A la defensa del disenso

A la defensa del disenso

Represión digital y defensa criptográfica de movimientos sociales

GLENCORA BORRADAILE

OREGON STATE UNIVERSITY
CORVALLIS, OR

open.oregonstate.education/defensadeldiseno

Contenido

Parte 2: Represión digital de movimientos sociales (en EUA)

Parte 3: Defensa de los movimientos sociales (en EUA)

Agradecimientos

Gracias a Michele Gretes por codesarrollar el CS175, y al Centro de Defensa de las Libertades Civiles por capacitarme y ayudarme con los borradores de este libro. También agradezco al mismo centro por crear un espacio para instruir a los activistas en seguridad digital.

Introducción: el porqué de la seguridad digital

En el verano de 2013, Edward Snowden sacudió al mundo con la divulgación de una mina de documentos de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), de la Agencia Central de Inteligencia (CIA, por sus siglas en inglés) y de un sinfín de otras agencias globales de tres letras. Durante más de un año hubo revelaciones semanales, si no diarias, de cuán extenso era el potencial para reunir información de dichas agencias, en especial las de Estados Unidos. Se percibía que la NSA tenía la capacidad de obtener cualquier información no cifrada que pasara por internet o por redes telefónicas, además de algunas informaciones de cifrado débil y algunas otras que no estuvieran cifradas en servidores corporativos. Esta percepción es cercana a la verdad.

En ese momento me encontraba involucrada en el activismo ambiental y estaba consciente de cómo los movimientos sociales habían padecido históricamente la represión del Estado a través del espionaje. La vastedad de la información que la NSA y la CIA eran capaces de recabar implicaba que los esfuerzos de represión por parte del Estado eran mucho más sencillos y eficaces. Entre más información conozca el Estado sobre tus actividades, más fácil le será interferir en tus metas.

Me preocupé. ¿Podríamos combatir el cambio climático, con las probabilidades en contra de todos los grupos que trabajaban para ello? ¿Y qué hay del racismo sistémico? ¿Teníamos alguna esperanza?

No mucho después de las revelaciones de Snowden, me asocié con el Centro de Defensa de las Libertades Civiles (CLDC, por sus siglas en inglés), una organización sin fines de lucro que brinda apoyo legal a los movimientos sociales que "buscan desmantelar las estructuras políticas y económicas que subyacen a la desigualdad social y la destrucción ambiental". El CLDC brinda capacitación para conocer los derechos legales de los participantes en movimientos sociales, con énfasis en cómo proteger e invocar los derechos de la Primera y la Cuarta Enmiendas: los derechos a la libre expresión y a no sufrir un allanamiento arbitrario. La vigilancia en masa mina estos derechos. Esto es claro en relación con los derechos de la Cuarta Enmienda, pero en cuanto a los de la Primera, académicos legales suelen señalar este *efecto escalofriante*: los ciudadanos limitan su libre expresión si saben que se les vigila. Para complementar las capacitaciones legales del CLDC, comencé a dar capacitaciones regulares sobre seguridad digital para activistas, con foco en la premisa de que **la codificación es la única forma de proteger tus derechos de la Primera y la Cuarta Enmiendas en el mundo moderno de la vigilancia en masa**. Este libro surgió de dichos esfuerzos educativos.

Descargar una aplicación “segura” no basta

No es suficiente descargar una aplicación “segura”. En primer lugar, ¿qué significa “segura”? La seguridad es un concepto complejo, subjetivo y de muchas facetas. Aunque estar completamente libre de riesgo suele ser algo inalcanzable, en especial cuando se trata de tecnologías digitales, es posible tener protecciones relativamente fuertes. Para evaluar o al menos explicar las protecciones relativas de una app (y convencer a un grupo de personas de aprovecharlas) se requiere cierto entendimiento de la criptografía y de cuál información está en riesgo (y con cuánta probabilidad) al usar cierta app o servicio digital.

Nuestras capacitaciones tan solo tocan la superficie de la información que me gustaría impartir. Los participantes en movimientos sociales suelen ser gente ocupada y quieren recomendaciones de seguridad digital simples y factibles de personas en quienes confían.

Mi meta con este libro (y el curso que lo acompaña en la Universidad Estatal de Oregon, CS175: Communications Security and Social Movements) es aumentar la cantidad de personas que saben lo suficiente como para dar dichas recomendaciones, o que al menos saben cómo y dónde aprender más acerca de ellas.

Alcance político de este texto

Como se puede inferir de las referencias a la Primera y Cuarta Enmiendas, este libro está basado en el ámbito político de Estados Unidos. Aunque mucho de esta obra será relevante fuera de Estados Unidos, se recomienda que quien aplique estos conocimientos en otros países busque apoyo adicional.

Perspectiva de este texto

Este libro no pretende ser exhaustivo, por tres razones:

1. Quiero que este libro sea accesible para cualquier persona con curiosidad. Entrar en más detalles sobre criptografía requeriría cierto nivel de conocimiento de matemáticas universitarias. También considero que no es necesario comprender protocolos específicos de criptografía para hacer recomendaciones racionales de seguridad digital (para ello, nos podemos apoyar en los expertos en ciberseguridad).
2. El estado de la vigilancia en masa y las aplicaciones disponibles para contrarrestar la vigilancia cambian constantemente. Incluso, al tiempo que doy los toques finales a este libro, estoy resistiendo los deseos de incluir las noticias más recientes sobre el potencial de vigilancia del Estado.

3. Quiero que este libro sea suficientemente corto para leerse en un fin de semana.

Este libro consta de estas tres partes.

Parte 1: Introducción a la criptografía

Esta es una introducción básica a la criptografía: presenta lo suficiente como para comprender lo básico acerca de cuál información está protegida, cuál no lo está y por qué. Algunos conceptos interesantes (por ejemplo, *secreto hacia adelante y cadena de bloques*) se han dejado de lado, pues sentí que estos temas avanzados podrían abrumar a mi audiencia. Sin embargo, tras leer la Parte 1, el lector con curiosidad podrá apreciar, por ejemplo, los artículos de Wikipedia sobre temas más avanzados, como los ya mencionados de secreto hacia adelante y cadena de bloques.

Al describir protocolos criptográficos, muchos se valen de personajes: Alice envía mensajes a Bob y Eve podría estar espiando sus comunicaciones. El curso que acompaña este libro se centra en los movimientos sociales de la era de la lucha por los derechos civiles, en especial en los movimientos relacionados con el Ejército Negro de Liberación y en su represión por el Estado.

Con el mismo propósito de ilustrar con ejemplos, en lugar de referir a Alice, Bob y Eve, se usa a lo largo del libro el ejemplo de Assata, quien se comunica con Bobby y Edgar los espía:

1. Assata Shakur fue miembro del Ejército Negro de Liberación y del Partido Pantera Negra a inicios de los años 70, fue objetivo del FBI (como se describe en el capítulo Mecanismos de represión de movimientos sociales, y sigue siendo refugiada política en Cuba.
2. Bobby Seale fue el cofundador del Partido Pantera Negra en la época de la lucha por los derechos civiles y también fue sujeto de vigilancia y acoso por parte del FBI.
3. J. Edgar Hoover fundó el FBI y se le ha considerado responsable de la vigilancia y esfuerzos represivos del FBI. Ocasionalmente, donde es apropiado, se alude a él como “el intermediario” (por ejemplo, en el capítulo El intermediario, donde “ataque de intermediario” es un término estándar de criptografía).

Aunque es probable que el resto de este libro requiera actualizaciones significativas en los siguientes años, es posible que la Parte 1 supere el paso del tiempo.

Parte 2: Represión digital de movimientos sociales (en EUA)

Esta es una parte bastante triste, puesto que visualiza lo siguiente:

1. Cómo han sido reprimidos históricamente los movimientos sociales en EUA (donde la vigilancia juega un papel), en el capítulo Mecanismos de represión de movimientos sociales.
2. Las estrategias de vigilancia y otras amenazas digitales que están en uso en EUA, en el

capítulo Amenazas digitales a movimientos sociales. En esta parte se emplea el término Estado para referirse a una constelación de organizaciones gubernamentales y no gubernamentales que constituye las estructuras establecidas de poder con los recursos y motivación necesarios para desplegar un amplio rango de estrategias represivas y medidas técnicas sofisticadas en contra de los movimientos sociales.

Esta parte es relativamente corta con el fin de avanzar a la última parte, que brinda más empoderamiento. En la Parte 2 se presentan *ejemplos ilustrativos* para dar una visión general de la forma en que se usan los mecanismos de represión de movimientos sociales y del tipo de vigilancia y otras amenazas digitales que están en juego. En especial en el capítulo Amenazas digitales a movimientos sociales nunca estaremos actualizados, pues nuevas amenazas y capacidades están en desarrollo y aplicándose constantemente. Es nuestra esperanza que cualquiera que lea esta parte continúe a la brevedad posible con la última parte.

Parte 3: Defensa de los movimientos sociales (en EUA)

La intención de esta parte es brindar empoderamiento. Comienza con el análisis de las amenazas (las cuales dependen del país y del contexto), para luego avanzar hacia las clases de herramientas disponibles para proteger tu información.

Hablamos de clases de herramientas y no de herramientas específicas porque estas pueden ir y venir dependiendo de si los proyectos o aplicaciones que las apoyan fracasan o aparecen, y no sería factible actualizar este libro múltiples ocasiones al año. Esta sección depende del país, pues la disponibilidad o el riesgo asociado con el uso de ciertas herramientas puede depender del contexto político. Por ejemplo, puede suponer un reto mayor usar Tor (un buscador anónimo de internet, que se discute en los capítulos Enrutado anónimo y Proteger tu identidad) en ciertos países que practican la censura de forma generalizada, como China.

Qué aprender a continuación

- ¿Qué es el cifrado?
- Mecanismos de represión de movimientos sociales

Recursos externos

- Civil Liberties Defense Center. “About.”

PARTE 1: INTRODUCCIÓN A LA CRIPTOGRAFÍA

¿Qué es el cifrado?

Lo que aprenderás

1. Los elementos básicos de la codificación: *texto en claro*, *texto cifrado*, *algoritmo criptográfico* (o protocolo criptográfico) y *clave criptográfica*
2. Cómo funcionan algunos métodos clásicos de cifrado
3. Formas en las cuales se puede romper el cifrado
4. Un cifrado indescifrable

Comencemos con lo más básico: el cifrado con papel y pluma, antes de avanzar hacia métodos de cifrado más complejos, los cuales son posibles gracias a las computadoras.

El cifrado es el proceso de codificación de un mensaje con la intención de que solo pueda ser descodificado (y leído) por el o los destinatarios. El método por el cual se codifica un mensaje original, o *texto en claro*, se conoce como *algoritmo criptográfico* o *protocolo criptográfico*. En casi todos los casos, la intención no es que el algoritmo criptográfico permanezca secreto. El mensaje codificado, ilegible, cifrado, se conoce como *texto cifrado* y puede compartirse con seguridad. La mayoría de los algoritmos criptográficos requieren de una parte adicional, la clave *criptográfica*, para cifrar y descifrar mensajes (codificar y decodificar).

Un código sencillo: el cifrado César

Consideremos el primer y quizás más sencillo cifrado: *el César*. En este, cada letra del mensaje se sustituye por la letra situada a un número específico de posiciones en el alfabeto. Por ejemplo, supongamos que se desea cifrar el siguiente texto en claro:

```
SI VOTAR CAMBIARA ALGO SERÍA ILEGAL
```

Si se sustituye cada letra del mensaje por la letra situada tres posiciones adelante en el alfabeto, de manera que `A` se convierte en `D`, `B` en `E`, y así sucesivamente hasta que `Z` regresa al inicio del alfabeto y se convierte en `C`, el texto en claro se convierte en el siguiente *texto cifrado*:

```
VL YRWDU FDOELDUD DNJR VHULD LNHJDN
```

Para descifrar este mensaje, el destinatario haría lo opuesto: sustituir cada letra del mensaje por la letra situada tres posiciones atrás en el alfabeto, de manera que `Z` se convierte en `W`, y `A` se

va hacia el final del alfabeto para convertirse en `X`. Para que el destinatario pueda descifrar el mensaje (rápidamente), debe conocer la *clave* del cifrado.

En el caso del cifrado César, la clave es la cantidad de lugares que se desplaza cada letra en el alfabeto; en este ejemplo, el número `3`. Una clave de cifrado César también puede representarse con la letra del alfabeto que resulte de la traducción de `A`. Por ejemplo, un desplazamiento de `3` lugares daría la clave `D`; un desplazamiento de `26` daría la clave `Z`, y un desplazamiento de 0 (desplazamiento de identidad), daría la clave `A`.

Repasemos los términos. En este ejemplo, para aplicar el algoritmo o protocolo criptográfico, deben seguirse estas simples instrucciones: "Para cifrar, sustituir cada letra del mensaje en texto en claro por la letra que se encuentre ***n*** letras hacia adelante. Para descifrar, sustituir cada letra del mensaje en texto cifrado por la letra que se encuentre ***n*** letras hacia atrás." La clave sería el valor del desplazamiento: ***n***.

Por supuesto, el César no es un cifrado fuerte y no deberías confiar en él para mantener tus planes en secreto. Todo lo que un adversario necesitaría para descifrar tu código secreto (texto cifrado) es probar todos los desplazamientos posibles hacia atrás en el alfabeto. No hay muchas posibilidades, así que no tomaría mucho; puesto que la clave `A` hace que el texto en claro y el cifrado sean iguales, solo hay veintiséis claves posibles. Este tipo de ataque se conoce como ataque de fuerza bruta; en este, un adversario intenta descifrar un mensaje cifrado probando todas las claves posibles. Este tipo de ataque es factible en el caso del cifrado César porque hay muy pocas claves posibles.

Un cifrado ligeramente más complicado: el Vigenère

El cifrado Vigenère consiste en un conjunto de cifrados César, cada uno con su propia clave. La clave suele presentarse como una palabra y la posición de cada letra de la palabra en el alfabeto indica cómo se desplaza la letra `A`, como en el cifrado César. Es más fácil ver esto en un ejemplo. Supongamos que se desea cifrar el siguiente texto en claro:

```
RESPETA MI EXISTENCIA O ESPERA RESISTENCIA
```

con la siguiente clave:

```
PODER
```

Haz lo siguiente:

- Codifica cada quinta letra, empezando con la primera letra del texto en claro (`R`, `T`, `X`...), con un cifrado César que iguale `A` con `P` (un desplazamiento de 16 o un cifrado César con clave `P` o `16`).
- Codifica cada quinta letra, empezando con la segunda letra del texto en claro (`E`, `A`, `I`...),

con un cifrado César que iguale `A` con `O` (un desplazamiento de 15 o un cifrado César con clave `O` o `15`).
- Codifica cada quinta letra, empezando con la tercera letra del texto en claro (`S`, `M`, `S`...), con un cifrado César que iguale `A` con `D` (un desplazamiento de 3 o un cifrado César con clave `D` o `3`).
- Codifica cada quinta letra, empezando con la cuarta letra del texto en claro (`P`, `I`, `T`...), con un cifrado César que iguale `A` con `E` (un desplazamiento de 4 o un cifrado César con clave `E` o `4`).
- Codifica cada quinta letra, empezando con la quinta letra del texto en claro (`E`, `E`, `E`...), con un cifrado César que iguale `A` con `R` (un desplazamiento de 18 o un cifrado César con clave `R` o `18`).

La aplicación de estos cinco cifrados César resulta en el siguiente texto cifrado:

```
CPPMNEM XE NITPPNXÑFW X OENAAL DBOQDFBJLSM
```

Para descifrar este cifrado, supongamos que un adversario conoce la longitud de la clave. El adversario intentaría descifrar el texto con todas las palabras posibles de tres letras (o en general, cualquier secuencia de tres letras). En este ejemplo, se requerirían cuando mucho `25 x 26 x 26 = 16,900` intentos, lo cual es más de lo que puede lograrse fácilmente a mano, pero una computadora puede hacerlo sin mayor complicación. Si el adversario no conoce la longitud de la clave, tendría que intentar con muchas más claves posibles para descifrar el cifrado con este método de fuerza bruta (tantas como `25 + 25 x 26 + 25 x 26 x 26 + …`). Observa que entre más larga es la clave, más difícil es aplicar métodos de fuerza bruta, y un adversario deberá trabajar más para descifrar el texto.

En contexto: La indescifrable libreta de un solo uso

Un cifrado Vigenère cuya clave sea una secuencia de letras elegidas *al azar* y que sea al menos tan largo como el mensaje en texto en claro hace posible un cifrado conocido como *libreta de un solo uso*. Históricamente, la clave misma se habría escrito en una libreta o papel y distribuido a las partes involucradas. Para cifrar, se aplica un cifrado Vigenère al texto en claro, donde cada letra de la libreta se usa solo una vez antes de proceder con la siguiente letra. El descifrado depende de que se tenga esta libreta de un solo uso, así como la posición inicial en la clave. Es *imposible* descifrar este cifrado sin la clave; es decir, es imposible adivinar la clave y descifrar el texto ya cifrado aun disponiendo de tiempo y recursos ilimitados. Esto es así porque un texto cifrado de una longitud dada puede corresponder con cualquier texto en claro de la misma longitud. Por ejemplo, sin conocer la clave aleatoria, el texto cifrado con libreta de un solo uso `SO DU CYFUK` podría (con igual probabilidad) corresponder al texto en claro `SI SE PUEDE`, o a `YO NO PUEDO`. Sin la clave no hay forma de saber cuál es el mensaje original. Omitir espacios entre palabras o cifrar los espacios entre palabras (usando un alfabeto de veintiocho

letras `ABCDEFGHIJKLMNÑOPQRSTUVWXYZ_`, donde `_` representa un espacio) haría mucho más difícil adivinar incluso el conjunto de posibles mensajes en texto en claro.

Por supuesto, la libreta de un solo uso tiene el problema práctico de cómo intercambiar la clave (la libreta misma), la cual sería tan larga como el mensaje o como la longitud total de todos los posibles mensajes futuros. A pesar de eso, se ha usado históricamente en grupos que comparten una libreta de un uso en persona y que luego se envían mensajes por canales inseguros. A finales de los años 80, el Congreso Nacional Africano (ANC, por sus siglas en inglés), que luchaba contra el *Apartheid* en Sudáfrica en aquel momento, empleó libretas de un uso para cifrar mensajes entre simpatizantes extranjeros y operativos dentro del país. Las libretas de un uso (las claves) eran transportadas físicamente por un sobrecargo de confianza que trabajaba en la ruta Ámsterdam-Johannesburgo. Dicho sea de paso, el ANC también computarizó el cifrado y descifrado y de esta manera hizo posible traducir mensajes cifrados en secuencias tonales transmitidas por una conexión telefónica y grabada o recibida en una contestadora de mensajes. Esto permitió la comunicación asincrónica.

Qué aprender a continuación

- Criptografía moderna

Recursos externos

- Jenkin, Tim. "Talking with Vula: The Story of the Secret Underground Communications Network of Operation Vula." Mayibuye: Journal of the African National Congress, octubre de 1995.

Criptografía moderna

Se recomienda leer el capítulo ¿Qué es el cifrado? antes de seguir con este.

Lo que aprenderás

1. Las implicaciones de la longitud de una clave en la seguridad
2. Qué es el software de fuente abierta y por qué es importante para la seguridad

La criptografía moderna no es algo que se hace a mano. Las computadoras lo hacen por uno, y los detalles de los algoritmos que emplean se encuentran más allá del alcance de este libro. Sin embargo, hay ciertos principios que ayudan a comprender mejor y a evaluar las herramientas de seguridad digital modernas.

Seguridad que requiere ataques de fuerza bruta

Los protocolos criptográficos modernos están diseñados para obligar al adversario (quien no posee la clave criptográfica) a emplear (casi) tanto tiempo como el que tomaría probar cada una de las claves posibles para descifrar el código. Recordemos que intentar cada una de las claves posibles se conoce como *ataque de fuerza bruta*. Los parámetros de un protocolo dado se eligen de manera que dicha cantidad de tiempo sea impráctica. Por lo general, el parámetro más importante es la longitud de la clave. Al igual que en el cifrado Vigenère, las claves más largas hacen necesario explorar más claves posibles para adivinar la clave correcta. Conforme pasa el tiempo y el poder y rapidez de procesamiento de las computadoras se incrementan, las claves deben ser más largas para garantizar que los ataques de fuerza bruta no sean factibles. Por esta razón, muchos protocolos criptográficos mencionarán el tamaño de la clave en términos del número de bits que se requiere para representar la clave. Las computadoras representan la información, incluyendo claves criptográficas, en binario (usando 0 y 1). Así como los números 0 a 9 representan los *dígitos* de un número decimal, los números 0 y 1 representan los *bits* de un número binario. ¿Cuántos números decimales de tres dígitos hay? 10 $\cdot$ 10 $\cdot$ 10 = 10^3 = 1000; es decir, los números del 0 al 999. De igual forma, hay 2 $\cdot$ 2 $\cdot$ 2 $\cdot$ 2 = 2^4 = 16 números binarios de cuatro bits.

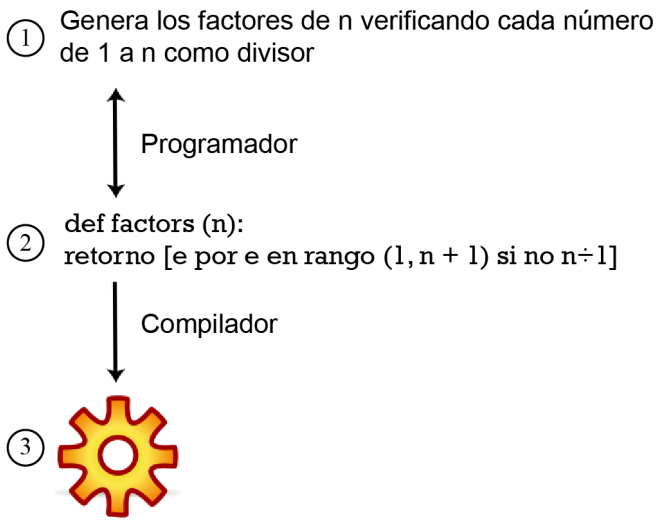
Por ejemplo, el protocolo criptográfico AES se conoce como AES-128 o AES-256 cuando usa el protocolo con claves de cifrado de 128 bits o de 256 bits, respectivamente. En el AES-128 hay 2^{128} = 340282366920938463463374607431768211456 claves posibles. En el AES-256 hay 2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936 claves posibles. Intentar cada una de las posibles claves, o incluso una pequeña fracción de ellas, en el AES-256 es inviable en términos computacionales, incluso considerando el poder de cómputo de Estados-nación como Estados Unidos.

La secrecía no garantiza la seguridad

Desde tan temprano como el siglo XIX, los matemáticos han tenido como criterio estándar que los esquemas criptográficos deben ser suficientemente seguros, aunque el método usado no sea secreto. Esto se basa en el siguiente principio: Si la seguridad requiere que el método permanezca secreto, entonces se corre el riesgo de que todos los mensajes que se hayan cifrado o vayan a cifrarse con ese método alguna vez sean revelados si dicho método llega a descubrirse. Por otro lado, si el método solo requiere que la clave sea secreta, entonces solo se arriesga que los mensajes cifrados con esa clave en particular sean divulgados si se vulnera la clave.

La transparencia es lo que da seguridad

De hecho, entre más transparencia haya en un método criptográfico, más confianza puedes tener en su seguridad. Para comprender esto, considera cómo se crea un programa de cifrado (o cualquier programa de cómputo). Todo comienza con un algoritmo para hacer el cifrado. Un programador convierte este algoritmo en un código fuente de cómputo. Una computadora compila dicho código fuente en el programa o aplicación que se ejecuta en tu computadora o teléfono.



Del algoritmo al código fuente, al código fuente compilado

Un buen programador debería poder traducir de un algoritmo (1) al código fuente (2) y de vuelta. Un profesional de la seguridad podría evaluar la seguridad de un protocolo criptográfico con base en el algoritmo, pero también debería evaluar el código fuente para estar seguro de su correcta implementación (de que no hay errores o *bugs*, intencionales o no). Sin embargo, como usuario, solo se tendría acceso al programa compilado (3). Desafortunadamente, solo con el código compilado es imposible que persona alguna reproduzca el código fuente.

Por tanto, a menos que el código fuente esté disponible, nadie puede estar seguro de que las declaraciones de seguridad de una app sean ciertas. Por otro lado, tan solo con el programa compilado, un pirata informático puede intentar penetrar la seguridad de la app. Muchos proyectos de software ponen su código fuente a disposición del público; a dicho software se le conoce como *software de código abierto* e incluye muchos proyectos reconocidos, de seguridad y de otra naturaleza, como Signal, Firefox y Linux. La alternativa es el *software de código cerrado*, común en proyectos que buscan monetizar su producto a través de la venta de software propietario, como Safari, Internet Explorer, Windows y Mac OS. Aunque es posible evaluar la seguridad del software de código cerrado (por ejemplo, a través de auditorías privadas), es mucho más difícil hacerlo de forma continua. Los proyectos de código abierto están abiertos al escrutinio público, lo cual da todas las oportunidades para que cualquier problema de seguridad (o de otra naturaleza) sea descubierto.

Proteger tu clave criptográfica da seguridad

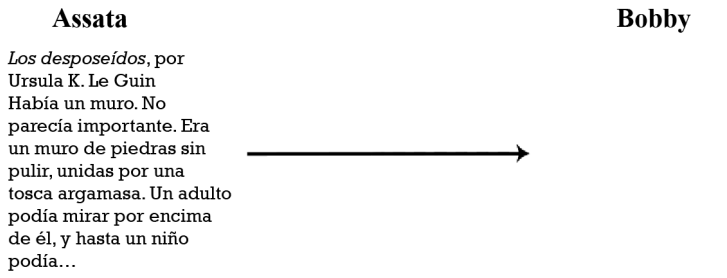
Puesto que el método de cifrado suele ser público en los protocolos criptográficos modernos, la seguridad se logra protegiendo la clave criptográfica. En la práctica, esto depende de dónde se localice la clave. En el caso de Signal, una app segura de mensajería instantánea, la clave

criptográfica es un archivo en tu teléfono; esta protege tu teléfono. En el caso de un administrador de contraseñas que sincroniza tus contraseñas en la nube, la clave que encripta el archivo que almacena todas tus contraseñas se deriva de o está protegida por la contraseña con la cual accedes a tu administrador de contraseñas.

Desconfiar de la infraestructura da seguridad

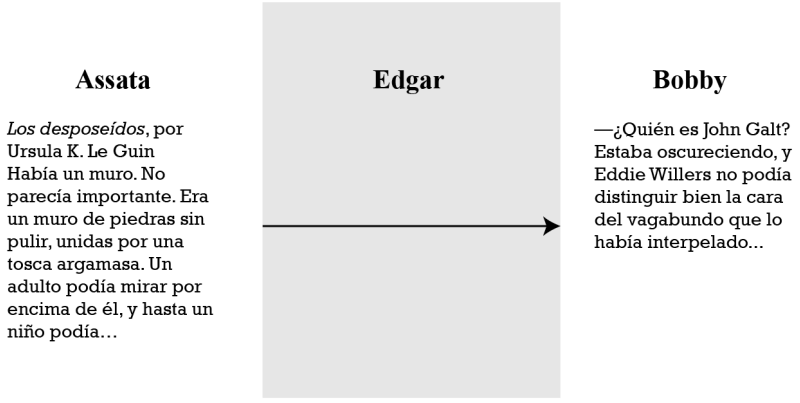
Aquí se ilustra por qué el cifrado de extremo a extremo es tan importante en la mensajería privada. Esto se cubre con mayor detalle técnico en el capítulo El intermediario.

En la siguiente figura, Assata (izquierda) intenta enviar un mensaje (*Los desposeídos*, por Ursula K. Le Guin) a Bobby (derecha) a través de internet:



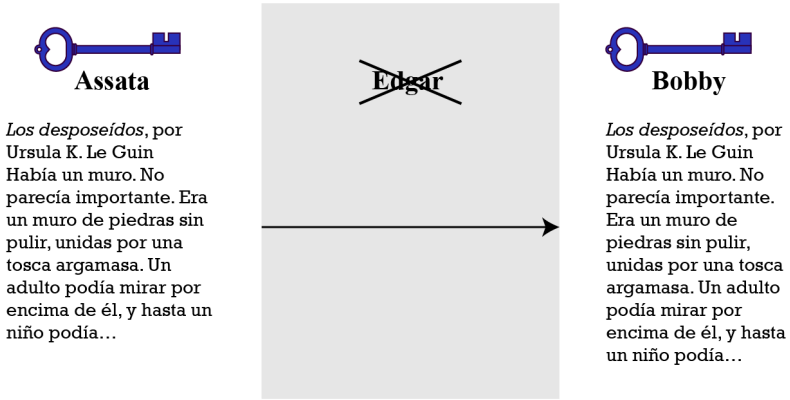
Assata intenta enviar un mensaje a Bobby

Pero el fantasma del malvado J. Edgar Hoover acecha la infraestructura. Este *intermediario* puede interceptar, leer y cambiar cualquier mensaje no protegido que se envíen nuestros dos amigos. Así:



Assata intenta enviar un mensaje a Bobby

(Edgar también podría solo leer el mensaje y enviarlo sin alterarlo.) Para empeorar la situación, decir que una aplicación usa “cifrado” (sin especificar quién guarda las claves) no garantiza que los mensajes permanezcan privados y auténticos. Por ejemplo, si un servidor entre los dos camaradas administra las claves criptográficas, cualquiera con acceso al servidor podría leer y modificar todos los mensajes entre ellos. Sin embargo, si Assata y Bobby cifran sus mensajes (con la llave azul), entonces Edgar no podrá leerlos y no podrá reemplazar el mensaje con uno que pudiera descifrarse con la misma llave azul:



El cifrado impide al intermediario cambiar el mensaje

¿Cómo saber si una aplicación usa cifrado de extremo a extremo? El mejor indicador es que exista alguna forma de verificar las claves criptográficas. Signal facilita esto con números de seguridad. Esto se describe con más detalle en el capítulo Autenticarse mediante firmado criptográfico.

Otra forma de reducir la exposición a un intruso malicioso es usar la mensajería entre pares (P2P), donde se dice que “no hay un servidor” que administre tus mensajes o contactos. Sin embargo, incluso esto puede ser engañoso: existe una enorme cantidad de infraestructura de internet entre tú y tus amigos, invisible para la mayoría de los usuarios y apps. Como se acaba de describir, esta infraestructura es precisamente lo que el Estado explota para efectuar vigilancia en masa indetectable, sin despertar sospechas.

En contexto: La máquina Enigma

Es posible que las primeras técnicas modernas de cifrado se hayan usado durante la Segunda Guerra Mundial. Antes de las computadoras modernas, los protocolos eran respaldados por sofisticados aparatos mecánicos. El más notable de estos es la máquina Enigma, usada en la Alemania nazi. Enigma es un aparato electromecánico que permitía establecer una clave específica, teclear el texto en claro y generar el texto cifrado. Con la misma clave, se podía teclear el texto cifrado y generar el texto en claro original.

La máquina Enigma, cortesía de Greg Goebel

La clave involucra un cierto orden y posición inicial de los rotores (se muestran en la imagen). La operación normal requería usar una clave nueva todos los días, y las claves se enumeraban por día en manuales distribuidos entre los operadores de las máquinas Enigma; eran esencialmente libretas de un solo uso con claves. Por cierto, se imprimían en tinta soluble al agua, lo cual permitía la rápida destrucción del manual cuando había riesgo de que cayera en manos enemigas.

Se realizaron grandes esfuerzos para descifrar mensajes cifrados en la máquina Enigma. Varias máquinas Enigma fueron incautadas durante la Segunda Guerra Mundial, pero aun teniendo la máquina, descifrar los mensajes era casi imposible (como ocurre con cifrados modernos cuyos métodos son públicos). Alan Turing, uno de los fundadores de la ciencia de la computación como disciplina, trabajó en el reservado Bletchley Park, la sede central de decodificadores británicos durante la Segunda Guerra Mundial. Turing diseñó el Bombe, un tipo de computadora específicamente diseñada para descifrar mensajes Enigma. El Bombe no fue suficiente. De hecho, descifrar mensajes Enigma sin la clave es increíblemente difícil incluso con las capacidades modernas de cómputo; al menos un famoso mensaje Enigma interceptado durante la guerra permanece sin descifrar en la actualidad. Sin embargo, el Bombe, en combinación

con el hecho de que la mayoría de los mensajes emitidos por la mañana contenían reportes del clima o la frase *Keine besonderen Ereignisse* ("nada que reportar"), permitió a los aliados descifrar mensajes Enigma en forma habitual.

Se ha estimado que el trabajo de Turing durante la guerra hizo posible acortarla más de dos años. Sin embargo, su trabajo permaneció sin reconocimiento durante su vida puesto que el trabajo hecho en Bletchley Park estaba reservado y, de hecho, se le criticó por no contribuir al esfuerzo de la guerra. Es aun más trágico que, como hombre homosexual, Turing fue perseguido por su propio gobierno hasta el punto de atribuirle un crimen en 1952. Acusado de cometer actos homosexuales, se le dio la opción de elegir la castración química o la prisión. Eligió lo primero, vivió otros dos años y supuestamente se suicidó por envenenamiento con cianuro.

Qué aprender a continuación

- Intercambiar claves para cifrar

Recursos externos

- Caraco, Jean-Claude, Rémi Géraud-Stewart y David Naccache. "Kerckhoffs' Legacy." 2020.

Créditos

Intercambiar claves para cifrar

Se recomienda leer el capítulo Criptografía moderna antes de seguir con este.

Lo que aprenderás

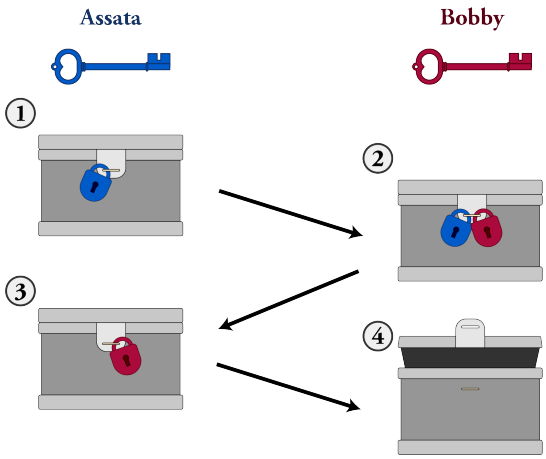
1. Cómo cifrar mensajes sin compartir previamente una clave criptográfica
2. El principal método para intercambiar claves en línea usado en la actualidad

Es posible espiar comunicaciones a través de internet en muchos puntos: el *hotspot* wi-fi al cual estás conectado directamente, tu proveedor de internet, el servidor que aloja las páginas web que visitas, portales nacionales y la vasta selección de enrutadores e interruptores ubicados en medio.

Sin un cifrado, todas estas comunicaciones pueden ser interceptadas por un espía, ya sea un acosador, un pirata informático o una agencia gubernamental. Pero con el fin de cifrar tus comunicaciones, necesitas acordar una clave con tu interlocutor. Si estás visitando un sitio web, ¿cómo intercambias de manera segura una clave con el servidor que aloja el sitio? Para acordar una clave sin reunirse y a través de canales de comunicación inseguros como internet, es necesario un método bipartito (por ejemplo, dos personas, una persona y un servidor, o dos servidores).

