa que todos los párrafos escondidos sean visibles.
(Sólo para Calc- editor de hojas de cálculo) Format (Formato) > Sheet (Hoja), revisa que no haya ninguna hoja escondida.

Capítulo 5: Correo Electrónico

El correo electrónico es, probablemente, el medio que más usas para estar contacto con tus colegas y fuentes. Es vital, es el medio por el que una nueva fuente podría ponerse en contacto contigo. Por esto, tener un correo seguro, no sólo para el uso diario con colegas, sino como un canal seguro para un contacto inicial, es importante para cualquier periodista.

Los riesgos que conlleva comunicarse por correo incluyen que alguien en tu contra pueda hacer
cualquiera de las siguientes acciones:

- Leer el contenido del correo.
- Leer el asunto.
- Ver con quién contactas, con qué frecuencia y cuándo.
- Interceptar los archivos adjuntos.
- Llevar a cabo ataques de man-in-the-middle (por intermediario).
- Ver desde dónde envías correos (ubicación).

Acciones de InfoSec:

- Usar contraseñas fuertes.
- Usar un proveedor de correo electrónico fiable.
- Encriptar tus correos.
- Verificar tus llaves.
- Poner la mínima información en el asunto.
- Enviar correos desde Tails (cuando sea necesario).
- Usar direcciones de correo anónimas para fines determinados.

Los riesgos

Como protección contra la mayoría de agentes no gubernamentales, usar una contraseña fuerte es una buena forma de defensa frente al acceso no autorizado a tu cuenta de correo. Sin embargo, en caso de agentes gubernamentales, puede no ser ninguna defensa.

Un proveedor de correo ‘fiable’ es el que cuenta con una buena infraestructura básica de seguridad y no se proporciona tus datos a una agencia de inteligencia rápidamente. Si no confías en el país en el que este proveedor está ubicado, es mejor no usar una dirección de correo de allí. Por ejemplo, sabemos que la estrategia de las agencias de inteligencia en E.E.U.U. y Reino Unido es grabar y guardar la mayor cantidad de comunicaciones de correo posibles. Aunque no consideres que en este momento tus comunicaciones por correo electrónico puedan ser de importancia para estas agencias, si tú y/o tu trabajo adquirís importancia en el futuro, podrá accederse de forma retroactiva a esas comunicaciones. Así que, si no confías en la manera en que los E.E.U.U. trata la

privacidad de los correos, sé consciente de que los proveedores de correo ubicados allí (Outlook, Gmail, Riseup, etc.) pueden estar sujetos a ese trato. Se cree que algunos proveedores de correo electrónico cooperan más que otros, pero a menos que gestiones tu propio servidor (o la organización para la que trabajes utilice un servidor propio en un país con buenas leyes de privacidad, como Suiza o Islandia), deberíamos dar por sentado que tus correos y sus metadatos no están seguros con ningún proveedor de correo. Otras cosas que debes tener en cuenta es si tienes que proporcionar tu número de móvil, un código postal/dirección o alguna otra dirección de correo para poder registrar una cuenta con un proveedor, ya que puede que quieras evitar facilitar esta información en el futuro (y en especial cuando estás usando una dirección de correo anónima).

Metadatos de correos

Los metadatos son datos acerca de datos. Los metadatos de correos electrónicos incluyen tanto el nombre del remitente como del destinatario, direcciones de correo e IP, información de la transferencia del servidor, fecha, hora y zona horaria, identificador único del correo y correos relacionados, tipo de contenido y codificación, registro de sesiones iniciadas por el cliente del correo con direcciones de IP, prioridades y categorías, encabezado del correo, status del correo y cualquier solicitud de acuse de recibo.

De por sí, esta información es importante y reveladora, pero muchas agencias de inteligencia y cuerpos policiales (y en algunos casos, hackers individuales) también son capaces de extraer el contenido entero del correo.

No se pueden proteger fácilmente los metadatos de tus correos electrónicos, así que el asunto debería ser minimalista o confuso, y quizá quieras ocultar tu verdadera ubicación/dirección IP utilizando el navegador Tor.

Ejemplo: En el verano de 2013 autoridades del gobierno de E.E.U.U. solicitaron acceso a los metadatos de un usuario, cuyo nombre no se ha divulgado, de Lavabit, un proveedor de correo seguro, además de las claves de encriptación privadas de la compañía (que permitirían el acceso a las contraseñas de usuarios). Supuestamente, lo pidieron porque no lograron acceder de forma encubierta. Se cree que este intento de obtener información se debió a que el informante de la NSA Edward Snowden tenía una cuenta de correo con Lavabit. La ley impedía al fundador de Lavabit comentar la naturaleza exacta de la solicitud del gobierno de Estados Unidos, como estaría prohibido para cualquiera al que se le pidiera algo así (lo cual hace que sea todavía más difícil evaluar la seguridad de nuestros proveedores de correo). En lugar de permitir que se invadiera la privacidad de un usuario, el fundador suspendió por completo Lavabit en agosto de 2013.

Encriptación del correo

Sin embargo, puedes proteger la privacidad del contenido de tu correo usando ‘criptografía de clave pública’. Este método convierte el contenido de tu correo en un código indescifrable (de momento). El correo encriptado puede entonces desencriptarse únicamente usando la ‘clave pública’ del destinatario.

Las siguientes instrucciones recomiendan seguir el GNU Privacy Guard, ‘GPG’ (una implementación de código abierto de ‘Pretty Good Privacy’, o PGP).

El uso de GPG, si bien es muy diferente al correo normal, no es difícil y conseguirás acostumbrarte a él muy rápidamente. Entender exactamente cómo funciona, sin embargo, es un poco más complicado.

Par de claves
En esencia, las claves son series de números largas y únicas, y cada usuario de una encriptación de correo tiene un par, una clave pública y una clave privada.

Tu clave pública: Tu clave pública es la que la gente usará para encriptar los correos que te manden. Al igual que incluir tu número en la guía telefónica, puedes escoger si quieres o no incluir tu clave pública en el servidor (si es una cuenta de correo secreta o anónima, quizá no quieras subir la clave al servidor de claves). Si optas por que tu clave pública aparezca en el servidor de claves, estará disponible abiertamente para que cualquiera pueda ponerse en contacto contigo de forma segura.

Tu clave privada: Tu clave privada te permite desencriptar correos de otros que se han puesto en contacto usando tu clave pública. Por tanto, aunque tu clave pública esté disponible, tu clave privada del par de claves es exactamente eso, ¡privada! Una clave privada corresponde a tu clave pública, asegurando que nadie más pueda usar tu clave pública sin autorización. Probablemente nunca llegarás a ver tu clave privada, pues se encuentra y trabaja bajo la protección del software GPG.

La extensión, aleatoriedad y sofisticación de la sólida criptografía asimétrica (claves de 4096 bits, de acuerdo a las instrucciones que exponemos más adelante) es la razón por la que encriptación sigue siendo, según sabemos, indescifrable.

Verificar claves

Es importante que verifiques que las claves de las personas a las que envías correos pertenecen realmente al destinatario previsto. Aunque la dirección de correo pertenezca a la persona con la que quieres contactar, existe una pequeña posibilidad (a niveles de alto riesgo) de que la clave pública no sea la suya. Esto se conoce como un ataque man-in-the-middle (por intermediario): interceptar comunicaciones de forma oculta haciéndose pasar por el destinatario. Necesitas asegurarte de que tanto la dirección de correo como la clave pública pertenezcan al mismo individuo. Ver ‘Verificar claves’ más adelante en este capítulo.

Proteger tu identidad y ubicación cuando envías correos

A niveles de alto riesgo, quienes deseen esconder su identidad real propia, o la de con los que se comuniquen, deberían usar cuentas de correo anónimas no asociadas con ningún otro aspecto de la identidad online, que no estén conectadas contigo de ninguna manera. Gmail y Hotmail suelen solicitar un número de teléfono o dirección de correo alternativa, así que estos proveedores no son ideales para crear cuentas anónimas. Vmail (https://www.vmail.me) y en varios países, GMX y Yandex permiten a los usuarios crear

cuentas sin dar esta información identificativa.

Sin embargo, si creas una cuenta de correo de forma anónima desde una conexión de internet asociada a ti, tu anonimato puede verse comprometido. Además, cuando envías y recibes correos, lo estás haciendo en internet, por lo que tu proveedor conoce tu ubicación el proveedor de internet (y potencialmente, alguien en tu contra). Si deseas que tu identidad y tu ubicación sean anónimas, puedes usar una cuenta anónima para enviar correos no encriptados por medio del servicio de correo con el navegador Tor (ver capítulo 3); o puedes usar el sistema operativo Tails, que esconde la ubicación real de todas las comunicaciones en internet desde tu ordenador portátil (ver capítulo 2). El cliente de correos de Tails (que permite encriptación) envía y recibe información/correos hacia y desde internet por medio de Tor, ocultando así la ubicación real de la conexión.

Quizá solo quieras proteger tu ubicación sobre el terreno más que tu identidad en sí. Para esto, usar el sistema operativo Tails es la única respuesta.

