ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

53/2015 18 noviembre de 2015

David Ramírez Morán

AFRONTANDO EL PROBLEMA DEL CIFRADO EN INTERNET

AFRONTANDO EL PROBLEMA DEL CIFRADO EN INTERNET

Resumen:

El cifrado de la información ha sido identificado por algunos Estados como una herramienta que facilita la acción de los delincuentes al permitir establecer comunicaciones que no se pueden intervenir, dificultar la atribución de los delitos que se cometen a través de las redes y complicar la investigación de actos delictivos al impedir el acceso a pruebas e información almacenadas en soportes digitales.
Se han planteado distintas alternativas que van desde la prohibición del uso del cifrado a la implantación de medidas que permitan a las autoridades acceder a la información. Los planteamientos responden a fines orientados a la seguridad y la defensa, aunque también suponen un riesgo ante la posibilidad de que terceras partes sean también capaces de acceder ilícitamente a la información a través de estos mecanismos.
Se plantea así un profundo dilema entre seguridad y privacidad, referida esta última no solo a los datos personales de los individuos, sino también a la información que intercambian los gobiernos, las empresas, las instituciones y las propias personas entre sí.

Abstract:

Information encryption has been identified by several states as a tool that easies the action of criminals by allowing the establishment of communication links that cannot be tapped, the attribution of the crimes by means of the networks and obstructing the investigation of crimes as they hinder the access to evidences and information stored on digital media.
Several alternatives have been proposed ranging from the full prohibition of the use of encryption to the implantation of measures that provide the authorities access to the information. The alternatives respond to aims focused on security and defence, although they also pose risks given the possibility that third parties might also be able to illegally access the information by these mechanisms.
So it stands a sound dilemma between security and privacy, referring this last not only to people's personal data, but also the information interchanged by governments, businesses, institutions and even individuals among them.

Palabras clave: Internet, cifrado, estados, puertas traseras, políticas

Keywords: Internet, encryption, states, backdoors, policies.

INTRODUCCIÓN

Los primeros usos de técnicas de cifrado se remontan al antiguo Egipto, hace más de 4.000 años, aunque hasta más de 1500 años después no existen evidencias de la utilización de estas técnicas para la protección de información. A lo largo de la historia la evolución del cifrado ha estado íntimamente relacionada con actividades como la seguridad, la política, el espionaje o la guerra. Así, cuando se trata el tema del cifrado y la intercepción de la información, uno de los primeros escenarios que viene a la cabeza es la máquina Enigma y su uso para el cifrado de las comunicaciones del ejército alemán durante la Segunda Guerra Mundial.

Con la popularización de internet como herramienta del día a día, el cifrado de la información ha trascendido estos entornos y ha pasado a convertirse en un elemento fundamental para la actual sociedad de la información.

En el ámbito de las organizaciones se ha convertido en un medio imprescindible para la distribución de una información que en muchos casos debe ser mantenida en secreto por motivos de confidencialidad, de competitividad, de secreto (industrial o comercial), etc.

Del mismo modo, las constantes advertencias para que los usuarios se aseguren de que están accediendo a las páginas seguras (*https)* en sus transacciones a través de internet no hace más que fomentar el cifrado de la información con vistas al uso seguro de internet por los ciudadanos: fines que persiguen tanto la Estrategia Europea de Ciberseguridad como la Estrategia Nacional de Ciberseguridad.

El cifrado es una herramienta de seguridad imprescindible a día de hoy, aunque también está siendo utilizada por actores que pueden aprovechar sus características con fines delictivos. La posibilidad de establecer comunicaciones cifradas instantáneas facilita la labor de intercambio de información entre delincuentes, a la vez que supone un escollo, en muchas ocasiones insalvable, para la prevención e investigación de estos delitos.

El cifrado es también una de las herramientas que contribuye, aunque no es la única, a la dificultad de atribución[1] de las acciones llevadas a cabo a través de internet. Es la tecnología que permite el funcionamiento de las redes privadas virtuales[2], entre las que se incluye The Onion Router (TOR) como ejemplo más conocido, que permiten anonimizar las conexiones y dificultar la determinación del ordenador desde el que se está realizando una conexión.

[1] Identificación de la persona o el ordenador
[2] Luis de Salvador. Redes de anonimización en internet: cómo funcionan y cuáles son sus límites Documento de Opinión 12/2012. Instituto Español de Estudios Estratégicos

Por lo tanto, el uso con fines delictivos de sistemas de comunicación y las redes privadas virtuales han llevado a varios Estados a plantearse cómo hacer frente a los problemas que el cifrado supone para la investigación de los delitos.