Un ejemplo físico: intercambiar un mensaje sin intercambiar una llave

Primero, consideremos el ejemplo físico que se ilustra abajo. Supongamos que Assata quiere enviarle un paquete a Bobby. Lo pone en una caja fuerte con una hebilla en la que caben diferentes candados (1) y pone un candado en la caja, del cual Bobby no tiene la llave. Assata le envía la caja a Bobby, quien no puede abrirla (y tampoco puede abrirla otra persona mientras está en tránsito). Luego, Bobby le pone su propio candado a la caja (2), un candado del cual Assata no tiene la llave, y se la reenvía. Cuando Assata recibe la caja, le quita su propio candado y envía la caja de vuelta a Bobby (3). Ahora Bobby puede abrir la caja porque solo está asegurada con su candado (4). La caja no puede abrirse en tránsito, pues un espía tendría que romper el candado de Assata, el de Bobby, o ambos.



Intercambiar un mensaje seguro sin compartir la llave

Esto ilustra que es posible enviar algo de forma segura sin reunirse antes para intercambiar (acordar) una clave. Sin embargo, no vamos a comenzar a enviar cajas fuertes por correo con el fin de intercambiar claves criptográficas. Lo que se necesita es una versión matemática de esto que se pueda usar con comunicaciones digitales.

Un ejemplo matemático: intercambiar un mensaje sin intercambiar una clave

Veamos cómo hacer esto sin cajas fuertes y candados. Supongamos que hay un protocolo de cifrado con el cual se puede cifrar cualquier texto (como se espera siempre), que el protocolo se puede aplicar en múltiples ocasiones para tener *capas* de cifrado (como también siempre se espera) y que dichas capas se pueden cifrar y descifrar en cualquier orden y terminar con el mismo resultado. Una operación matemática que satisfaga esta última propiedad se conoce como *conmutativa*. (Todos los protocolos descritos en el capítulo ¿Qué es el cifrado? son conmutativos.) Veamos esto con un ejemplo, usando el cifrado Vigenère.

Assata cifra el siguiente mensaje

`EN ALGUN MOMENTO HUBO EN ESTE MUNDO BOSQUES QUE NO ERAN DE NADIE`

con un cifrado Vigenère y la clave `ALDO`, para obtener el siguiente texto cifrado:

`EY DZGFQ AOXHBTZ KIBZ HB EDWS MFQRO MRGQFHG QFH BO PUON OH BAOLS`

Luego, le envía el resultado a Bobby, aunque ¡él no tiene la clave! Bobby, a su vez, cifra este texto ya cifrado con un cifrado Vigenère y el código `LEOPOLDO`, para obtener el siguiente texto doblemente cifrado:

```
PC ROUQT OZBVQHK NWMD VQ SOZG XJEGC XUUBJVV EQK PZ TIDB ZK PLSZH
```

Posteriormente, Bobby le envía el resultado a Assata, quien "descifra" el mensaje con su clave (`ALDO`) y obtiene el siguiente mensaje (aun cifrado):

```
PR OAUFQ AZQSCHZ KIMS SC SDWS XYBSC MRGBYSH EFH BZ IFPB OH BLHWT
```

Assata le envía de nuevo el resultado a Bobby, quien finalmente lo descifra con su propia clave (`LEOPOLDO`) y obtiene el mensaje que Assata quería enviarle en primer lugar:

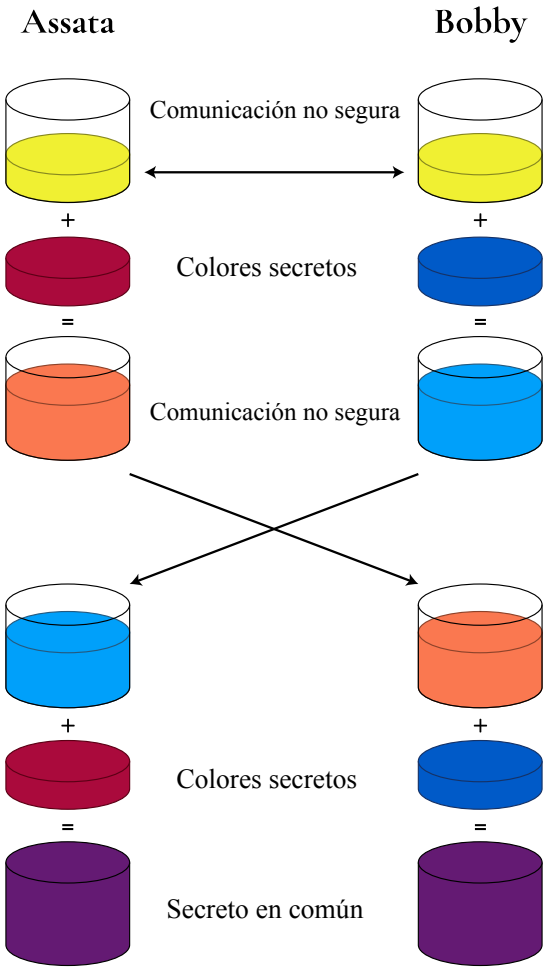
```
EN ALGUN MOMENTO HUBO EN ESTE MUNDO BOSQUES QUE NO ERAN DE NADIE
```

Se debe observar que en este ejemplo Assata no compartió su clave (`ALDO`) con nadie, y Bobby tampoco compartió la suya (`LEOPOLDO`) con nadie. Puesto que el cifrado Vigenère es conmutativo, no importa que el mensaje estuviera cifrado con la clave de Assata, luego con la de Bobby, luego descifrado con la de Assata y finalmente descifrado con la de Bobby. Lo único que importa es que el mensaje fue cifrado y descifrado una vez con cada una de las claves. Cualquier espía vería solamente uno de los tres textos cifrados intermedios.

Un ejemplo físico: acordar un secreto por un canal no seguro

En los sistemas criptográficos modernos, en lugar de enviar el mensaje completo una y otra vez, con diferentes capas de cifrado, se hace un intercambio inicial, parecido a los ejemplos anteriores, para acordar una clave. Podríamos imaginar que Assata, en lugar de enviar el mensaje `EN ALGUN MOMENTO HUBO…`, envía una clave criptográfica para usar en una comunicación más amplia. Describiremos el fundamento matemático para el intercambio de claves como se usa en casi todas las comunicaciones modernas, conocido como *protocolo criptográfico Diffie-Hellman*.

Primero, veamos cómo se hace con pinturas y no con matemáticas (se ilustra a continuación). Se asumirá que, si se mezclan dos colores de pintura, no es posible volver a separarlos; específicamente, aunque se supiera cuál fue uno de los colores iniciales, no se podría determinar con cuál color se mezcló para obtener el color resultante.



Elaboración de un secreto en común, con pinturas

Assata y Bobby comienzan acordando un color de pintura (en este ejemplo, el amarillo) y una cantidad, digamos, 10 mL (1). Esto pueden hacerlo a través de un canal de comunicación no seguro, pero deben asumir que entonces un espía también conocerá el color y la cantidad. Después, Assata elige un color (en este caso, el bermellón) y lo mantiene en secreto (2). Luego, mezcla 10 mL de amarillo con 10 mL de bermellón y obtiene un color anaranjado (3), y lo envía a Bobby a través del canal no seguro, en el entendido de que un espía también lo verá. Bobby hace lo mismo, con su propio color secreto (4).

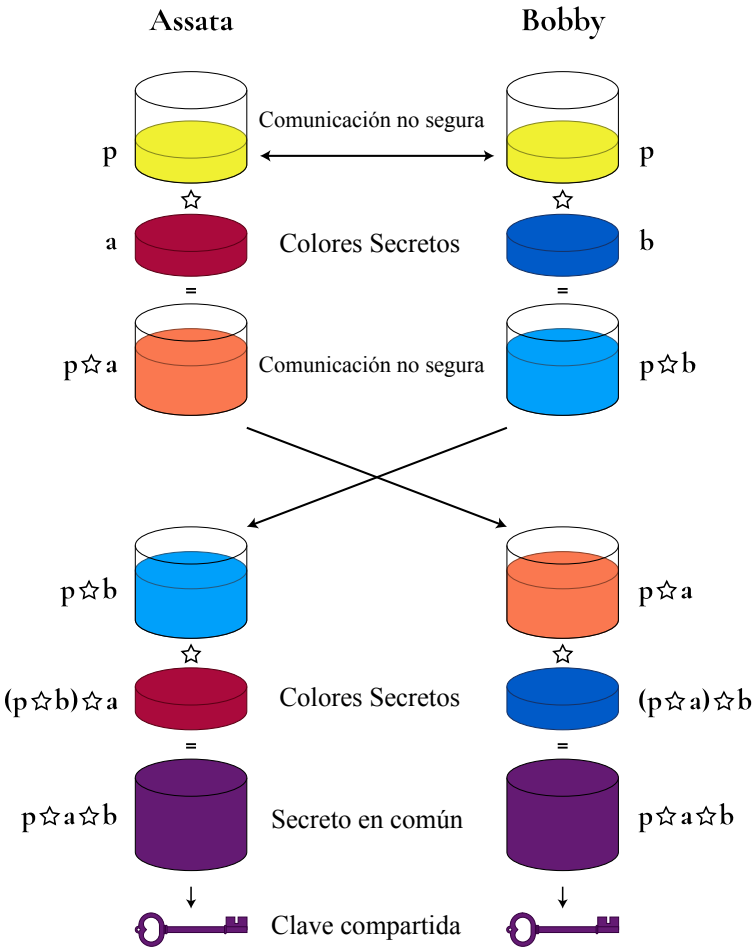
Ahora, a la muestra de pintura enviada por Bobby (5), Assata le añade 10 mL de su color secreto (6), lo cual resulta en un violeta intenso (7). Bobby hace lo mismo. El desagradable color violeta intenso de Assata se obtiene mezclando 10 mL de cada uno de estos colores: amarillo, su color secreto y el color secreto de Bobby. El color resultante de Bobby se obtiene mezclando 10 mL de amarillo, 10 m de su color secreto y 10 m del color secreto de Assata. ¡Así que Bobby obtiene el mismo desagradable color violeta intenso (8)! ¿Puede el espía crear el color violeta intenso? El espía ve el amarillo (1), la mezcla de amarillo con el color secreto de Assata (3) y la mezcla de amarillo con el color secreto de Bobby (5). Pero para crear ese horrible violeta intenso, el espía

tendría que separar las mezclas de colores para obtener los colores secretos de Assata o Bobby, lo cual no puede hacer.

El protocolo criptográfico Diffie-Hellman

Repasemos este mismo proceso matemáticamente. Esto se hace con una operación matemática conmutativa que sea difícil o imposible revertir. Una operación matemática o función difícil o imposible de revertir se conoce como *función unidireccional*. Representemos nuestra operación matemática con el símbolo ☆; es decir, a ☆ b = c para algunos números *a*, *b* y *c*. *Conmutativo* significa que a ☆ b = b ☆ a. Por otra parte, que ☆ sea *unidireccional* significa que si se conoce *b* y *c*, no se puede deducir fácilmente qué es *a*. En la práctica, solo se debería poder descifrar qué es *a* mediante un ataque de fuerza bruta o casi de fuerza bruta (probar todas y cada una de las posibilidades para *a*). Pensemos en ☆ como el signo de multiplicación (el cual es conmutativo, pero no unidireccional). Para aquellos con inclinación hacia la matemática, ☆ puede ser una exponenciación modular para implementaciones reales de Diffie-Hellman.

A continuación se ilustra la forma en que Assata y Bobby se ponen de acuerdo sobre un número *p*, el cual es público (1). Assata elige un número secreto *a* (2), hace el cálculo *p* ☆ *a* (3) y envía el resultado a Bobby. Puesto que ☆ es unidireccional, un espía conocería *p* y *p* ó*a*, pero no podría determinar *a* (con facilidad). Bobby elige un número secreto *b* (4), hace el cálculo *p* ☆ *b* y envía el resultado a Assata (5). Un espía conocería *p* ☆ *b*, pero no *b*. Luego, Assata hace el cálculo (*p* ☆ *b*) ☆ *a* (7) usando el mensaje de Bobby (5) y su propio número secreto (6). Entonces, Bobby hace el cálculo (*p* ☆ *a*) ☆ *b* (8) usando el mensaje de Assata (3) y su propio número secreto (4). Puesto que ☆ es conmutativo, (*p* ☆ *b*) ☆ *a* = (*p* ☆ *a*) ☆ *b*, así que Assata y Bobby ahora han calculado un número común. Puesto que el espía solo conoce *p* ☆ *a*, *p* ☆ *b* y *p*, y puesto que ☆ es unidireccional, no cuenta con medios eficientes para calcular el número común que calcularon Assata y Bobby: es un secreto entre Assata y Bobby. Por tanto, Assata y Bobby pueden usar este número compartido como su clave criptográfica.



Cómo acordar una clave secreta

Usar el protocolo Diffie-Hellman

El protocolo Diffie-Hellman es un método de uso generalizado para acordar una clave criptográfica. Es el fundamento de la mayoría de las formas de comunicación cifrada que encontrarás. Lo que es más notable: es la base del intercambio de claves cuando te conectas con un sitio https. Cuando visitas un sitio, la dirección URL se inicia con http:// o con https://. En el primer caso, ninguna de tus comunicaciones con el servidor del sitio está cifrada; en el segundo sí lo están y la clave que se usa para ello se genera usando el protocolo Diffie-Hellman.

En contexto: Cuando algo bueno sale mal

Recuerda que lo primero que hicieron Assata y Bobby fue ponerse de acuerdo en un número *p* que formó la base de su intercambio de claves.

Este número es público, pero asumimos que nuestra operación matemática ☆ era unidireccional, así que estaba bien que *p* fuera del conocimiento público. Sin embargo, alguien con muchos recursos de cómputo (como un Estado-nación adinerado) puede invertir la operación ☆ (para funciones como la exponenciación modular usada como ☆ en el mundo real) en dos fases. La primera fase toma mucho tiempo y debe efectuarse para un valor específico de *p*. La segunda fase puede hacerse con mucha rapidez (en tiempo real) para el mismo valor de *p*, suponiendo que la primera fase se ha completado. Esto significa que todos deberían *evitar usar* el mismo valor de *p*; deberían usar diferentes valores de *p*, y cambiarlos con frecuencia.

Sin embargo, en 2015, investigadores demostraron que 18 por ciento del millón de dominios https principales usa el mismo valor de *p*. Otros dos protocolos de comunicación que dependen del protocolo de intercambio Diffie-Hellman son SSH (*Secure Shell*) y VPN (*Virtual Private Network*). Los mismos investigadores demostraron que 26 por ciento de los servidores SSH y 66 por ciento de los VPN usan el mismo valor de *p* en su intercambio Diffie-Hellman. Esto significa que un adversario con recursos tendría muy poca dificultad para deshacer el cifrado.

Aunque el protocolo Diffie-Hellman es fuerte y confiable, esto pone de relieve que quienes implementan los protocolos necesitan hacerlo con cuidado para asegurarse de que, de hecho, son seguros.

Qué aprender a continuación

- El intermediario
- Criptografía asimétrica

External Resources

- Adrian, David, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, et al. "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice." En *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 5-17. Denver: ACM, 2015.

Créditos

- lockbox © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license
- diffie-hellman-concept-a © Lorddota adaptado por OSU Ecampus is licensed under a CC BY-SA (Atribución CompartirIgual) license
- diffie-hellman-concept © Lorddota adaptado por OSU OERU is licensed under a CC BY-SA (Atribución CompartirIgual) license
- diffie-hellman © Lorddota adaptado por OSU OERU is licensed under a CC BY-SA (Atribución CompartirIgual) license

Hash criptográfico

Se recomienda leer el capítulo Criptografía moderna antes de seguir con este.

What You'll Learn

1. Qué hace una función hash
2. Qué hace una función hash criptográfica y cómo se distingue de una función hash normal
3. Algunos ejemplos del uso de funciones hash criptográficas

Una *función hash* es cualquier función (computacional) que transforma datos de un tamaño arbitrario (por ejemplo, un nombre, un documento o un programa de cómputo) en datos de un tamaño fijo (por ejemplo, un número de tres dígitos o un número de 16 bits). El resultado de una función hash se conoce como resumen, huella digital, valor hash o, simplemente, hash (del *mensaje* de entrada).

Una función *hash criptográfica* tiene las siguientes propiedades que la hacen útil en aplicaciones criptográficas:

1. El mismo mensaje *de entrada* siempre producirá el mismo hash de salida.
2. No es posible generar el mensaje de entrada a partir del valor hash de salida, excepto por medio de un ataque de fuerza bruta (es decir, probando todos y cada uno de los mensajes de entrada posibles).
3. No es posible encontrar dos mensajes de entrada diferentes que produzcan el mismo valor hash de salida.
4. Un pequeño cambio en el mensaje de entrada cambia tanto el valor hash de salida que el nuevo valor hash parece no tener ninguna relación con el anterior.

De estas propiedades, las dos primeras son similares en la mayoría de los protocolos de cifrado. Si se cifra el mismo mensaje en dos ocasiones diferentes puede esperarse el mismo resultado, suponiendo que se use la misma clave criptográfica. Tan solo con el texto cifrado, no es posible generar el texto en claro (sin la clave criptográfica). Sin embargo, con la clave criptográfica, el cifrado permite retroceder desde el texto cifrado hasta el texto en claro. Las funciones hash son, de manera inherente, unidireccionales; es decir, no hay una clave para retroceder. Que el resultado se conozca también como resumen o huella digital es una analogía útil: aunque la

salida de una función hash criptográfica no cifra toda la información del mensaje original (en la misma forma que lo hace un texto cifrado), sí cifra suficiente información para identificar el mensaje de entrada. Lo anterior, con base en las propiedades 1 y 3, y en que es muy difícil de falsificar (propiedad 2).

Veremos aplicaciones de las funciones hash criptográficas en los capítulos El intermediario, Contraseñas y Criptografía asimétrica. Pero veamos aquí una aplicación sencilla, conocida como el *esquema de compromiso*.

Usar funciones hash criptográficas para probar cuán listo eres

Assata y Bobby intentan resolver un difícil problema matemático. Assata obtiene la respuesta (S) primero y quiere probarle a Bobby que la ha obtenido antes que él sin decirle la solución. Así que Assata toma un hash criptográfico de la solución S, hash(S), y se lo da a Bobby. Puesto que el hash es criptográfico, Bobby no puede deducir S a partir del hash(S) (propiedad 2). Cuando Bobby resuelve eventualmente el problema, encuentra S por sí mismo, puede calcular el hash(S) y verificar que el resultado es el mismo que Assata le compartió. Por las propiedades 1 y 3, Bobby sabe que el mensaje de entrada de Assata en la función hash debe ser el mismo que el suyo, lo cual prueba que Assata resolvió primero el problema. (La propiedad 4 no se usa aquí, pero, sin ella, si Assata hubiera obtenido una solución cercana a la correcta pero no correcta, los dos resultados podrían haber sido tan similares que una comparación somera podría no haber mostrado que eran diferentes.)

¿Cómo se ven las funciones hash?

Hay muchas funciones hash criptográficas en uso en la actualidad, pero describirlas en detalle rebasa el alcance de este libro. Sin embargo, para dar una idea de cómo se ven, se presenta aquí un ejemplo que satisface algunas, aunque no todas, las propiedades de las funciones hash criptográficas.

La función hash de ejemplo se llama `XOR en trozos`. La disyunción exclusiva, `XOR`, es una función en la cual, dado un par de valores de entrada, el resultado es verdadero (o 1) si los valores de entrada son diferentes; de otra manera, es falso. Por ejemplo, `manzana XOR plátano = 1`, `manzana XOR manzana = 0`, `0 XOR 1 = 1`, `1 XOR 1 = 0`. Podemos tomar una cadena de `XOR` en números binarios (0s y 1s) y obtener una respuesta significativa: `1 XOR 1 XOR 0 = 0`, `1 XOR 1 XOR 0 XOR 1 = 1`. Para una secuencia de números binarios, `XOR` resulta en `1` si hay una cantidad impar de 1s en la cadena y en 0 en el caso contrario.

`XOR en trozos` opera con base en un código binario. (Si el valor de entrada no es binario, se puede representar primero en binario, como lo haría una computadora.) Se agrupa el valor de entrada en trozos de igual tamaño que el resultado de la función hash; por ejemplo, en grupos de ocho bits. Se alinean los trozos verticalmente y luego se aplica `XOR` al contenido de cada columna, como se muestra a continuación:

```
        entrada: 00111011 11101101 00101000 00101011 01011000 11001110

      en trozos: 00111011
                 11101101
                 00101000
                 00101011
                 01011000
                 11001110

columnas en XOR: 01000011 (resultado)
```

Esta es una función hash puesto que no importa la longitud del valor de entrada; el valor de salida siempre tendrá la misma longitud (ocho bits en este ejemplo). Se puede ver que `XOR en trozos` satisface la primera propiedad de las funciones hash criptográficas. Sin embargo, falla en el resto de las propiedades. Es fácil crear un mensaje de entrada (aunque no necesariamente sea el mensaje inicial deseado), dado un valor hash resultante. Por ejemplo, se podría concatenar 11111111 11111111 en el resultado del hash. Por la misma razón, se podrían generar múltiples mensajes con el mismo hash resultante. Finalmente, cambiar un solo bit del mensaje de entrada cambiaría un solo bit en el hash resultante.

En contexto: Los hash criptográficos violan tus derechos de la Cuarta Enmienda

En 2008, un juez de distrito en Estados Unidos emitió el fallo de que si el gobierno de ese país quiere hacer hashes criptográficos con datos personales necesita obtener primero una orden judicial. En el caso en cuestión, un agente especial de la Oficina del Fiscal General de Pennsylvania copió el disco duro de la computadora de un sospechoso. El agente especial calculó un hash criptográfico de la copia (de manera que pudiera compararse posteriormente con el original y comprobar así que no se hubiera alterado, con base en las propiedades 1 y 3). Luego, el agente usó una herramienta forense que calculó un hash criptográfico de cada archivo (incluyendo archivos eliminados, pero no sobrescritos) del disco duro copiado y los comparó con hashes de archivos en una base de datos de archivos ilegales. El agente encontró tres coincidencias entre hashes de archivos en el disco duro y hashes de su base de datos. Gracias a las propiedades 1 y 3, esto significa que el disco duro contenía al menos tres archivos ilegales. El juez del caso dictaminó que esta práctica (de hacer hashes con los archivos y compararlas con hashes conocidos) constituye un *allanamiento* del disco duro, lo cual viola los derechos de la

Cuarta Enmienda del acusado a estar protegido contra allanamientos e incautaciones arbitrarios. El resultado fue que la evidencia no pudo usarse en un juicio.

Es necesario revelar los particulares del caso, el cual involucra la posesión de pornografía infantil. Aunque nunca defenderemos el derecho a poseer (o crear o distribuir) pornografía infantil, es importante imaginar un poder (en este caso, el poder de determinar la existencia de archivos específicos en una computadora) que podría usarse en una forma en la que *no* querrías que se usara: ¿música que un amigo compartió contigo?, ¿imágenes de derrames de petróleo?, ¿imágenes de protestas de #blacklivesmatter?, ¿artículos del *Earth First Journal*?

What to Learn Next

- Contraseñas
- El intermediario
- Autenticarse mediante firmado criptográfico

External Resources

- United States of America v. Robert Ellsworth CRIST, III, Defendant. Criminal Action No. 1:07-cr-211. 627 F.Supp.2d 575 (2008).

El intermediario

Se recomienda leer los capítulos Intercambiar claves para cifrar y Hash criptográfico antes de seguir con este.

Lo que aprenderás

1. Qué es un ataque de suplantación
2. Qué es un ataque de intermediario
3. La diferencia entre un ataque pasivo de intermediario y un ataque activo de intermediario
4. Cómo descubrir los ataques de intermediario que ocurren durante el intercambio de claves, usando huellas digitales

En el capítulo Intercambiar claves para cifrar aprendiste cómo dos personas pueden acordar una clave criptográfica, incluso sin conocerse. Aunque este es un método robusto, tiene la limitación de que en internet es difícil estar seguro de que en verdad te estás comunicando con la persona o entidad con quien quieres comunicarte, ya sea un amigo a quien quieres enviarle mensajes instantáneos o correos electrónicos o el servidor desde el cual deseas cargar una página web. Primero mostraremos, usando el ejemplo de la caja fuerte del capítulo Intercambiar claves para cifrar, cómo un espía puede interceptar tu comunicación, y luego mostraremos cómo ocurre esto en un protocolo de intercambio Diffie-Hellman. Estas interceptaciones de comunicación se conocen como *ataques*.

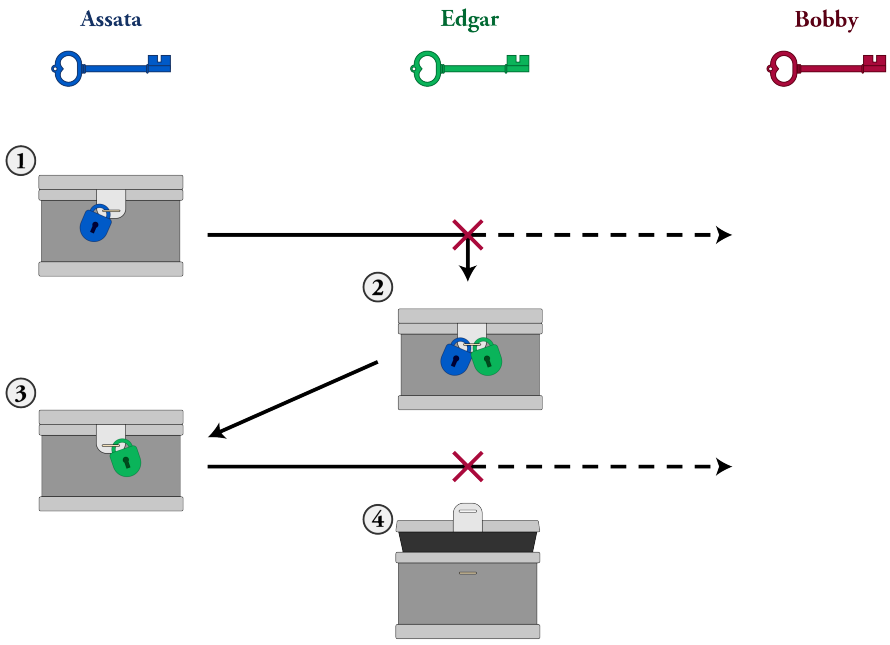
Un ataque físico de intermediario

Recuerda que Assata pudo enviarle a Bobby un paquete seguro en una caja fuerte de ida y vuelta tres veces: una vez con su propio candado, otra vez con su candado y el candado de Bobby y, finalmente, solo con el candado de Bobby. Pero ¿cómo supo ella que en realidad fue Bobby quien recibió el paquete? Y ¿cómo supo que era el candado de Bobby cuando ella recibió la caja fuerte de vuelta?

A continuación se ilustra el supuesto de que Edgar intercepta la caja fuerte que Assata le envía a Bobby con su candado (1). Edgar podría reenviarle la caja a Assata con su propio candado (2). A

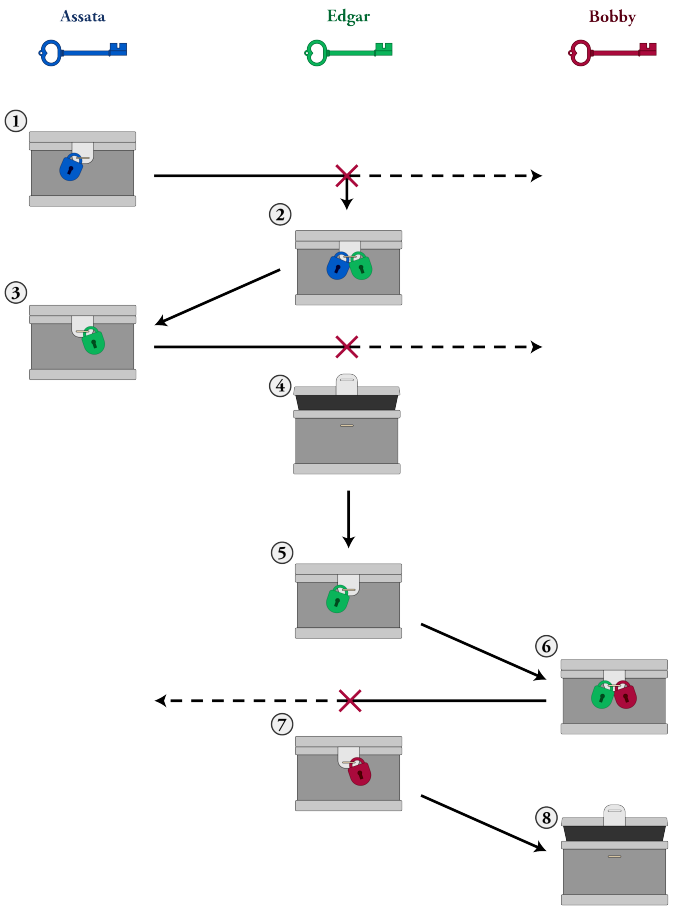
menos de que Assata pudiera identificar la diferencia entre un candado de Edgar y uno de Bobby, ella supondría que el candado es de Bobby, quitaría su candado y le reenviaría el paquete a Bobby (3). Si Edgar intercepta el paquete de nuevo, ahora podrá abrir la caja y examinar el contenido del paquete, puesto que ahora solo tiene su propio candado (4).

Para hacer esto, Edgar debe interceptar todos los envíos de Assata a Bobby. Este ataque a las comunicaciones de Assata hacia Bobby es un *ataque de suplantación*: Edgar está suplantando a Bobby. (Este no suele considerarse un ataque de intermediario.)



Ataque de suplantación

En la situación descrita, Bobby nunca recibe el paquete. Edgar podría ir incluso más allá (se ilustra a continuación). Edgar podría, después de abrir la caja fuerte de Assata (4), enviarle la caja a Bobby usando una imagen especular del mismo método de tres intercambios, de manera que Bobby piense que está recibiendo una caja con el candado de Assata (5-8).



Ataque de intermediario

Edgar pasa el mensaje original de Assata (aunque lo revisa él mismo); llamamos a esto un *ataque pasivo de intermediario*. Si Edgar sustituyera el paquete con otro completamente diferente, lo llamaríamos *ataque activo de intermediario*. En cualquier caso, Edgar tendría que interceptar todos los paquetes entre Bobby y Assata, puesto que los paquetes estarían dirigidos a Bobby o Assata, no a él.

Este tipo de ataques se conocen como ataques de intermediario porque Edgar es el intermediario en la comunicación entre Assata y Bobby.

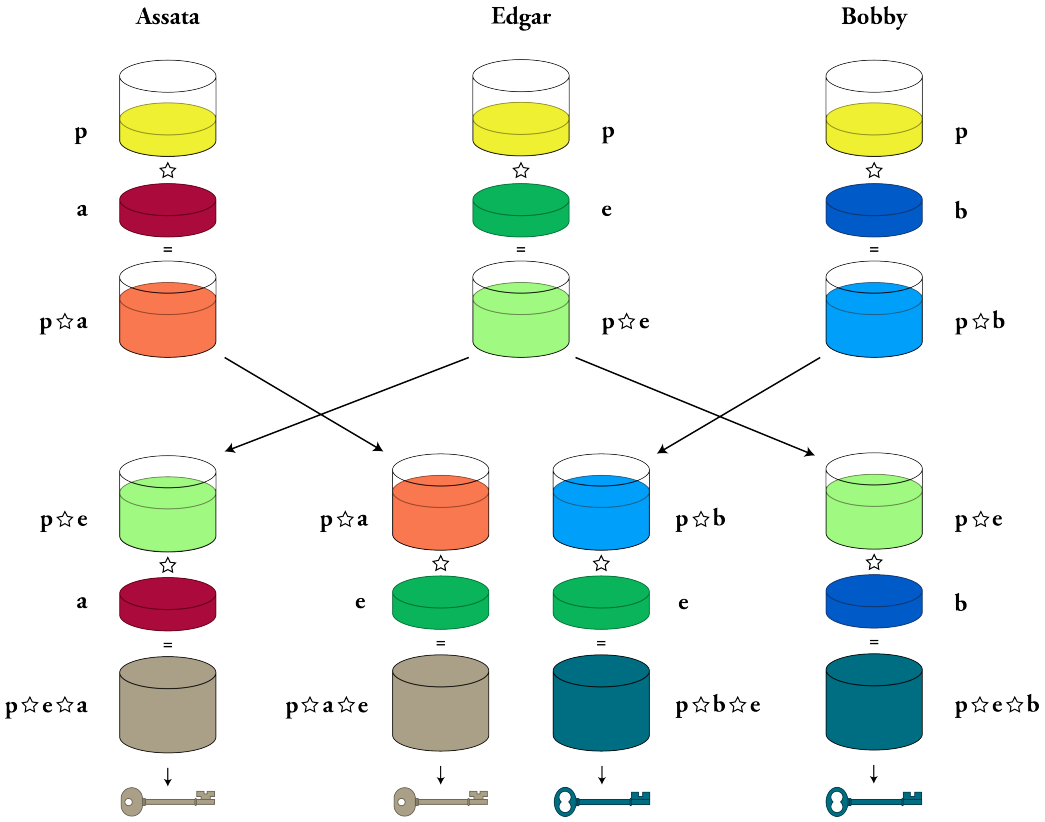
Un ataque de intermediario contra el protocolo Diffie-Hellman

Veamos cómo se desarrolla esto en el protocolo de intercambio Diffie-Hellman, usando la notación introducida en el capítulo Intercambiar claves para cifrar. Recuerda que, para generar

una clave, Assata y Bobby deben acordar primero un número *p*. Assata elige el número *a*, calcula *p* ☆ *a* y le envía

el resultado a Bobby. Bobby elige el número *b*, calcula *p* ☆ *b* y le envía el resultado a Assata. Assata y Bobby (y nadie más) pueden ahora calcular *p* ☆ *a* ☆ *b*, el cual usan como clave criptográfica para su comunicación cifrada.

Sin embargo, supongamos que Edgar puede interceptar las comunicaciones de Assata y Bobby. Luego, Edgar puede hacer un protocolo de intercambio Diffie-Hellman con Assata y otro con Bobby (se ilustra a continuación). Assata pensará que está haciendo un protocolo de intercambio Diffie-Hellman con Bobby, aunque en realidad estará intercambiando claves con Edgar, lo que dará como resultado la clave beige *p* ☆ *a* ☆ *e*. Bobby pensará que está haciendo un protocolo de intercambio Diffie-Hellman con Assata, aunque en realidad estará intercambiando claves con Edgar, lo que dará como resultado la clave verde azulada *p* ☆ *b* ☆ *e*. Al final, Assata y Edgar habrán compartido una clave (izquierda), y Edgar y Bobby habrán compartido otra (derecha). Pero Assata y Bobby pensarán que han compartido claves solo entre ellos.



Ataque de intermediario contra el protocolo Diffie-Hellman

Cuando Assata y Bobby comiencen a usar lo que piensan que es su clave compartida, Edgar tendrá que continuar con la trampa para no ser descubierto. Assata cifrará un mensaje con la clave que ella tiene. Si este mensaje llega a Bobby, él no podrá descifrar el mensaje ¡porque no tiene la misma clave! Lo que Edgar debe hacer es interceptar el mensaje cifrado y descifrarlo con la clave que compartió con Assata. Ahora, Edgar tiene dos opciones: simplemente, puede leer el

mensaje, cifrarlo con la clave que comparte con Bobby y enviárselo. Este sería un ataque pasivo de intermediario; es decir, Edgar lee los mensajes entre Assata y Bobby, los cuales piensan que nadie más puede leerlos.