Notas básicas sobre la encriptación de correo

Ten en cuenta que la encriptación de correo no esconde metadatos, como con quien estás hablando, el asunto de tu correo o tu ubicación (aunque, como hemos comentado, puedes esconder tu ubicación usando Tor/Tails). Es una buena idea que las personas en riesgo a todos los niveles escriban encabezados misteriosos o confusos.

No puedes encriptar o desencriptar correos desde tu móvil. Aunque es posible instalar estos programas en algunos teléfonos Android, está desaconsejado ya que los móviles son fundamentalmente inseguros (ver capítulo 7).

Tampoco puedes encriptar y desencriptar correos desde tu navegador de red (a menos que estés usando el sistema operativo Tails), tendrás que usar el cliente de correos Thunderbird en tu escritorio, con el software adicional de encriptación y desencriptación, para encriptar y desencriptar correos usarás.
Finalmente, sólo puedes enviarle correos encriptados a otras personas que también usen un correo encriptado. Esta era una comunidad muy pequeña pero en el mundo post-Snowden, está creciendo exponencialmente.

Instrucciones de instalación para correo encriptado

1. 1. UBUNTU/LINUX: Cliente de correos Thunderbird y software de encriptación GPG

Ubuntu viene precargado con Thunderbird (cliente de correo) y software de encriptación GPG.
Usa la herramienta de búsqueda en Ubuntu en la parte superior izquierda de tu escritorio.

1. 1. MAC: Descarga el cliente de correos Thunderbird y software de encriptación GPG

Necesitarás descargar:

- Un **cliente** de correo/gestor de correo de escritorio. Nosotros recomendamos el

cliente de Mozilla de código abierto ‘Thunderbird’
http://www.mozilla.org/en-US/thunderbird/

- **GPG** – GNU Privacy Guard (Guarda de Privacidad GNU), que es software de encriptación:
https://gpgtools.org/ La primera opción de descarga, en rosa, ‘Download GPG suite’ será la versión más reciente . Haz clic en ella para descargarlo. Haz clic en la descarga cuando haya acabado y sigue los pasos del asistente de instalación.

Cuando las descargas hayan terminado, abre Thunderbird desde ‘Descargas’ y arrastra el icono de Thunderbird al interior de la carpeta ‘Aplicaciones’.

1. 1. WINDOWS:

Necesitarás descargar:

- Un **cliente** de correo/gestor de correo de escritorio. Nosotros recomendamos el cliente de Mozilla de código abierto ‘Thunderbird’.
http://www. mozilla. org/en-US/thunderbird/
- **GPG** – GNU Privacy Guard (Guarda de Privacidad GNU), que es software de encriptación
http://www.gpg4win.org/download.html La primera opción de descarga, en verde, será la versión más reciente de GPG. Haz clic en ella para descargarla. Haz clic en la descarga cuando haya acabado y sigue los pasos del asistente de instalación.

1. 2. UBUNTU/LINUX, MAC y WINDOWS:

En Windows, haz clic en la descarga para instalar Thunderbird. Thunderbird cuenta con un breve asistente de configuración. Selecciona la instalación estándar, confirma la ubicación del archivo del programa y haz clic en ‘Siguiente’ para completar y terminar la instalación.
Abre Thunderbird. Si lo haces por primera vez, puede que pida ‘Integración’. Sáltate este paso y deselecciona ‘Ejecutar siempre esta verificación al iniciar Thunderbird’.

Thunderbird también te pedirá configurar tu cuenta de correo y te ofrecerá una dirección de correo nueva. Haz clic en ‘Omitir y usar mi cuenta existente’. Introduce la dirección de correo que desees usar para la encriptación y su contraseña. Deberías decidir si seleccionas ‘Recordar contraseña’ o no. Puede ser más seguro si no permites que tu ordenador recuerde la contraseña, pero entonces tendrás que introducir tu contraseña cada vez que abras Thunderbird. Haz clic en ‘Continuar’.
Nota: Por motivos obvios, si usas una cuenta de correo anónima, ¡no introduzcas tu nombre real!
Deberías ver ‘Configuración encontrada en la base de datos ISP de Mozilla’.

Resolución de problemas: Si recibes el mensaje ‘La configuración no puede verificarse’, puede deberse a que tu proveedor de correo usa verificación con dos factores (p. ej. muchas cuentas de Gmail usan verificación en dos pasos). En este caso, tu proveedor puede enviarte un correo, o mostrar una página en el navegador, para notificarte que se

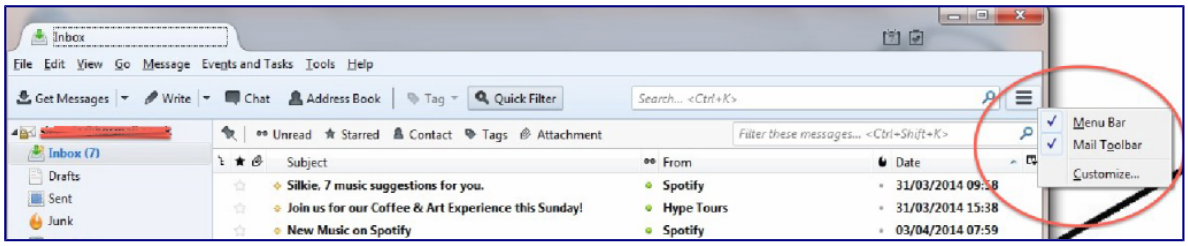
ha intentado acceder a tu cuenta con un cliente de correo y pedirá que te identifiques. Como alternativa, algunos usuarios de Gmail que usan verificaciones en dos pasos necesitarán una 'contraseña específica de aplicación'. Para conseguirla, ve a 'Autorizar aplicaciones y páginas web' en la configuración de tu cuenta de Google. Para más información, visita:
https://support.google.com/mail/answer/1173270?hl=en

Ahora tienes la opción de escoger IMAP o POP3. Escoge IMAP si usas correo online, y haz clic en 'Finalizar'.

Información del experto: A diferencia de POP, IMAP ofrece comunicación de doble vía entre tu correo online y tu cliente de correo de escritorio, así que cualquier cambio que hagas en tu cliente de correo se aplica a tu cuenta online (p. ej. si marcas un correo como 'leído' en Thunderbird, con IMAP, aparecerá también como 'leído' en tu correo online).

2. Extensión de seguridad Enigmail

En la parte superior de la ventana de Thunderbird, haz clic en 'Herramientas' > 'Add-ons' > 'Extensiones'. Si ves 'Enigmail', ya tienes Enigmail. Si no, ve a la barra de búsqueda en la parte superior derecha de la ventana, y busca 'Enigmail'. Haz clic en 'Instalar', y reinicia Thunderbird. Cuando Thunderbird se reinicie, puedes cerrar la pestaña del 'Gestor de add-ons'.
Nota: si no tienes una barra de menú en la parte superior de tu ventana de Thunderbird, haz clic con el botón derecho en el icono de menú de tres líneas en la parte superior derecha de la ventana en Thunderbird y selecciona 'Barra de menú'.



3. Par de claves

En la parte superior de la ventana de Thunderbird, haz clic en Enigmail> Key Management (Administración de claves). En la barra superior de herramientas, haz clic > 'Generar' > 'Nuevo par de claves'.

- Debería de estar seleccionada la dirección de correo que desees usar para correo encriptado.
- Marca 'Usar la clave generada para la identidad seleccionada'. Selecciona expiración de la clave a 5 años.
- Introduce una contraseña (esta es la contraseña para tu correo encriptado, no solo tu cuenta de correo online., y debería de ser muy segura).
- El cuadro 'Comentario' añade un comentario público para tu clave pública permites que aparezca en el servidor de claves (¡así que no escribas ninguna pista!).
- En 'Caducidad de clave', selecciona que caduque en 5 años.

- Haz clic en la pestaña ‘Avanzado’ y selecciona el tamaño máximo de la clave de 4096, y tipo de clave ‘RSA’.
- Haz clic en ‘Generar clave’ y mueve tu ratón alrededor de la pantalla mientras se genera tu clave (esto ayuda a la ‘fuente de aleatoriedad’ que se usa para generarla). Esto puede llevar algunos minutos.
- Aparecerá un recuadro informándote de que se ha completado la generación de la clave. Haz clic en ‘Generate Certificate’ (Generar Certificado) en este recuadro (se crea un certificado de suspensión que necesitarás cuando desees invalidar la clave, por ejemplo, si se pierde o se ve comprometida la clave). Guarda los certificados de suspensión en algún lugar seguro. Ahora te pedirá introducir tu contraseña para completar esta acción.

Configurar Thunderbird

Vuelve a Thunderbird para cambiar la configuración.

