Cifrado

Informe de la Internet Society

03 June 2016

Introducción

El cifrado está en todas partes. Se utiliza para proteger los datos que se envían desde todo tipo de dispositivos a través de todo tipo de redes. Además de proteger contraseñas y documentos almacenados y que son "solo para sus ojos", el cifrado se utiliza para proteger la información que se intercambia cada vez que alguien utiliza un cajero automático, realiza una compra desde su *smartphone*, hace una llamada desde su teléfono móvil o presiona un botón de su llavero remoto para abrir su automóvil. Se trata de una tecnología versátil cada vez más omnipresente en nuestra vida diaria y es fundamental para la seguridad de gran parte de lo que hacemos.

El cifrado electrónico, es decir, el proceso de transformar o encriptar los datos de manera que solo puedan ser leídos por quien tenga los medios necesarios para devolverlos a su estado original, se utiliza comúnmente para proteger los datos almacenados en los sistemas informáticos y los datos transmitidos a través de redes informáticas, entre ellas Internet. En el caso de los datos comunicados a través de una red, el cifrado moderno transforma los datos usando una clave o valor secreto que solo conocen el destinatario y el remitente. En el caso de los datos almacenados, este valor secreto normalmente solo es conocido por su propietario.

El cifrado y sus técnicas relacionadas también se utilizan para construir mayor seguridad para las transacciones financieras y proteger las comunicaciones privadas de los usuarios finales. A modo de ejemplo podemos mencionar la posibilidad de establecer si los datos han sido manipulados (integridad de los datos), aumentar la confianza de los usuarios con respecto a que se están comunicando con los destinatarios que pretendían (autenticación), y formar parte de los protocolos que proporcionan la prueba de que los mensajes fueron enviados y recibidos (no repudio).

Las tecnologías de cifrado permiten que los usuarios de Internet protejan la confidencialidad de sus datos y comunicaciones contra la vigilancia y las intrusiones no deseadas. El cifrado también proporciona una base técnica para la confianza en Internet. Promueve la libertad de expresión, el comercio, la privacidad y la confianza de los usuarios, a la vez que ayuda a proteger los datos contra actores malintencionados. Por estas razones, la Internet Society cree que el cifrado debería ser la norma para el tráfico y el almacenamiento de datos en Internet.

Dado que ciertos actores malintencionados pueden utilizar el cifrado para ocultar sus actividades o secuestrar datos de los usuarios (por ejemplo, usando ransomware[1]), algunos miembros tanto de las agencias de seguridad gubernamentales como de las fuerzas del orden han expresado su preocupación con respecto al impacto negativo que el cifrado podría tener sobre su capacidad de aplicar la ley y proteger a los ciudadanos.

La Internet Society reconoce las preocupaciones de las fuerzas del orden y se mantiene firme en su convicción de que el cifrado es una solución técnica importante que todos los usuarios de Internet —individuos, gobiernos, empresas y otras comunidades— deberían utilizar para proteger sus comunicaciones y sus datos. Creemos que, bien intencionado o no, cualquier intento legal y/o técnico de limitar el uso del cifrado tendrá un impacto negativo sobre la seguridad de los ciudadanos respetuosos de la ley.

Consideraciones clave

En la práctica, el cifrado toma las siguientes formas generales:

- **El cifrado simétrico** utiliza una clave idéntica para cifrar y descifrar el mensaje. Tanto el emisor como el receptor tienen acceso a la misma clave. Aunque es rápido y eficaz desde el punto de vista de las computadoras, si se utiliza cifrado simétrico hay que verificar que la clave se entregue al destinatario de forma confiable y que no caiga en las manos equivocadas.

- También conocido como cifrado de clave pública, el **cifrado asimétrico** es una forma de cifrado unidireccional. Las claves vienen de a pares y la información cifrada con la clave pública solo puede ser descifrada usando la clave privada correspondiente. El receptor publica públicamente una clave para que el emisor cifre sus datos. Luego el destinatario utiliza una clave privada para descifrarlos. Este tipo de cifrado es similar a un buzón con candado, al que se puede entregar correspondencia a través de una ranura pero solo la puede recuperar el propietario con ayuda de su llave. El cifrado de clave pública es más seguro que el cifrado simétrico, ya que no hay necesidad de trasferir la clave.