La otra opción de Edgar es cambiar el mensaje de Assata, cifrarlo con la clave que comparte con Bobby y enviárselo. Este sería un ataque activo de intermediario. En cualquier caso, Edgar debe interceptar continuamente las comunicaciones entre Assata y Bobby porque, de otra forma, uno de ellos recibiría un mensaje cifrado con una clave que no tiene, lo cual les alertaría sobre el intermediario.

Detectar un ataque de intermediario con hashes criptográficos: huellas digitales

Si Assata y Bobby, después de desarrollar un protocolo de intercambio Diffie-Hellman, pueden comparar sus claves y verificar que son iguales, entonces podrán estar seguros de que un espía no ha montado un ataque de intermediario y que solo podría ver sus comunicaciones cifradas. Como recordatorio, esto obedece a que las partes del protocolo Diffie-Hellman que un espía puede ver no le permiten crear las partes ocultas de las claves que Assata y Bobby eligieron (*a* y *b* en la ilustración anterior). De hecho, la forma más sencilla de identificar un ataque de intermediario es que Assata y Bobby comparen sus claves.

Aunque puede haber ciertos problemas con este plan:

Si Assata y Bobby intentan comparar sus claves, ¿no podría Edgar manipular la comunicación de manera que parezca que se trata de la misma clave?

¡Por supuesto! Entonces, Assata y Bobby deberían comparar sus claves a través de un canal de comunicación distinto. Por ejemplo, si originalmente se comunicaban por internet, deberían comparar sus claves por teléfono. La suposición es que sería mucho más difícil para Edgar interceptar las comunicaciones de Assata y Bobby a través de todos los diferentes canales de comunicación que podrían usarse para comparar claves. Idealmente, Assata y Bobby podrían reunirse para comparar claves. De cualquier forma, esto se conoce como *comparación fuera de banda*, donde "banda" es el canal de comunicación, y las claves deberían compararse fuera de la banda de comunicación a través de la cual se intercambiaron.

Pero si Assata y Bobby tienen otro medio de comunicación, ¿entonces por qué no intercambian claves en la forma tradicional, sin matemáticas complicadas de las cuales preocuparse?

Porque las claves criptográficas, en los métodos modernos de criptografía, son muy largas: de cientos de miles de caracteres. Podría ser engorroso hacer un intercambio manual de claves. Si el diseñador de un método de comunicaciones seguras quisiera automatizar el intercambio de claves a través de un canal de comunicación distinto, ese diseñador tendría que especificar ese canal secundario, lo cual haría engorroso al sistema seguro de comunicaciones: imagina tener

que hacer una llamada telefónica para poder visitar un sitio web. Asimismo, Edgar también sabría por cuál canal se estarían intercambiando las claves y podría hacerla de intermediario en ese canal.

Entonces, ¿siendo tan largas, no es engorroso comparar claves?

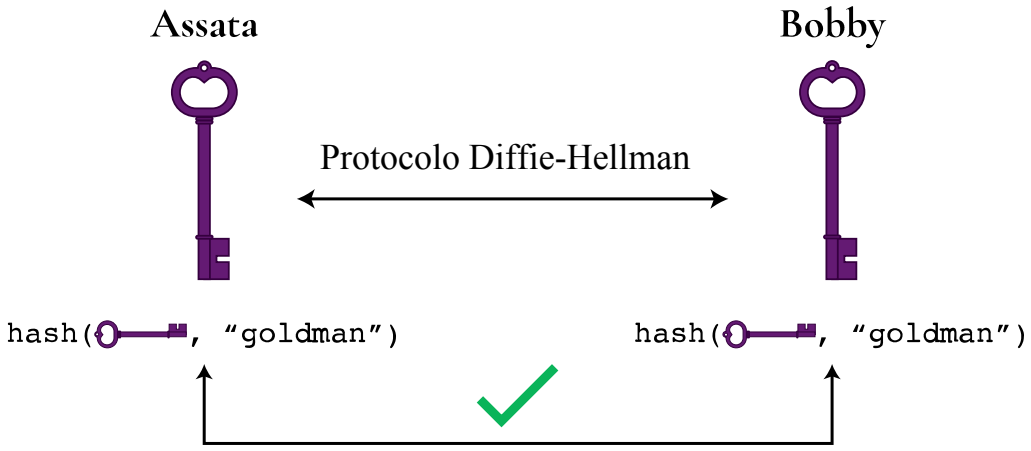
¡Por supuesto! Así que, en lugar de comparar toda la clave, Assata y Bobby comparan los hashes criptográficos de sus claves, como se describió en el capítulo Hash criptográfico. Recuerda las siguientes propiedades del hash criptográfico: (1) Hace al mensaje de entrada (en este caso, la clave) mucho más corto. (2) Es prácticamente imposible encontrar dos mensajes de entrada (en este caso, dos claves) que tengan el mismo hash de salida, por lo cual Edgar no podrá hacer un protocolo Diffie-Hellman con Assata y Bobby para que los hashes sean iguales. (3) No puede revertirse, por lo cual, si alguien interceptara el hash, no podría recrear el mensaje de entrada (en este caso, la clave).

Como recordarás, la función hash también se conoce como huella digital (*fingerprint* en inglés), así que al proceso de comparar los hashes criptográficos de claves se le conoce como *fingerprinting*. Distintas aplicaciones de comunicación usan terminología distinta para esto, incluyendo: *números de seguridad, verificación* y *autenticación*.

Fingerprinting en la misma banda

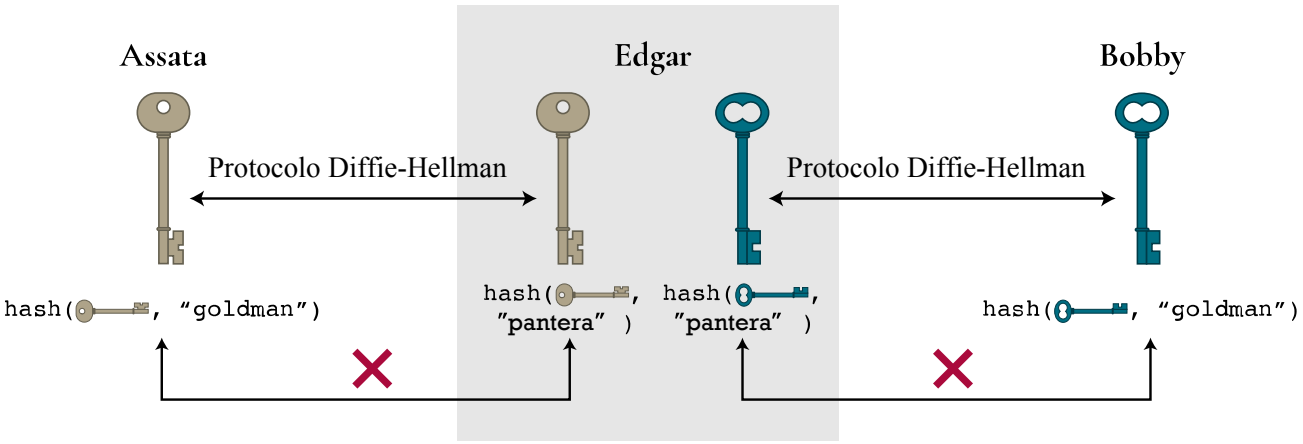
Hay dos métodos para comparar claves en la misma banda que no se usan con frecuencia pero que son ingeniosos y son variaciones del *fingerprinting* fuera de banda descrito anteriormente.

El primero depende del uso de una contraseña débil. Si tanto Assata como Bobby saben algo que su supuesto adversario no sabe, como el nombre de la primera mascota de Assata o la calle en la que creció Bobby (por ejemplo, Goldman), entonces Assata y Bobby pueden usarlo como una contraseña débil. Assata combina su clave con la contraseña débil (Goldman) y calcula el hash criptográfico del resultado. Bobby hace lo mismo con su clave. Luego, Assata y Bobby comparan el resultado *en la misma banda* (por ejemplo, por el canal de comunicación a través del cual se están comunicando). Gracias a las propiedades del hash criptográfico, Assata y Bobby solo obtendrán el mismo resultado si tienen la misma clave y la misma contraseña:



Fingerprinting

Si Edgar está en el papel de intermediario, entonces comparte una clave con Assata y una clave diferente con Bobby. Edgar tendría que arriesgar pasar el hash de Assata a Bobby o tendría que adivinar la contraseña débil para poder calcular un resultado igual al que Assata calculó y al que Bobby calculó (como en la figura siguiente). La contraseña no necesita ser fuerte porque solo unos cuantos intentos incorrectos (por ejemplo, "pantera") serían tolerados por Assata y por Bobby antes de sospechar que hay un intermediario; es decir, un ataque de fuerza bruta por parte de Edgar no es factible.



Fingerprinting para descubrir un ataque de intermediario

El segundo método se usa para comparar claves en llamadas de voz y video. Aquí, Assata hace de su clave un hash de dos palabras que solo un humano puede leer (en lugar de una cadena de números y caracteres, como hemos visto). Luego, Bobby hace lo mismo. Si Assata y Bobby tienen la misma clave, es decir, si no hay un intermediario, entonces tendrán el mismo par de palabras. Assata lee la primera palabra y Bobby lee la segunda palabra, de manera que comparan el resultado del hash. Si Edgar está en medio, Assata y Bobby tendrán un par de palabras diferente. Para sostener su engaño, Edgar tendría que sintetizar las voces de Assata y Bobby

(y posiblemente videos también) para decir las palabras que Edgar comparte con Assata y con Bobby.

La posibilidad de hacer *fingerprinting* es una protección, aun si no lo haces

Si un método de comunicación segura no permite comparar claves (*fingerprint*), entonces usar un cifrado de extremo a extremo ofrece poco beneficio. Los ataques de intermediario pueden ser automatizados en nuestro sistema de vigilancia global, de manera que si no es posible detectar un ataque de intermediario (a través del *fingerprinting*) da igual si se hace por defecto. Sin embargo, si es posible hacer *fingerprinting*, entonces el intermediario se arriesga a ser descubierto, en especial si los ataques son automatizados y efectuados en forma amplia. Para evitar el despliegue generalizado de intermediarios no es necesario que todos hagan el proceso de *fingerprinting* mientras algunos usuarios lo hagan.

Por supuesto, el *fingerprinting* es esencial para la seguridad de las comunicaciones de aquellos usuarios que tienen riesgo de estar bajo vigilancia.

¿Qué hacer si no se puede hacer *fingerprinting*?

En muchas formas de comunicación no es posible hacer *fingerprinting*. Un ejemplo es cuando se accede a un sitio por medio de un https. Cuando se usa un https, el buscador y el servidor del sitio web generan una clave criptográfica por medio de un protocolo Diffie-Hellman. Sin embargo, no es práctico que los usuarios contacten a los servidores de los sitios web por medio de canales alternos de comunicación para hacer *fingerprinting* de claves antes de acceder al contenido de los sitios. Por supuesto, no conoces la voz del operador del servidor del sitio web ni comparten el conocimiento de datos que puedan usar en métodos de comparación en banda. En este caso se usan métodos alternos para validar claves, con criptografía asimétrica y autoridades certificadoras. En el capítulo Criptografía asimétrica se describe justamente eso.

En contexto: El Gran *Firewall* de China

Muchos saben que en China hay gran censura de internet gracias al Gran *Firewall* de China. A partir de mediados de enero de 2013, partes de GitHub, un sitio usado esencialmente para alojar código de programación pero que también puede usarse para compartir información más general, fueron bloqueadas en China. Para el 21 de enero de 2013, todo el dominio había sido bloqueado. Sin embargo, dado el papel central de GitHub en el desarrollo computacional y de negocios, y dada la importancia de este sector para la economía China, gracias a la respuesta

pública se logró desbloquear GitHub para el 23 de enero de 2013. El 25 de enero, una petición publicada en WhiteHouse.gov había comenzado a solicitar que se negara la entrada a Estados Unidos a aquellos vinculados con la creación del Gran *Firewall* de China. La petición hacía referencia a una página de GitHub creada el mismo día en la que se nombraba a personas de origen chino acusadas de contribuir a la infraestructura de censura en China. El siguiente día aparecieron reportes en las redes sociales de un ataque de intermediario a los usuarios que accedían a GitHub, lo que mostró que el equivalente de la verificación con *fingerprinting* para acceder a un sitio vía https estaba fallando. El gobierno chino había entendido que no podía bloquear GitHub y, puesto que GitHub admite https, el Gran *Firewall* no podía bloquear el acceso a páginas específicas dentro de GitHub (por ejemplo, con base en coincidencias en palabras clave) porque https cifra esa información contra espías. La siguiente opción era un ataque de intermediario. Cualquier usuario que ignorara las advertencias de los ataques estaría en riesgo de que su gobierno supiera cuáles páginas visitaba o incluso editaba. El gobierno chino es el presunto implementador de ataques de intermediario generalizados entre usuarios en China y otros grandes prestadores de servicios de internet como Outlook, iCloud de Apple y Google.

China no está sola en el uso de ataques de intermediario. Ataques similares se han observado en Siria y también en Irán.

Qué aprender a continuación

- Proteger tus comunicaciones

Recursos externos

- GreatFire proporciona herramientas para acceder a un internet sin censura en China y reporta y verifica censura y vigilancia china en internet. En particular, GreatFire ha reportado y verificado ataques de intermediario, presuntamente por parte del gobierno chino, contra Outlook, iCloud de Apple, Google y GitHub.
- Eckersley, Peter. "A Syrian Man-in-the-Middle Attack against Facebook." Electronic Frontier Foundation, 5 de mayo de 2011.
- Electronic Frontier Foundation. "Iranian Man-in-the-Middle Attack against Google Demonstrates Dangerous Weakness of Certificate Authorities." 29 de agosto de 2011.

Créditos

- mitm-impersonation-a © OSU Ecampus is licensed under a CC BY-NC (Atribución NoComercial) license
- mitm-impersonation © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license
- mitm-a © OSU Ecampus is licensed under a CC BY-NC (Atribución NoComercial) license
- mitm © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license
- dhe-mitm © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license
- fingerprinting © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license
- fingerprinting-mitm © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license

Contraseñas

Se recomienda leer el capítulo Hash criptográfico antes de seguir con este.

Lo que aprenderás

1. Cuando “protegido con contraseña” significa que algo está cifrado y cuando no significa eso
2. Cómo se vence a las contraseñas
3. Cuáles prácticas puedes usar para minimizar riesgos con tus contraseñas
4. Cómo generar claves criptográficas a partir de contraseñas

Cuando “protegido con contraseña” no significa cifrado

Todas las contraseñas se usan para obtener acceso. Las *contraseñas de cuenta* se usan para otorgar acceso a cuentas en línea. Sin embargo, es raro que la información en dichas cuentas esté cifrada con una clave que el usuario controla, y es probable que la información no esté cifrada en absoluto. Es decir, la información suele ser legible para el proveedor (por ejemplo, Google y Dropbox). Otras contraseñas se usan para *desbloquear* un archivo o documento cifrado, y nos referiremos a ellas como *contraseñas de cifrado*. Usar una contraseña para tu cuenta es como decirle tu nombre a un guardia para que lo verifique en una lista de huéspedes aprobados, mientras que el uso de una contraseña de cifrado equivale más a usar una llave para cerrar una caja de seguridad. En el primer caso, depende del guardia (una metáfora para tu proveedor de internet) darte acceso. En el segundo, la caja de seguridad representa el texto cifrado, y el contenido de la caja es el texto en claro; obtener acceso al texto en claro es imposible (o al menos impráctico) sin la llave o la contraseña. De hecho, algunas veces las claves criptográficas se generan a partir de una contraseña, como se describe a continuación.

Ahora bien, aunque tu información no queda cifrada con una contraseña de cuenta, de todas formas, deberías minimizar la cantidad de personas que pueden tener acceso a tu información. Pero para entender por qué recomendamos ciertas prácticas, es necesario comprender cómo se puede comprometer una contraseña.

Descifrado de contraseñas

Las contraseñas pueden comprometerse o *descifrarse* una por una o en bloque, como, por ejemplo, todas las contraseñas de todas las cuentas en un sistema dado. Las contraseñas son mercancías de valor. Puesto que las personas suelen usar la misma contraseña para muchas cuentas y que muchos usan (muy malas) contraseñas populares (`123456`, `contraseña`, `qwerty`, `admin`, `bienvenido`, por dar solo algunos ejemplos reales), descubrir las contraseñas usadas en un servicio puede poner en riesgo las cuentas de un servicio diferente y posiblemente también de otra persona.

Consideremos las formas de comprometer una contraseña.

Para descifrar una contraseña, un adversario podría lograrlo por la misma vía en que tú tecleas tu contraseña; por ejemplo, mediante un sitio web. Es relativamente fácil para el operador de un sitio web brindar protección contra esto; por ejemplo, bloqueando una cuenta después de varios intentos fallidos de introducir una contraseña o forzando retrasos después de la introducción de una contraseña para desacelerar la repetición de intentos. Otra manera en que el proveedor de una cuenta puede ayudar es permitir la autenticación de dos factores; esto es, que, aparte de introducir una contraseña para entrar en una cuenta, también debes introducir un código de autenticación enviado en un mensaje de texto o a través de una app en tu teléfono inteligente, o usando una llave física de autenticación (como YubiKey). Para comprometer tu cuenta, un adversario necesitaría tu contraseña, así como el dispositivo en el cual recibes el código de autenticación.

Un adversario también podría acceder físicamente al dispositivo (teléfono o computadora) en el cual introduces tu contraseña. Lo que es más probable (y se reporta con frecuencia en las noticias) es que el servidor donde se aloja tu contraseña resulte comprometido o jaqueado. En este caso, no serán solo tu nombre de usuario y contraseña los que resultarán comprometidos; todos aquellos que tengan una cuenta en ese sistema estarán en riesgo. Aunque es probable que un adversario que haya obtenido acceso a la base de datos de contraseñas de ese servidor tenga acceso a la información de tu cuenta, como se sugirió anteriormente, el objetivo del jaqueo podría ser obtener acceso a otro servicio completamente distinto.

Un proveedor de servicios responsable no almacenaría tu contraseña como texto en claro en su servidor, sino en un hash criptográfico. Para descifrar una contraseña (o todas las contraseñas), un adversario calcula el hash criptográfico de una supuesta contraseña y lo compara con la base de datos de contraseñas robadas. En la práctica, las herramientas para descifrar contraseñas (por ejemplo, John the Ripper) usan tres técnicas:

1. Ataques de diccionario: probar palabras de diccionario, variaciones comunes de palabras de diccionario (por ejemplo, `c0n7ra53n4`, `l1b3r74d`) y contraseñas previamente descifradas.
2. Fuerza bruta: probar todas las combinaciones posibles de letras y números o símbolos (por razones prácticas, este método solo funciona con contraseñas relativamente cortas).
3. Hashes precalculados: comparar contra una tabla de hashes criptográficos de contraseñas posibles calculados con anterioridad.

Un usuario podría frustrar las primeras dos técnicas usando buenas prácticas para crear contraseñas (descritas a continuación). Un proveedor de servicios puede hacer que el descifrado de contraseñas sea menos práctico usando una función hash criptográfica que sea lenta de calcular o que use mucha memoria.

Esto no sería notorio con una sola contraseña (como cuando inicias sesión), pero haría muy lento el cálculo de los hashes durante su descifrado.

Un proveedor de servicios puede dificultar aún más el uso de hashes precalculados si agrega una secuencia larga de caracteres aleatorios (condimento) a tu contraseña cuando inicias sesión. Este "condimento" puede almacenarse como texto en claro con tu nombre de usuario, de manera que un adversario también tendría esta información, pero no habría tenido el "condimento" cuando preparó la tabla de hashes precalculados. Por otra parte, si dos usuarios tuvieran la misma contraseña, puesto que su "condimento" sería diferente, el hash criptográfico de sus contraseñas con condimento también sería diferente. Esto obligaría al atacante a descifrar cada contraseña de manera individual.

Debido a lo anterior, estás confiando en que tu proveedor de servicios en línea almacena y protege de manera responsable tu información de usuario, incluyendo el hash de tu contraseña, si es que la ha hasheado. El resto depende de ti.

Las mejores prácticas para crear contraseñas

Para protegerte contra los métodos descritos en la sección anterior, tu contraseña debería ser suficientemente larga (para evitar ataques de fuerza bruta), ser poco común (para evitar ataques de diccionario) y no ser reusada (para que, si una de tus cuentas resulta comprometida, tus otras cuentas no lo estén también)

Para lograrlo, usa un administrador de contraseñas que genere y almacene todas las contraseñas, sin que necesites teclearlas manualmente. El administrador generará contraseñas aleatorias fuertes, como `bdY,Fsc_7\&*Q+cFP`. Esta es una excelente contraseña, de las que no debes teclear; es decir, una que el administrador de contraseñas introducirá por ti.

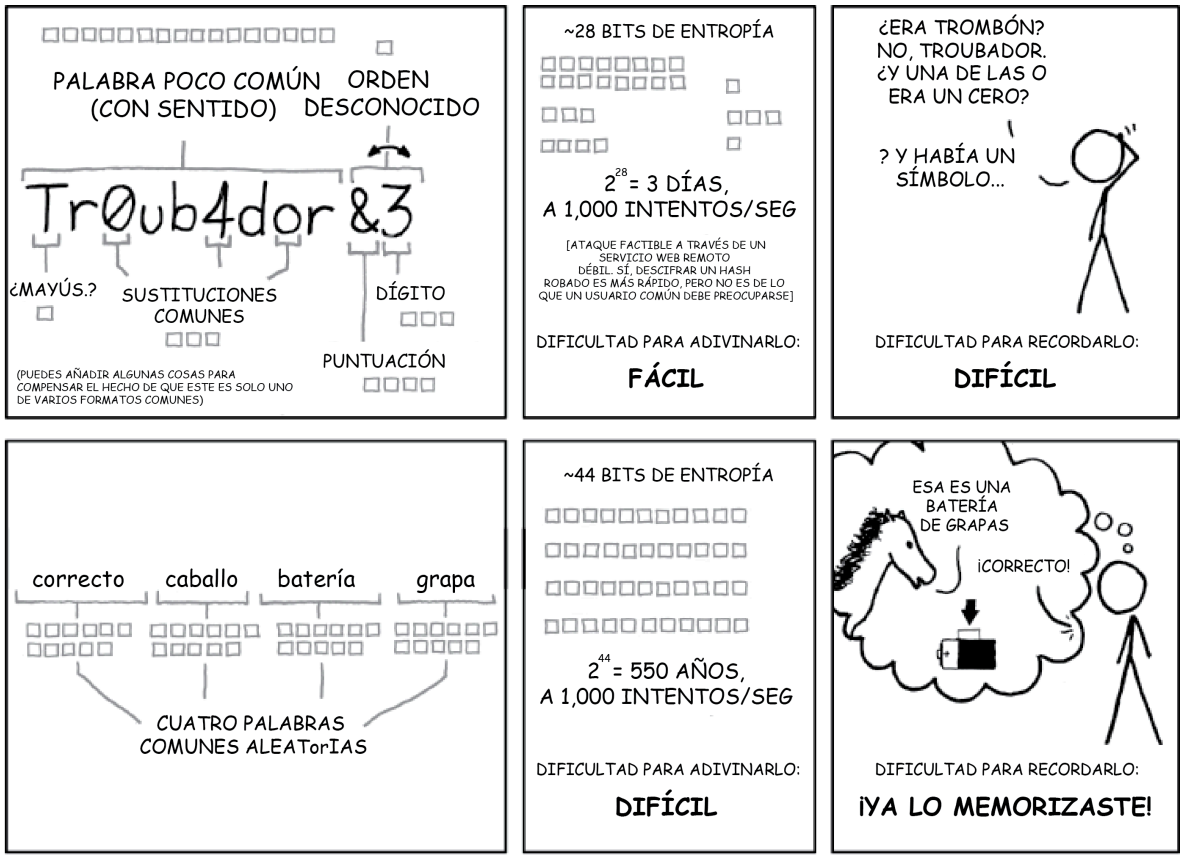
En el caso de contraseñas que es necesario teclear (por ejemplo, la contraseña que introduces en tu teléfono, la contraseña con la cual proteges el administrador de contraseñas o la que usas para

cifrar el acceso o bloquear tu computadora), usa una contraseña creada con Diceware; es decir, una secuencia aleatoria de palabras, como:

```
nadar.gracias.belez.zanahoria.torno.maleta
```

También puedes generar esta contraseña manualmente usando dados y una lista de palabras. Muchos administradores de contraseñas también generan dichas contraseñas, aunque es probable que no necesites muchas de ellas.

Observa que los dos ejemplos anteriores fueron generados aleatoriamente. Esto es importante porque, aunque pienses que tu contraseña es excelente y fuerte, si la creaste con tu propio cerebro es probable que también la haya creado el cerebro de alguien más, y por tanto es susceptible a ataques de diccionario.



Seguridad de la contraseña XKCD

Generar claves criptográficas a partir de contraseñas

En algunos casos, las contraseñas se usan para desbloquear un archivo o dispositivo bloqueado. En este caso, se genera una clave criptográfica a partir de una contraseña o frase de contraseña usando una función de derivación de clave (KDF, por sus siglas en inglés), que es, en esencia, una función hash criptográfica. ¿Cómo funciona esto? Repasemos las propiedades de las funciones hash criptográficas.

1. *Sin importar la longitud del mensaje de entrada, el mensaje de salida siempre será del mismo tamaño.* Así que, sin importar cuán corta (¡o débil!) sea tu contraseña, obtendrás una clave criptográfica del tamaño correcto. (Pero una contraseña corta y débil es susceptible a ser descifrada por los métodos antes mencionados.)
2. *El mismo mensaje de entrada siempre producirá el mismo hash de salida.* De esta forma, tu contraseña siempre generará la clave criptográfica correspondiente que necesitas.
3. *No es posible generar el mensaje de entrada a partir del valor hash de salida.* Si alguien lograra obtener tu clave criptográfica, no podría recrear tu contraseña.
4. *No es posible encontrar dos mensajes de entrada diferentes que produzcan el mismo hash de salida.* Es poco probable que alguien que intentara descifrar tu contraseña encontrara otra que produjera la misma clave criptográfica que la tuya.
5. *Un pequeño cambio en el mensaje de entrada cambia tanto el valor hash de salida que el nuevo valor hash parece no tener ninguna relación con el anterior.* Esta propiedad no es tan útil para la generación de una clave criptográfica.

En contexto: Cuando las precauciones no bastan

En 2016, la cuenta de Twitter y dos cuentas de correo electrónico de DeRay Mckesson, activista por muchos años, fueron comprometidas en un ataque dirigido, a pesar de que tenían un protocolo de autenticación de dos factores. Para obtener el control del teléfono de Mckesson, su adversario llamó a Verizon y solicitó una nueva tarjeta SIM, y sabía suficiente sobre Mckesson para convencer a Verizon. Una vez que el adversario tuvo acceso al número telefónico de Mckesson, pudo obtener códigos para reestablecer sus contraseñas y obtener así acceso a sus cuentas. Este es un recordatorio de que ninguna medida de seguridad es perfecta, y quienes son susceptibles de sufrir ataques dirigidos (en este caso, Mckesson era un blanco debido a su apoyo al movimiento Black Lives Matter) deben ejercer vigilancia adicional. En este caso, el acceso al teléfono de Mckesson permitió reestablecer contraseñas y degradó la protección de sus cuentas de dos factores a un factor: solo el acceso a su teléfono dio al adversario de Mckesson acceso a sus cuentas, en lugar de la contraseña más el acceso al teléfono.

Qué aprender a continuación

- Proteger tus dispositivos

Recursos externos

- Dreyfuss, Emily. "@Deray's Twitter Hack Reminds Us Even Two-Factor Isn't Enough." *Wired*, 10 de junio de 2016.
- Wikipedia. "John the Ripper." 29 de diciembre de 2020.
- TeamPassword. "Top 50 Worst Passwords of 2019." 18 de diciembre de 2019.

Créditos

Criptografía asimétrica

Se recomienda leer el capítulo Intercambiar claves para cifrar antes de seguir con este.

Lo que aprenderás

1. La diferencia entre la criptografía simétrica y la asimétrica
2. Cómo funciona la criptografía asimétrica

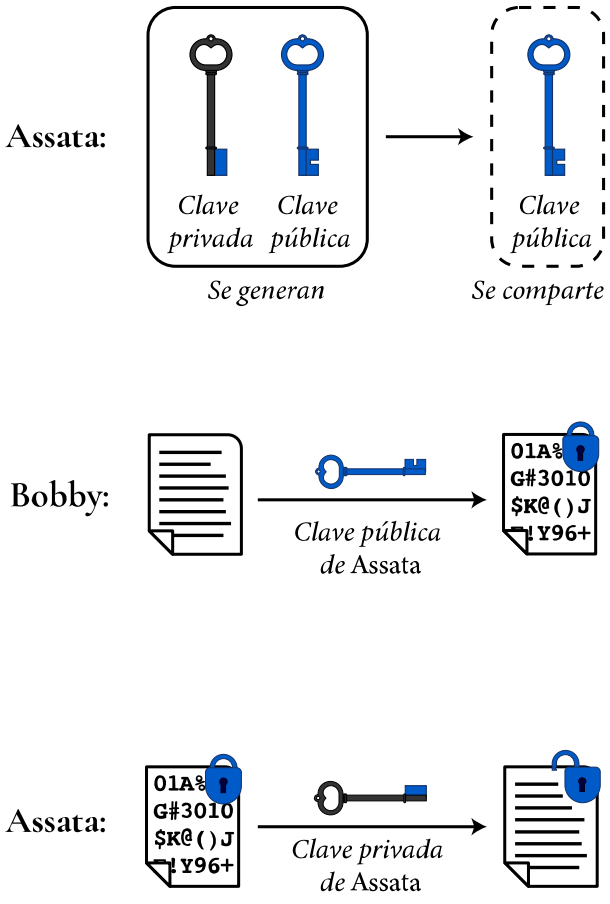
Los protocolos criptográficos pueden clasificarse en dos categorías principales. En la *criptografía simétrica*, la clave que se usa para descifrar un mensaje es la misma que (o es fácil transformarla a partir de) la clave usada para cifrar el mensaje. Este es el caso de los cifrados básicos (César, Vigenère y la libreta de un solo uso) descritos en el capítulo ¿Qué es el cifrado? Aunque, por supuesto, hay cifrados simétricos modernos que se usan, por ejemplo, para cifrar los datos en tu teléfono o computadora. Como hemos visto, usar estos protocolos para comunicarse puede ser un reto puesto que primero debes encontrar una forma de intercambiar la clave con tu interlocutor de manera privada. El protocolo criptográfico Diffie-Hellman ofrece un método para que dos personas generen una clave compartida (la cual puede usarse en un protocolo criptográfico de clave simétrica) a través de un canal inseguro (como internet).

La *criptografía de clave asimétrica* o *criptografía de clave pública* resuelve el problema de compartir la clave en una forma diferente. En lugar de usar una sola clave para cifrar y descifrar, la criptografía asimétrica usa dos claves: una para cifrar (conocida como *clave pública*) y otra para descifrar (conocida como *clave privada*). Este par de claves tiene las siguientes propiedades:

1. No es posible generar la clave privada a partir de la clave pública: ambas se generan juntas.
2. Un mensaje cifrado con una clave pública solo podrá ser descifrado (factiblemente) con la clave privada correspondiente.

Supongamos que Bobby desea enviar a Assata un mensaje cifrado. Assata crea un par de claves privada/pública y le envía a Bobby su contraseña pública (por un canal inseguro). Bobby usa la clave pública para crear el texto cifrado y se lo envía a Assata. El texto cifrado *solo* podrá descifrarse usando la clave privada de Assata.

Aunque cualquiera puede tener la clave pública de Assata, lo *único* que puede hacerse con ella es cifrar mensajes que solo podrán descifrarse con la clave privada de Assata. Por tanto, la seguridad se garantiza manteniendo privada la clave privada: secreta y segura.



Generar las claves pública y privada, compartir una clave pública, cifrar con una clave pública y descifrar con una clave privada

Con este modelo, cualquiera puede publicar su clave pública. Por ejemplo, Assata podría publicar su clave pública en línea de manera que cualquiera que desee enviarle un mensaje cifrado podría cifrarlo primero con su clave pública. De igual manera, Bobby podría crear su propio par de claves pública y privada y publicar su clave pública en línea para que otros puedan enviarle mensajes encriptados que sólo él podría descifrar con su clave privada (guardada de forma segura).

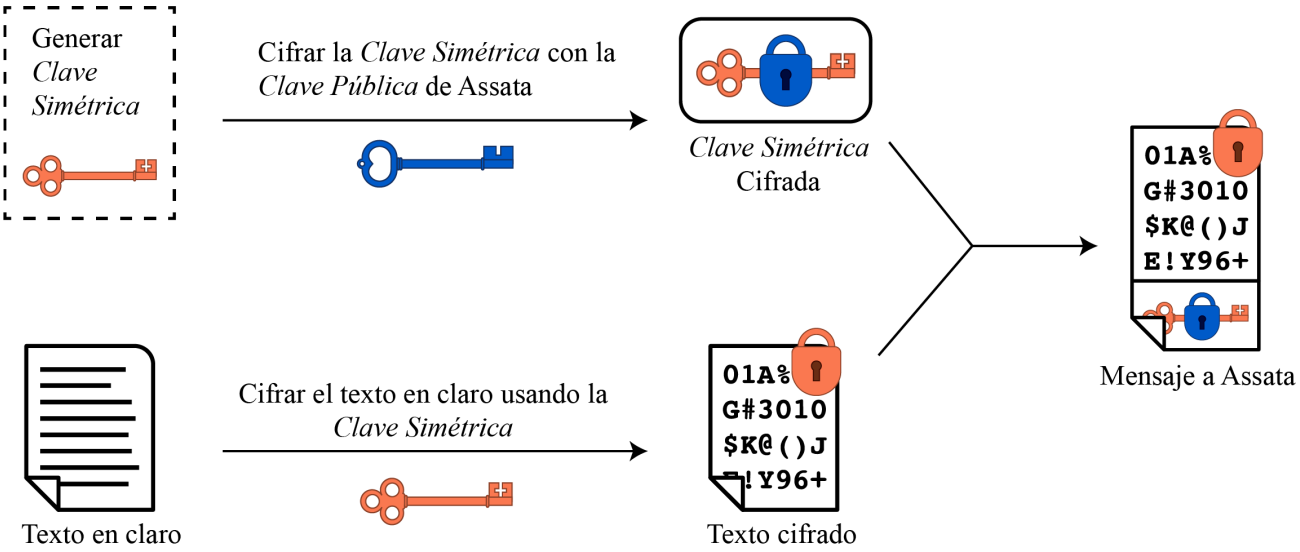
Repaso del protocolo Diffie-Hellman: ¿Criptografía asimétrica o simétrica?