¿POR QUÉ CIFRAR LA INFORMACIÓN?

El secreto de las comunicaciones es un derecho protegido legalmente en la mayor parte de los países, entre los que se incluyen todos los de la Unión Europea. El mero hecho de intentar acceder a información de terceros constituye un ilícito con consecuencias penales. De hecho, de un tiempo a esta parte, se ha sucedido la actualización de las legislaciones nacionales para incluir los nuevos escenarios que han surgido con la eclosión de internet, aunque se mantiene, en todo caso, el principio de que las comunicaciones son inviolables, salvo con motivo de la investigación de delitos.

Desde este punto de vista no sería necesario que los usuarios tuvieran acceso a tecnologías de cifrado dado que la privacidad de su información ya se encuentra protegida. En la práctica, las consecuencias asociadas a que una tercera persona acceda a cierta información pueden ser irreversibles, haciendo insuficiente la protección que proporcionan las medidas legislativas. Los usuarios deben contar con las herramientas necesarias para hacer un uso seguro de los sistemas de información y es aquí donde entra en juego el uso del cifrado.

Cada vez se está produciendo una mayor concienciación de los ciudadanos sobre la repercusión que puede tener que terceras personas conozcan información privada, como las ausencias del domicilio, las costumbres, etc. Surge así la demanda a los prestadores de servicios y a los desarrolladores de aplicaciones de comunicación para que sus herramientas cifren la información en tránsito. Se dificulta así el acceso a la información en los puntos más críticos, como son la conexión del terminal del usuario a internet, que en muchos casos se realiza en condiciones de seguridad insuficientes. Estas capacidades de cifrado se han popularizado y se encuentran actualmente a disposición de la práctica totalidad de la ciudadanía, y, aunque fueron creadas con fines lícitos, se han convertido también en herramientas útiles para fines delictivos. A pesar de que actualmente se cuenta con estas herramientas de forma mucho más accesible, ya en 2001 se identificó el uso de las técnicas de cifrado para la coordinación de atentados terroristas.[3]

[3] Terror groups hide behind Web encryption http://usatoday30.usatoday.com/tech/news/2001-02-05-binladen.htm

LO QUE PLANTEAN LOS PAÍSES

Poco después del atentado de París al semanario Charlie Hebdo, el primer ministro de Reino Unido, David Cameron, denunció la existencia de sistemas de comunicación que permiten cifrar la información e impiden la intervención de las comunicaciones por parte de los servicios de seguridad, ni siquiera bajo petición judicial.

> «We want to allow a means of communication between two people which even *in extemis* with a signed warrant from the home secretary personally that we cannot read? ... My answer to that question is no, we must not. The first duty of any government is to keep our country and our people safe».[4]

Poco después el presidente Barack Obama[5] se alineaba con la iniciativa del Primer Ministro por la que se planteaba la implantación de medidas que posibilitaran el acceso por parte de las fuerzas de seguridad a la información de las comunicaciones cifradas.

El director del FBI hacía en el mes de julio, ante el Comité Judicial del Senado, una declaración[6] contrastando lo que denominaba como «going dark», que podría traducirse como «quedar a ciegas», con las implicaciones sobre la privacidad de los ciudadanos y las medidas legislativas con las que se restringen estrictamente las condiciones que deben cumplirse para que las fuerzas de seguridad puedan acceder a la información. Manifestaba así la necesidad de disponer de las herramientas que permitieran acceder al contenido de esas comunicaciones cifradas con fines de seguridad, a la vez que defendía el derecho a la privacidad.

El Gobierno de Estados Unidos también pidió al *Grupo de Trabajo sobre Cifrado* que realizara una investigación sobre las alternativas e implicaciones de la implantación de medidas para hacer posible el acceso a la información de este tipo de comunicaciones. El borrador del informe que se filtró a la prensa[7] incluía lecciones aprendidas durante la elaboración del informe, algunos desafíos técnicos que debían considerarse y consideraciones a tener en

[4] http://uk.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1

[5] Obama Sides with Cameron in Encryption Fight http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/

[6] https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

[7] Obama administration explored ways to bypass smartphone encryption https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html

cuenta en la elaboración de políticas al respecto[8].

Se identificaron cuatro lecciones aprendidas:

- No existe una solución técnica única que dé acceso a todos los sistemas y todos los medios. Cada empresa tendría que desarrollar aproximaciones técnicas específicas e sus productos y servicios.

- Las distintas implementaciones del cifrado requieren aproximaciones diferentes para afrontar los riesgos, implicaciones políticas, así como los mecanismos para limitar la cantidad de información a la que se puede acceder de acuerdo a la situación particular.