- **Cifrado de extremo a extremo** es cualquier forma de cifrado en la que solo el remitente y el destinatario pueden leer el mensaje. El aspecto más importante del cifrado de extremo a extremo es que ningún tercero, ni siquiera la parte que proporciona el servicio de comunicación, conoce la clave de cifrado. Los ejemplos de cifrado de extremo a extremo incluyen los protocolos PGP (Pretty Good Privacy) y OTR (Off-the-Record Messaging). Los ejemplos de servicios de comunicación con cifrado de las comunicaciones incluyen iMessage de Apple,Telegram y Threema. Electronic Frontier Foundation ha publicado una tarjeta de puntuación para servicios de mensajería[1] que ofrece información sobre las características de diversas aplicaciones.

- **Cifrado de datos en reposo** es cualquier forma de cifrado que protege los datos físicamente almacenados en forma digital (por ejemplo, en computadoras, discos de almacenamiento, dispositivos móviles o la Internet de las Cosas).

En la práctica, el cifrado se aplica por capas. Por ejemplo, un usuario cifra sus mensajes de correo electrónico usando PGP o S/MIME (Secure/Multipurpose Internet Mail Extensions) y el proveedor de correo electrónico (por ejemplo, Gmail) cifra la transmisión de los mensajes usando HTTPS.

Es importante tener en cuenta que el cifrado no necesariamente implica que todos los datos de la comunicación serán ilegibles. Por ejemplo, los metadatos de las comunicaciones (incluyendo los identificadores de remitente y destinatario, la longitud del mensaje, la localización, la fecha y la hora, y los datos utilizados por las fuerzas de aplicación de la ley) pueden estar disponibles en texto plano.

Desafíos

1 Ver https://www.eff.org/secure-messaging-scorecard.

Junto con su naturaleza versátil y a su uso por parte de diferentes actores, la amplia disponibilidad del cifrado presenta una serie de desafíos.

- L**ibertad de expresión, anonimato y abuso.** Las tecnologías de cifrado facilitan las comunicaciones anónimas, un potencial salvavidas para ciudadanos y activistas en regímenes opresivos y personas en comunidades vulnerables, como por ejemplo las víctimas de violencia doméstica, las personas incluidas en los programas de protección de testigos y los policías encubiertos. Sin embargo, esta misma tecnología también puede ayudar a los actores malintencionados a esconder sus actividades y comunicaciones con ayuda de herramientas de anonimato y así dedicarse al ciberacoso y otras formas de abuso en línea.

  La Internet Society reconoce el legítimo objetivo de los estados nacionales de proteger a sus ciudadanos, pero advierte contra los intentos de regular la tecnología para impedir que los delincuentes se comuniquen de forma confidencial. Este enfoque pone en riesgo la capacidad de los ciudadanos respetuosos de la ley de proteger la confidencialidad de sus datos y comunicaciones y pone en peligro sus derechos de privacidad, libertad de expresión y opinión. Tal como se describe en nuestro informe Seguridad colaborativa[2], el objetivo general de la seguridad debería ser fomentar la confianza en Internet y garantizar el éxito continuado de Internet como motor de innovación económica y social.

- **Tensión entre seguridad y privacidad.** Los debates en torno a las políticas sobre cifrado suelen presentar el tema como un enfrentamiento entre la seguridad y la privacidad, una búsqueda de equilibrio entre la responsabilidad de los gobiernos de proteger a sus ciudadanos y los derechos de los ciudadanos de proteger su privacidad contra intrusiones gubernamentales, comerciales o criminales. La Internet Society sostiene que seguridad y privacidad no son conceptos necesariamente irreconciliables. Por el contrario, pueden reforzarse mutuamente: la confianza de los usuarios surge a partir de una sensación tanto de privacidad como de seguridad. Por ejemplo, la confianza en que un mensaje estará seguro (solo lo leerá el destinatario) contribuye al florecimiento de una variedad de servicios en Internet, particularmente el comercio electrónico.

- **Puertas traseras de cifrado.** Se refiere a la idea de que una herramienta puede ayudar a que un tercero no autorizado acceda y descifre datos cifrados sin tener acceso a las claves. Estas puertas traseras también permitirían acceder al contenido de forma encubierta. El consenso entre los técnicos[3] es que la introducción de puertas traseras mediante cualquiera de las técnicas que hoy en día se proponen pone en riesgo a los usuarios legítimos y es poco probable que evite que los criminales se comuniquen de forma clandestina. Los actores maliciosos probablemente encontrarán medios de comunicación alternativos, mientras que los usuarios promedio quizás no tendrán a su alcance las mismas herramientas. Esto podría tener un doble efecto: las comunicaciones de los

2 Ver http://www.internetsociety.org/collaborativesecurity.
3 Ver Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Declaración del IAB sobre confidencialidad en Internet, W3C TAG Finding: End-to-End Encryption and the Web, Hallazgo del W3C TAG: Securing the Web, Publicación en el blog de M3AAWG: MAAWG Endorses "Keys Under Doormats" End-to-End Encryption Recommendations, y el comunicado de prensa de WITSA: Global ICT Industry Opposes Backdoor Decryption.

criminales podrían continuar inmunes a la vigilancia mientras que las comunicaciones de los usuarios podrían quedar en una situación de vulnerabilidad frente a las actividades de intercepción por parte de los gobiernos o de actores malintencionados que hayan descubierto cómo explotar las puertas traseras.