Configuración avanzada

- Enigmail > Preferencias > Mostrar configuración avanzada.
- Básico > Configuración de la contraseña: aquí deberías seleccionar cuánto tiempo deseas que Thunderbird recuerde tu contraseña para el par de claves.
- Enviar: SeleccionaConfiguración de encriptación manual) y marca los siguientes:
    - Encripta/cifra respuestas a mensajes encriptados/cifrados.
    - ‘Cuando sea posible, en ‘Enviar encriptado automáticamente’.
    - ‘Todas las claves disponibles, en ‘Aceptar para enviar cifrado’.
    - ‘Siempre’, en ‘Confirmar antes de enviar’.
      Nota: esta es una herramienta muy útil que, cada vez que envías un correo, te permite saber, si este ha sido cifrado y encriptado, así es menos probable que envíes un correo sin encriptarlo
- Selección de claves: Marca ‘Reglas para cada destinatario’, ‘Por dirección de correo según el administrador de claves), y ‘Manualmente si faltan las claves’.
- Avanzado: recomendamos que marques ‘Reajustar el texto cifrado HTML antes de enviar’, ya que el texto HTML no funciona bien con correos encriptados.

Haz clic en ‘OK’.

Guardar carpetas localmente
Esto es particularmente útil para guardar borradores. No conviene que tus borradores, e-mails sin encriptar, se guarden en tus carpetas de correo online. Por el contrario, deberías guardarlos localmente en tu disco duro para tener más control sobre su seguridad.

En la barra del menú en la parte de la ventana de Thunderbird, verás todas tus carpetas de correo. En la parte inferior, están ‘Carpetas Locales’, haz clic con el botón derecho y selecciona ‘Nueva carpeta’. Puede ser útil crear carpetas locales para ‘Enviados’ y ‘Borradores’.

Haz clic en ‘Editar’ (Linux) o ‘Herramientas’ (Mac/Windows) > ‘Configuración de cuenta’ > ‘Copias & Carpetas’. Aquí puedes seleccionar dónde guardar los mensajes. Por ejemplo, en ‘Borradores y plantillas’, selecciona ‘Carpetas locales’, como la ubicación en la que guardar los borradores.
En la misma ventana [‘Edit’ (Linux) o ‘Tools’ (Mac/Windows) > Account Settings] haz clic en Seguridad de OpenPGP)> marca ‘Encriptar borradores al guardar’.

Correo en texto sin formato
HTML no se encripta muy bien, así que es preferible escribir mensajes en texto plano. ‘Editar’ (Linux) o ‘Herramientas’ (Mac/Windows) > ‘Configuración de cuenta’ > ‘Redacción y dirección’. Deselecciona ‘Redactar mensaje en formato HTML’.

Compartir tu firma PGP con contactos
Siempre deberías firmar los mensajes encriptados para ayudar al destinatario a verificar que eres el auténtico remitente. Compartir tu firma PGP con las personas a las que envías correos, aunque no estén encriptados, también ayuda al destinatario (si tienen Enigmail) a verificar que eres el verdadero remitente (no un imitador). Si el destinatario no usa encriptación PGP, firmar correos sin encriptación indica que normalmente usas encriptación PGP. ¡Puede ser confuso para quien esté informado!

‘Editar’ (Linux) o ‘Herramientas’ (Mac/Windows) > ‘Configuración de cuenta’ > ‘Seguridad de OpenPGP’.
‘Activar asistencia (Enigmail) de OpenPGP para esta identidad’ debería estar marcado. Marca ‘Firmar mensajes encriptados por defecto’. Si lo deseas, marca también ‘no encriptados por defecto’. Cuando firmas un mensaje, esté o no encriptado, ayudas al destinatario (si usa Enigmail) a verificar que eres el auténtico remitente (no un impostor). Haz clic en ‘OK’.

Muestra públicamente tu clave pública
Subir tu clave pública al servidor de claves es como añadir tu número de teléfono en la guía telefónica. Permite que la gente busque tu nombre/dirección de correo y localice tu clave pública para enviarte correos encriptados. Esto es muy útil para periodistas que invitan a usar correo encriptado y desean proteger la confidencialidad de sus fuentes. Sin embargo, si estás configurando una encriptación para una dirección de correo anónima que usarás solo para comunicarte con individuos específicos, de alto riesgo, no te beneficia subir tu clave pública al servidor de claves.

Enigmail > Administración de claves
Marca ‘Mostrar todas las claves por defecto’. Haz clic con el botón derecho en tu dirección de correo, y selecciona ‘Subir claves públicas al servidor de claves’ si deseas que la gente pueda contactar contigo. El servidor por defecto (pool.sks-keyservers.net) está bien.

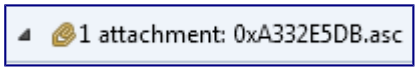
Para buscar una clave pública
Busca un nombre/dirección de correo para ver si esa persona tiene una clave pública registrada que te permita mandarle correos encriptados (es como buscar un número en la

guía telefónica).
Enigmail > ‘Administración de claves’ > ‘Servidor de claves’ (en la barra de herramientas superior) > ‘Buscar claves’. Introduce el nombre o dirección de correo de la persona y mira los resultados. Marca la dirección de correo cuya clave desees importar y presiona ‘OK’.

Importar una clave
Si ya tienes la clave de tu contacto en un archivo o en la red, pero necesitas importarla a tu gestor de correos en Thunderbird.

Importar una clave desde un fichero:
En Thunderbird, ve a Enigmail > ‘Administración de claves’. Ahora regresa a la barra de herramientas superior y haz clic en ‘Archivo’ > ‘Importar claves desde un fichero’.

Importar una clave del correo:
Si tu contacto ha adjuntado su clave pública en un correo, haz clic con el botón derecho en el anexo .asc y haz clic en ‘Importar Clave OpenPGP’. Esto se vería:



Importar una clave desde un bloque de texto:

Mucha gente tiene publicada en su página web su ‘bloque’ de clave pública (el texto completo completo de la clave pública). Esto permite que la gente confíe en la página web como fuente de la clave en vez del servidor de claves y puede ayudar a evitar ataques man-in-the-middle (por intermediario).

Simplemente copia el bloque de clave entero (el bloque completo, como se ve debajo), después en Thunderbird ve a Enigmail > ‘Administración de Claves’ > (Vuelve a la barra de herramientas) ‘Editar’ > ‘Importar claves desde el portapapeles’ > haz clic en ‘Importar’ en la caja de confirmación.

—–BEGIN PGP PUBLIC KEY BLOCK—–Version: GnuPG v1. 4. 11 (GNU/Linux)
mQINBFOypIgBEADEXjFLXnFDraRWa6YzzdnOSgKJKOzDSaonyQvh25lQGVOIwbg2
J1AfC+Ro3xhAxxXlkYzIwqeVIxlfNXCzZqn2KE7P0udF4EVrkVsWP1VcXSB65V0K
7BURi5hFFNNsk2UdnQdwcSbP77cZDkgDJofXF5hrUNlTCoLhxZ2WvpT9FfOR+Ph2
Sr/SIfcQ9K6ktsGpG5y6KafpvtI9sI+eoSOXxDdSJyelq27mM492pcnfWjD6m1vJ
61U98CjBqLIHSrsgxVivNbRxOrler5avxZjP5+691TDRCtBIn3+2WqWrzXKfMn44
l+iIKiqllMNJhmsuP3bEWHKGDZFk2/MafAqBWuXHOfclADX4GligLnv3EXmShlYd
uKtRSPvpcCwuKgM6cVjCBrpLB+lbbq+6ILMDrTt9n4WoV3kb5iUMV5gMrNTSdp8m
Gs7zMZQFXsavlR7CjKTIFhmnPYK+v4262m7ZWvXzCVIseAtbIRYMWptzolMRSzBZ
gqfcTeTQYWd1jWrbyAziE22wmfvUtqUlRQbh/okiCEcObHsPAr4QGtHyRBzBHkub
XjHopG4E+Zh1KbHTlg/wftfKDdODDfgkrrgWkIToe6xS14OogX/Bk6Al6crn4d2R
OV36KWeVx25EfVYlmEE+62mF3GrquzxKAkx2UF7s2Jk+JIlpZUCZuMZMdwARAQAB
tB5DSUogaW5mb3NlYyA8aW5mb3NlY0B0Y2lqLm9yZz6JAj4EEwECACgFAlOypIgC

GyMFCQlmAYAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEE3Wpo5+
+N4yJgUP/Atbshkafwk+GfNcsauNfqSg6u4V3p8DpBTAE4oUUk753gPSJVBiGsigztmCSpx
J6N7iqIDZ0f72AhqSlbwZ34NDPBVKrL7jRcSIwzFvTIAy1MYz9eR2cWCS1ff6XMY+
Oac1RD+J3ksY6DfLzJfZWORAHcITuBzIgZZ47DwCGNzey0zIHS/u8w7o71C+h0WV
oNFPdz1CidxCtretZkeSqvBcUNJWvx3r90Foh31otqhneCwrXgp1JNEZx/xKypex
cReY+N6UyKQMeDOn7gj0O+fuxEqSsSx8IgtALrevm37JLz732wEZIBHiB6fh+s8i
M0TpcMC//9sbL86GXGwUdosbrGnPoCCMsgE3jDJqIVz4jEoN5XPffYCmSWNb2w9s
LfQBny8s0JcRgxClytdOCDHOboBJS3ytUnUcHo/NvkpAeCEGCTvaoOtlRywdF55p
G8izK3brjKEY/1dGAx5g6aWi1iraSBOM1AHeZ/J8KOMRcEwU8sozuNeomGrSWNdR
bDTaD37F0TBOzxx+QNjeSiVzleLJeHBHyZCpizXOe2wWEtRLq9WRHM4VUI/UGHOL
xChZhwLailgkmh13eH1+47mTArbrl+P7R6Y79bmw+wld3EaE9XbnKois1on8uciW
cr2qHr/PvPN8o+4hJ7rsmsZBvX9JI+74ouyIsp0qWSrXiQIcBBMBAgAGBQJTsqfx
AAoJECN9TFARig7CU2YP/igQSe8pXbJAhrQPtTk7HByHITESlrE51uFRwCVbvTav
sRN3978ob4B7QZanVlUH2YarDoLn/a90kmpECZdxlh0ZTlKKfj32jLNTWySbiQUc
i/rOgli8NS7jezqauo+sB7ofPP/o3DKU4QvnRSSqyIxhgae80F+mnkAOyTTWDi7H
NHGq2sdLBOQALHVIVUJ5SOOEANYKZYklrR7v4iK0pc0TZDLdJ3Vm5T05N8vjCzLa
TRMgNh397ElnR9n6AGw+QRKlA21i7dAxTMecaC0nYmZx/ZVkxMRXtiSjbr2OZl63
gVxUlSo0eOjcHUX3LsX9OTew2Z+1jjaXrPJmJkxghxL/BkZx5V+knn9wTaJdP0r6
mO32n/lPEtG0mYeQQS4ZYbathSVqsY/QODG+7grce6mJUU3jzzo6AzfHMBRdipRb
bFrnOoVsDMuu4kRvPzDXiu4kJZxZiwinDuen5uu8//QUyuVXk1s3ATUiwUGgK8F2
CuYlut1/5E5x+MFS21IRCf2O3tFh8WIheO4BwQXErZ7FY9L7aaZa93WAcl6ueHUM
IBEs06+CaPUQCcWnxO2qwZm76aYNKwsVqptKEXcZ/mofo12/pgOjVtddLw9+4zpK
Gmk2erPtMPp4eMwBkZVcRz9kGfzFn3fNanmCQ22NW5x/HFrsi/+ZSURcO/Pcp8yk
uQINBFOypIgBEADIThi9K7ioKz8vqSR3yrQ1Vp9NjPit2urzgJhW3HjLenVfvwQ1
zAoks1jDoOwuFizV9vpWpHN/ovRZqJQiKwsOhaOU8FboLrwmQMvzFaf+SrIQjVM9
YOZimEEL8a2va8M9bn8pfPO9L3beq4bWgNnxZEhEOg4ovscXUfp+ktDG/L5f5z+R
77Co07XUM8KrNcYlDL76lKNrNumUTGJu/F+LR7LnNyRmpMi91LcyX4UkRar9xdTB/Omp
wBqbH4hG3hl4xB329NL5jsCAL6gqDKIe/bD6oecWhY2GodrX9bqtwCyMGb6/
rS+2Rv4ggwnRroRTGIlB2I+LlqRfMI2XZVZp9gt0Vj25D7LBmxyffGOFIzjtrXfG
yVavBQo/cHB8uSCWlPi9bQ5ZF82f9e42IazeWwrpUkyFQpiy4m8JTL2kMKt7tWEN
MI2jYPIjHnhjwBGXjyAGWchM4F0TO6q+714SxtvDQKPemWqopnKbLlQSY9OzPxRv
jK1iFOYLDCBu/uYyKsll4pqr5OokRs8Q9fO9MU+jye8O48mu91vP070bHYAKvw9N
4B28acET9JlpQOHmhLWRENz4ZNap8fe1BAhHg2AE7M4ZQUS6GkPGeUclhZhC7vs5/ty
9IHA2bk2+fMwDr+Oye2lDife0JtbL3+krD9RLqEpSZ8SDq/BNvYJcUQARAQAB
iQIlBBgBAgAPBQJTsqSIAhsMBQkJZgGAAAoJEE3Wpo5++N4yCp8P+wW7y5fbdt/O
F+4IUuVIun8yH62iQbfUBL21rWKXaTBywyWpLvlOjfA1qy1VFZnDGoGrkc6LEhFE
Wb7a53GzFyVNSM1K/U+SF0UtdT2h0WFDqwphjtD71+L6uOve0ahRyTq0PTXnk/uT
JfQ76yt7ld/6cHvvtcpYMk2n9IbeVuTWdjXLEG5Gmr4rDThUppq26oVYG5KGCuuW
s5J+k6gLPh9oNL5KKO8t8vHYbGEx3rMcdSYXXZDvYZZUDcjTE3hVXXFN3xwyHObE
L20UGFJ6y3GTL2jH0iSRtquAJlMMwttey5DOUPULu5z9prHSo961SkkZqXDhbgBp
ZO6Av0Q9FyTYoxfhhf3KH5v4CivmrPZYRD/gu/doO2JGqRyWYGDYOy0E8rgNY8wJ
JD9rMneDB9qE4vsv3AmYIF5ov5dkuQe6xSTpS11h20aokru9fJvTpNNNan8A/cPu
Y1Qvc06qzz0eHG4VnyAGBZ3j4cbT9BSKBtSl36aLCNa60Kzl4qLxSFO/+wDb6dgf

ToHfdTNDZT4SVjhfzoBVslNIbXzF1rgDGgBax2aR856hHfx4GERROSZZVBvPtjqy
5TrFSI9NsdNwmetMh8rxb+dz+fJYEE5yrNs9MJPHVgeVgj0UJLawhlCGME+/lPFJ
Cr8XhDwzI2n6gFvwtWQ1NNMqdn1UiF+Y=3DCe——
END PGP PUBLIC KEY BLOCK——

Verificar claves
Asegúrate que la persona con la crees comunicarte es realmente quien dice ser.

En Thunderbird, ve a Enigmail > Administración de claves' > haz clic con el botón derecho en la dirección de correo seleccionada > 'Propiedades de la clave'. Aquí veras la identificación de la clave y la huella digital de la persona. Puedes verificar que esa clave corresponde a la persona intercambiando las huellas digitales mediante otro método de comunicación (en persona, por teléfono, en su tarjeta de presentación/página web), y comprobando que sean exactamente iguales. En la misma ventana puedes hacer clic en 'Seleccionar acción' > 'Establecer confianza en el propietario' > y selecciona hasta qué punto confías que esa clave pertenezca al interesado.

Agregar una firma de correo ordinario
Con tu nombre, cargo, página web, dirección/es de correo, huella de PGP, etc.

'Editar' (Linux) o 'Herramientas' (Mac/Windows) > 'Configuración de la cuenta'.
Aquí puedes introducir texto para firmar a tus correos.
'Edita') (Linux) o 'Herramientas' (Mac/Windows) > 'Configuración de cuenta > 'Redacción y Dirección'.
Selecciona 'Incluir firma en las respuestas'.

Recibir correos nuevos
Puedes decidir la frecuencia con la que el cliente de correo busca mensajes nuevos.
'Editar' (Linux) o 'Herramientas' (Mac/Windows) > 'Configuración de cuenta' > 'Configuraciones del servidor'.

¡Envía un correo encriptado!

Cuando hayas completado la instalación, envía un correo de prueba a otra persona que tenga correo encriptado. Importa su clave o encuéntrala en el servidor, y asegúrate de verificarla y registrar que confiasen su clave antes de enviar un correo (de otra forma, puede que el cliente no te permita enviarle un correo encriptado) ¡Así, Thunderbird fomenta una buena seguridad en la información!).

Escoge un destinatario cuya clave ya hayas importado y verificado, y en el que confíes. Escribe tu correo y antes de hacer clic en 'Enviar', haz clic en el icono de candado para cerrarlo y encriptar el mensaje, o ve a 'Enigmail' dentro de la ventana para redactar correo y haz clic en 'Encriptación Apagada' para activar la encriptación. Presiona 'Enviar, y la caja de confirmación debería decir que tu correo está tanto firmado como encriptado (si no, retrocede y comprueba que seleccionaste encriptar). ¡Haz clic en 'Enviar Mensaje' y tu mensaje encriptado se enviará!
Ahora que le has enviado a esta persona un correo encriptado, se creará por defecto una función que hará que los futuros correos a esta persona se encripten.

Compartir tu clave pública con un particular

La primera vez que le envíes un correo encriptado a un contacto, deberías adjuntar tu clave pública para que pueda responderte con un mensaje encriptado. En la ventana para redactar el correo, a la derecha de los iconos del candado de encriptación y el lápiz de firma, hay una opción para ‘Adjuntar Mi Clave Pública’. Selecciónala para adjuntar tu clave pública al correo. Otra opción, haz clic en ‘Enigmail > ‘Adjuntar Mi Clave Pública’.