- Cada escenario de cifrado requiere técnicas diferentes según se trate, por ejemplo, de intervenir una comunicación instantánea, acceder a información en un disco duro en posesión del usuario, acceder a la información de ese mismo duro una vez requisado, etc.

- El acceso indiscriminado a toda la información podría ser objeto de rechazo por amplios sectores que podrían ver insuficientes las acciones legislativas. Podrían considerar una solución de compromiso la implantación de medidas tecnológicas de filtro dela cantidad de información a la que se tiene acceso.

También se resaltaron los siguientes desafíos técnicos:

- Durante los años 90 el uso de técnicas de cifrado fuerte estaba reservado a los estados mientras que en la actualidad existe una mayor accesibilidad a estas tecnologías.

- No existe una autoridad única a la que requerir que las soluciones incorporen los mecanismos de acceso para los servicios de seguridad debido al uso de software libre para la implementación de productos y servicios.

- El cifrado se puede apilar, es decir, es posible cifrar la información con un algoritmo comprometido y, previamente, aplicar otro cifrado adicional que no se adaptara a las medidas desarrolladas y además de forma no demasiado complicada. Se impediría así el objetivo de tener acceso a la información.

[8] https://assets.documentcloud.org/documents/2430092/read-the-obama-administrations-draft-paper-on.pdf

Por último, con objeto de minimizar el impacto y limitar los riesgos asociados se propusieron ocho principios que deberían tenerse en cuenta en caso de implantar este tipo de técnicas.

- La recolección de información debe estar enfocada y no ser masiva.
- Evitar que el gobierno pueda acceder de forma opaca sin participación de un tercero.
- Imponer tecnologías que limiten el acceso y frente al uso de límites solo regulatorios.
- Adopción internacional de la solución propuesta por EE.UU.
- Maximizar la seguridad y minimizar la complejidad.
- Minimizar el impacto de una explotación maliciosa de estos medios de acceso.
- Minimizar los impactos negativos en la innovación.
- Los proveedores deberían diseñar soluciones para sus productos y servicios pues no hay una solución única para todos los escenarios.
- Evitar minar la confianza en la seguridad.

Finalmente Estados Unidos ha descartado[9] la implantación oficial de este tipo de medidas ante la sospecha fundada de que el intento fallara política y tecnológicamente. Estas medidas podrían incrementar el riesgo de que, en palabras del presidente Obama, China, Rusia, cibercriminales y grupos terroristas también tuvieran acceso a la información.

No cabe duda de que las consecuencias económicas para las empresas americanas serían devastadoras. Después de lo que ha ocurrido con la declaración de la invalidez del acuerdo Safe Harbor entre la UE y EEUU, esto supondría el freno definitivo a su actual tendencia hacia la nube y a la prestación de servicios frente a la venta de paquetes de software de ejecución local.

Reino Unido está desarrollando una nueva ley[10] que dota a los servicios de seguridad de mayor capacidad para acceder a la información, incluyendo la obligación de que las empresas proporcionen las claves de cifrado de las comunicaciones cuando les sean solicitadas.

[9] Obama Won't Seek Access to Encrypted User Data http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html

[10] UK surveillance powers explained http://www.bbc.com/news/uk-34713435

CONCLUSIONES

La facilidad con la que se puede acceder a técnicas de cifrado fuerte por la práctica totalidad de los internautas se ha identificado como un vector de riesgo porque permite que los delincuentes puedan aprovechar todas las ventajas de los sistemas de información. La imposibilidad de acceder a la información que circula por estos sistemas supone un riesgo para la prevención y la investigación de delitos.

Las soluciones propuestas pasan por dotar a los sistemas de mecanismos que permitan a los servicios de seguridad acceder a esta información. Sin embargo la implantación de este tipo de sistemas también puede tener un coste muy superior a los beneficios que reporta. Un ejemplo de ello es que la flexibilidad de las tecnologías también hace fútiles estas aproximaciones, dada la facilidad con la que se pueden incorporar técnicas de cifrado adicionales o implementar vías de comunicación segura alternativas.

Las contrapartidas asociadas a la implantación de medidas de acceso a la información tienen un desorbitado impacto, que podría frenar en seco la expansión del uso de las tecnologías de la información. Ante esta situación, los gobiernos están siendo muy cautos en la implementación de estas medidas. Es necesario un análisis preciso del compromiso entre beneficio y consecuencias antes de legislar en esta línea, porque son muchos los derechos, aspectos y actores involucrados.

David Ramírez Morán
Analista del IEEE