Repasemos el protocolo Diffie-Hellman teniendo en mente las criptografías simétrica y asimétrica. Recordemos que Assata y Bobby acuerdan un número *p* de forma pública e insegura. Assata elige un número *a* (secreto) y calcula *p* ☆ *a* para enviárselo de manera pública e insegura a Bobby. Podríamos entonces considerar *a* como la clave privada de Assata, *p* ☆ *a* como su clave pública y este esquema como parte de un protocolo de clave asimétrica. Pero Bobby elige su propio número secreto *b* y lo combina con la clave pública de Assata para obtener *p* ☆ *a* ☆ *b*. De igual manera, Assata combina la "clave pública" de Bobby (*p* ☆ *b*) con su propia clave privada para obtener *p* ☆ *b* ☆ *a*. Puesto que *p* ☆ *a* ☆ *b* = *p* ☆ *b* ☆ *a*, Assata y Bobby tienen una clave común que pueden usar para cifrar y descifrar. Así, esto forma parte de un protocolo de clave simétrica. Por dichas razones, el protocolo Diffie-Hellman se encuentra en algún lugar entre la criptografía de clave asimétrica y la criptografía de clave simétrica.

Combinar criptografía asimétrica y simétrica

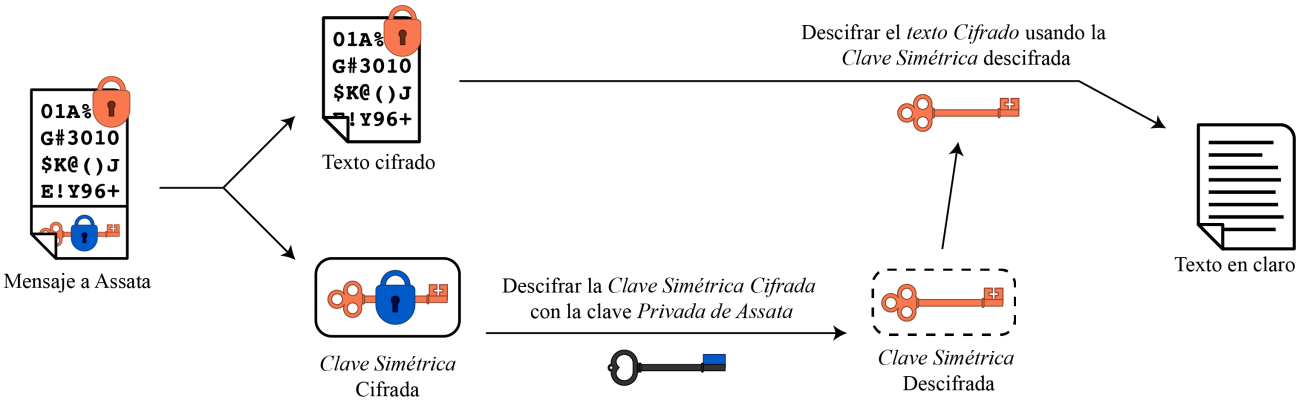
La criptografía asimétrica suele ser más costosa en términos computacionales que la de clave simétrica. Para lograr las mismas garantías de seguridad (por ejemplo, contra ataques de fuerza bruta y otros ataques), las claves públicas asimétricas deben ser mucho más largas que las simétricas. Asimismo, el propio cifrado toma más tiempo usando claves asimétricas que claves simétricas. También existe el problema de que, mientras más tiempo usas una clave para cifrar, más ejemplos hay de texto cifrado que pueden usarse en intentos de romper el cifrado (que no sean de fuerza bruta); es decir, las claves tienden a *caducar*.

Por estas razones, las claves públicas suelen usarse para descifrar una clave simétrica para una determinada *sesión* (comunicación). Supongamos que Bobby desea enviarle a Assata un mensaje cifrado. Bobby genera una clave criptográfica simétrica y cifra el mensaje con ella usando un cifrado simétrico. Luego, *cifra la clave simétrica* con la clave pública de Assata y, finalmente, le envía el mensaje y la clave cifrados, como sigue:



Combinación de criptografías simétrica y asimétrica (cifrado)

Assata descifra la clave cifrada con su clave privada y usa el resultado para descifrar el texto cifrado, como sigue:



Combinación de criptografías simétrica y asimétrica (descifrado)

Puesto que la clave pública solo se usa para cifrar claves (que suelen ser secuencias de apariencia aleatoria), la clave pública no caduca ya que los métodos para romper el cifrado que dependen de frases en lenguaje humano fallarían. Un beneficio adicional es que, si se logra romper el cifrado de un mensaje, eso no ayuda a romper el cifrado de un mensaje diferente, puesto que cada mensaje se cifra con una clave distinta.

En contexto: Activismo antinuclear y *Pretty Good Privacy*

Una implementación bastante robusta de la criptografía asimétrica es PGP, siglas en inglés de la afirmación (que se queda corta) *privacidad bastante buena*. (Una versión interoperable, gratuita y de fuente abierta de PGP es GPG o GNU Privacy Guard.) El cifrado PGP suele usarse para cifrar comunicaciones por correo electrónico con varios plug-ins y clientes de correo que admiten cifrado PGP. Existen algunos directorios en línea (sincronizados) de claves PGP, cada una asociada con una dirección electrónica, que permiten a Bobby localizar la clave PGP de Assata para enviarle un correo cifrado.

Phil Zimmermann, un activista antinuclear por muchos años, creó PGP en 1991 para que personas con los mismos intereses pudieran usar servicios de tablón de anuncios (BBSs, el Reddit de los 80) y guardar mensajes de manera segura. Desarrolló PGP como un proyecto de fuente abierta, que no requería una licencia para su uso no comercial. Lo publicó inicialmente en un foro especializado en movimientos políticos comunitarios, principalmente en el movimiento por la paz. Así, PGP se abrió camino en un foro para distribuir código fuente y rápidamente encontró su salida de Estados Unidos. Usuarios y simpatizantes incluían disidentes en países totalitarios, promotores de libertades civiles y *cypherpunks*. Sin embargo, en ese tiempo, los criptosistemas que usaban claves de más de 40 bits eran considerados munición en la definición de la regulación de exportaciones de Estados Unidos. Inicialmente, PGP fue diseñado para admitir claves de 128 bits. En febrero de 1993, Zimmermann se volvió blanco de una investigación criminal formal del gobierno de EU por el cargo de "exportación de munición sin una licencia". Zimmermann la enfrentó publicando todo el código fuente de PGP en un libro, el cual se distribuyó y vendió ampliamente. Cualquiera que deseara construir su propia copia de PGP podría simplemente quitar las tapas del libro, separar las páginas y escanearlas con un programa OCR, para crear un conjunto de archivos de texto de código fuente. En tanto que la exportación de munición (armas, bombas, aviones y software) estaba (y sigue estando) restringida, la exportación de libros está protegida por la Primera Enmienda. Después de varios años, la investigación sobre Zimmermann se cerró sin imputarle cargos criminales a él o a cualquier otro.

La legislación sobre exportaciones de criptografía desde Estados Unidos sigue siendo aplicable, pero se liberalizó sustancialmente a finales de los años 90 del siglo pasado. PGP ya no satisface la definición de un arma no exportable.

Qué aprender a continuación

- Autenticarse mediante firmado criptográfico

Recursos externos

- Electronic Frontier Foundation. "A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?" *Surveillance Self-Defense*, 29 de septiembre de 2014.
- Zimmermann, Phil. "Why I Wrote PGP." 1999.

Créditos

Autenticarse mediante firmado criptográfico

Se recomienda leer los capítulos Hash criptográfico y Criptografía asimétrica antes de seguir con este.

Lo que aprenderás

1. Cómo obtener el equivalente digital de una firma
2. Cómo usar las firmas criptográficas para brindar autenticidad
3. Qué significa autenticidad electrónica
4. Cómo usar las firmas criptográficas para diseminar confianza

Los sistemas criptográficos asimétricos pueden usarse con frecuencia para brindar autenticidad. En PGP, esto se facilita debido a la naturaleza complementaria de las claves pública y privada. Primero, se crean dos claves criptográficas, cualquiera de las cuales puede usarse como clave pública. La elección de cuál tendrá esta función es meramente arbitraria; es decir, cualquiera de ellas puede usarse para descifrar, siempre y cuando la otra se use para cifrar (y clave la privada sea justamente eso, para brindar seguridad).Una vez que se ha asignado una de las claves criptográficas como pública y la otra como privada, aun puedes usar tu clave privada para cifrar un mensaje. Sin embargo, cualquiera que tenga la clave pública podría descifrarlo. Si haces pública tu clave *pública*, cualquiera podrá descifrar tu mensaje y esto haría inútil el uso del cifrado para obtener privacidad en tus mensajes.

Esto ilustra muy bien que la única persona que podría haber cifrado un mensaje que puede descifrarse con *tu* clave pública eres *tú*, la misma persona que tiene *tu clave privada*. Cifrar un mensaje con tu clave privada brinda el equivalente digital de una firma y se le conoce como *firmado criptográfico*. De hecho, el firmado criptográfico brinda dos propiedades de la *autenticidad*:

1. *Atribución*. Tú escribiste el mensaje (y no alguien más).
2. *Integridad*. El mensaje fue recibido como fue escrito; es decir, no fue alterado.

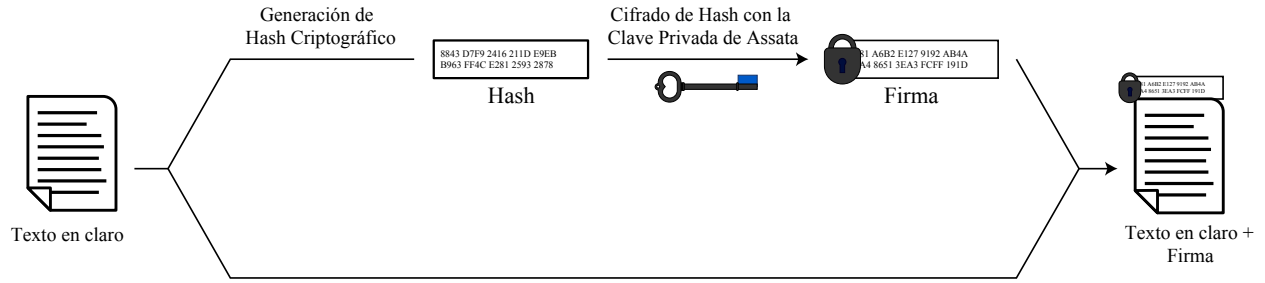
La segunda propiedad proviene del hecho de que una alteración tendría que modificar el texto cifrado de tal forma que descifrarlo con tu clave pública generaría el texto alterado según lo pretendía el intruso. Pero esto es completamente inviable.

Estas propiedades solo son significativas si tú eres la única persona en control de tu clave privada, puesto que cualquiera que la obtenga podría firmar criptográficamente su propio texto alterado.

Firmado criptográfico de hashes criptográficos

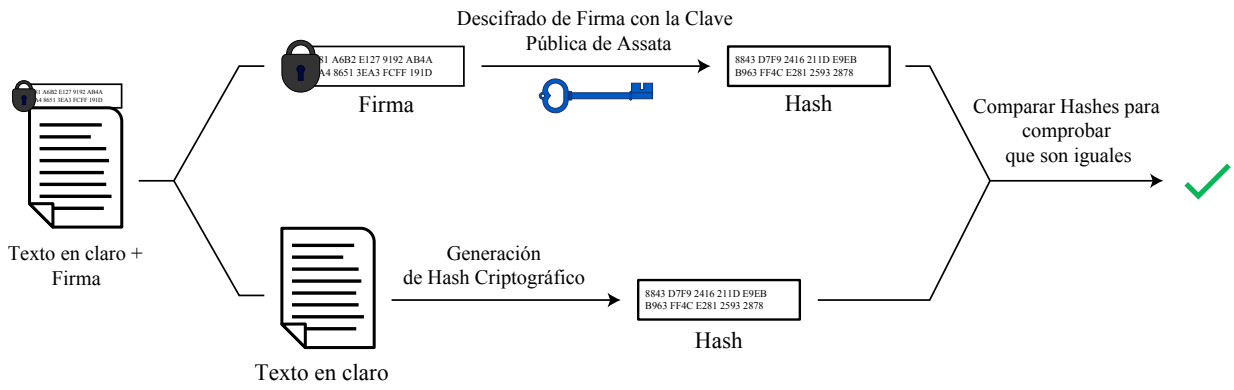
En la práctica, en lugar de cifrar todo el mensaje, uno podría cifrar un hash criptográfico (también conocido como valor hash o huella digital) del mensaje con el propósito de hacer un firmado criptográfico. Esto se hace por motivos de eficiencia. Consideremos el protocolo de que Assata firme un mensaje y Bobby verifique la firma, como se ilustra a continuación.

Assata toma un hash criptográfico de su mensaje y cifra el resultado con su clave privada; con esto crea una firma, que puede adjuntar al mensaje:



Creación de una firma

Bobby toma la firma y la descifra con la clave pública de Assata, lo que resulta en el mismo hash que Assata generó. Luego, toma su propio hash criptográfico del mensaje y compara el resultado con el hash descifrado que recibió de Assata:



Es inviable falsificar funciones hash criptográficas

Puesto que es inviable falsificar una función hash criptográfica, los dos hashes que Bobby genera (uno a partir directamente del mensaje de Assata y otro de la firma de Assata) son iguales; por tanto, sabemos dos cosas:

1. Solo Assata pudo haber generado la firma. Solo Assata podría cifrar algo que pueda descifrarse con su clave pública, puesto que ella es la única en posesión de su clave privada.
2. El mensaje no ha sido alterado desde que Assata lo escribió. Si alguien hubiera alterado el mensaje, el hash del mensaje sería diferente del contenido en la firma. Por tanto, un impostor tendría que falsificar una nueva firma, pero no puede generarla sin la clave privada de Assata.

En conclusión, hemos obtenido autenticidad en forma criptográfica.

Observa que Edgar, en un ataque de intermediario, podría simplemente eliminar la firma. Entonces, para que el firmado criptográfico sea efectivo, debes acordar usarlo todo el tiempo. Las modernas apps de mensajería con cifrado de extremo a extremo suelen contar con firmado integrado por defecto, aunque esto es invisible para el usuario promedio.

Aplicaciones de firmado criptográfico

Como en el ejemplo anterior, el firmado criptográfico puede brindar autenticidad a los mensajes de manera similar a como antes lo hicieron las firmas autógrafas o los sellos de cera. Sin embargo,

puedes firmar criptográficamente mucho más que solo mensajes (por ejemplo, correos electrónicos).

Verificación de software

Tal vez el uso más explícito y común de las firmas criptográficas se da en la verificación de software, aun cuando no estés consciente de ello. El software, como las apps, solo hará lo que sus desarrolladores pretendían que hiciera y dicen que hace, si no ha sido alterado a medio camino entre el desarrollador y tu computadora o teléfono. Un programa o app es en realidad solo un archivo electrónico (o conjunto de archivos), consistente en una secuencia de caracteres o un tipo de mensaje. Si un desarrollador ha firmado su software con criptografía de clave pública, un usuario cuidadoso puede verificar la firma obteniendo la clave pública del desarrollador y haciendo la validación que se ilustró antes. (El desarrollador debería proporcionar su clave pública por un canal diferente del canal por el que descargaste el software. Esto permitiría hacer una comparación fuera de banda, como se describió en el capítulo El intermediario: la clave pública que usas para hacer la validación está fuera de la banda del mensaje o la descarga de software.)

Gestionar la validación de huellas digitales y la red de confianza

Para confiar en la clave pública de Assata, Bobby debería verificarla a través de la huella digital de la clave, como se ha descrito. De otra forma, Edgar, el intruso, podría suministrar a Bobby una clave pública compatible con una clave privada en su poder.

Pero si Bobby ha verificado que la clave pública de Assata en realidad es de ella, entonces puede hacer el firmado criptográfico de la clave pública de Assata con su propia clave privada. Esto le permitirá a Bobby conservar un registro de las claves públicas que ha verificado, así como compartir la clave de Assata con otras personas, como se describe a continuación.

Supongamos que Cleaver quiere enviarle un mensaje cifrado a Assata y que también quiere asegurarse de que Edgar no va a estar de intermediario. Pero Cleaver no tiene un canal secundario a través del cual verificar la clave pública de Assata. Sin embargo, Cleaver ha recibido y verificado la clave pública de Bobby, así que Bobby puede enviarle la clave pública de Assata a Cleaver, con su firma. Si Cleaver confía en Bobby y ha verificado su clave pública, entonces puede verificar su firma en la clave pública de Assata y, en consecuencia, confiar en que es genuina.

En contexto: Canarios de seguridad

Los *canarios de seguridad* o *declaraciones canario* informan a los usuarios de que su proveedor *no* ha sido sometido a procesos legales o de otra naturaleza, al momento de la publicación, que

podrían poner en riesgo a los usuarios: filtraciones de datos, divulgación de claves de cifrado o accesos de puerta trasera al sistema. Si el anuncio no se actualiza en una fecha sugerida, los usuarios podrán inferir que ha habido un problema que podría poner en riesgo sus datos pasados y futuros. Por ejemplo, Riseup.net publica una declaración canario trimestral firmada criptográficamente para poder verificar su autenticidad; es decir, que en efecto la gente de Riseup.net escribió esa declaración. Riseup.net incluye un vínculo a un artículo periodístico fechado el día de emisión de su declaración para brindar evidencia de que la declaración no fue publicada antes de dicha fecha.

El uso de canarios de seguridad se inició en Estados Unidos como una forma de eludir órdenes de censura que acompañan ciertos procesos legales en los cuales el gobierno de ese país puede obligar a alguien a retener comunicaciones. Por otro lado, el gobierno de Estados Unidos casi nunca puede obligar a alguien a decir algo (en especial algo que no es cierto), de manera que no podría obligar a un proveedor a publicar una declaración canario que afirmara, falsamente, que nada ha ocurrido.

El término tiene su origen en el uso de canarios en las minas de carbón para detectar gases tóxicos: si el canario muere, ¡es necesario disipar el aire rápidamente!

Qué aprender a continuación

- Metadatos

Recursos externos

- Riseup. "Canary Statement." Consultado el 9 de febrero de 2021.
- Tor Project. "How Can I Verify Tor Browser's Signature?" Consultado el 9 de febrero de 2021.

Créditos

Metadatos

Lo que aprenderás

1. Qué son los metadatos
2. Qué pueden revelar los metadatos
3. Por qué es difícil proteger los metadatos

¿Qué son los metadatos?

Los metadatos son toda la información *acerca de* los datos, no los datos mismos. La mejor manera de ilustrarlo es con algunos ejemplos.

1. En el caso de una llamada telefónica, los metadatos incluirán los números telefónicos involucrados, la hora de inicio de la llamada y su duración. En el caso de llamadas por celular, es probable que los metadatos incluyan la ubicación del teléfono (las coordenadas GPS), la torre celular a la que estaba conectado e incluso el tipo de teléfono utilizado. Los metadatos de llamadas telefónicas no incluirían la propia transmisión de audio (esta sería "los datos"). Históricamente, el registro de metadatos de llamadas telefónicas se ha hecho con el objeto de facturar el servicio.
2. La mayoría de las fotografías digitales modernas incluyen información sobre la hora y lugar en que se tomó la fotografía, el tipo de cámara usado y sus configuraciones. En este caso, la fotografía constituye los datos. Muchos sitios, como Facebook, Twitter e Instagram, eliminan estos metadatos para proteger tu privacidad cuando cargas una fotografía o video. Otros, como Google, Flickr y YouTube, no lo hacen.
3. Casi todas las impresoras a color modernas, a petición del gobierno de Estados Unidos a los fabricantes y por temor a su uso en la falsificación de dinero, imprimen un código forense en cada página, que podría o no ser visible. En este caso, la hoja de papel (menos el código forense) constituye los datos y la información codificada en el código forense, los metadatos. Se sabe que el código forense, visible o no al ojo humano, puede incluir el día y hora en que se imprimió la hoja, así como el número de serie de la impresora.

La primera revelación de Edward Snowden puso en evidencia que la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) de Estados Unidos recababa todos los metadatos de las llamadas hechas por clientes de Verizon, lo cual obligó a traer los metadatos a la conversación y a la conciencia pública. El resultado fue un debate sobre la invasión a la privacidad.

Previamente, ese mismo año, Associated Press (AP) se resistió a la entrega de metadatos requerida por medio de una orden judicial del Departamento de Justicia. AP declaró: "Estos registros, que potencialmente contienen comunicaciones con fuentes confidenciales, de todas las actividades periodísticas emprendidas por la AP durante el periodo de dos meses brindan un mapa de las operaciones informativas de la AP y revelan información sobre las actividades y operaciones de dicha organización, las cuales el gobierno no tiene razón concebible alguna para conocer." Una opinión de la corte señaló que, al recabar datos de GPS a través de dichos metadatos, "se puede deducir si alguien es un feligrés, bebedor empedernido, visitante frecuente del gimnasio, marido infiel o paciente externo recibiendo tratamiento médico, o bien si está asociado con ciertos individuos o grupos políticos."

En un documento interno, la NSA se ha referido a los metadatos como "una de las herramientas más útiles" de la agencia.

Metadatos e internet

Cuando visitas un sitio web, se envía información entre tu computadora y el servidor del sitio a través de internet. En términos sencillos, se envía un mensaje de tu computadora al servidor solicitando el contenido del sitio, y luego se envía dicho contenido desde el servidor hacia tu computadora. La información enviada a través de internet se conoce como *tráfico*, y cualquier mensaje enviado se divide en muchos mensajes más pequeños, o *paquetes*. Cada paquete tiene tres partes principales:

1. El *encabezado* incluye la dirección de internet del remitente y del receptor (por ejemplo, tu computadora y el servidor del sitio) y una descripción del tipo de datos que se envía (por ejemplo, HTML).
2. Los *datos* son el contenido del mensaje (por ejemplo, el contenido de la página web o parte de la página web).
3. El *trailer* o *pie de página* señala el final del paquete y proporciona prueba de que este no ha sido corrompido en tránsito (con una función hash).

Los metadatos se componen del encabezado y el pie de página. Es difícil proteger u ocultar el encabezado puesto que indica a dónde debe enviarse un paquete. Al igual que en una carta, es necesaria una dirección de entrega. Tu dirección de internet, o dirección IP, está vinculada con tu ubicación física; de hecho, es frecuente que tu ubicación física pueda determinarse a partir de tu IP.

Esta descripción es válida para cualquier información enviada a través de internet, incluyendo correos electrónicos, transmisión de video en directo (*streaming*), llamadas VOIP y mensajes instantáneos.

En contexto: Proteger a un denunciante

En mayo de 2017, Reality Winner reveló documentos de la NSA para reportar la interferencia de Rusia en las elecciones presidenciales de 2016 en Estados Unidos. Su arresto, días antes de que la historia fuera publicada, causó mucha especulación sobre cómo fue identificada tan rápidamente como la denunciante. Muchos señalaron al sitio *Intercept* debido a su manejo de la historia.

Reality Winner había enviado de forma anónima a *Intercept* una impresión a color de los documentos. Como es práctica común en el periodismo, *Intercept* envió una fotografía de los documentos a la NSA para su verificación. Asimismo, tacharon algunas cosas en la fotografía y la publicaron en su informe. Poco después de la publicación de la historia, varias personas señalaron que el código forense de la impresora era visible en la fotografía y mostraba el día y hora en que se imprimió el documento, así como el número de serie de la impresora. Aunque es posible que el FBI haya identificado a Reality Winner a partir de esta información (para proteger a su fuente, *Intercept* debió haber ocultado el código forense de la fotografía), es más probable que la hayan delatado los registros de acceso a los documentos en su computadora de trabajo.

Qué aprender a continuación

- Enrutado anónimo

External Resources

- CNN. "AP Blasts Feds for Phone Records Search." 14 de mayo de 2013.
- *Electronic Frontier Foundation*. "Justice Department Subpoena of AP Journalists Shows Need to Protect Calling Records." 14 de mayo de 2013.
- *Electronic Frontier Foundation*. "Secret Code in Color Printers Lets Government Track You." 16 de octubre de 2005.
- Snowden Archive—the SIDtoday Files. "The Rewards of Metadata." *Intercept*, 23 de enero de 2004.
- *New Yorker*. "The Metadata Program in Eleven Documents." 31 de diciembre de 2013.
- *Intercept*. "Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election." 5 de junio de 2017.
- Atlantic. "The Mysterious Printer Code That Could Have Led the FBI to Reality Winner." 6 de junio de 2017.

Enrutado anónimo

Se recomienda leer los capítulos Intercambiar claves para cifrar y Metadatos antes de seguir con este.

Lo que aprenderás

1. Quién tiene acceso a qué en internet
2. Tecnologías que posibilitan las comunicaciones anónimas en línea
3. Qué es el anonimato y sus inconvenientes

Para comunicarte en línea, es necesario dirigir paquetes de información a tu computadora, ya sea información de una conversación a través de mensajería instantánea o correo electrónico o proveniente de búsquedas en la web. En esta sección, nos centramos principalmente en las búsquedas en internet, aunque las mismas ideas son válidas en casi todos los escenarios. La dirección de tu computadora, o dirección IP, es la forma en que las comunicaciones llegan a ella, tal y como una dirección física permite que un paquete o sobre llegue a tu buzón. Por la misma razón, la actual dirección IP de tu computadora (que cambia según el lugar donde te conectes a internet) está relacionada con tu ubicación física. La precisión de esa ubicación física depende de cuánta información revele el proveedor de servicios de internet (ISP, por sus siglas en inglés) y a quién esté dispuesto a revelar dicha información. El ISP sabe desde cuál cable, línea telefónica o torre celular estás recibiendo tráfico de internet, pero tal vez solo proporcione tu código postal a los sitios web de geolocalización IP, o tal vez proporcione la ubicación de una casa específica.

Tu dirección IP es solo una pieza de metadatos necesaria para obtener información de tu computadora. Sin embargo, cuando navegas en la web, muchos otros metadatos que no son estrictamente necesarios se transmiten para “maximizar tu experiencia de búsqueda”. Esta información incluye datos como los *plug-ins* que usas en tu buscador, tu zona horaria y el tamaño de tu pantalla, que pueden usarse como identificadores únicos en las direcciones IP que usas para conectarte a internet.

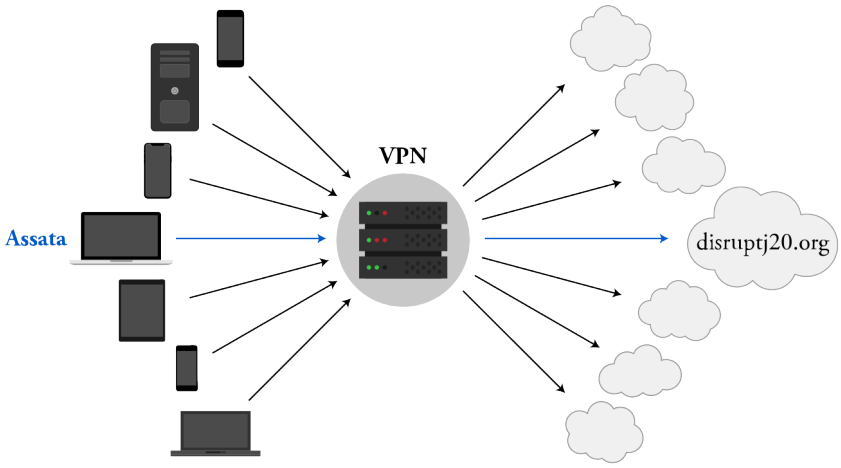
¿Quién tiene acceso a todos estos metadatos que pueden usarse para identificarte? Sin un cifrado, así como el uso de https, cualquier espía podría obtener acceso a estos metadatos y al contenido de tus comunicaciones. El cifrado podría proteger algunos metadatos contra tu ISP y cualquier espía (como cuál buscador usas) pero no tu dirección IP ni los dominios de la web que visitas. Asimismo, los servidores de los sitios que visitas tendrían acceso a tus metadatos, así como a cualquier contenido.

Dado que los metadatos se usan para obtener información sobre ti, ¿hay forma de proteger estos metadatos, y contra quién podrías protegerlos? A continuación se describen dos formas de hacer anónimas tus búsquedas en la web.

Confiar en el intermediario: redes privadas virtuales

La tecnología de las redes privadas virtuales (VPN, por sus siglas en inglés) comenzó como un medio para extender una red local (como la red de una universidad o una compañía) a ubicaciones remotas (como una residencia fuera del campus u oficinas en casa) de manera que, sin importar dónde te encontraras, pudieras acceder a los mismos recursos que si estuvieras en las redes locales (como ocurre con las suscripciones a bibliotecas y a software). Mientras estés conectado a una VPN, el anfitrión de una página web verá la dirección IP de la red local que la VPN está extendiendo *como tu dirección*, la dirección de tu casa. Por esta razón, el uso de las VPN se ha vuelto popular para volver anónima la ubicación.

Una VPN funciona como un intermediario (ojalá que inofensivo), como se ilustra a continuación. En lugar de enviar todas sus solicitudes a la web de forma directa, Assata las envía a su VPN, la cual recaba sus solicitudes de internet por ella y luego le retransmite los resultados. Los detalles de cómo funciona esto varían entre diferentes servicios de VPN, pero usualmente las comunicaciones entre tú y la VPN están cifradas. La cualidad protectora de la VPN reside en que muchas otras personas también se conectan a ella. Un espía que observara las comunicaciones hacia y desde una VPN podría identificar a los individuos conectados a la VPN, así como las solicitudes que esta recaba, pero idealmente sería incapaz de relacionar dichas solicitudes con los usuarios correspondientes puesto que hay muchas solicitudes simultáneas hacia y desde la VPN.



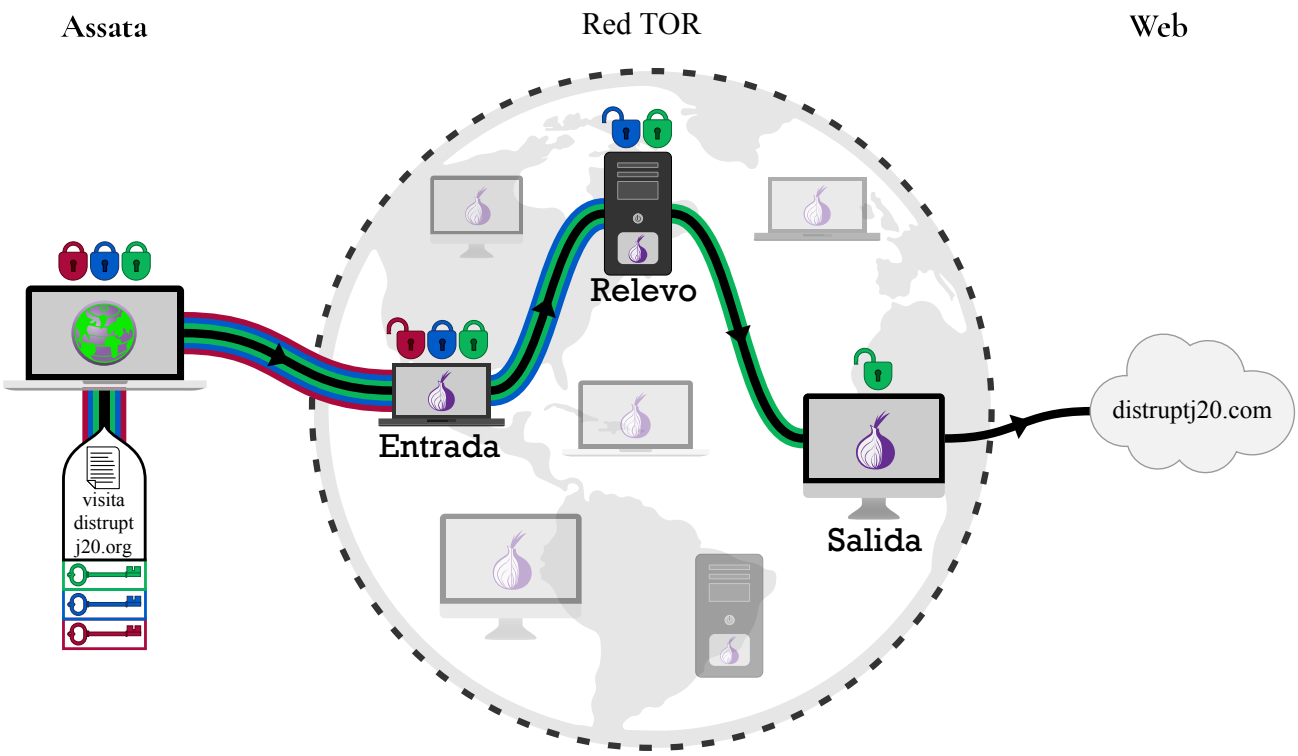
Redes privadas virtuales

Por supuesto, el proveedor de VPN conoce tu comportamiento en internet y, con su cooperación, un adversario también podría conocerlo: es decir, estás confiando esa información a tu proveedor de VPN.

Sin embargo, tu ISP (sin una VPN) tiene acceso a esa misma información: estás poniendo la misma confianza en tu proveedor de VPN que en tu ISP. La diferencia es que tu ISP no oculta tu dirección IP a los servidores destinatarios en internet, mientras una VPN sí lo hace. Por otro lado, el uso de la misma VPN en diversas ubicaciones de conexión (por ejemplo, tu casa, tu trabajo, la cafetería) conlleva cierto aumento del riesgo para la privacidad, pues da un panorama más completo de tu uso de internet que el que brindaría el ISP de cada una de esas ubicaciones.

Desconfiar del intermediario: Tor

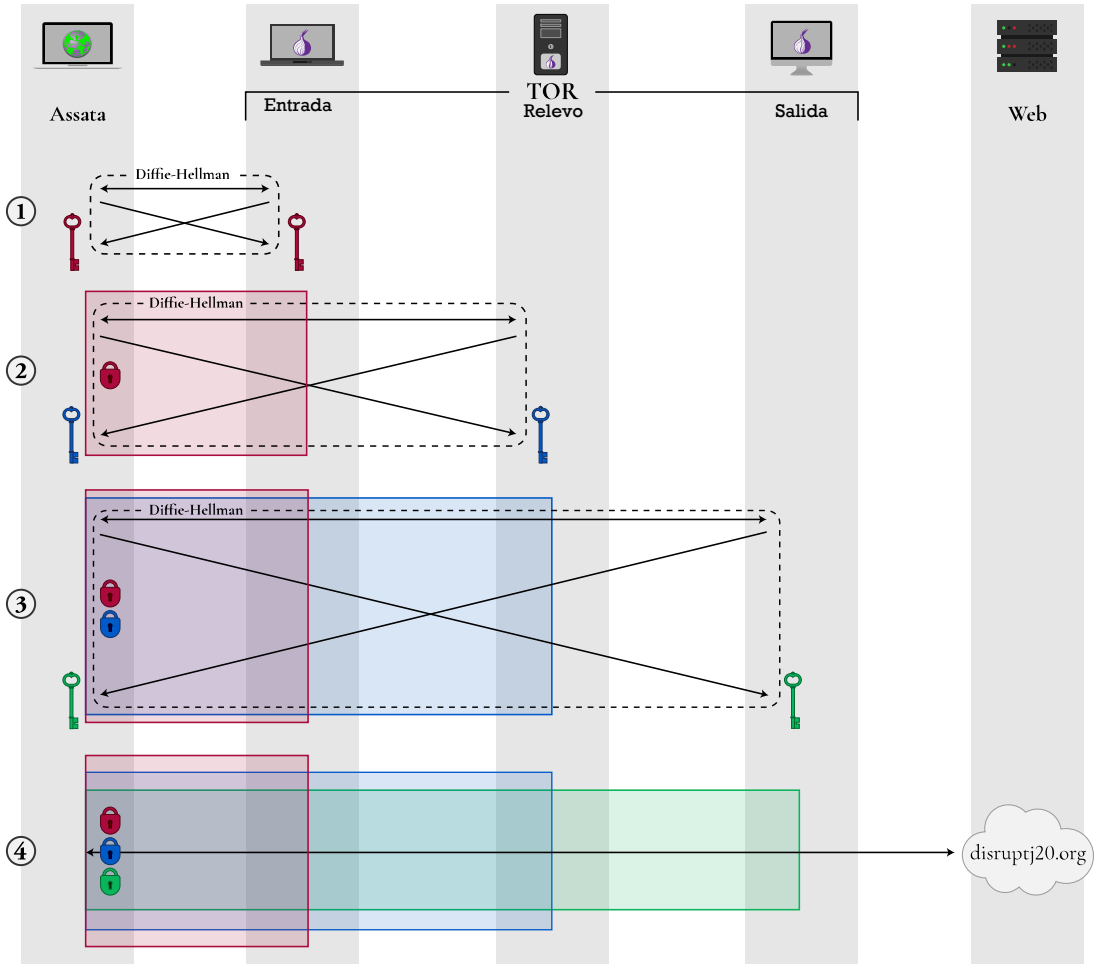
The Onion Router, también conocido como Tor, es un medio para acceder a internet de forma anónima: elude problemas de confianza y deriva su nombre de que usa *capas* de cifrado (como las capas de una cebolla). En lugar de usar un solo intermediario a quien confías toda tu información, usas (al menos) tres intermediarios elegidos al azar entre una selección de miles de servidores voluntarios, según se ilustra a continuación. El tráfico a través de esta ruta de intermediarios está cifrado de manera que el primer nodo (entrada) solo sabe que estás accediendo a internet por medio de Tor; el segundo nodo (un relevo) solo sabe que alguien está accediendo a algo en internet a través de Tor (pero no específicamente quién o qué) y el último nodo (salida) solo sabe que un usuario Tor está solicitando una cierta página web (por ejemplo), pero no cuál usuario Tor.