Enviar/recibir adjuntos

También puedes encriptar y desencriptar adjuntos en tus correos con GPG.
Cuando envíes archivos adjuntos en un correo encriptado, puedes escoger también si encriptar los o no. Escribe el correo, adjunta el archivo normalmente y haz clic en ‘Enviar. Antes de que el correo se envíe, te dará cuatro opciones. La primera opción es encriptar únicamente el mensaje, pero no los adjuntos. La segunda es encriptar el mensaje y también cada adjunto individualmente.

Opta por la segunda opción ‘Encriptar y firmar cada adjunto por separado y enviar el mensaje usando PGP en línea’, y haz clic en OK. Entonces, un recuadro confirmación aparecerá, como de costumbre, diciéndote que el mensaje y los adjuntos han sido firmados y encriptados. Haz clic en ‘Enviar Mensaje’ para confirmar, y se enviarán el correo y el adjunto.

Cuando alguien te envía un adjunto encriptado, haz clic con el botón derecho en el adjunto y haz clic en ‘Desencriptar y guardar como’. Guárdalo en la ubicación que prefieras y después ve a esa ubicación y encuentra/abre el adjunto.

Por supuesto, si envías un adjunto que ya ha sido encriptado por otros medios (p. ej. TrueCrypt), no necesitas encriptarlo otra vez usando GPG.

Agregar una cuenta nueva

Puede que desees agregar otra cuenta de correo a Thunderbird, tanto si tienes pensado usar encriptación en esa cuenta como si no.
En Thunderbird ve a ‘Herramientas’ (o ‘Editar’ en Linux) > ‘Configuración de cuenta’ > ‘Acciones de Cuenta’ > ‘Agregar cuenta de correo’.

Capítulo 6: Mensajería Instantánea

La mensajería instantánea es una forma excelente de entablar y mantenerse en contacto con una fuente. Instalar programas de mensajería instantánea encriptados y con un cifrado OTR (“off-the-record”) es muy rápido y fácil especialmente si lo comparamos con la configuración del correo encriptado. Al usar estos programas, puedes tratar los protocolos de seguridad necesarios antes de continuar conversaciones, encontrarte con alguien, mandar correo electrónico, compartir documentos/información, etc. También es una herramienta útil para hablar con colegas cuando estás colaborando de forma remota en un proyecto.

La mensajería instantánea OTR te permite tener una conversación privada que no sólo está encriptada, sino que tampoco se guarda, y por lo tanto puedes negar haberla mantenido. Esto quiere decir que resultaría plausible que una conversación en la que supuestamente participa una cuenta asociada a ti realmente no tenga nada que ver contigo.

Información del experto: Al igual que el correo encriptado, la mensajería OTR usa claves públicas para verificar que un contacto es quien se dice ser. Sin embargo, cada vez que inicias una conversación con un contacto (que ha sido verificado por su clave pública se encripta usando claves nuevas, desechables. No te preocupes, no tienes que hacerlo tú mismo ni revisarlo, el programa realiza esta encriptación de forma automática.

Si utilizas Linux o Windows, recomendamos que uses un cliente de mensajería instantánea llamado Pidgin, con una extensión OTR.

Si utilizas Mac, recomendamos un cliente de mensajería instantánea llamado Adium.

Los usuarios de Pidgin y Adium pueden comunicarse fácilmente entre sí. Sin embargo, los métodos de verificación para los dos clientes de mensajería son diferentes. Ver ‘Verificar contactos’.

Instrucciones para Adium de Mac:

1. **Descarga Adium**
   Descarga e instala ‘Adium’ para Mac – http://adium.im/
2. **Crear y configurar una cuenta IM**
   - Una vez descargado, abre Adium y ve a (en la parte superior) ‘Archivo’ > Añadir cuenta’ > ’XMPP’.
   - Primero, quizá quieras configurar Adium para conectarte solamente a tu cuenta de mensajería instantánea mediante Tor para proteger tu ubicación real (especialmente útil si deseas usar esta cuenta de forma anónima). En la pestaña ‘Proxy’ marca ‘usar proxy’ y escoge ‘SOCKS5’ en la lista desplegable. En el campo ‘Servidor’, introduce‘127.0.0.1’ y en el campo ‘Puerto’ introduce ‘9150’.
   - Los campos de usuario y contraseña son opcionales, pero si los utilizas Tor

usará circuitos diferentes para Adium que para todo lo demás, aumentando tu anonimato. Ten en cuenta que ahora será necesario que tengas el navegador Tor abierto (ver Capítulo 3) cuando desees conectarte a esta cuenta.

- En la pestaña ‘Cuenta’ escoge un nombre (anónimo) y agrega un dominio al final para tu ID de Jabber (por ejemplo, @jabber.ccc.de se usa mucho. Ver una lista de opciones en https://list.jabber.at). Una ID de Jabber completa podría ser, por ejemplo, kissinger@jabber.ccc.de. En ‘Contraseña’, escoge una contraseña fuerte. No hagas click aún en ‘Registrar nueva cuenta’.
- En la pestaña ‘Opciones,’ marca ‘Requiere SSL/TLS’ y marca ‘ Comprobaciones esctictas de certificados’. En ‘Recurso, teclea ‘anonymous’.
- En la lengüeta de ‘Privacidad’, en el menú desplegable de ‘Encriptación’, haz clic en ‘Forzar encriptación y rechazar texto plano’ (la última opción de la lista).
- Regresa a la pestaña de ‘Cuenta’ y haz clic en ‘Registrar nueva cuenta’. Aparece una ventana nueva: en ‘Servidor’, escribe el dominio que escogiste previamente (p. ej. ‘jabber.ccc.de’ si hubieras escogido este), después haz clic en ‘Solicitar cuenta nueva’. En un momento, debería de decirte que tu cuenta se ha creado con éxito.

3. **Configurar Adium**
   Ve a Adium > ‘Preferencias’ > ‘General’ > deselecciona ‘Archivar mensajes’.

Instrucciones de Pidgin en Linux (Ubuntu)/Windows

1. **Descargar Pidgin y el plug-in OTR**
   Pidgin y OTR son software que a menudo está incluido en las distribuciones de Linux, así que simplemente busca en el ‘Centro de Software’ de Ubuntu (u otras distribuciones Linux).
   Descarga e instala Pidgin en www.pidgin.im (Windows), si estás en Ubuntu, se te redirigirá al PPA (Archivo de Paquete Personal) de Pidgin, así que descarga ese.

   En Windows, descarga después la extensión OTR desde https://otr.cypherpunks.ca. En Ubuntu, ve al ‘Centro de Software’ de Ubuntu, busca Pidgin OTR e instala el ‘Extensión OTR para Pidgin’.

2. **Configurar Pidgin**
   Abre Pidgin. Si esta es la primera vez abres Pidgin, no tendrás una cuenta configurada y aparecerá ‘Añadir una cuenta’. Haz clic en ‘Añadir’ (si no aparece este mensaje, ve a ‘Cuentas’ > ‘Administrar cuentas’ > ‘Añadir’).

   - Primero, quizá desees configurar Pidgin para conectarte solamente a tu cuenta de mensajería instantánea mediante Tor para proteger tu ubicación real, especialmente útil si deseas usar esta cuenta de forma anónima. En la pestaña ‘Proxy’ marca ‘Conectar usando proxy’ y escoge ‘SOCKS5’ de la lista desplegable. En el campo de ‘Servidor’ teclea ‘127. 0. 0. 1’ y en el campo de ‘Puerto’ teclea ‘9150’. Los campos de usuario y contraseña son

opcionales, pero si los utilizas, Tor usará para Pidgin circuitos diferentes a los que emplea para todo lo demás, aumentando tu anonimato. Nota que ahora necesitarás tener el navegador Tor abierto (ver Capítulo 3) cuando desees conectarte a esta cuenta.

- En la lengüeta de ‘Básico’ selecciona XMPP/Jabber (NO Facebook XMPP) bajo ‘Protocolo’ y escoge un nombre de usuario (anónimo). En ‘Dominio’, escribe tu dominio seleccionado (por ejemplo, @jabber.ccc.de) . Ver una lista de opciones aquí https://list.jabber.at).). Bajo ‘Recurso, teclea ‘anonymous’. Crea una contraseña fuerte.
- Haz clic en la pestaña de ‘Avanzado’ y en ‘Seguridad de la conexión’, asegúrate de que ‘Requiere encriptación’ esté seleccionado.
- Haz clic para volver a la pestaña ‘Básico’ y asegúrate de marcar ‘Crear esta nueva cuenta en el servidor’ en la parte inferior de la ventana antes de presionar ‘Añadir’.

3. **Crear una cuenta IM**
   Tu dirección de Jabber debería aparecer en la ventana ‘Cuentas’. Marca el recuadro de ‘Activada’ y después haz clic en ‘Registrar’ dentro de la ventana ‘Registrar nueva cuenta XMPP’ que aparece.
4. **Configurar OTR**
   En Pidgin, ve a ‘Herramientas’ > ‘Plug-ins’ > marca ‘Mensajería Off-the-record ‘. Después haz clic en ‘Configurar plug-in’. Marca todas las configuraciones OTR por defecto: ‘Activar mensajería privada’; ’Iniciar mensajería privada automáticamente’; ‘Requerir mensajería privada’, y ‘No archivar conversaciones OTR’. Ahora haz clic en ‘Generar’ para crear una clave para tu cuenta.