- **Tecnología resistente a la manipulación.** Si hablamos de cifrado, la tecnología resistente a la manipulación (*tamper-resistant technology*) tiene dos objetivos: primero, hacer que sea difícil para los atacantes modificar la tecnología; segundo, dejar en evidencia cualquier manipulación. Utilizadas conjuntamente con el cifrado, las medidas antimanipulación pueden ayudar a evitar (1) el ingreso a un dispositivo después de varios intentos de conexión; y (2) la instalación de puertas traseras de cifrado, *rootkits* (código malicioso diseñado para acceder a diferentes áreas de una computadora sin autorización) y otros tipos software malicioso. En los últimos años, la tendencia ha sido hacia un mayor uso de tecnología y mecanismos resistentes a la manipulación que automáticamente borran los datos si se dan determinadas condiciones (por ejemplo, después de 10 intentos fallidos de introducir una contraseña). Aunque la tecnología resistente a la manipulación ayuda a proteger la integridad de la tecnología, también puede generar dificultades cuando las fuerzas de la ley intentan obtener acceso a las comunicaciones y los datos de los actores maliciosos en cumplimiento de una orden judicial[4].
-

Principios rectores

La Internet Society ofrece los siguientes principios rectores para las políticas:
Confidencialidad y anonimato. Para apoyar la libre expresión de los derechos humanos –entre ellos la privacidad y la libertad de expresión–, las personas deben poder comunicarse a través de Internet de forma confidencial y anónima.

- **Seguridad de los datos.** Así como los individuos tienen derecho a proteger sus activos y su propiedad fuera de línea, también deberían tener el derecho de utilizar cifrado y otras herramientas para proteger sus datos, activos digitales y actividades en línea. Alentamos al desarrollo abierto y la amplia disponibilidad de tecnologías de seguridad de datos.

- **Confianza.** La confianza de los usuarios es fundamental para el crecimiento y la evolución de Internet. Además, cada vez más usuarios se están dando cuenta del valor que tiene el uso de aplicaciones y servicios seguros y respetuosos de la privacidad. Fomentamos la inclusión de mecanismos confiables para la autenticación, la confidencialidad y la integridad de los datos como componentes vitales para la construcción de productos y servicios de confianza. También creemos que los marcos legales deben apoyar los derechos humanos, entre ellos el derecho a la privacidad.

- **Cifrado.** El cifrado debería ser la norma para todo el tráfico de Internet. El trabajo en este sentido es una importante adición a los esfuerzos que está

4 Este problema es el meollo de un caso reciente presentado ante el Tribunal de Distrito del Distrito Central de California que involucra a la Oficina Federal de Investigaciones de Estados Unidos y a Apple.

realizando la comunidad técnica para abordar la vigilancia omnipresente. Se recomienda a los diseñadores y desarrolladores de productos y servicios digitales verificar que los datos de los usuarios, ya sea archivados o comunicados, estén cifrados por defecto. Siempre que sea posible, se deberían implementar soluciones de cifrado de extremo a extremo. Además, se anima a los operadores de redes y servicios a desplegar cifrado donde aún no se haya desplegado, y se insta a los administradores de políticas de firewall a que permitan el paso de tráfico cifrado.

- **Tecnología resistente a la manipulación.** Se debería continuar desarrollando e implementando tecnología resistente a la manipulación que apoye al cifrado. Los gobiernos no deberían exigir el diseño de vulnerabilidades en las herramientas, tecnologías o servicios. Además, los gobiernos no deberían exigir que las herramientas, tecnologías o servicios sean diseñados o desarrollados para permitir que terceros accedan al contenido de los datos cifrados. Los gobiernos también deberían apoyar el trabajo de los investigadores en el área de la seguridad y de otras personas que identifican y divulgan de manera responsable las vulnerabilidades de seguridad y privacidad detectadas.

- **Despliegue.** Un mayor despliegue de mecanismos de seguridad tales como el cifrado generará desafíos para el diseño, el desarrollo, la gestión y la usabilidad de las redes. La gestión de redes, la detección de intrusiones y la prevención del correo no deseado (*spam*) enfrentarán nuevos requisitos funcionales y es de esperar que surjan nuevos desafíos económicos y de políticas.