Tor

Esto se logra usando protocolos de intercambio Diffie-Hellman, primero con el nodo de entrada, luego con el de relevo y finalmente con el de salida, como se ilustra a continuación. (1) Assata establece una clave criptográfica que comparte con el nodo de entrada (al cual llamaremos *clave de entrada*, en rojo). Esto establece un canal de comunicación cifrada entre Assata y el nodo de entrada. (2) Assata usa este canal cifrado para comunicarse con el nodo de relevo por medio del nodo de entrada. El tráfico entre los nodos de entrada y de relevo no está cifrado, pero Assata usa este canal por medio del nodo de entrada para establecer una clave criptográfica que ella comparte con el nodo de relevo (la *clave de relevo*, en azul).

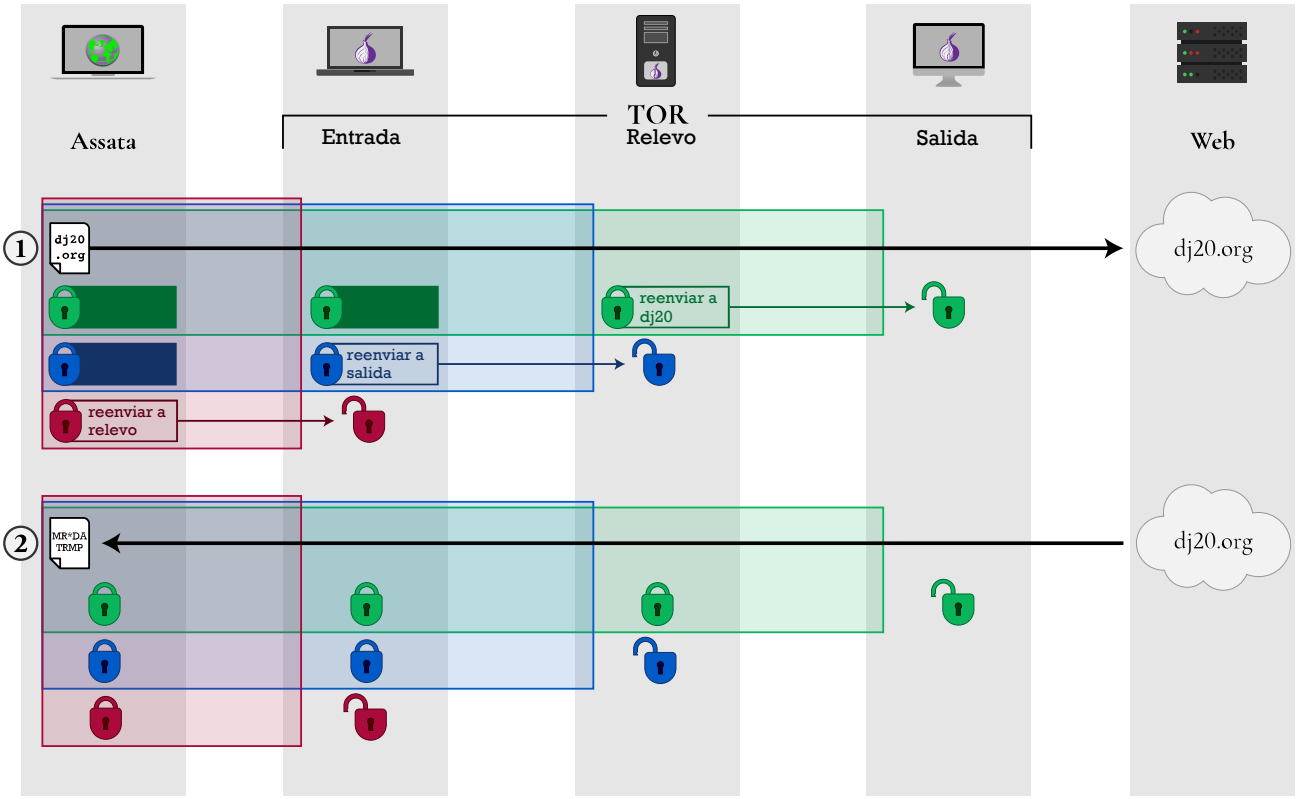
Lo único que el nodo de relevo sabe es que está estableciendo una clave compartida con cierto usuario Tor, pero no conoce la identidad de dicho usuario. (3) Este proceso se repite para establecer una clave de cifrado que Assata comparte con el nodo de salida (la *clave de salida*, en verde). (4) Esto crea una secuencia de claves (rojo, azul, verde) que posibilitan el cifrado entre Assata y los nodos de entrada, relevo y salida, respectivamente.



La forma en que Tor establece claves en rondas de intercambios Diffie-Hellman

Para enviar una solicitud a disruptj20.org, Assata cifra la solicitud con la clave verde y la dirige al nodo de salida; luego, la envuelve en un mensaje dirigido al nodo de relevo y lo cifra con la clave azul; después, envuelve esto en un mensaje dirigido al nodo de entrada y lo cifra con la clave roja. El mensaje es enviado entonces al nodo rojo. El nodo de entrada elimina la primera *capa* de cifrado (con la clave roja que el nodo de entrada comparte con Assata), lo cual revela el mensaje dirigido al nodo de relevo. El nodo de relevo elimina la segunda *capa* de cifrado (con la clave azul que el nodo de relevo comparte con Assata), lo cual revela un mensaje dirigido al nodo de salida. El nodo de salida elimina entonces la tercera *capa* de cifrado (con la clave verde que el nodo de salida comparte con Assata), lo cual revela un mensaje dirigido a disruptj20.org., el cual es remitido por el nodo de salida. Esto se ilustra a continuación.

Para que disruptj20.org envíe información de vuelta a Assata, el servidor web envía la información de vuelta al nodo de salida. Este hace el cifrado con la clave verde y la envía al nodo de relevo, el cual, a su vez, hace el cifrado con la clave azul y la envía al nodo de entrada. Este último hace su cifrado con la clave roja y envía la información a Assata. Assata puede eliminar las tres *capas* de cifrado porque ella tiene todas las claves necesarias, como se ilustra a continuación.



Cómo atraviesa la información la red Tor

Para recrear tu ruta por la red Tor y, en consecuencia, tu solicitud a la web, tu adversario podría necesitar controlar los tres nodos que elegiste como entrada, relevo y salida. Incluso un adversario que controlara 80 por ciento de la red Tor tendría solo 50 por ciento de probabilidades de controlar los tres nodos que elegiste. Puesto que hay miles de nodos Tor (que cualquiera puede ofrecerse a operar), esto es improbable.

Un ataque alternativo que un adversario podría emprender es un *ataque de confirmación*. En este escenario, el adversario intentaría probar que has visitado un servicio web en específico. Si pudiera acceder a tu tráfico web (por ejemplo, a través de tu ISP) y al tráfico del servicio web objetivo (por medios legales o ilegales), tu adversario podría relacionar tu uso de Tor para acceder al servicio web, con base en el horario del servicio web. Este tipo de correlación se usó en el caso contra Jeremy Hammond, quien fue condenado por actividades de piratería informática realizadas por el colectivo activista Anonymous.

Tor ha sido atacado en otras ocasiones, pero el proyecto Tor reacciona rápidamente para mejorar su tecnología y seguridad. En el capítulo Proteger tu identidad se discuten los obstáculos para la navegación anónima y los inconvenientes que enfrentará un usuario, así como las mejores prácticas para acceder a la web de forma anónima.

Uso y obstáculos para el uso de tecnologías de búsqueda anónima

Muchas personas usan las VPN y Tor para acceder a una web sin censura en países donde la censura de internet es común, como China e Irán.

Sin embargo, hay evidencia de que se puede recopilar tráfico de una VPN a partir de los metadatos de comunicaciones en internet, y los gobiernos pueden valerse de esto para bloquear dichas comunicaciones, como han hecho los de China y Siria en sus esfuerzos de censura. Se sabe que otros países, como Irán, bloquean el acceso a ciertos proveedores de VPN no autorizados por el gobierno.

Puesto que los nodos de Tor están listados públicamente, es posible bloquear el uso de Tor como un todo (un gobierno puede hacerlo, por ejemplo). Esto se consigue bloqueando todo tráfico dirigido a los nodos de Tor. Este bloqueo puede superarse con el uso de *puentes*, un conjunto de nodos de Tor que no están listados públicamente y que pueden usarse en lugar de los nodos de entrada listados públicamente. Para acceder a un pequeño conjunto de nodos *puente*, debes solicitarlo enviando un correo electrónico al proyecto Tor desde una cuenta restringida (por ejemplo, Google, Riseup! o Yahoo!). También se puede bloquear a Tor mediante una inspección de paquetes; es decir, verificando los metadatos de las comunicaciones (como con el tráfico de una VPN). El proyecto Tor hace que eso sea complicado confundiendo el tráfico de Tor en internet, de manera que no parezca tráfico de Tor.

Las VPN y Tor también se usan para obtener acceso a sitios específicos que podrían no estar disponibles en tu jurisdicción debido a una política del anfitrión web. Eso es común en plataformas de medios como Hulu y Netflix. Para contrarrestar esto, las compañías suelen bloquear el acceso a su contenido desde proveedores de servicios VPN conocidos o desde nodos de salida de Tor.

En contexto: Disruptj20

El 20 de enero de 2017 surgieron protestas en masa relacionadas con la investidura del cuadragésimo quinto presidente de Estados Unidos. Gran parte de la organización de dichos eventos se coordinó en el sitio disruptj20.org. En agosto de 2017 se reveló que el Departamento de Justicia de Estados Unidos había emitido una orden judicial dirigida al anfitrión de disruptj20.org, DreamHost, para obtener, entre otras cosas, “todas las solicitudes HTTP y registros de errores”, los cuales incluirían las direcciones IP de todos los individuos, presuntamente 1.3 millones de personas, que visitaron el sitio web, así como las subpáginas que visitaron, con cuánta frecuencia lo hicieron y cualquier texto que cualquier usuario hubiera tecleado en la página web.

Por supuesto, las tecnologías de navegación anónima habrían protegido las direcciones IP de dichos visitantes al sitio.

Qué aprender a continuación

- Proteger tu identidad

Recursos externos

- The Great Firewall of China realiza un seguimiento de cuáles y cuántas o cuántas veces los sitios son censurados en China.
- Search Warrant to DreamHost, agosto de 2017.

Créditos

PARTE 2: REPRESIÓN DIGITAL DE MOVIMIENTOS SOCIALES (EN EUA)

Mecanismos de represión de movimientos sociales

Antes de leer este capítulo sería buena idea volver a leer la Introducción: el porqué de la seguridad digital para recordar que el enfoque principal de este libro son los movimientos sociales en Estados Unidos.

Lo que aprenderás

1. Cómo reprime el gobierno de Estados Unidos los movimientos sociales
2. Qué fue COINTELPRO (Counter Intelligence Program) y qué mecanismos usó para reprimir movimientos sociales

En Estados Unidos hay una larga historia de interferencia en los esfuerzos de los movimientos sociales, incluso dentro del mismo territorio, y en particular de los movimientos de liberación y de izquierda. Movimientos de organización laboral, de independencia, derechos civiles y en favor del medio ambiente han sido objeto de la oposición del gobierno de Estados Unidos, con frecuencia siguiendo las órdenes o en cooperación con grandes corporaciones.

Con el propósito de luchar contra los riesgos asociados con que un movimiento social *no* procure la seguridad digital, es útil revisar la forma en que el Estado ha interferido en el pasado en dichos movimientos. Esta historia puede resultar abrumadora y puede ser tentador desestimarla como algo que ocurrió en el pasado pero que no sucede ahora. Repasarla también puede conducir al derrotismo, en especial a la luz de las herramientas mejoradas digitalmente que el Estado puede usar contra un adversario (percibido o real).

Sin embargo, puesto que no debemos condenarnos a repetir errores del pasado, es necesario repasar la historia y aprender las lecciones pertinentes para que nuestros movimientos tengan mayor éxito en el futuro. Con el objeto de lograr esto sin convertir este libro en un libro de historia, recurriremos al trabajo académico de Jules Boykoff, quien categorizó las formas en que Estados Unidos se entrometió en los movimientos sociales del siglo XX. Boykoff menciona doce *métodos de represión*, que hemos compactado en siete en esta presentación.

Comprender estos modos históricos nos permitirá predecir la forma en que la vigilancia digital podría apoyar dichos modos, como se discutirá en el capítulo Amenazas digitales a movimientos sociales. Pero, lo que es más importante, podremos ver cómo el cifrado y la procuración de higiene digital pueden proteger a los movimientos sociales contra (algunas de) estas fuerzas contrarias, como se verá en la *Parte 3* de esta obra.

Modos de represión

A continuación se presentan siete formas en que Estados Unidos ha reprimido y continúa reprimiendo movimientos sociales, con algunos ejemplos de sus usos. Desafortunadamente, estos ejemplos están lejos de ser exhaustivos.

1. Violencia directa

Golpizas, bombardeos, tiroteos y otras formas de violencia han sido perpetrados por el Estado u otras instituciones o nodos de poder en contra de ciudadanos disidentes.

Lo anterior podría haber sido resultado de la vigilancia policial de grandes grupos (como cuando la Guardia Nacional del Ejército de Ohio disparó a estudiantes durante una protesta contra la guerra en la Universidad Estatal Kent y asesinó a cuatro personas e hirió a otras nueve) o de asesinatos planeados (como en la redada nocturna organizada por el FBI contra el líder del Partido Pantera Negra, Fred Hampton). A riesgo de subestimarlas, estas acciones desalientan la participación en movimientos sociales por el temor a perder la vida o la integridad física.

2. El sistema legal

El sistema legal permite hacer arrestos para acosar, persecuciones y audiencias públicas, y el uso de leyes extraordinarias para interferir en las actividades de determinados individuos de manera sesgada. El Estado arresta a activistas por cargos menores que suelen ser falsos y algunas veces basados en estatutos inciertos que han permanecido en los libros, enterrados e inactivos, aunque han sido la vía para efectuar persecuciones legales selectivas. Las acusaciones y audiencias públicas pueden llevar a los disidentes a la cárcel o agotar sus recursos económicos en procedimientos legales que desvían su activismo e inmovilizan a los movimientos. Se ha desalentado de presentar ideas disidentes a personas que actualmente respaldan o que podrían ser aliados de alguna causa. Las acusaciones y audiencias difundidas por los medios de comunicación masiva resuenan en la esfera pública. Otra forma de represión legal es que el Estado promulgue y ejecute leyes y reglas extraordinarias para mantener atados a los activistas en el laberinto de la justicia criminal. Así es como se ha usado el sistema legal para sofocar el disenso.

Ciertos programas cuestionables para detener y cachear arbitrariamente han permitido a oficiales hacer justamente eso sin una causa probable. La existencia de zonas de libre expresión limita en gran medida la hora, el lugar y la forma en que es posible protestar. Quienes fueron arrestados en protestas protegidas por la Primera Enmienda durante la investidura de Donald Trump enfrentaron acusaciones por las cuales era muy improbable llegar a una condena. Asimismo, ciertos delitos como el incendio intencionado o la destrucción de propiedad suelen ser elevados a terrorismo cuando van acompañados de un motivo político, lo cual permite al Estado incrementar significativamente las penas asignadas. Otras leyes están diseñadas específicamente para disuadir el activismo, como las llamadas "leyes mordaza", que criminalizan la filmación de operaciones de la agricultura (que se hace para exponer el abuso de animales).

3. Privación del empleo

Las creencias o actividades políticas de una persona pueden ser causa de sufrir la amenaza o hasta la pérdida del empleo. Algunos disidentes no son contratados, en primer lugar, debido a sus posturas políticas. Esto es perpetrado por los empleadores, aunque el Estado tiene una influencia directa o indirecta.

En tiempos recientes, hemos visto a profesores universitarios perder sus trabajos o a quienes han perdido ofertas de trabajo, como Steven Salaita, cuya oferta para trabajar como profesor de estudios sobre los nativos de América del Norte fue retirada tras las objeciones de algunos donadores de la universidad a una serie de Tweets de Salaita críticos de Israel y el sionismo. Desde hace varios años (aunque esto fue derogado por una corte federal), se solicitó a los contratistas del gobierno de Texas firmar un pliego en el que se comprometían a no participar en el movimiento pro-Palestina: Boicot, Desinversiones y Sanciones, so pena de cancelación de sus contratos. Esto tuvo como resultado el despido de un ciudadano estadounidense de ascendencia palestina que trabajaba como patólogo del habla en una escuela y que se negó a firmar dicha declaración.

4. Vigilancia abierta

El objetivo de la vigilancia abierta no es recabar información (lo cual se logra mejor en secreto), sino intimidar. Con ella se pretende lograr un *efecto inhibidor* en virtud del cual las personas reprimen su discurso y acciones por temor a represalias. Esta vigilancia puede incluso ahuyentar a quienes ya son activistas o desmotivar a otros posibles activistas. Aunque se ha considerado que el *efecto inhibidor* es inconstitucional, es difícil de probar en una corte que de hecho se ha hecho un daño y por tanto resulta un medio seguro de represión (desde la perspectiva de quien vigila).

El FBI cuenta con una larga historia de practicar la técnica de "tocar y hablar", que consiste simplemente en visitar la casa de disidentes y activistas (y de sus familiares y empleadores) para "conversar", con el objetivo de que la gente sepa que están bajo vigilancia.

5. Vigilancia encubierta

La vigilancia también puede enfocarse, como con el uso de espías, las intervenciones telefónicas y órdenes judiciales para obtener información, así como con el uso de infiltrados (agentes encubiertos que se vuelven miembros de un grupo-objetivo) e informantes (miembros de cierto grupo a quienes se paga o amenaza con el fin de extraer información). Y también puede dispersarse, como en la acumulación, almacenamiento y análisis de información perteneciente a individuos y grupos, obtenida a través de la vigilancia por internet, la violación de la correspondencia y otras técnicas de vigilancia en masa.

La dimensión del programa de informantes del FBI es considerable: en 2008 contaba con más de quince mil informantes. Después de los ataques del 11 de septiembre de 2011 (9/11), el FBI y grandes agencias de seguridad como el Departamento de Policía de Nueva York (NYPD, por sus siglas en inglés) volcaron sus programas de inteligencia contra las comunidades musulmanas estadounidenses. Esto incluyó la vigilancia estrecha por parte del FBI de abogados, profesores, y del director ejecutivo de la organización más grande de derechos civiles de musulmanes en Estados Unidos (Council on American-Islamic Relations). El NYPD tomó como objetivos a mezquitas y asociaciones estudiantiles, organizaciones y negocios de musulmanes mediante el uso de informantes, infiltrados y vigilancia. La supuesta lógica del NYPD era identificar "terroristas" potenciales a través de la identificación de "indicadores de radicalización", que incluían actividades protegidas por la Primera Enmienda, como "usar vestimenta según la tradición islámica [y] usar barba", al igual que "involucrarse en activismo social".

6. Engaño

El término *Snitchjacketing* se aplica cuando una persona (con frecuencia un infiltrado) crea sospechas de que un verdadero activista es un informante del Estado o se presenta de alguna otra forma maliciosa en un movimiento social. Se conoce como *agentes provocadores* a los infiltrados o informantes cuyo objetivo es promover la violencia y actividades o tácticas ilegales (en lugar de simplemente reportar sobre actividades) con el propósito de atrapar legalmente o desacreditar a un grupo. La falsa publicidad es el uso de documentos fabricados, diseñados para dividir o minar la solidaridad en las organizaciones de activistas. Dichos documentos cuestionables, ofensivos y algunas veces violentos, tienen la intención de crear tensión dentro de y entre grupos.

Infiltrados del FBI han actuado como agentes provocadores conduciendo grupos hacia un camino de actividades ilegales que de otra forma no habrían seguido. Mohamed Mohamud era un estudiante de la Universidad Estatal de Oregon que fue contactado por un agente encubierto del FBI que durante un periodo de cinco meses sugirió y proporcionó los medios para que Mohamud hiciera detonar explosivos durante la ceremonia de encendido del árbol de Navidad de Portland, el 26 de noviembre de 2010. La bomba era falsa, pero Mohamud fue sentenciado a treinta años de prisión.

Eric McDavid pasó casi nueve años en prisión acusado de conspirar para dañar propiedad corporativa y gubernamental después de que un informante pagado por el FBI actuó como agente provocador: incitó al grupo de McDavid a cometer destrucción de propiedad y les proporcionó información para hacer bombas, dinero para comprar los materiales necesarios, transporte y una cabaña para trabajar. La sentencia de McDavid fue revertida debido a que el FBI omitió revelar a la defensa evidencias potencialmente exculpatorias.

7. Influencia de los medios de comunicación masiva

Existen dos tipos principales de manipulación mediática: (1) creación de historias; en este caso, el Estado hace uso de sus contactos en la prensa para publicar artículos generados por el gobierno, palabra por palabra o con ajustes menores, y (2) intimidación; el Estado intimida a periodistas o editores para evitar que información no deseada llegue a publicarse. Además de eso, el menoscabo efectuado por los medios masivos muestra a los disidentes como ridículos, extraños, peligrosos o fuera de sintonía con la sociedad en general.

Es frecuente que esto se deba más al apego responsable de los medios a las normas y valores periodísticos que a alguna conspiración. Las subestimaciones de los medios ocurren cuando los activistas y el Estado presentan cálculos discrepantes sobre las dimensiones de protestas, marchas y otras actividades; ante esto, los medios tienden a aceptar las bajas cifras del Estado. También ocurre que los medios hacen compensaciones falsas entre la cantidad de disidentes y de aquellos que se oponen a las manifestaciones. Muchos esfuerzos disidentes nunca llegan al orden del día de los medios de comunicación masiva o quedan enterrados en las secciones más pequeñas de los periódicos. No solo el Estado, sino también las organizaciones de medios más poderosas o sus dueños pueden perpetrar este tipo de represión.

Tras la invasión de Irak después del 9/11, las opiniones contra la guerra fueron minimizadas de forma consistente ya que recibieron poca cobertura. Solo por poner un ejemplo, en septiembre de 2006 el *Oregonian* informó de esta forma sobre protestas contra la guerra que reunieron en las calles a más de 200 mil personas en todo Estados Unidos: reportó una protesta contra la guerra de 100 mil personas en Washington, DC, en la página 10, junto a un artículo sobre una protesta en Portland. El artículo estimaba la presencia de cien personas en esta última protesta, aunque evidencia aérea mostraba más de 3 mil. En cambio, una manifestación contraria a la protesta antiguerra en Washington, DC, fue cubierta en la página 2, con una fotografía y un texto más grandes, aunque solo 400 personas asistieron a ella.

Interferencia en las tecnologías de la información

Este libro sería omiso si no mencionáramos la censura y otras interferencias en las tecnologías de la información. Se trata de una forma adicional de represión, con especial pertinencia en la Era de

la Información, que se entrecruza con el engaño y la influencia de los medios de comunicación masiva y a través de la cual se bloquea el acceso a internet o la infraestructura relacionada o se deniega de alguna otra forma el acceso a ella a los movimientos sociales: por ejemplo, inhabilitando el acceso a internet o a redes celulares durante una protesta, censurando ciertos sitios o tipos de tráfico de internet o bajando el sitio web de algún movimiento social.

Boykoff no incluye en su catálogo esta forma de represión porque su uso no se ha extendido dentro de Estados Unidos a manos de Estados Unidos, principalmente debido a las protecciones constitucionales del país. Sin embargo, su uso sí se ha extendido al rededor del mundo. Se sabe que ciertos gobiernos bloquean el acceso a internet en el ámbito nacional (como en el apagón de internet de una semana en Irán, usado como medio para reprimir las protestas) o limitan el acceso a ciertos recursos (como El Gran *Firewall* de China, que bloquea Google, Facebook, Twitter y Wikipedia). Compañías estadounidenses también participan en esto, pues se someten a la censura extranjera: Zoom (un servicio de conferencias) canceló a petición de China las cuentas de tres activistas que habían planeado eventos para conmemorar la masacre de la plaza de Tiananmén.

En contexto: COINTELPRO y la era de COINTELPRO

Entre los años cincuenta y los años setenta del siglo pasado, el FBI llevó a cabo un conjunto de actividades secretas, de contrainteligencia nacional, que se conocen ahora como COINTELPRO, bajo el liderazgo del entonces director del FBI, J. Edgar Hoover.

COINTELPRO se originó a partir de los programas anticomunistas del gobierno de Estados Unidos, durante el Temor Rojo, y pretendía "alterar por cualquier medio necesario" la organización y esfuerzos de activistas de movimientos como Poder Negro, en favor de la independencia de Puerto Rico y de los derechos civiles, por mencionar algunos. En relación con los movimientos en favor de los derechos civiles y con Poder Negro (e incluyendo las actividades de Martin Luther King, Jr.), COINTELPRO tenía órdenes de "exponer, alterar, distraer o neutralizar de alguna otra forma las actividades de organizaciones y agrupaciones de nacionalismo negro de tipo opositor, de su liderazgo, portavoces, miembros y simpatizantes, para contrarrestar su propensión a la violencia y al desorden civil".

COINTELPRO fue expuesto gracias al robo de cajas llenas de documentos confidenciales del FBI obtenidos en un robo realizado en 1971, por parte de la Comisión Ciudadana para Investigar al FBI. Sus miembros hicieron público esto tras las revelaciones de Ed Snowden, y los documentos restantes de COINTELPRO salieron a la luz gracias a la ley de acceso a la información (Freedom of Information Act, FOIA). La filtración hecha por la comisión dio como resultado la formación del Comité Church del Senado de Estados Unidos en 1975, el cual reprendió al FBI por realizar "actividades de inteligencia nacional que han invadido la privacidad personal y violado los derechos a la libre asamblea y a la expresión política" y, por último, canceló COINTELPRO. El Comité Church prologó su reprimenda de este modo:

> Hemos visto que algunos segmentos de nuestro gobierno, en sus actitudes y acciones, han adoptado tácticas indignas de una democracia y que en ocasiones evocan regímenes totalitarios. Hemos observado un patrón en el cual programas que se iniciaron con metas limitadas, como evitar la violencia criminal o identificar a espías extranjeros, se expandieron a lo que testigos describieron como "aspiradoras" que succionaban toda información sobre actividades legales de ciudadanos estadounidenses. La tendencia de las actividades de inteligencia a expandirse más allá de su alcance inicial es un tema que atraviesa todos los aspectos de nuestros hallazgos investigativos. Los programas de recopilación de inteligencia generan de forma natural una demanda permanentemente creciente de datos nuevos. Y una vez reunida esa inteligencia, hay fuertes presiones para usarla en contra del objetivo.

Los siguientes modos de represión fueron usados por el FBI o sus asociados como parte de COINTELPRO o contra los blancos de COINTELPRO.

1. *Violencia directa*

El asesinato de Fred Hampton mencionado anteriormente fue una operación conjunta del FBI y el Departamento de Policía de Chicago. Fred Hampton era el presidente del Partido Pantera Negra, una organización política socialista revolucionaria de finales de los años sesenta y los setenta del siglo pasado, cuyo propósito era proteger a estadounidenses negros y ofrecer programas sociales (como desayunos y clínicas de salud). El Partido Pantera Negra (BPP, por sus siglas en inglés) fue categorizado como un "grupo de odio nacionalista negro" por el FBI, para incluirlo como blanco de COINTELPRO. El asesinato de Hampton fue respaldado por otros medios de represión, incluyendo:

- *Vigilancia encubierta*. Un infiltrado pagado por el FBI proporcionó inteligencia que hizo posible la redada que condujo al asesinato de Hampton.
- *Engaño*. El mismo infiltrado creó una atmósfera de desconfianza y suspicacia en el interior del BPP gracias a que hizo *snitchjacketing* con otros miembros del partido.
- *Influencia de los medios de comunicación masiva*. Tras el asesinato de Hampton, se caracterizó a los miembros del BPP como *demonios populares*, pues las representaciones de los medios se volvieron cada vez más distorsionadas.

2. *El sistema legal*

Angela Davis, comunista, integrante del Partido Pantera Negra y blanco de COINTELPRO, fue acusada de "secuestro agravado y asesinato en primer grado" por la muerte de un juez de California que fue secuestrado y asesinado durante una melé con la policía, aunque Davis no

estaba en la escena. El estado de California sostuvo que las armas usadas por los secuestradores eran propiedad de Davis y consideró que "todas las personas relacionadas con la comisión de un crimen, ya sea que hayan cometido el acto que constituye la ofensa directamente o no, [...] son actores en cualquier crimen cometido de esta forma". No se pudo localizar a Davis en ese momento, y J. Edgar Hoover la incluyó en la lista de los "Diez fugitivos más buscados" por el FBI. Meses más tarde, Davis fue arrestada y pasó dieciséis meses en prisión a la espera de un juicio en el cual la declararon inocente.

3. *Privación del empleo*

Antes de su batalla con el sistema legal, Davis fue despedida de su trabajo como profesora de filosofía en la Universidad de California en Los Ángeles (UCLA, por sus siglas en inglés) debido a su afiliación al Partido Comunista durante su primer año de empleo, en 1969. Se consideró que era inapropiado que enseñara en el sistema de California. Su despido se dio a petición del entonces gobernador de California, Ronald Reagan, quien adujo una ley de 1949 que prohibía la contratación de comunistas en la Universidad de California. Esto pone de realce la persistencia de la época del *Temor Rojo* y el Macartismo, los cuales permearon las décadas de los cuarenta y los cincuenta del siglo pasado. El FBI promovió la demonización del comunismo a través de su programa COMINFIL (Infiltración comunista), predecesor de COINTELPRO, el cual rastreó y siguió las actividades de movimientos laborales, de justicia social y de igualdad racial.

4. *Vigilancia abierta*

En la primera tanda de documentos del FBI sobre COINTELPRO que vio la luz se encontraba un documento titulado "Notas sobre la Nueva Izquierda". Nueva Izquierda se refiere a un extenso movimiento político de los años sesenta y setenta del siglo pasado, cuyos grupos hacían campaña sobre temas sociales como los derechos civiles y políticos de las mujeres y los homosexuales y en favor del derecho al aborto. En la discusión sobre cómo enfrentar los "problemas planteados por la Nueva Izquierda", el memorando de la oficina local del FBI en Filadelfia señala que "[h]ubo un consenso bastante general de que procede hacer más entrevistas con estos sujetos y parásitos por muchas razones, la principal de las cuales es que aumentará la paranoia endémica de estos círculos y también servirá para hacerles saber que hay un *agente del FBI detrás de cada buzón*. Además, algunos resultarán abrumados por las personalidades apabullantes de los agentes que contacten y se ofrecerán a comunicarlo a todos, tal vez en forma continua".

5. *Vigilancia encubierta*

El Comité Church reportó vigilancia encubierta que "no solo era excesiva en su extensión, sino también conducida con frecuencia a través de medios ilegales o inapropiados". Es de resaltar

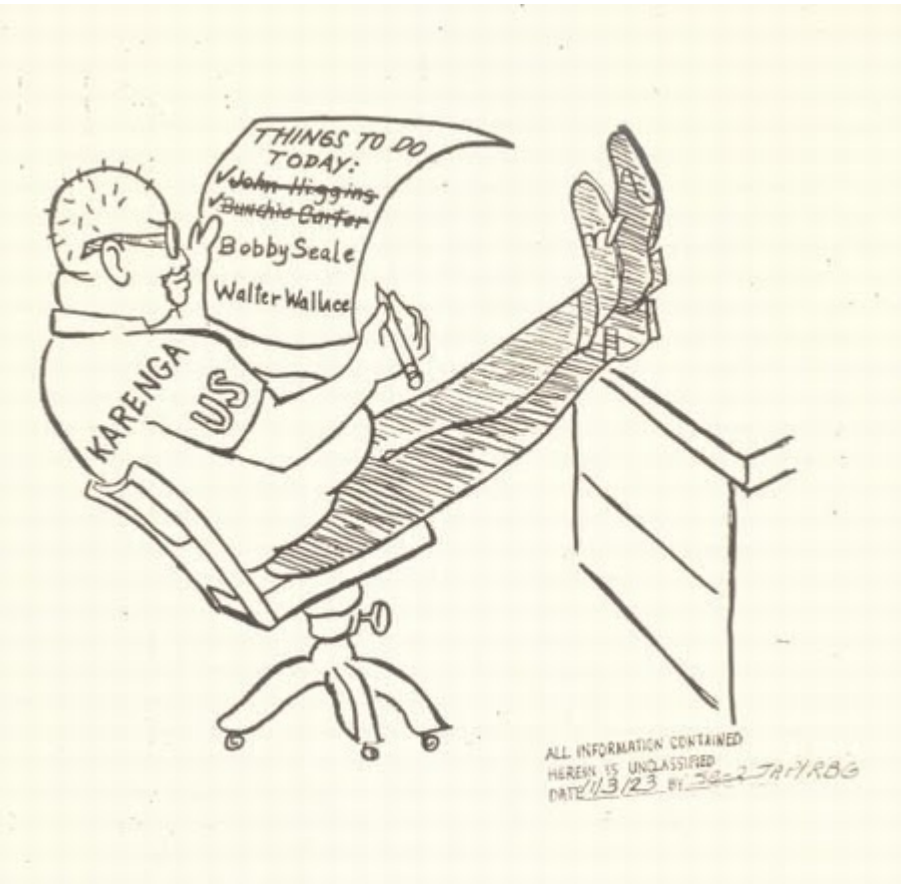
que tanto la CIA como el FBI tenían “programas para abrir correspondencia” que violaban y fotocopiaban en gran escala cartas enviadas dentro de Estados Unidos: cerca de un cuarto de millón por parte de la CIA entre 1953 y 1973 y 130,000 por parte del FBI entre 1940 y 1966. Además, tanto la CIA como el FBI mintieron al presidente Nixon sobre la continuación de dichos programas.