   Ve a ‘Herramientas’ > ‘Preferencias’ > ‘Registros’, y deselecciona todas las opciones de registros.

¡Felicidades! Ahora puedes disfrutar de chats confidenciales, encriptados.

Empezar a usar OTR

Agregar un contacto

Pidgin

En Pidgin, ve a ‘Amigos’ > ‘Añadir amigo’ y teclea su dirección completa antes de presionar ‘Añadir’. La próxima vez que tu contacto esté en línea, recibirá una solicitud de autorización tuya.
Para empezar una conversación con un contacto en línea, haz doble clic en un amigo/contacto de tu lista, y haz clic en OTR > ‘Iniciar conversación privada’ en la ventana del chat.

Adium

En Adium, ve a ‘Contacto’ en la barra de herramientas superior > ‘Añadir contacto’. En ‘Tipo de contacto’, dando por hecho que tu contacto también está usando Jabber,

selecciona XMPP/Jabber, introduce su dirección completa en ‘ID de Jabber’, y haz clic en ‘Añadir.

Autenticar/verificar a un contacto

Lo ideal sería usar verificación por huella dactilar y, si conoces a la persona lo bastante bien, ambos os haréis una pregunta de la que sólo la otra persona conoce la respuesta.

Pidgin

Si aún no has verificado a un contacto, haz doble clic en su dirección para abrir una ventana de chat con él, ve a OTR en la ventana de chat y haz clic en ‘Autenticar amigo’. Puedes autenticarlo mediante:

- Una pregunta y respuesta:
    - Un buen método y personalizado.
- Un secreto compartido:
    - Tiene que ser haberse acordado previamente mediante un método de comunicación diferente, por lo que resulta menos útil.
- Verificación de huella digital:
    - Un método útil y seguro.
    - El único método por el que usuarios de Adium y Pidgin pueden autenticarse unos a otros.

En esa ventana, selecciona ‘Verificación manual por huella digital manual’ como el ‘Método’ y entonces verás la supuesta huella digital de tu contacto. Comprueba la huella y, si está bien, selecciona la opción para verificar que, efectivamente, es la huella correcta y haz clic en ‘Autenticar’.

Adium

Si aún no has autenticado a tu contacto, haz doble clic en su dirección para abrir una ventana de chat con él (aunque aparezca no estar conectado, aparecerá como desconectado y ‘no autorizado’ hasta que lo verifiques). Haz clic en el icono de candado y selecciona ‘Iniciar Conversación OTR Encriptada’. El candado debería cerrarse. Con la ventana de chat aún abierta, ve a la barra de herramientas superior en Adium, haz clic en ‘Contacto’ > ‘Encriptación’ > ‘Verificar’. Entonces verás la supuesta huella digital de tu contacto.

Comprobar huellas

Lo ideal sería que cada uno comprobara la huella del otro mediante un medio de comunicación que no fuera IM (correo, teléfono). Si no hay una forma segura de hacerlo, un amigo común o una tercera persona puede pasarle una versión incompleta de tu huella al contacto (por ejemplo, 0—A7-0 D—706-D 2—65–1 –3D-9C2 0-57B—1) por mensajería instantánea, y enviarte a ti la de tu contacto, para que ambos podáis comprobar la supuesta huella digital mostrada. Redactar partes de tu huella digital puede ayudar a evitar ataques de suplantación por parte de un man-in-the-middle (ataque por

intermediario).

Encontrar tu propia huella

Los usuarios de Adium pueden encontrar su huella digital en Adium > ‘Preferencias’ > ‘Avanzado’ (pestaña horizontal) > ‘Encriptación’ (pestaña en la columna de la izquierda).

Los usuarios de Pidgin pueden encontrar su huella digital abriendo una ventana de chat con un contacto, haciendo clic en el icono pequeño de amigo (a la derecha de ‘OTR’) > ‘Re/Autenticar amigo’ > ‘Verificación manual por huella digital manual’.

Por favor, ten cuidado: no permitas que Adium o Pidgin recuerden tu contraseña automáticamente, ya que puede que no se guarde de forma segura. Deberías introducir tu contraseña de Jabber manualmente cada vez que inicies una sesión.

Capítulo 7: Teléfonos & Llamadas De Voz/Video Por Internet

Seguridad móvil

Para muchos de nosotros, el teléfono inteligente tiene gran importancia y valor en nuestro trabajo y en la vida diaria. En efecto, las ventajas de estar constantemente conectados a nuestras cuentas de correo, navegadores, redes sociales, agendas; así como tener acceso a una cámara y grabadora de voz de alta calidad, hacen que sea una herramienta valiosa. Sin embargo, se trata de una herramienta que no es posible que sea segura.

La única solución para asegurar la información con teléfonos móviles sería usar teléfonos desechables con diligencia y cautela.

Riesgos del teléfono:

- Registro automático de tus ubicaciones actuales/anteriores.
- Recogida automática de metadatos, ya sea el número de teléfono y ubicación de cada interlocutor; números de serie únicos de los teléfonos involucrados; hora y duración de la llamada; número de tarjetas de llamadas telefónicas.
- Robo y pérdida de datos.
- Que se acceda de forma remota a la información del teléfono cuando se conecta a una red Wi-Fi pública.
- Que se acceda de forma remota a toda la información en cualquier momento que el teléfono esté encendido.
- Intervención, interceptación o grabación del teléfono/mensajería de voz.
- Activar de forma remota y encubierta el micrófono para grabar audio.
- Activar de forma remota y encubierta la cámara para hacer imágenes.

Vigilancia por emboscada de teléfonos

Todos los teléfonos filtran enormes cantidades de información sobre nosotros a las agencias de inteligencia y sabemos, por las revelaciones de Snowden, que los programas que recogen el audio completo de cada llamada individual dentro de un país dado están, cuanto menos, ya en funcionamiento y en período de prueba en algunos países. Este tipo de vigilancia es muy peligrosa para la democracia, no digamos para el periodismo, y puede permitir que se investigue con carácter ‘retroactivo’ de una forma muy invasiva de aquellos individuos, que despierten el interés de las agencias de inteligencia en un futuro.

Por tanto, vale la pena que cuando uses tu móvil lo tengas presente, ya sea por tí, por tus fuentes o por tus colegas, que pueden ser blanco de las agencias de inteligencia ahora o en un futuro. No son dispositivos seguros de comunicación, así que piensa cómo deseas usarlos.

Vigilancia de teléfono dirigida

Bajo riesgo

En un bajo nivel de riesgo, la amenaza es principalmente física, que alguien acceda al terminal. Si esto sucede, hasta un hacker muy poco sofisticado o la policía pueden decodificar tu contraseña (si está bloqueado por contraseña), así que esto sólo ofrece una protección mínima. Si estás en un bajo nivel de riesgo, asegúrate de hacer una copia de seguridad de la información y de la transmisión y enviar cuanto antes a una nube de almacenamiento segura cualquier video o grabación de sonido hechos en ese dispositivo.

También puedes usar aplicaciones para rastrear tu aparato si alguien lo hurta. Para iPhone, por ejemplo, Apple ofrece un app gratis llamada ‘Encuentra mi iPhone’ que te proporciona la ubicación actual de tu teléfono. Otra aplicación antirrobo gratis es ‘Prey’, que una vez comunicas que tu teléfono ha sido robado, grabará no sólo la ubicación actual del teléfono, sino también cualquier ubicación del teléfono registrada desde que se comunique el robo.

Medio riesgo

En un nivel de riesgo medio, puede que te encuentres con un contrario que trate de acceder a tu información, no sólo físicamente, sino de forma remota. Cuando conectas tu teléfono a una wifi pública, por ejemplo, un hacker no experto puede interceptar bastante información sobre ti y tus cuentas conectadas, como correo y redes sociales. Por lo tanto, en un nivel de riesgo medio, puede que ya te plantees evitar el teléfono inteligente como herramienta de trabajo, o al menos vigilarlo muy de cerca, cerrando aplicaciones después de su uso, apagando el wifi, y usando el modo avión cuando no necesites estar conectado.

> Nota sobre teléfonos inteligentes: los teléfonos inteligentes tienen muchos puntos vulnerables, algunos de los cuales están en el hardware y no se pueden corregir. Puedes usar software de código abierto en teléfonos inteligentes y hasta chats encriptados. Sin embargo, como descubrimos en ‘Proteger el Sistema’, cuando el hardware es vulnerable, el software no puede proporcionarte una seguridad real. Por lo tanto, a efectos de esta guía no trataremos estas aplicaciones.

Como demostró el reciente escándalo de hacking de teléfonos en el Reino Unido, hackers inexpertos que trabajaban para periodistas sin ética pudieron escuchar la mensajería de voz de terceras personas. Los investigadores privados también tienen la habilidad de ‘pinchar’ (es decir, escuchar a escondidas) no sólo la mensajería de voz, sino las llamadas hechas y recibidas por un número determinado. Por este motivo, deberías pensártelo dos veces antes de discutir cualquier cuestión delicada en tu teléfono (móvil o línea fija).