- **Soluciones de múltiples partes interesadas.** Los criminales se pueden comunicar de forma confidencial y anónima. Confrontar con éxito las repercusiones requiere la acción concertada de múltiples partes interesadas. La Internet Society reafirma su compromiso de facilitar la participación de todas las partes interesadas y de desempeñar un papel activo y técnicamente informado en el desarrollo de soluciones.

Además, la Internet Society ha firmado la petición "Secure the Internet"[5] en apoyo a los principios de la misma, es decir, que los gobiernos no deberían:

- Prohibir ni limitar el acceso de los usuarios a las tecnologías de cifrado, prohibir el uso de cifrado por grados o tipos;

- Exigir el diseño o la implementación de "puertas traseras" (*backdoors*) o vulnerabilidades en herramientas, tecnologías o servicios;

- Requerir que las herramientas, tecnologías o servicios sean diseñados o desarrollados para permitir el acceso de terceros a datos sin cifrar o a las claves de cifrado;

- Tratar de debilitar o socavar los estándares de cifrado o influir intencionalmente en su desarrollo, a menos que sea para promover un mayor nivel de seguridad de la información;

5 Ver https://www.securetheinternet.org/.

- Exigir algoritmos, estándares, herramientas o tecnologías de cifrado inseguros;

- Obligar o presionar a cualquier entidad, por acuerdo público o privado, para que participe en actividades que no sean compatibles con sus principios.

Otros recursos

La Internet Society ha publicado varios *papers* y otros contenidos relacionados con este tema. Estos materiales están disponibles de forma gratuita en el sitio web de la Internet Society y muchos se pueden consultar en nuestra página sobre cifrado (https://www.internetsociety.org/encryption).

Publicaciones de la Internet Society

- Internet Society responde a los informes según los cuales el gobierno de Estados Unidos puede eludir las tecnologías de encriptación, https://www.internetsociety.org/news/internet-society-responds-reports-us-government's-circumvention-encryption-technology

- Internet Society Commends Internet Architecture Board Recommendation on Encryption-by-Default for the Internet, https://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default

- Internet Society Submission to the U.N. Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression and Opinion Regarding the Use of Encryption and Anonymity in Digital Communications, http://www.internetsociety.org/doc/internet-society-submission-un-special-rapporteur-protection-and-promotion-right-freedom

Entradas de blog

- Freedom of Speech: Rethinking the Role of Encryption, https://www.internetsociety.org/blog/2013/05/freedom-speech-rethinking-role-encryption

- Encryption Backdoors Decrease Trust In The Internet, https://www.internetsociety.org/blog/tech-matters/2015/05/encryption-backdoors-decrease-trust-internet

- Strong Support From The UN Special Rapporteur David Kaye For Anonymity And Encryption, http://www.internetsociety.org/blog/public-policy/2015/06/strong-support-un-special-rapporteur-david-kaye-anonymity-and-encryption

- No keys under the doormat please, https://www.internetsociety.org/blog/public-policy-tech-matters/2015/08/no-keys-under-doormat-please

- The Fundamental Tension Between Safety And Privacy (And The UK's Proposed Encryption Ban), https://www.internetsociety.org/blog/public-

policy/2015/01/fundamental-tension-between-safety-and-privacy-and-uks-proposed

- Internet Society Supports the Let's Encrypt Initiative to Increase End-to-End Encryption, https://www.internetsociety.org/blog/tech-matters/2015/10/isoc-supports-lets-encrypt-initiative-increase-end-end-encryption

- Imagine an encrypted world! A workshop at IGF, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/11/imagine-encrypted-world-workshop-igf-2015

- Encryption and law enforcement: aiming for trust, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/12/encryption-and-law-enforcement-aiming-trust

- Let's Encrypt Enters Public Beta to Increase Encryption on the Internet, https://www.internetsociety.org/blog/tech-matters/2015/12/lets-encrypt-enters-public-beta-increase-encryption-internet

- Internet Society signs "Secure the Internet" Online Petition, http://www.internetsociety.org/blog/tech-matters/2016/02/internet-society-signs-secure-internet-online-petition

- Encryption Backdoors Come In All Guises - Reacting to Apple's Customer Letter, https://www.internetsociety.org/blog/public-policy/2016/02/encryption-backdoors-come-all-guises-reacting-apples-customer-letter

Presentaciones e informes de talleres

- Barriers to Deployment: Probing the Potential Differences in Developed and Developing Infrastructure, https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_27.pdf