6. *Engaño*

Era común que el FBI enviara cartas o volantes para sembrar la discordia entre grupos afines. A continuación se muestra una caricatura hecha por operativos del FBI para falsear la imagen de participantes en movimientos e incitar a la violencia entre los grupos de nacionalismo negro Organización US (coestablecido por Maulana Karenga) y el Partido Pantera Negra, cuyos miembros más prominentes eran Huey Newton, David Hilliard, Bobby Seale, John Huggins y Bunchy Carter). La caricatura muestra a Karenga eliminando al BPP. Posteriormente, el FBI reivindicó la muerte de dos miembros del BPP a manos de tiradores del gobierno de Estados Unidos.

7. Influencia *de los medios masivos de comunicación*

La manipulación de los medios de comunicación masiva fue un principio explícito de COINTELPRO contra la Nueva Izquierda. De acuerdo con el Comité Church, “Gran parte de los esfuerzos de propaganda del FBI implicaron dar información a fuentes “amigables” de los medios, en quienes podían confiar que no revelarían los intereses del Buró. La División de Registros Criminales del Buró fue responsable de las relaciones públicas, incluyendo todos los contactos de la oficina central con los medios. En el curso de su trabajo (la mayor parte del cual no tenía que ver con COINTELPRO), la División compiló una lista de fuentes “amigables” de los medios, quienes escribieron historias en favor del Buró. Las oficinas locales también tenían “fuentes confidenciales” (informantes no pagados del Buró) en los medios, y se aseguraron de obtener su cooperación.”



Caricatura del FBI para incitar a la violencia

Qué aprender a continuación

- Amenazas digitales a movimientos sociales
- Defensa contra la vigilancia y la represión

External Resources

- Boykoff, Jules. *Beyond Bullets: The Suppression of Dissent in the United States*. AK, 2007. Oakland, CA.
- Wikipedia. "2019 Internet Blackout in Iran." 18 de diciembre de 2020.

- Shieber, Jonathan. "Zoom Admits to Shutting Down Activist Accounts at the Request of the Chinese Government." *TechCrunch*, junio de 2020.
- Duane de la Vega, Kelly, y Katie Galloway. "Eric and 'Anna.'" *Field of Vision*, 19 de noviembre de 2015.
- US Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Intelligence Activities and the Rights of Americans*. Report No. 94-755. Washington, DC: US Government Printing Office, 1976.
- Churchill, Ward, y Jim Vander Wall. *The COINTELPRO Papers: Documents from the FBI's Secret Wars against Domestic Dissent*. South End, 1990. Cambridge, MA.

Créditos

Amenazas digitales a movimientos sociales

Se recomienda leer los capítulos ¿Qué es el cifrado? y Metadatos. Después de leer la presente sección, asegúrate de leer también el capítulo Defensa contra la vigilancia y la represión.

Qué aprender a continuación

1. Qué es el modelado de amenazas
2. Quiénes están involucrados en la vigilancia y las estrategias que usan
3. Ejemplos de tácticas y programas usados en la vigilancia

Aquellos movimientos sociales que desafían a individuos, organizaciones y estructuras sociales de poder enfrentan un amplio rango de riesgos de vigilancia. Las amenazas específicas varían grandemente en su sofisticación técnica, sus probabilidades y su potencial de daño. El **modelado de amenazas** es un proceso mediante el cual una organización o individuo considera el rango de sus adversarios, estima la probabilidad de que sus datos y dispositivos sean víctimas de un ataque y, finalmente, considera el daño que sufriría si los ataques tuvieran éxito. (Y luego trabaja para proteger los datos que corren más riesgo y cuya pérdida o acceso no autorizado le provocaría el mayor daño.)

Reflexionemos sobre la vigilancia en el siguiente orden, con el objeto de discernir cómo protegerse:

- ¿Quién es tu **adversario**? ¿Es el nazi del vecindario, que quiere tomar venganza por tu anuncio en favor de Black Lives Matter? ¿Es una corporación petrolera que se opone a tu activismo contra los oleoductos? ¿Es el gobierno de Estados Unidos, que intenta evitar que hagas denuncias? Si entiendes quién es tu adversario puedes teorizar sobre sus recursos y capacidades.
- ¿Tu adversario está específicamente en contra de ti? ¿Está intentando descubrir quién eres o reuniendo información con la idea de obtener la tuya? ¿Cuál es la **estrategia de vigilancia** que utilizaría con más probabilidad? Esto te ayudará a entender el *tipo* de datos en riesgo y *dónde* podría correr riesgo tu información.
- ¿Cuáles **tácticas de vigilancia** específicas utilizará tu adversario para obtener los datos que

desea? Esto te ayudará a comprender *cómo* proteger tus datos.

Se examinan los riesgos de vigilancia en función del adversario porque resulta estratégico hacerlo. Nadie puede obtener una seguridad digital perfecta, pero sí se puede ser inteligente al decidir dónde invertir los esfuerzos para protegerse contra la vigilancia. En una discusión real en una organización o movimiento social para modelar las amenazas, definir *quiénes* son los adversarios potenciales suele ser más sencillo que identificar *cómo* llevarían a acabo sus ataques.

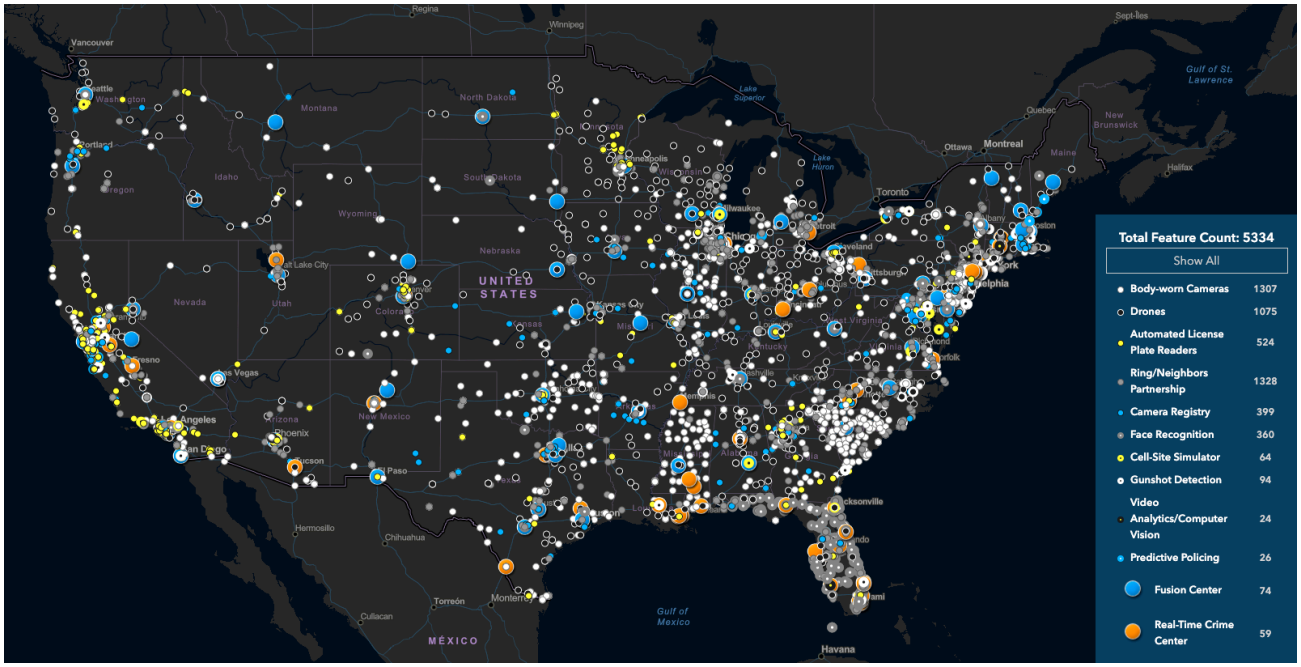
La identificación del adversario es la que informa sobre el rango de técnicas de las que este dispone (dependiendo de sus recursos y autoridad legal) y, a la vez, sobre las conductas y tecnologías de protección que la organización afectada puede usar.

Vigilancia de los adversarios

Es usual que pensemos en los adversarios en términos de los recursos que están a su alcance. Para los propósitos de esta obra, nos limitaremos a tres categorías de adversarios:

Los **Estados nación** tienen acceso a la mayoría de los recursos, de modo que puede parecer que su potencial de vigilancia es ilimitado. Aun así, es improbable que puedan romper cifrados sólidos. Aquí, pensamos en la Agencia de Seguridad Nacional (NSA) como la entidad con acceso al arsenal de vigilancia más sofisticado. Las revelaciones de Edward Snowden en 2013 brindan la ventana más completa sobre las posibilidades de vigilancia en el nivel de los Estados nación y están disponibles en el Snowden Surveillance Archive.

Las **grandes corporaciones** y los **cuerpos policiales locales** suelen contar con abundantes recursos y comparten información entre ellos, aunque no necesariamente tienen acceso a los recursos de los Estados nación. Sin embargo, el uso de la tecnología en la práctica de la vigilancia es generalizado en las agencias policiales de Estados Unidos, como se ilustra en esta impresión de pantalla del Atlas de Vigilancia de la Electronic Frontier Foundation.



Atlas de las tecnologías de vigilancia policial

Los individuos son quienes cuentan con menos recursos, aunque podrían conocerte personalmente y, por tanto, podrían usar técnicas de ingeniería social con mayor eficacia para obtener tus datos.

Observa que las técnicas disponibles para adversarios con pocos recursos también están disponibles para los que tienen muchos recursos. Por ejemplo, las grandes corporaciones y los cuerpos policiales emplean informantes e infiltrados, que pueden ser individuos que conoces personalmente.

Asimismo, aunque las herramientas de vigilancia más sofisticada no suelen estar disponibles para los adversarios con menos recursos, este no es siempre el caso: los departamentos de policía de las grandes ciudades podrían tener acceso a los recursos de nivel nacional (por ejemplo, gracias al intercambio de datos facilitado por centros de fusión) y un vecino nazi particularmente avezado podría tener destrezas avanzadas de piratería informática que le permitirían efectuar ataques de nivel corporativo.

De este modo, aunque estas categorías no tienen límites claros, pueden ser un punto de partida para comprender los riesgos y centrarse así en las estrategias *más probables* de tus adversarios, así como en tus puntos débiles *más probables*.

Estrategias de vigilancia

Existen dos estrategias generales de vigilancia: en masa y dirigida.

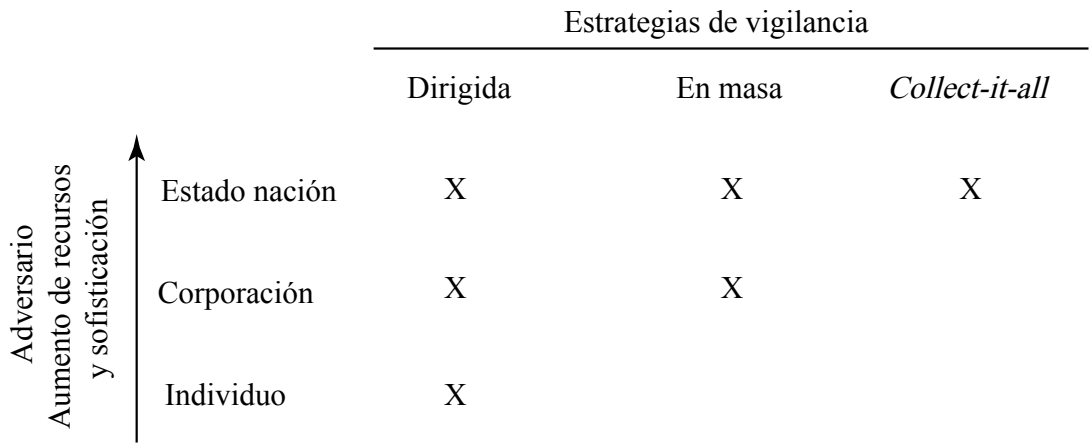
La **vigilancia en masa** recaba información sobre poblaciones enteras. Esto puede hacerse con el propósito de comprender mejor a una población; por ejemplo, reunir y analizar datos relacionados con la salud puede ayudar a identificar y vigilar brotes de enfermedades. La vigilancia en masa también puede usarse como estrategia para identificar a individuos de interés dentro de la población vigilada; por ejemplo, se puede usar el video transmitido por cámaras de seguridad para identificar a personas involucradas en daños a la propiedad. Este tipo de vigilancia también puede brindar información sobre individuos específicos; por ejemplo, la información obtenida mediante el despliegue masivo de cámaras para vigilar placas de vehículos puede usarse para rastrear los movimientos de una persona específica.

La **vigilancia dirigida** solo reúne información sobre un individuo o un grupo pequeño de individuos; por ejemplo, interceptando las comunicaciones de un individuo en particular. La vigilancia dirigida supone la existencia de sospechas previas y *es posible* que pueda ser controlada: por ejemplo, la policía debería obtener una orden judicial con base en causa probable antes de interceptar los correos de alguien.

Históricamente, había una división clara entre la vigilancia dirigida y la vigilancia en masa. Sin embargo, en la era digital se pueden desplegar muchas tácticas de vigilancia dirigida a escala masiva, como se discutirá más adelante. Además de esta división clásica de las estrategias de vigilancia, abordaremos una estrategia mayor única de la era digital.

Collect-it-all (Recábalo todo) puede verse simplemente como vigilancia en masa con esteroides, aunque va mucho más allá de lo que históricamente podría haberse considerado como vigilancia en masa. En tanto que la vigilancia en masa puede incluir cosas como cámaras de seguridad, la vigilancia de transacciones bancarias y el escaneo de correos electrónicos, *collect-it-all* pretende absorber toda información digitalizada. *Collect-it-all* va incluso más allá: digitaliza y reúne toda la información que no está en línea o no está disponible (por ejemplo, video de cámaras de circuito cerrado). El general Keith Alexander, exdirector de la NSA y a quien se atribuye el concepto de *collect-it-all,* desarrolló estrategias de vigilancia en masa tras los eventos 9/11 y de Irak, las cuales se han descrito así: "En lugar de buscar una aguja en un pajar, su enfoque fue 'recaben todo el pajar, reúnanlo, clasifíquenlo y guárdenlo… y, sea lo que sea que desees, solo ve y búscalo.'" Es probable que esta sea la inspiración de muchos programas de la NSA revelados por Edward Snowden, los cuales señalamos a continuación.

Distintos adversarios despliegan distintas estrategias de vigilancia o, mejor dicho, los adversarios con menos recursos suelen estar más limitados en estrategias, como se ilustra aquí:



Adversarios y sus estrategias de vigilancia

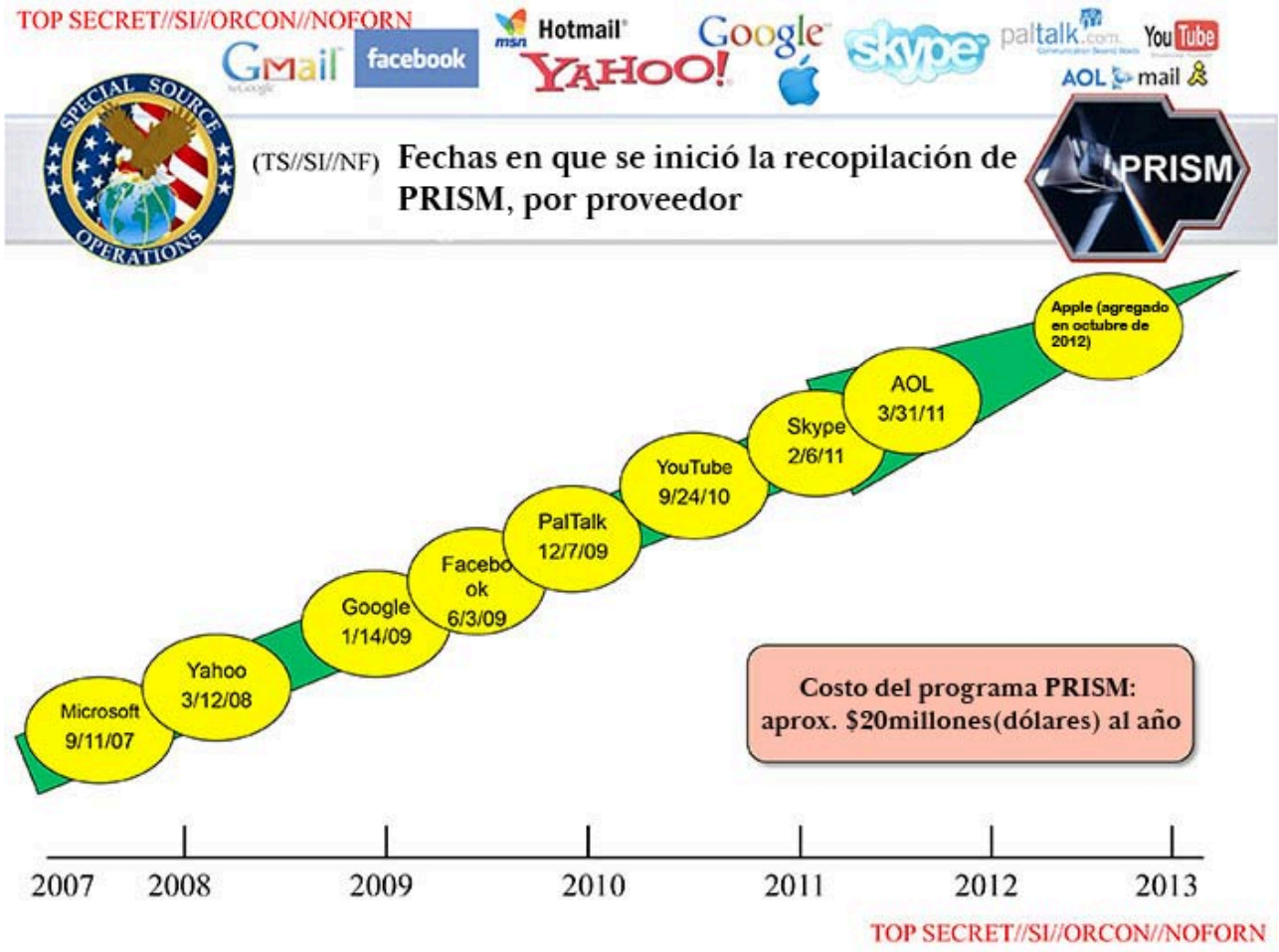
Tácticas de vigilancia

Una revisión de todas las tácticas de vigilancia disponibles para los adversarios de todos los niveles llenaría una enciclopedia. Aquí se ilustran solo algunos ejemplos de programas y tácticas de vigilancia que respaldan las estrategias mencionadas. Luego, se ilustran estos programas de acuerdo con el nivel mínimo de sofisticación requerido para usar la táctica, así como la cantidad de personas cuya información sería recabada con ella.

Interceptar y reunir datos en masa

Comenzaremos con lo que probablemente la mayoría pensaría al considerar la vigilancia en masa: la interceptación y posible almacenamiento de una vasta cantidad de comunicaciones. Muchos programas de interceptación en masa quedaron al descubierto como parte de las revelaciones de Edward Snowden en 2013. **STORMBREW**, **FAIRVIEW** y **BLARNEY** son tres programas a través de los cuales la NSA reúne información en tránsito en asociación con compañías de telecomunicaciones y obtiene acceso a datos que atraviesan cables de datos submarinos. Esto les permite recabar cualquier contenido sin cifrar y todos los metadatos asociados, en su tránsito del punto de origen al punto de destino. Sin embargo, estos programas no pueden ver contenido cifrado en tránsito, como correos o archivos almacenados en la nube. El programa **PRISM** es una asociación de la NSA con diversas compañías de internet (como Google, Microsoft y Facebook, como se ilustra a continuación) para otorgar acceso a la NSA a datos contenidos albergados en servidores de esas compañías.

Es decir, si la información está cifrada en tránsito y, por tanto, no puede recabarse a través de STORMBREW, FAIRVIEW y BLARNEY, entonces la NSA puede obtenerla por medio de PRISM, a menos que la información esté cifrada en los servidores de la compañía de internet involucrada con una clave controlada por el usuario.



Recopilación de PRISM, Agencia de Seguridad Nacional

Agregación y análisis de datos

Una vez que se cuenta con una enorme cantidad de datos obtenidos por vigilancia, ¿qué hacer con ellos? ¡De seguro el hombre no podrá encontrar mi minúscula aguja en todo ese pajar! Aquí es donde entra la minería de datos, desde búsquedas básicas (¡espeluznante!) hasta modelos predictivos de aprendizaje automatizado, la cual pone a disposición de adversarios poderosos grandes cantidades de datos obtenidos mediante vigilancia (a través de fuentes diversas).

La función más básica de la minería de datos es la posibilidad de hacer búsquedas; es decir, dada una gran cantidad de datos, la capacidad de recabar un dato de interés, como aquel relacionado con una persona en particular. **XKEYSCORE** funciona como una búsqueda de Google

en los datos de la NSA almacenados en masa. Aunque la función es básica, la increíble cantidad de información a la que tiene acceso (incluyendo la de los programas de la NSA mencionados antes) hace de XKEYSCORE (y de cualquier programa relacionado) un recurso solo accesible a los adversarios más poderosos.

Por otro lado, **Dataminr** busca información disponible públicamente (como publicaciones en redes sociales) para revelar y brindar detalles acerca de crisis emergentes (como en las actualizaciones de información sobre COVID-19 y las protestas por el asesinato de George Floyd) que pone a disposición de sus clientes, entre los cuales están salas de prensa, departamentos de policía y gobiernos, a través de medios automatizados (software) y manuales (análisis humano).

Dataminr y otras plataformas de monitoreo de redes sociales, de las cuales hay docenas sino es que cientos, han estado bajo ataque por su vigilancia de discurso protegido por la Primera Enmienda, en especial del denominado Movement for Black Lives. En varios casos, Twitter y Facebook han bloqueado el fácil acceso a sus datos de compañías de monitoreo de redes sociales, tras reclamos públicos por su mal uso.

Más allá de esto se encuentra **Palantir**, una de muchas plataformas de vigilancia policial, que supuestamente predice dónde es necesaria la presencia policial: una intersección en una calle, un vecindario o un individuo. En realidad, estas plataformas logran poco, pero refuerzan reglas racistas. Las plataformas de vigilancia policial predictiva usan datos actuales como punto de partida y tienden a enviar a la policía a lugares donde ha estado antes. Dado que las comunidades de color y los vecindarios empobrecidos tienen ya una presencia notable de policía, los modelos predictivos simplemente envían a la policía de nuevo a dichos lugares, sin importar que ahí se estén cometiendo o no crímenes en ese momento.

Incluso más allá se encuentra **EMBERS** (Reconocimiento temprano de eventos basado en modelos usando sustitutos, por sus siglas en inglés). Se ha usado desde 2012 para predecir "disturbios civiles como protestas, huelgas y eventos de 'ocupación'" en "múltiples regiones del mundo" mediante la "detección de actividades de organización en curso y la generación de advertencias en consecuencia". Las advertencias son completamente automáticas y pueden predecir "el cuándo de la protesta, así como el dónde (hasta un nivel de detalle de la ciudad)", con un promedio de 9.76 días de anticipación. Depende completamente de datos disponibles públicamente, como publicaciones en redes sociales, noticias, precios de alimentos y tasas de cambio.

Recabado dirigido de datos

Otra táctica de vigilancia que viene a la mente es la intervención telefónica. Su equivalente moderno es mucho más fácil de instalar que en un cable físico de comunicaciones. Una de las versiones modernas es el *simulador de sitios celulares* (**CSS**, por sus siglas en inglés), una torre celular en miniatura (suficientemente pequeña para montarse sobre una camioneta). Esta torre brindará la mejor señal celular a los teléfonos de un área, así que estos se conectarán a ella. En

el nivel más básico, un CSS revelará las identidades de los teléfonos en el área. (Imagina su uso en el lugar de una protesta.) Diferentes dispositivos CSS tienen diferentes potenciales. Algunos tan solo transmiten las comunicaciones desde y hasta la red celular más amplia, al tiempo que obtienen los metadatos. Otros dispositivos CSS pueden degradar el servicio; por ejemplo, de 3G a GSM, lo cual elimina el cifrado en tránsito de las comunicaciones celulares del proveedor de servicios y brinda acceso al contenido de los mensajes. En otros casos, los CSS pueden bloquear las comunicaciones celulares cuando los teléfonos se conectan a ellos, no pasando la información a la red celular. Es común que las organizaciones policiales cuenten con dispositivos CSS (como se ilustra en el mapa al inicio de este capítulo).

También se puede montar equipo de vigilancia (incluyendo CSSs y video de alta resolución) en *drones* de vigilancia o en vehículos aéreos no tripulados (**UAV**, por sus siglas en inglés), lo cual aumenta en forma significativa el alcance de la vigilancia, de unas cuantas cuadras a toda una ciudad. Este es un ejemplo en el cual tácticas de vigilancia dirigida se extienden a un nivel en masa. Los sistemas de vigilancia persistente han facilitado que muchos departamentos de policía en EUA usen UAVs. Los UAV con tecnología de vigilancia persistente usan cámaras de resolución extremadamente alta que cubren más de 32 millas cuadradas para poder rastrear los movimientos de autos y personas. También almacenan un historial de manera que se pueda rastrear movimientos hacia atrás en el tiempo.

Por supuesto, es poco frecuente que sea necesario recabar información de forma encubierta. Algunas veces basta con solicitarla con cortesía. En Estados Unidos se usan citatorios y órdenes judiciales para solicitar información a proveedores corporativos. Mientras que para obtener una orden judicial es necesario tener una causa probable (en el sentido legal), no lo es para obtener un citatorio. Como lo señala en su informe de transparencia, Google recibe cerca de 40 mil solicitudes de información al año, aproximadamente un tercio de ellas mediante citatorio judicial. Google entrega información en cerca de 80 por ciento de los casos y, en promedio, cada solicitud afecta a dos cuentas de usuarios (es decir, cada solicitud es bastante dirigida). Es digno de mención que el contenido de los correos electrónicos se puede obtener mediante un citatorio judicial. Aunque es sencillo solicitar citatorios y órdenes judiciales, en general, solo los adversarios gubernamentales pueden acceder a ellos.

Ataque a dispositivos

Las tácticas anteriores están encaminadas a recabar información durante su tránsito o cuando está en la nube. Sin embargo, tu dispositivo (teléfono o computadora) es un destino final de donde es posible extraer datos directamente. Esto puede ocurrir si la policía confisca tu dispositivo durante una detención o cateo. En el capítulo Proteger tus dispositivos se discute esto con más detalle, pero aquí se destacan algunas tácticas para extraer datos de estos dispositivos.

Cellebrite es una compañía israelí especializada en herramientas para la extracción de datos de teléfonos y otros dispositivos, como el *Universal Forensic Extraction Device* (**UFED**), que es suficientemente pequeño para llevarlo en un portafolio y puede extraer datos rápidamente de

casi cualquier teléfono. Sin embargo, para ello se requiere el control físico del teléfono. NSO Group (otra compañía israelí) vende la posibilidad de instalar en forma remota el software espía (*spyware*) **Pegasus** en teléfonos iPhone y Android. Este software permite extraer mensajes de texto, metadatos de llamadas y contraseñas, entre otros datos. La NSA cuenta con una familia de software malicioso (*malware*) conocida como **QUANTUM**, que permite recabar datos o evitar que lleguen al dispositivo destinatario. La NSA tiene los medios para instalar este malware en masa, a través de su sistema **TURBINE**, el cual puede disfrazar los servidores de la NSA como, por ejemplo, servidores de Facebook para inyectar malware en el dispositivo deseado.

Aunque Pegasus y QUANTUM pueden desplegarse ampliamente, hacerlo puede ser peligroso en términos políticos ya que las protestas públicas suelen seguir al descubrimiento de su uso. Entre más amplia e invasiva es la tecnología de vigilancia empleada, más probable es que se descubra, como ocurrió en el caso de Pegasus.

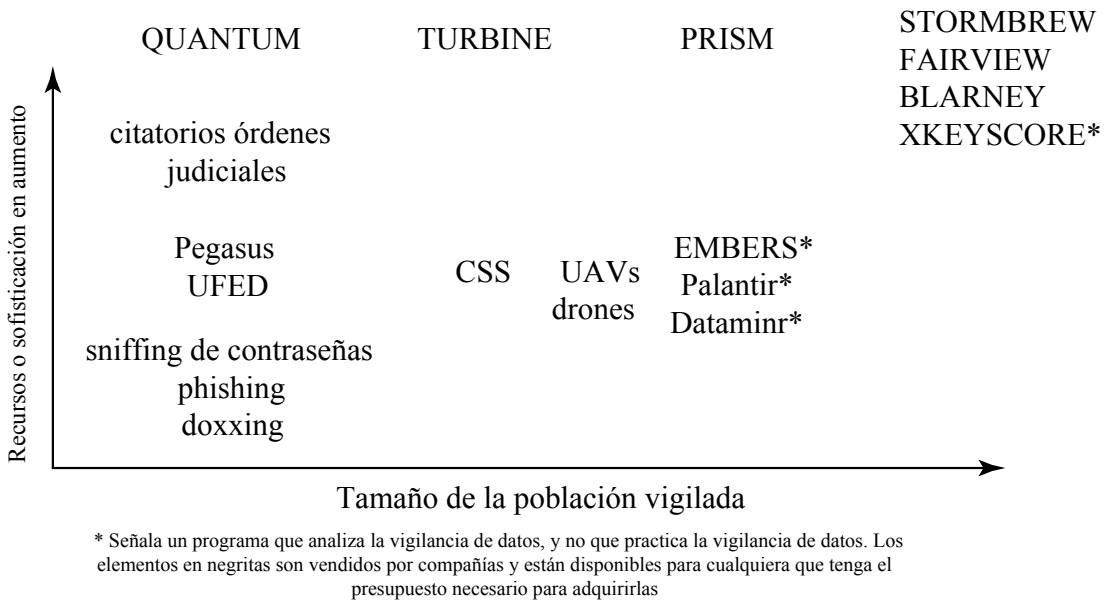
Acoso personalizado

Aunque se encuentra fuera del ámbito de la vigilancia típica, debe tenerse en mente el acoso personalizado al considerar los riesgos para la seguridad digital. *Doxxing*, *phishing* y *sniffing* de contraseñas son técnicas disponibles para un adversario con pocos recursos, pero no deberían ignorarse por esa razón. Tal vez quieras repasar la historia del activista de Black Lives Matter, DeRay Mckesson, del capítulo Contraseñas, cuya cuenta de Twitter resultó comprometida a pesar de que usaba autenticación de dos factores. Lo único que su adversario necesitó fue acceso a cierta información personal, la cual podría estar disponible en fuentes públicas o por conocimiento personal.

Doxxing es el proceso de publicar (por ejemplo, en un sitio de discusión) la información personal de un blanco, lo cual causaría daño o vergüenza pública al individuo afectado. Aunque es muy fácil hacer esto, también es muy difícil protegerse: una vez que hay información disponible sobre ti en línea, es complicado o imposible eliminarla.

Phishing es una táctica que incluye métodos para obtener información personal, como contraseñas, a través de correos electrónicos y sitios tramposos. Mientras que el phishing puede practicarse en gran escala, su modalidad más exitosa (*spear phishing*) afecta a individuos usando información ya conocida para mejorar su probabilidad de éxito.

Sniffing de contraseñas es algo que puede requerir tan poca tecnología como simplemente observar de reojo para ver la contraseña que tecleas o puede involucrar un registrador de tecleo (*keylogger*) para grabar la contraseña conforme la tecleas, aunque esto requiere instalarlo en tu dispositivo, para lo cual hay métodos de diferentes niveles de sofisticación. La forma tradicional captura una contraseña a medida que pasa por la red, lo cual es posible si el tráfico no está cifrado; nuevamente, este método posee distintos niveles de sofisticación, pero sin duda un individuo con destreza podría ponerlo en práctica.



Tácticas de vigilancia

En contexto: Standing Rock

En 2016, opositores a la construcción del Oleoducto para Acceso a las Dakotas (DAPL, por sus siglas en inglés) organizaron un campamento de protesta en la confluencia de los ríos Missouri y Cannonball, área bajo la cual estaba planeado que pasara el oleoducto. El oleoducto amenazaba la calidad del agua potable en el área, habitada por muchas comunidades de nativos americanos y que incluye la Reserva India Standing Rock. Eventualmente, el campamento de protesta albergó a miles de personas y permaneció durante diez meses.

Energy Transfer Partners, la compañía constructora del DAPL, emplea fuerzas de seguridad privada, las cuales, a pocos meses del levantamiento del campamento de protesta, lanzaron perros de ataque contra los manifestantes. Además de esto, Energy Transfer Partners contrató a TigerSwan para ayudar en la represión del movimiento de protesta. TigerSwan es una compañía privada de mercenarios que tuvo su inicio en Afganistán como contratista del gobierno estadounidense durante la guerra de terror. TigerSwan utiliza tácticas de contraterrorismo militar y se refirió a los manifestantes nativos americanos y a otros que los apoyaban como insurgentes; los comparó (en forma explícita) con los combatientes yihadistas contra quienes TigerSwan tuvo su debut. La vigilancia de TigerSwan incluye monitoreo de redes sociales, grabación de video aéreo, espionaje por radio, infiltrados e informantes.

A la postre, fueron convocadas fuerzas policiales de los niveles local, regional y federal. TigerSwan entregaba reportes de la situación a los cuerpos policiales estatales y locales y estaba en comunicación constante con el FBI, el Departamento de Seguridad Nacional, el Departamento

de Justicia, el Cuerpo de Alguaciles y la Oficina de Asuntos Indígenas. Aunque sería ilegal que los cuerpos policiales gubernamentales aplicaran las tácticas empleadas por TigerSwan (aunque no todas), el Estado puede darle la vuelta a esto recibiendo información a través de compañías privadas. Esta es una práctica común en muchos cuerpos policiales: los departamentos de policía compran información recabada por entes privados que, de ser obtenida por el Estado, violaría la Cuarta Enmienda.

La alianza pública-privada entre cuerpos policiales del gobierno, Energy Transfer Partners y TigerSwan fue determinante para poner fin al campamento de protesta. Eventualmente, el Estado expulsaría violentamente a los manifestantes con gas lacrimógeno, granadas aturdidoras y carros lanza-agua (en un clima con temperaturas bajo cero), lo que dio como resultado cerca de 300 manifestantes heridos (incluyendo una mujer que por poco pierde un brazo).

Aunque el campamento concluyó y el oleoducto se construyó, la oposición continua llevó finalmente a un fallo de la corte en virtud del cual el oleoducto debía cerrarse y vaciarse de petróleo para completar una nueva revisión de su impacto ambiental.

Es importante recordar que, aunque la vigilancia en masa reúne información sobre casi todos, el daño que causa presenta variaciones. Se vigila en mayor grado a ciertos grupos, o bien, se usa en forma desproporcionada la información de ciertos grupos. Algunos ejemplos de grupos en Estados Unidos que sufren un daño desproporcionado por la vigilancia del Estado y corporativa son los musulmanes estadounidenses, los negros y afroamericanos, los nativos americanos y los participantes en movimientos sociales, como discutimos en el capítulo Mecanismos de represión de movimientos sociales.