Alto riesgo

En un alto nivel de riesgo, un teléfono es básicamente tu adversario. Como mínimo, guarda tu ubicación y todos los metadatos asociados con el dispositivo y los pone a disposición de una agencia de inteligencia parte de Five Eyes. En el peor de los casos,

puede registrar de forma encubierta el contenido de todas tus llamadas, por no hablar de toda la información del teléfono, y puede automatizar el micrófono y la cámara para grabar audio e imágenes (si tiene cámara). Este tipo de vigilancia de teléfonos es muy fácil y básicamente tiene coste cero para las agencias de inteligencia, así que no tienes que ser necesariamente un blanco importante para ellos para que justifiquen este tipo de invasión de la privacidad.

La única forma verdaderamente segura de comunicarse por teléfono es usar teléfonos desechables.
Lo ideal es que tu teléfono desechable y tu teléfono habitual nunca emitan señales al mismo tiempo, ya que (si eres un objetivo), tu teléfono habitual puede recoger la señal de tu teléfono desechable, convirtiéndolo también un blanco.

Antes de usar un teléfono desechable, asegúrate de que el teléfono que usas habitualmente (p. ej. tu teléfono inteligente) no esté emitiendo señales. Poner el teléfono en modo avión, retirar la batería (no te molestes en intentarlo con el iPhone), apagarlo está bien, pero no basta. Haz todas estas cosas y después mételo en una jaula Faraday. Las soluciones más comunes son latas de galletas, algunos refrigeradores o incluso ¡cocteleras de acero inoxidable! El teléfono tiene que estar completamente aislado en metal (comprueba que funciona tratando de llamar al teléfono). Es una buena idea encontrar y llevar siempre contigo una lata pequeña en la que puedas meter tu teléfono, y, en una reunión importante, asegúrate de que todos los asistentes han hecho lo mismo (una lata de galletas grande funciona bien en este caso).

Un teléfono desechable es un teléfono barato, que puedes tirar, comprado con dinero en efectivo y de baja tecnología, con una tarjeta SIM de prepago que no esté registrada con tu nombre, que ha de usarse sólo con un fin concreto. En algunos países, puede que sea difícil comprar una tarjeta SIM sin registrar tus datos personales. Por tanto, lo ideal es comprar un teléfono de segunda mano, o tener un contacto que pueda obtener este tipo de tarjetas SIM.

Después de usar un tiempo el teléfono, puede quedar asociado a ti y atraer vigilancia, llegados a este punto deberías destruirlo y usar otro nuevo. Cambiar la tarjeta SIM no es suficiente, cada terminal telefónico tiene un número IMEI (International Mobile Equipment Identity , o identidad internacional de equipo móvil) que identifica tu teléfono. Si se ha identificado la tarjeta SIM como tuya, el IMEI también, así que será necesario que destruyas el teléfono.

Debido a que las agencias de inteligencia graban el audio completo de todas las llamadas, por no hablar de la facilidad con la que pueden grabar la llamada de uno de sus objetivos, deberías de evitar compartir información especialmente delicada, incluso con un teléfono desechable.

Llamadas de voz y vídeo por Internet

El software que provee llamadas de voz y video por internet (Voice over Internet Protocol, VoIP, protocolo de voz por internet), como Skype, es enormemente útil y conocido, y

Skype tiene 700 millones de usuarios. Sin embargo, Skype no ofrece mucha seguridad, y no existe todavía una alternativa segura, fácil de usar.

Entre las revelaciones de Snowden hay detalles sobre la capacidad de la NSA para interceptar y guardar comunicaciones por Skype. Deberíamos dar por sentado que todas las comunicaciones por Skype no son sólo entre nosotros y nuestros contactos, sino también con agencias de inteligencia.

Ejemplo: Glenn Greenwald cuenta que usó Skype en Hong Kong para llamar a David Miranda, su pareja, que estaba en Río, para decirle que recibiría algunos documentos encriptados por correo, y que los guardara de forma segura. Greenwald nunca mandó esos archivos, pero 48 horas más tarde, robaron el laptop de Miranda de su casa en Río.

Deberíamos también dar por sentado que no sólo las agencias más sofisticadas o quienes se aprovechan de los fallos de seguridad acceden de forma encubierta. Por ejemplo, se sabe que la policía secreta de Egipto ha comprado herramientas de intrusión en Skype y activistas ambientales que trabajan en Asia han informado de ataques man-in-the-middle (por intermediario) en Skype.

Se están desarrollando llamadas de voz y video seguras, entre los proyectos en curso están: Jitsi (ver https://jitsi.org) y Tox (ver https://tox.im). Aunque estos proyectos son alentadores, aún están en desarrollo y es demasiado pronto para saber qué grado de seguridad pueden ofrecer y qué facilidad de uso tienen.

Capítulo 8: Contraseñas

Todos los sistemas y herramientas mencionados en este libro usan contraseñas como método para identificar correctamente a los usuarios autorizados y protegerse contra el acceso no autorizado. Las contraseñas fuertes son vitales como defensa en todos los niveles de seguridad de la información.

Sin embargo, sé consciente de que las contraseñas de cuentas online son ante todo una defensa contra hackers que no trabajan para el Estado (que también son capaces de conseguir programas comerciales cada vez más sofisticados para descodificar contraseñas). Puede que a nivel estatal se acceda por la puerta trasera a tus cuentas online, lo que provoca que en último término tu contraseña no tenga valor alguno. Esta es una buena razón para encriptar tus correos. Puedes tener una contraseña de Hotmail increíblemente fuerte, pero esto no impide que de todos modos las agencias de inteligencia fuercen a Hotmail a entregarles todos tus correos (o más probable, interceptar y guardarlos sin permiso). Si tus correos están encriptados, todo lo que Hotmail puede entregar es un amasijo de código (hasta el momento) indescifrable.

Así que, si bien las contraseñas fuertes siempre son una buena idea, aquellas contraseñas que protegen tu sistema (p. ej. encriptación del disco duro) y tus programas de encriptación son mucho más importantes que las contraseñas de las cuentas online.

Riesgos:

- Olvidar y perder contraseñas.
- Burlas contraseñas mediante accesos por puerta trasera (cuentas online).
- Hacking (hacking de contraseñas relativamente inexperto).
- Decodificación de contraseñas (experto).
- Programas para registrar las teclas pulsadas.
- Revelar una contraseña por la fuerza.

Acciones de InfoSec:

- Aprender a crear contraseñas fuertes.
- Usar el gestor de contraseñas KeePassX (si confías en tu sistema). KeePassX es un gestor de contraseñas de código abierto que puede generar y guardar nombres de usuario y contraseñas en una base de datos local, encriptada y protegida por tu contraseña maestra. Está disponible para Linux, Mac y Windows.
- Guardar las contraseñas más importantes solamente en tu cabeza.
- Usar volúmenes escondidos para archivos importantes encriptados.

Decodificación de contraseñas: entender los riesgos

Si tu sistema no es seguro, descodificar tu contraseña durante un ataque dirigido es simple. Alguien en tu contra podría introducir un registrador de teclas en tu sistema para

guardar cada pulsación físicamente o de forma remota. Esto querría decir que captura todo lo que escribes, incluyendo tu contraseña. No es un ataque altamente sofisticado, pero invalida totalmente otras medidas de seguridad. Por esto, es muy importante asegurar tu sistema desde el primer momento, como indicamos en los capítulos uno y dos.

No obstante, si tu sistema es seguro y tu adversario no puede usar herramientas de registro de teclas, un atacante puede intentar descodificar las contraseñas que protegen tu sistema, software y cuentas (y esto puede ser o un hackeo a gran escala que afecte a miles de usuarios, o un ataque dirigido contra un individuo).

En todo el mundo, las autoridades usan programas de descodificación de contraseñas, pero también están disponibles versiones más complejas como productos comerciales. Un descodificador de contraseñas puede probar automáticamente como mínimo ocho millones de contraseñas por segundo y puede funcionar durante días en varios ordenadores simultáneamente. Para un blanco de perfil alto, un decodificador de contraseñas puede funcionar en múltiples ordenadores durante meses.

Los descodificadores de contraseñas prueban primero las contraseñas más comunes. Una contraseña típica consiste en una raíz con un apéndice. La raíz no es necesariamente una palabra del diccionario, pero es algo pronunciable. Un apéndice es un sufijo (90% de las veces) o un prefijo (10% de las veces). Un programa de decodificación empezaría de forma típica con un diccionario de 1. 000 contraseñas comunes, como “letmein,” “temp,” “123456,” y así, y después probarlos con alrededor de 100 apéndices de sufijo comunes: “1,” “4u,” “69,” “abc,” “!,” etc. Se cree que alrededor de una cuarta parte del total de contraseñas puede ser descifrada con sólo estas 100.000 combinaciones.

Los descodificadores usan diferentes diccionarios: palabras en inglés, nombres, palabras extranjeras, patrones fonéticos, etc. para las raíces; dos dígitos, fechas, símbolos suelto, etc. para los apéndices. Utilizan los diccionarios con varias mayúsculas y substituciones comunes: “$” para “s”, “@” para “a,” “1” por “l” etcétera. Esta estrategia descifra rápidamente alrededor de dos tercios de todas las contraseñas.