Qué aprender a continuación

Te invitamos a que, después de este funesto recuento de las formas en que es posible obtener tus datos, comiences a leer inmediatamente el capítulo Defensa contra la vigilancia y la represión.

Recursos externos

- Electronic Frontier Foundation. "Atlas of Surveillance." Consultado el 9 de febrero de 2021.
- Department of Homeland Security. "Fusion Centers." Consultado el 9 de febrero de 2021.
- Google. "Transparency Report." Consultado el 9 de febrero de 2021.
- Nakashima, Ellen, y Joby Warrick. "For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All.'" Washington Post, 14 de julio de 2013.

- Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Londres: Hamish Hamilton, 2015.
- N, Yomna. "Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks." *Electronic Frontier Foundation*, 28 de junio de 2019.
- Stanley, Jay. "ACLU Lawsuit over Baltimore Spy Planes Sets Up Historic Surveillance Battle." *American Civil Liberties Union*, 9 de abril de 2020.
- Biddle, Sam. "Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr." *Intercept*, 9 de julio de 2020.
- Ahmed, Maha. "Aided by Palantir, the LAPD Uses Predictive Policing to Monitor Specific People and Neighborhoods." *Intercept*, 11 de mayo de 2018.
- Muthiah, Sathappan, Anil Vullikanti, Achla Marathe, Kristen Summers, Graham Katz, Andy Doyle, Jaime Arredondo, et al. "EMBERS at 4 Years: Experiences Operating an Open Source Indicators Forecasting System." En *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining—KDD '16*, 205–14. San Francisco: ACM, 2016.
- Boot, Max. "Opinion: An Israeli Tech Firm Is Selling Spy Software to Dictators, Betraying the Country's Ideals." Washington Post, 5 de diciembre de 2018.
- *Intercept*. "Oil and Water." 2016–17.
- Fortin, Jacey, y Lisa Friedman. "Dakota Access Pipeline to Shut Down Pending Review, Federal Judge Rules." *New York Times*, 6 de julio de 2020.

Créditos

PARTE 3: DEFENSA DE LOS MOVIMIENTOS SOCIALES (EN EUA)

Defensa contra la vigilancia y represión

Se recomienda leer los capítulos Mecanismos de represión de movimientos sociales y Amenazas digitales a movimientos sociales antes de seguir con este.

Lo que aprenderás

1. Qué es el modelado de amenazas
2. Estrategias para reducir amenazas a tu seguridad digital

Tal vez hayas escuchado que no existe la seguridad digital perfecta, y estamos de acuerdo. El potencial de vigilancia de un adversario con suficientes recursos es ilimitado y las posibilidades descritas en el capítulo Amenazas digitales a movimientos sociales apenas rascan la superficie. Sin embargo, no todos los riesgos son iguales; no es igualmente probable que se use una u otra herramienta de vigilancia y hay muchas cosas que una persona o un grupo puede hacer para reducir las amenazas debidas a la vigilancia.

Podemos modelar una amenaza digital a la seguridad en términos de la siguiente relación:

$$\text{amenaza} \propto \frac{(\text{potencial de vigilancia}) \times (\text{riesgo de represión})}{\text{esfuerzo necesario para obtener datos}}$$

En este modelo, el **potencial de vigilancia** se refiere al nivel de recursos de tu adversario, como se discute en el capítulo Amenazas digitales a movimientos sociales. El **riesgo de represión** se refiere a las formas en las que tu adversario podría tratar de debilitarte, como se describe en el capítulo Mecanismos de represión de movimientos sociales.

Es importante tener en mente que la vigilancia apoya a la represión directa e indirectamente. Muchos de los ejemplos presentados en el capítulo Mecanismos de represión de movimientos sociales tuvieron como sustrato, de hecho, mecanismos de vigilancia:

- La **violencia directa** infligida al líder del Partido Pantera Negra, Fred Hampton, quien fue asesinado, tuvo el respaldo del conocimiento detallado de su horario y de la distribución de su departamento.
- El Departamento de Justicia de Estados Unidos emitió amenazas de sanciones a través del **sistema legal** en contra de los organizadores de las protestas contra la investidura de Donald Trump. Para ello, solicitaron toda la información del tráfico web de la página de una organización (esto se describe al final del capítulo Enrutado anónimo).
- La **privación del empleo** de la que fue objeto Steven Salaita fue resultado de la vigilancia de la actividad de su cuenta de Twitter.
- El **engaño** con el cual actuó el FBI en contra de Mohamed Mohamud se inició con la vigilancia de su correo electrónico.

Reducir la amenaza

Es posible disminuir el riesgo representado por amenazas digitales *disminuyendo* el potencial de vigilancia o el riesgo de represión, o bien, *aumentando* el esfuerzo requerido para obtener nuestros datos.

Reducir el potencial de vigilancia

La mayoría de los activistas tienen poco control inmediato sobre el potencial de vigilancia. Sin embargo, ha habido numerosos esfuerzos loables para regular la vigilancia, con cierto grado de éxito, como la prohibición del reconocimiento facial y del uso de CSSs en ciertas jurisdicciones. Pero, a menos que tu trabajo en un movimiento social esté orientado a la prohibición o limitación de la vigilancia, este camino te alejaría de tus metas.

Reducir el riesgo de represión

Asimismo, los activistas tienen poco control sobre el riesgo de represión. Podrías minimizar este riesgo si redujeras la amenaza que representas para tu adversario, pero esto sería sucumbir al *efecto inhibidor*.

Aumentar el esfuerzo requerido para obtener tus datos

Lo anterior nos deja con aumentar el esfuerzo requerido para obtener nuestros datos, lo que constituye el objeto del resto de este libro. Aunque es importante proteger todos los datos (entre más conozca de ti tu adversario, más podrá debilitarte), te invitamos a dirigir cualquier esfuerzo

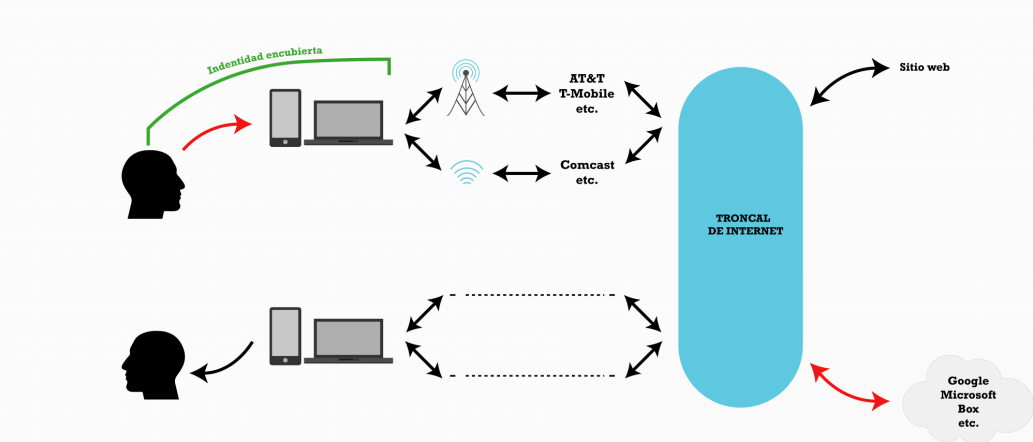
adicional para protegerlos hacia las estrategias que más protección brindan. Así, para *guiar* dicho esfuerzo debes tener en mente el potencial de vigilancia de tus adversarios y las formas en que sería más probable que repriman tus esfuerzos. Con este fin, es recomendable que te centres en proteger datos que

1. es más probable que sean usados para reprimir tus esfuerzos, y
2. sean más vulnerables a la vigilancia.

Será posible entender el inciso 1 a través de una profunda comprensión de los esfuerzos y los adversarios de un movimiento social. Para analizar el inciso 2 es necesario entender dónde están tus datos (se describe a continuación) y cómo protegerlos (lo cual se discutirá en los capítulos restantes de este libro).

¿Dónde están tus datos?

Se pueden adoptar distintas estrategias de protección dependiendo de dónde resida la vulnerabilidad de los datos. Tu información se convierte en datos cuando se pone en un dispositivo (por ejemplo, un teléfono celular o laptop) y luego puede transmitirse por internet, a través de proveedores de servicios. Aquí se distingue entre sitios web donde solo navegas y proveedores de nube donde tus datos pueden almacenarse (desde Google hasta Facebook).



Dónde se encuentran tus datos

En los capítulos restantes se discute cómo proteger la ubicación de tus datos. En el capítulo Cultura de seguridad se discute cómo decidir si convertir tu información en datos (cuando tú tienes control sobre ella) y si almacenar tus datos en la red; es decir, si deseas que tus datos se transmitan por las flechas de la red. En el capítulo Proteger tus dispositivos se analiza cómo proteger datos almacenados en dispositivos bajo tu control (por ejemplo, tu laptop y teléfono celular). En el capítulo Proteger tus comunicaciones se discute cómo proteger tus datos mientras se transmiten desde ti hasta su destino, ya sea un sitio web, un proveedor de nube o una persona.

En el capítulo Proteger tus datos remotos se analiza cómo proteger datos almacenados en la nube, si es que tú tomaste la decisión de hacerlo. Luego, en el capítulo Proteger tu identidad se analiza cómo proteger tu identidad; es decir, cómo ser anónimo o usar un seudónimo en línea y cómo abrirse camino entre la censura. Finalmente, en la conclusión se discute cómo seleccionar herramientas de seguridad digital y se presentan los principios que usamos para nuestras recomendaciones.

En contexto: Edward Snowden

En los años previos a 2013, Edward Snowden reunió datos en sus lugares de trabajo (principalmente, subcontratistas de la NSA) a los que tuvo acceso en su función de administrador de sistemas. Las filtraciones de Snowden de enormes cantidades de material clasificado ilustraron cuán avanzadas y ampliamente usadas eran las tácticas de vigilancia de muchos de los gobiernos más poderosos del mundo. Sin embargo, para hacer estas revelaciones, Snowden se enfrentó a un adversario poderoso: la misma Agencia de Seguridad Nacional.

Era improbable que Snowden consiguiera un anonimato duradero; su propósito era mantener su conducta (recabar información) y su meta (denunciar) ocultas por tiempo suficiente para revelar la información a periodistas, quienes la reportarían de forma responsable, y, con suerte, por tiempo suficiente para poder llegar a un lugar seguro, donde pudiera vivir en libertad. Tomó meses para que Snowden lograra establecer un canal de comunicación cifrado con Glenn Greenwald (un periodista conocido por sus valientes y profundos reportajes), pese a que esto ocurrió en la época del *plug-and-play* (conectar y usar) y de las apps de mensajería cifrada de extremo a extremo. Pero una vez que comenzaron los reportajes de las revelaciones de Snowden, supo que su identidad sería descubierta y él mismo la hizo pública. Snowden no terminó donde había esperado (América Latina). Su pasaporte estadounidense fue cancelado durante su vuelo desde Hong Kong (donde hizo sus filtraciones a Glenn Greenwald) a Rusia, lo que le impidió futuros vuelos. Snowden pidió asilo en Rusia.

Sin embargo, Snowden tuvo éxito como denunciante; los reportes duraron años y hubo numerosos cambios a nuestras comunicaciones. En la actualidad, el cifrado se encuentra ampliamente disponible; tanto así, que muchas personas no saben cuándo sus conversaciones están cifradas de extremo a extremo.

Qué aprender a continuación

- Cultura de seguridad

Recursos externos

- AnarchoTechNYC. "Persona Based Training Matrix." 9 de junio de 2020.
- Electronic Frontier Foundation. "Your Security Plan." *Surveillance Self-Defense*, 1 de agosto de 2014.
- Snowden, Edward J. Permanent Record, 2019. Metropolitan Books.

Créditos

Cultura de seguridad

Se recomienda leer el capítulo Defensa contra la vigilancia y la represión antes de seguir con este.

Lo que aprenderás

1. Qué es la cultura de seguridad para movimientos sociales
2. Por qué la cultura de seguridad es esencial para la seguridad digital

Los movimientos sociales, conscientes de la historia de represión contra informantes por parte del Estado y adversarios privados, han desarrollado lo que se conoce como *cultura de seguridad*. Este término se refiere a acuerdos para compartir información y a otras prácticas de los grupos para minimizar los efectos negativos de la infiltración, la vigilancia y otras amenazas de represión hacia su trabajo, sus miembros y los movimientos sociales en términos más amplios; es decir, *seguridad* en este contexto se refiere a algo mucho más amplio que la seguridad digital. El término *cultura* implica aspirar a principios de seguridad y prácticas para volverse reflexivo e intuitivo. Una cultura de seguridad ideal ayuda a un grupo a comunicarse en forma fácil y segura y a incorporar nuevos miembros (si se desea), al tiempo que evita una paranoia excesiva o gravosos procedimientos y políticas.

Aunque las perspectivas y prácticas de cultura de seguridad varían ampliamente, algunos principios generales a los que deberías apegarte son los siguientes:

1. Comparte solo la información estrictamente necesaria
2. Si te has organizado con otros, conoce a los miembros de tu grupo lo mejor posible
3. Evita chismes y rumores

La cultura de seguridad confluye con la seguridad digital

Exploremos algunos de estos elementos en detalle y cómo se relacionan con la seguridad digital.

Lo estrictamente necesario: minimizar la información que se comparte y digitaliza

El primer principio para guardar secretos es minimizar la cantidad de personas a quienes se les confían. Es cierto que existe un espectro de sensibilidad de la información: desde anuncios públicos hasta reuniones abiertas; desde comunicados de prensa en proceso hasta lugares y horarios específicos de acciones concretas. Decidir qué información es necesario proteger y tener el cuidado de hacerlo es solo parte del panorama; las personas también necesitan aceptar que no tendrán acceso a información sensible a menos que la requieran para hacer su trabajo.

Desde una perspectiva de seguridad digital, esto también implica decidir qué información digitalizar. (¿En verdad necesitas un documento en Google que enumere a todas las personas que planean asistir a una protesta? ¿De verdad es necesario publicar fotografías identificables de los asistentes? ¿Es necesario que esas publicaciones sean públicas y con geolocalización?) Limitar la cantidad de información y la extensión con que se comparte va de la mano con buenas prácticas de seguridad digital, porque no existe plataforma o medio de comunicación que pueda considerarse perfectamente seguro.

Antes de adoptar medidas específicas de seguridad digital (como usar tecnología complicada de cifrado de extremo a extremo), considera qué información debe almacenarse, compartirse o, incluso, existir en formato digital. Tal vez (de no ser por la pandemia actual) deberíamos reunirnos y discutir ideas en persona tanto como sea posible. Ten en mente que es muy fácil copiar cualquier información digital, así que cualquier cifrado, por robusto que sea, solo puede proteger la información en el mismo grado en que se pueda confiar en cada persona con acceso a ella. Ni siquiera una app o plataforma digital con un diseño perfectamente seguro puede evitar que la información resulte comprometida por un infiltrado o traidor dentro de un grupo.

Conociéndose: aprobar y construir confianza

Familiarízate con las personas con quienes trabajas, de manera que puedas confiar en ellas sin importar cuáles sean los riesgos que decidan afrontar juntos. Pero cuando decides digitalizar información, estás potencialmente admitiendo a más “personas” (corporaciones y el Estado) en el círculo de tu organización. Si tu grupo usa, por ejemplo, Gmail para comunicaciones entre los miembros, entonces Google también tiene todos esos correos, los cuales pueden ser sujeto de una orden judicial por parte del Estado para su entrega. Así que debes asumir que cualquier entidad podría tener acceso a tus datos *no cifrados*, ya sea una persona con quien interactúes o tus proveedores de servicios de internet, de almacenamiento en la nube o de correo electrónico.

No transmitas o difundas rumores

Movimientos sociales del pasado han sido aplastados por chismes y rumores, que el Estado ha usado para su ventaja, aprovechando nuestras debilidades humanas, como se discute en el capítulo Mecanismos de represión de movimientos sociales: la práctica de *snitchjacketing*, el uso de agentes provocadores y de publicidad falsa como tácticas para engañar, dependen de que los participantes confíen en la fuente de dichos engaños y repitan la información.

Para tener seguridad digital, debemos aspirar a acreditar la fuente de la información. Esto es especialmente importante en línea, donde es más fácil pretender ser alguien sin serlo, ya sea a través de medios de poca tecnología (como el uso de cuentas falsas o robando una cuenta) o de tecnología de punta (como redirigir el tráfico de la red). En el capítulo Proteger tus comunicaciones se discute cómo autenticar fuentes digitales, así como en la conclusión Elección de herramientas de seguridad digital.

Una consideración elemental es cómo usamos las redes sociales, donde abundan los chismes y rumores y donde la exposición de los detalles de nuestras vidas personales hace innecesaria la infiltración para conocer nuestra posibles debilidades. Las plataformas de redes sociales solo deberían usarse para distribuir información pública y las conversaciones que ahí ocurren no deben considerarse privadas en ningún caso.

Estas acciones tienen el potencial de protegerte contra la vigilancia en redes sociales, órdenes judiciales, de cateo y el *doxxing*.

En contexto: Los principios de Saint Paul

En vísperas de la Convención Nacional Republicana de 2008 en Saint Paul, Minnesota, distintos movimientos sociales se unieron en oposición al apoyo del Partido Republicano a la guerra en Irak. La coalición de grupos en protesta adoptó los siguientes principios en vísperas de la convención con el objetivo de hacer lugar a las diferentes visiones y estrategias de los grupos, así como de reducir las posibilidades de que los riesgos enfrentados por un grupo afectaran a los demás:

1. Nuestra solidaridad estará fundamentada en el respeto a la diversidad de tácticas y planes de otros grupos.
2. Las acciones y tácticas usadas estarán organizadas para conservar una separación de tiempo o espacio.
3. Cualquier debate o crítica se mantendrá dentro del movimiento y se evitará hacer pública cualquier denuncia de compañeros activistas o de eventos.
4. Nos oponemos a cualquier represión del Estado al disenso, incluyendo la vigilancia, infiltración, perturbación y violencia. Convenimos en no brindar apoyo a los cuerpos policiales en acciones en contra de activistas y de otros.

Estas reglas se conocen ahora como los "Principios de Saint Paul" y muchas coaliciones de grupos los han adoptado desde entonces. Los principios elevan las nociones de cultura de seguridad de un nivel intragrupal a uno intergrupal. Están diseñados para ayudar a diferentes grupos a unirse cuando tienen el mismo objetivo ulterior, aunque no estén de acuerdo en cómo llegar a él, y aumentar de ese modo la posibilidad de éxito del movimiento global en su meta compartida.

Qué aprender a continuación

- Proteger tus dispositivos
- Proteger tus comunicaciones
- Proteger tu identidad

Recursos externos

- Wikipedia. "2008 Republican National Convention." 11 de enero de 2021.
- Activistsecurity.org. *A Practical Security Handbook for Activists and Campaigns*. Civil Liberties Defense Center, mayo de 2007.
- Sprout Anarchist Collective. "What Is Security Culture?" 2012.

Proteger tus dispositivos

Se recomienda leer los capítulos Contraseñas y Amenazas digitales a movimientos sociales antes de seguir con este.

Lo que aprenderás

1. Formas comunes en que los teléfonos celulares y computadoras suelen resultar comprometidos
2. Estrategias para proteger teléfonos celulares y computadoras

La cantidad de datos que almacenas en tu teléfono y laptop es asombrosa: contactos, correos electrónicos, fotografías, documentos, calendarios, devoluciones de impuestos, datos bancarios y, en el caso de un teléfono inteligente, con frecuencia una historia detallada de tu ubicación durante todo el tiempo que has tenido ese teléfono. Muchos de estos datos también los compartes con tus proveedores de almacenamiento en la nube (por ejemplo, Apple, Google y Dropbox). Pero ese es el foco del capítulo Proteger tus datos remotos; aquí nos centraremos en proteger los datos que almacenas contigo, en tu teléfono celular o laptop, de ataques remotos o físicos.

Ataques físicos

Con *ataque físico* nos referimos a que tu adversario obtiene acceso físico a tu dispositivo a través de su extravío, robo o confiscación. Es posible que pierdas tu teléfono en un momento inoportuno que lo ponga en las manos de un adversario en lugar de las manos de un buen samaritano, o que tu adversario robe tu teléfono. Quizás sea más probable que tu teléfono sea confiscado al cruzar una frontera o durante un arresto, ya sea planeado o no planeado.

A quienes fueron detenidos en los arrestos en masa ocurridos durante las protestas contra la investidura presidencial del 20 de enero de 2017 (J20) se les confiscaron sus teléfonos, los cuales fueron inspeccionados con una herramienta de la compañía israelí Cellebrite, que extrae toda la información de un dispositivo (teléfono o computadora) y de todas las cuentas remotas a las cuales ese dispositivo tiene acceso (por ejemplo, Google, Facebook o Dropbox). En el artículo

“How to Protect Yourself from the Snitch in Your Pocket”, un acusado por el J20 describió las ocho mil páginas de datos que la herramienta de Cellebrite extrajo de su teléfono confiscado. Recibió la siguiente información de su abogado mientras preparaba su defensa:

- Una lista de todos mis contactos, incluyendo los números telefónicos y correos electrónicos que me contactaron y que no fueron almacenados en mi teléfono, así como un conteo de cuántas veces los llamé y envié mensajes o correos electrónicos, o me llamaron y enviaron mensajes o correos electrónicos.
- La cantidad de correos que recibí y envié y los borradores a cuentas de correo específicas, y cuántos eventos de calendario compartí con dichas cuentas; la cantidad de llamadas de entrada, de salida o perdidas de cada número y si éste se encontraba en mis contactos, así como la duración total de las llamadas entre ese número y el mío. Si estaban en mis contactos y el alias con el cual los llamo desde mi teléfono.
- La cantidad de mensajes SMS recibidos y enviados o borradores dirigidos a cierto número; el contenido de todos los mensajes, incluso si habían sido eliminados, y contando los borradores.
- Contactos de WhatsApp, sus “nombres de usuario” (es decir, el número telefónico junto con su cuenta) y cuántas conversaciones o llamadas tuvieron lugar entre ellos y yo.
- Todas las aplicaciones, cuándo se instalaron o eliminaron, la fecha de último uso, de compra, y los permisos que tenían.
- Archivos de audio almacenados en Google Drive, así como cualquier podcast, nota de voz y tonos de llamada. Fechas de creación, eliminación, modificación y último acceso.
- Todos los eventos de calendario, asistentes invitados, etiquetas de ubicación, etcétera.
- Información tradicional del historial de llamadas, como se esperaría.
- Fecha y hora de todas las conexiones con torres a las cuales se conectó mi teléfono alguna vez, así como su ubicación, vinculada de forma muy conveniente a Google Maps. Un mapa mundial con todas las torres celulares a las que tuvo acceso mi teléfono.
- Conversaciones desde Signal, WhatsApp, SMS, Google Hangouts, TextSecure, GroupMe y Google Docs; una lista de todos los participantes en dichas conversaciones; el cuerpo del texto; si se leyó o no, con fecha de envío y lectura; si estaba destacado o eliminado; todos los documentos adjuntos; las conversaciones incluían las de hace años, incluso antes de que tuviera un teléfono inteligente.
- Toda la información de mis contactos, aunque el contacto hubiera sido eliminado.
- Cookies del buscador de internet.
- Cualquier documento que se haya abierto alguna vez en mi teléfono, incluyendo documentos de texto, adjuntos, Google Docs y los creados por las apps.
- Correos electrónicos y borradores, incluyendo toda la información de envío, el texto completo y hasta 16 documentos adjuntos.
- Imágenes, fotografías, videos, así como su fecha de creación o acceso y todos los

metadatos.

- Noventa y seis tuits aleatorios desde una de mis cuentas de Twitter, algunos de ellos de 2013.
- Una lista de todas las redes wifi con las cuales se conectó mi teléfono alguna vez, sus contraseñas, identificadores de hardware y cuándo me conecté con ellas.
- Las últimas cinco veces en que mi teléfono se encendió, incluyendo dos veces dos meses después de que perdí acceso a él.
- Historial de búsquedas en la web y en Play Store.
- Una lista de todas las palabras tecleadas alguna vez en mi teléfono y cuántas veces fue tecleada cada una, incluidos correos electrónicos como palabras, así como palabras que incluí en el diccionario para que no siguieran apareciendo en la autocorrección.
- Lo que llaman mi *cronología*: todas las acciones que ejecuté (mensajes de texto, correos, búsquedas web, uso de apps, búsquedas en mapas, conexiones wifi o con nuevas torres celulares, etcétera), con su fecha para su fácil clasificación.

¿Qué puedo hacer?

Un detective que atestiguó en un juicio por el J20 señaló que en aquellos teléfonos que tenían habilitado el cifrado solo había podido acceder a información básica de los dispositivo y no al contenido almacenado en ellos. Los iPhones y dispositivos Android dotados de sistemas operativos actualizados cuentan con cifrado habilitado por defecto, en tanto que en computadoras Apple y Microsoft es necesario habilitar esta función. Sin embargo, cifrar tu dispositivo tampoco es una panacea. El cifrado que protege tu dispositivo es tan robusto como la contraseña que lo protege.

Desafortunadamente, las contraseñas para el cifrado de dispositivos experimentan una contradicción entre conveniencia y seguridad. Una frase de contraseña (como se describe en el capítulo Contraseñas) puede requerir seis o más palabras para resistir un ataque físico, pero puede resultar engorroso teclear dicha frase con frecuencia. Hay algunas opciones, y todas implican sacrificios. En teléfonos celulares y laptops puedes modificar la configuración para cambiar la frecuencia con la que es necesario teclear la contraseña, frase de contraseña o código de desbloqueo. (Observa que este cifrado solo está en efecto cuando hay una pantalla de bloqueo habilitada.) O puedes modificar la robustez (longitud) de tu contraseña, frase de contraseña o código de desbloqueo en función de la situación. Sin embargo, estas estrategias dependen de que conozcas en qué momento tu situación requiere mayores niveles de seguridad y de que incrementes tu nivel de seguridad de manera congruente.

En el caso de los teléfonos y algunas laptops, es frecuente que se pueda elegir entre una frase de contraseña o un registro biométrico (como una huella digital). Una huella digital resulta más

conveniente que una contraseña tecleada. Para los propósitos del cifrado, tu huella digital se uniría con una frase de contraseña (tan robusta como sea posible). Sin embargo, si tu dispositivo fuera confiscado por cuerpos policiales, podrían forzarte a presentar tu huella digital. Por tanto, cuando hay mucho riesgo de que ocurra una confiscación, debería considerarse eliminar la posibilidad de desbloquear el dispositivo con registros biométricos.

Existen protecciones adicionales contra la interferencia física que uno podría considerar. Un protector de pantalla de privacidad puede evitar que un espía vea las contraseñas (y cualquier otra cosa) que teclees. Las bolsas Faraday pueden impedir que tu teléfono transmita o reciba información; entre otras cosas, esto puede evitar que tu teléfono registre información de ubicaciones. Algunos fabricantes de teléfonos celulares brindan la posibilidad de borrar un teléfono en forma remota y, aunque esto podría ceder el control de tu dispositivo a las mismas corporaciones que podrían compartir tu información con tus adversarios (como se discute en el capítulo Proteger tus datos remotos), puede ser una herramienta útil en ciertas situaciones.

Ataques remotos

Cuando decimos ataque remoto nos referimos a que un adversario podría acceder a los datos de tu teléfono o laptop a través de una conexión de internet o de datos. Existen compañías que diseñan y venden la opción de infectar teléfonos (suelen centrarse en teléfonos inteligentes) con malware que permite al cliente (tu adversario, ya sea una corporación o agente gubernamental) obtener acceso remoto a parte de o toda tu información.

Por ejemplo, Citizen Lab descubrió el uso amplio y diverso del software espía Pegasus, creado y vendido por otra compañía israelí, NSO Group. Valiéndose de ingeniería social para convencer al objetivo de hacer clic en un link, el spyware permite encender el micrófono y grabar desde la cámara del teléfono afectado; registrar llamadas, mensajes de texto (incluso aquellos con cifrado de extremo a extremo) y ubicaciones GPS, y enviar toda esta información al adversario del objetivo. Citizen Lab reportó que se efectuaron ataques con Pegasus contra Ahmed Mansoor, un defensor de derechos humanos con sede en Emiratos Árabes Unidos, y contra veintidós individuos en México, desde políticos en campaña contra la corrupción en el gobierno hasta científicos en favor de un impuesto federal a las bebidas azucaradas.

¿Qué puedo hacer?

Como en el caso de los que vende NSO Group, los ataques remotos dependen de fallas en el software de cómputo conocidas como *de día cero*. Dichas fallas suelen ser desconocidas para el proveedor del software (por ejemplo, Apple o Microsoft). Hasta que son descubiertas (lo cual ocurre en el *día cero*), no hay posibilidad de que el proveedor pueda haber arreglado o enmendado la vulnerabilidad, así que no hay posibilidad de que una víctima pueda protegerse.

La seguridad de las computadoras suele ser un juego entre gatos y ratones. Los productos de desarrolladores de malware y spyware (como NSO Group) solo son buenos en la medida en que sus objetivos (mejor dicho, compañías como Apple, Google y Microsoft) desconozcan el despliegue del malware. En cuanto lo descubren, corrigen sus productos de manera que el malware deja de ser eficaz.

Sin embargo, dichas correcciones solo funcionan si el objetivo (tú) mantiene el dispositivo actualizado. Por tanto, la conclusión en este punto es que *debes instalar todas las actualizaciones de seguridad en cuanto estén disponibles*. Desafortunadamente, los teléfonos inteligentes no reciben actualizaciones de seguridad de manera indefinida; de hecho, en el caso de algunos dispositivos, como el Nokia 5.3, su sistema operativo (Android) solo es compatible con éste durante algunos años. Es posible verificar si un teléfono Apple o Android está recibiendo actualizaciones de seguridad en la app de configuración del dispositivo.

Para instalar productos de malware en el dispositivo de un blanco, suele ser necesario el phishing: convencer a la persona de hacer clic en un vínculo o de abrir un archivo (en un correo electrónico o en un mensaje de texto). Así que lo segundo que puedes hacer es *tener cuidado de a qué le das clic*. ¿Conoces al remitente? ¿Estás esperando algo de ese remitente? ¿Hay algo que parezca sospechoso? Fue, de hecho, estar alerta lo que permitió a Ahmed Mansoor evitar la infección de spyware: envió el mensaje de texto sospechoso a Citizen Lab, lo cual condujo a la denuncia del spyware de NSO Group.

Finalmente, *ten cautela con las aplicaciones que instalas y los permisos que les concedes*. ¿Necesita una app de linterna tener acceso a tus contactos y a tu cámara? ¿En verdad necesitas instalar el juego creado por un desarrollador de software desconocido? Todas las aplicaciones que instalas son un vector potencial de malware, así que es una buena oportunidad para practicar el minimalismo.

En contexto: Comprometer los teléfonos de manifestantes

En septiembre de 2020 salió a la luz que el Departamento de Seguridad Nacional “extrajo información de los teléfonos de manifestantes” durante el verano de 2020 en Portland, Oregon. Supuestamente, gracias a un novedoso método para clonar teléfonos celulares, el gobierno pudo interceptar comunicaciones desde los teléfonos de manifestantes. Aunque esto es alarmante, y probablemente ilegal, los detalles del ataque permanecen en reserva. Sin embargo, podemos intentar inferir métodos probables de ataque y posibles prácticas de protección.

Si el método de clonación requiere un ataque físico, es probable que los teléfonos comprometidos hayan sido confiscados en arrestos previos durante ese verano. Sin embargo, esto restringe el potencial de vigilancia a los teléfonos de los arrestados y permite que estos dejen de confiar en sus teléfonos o que restablezcan la configuración de fábrica para eliminar cualquier malware.

Por otra parte, si el método de clonación puede efectuarse en forma remota, esto expande en gran medida la cantidad de teléfonos que pueden resultar comprometidos y no tienen una señal de alerta.

En cualquier caso, el uso de cifrado en tránsito y de extremo a extremo podría aun así proteger las comunicaciones de tu teléfono (aunque quizás no los metadatos), como puedes aprender en el capítulo Proteger tus comunicaciones.

Qué aprender a continuación

- Proteger tus comunicaciones
- Proteger tu identidad

Recursos externos

- *Earth First! The Journal of Ecological Resistance*. "How to Protect Yourself from the Snitch in Your Pocket." Invierno de 2017-18. (En protestarchive.org se encuentra una versión digital del artículo.)
- Marczak, Bill, y John Scott-Railton. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender." Citizen Lab, 24 de agosto de 2016.
- Schiano, Chris. "Criminalizing Dissent: Contested Evidence Introduced in J20 Trial Testimony." Unicorn Riot, 30 de noviembre de 2017.
- Klippenstein, Ken. "Federal Agencies Tapped Protesters' Phones in Portland." Nation, 21 de septiembre de 2020.
- Vice Media Group. "Phone Crackers." Consultado el 9 de febrero de 2021.

Proteger tus comunicaciones

Se recomienda leer los capítulos El intermediario, Contraseñas, y Amenazas digitales a movimientos sociales antes de seguir con este.

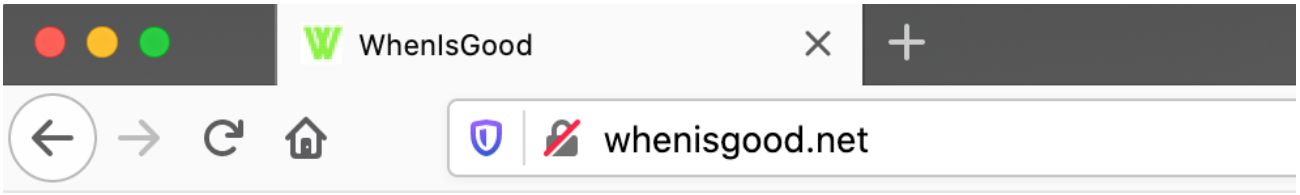
Lo que aprenderás

1. La diferencia entre cifrado en tránsito y cifrado de extremo a extremo
2. Quién tiene acceso a tu información cuando no usas un cifrado
3. Quién tiene acceso a tu información cuando usas un cifrado en tránsito
4. Quién tiene acceso a tu información cuando usas un cifrado de extremo a extremo

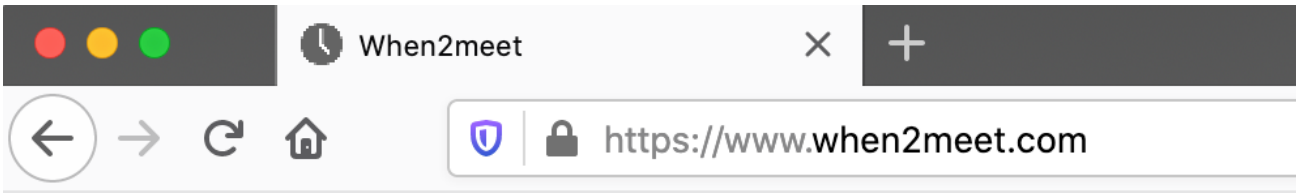
La mejor forma de proteger tus comunicaciones en línea es a través de un cifrado. Sin embargo, no todos los cifrados protegen en el mismo grado. Aquí nos centraremos en los conceptos que distinguen entre los grados de protección.

Cifrado o no cifrado

La versión más básica del cifrado de comunicaciones es el cifrado en tránsito, en el que tu información se cifra entre tu computadora y un servidor. En el contexto de las búsquedas en internet, esto es lo mejor para proteger el contenido (aunque no los metadatos) de tus comunicaciones contra un adversario. La mayoría de los buscadores de internet indican si tu búsqueda está cifrada por el URL, como se ilustra a continuación.



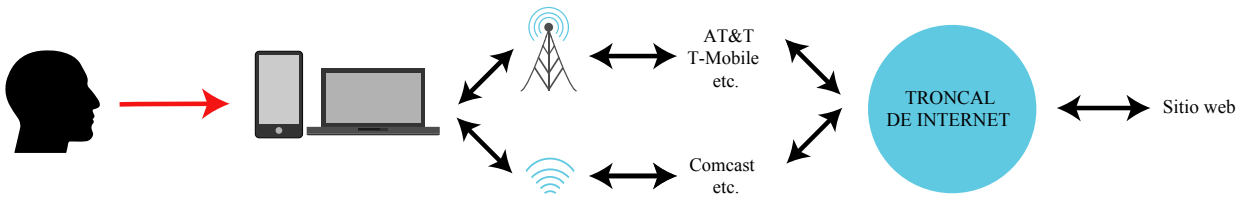
HTTP, no cifrada



HTTPS, cifrada

En el primer ejemplo, la información se transmite sin cifrar. El URL completo, en este caso, es `http://whenisgood.net`, donde `http` indica que se está accediendo a la web sin un cifrado. Este buscador (Firefox) pone esto de realce con un candado tachado. En el segundo ejemplo, la información sí está cifrada: `https` indica que se está accediendo a la web con un cifrado, donde `s` significa *seguro*.

Cuando usas `http`, todas las entidades situadas en el camino entre tú y el sitio web que se ilustran a continuación pueden acceder al contenido de tu búsqueda (como las imágenes que se cargan y cualquier información que teclees en un formato web). Además, cualquiera que esté espiando las comunicaciones entre las entidades situadas en esta ruta (como entre la red de Comcast y la troncal de internet) también podría tener acceso al contenido de tu búsqueda. Decimos *podría* porque las comunicaciones entre dos entidades en esta ruta podrían estar cifradas. Por ejemplo, las comunicaciones entre un teléfono celular y una torre celular están cifradas en la mayoría de los casos.

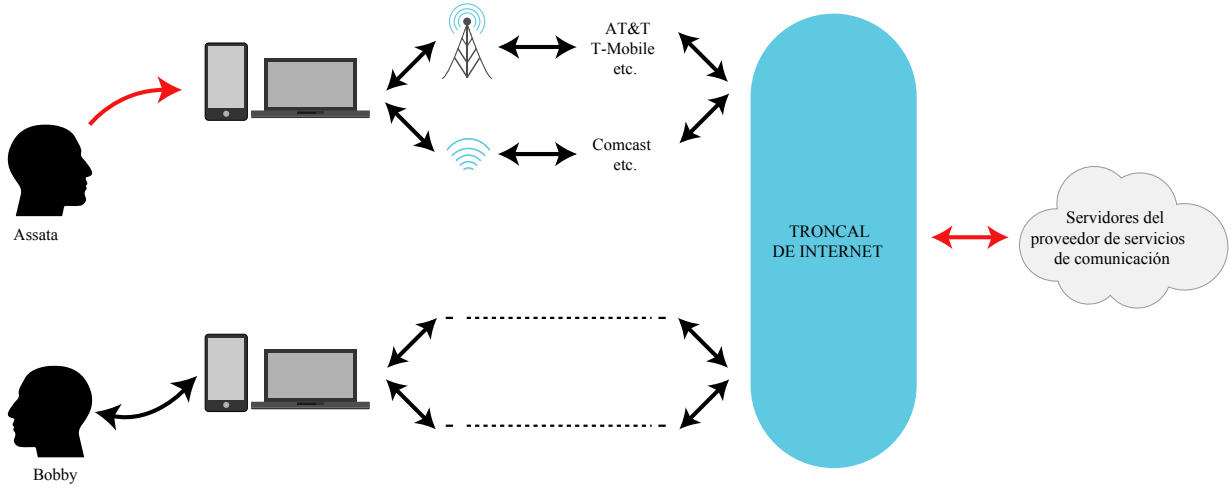


Quién tiene acceso a tus datos de búsqueda

Por el contrario, cuando usas `https` solo tú y el sitio web (técnicamente, los servidores que hospedan el sitio web) tienen acceso al *contenido* de tu búsqueda. Usamos aquí el término *contenido* porque ciertos metadatos seguirán siendo del conocimiento de entidades situadas en la ruta entre tú y el sitio web, como el URL básico del sitio, la cantidad de tiempo que navegaste en él y la cantidad de información que descargaste.

Cifrado en tránsito

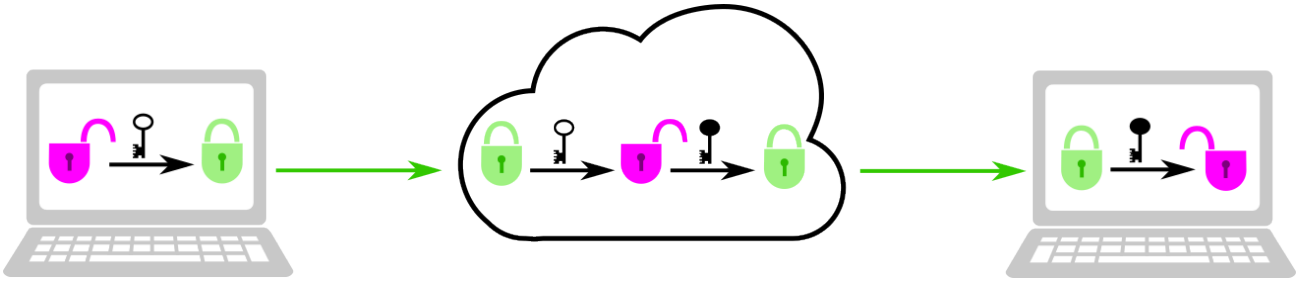
Cuando nos comunicamos con otra persona por correo electrónico, mensajería instantánea o video chat, esas comunicaciones (en la mayoría de casos) son enrutadas a través del proveedor de comunicaciones (por ejemplo, los servidores de Google para el correo o los de Microsoft para llamadas de Skype), como se ilustra a continuación. En la actualidad, estas comunicaciones suelen estar cifradas, aunque solamente entre tú y el proveedor de comunicaciones. Es decir, aunque las entidades y espías no tienen acceso al contenido de las comunicaciones a lo largo del camino entre Assata y los servidores del proveedor de servicios (centro), ni entre dichos servidores y Bobby (aunque pueden dar un vistazo a los metadatos), el proveedor de comunicaciones *sí* tiene acceso al contenido.



Quién tiene acceso a los datos de tus comunicaciones

Conocemos esto como cifrado en tránsito porque el contenido está cifrado durante su tránsito entre Assata y el proveedor de comunicaciones y entre este y Bobby. Las claves del cifrado en tránsito se generan en forma separada para cada parte de la ruta entre Assata y Bobby, como se ilustra a continuación. El proveedor (centro) ejecuta un intercambio Diffie-Hellman con Assata y genera una clave compartida; luego, ejecuta otro intercambio Diffie-Hellman con Bobby y genera una clave compartida *diferente*. Cuando Assata envía un mensaje a Bobby a través del proveedor, el mensaje se cifra primero con la clave que Assata comparte con el proveedor y luego

se le transmite al proveedor. El proveedor descifra el mensaje con la clave que comparte con Assata. Luego, el proveedor vuelve a cifrar el mensaje con la clave que comparte con Bobby antes de transmitirle el mensaje. Entonces, Bobby puede descifrar el mensaje. Por tanto, el mensaje solo existe en forma descifrada en los dispositivos de Assata y de Bobby y en los servidores del proveedor; es decir, solo se encuentra cifrado cuando está en tránsito entre esas entidades.



Cifrado en tránsito

Cifrado de extremo a extremo

En tanto que el cifrado en tránsito protege tus comunicaciones de cualquier adversario (como tu proveedor de servicios de internet—ISP, del punto de acceso wifi o de un mirón situado a lo largo de los canales de comunicación), el proveedor de comunicaciones sigue teniendo acceso a toda la información. Incluso si el proveedor no es un adversario directo, podría compartir dicha información con un adversario (a través de un citatorio o de una orden judicial). El cifrado de extremo a extremo (E2EE, por su nombre en inglés) protege tus comunicaciones incluso del proveedor de comunicaciones.

Para que ocurra un E2EE (se ilustra a continuación), Assata y Bobby intercambian claves (mediante un intercambio Diffie-Hellman u otro procedimiento similar). En el tránsito de sus comunicaciones *a través* del proveedor (en tanto el proveedor no efectúe un ataque de intermediario), estas están cifradas con una clave a la cual solo Bobby y Assata tienen acceso. Es decir, el mensaje solo existe en forma descifrada en los dispositivos de Assata y Bobby. Los dispositivos de Assata y Bobby son los *extremos* de la comunicación, de ahí el nombre *cifrado de extremo a extremo*.

Cifrado de extremo a extremo

Autenticación

Mientras que el E2EE es el estándar de referencia, hay otras consideraciones para tener en cuenta. Como se mencionó antes, el cifrado de extremo a extremo solo puede establecerse si el proveedor de comunicaciones (o un tercero) no efectúa un ataque de intermediario al comienzo del intercambio de claves. Sin embargo, como hemos visto en el capítulo El intermediario, si Assata y Bobby verifican sus claves a través de canales independientes, pueden determinar si ha ocurrido un ataque de intermediario y, por tanto, si sus comunicaciones están verdaderamente cifradas de extremo a extremo.

Aunque muchas aplicaciones o servicios que afirman ofrecer E2EE brindan la posibilidad de verificar claves, muchos no lo hacen, lo cuan aporta pocas garantías que permitan confiar en las promesas de E2EE. Además, la mayoría de las aplicaciones E2EE que sí brindan la posibilidad de verificar claves operan bajo el criterio de confianza en el primer uso (TOFU, por sus siglas en inglés). Es decir, las comunicaciones pueden iniciarse sin haber verificado claves primero. Sin embargo, aunque la verificación de claves es la única forma de garantizar E2EE, la existencia de la *posibilidad* de verificarlas es una protección contra los ataques de intermediario automatizados, puesto que tan solo una pequeña fracción de usuarios que verificara sus claves pondría al descubierto ataques de intermediario generalizados.

Y, por supuesto, E2EE solo protege las comunicaciones entre dispositivos; es decir, no protege los datos que se encuentran en el dispositivo. Se debe combinar el uso de apps E2EE con contraseñas robustas que protejan la cuenta o dispositivo.

En contexto: Videollamadas grupales

Existen muchas aplicaciones y servicios para hacer videollamadas entre dos o más personas, con diversos grados de seguridad. A continuación se ofrecen tres ejemplos:

- Wire brinda el modelo de referencia en E2EE. Cada usuario tiene una cuenta a la cual puede acceder desde diversos dispositivos (por ejemplo, laptop y teléfono inteligente). Existe una clave pública para cada dispositivo que se usa para establecer una clave de cifrado para cada sesión (videoconferencia), y las huellas digitales de dichas claves pueden compararse para validar un verdadero E2EE. Wire permite hacer videollamadas E2EE entre grupos de hasta doce usuarios.
- Zoom permite hacer videollamadas entre grupos mucho más grandes y sí brinda E2EE, en el sentido de que una transmisión de video es cifrada y descifrada por los usuarios con la misma clave. Sin embargo, los servidores de Zoom son los que establecen y distribuyen estas claves. Puesto que Zoom tiene acceso a la clave de cifrado, este no puede considerarse un verdadero E2EE. Además, no existe un mecanismo para que los usuarios verifiquen las claves de cifrado. Desde el verano de 2020, Zoom tiene una propuesta para establecer claves que

permitan hacer un verdadero E2EE, pero todavía no la ha implementado.
- Jitsi Meet también permite hacer videollamadas entre grupos grandes, pero solo con cifrado en tránsito. Sin embargo, Jitsi Meet puede alojarse en cualquier servidor (incluyendo el tuyo, si lo deseas). Hay también una instancia en la que Jitsi Meet está alojada por May First, una organización sin fines de lucro que brinda soluciones técnicas a movimientos sociales y que es un tercero en quien muchos grupos confían. Aunque May First tiene acceso a estas comunicaciones, algunos preferirían confiar en May First que en una solución con fines de lucro como Zoom.

Qué aprender a continuación

- Proteger tus dispositivos
- Proteger tus datos remotos
- Proteger tu identidad

Recursos externos

- Blum, Josh, Simon Booth, Oded Gal, Maxwell Krohn, Julia Len, Karan Lyons, Antonio Marcedone, et al. "E2E Encryption for Zoom Meetings." Zoom Video Communications, 15 de diciembre de 2020.

Créditos

Proteger tus datos remotos

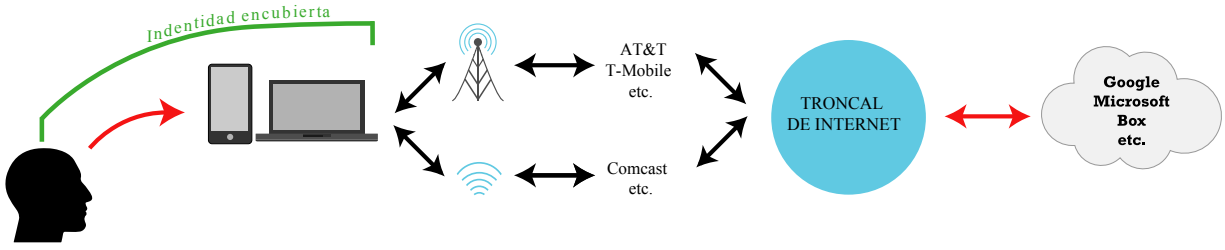
Se recomienda leer el capítulo Proteger tus comunicaciones antes de seguir con este.

Lo que aprenderás

1. Quién tiene acceso a tus datos en la nube
2. Qué parte de tus datos está en la nube

La nube es ubicua. Desde inicios de los años 2000, los datos han dejado de almacenarse en forma exclusiva (o incluso parcial) en tu dispositivo, sino que ahora se almacenan en los servidores de compañías que administran tu dispositivo o sistema operativo o a cuyo servicio te has suscrito. Si los datos no están cifrados con una clave bajo tu control, dichos datos están en riesgo de resultar comprometidos.

Acceder a tus datos remotos o en la nube es similar a acceder a una página web, como se ilustra a continuación. En la mayoría de los modelos de acceso a datos almacenados en la nube, la información está protegida por cifrado en tránsito, lo cual protegería tus datos de adversarios potenciales en la ruta de tu dispositivo a los servidores del proveedor de almacenamiento (como se muestra abajo).



Quién tiene acceso a tus datos en la nube

Sin embargo, como se explica en el capítulo Amenazas digitales a movimientos sociales, adversarios en agencias gubernamentales podrían acceder a datos almacenados en forma remota (y que no están cifrados) a través de un citatorio u orden judicial, o los datos simplemente podrían ser compartidos con un tercero. Desafortunadamente, aun si evitamos las formas más

explícitas de datos remotos (como lo que ofrecen Dropbox o Google Drive), muchos de nuestros dispositivos promueven que hagamos respaldos remotos de todos nuestros datos (como lo hacen los dispositivos Apple en iCloud), y en algunos casos es muy difícil evitarlo (como lo es para dispositivos Android con una cuenta de Google). Esto incluye potencialmente una gran cantidad de información que comprende tus direcciones, calendarios, ubicación histórica, información de navegación... posiblemente todo lo que haces con tu computadora.

En contexto: Almacenamiento en la nube por confianza o cifrado

Existen muchas opciones de almacenamiento en la nube. En la siguiente lista se describen algunas opciones que ilustran su diversidad, desde opciones no cifradas y no confiables a no cifradas pero confiables, hasta opciones cifradas.

- Google ofrece almacenar gratuitamente toda tu información (correos electrónicos, archivos, información de contactos, respaldos de tus dispositivos). Por supuesto, extraen valor de esto utilizando tus datos, pero no pueden hacerlo si tus datos están cifrados con una clave bajo tu control exclusivo (por lo que no lo están). Como vimos en el capítulo Amenazas digitales a movimientos sociales, Google entrega datos en respuesta a aproximadamente 80 por ciento de las órdenes judiciales que recibe.
- El software ownCloud ofrece almacenamiento en la nube del tipo de Box o Dropbox, pero, al igual que los productos Google, solo usa cifrado en tránsito. (Una versión empresarial de ownCloud sí ofrece cierto almacenamiento y función de compartir archivos con cifrado de extremo a extremo.) Sin embargo, ownCloud, al igual que la app de videoconferencias Jitsi Meet, puede alojarse en cualquier servidor (incluyendo el tuyo). También, al igual que Jitsi Meet, hay una instancia en la que ownCloud está alojada por May First, un proveedor de servicios en el que muchos confían. Aunque May First tiene acceso a tus datos almacenados, algunos preferirían confiar en May First que en Google.
- CryptPad es una plataforma de edición colaborativa que ofrece una alternativa a Google Docs con cifrado de extremo a extremo. Se accede a los documentos por medio de un vínculo que incluye una clave para descifrar el documento, pero esa clave aparece después de un # en el URL; por ejemplo: `https://cryptpad.fr/pad/#/2/pad/edit/bpsky2zF5La8sZ_i-6r_cTj9fPL+`. La parte del URL posterior al signo # es conocida como fragmento identificador y no se transmite al servidor, sino que se usa solamente dentro del buscador; en este caso, para descifrar una libreta determinada. Puesto que la clave de cifrado es parte del URL, debe tenerse precaución al compartir ese vínculo (es decir, compartirlo solamente a través de un canal cifrado, como Signal).
- Keybase tiene diversos atractivos, incluyendo un sistema de almacenamiento cifrado de extremo a extremo, similar al de ownCloud o al de Dropbox. A diferencia de CyptPad, Keybase ofrece apps que operan localmente en un dispositivo (*standalone apps*) y no desde un buscador, y se encarga de la gestión de claves.

Qué aprender a continuación

- Todos los capítulos restantes de la Parte 3

Créditos

- where-your-cloud-data-is © OSU OERU is licensed under a CC BY-NC (Atribución NoComercial) license

Proteger tu identidad

Se recomienda leer el capítulo Criptografía asimétrica y Enrutado anónimo antes de seguir con este.

Lo que aprenderás

1. La diferencia entre anonimato y seudonimato
2. Tres formas distintas de usar Tor
3. Algunas cosas que nunca deberías hacer usando Tor

En el capítulo Enrutado anónimo comparamos y contrastamos redes privadas virtuales (VPN) y Tor como dos métodos para encubrir nuestros metadatos en línea. Esto puede ayudar a lograr el anonimato o el seudonimato, aunque esto es difícil de mantener en el largo plazo. En este capítulo nos centraremos en las habilidades para usar Tor más que una VPN, pero estas lecciones son válidas también para usar una VPN. También es necesario recordar que cuando se usa una VPN, el proveedor sabe quién eres y conoce los metadatos de tus comunicaciones por internet (y el contenido, si no está cifrado). Aunque nos centraremos en el uso de Tor a través de Tor Browser, debes saber que hay otras aplicaciones (como aplicaciones de mensajería segura o incluso sistemas operativos) que enrutan las solicitudes de internet a través de la red Tor.

Anonimato versus seudonimato

Antes de describir diferentes formas de usar Tor, consideremos la diferencia entre anonimato y seudonimato. Estos términos se usan en formas distintas en contextos distintos; aquí hemos restringido su uso a las comunicaciones y conductas en línea.

Anonimato se refiere a no tener un nombre o, en términos más generales, ningún identificador que pueda relacionarse contigo. Si visitas un mismo sitio web en forma anónima hoy y también mañana, el sitio no debería saber ni siquiera que se trata de la misma persona en ambas ocasiones. Lo único que dicho sitio debería saber es “alguien me visitó ayer en forma anónima” y “alguien me visitó hoy en forma anónima”.

Seudonimato se refiere al uso de un nombre falso, que nadie o pocos vinculan contigo. Por ejemplo, Samuel Clemens publicó bajo el seudónimo Mark Twain, aunque, por supuesto, su editor

y otros sabían quién era el verdadero autor. Edward Snowden usó el seudónimo Cincinnatus cuando contactó al periodista Glenn Greenwald. Greenwald no sabía quién lo había contactado como Cincinnatus, y puesto que Snowden usó Tor para contactarlo, tampoco lo sabía nadie más. Sin embargo, el uso repetido del seudónimo Cincinnatus por Snowden permitió a Greenwald relacionar diferentes comunicaciones que él y su colega Laura Poitras habían recibido de Snowden. Aquí usaremos seudonimato para referirnos a la posibilidad de vincular sesiones de comunicación distintas y anónimas bajo una sola identidad.

Formas de usar Tor

Es posible usar Tor para ocultar información sobre tu identidad (como tu ubicación física) para conseguir anonimato y seudonimato. El usuario novato puede acceder a Tor por medio del buscador Tor Browser o de aplicaciones compatibles con Tor. El usuario más avanzado puede enrutar sus comunicaciones desde un *non-web browser* a través de Tor, usando un sistema operativo (como Tails o Whonix) que conduce todo su tráfico web por medio de Tor.

Ocultar tu ubicación física

Al usar el navegador Tor Browser, como cualquier otro navegador, incluso para acceder a correos electrónicos o nombres de usuario de redes sociales vinculados contigo, estarás ocultando tu ubicación física a esas cuentas. Cada vez que abres una nueva pestaña o ventana de Tor, y después de cierto retraso, Tor enruta tus solicitudes web por medio de otra ubicación. Sin embargo, muchas plataformas de correo y redes sociales etiquetarán la actividad de tu cuenta como sospechosa si accedes a ella desde diferentes ubicaciones, como parecerá cuando lo hagas usando Tor. Así que, aunque es posible usar Tor todo el tiempo para cualquier cosa, es probable que no sea práctico. Si puedes sortear estas dificultades, de todas formas tienes que ser astuto para esconder en forma consistente tu ubicación física, *evitando* las siguientes conductas:

- Consignar información que te identifique en un sitio web (como tu dirección).
- Descargar un documento que podría acceder a parte de su contenido por medio de la web (como una fotografía) y abrirlo fuera de Tor Browser (los documentos Word y los pdf pueden hacer esto). Si necesitas acceder a un documento así, desconéctate de internet antes de abrirlo.

Obtener el anonimato

El uso de Tor puede ayudarte a lograr el anonimato. Sin embargo, tendrás que restringir tus conductas y asegurarte de no filtrar información que podría romper tu anonimato. De este modo,

para conservar el anonimato, es necesario *evitar* las siguientes conductas durante tu *sesión anónima* (además de las señaladas para ocultar tu ubicación física):

- Iniciar sesión en cuentas (por ejemplo, de redes sociales, de correo electrónico o bancarias).
- Visitar tu propio sitio web repetidamente.

Obtener y conservar el seudonimato

Si creas un seudónimo no relacionado con tu identidad verdadera con el fin, por ejemplo, de publicar comunicados de prensa o participar en foros, Tor puede ayudarte a asegurarte de que tu seudónimo permanezca desvinculado de tu identidad verdadera. Sin embargo, para hacer que ambas identidades sigan siendo independientes es necesario que *evites* las siguientes conductas:

- Acceder a diferentes identidades seudónimas (o a una identidad seudónima y la real) en la misma sesión, ya que esto puede vincular ambas identidades.
- Acceder a una cuenta seudónima incluso una vez fuera de Tor.
- Usar autenticación de dos factores con un teléfono (ya que tu teléfono, aunque sea de prepago, puede revelar tu ubicación física).
- Publicar medios que revelen metadatos (como la ubicación).

Considera que mientras más tiempo intentes conservar una identidad seudónima, te estarás dando más oportunidades de cometer algún error. Además de los errores mencionados, tu estilo de escritura también puede usarse para identificarte mediante la estilometría.

Advertencias sobre Tor

Hay algunos aspectos adicionales a considerar cuando se accede a internet vía Tor.

Como con cualquier tecnología para la protección, nada es perfecto. Si un adversario, Edgar, es capaz de observar la conexión de Assata a la red de Tor y su conexión cuando sale de la red de Tor (hacia el sitio web de Bobby), Edgar podrá determinar que Assata está visitando el sitio de Bobby. Esto se conoce como *ataque temporal de extremo a extremo* o *ataque de correlación*.

Si intentas usar aplicaciones no diseñadas para usar con Tor en una red Tor, es posible que filtren información que te identifique, como la resolución de tu pantalla o alguna configuración única que pudieras tener.

Finalmente, cuando uses Tor, considera que solo brinda anonimato; es decir, para obtener privacidad es necesario que accedas a páginas web usando cifrado de extremo a extremo por medio de https (aunque, desafortunadamente, no todos los sitios lo permiten).

En contexto: Obtener el verdadero Tor Browser

Las herramientas que usas para protegerte en línea solo son útiles si son las auténticas. En 2019 se descubrió que personas interesadas en robar Bitcoin (con éxito) estaban promoviendo una versión falsa de Tor Browser. Hicieron disponible el "Tor Browser" malicioso a través de dominios incorrectos como tor-browser[.]org y torproect[.]org (en lugar del dominio auténtico, torproject.org). Para protegerte de errores como hacer descargas del servidor incorrecto o de un ataque de intermediario que te provea de una app maliciosa, apps como Tor Browser permiten que verifiques la firma de una descarga, como se explica en el capítulo Criptografía asimétrica.

Qué aprender a continuación

- Todos los capítulos restantes de la Parte 3

Recursos externos

- Hancock, Alexis. "Phony HTTPS Everywhere Extension Used in Fake Tor Browser." Electronic Frontier Foundation, 31 de octubre de 2019.
- Tails. Consultado el 9 de febrero de 2021.
- Tor Project. "Tor Project: Overview." Consultado el 9 de febrero de 2021.
- Whonix. "Tips on Remaining Anonymous." 26 de diciembre de 2020.
- Whonix. "Whonix: Software That Can Anonymize Everything You Do Online." Consultado el 9 de febrero de 2021.

Conclusión: elección de herramientas de seguridad digital

Se recomienda leer esta sección al final.

Lo que aprenderás

1. Criterios para evaluar y elegir herramientas de comunicación

Existen muchas herramientas de seguridad digital de donde elegir. Decidir cuál usar puede resultar apabullante. Para recomendar una herramienta, tratamos de elegir una que permita minimizar los problemas de confianza en sus proveedores. Los *criterios requeridos* enumerados a continuación han sido seleccionados con esto en mente. Hemos incluido *criterios técnicos adicionales* que sería bueno satisfacer, aunque no son esenciales. Finalmente, hay ciertos *criterios no técnicos* que ofrecen los proveedores de tecnología que pueden ayudar a elegir entre un sinnúmero de opciones.

Es improbable que una herramienta sea perfecta, como ilustraremos con ejemplos. Parte del proceso de selección es encontrar la herramienta correcta para el grupo que la usará. Esto puede implicar hacer concesiones, incluso en los criterios requeridos. Y observa que no todos los criterios son aplicables a todas las herramientas. Por ejemplo, Tor Browser brinda la posibilidad de navegar internet en forma anónima, pero por sí solo no aspira a brindar un cifrado de extremo a extremo, así que el primer criterio no se le aplica.

Finalmente, elige una herramienta con cuidado y pruébala antes de pedir a muchas personas que la adopten. Existe un costo social en pedirle a la gente que use algo nuevo o que cambie sus prácticas, y es deseable minimizar la frecuencia con que se hace.

Criterios requeridos

1. El **cifrado de extremo a extremo** (como se describe en el capítulo Proteger tus comunicaciones) nos permite apegarnos al principio de cultura de seguridad de minimizar la cantidad de partes en las cuales se debe confiar. El cifrado de extremo a extremo permite

reservar tus datos del proveedor de la herramienta (aunque no necesariamente los metadatos). Implementar el cifrado de extremo a extremo es el criterio más importante para proteger los derechos de los participantes en movimientos sociales (y de todos).

2. Si una herramienta brinda la **posibilidad de autenticar las claves de tus contactos** a través de *fingerprinting*, esto te permitirá evitar ataques de intermediario, como se describe en el capítulo El intermediario. Lo que es más, si la herramienta no brinda esta posibilidad, su proveedor podría efectuar ataques de intermediario de manera generalizada sin que nadie se diera cuenta.
3. Contar con un **cliente de fuente abierta** permite a la comunidad de profesionales en ciberseguridad en general verificar, por ejemplo, que el cifrado de extremo a extremo se implemente en forma robusta. En el capítulo Criptografía moderna se describe lo que significa *código fuente* y *fuente abierta*. Por *cliente* entendemos el código de una app que se ejecutaría en tu dispositivo, a diferencia del software que se ejecutaría en los servidores del proveedor. También sería ideal tener un software de fuente abierta para el servidor, pero muchas apps mantienen cerrado su software para proteger su propiedad intelectual. Sin embargo, puesto que el cifrado ocurre en el dispositivo, es suficiente verificar cuánta información vería el servidor examinando el código fuente del cliente.
4. Contar con la **posibilidad de autenticar la app** hace lo que el término indica: se requiere más que el simple acceso al código fuente. También es necesario poder verificar que la app que descargas es la que proviene del código fuente. Esto involucra dos pasos: (1) verificar que la app que ejecutas en tu dispositivo realmente puede crearse a partir del código fuente (abierto) publicado y (2) asegurarse de que la app o código fuente es de hecho el mismo que el proveedor ofrece (que no es objeto de una estafa, como en la historia que aparece al final del capítulo Proteger tu identidad, o de un ataque de intermediario). El primer paso raramente está al alcance de cualquier usuario y podría ser muy difícil llevarlo a cabo. Pero el segundo puede hacerse (y lo es en el caso de muchas herramientas) mediante firmas criptográficas, como se describe en el capítulo Autenticarse mediante firmado criptográfico.
5. Una aplicación debería estar en **desarrollo activo** y contar con **desarrolladores que reaccionan rápidamente** ya que, de lo contrario, no seguirá el paso ni siquiera de las actualizaciones más básicas, como los cambios en los sistemas operativos (por ejemplo, Android o iOS). Además, si se encuentra un problema en la app, es necesario arreglarlo con rapidez para mantener segura la información de todos sus usuarios.

Criterios técnicos adicionales deseables

1. Una herramienta de seguridad digital debería ser **multiplataforma y ampliamente accesible**. *Multiplataforma* significa que puede ejecutarse (idealmente y si es aplicable) en sistemas operativos Linux, Mac y Windows, así como en teléfonos inteligentes Android y iOS. Además, estas herramientas deberían reproducirse bien con lectores de pantalla y otras funciones de accesibilidad. Las concesiones en esta materia no deberían tomarse a la ligera. Tal vez en este momento todos en tu grupo tienen dispositivos Android, así que podría estar

bien usar una herramienta exclusiva para Android… por ahora. Pero ¿qué pasaría si en el futuro alguien que no tiene un Android (o teléfono inteligente alguno) quisiera unirse al grupo?

2. Las **auditorías de seguridad** ocurren cuando un tercero (responsable y respetado) evalúa la seguridad de una herramienta dada examinando su código y prácticas en los servidores. Para algunas herramientas, esta es una petición inadmisible. Por ejemplo, Whonix, un sistema operativo centrado en el anonimato y la seguridad, basado en Linux, no se ha sometido a una auditoría de seguridad. Pero ningún sistema operativo se ha sometido a una auditoría de seguridad completa.
3. Una herramienta que brinde **anonimato** o **seudonimato** es más deseable. Podría incluso llegar a ser compatible con Tor. O podría facilitar la creación de cuentas seudónimas (por ejemplo, no solicitando un número telefónico o correo electrónico para registrarse).
4. Las **configuraciones por defecto** tienen un gran efecto en las prácticas de los usuarios. En el curso de los años hemos visto diversas aplicaciones de mensajería que no cuentan con cifrado habilitado por defecto. ¿Cuántos usuarios olvidarán habilitar el cifrado al iniciar una nueva conversación?
5. El **grado de centralización** de una herramienta puede tener un efecto en la calidad del servicio y modificar la cantidad de datos que controla una sola entidad. Por ejemplo, una app de comunicaciones puede enrutar todas las comunicaciones a través del servidor del proveedor o se puede usar al servidor para iniciar la comunicación y que a partir de ahí los datos transiten directamente entre los usuarios (a través de internet, pero no del servidor del proveedor). Esto último se conoce como *comunicación entre pares* (P2P, por su nombre en inglés) y puede mejorar la calidad de la llamada (puesto que acorta la distancia en la red), así como reducir la cantidad de metadatos disponibles para el proveedor (como la longitud de la llamada). Otra opción es permitir la *federación*. Consideremos, como ejemplo, el correo electrónico: se pueden enviar correos entre diferentes proveedores (por ejemplo, de Google a Microsoft). Por otro lado, Signal solo permite que dos usuarios se comuniquen si ambos usan Signal y establecen sus llamadas a través de servidores de Signal.

Criterios no técnicos

1. El **modelo financiero** de un proveedor puede influir en la posibilidad de acceder a una herramienta (si es necesario pagar por el acceso), en la estabilidad de largo plazo de la herramienta (¿qué pasa si se les acaba el dinero?) y en las motivaciones del proveedor (¿están monetizando tus datos o metadatos?). Las opciones van desde el acceso gratuito, pasando por el modelo *freemium* (el pago por servicios adicionales a los servicios gratuitos), hasta el modelo de pago para usar. Si una herramienta es gratuita, uno debería preguntarse por qué lo es. ¿La administra una gran compañía que puede monetizar los metadatos (como Facebook, que tiene acceso a las redes de contactos de WhatsApp)? ¿O es administrada gracias a donaciones y becas?
2. Si una herramienta está **orientada a movimientos**, esto podría ser positivo o negativo. Como

se analiza al final del capítulo Proteger tus comunicaciones, una opción de videollamadas no cifradas ofrecida por la organización orientada a movimientos May First resultaba más confiable que la opción de Zoom, del cual se sabe que se ha prestado a la censura y a compartir datos con autoridades. Por otro lado, una opción de VPN ofrecida por la organización orientada a movimientos Riseup podría llamar más la atención de las autoridades que simplemente esconderse entre los muchos usuarios de una VPN.

3. La **transparencia del proveedor** puede ayudar a crear confianza. La mayoría de las grandes compañías publican reportes de transparencia, como se discute en el capítulo Defensa contra la vigilancia y la represión. Sin embargo, en muchos casos estos reportes solo ponen de realce lo mucho que dichas compañías están dispuestas a compartir sus datos con tus oponentes. Otra opción es el *canario de seguridad*, que se examina en el capítulo Autenticarse mediante firmado criptográfico.

Qué aprender a continuación

Existen diversas guías y recursos que ahondan en temas relacionados con usuarios o aspectos específicos que recomendamos estudiar:

- Digital Defenders Partnership. "Digital First Aid Kit." Consultado el 9 de febrero de 2021.
- Electronic Frontier Foundation. "Security Education Companion." Consultado el 9 de febrero de 2021.
- Electronic Frontier Foundation. "Surveillance Self-Defense." Consultado el 9 de febrero de 2021.
- Tactical Technology Collective. "The Holistic Security Manual." Holistic Security. Consultado el 9 de febrero de 2021.
- Tactical Technology Collective and Frontline Defenders. "Digital Security Tools and Tactics." Security in a Box. Consultado el 9 de febrero de 2021.