El atacante puede introducir en el descodificador cualquier información personal disponible sobre el creador de la contraseña. Un buen decodificador de contraseñas probará nombres y direcciones de la libreta de direcciones (códigos postales son un apéndice común), fechas significativas, y cualquier otra información personal que tenga.

Si tu hardware no es seguro (¡la raíz de todos los problemas!), es posible lanzar un ataque especialmente amplio. Un atacante puede indexar el disco duro de un blanco y crear un diccionario que incluya cualquier cadena de caracteres, incluidos los archivos borrados. Si alguna vez has guardado tu contraseña en un archivo extraño, o si el programa lo ha guardado en la memoria, este proceso dará con él y contribuirá al proceso de descodificar tu contraseña.

Cómo crear una contraseña fuerte
Una contraseña fuerte es la que elude el proceso de descodificación descrito.

Gestor de contraseñas

Una opción es usar software de código abierto que gestione contraseñas como KeePassX para generar aleatoriamente contraseñas alfanuméricas, largas (también con símbolos, si se admiten para una contraseña concreta), y después guardarla en tu propia base de datos encriptada de contraseñas. Si confías en las otras capas de tu sistema, esta es una opción bastante sólida.

Además, es una buena manera de guardar múltiples contraseñas complicadas para múltiples cuentas, ya que KeePassX también tiene campos para insertar URLs, nombres de cuentas y comentarios para cada contraseña, de modo que puedes guardar de forma segura toda la información que necesites. Las contraseñas generadas aleatoriamente no son puede memorizarse, lo que sirve como función de seguridad. No obstante, KeePassX te permite simplemente copiar y pegar contraseñas desde la base de datos, así que ni siquiera tienes que escribirlas.

Hay cierto debate sobre la efectividad de estos programas para generar contraseñas aleatorias, pero al cerebro humano también se le da bastante mal el azar, de modo que sigue siendo una de las mejores opciones que tenemos por el momento.

Necesitarás crear una contraseña para KeePassX, tiene que ser extremamente fuerte. Deberías intentar guardar esta contraseña sólo en tu cabeza.

Estrategia Schneier

Deberías utilizar contraseñas creadas manualmente para encriptar todo tu sistema, cualquier USB encriptado o archivos de suma importancia (p. ej. documentos de la fuente) y tu gestor de contraseñas. Estas contraseñas importantes deberían de estar guardadas solamente en tu memoria, por tanto, tienen que ser fáciles de memorizar.

Por supuesto, para minimizar cualquier daño en caso de que una contraseña llegara a verse comprometida, tendrías que evitar reutilizar las contraseñas.

Para crear de manera manual una contraseña, recomendamos la ‘estrategia Schneier’, un método recomendado por Bruce Schneier, un criptógrafo y experto en seguridad de prestigio internacional.
Schneier aconseja elegir frases fáciles de recordar y reducir las palabras a iniciales, símbolos y números con el fin de convertirla en contraseña.

Por ejemplo, “este cerdito fue al mercado” puede convertirse en “ecfue@lmrkd”. Esa contraseña de nueve caracteres no estará en el diccionario de nadie. Escoge tu propia frase, algo personal, pero no relacionado obviamente contigo mediante datos públicos. He aquí algunos ejemplos:

- Cyt7amhtmcdpai. . . = Cuando yo tenía siete años, mi hermana tiró mi conejo de peluche al inodoro.

Wow. . . eshf = Wow, ese sillón huele fatal.

- Hmti3mp0e1gnml~ = Hace mucho tiempo, en una galaxia no muy lejana.
- hEMMlcw55:utvmecer@gur@ uTVM,TPw55:utvm,tpwstillsecure = Hasta este mismo momento, la contraseña w55:utvm era segura.

(Por supuesto, no uses ninguno de los ejemplos anteriores, ahora que las hemos usado, ya no son válidas como contraseñas fuertes).

Si te fuerzan a revelar una contraseña

Esperemos que nunca te encuentres en esta situación. Pero, supongamos que un grupo o agencia con malas intenciones te ha interceptado cuando llevabas una memoria USB encriptada (con tus archivos más importantes o documentos de tu fuente), y están dispuestos a llegar a medidas extremas para obtener la contraseña que les permita desencriptar esa memoria. ¿Qué haces?

En casos así, puede ser de ayuda tener en tu lector USB un volumen oculto. Un volumen oculto no es visible para nadie y no parece ocupar espacio en el lector. Como tal, puede sobreescribirse fácilmente. Sin embargo, esto quiere decir que el volumen visible encriptado puede servir como señuelo y proporcionarte una negación plausible. En el volumen encriptado visible, puedes guardar archivos que podrían razonablemente requerir seguridad y encriptación, y este volumen tiene su propia contraseña. Sin embargo, el volumen encriptado oculto se asienta de forma no detectable bajo el volumen visible, y tiene una contraseña separada.

Puedes crear un volumen encriptado oculto con TrueCrypt (ver capítulo 4). Este método puede ayudar a proteger la información si intentan interceptarla, pero no si se pierde, Puede destruirse o sobreescribirse fácilmente, por lo que deberías hacer siempre una copia de seguridad de los archivos importantes.

(Buena parte de este capítulo se ha adaptado del blog de Bruce Schneier, https://www.schneier.com/ . Agradecemos al Sr. Schneier el permiso para usar su trabajo).

Glosario

Término	Definición
Air-gapped (Aislamiento)	Una medida de seguridad por la cual un laptop se mantiene completamente desconectado de la red, separado de redes locales e internet
Puertas traseras	Vulnerabilidades de seguridad encubiertas, que permiten sortear los mecanismos de seguridad conocidos del sistema, permitiendo acceso no detectable al ordenador o a su información.
BIOS	'Basic Input/Output System' (Sistema Básico de Entrada/Salida), un conjunto de instrucciones en el firmware que controlan operaciones de entrada y salida
Bridges(Tor) (Puentes)	Nodos de Tor (ordenadores que reciben tráfico de entrada a la red Tor y lo transmiten) que ayudan a sortear la censura
Emboscada/Dragnet	Sistema de vigilancia masiva llevado a cabo por medio de programas que filtran y recogen la información online y las telecomunicaciones a nivel mundial
Jaula Faraday	Un recipiente metálico que impide la entrada o fuga de un campo electromagnético
Firmware	Software programado en el hardware que proporciona instrucciones para que un dispositivo físico pueda comunicar con el resto del sistema (incluye BIOS)
Hardware	Los elementos físicos que componen un sistema informático
Malware	Software malicioso, con frecuencia spyware, diseñado para interferir o dañar el sistema de un ordenador
Ataque de Man-in-the-middle(hombre-en-el-medio)	Interceptación encubierta de comunicaciones, mediante la suplantación

	del objetivo del ataque
Metadatos	Datos sobre datos
Middleware	Software que permite el intercambio de información entre dos programas separados y a menudo, ya existentes p.ej. permite a los programas acceder a una base de datos
Open source (Código abierto)	Software distribuido libremente, cuyo código fuente está disponible públicamente
Sistema operativo	Software que controla el ordenador cuando se inicia, le dice al ordenador qué hacer y cómo hacerlo, y es la interfaz a través de la cual utilizas el ordenador

Sobre los autores

Silkie Carlo es una periodista y activista afincada en Londres. Se licenció en Ciencias Políticas, Psicología y Sociología por la Universidad de Cambridge en el 2012, donde investigó sobre la posibilidad de revertir la justificación del sistema, usando WikiLeaks como ejemplo. Silkie ha trabajado con informantes de inteligencia y ha escrito artículos sobre informantes para VICE. Ocasionalmente, da clases de Ciencias Sociales además de trabajar en el campo de la seguridad de la información.

Arjen Kamphuis es co-fundador y desde el 2005 director jefe de tecnología en Gendo (http://www.gendo.ch/en/blog/arjen). Anteriormente había trabajado para IBM como arquitecto de tecnología de la información, formador y asesor informático. Como director jefe de tecnología asesora en materia de política tecnológica a varios gobiernos nacionales, organizaciones sin ánimo de lucro y empresas de la lista Fortuna-500. Desde 2009, Arjen ha estado formando a periodistas, políticos, abogados, trabajadores en materia de derechos humanos e informantes para defender sus comunicaciones y datos de intrusiones o manipulaciones de gobiernos o corporaciones.

–

Te agradeceríamos mucho cualquier comentario que quieras hacernos sobre este libro.
Por favor enviar un correo a infosec@tcij.org.
KeyID :0x7EF8DE32
FP: D0C5 A200 A49B E194 7AE4 A7C8 4DD6 A68E 7EF8 DE32
También puedes usar esta dirección para cualquier pregunta técnica o consejo.
Este manual se está traduciendo al árabe, chino, francés, alemán, portugués y otros idiomas.

Por Silkie Carlo
y Arjen Kamphuis

La edición en español y su distribución se ha realizado con la colaboracón de Xnet