Trazabilidad y ciberseguridad

Ciclo de talleres para expertos sobre el cifrado en la India

Noviembre de 2020

La trazabilidad, o la capacidad de rastrear al originador de un determinado contenido o mensaje, se sitúa en el centro del debate en torno a las normas de las plataformas en línea y los proveedores de comunicaciones que se está llevando a cabo en la India. A fines de 2018, el Ministerio de Electrónica y Tecnología de la Información (MeiTy) de la India propuso modificaciones a las Normas sobre Tecnología de la Información (Directrices para intermediarios) en virtud de la ley sobre Tecnología de la Información.[1] Entre las modificaciones propuestas se incluye una demanda de trazabilidad, descrita como "permitir el rastreo de tal originador[2] de información en su plataforma". La modificación pondría la responsabilidad por el contenido publicado por los usuarios en el proveedor o la plataforma de Internet, en caso de no proporcionarse trazabilidad. A principios de 2019, el MeiTy invitó al público a comentar la modificación preliminar[3] y, además, unos 30 expertos en ciberseguridad y cifrado enviaron una carta abierta al MeiTy, en la que expresaron inquietudes sobre las modificaciones propuestas a principios de 2020.[4] La trazabilidad está asimismo en debate en un caso actual del Tribunal Supremo de Madrás entre varias plataformas en línea importantes y el gobierno a propósito del acceso por parte de las fuerzas de seguridad al contenido que generan los usuarios.[5]

En el centro del debate en curso se plantean preguntas sobre:

- la viabilidad de la trazabilidad dentro de las comunicaciones con cifrado de extremo a extremo[6]
- qué métodos están disponibles para habilitar la trazabilidad, y
- cuáles son las ramificaciones de cada uno.

Dos técnicas, el **uso de firmas digitales** y el **uso de metadatos**, se han propuesto como métodos para lograr la trazabilidad en las comunicaciones de extremo a extremo, tales como aplicaciones de envío de mensajes (p. ej., WhatsApp). No obstante, para cumplir los requisitos de trazabilidad, puede que las plataformas se vean obligadas a permitir el acceso al contenido de las comunicaciones de sus usuarios, **rompiendo el cifrado de**

1 Normas sobre tecnología de la información [Directrices para intermediarios (Modificación)].
2 En virtud de la Ley sobre tecnología de la información de la India, un originador se define como "la persona que envía, genera, almacena o transmite cualquier mensaje electrónico o hace que un mensaje electrónico se envíe, genere, almacene o transmita a otra persona pero no incluye un intermediario"
3 https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf
4 https://www.internetsociety.org/open-letters/india-intermediary-guidelines/
5 https://www.medianama.com/2019/09/223-sc-adjourns-hearing-on-facebook-transfer-petition-till-september-24/
6 El cifrado de extremo a extremo (E2E), donde las claves necesarias para descifrar una comunicación cifrada residen solo en los dispositivos que se comunican, proporciona el mayor nivel de seguridad y confianza, porque debido al diseño, solo el destinatario tiene la clave para descifrar el mensaje.

extremo a extremo y debilitando de manera considerable la seguridad y la privacidad de su producto, a fin de habilitar la trazabilidad.

En una serie de debates bajo la Regla de Chatham House que llevó a cabo Internet Society en colaboración con Medianama, un grupo internacional de expertos en ciberseguridad y políticas examinó el asunto de la trazabilidad de los mensajes en el contexto de la India. Los expertos tuvieron importantes inquietudes en torno a los dos métodos técnicos frecuentemente propuestos para habilitar la trazabilidad: el uso de firmas digitales y el uso de metadatos. No solo se citaron como amenazas a la privacidad y la seguridad de los usuarios, sino que también se puso en duda su capacidad para atribuir un mensaje a su originador de manera fiable. Habilitar el acceso de terceros al contenido de las comunicaciones de los usuarios a fin de posibilitar la trazabilidad plantea inquietudes adicionales sobre seguridad y privacidad.

Firmas digitales

Algunos recomendaron que se añada la firma digital del remitente[7] a los mensajes, para poder identificar al originador del mensaje. Por ejemplo, en el caso del Tribunal Supremo de Madrás, el doctor V. Kamakoti propuso la utilización de firmas digitales para rastrear al originador de un mensaje reenviado dentro de WhatsApp.[8] En la propuesta de Kamakoti, la firma del originador sería visible a todos en la cadena de mensajes o estaría cifrada utilizando una clave pública suministrada por WhatsApp. Utilizando la clave privada correspondiente, WhatsApp podría descifrar la información del originador si hay una orden judicial.

Sin embargo, son muchos quienes plantean inquietudes en cuanto al uso de las firmas digitales para posibilitar la trazabilidad, inclusive los expertos que participan en los debates de Internet Society:

- **La atribución digital no es absoluta y es vulnerable a la suplantación de identidad:** para que haya responsabilidad penal, se debe demostrar culpa sin dejar lugar a dudas razonables; un requisito difícil de satisfacer, en especial dadas la facilidad y la extensión de la suplantación de identidad en Internet. Es muy difícil probar que la persona A, el usuario del celular/la computadora A, efectivamente envió aquellos mensajes dirigiendo una campaña de desinformación, incluso si las fuerzas de seguridad tienen la id. del remitente. Para determinar si el *uso* del dispositivo de una persona constituye necesariamente una prueba del *uso del dispositivo por parte de la persona* se requiere información adicional.[9] Más preocupante aun es que usuarios inocentes puedan verse implicados en conductas ilícitas debido al obrar de criminales cibernéticos que suplantan sus identidades de remitente. Esta inquietud se reflejó en la propia respuesta de WhatsApp a la propuesta de Komakoti, en la que señalaron que "actores maliciosos podrían usar versiones modificadas de la aplicación de WhatsApp para atribuir un número telefónico diferente a un mensaje".[10]

- **Las firmas digitales agregan vulnerabilidades.** Las claves privadas para firmas digitales, en especial si las guarda un tercero ajeno a la conversación, como el proveedor del servicio de comunicación, serían un blanco valioso para los actores maliciosos. En la propuesta de Kamakoti, por ejemplo, un tercero comprometido tendría el potencial de ver cuándo un usuario determinado envía un mensaje, al recibir y descifrar la información del originador. Si se utiliza mal, el enfoque de la \"firma digital\" amenaza gravemente la libertad de expresión de los ciudadanos y puede exponer a los individuos (inclusive los más vulnerables y marginados) a suplantaciones de identidad, acosos y persecuciones.

7 Una firma digital es un mecanismo que garantiza la autenticidad de un mensaje o la información que se envía. Le permite al remitente del mensaje adjuntar un código que actúa como firma. De manera similar a la firma manuscrita de una persona, es única para cada firmante, y se puede comparar con un cierre a prueba de manipulaciones que garantiza que la información no se ha alterado de manera alguna desde su envío.

8 https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/

9 Por ejemplo, otra persona puede estar utilizando su dispositivo.

10 https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/

- **La funcionalidad entre plataformas sería inviable.** Puesto que los distintos servicios y plataformas están regulados por protocolos diferentes, los métodos que intentarían funcionar entre plataformas serían inviables. La trazabilidad entre plataformas también es difícil en sistemas federados como el correo electrónico o Chat de relé de Internet (IRC). Los métodos que proporcionan trazabilidad entre distintas plataformas, como usar la misma firma digital obligatoria en el texto de cada mensaje de cada plataforma a nivel mundial, serían difíciles de implementar. Posiblemente se requeriría un registro central de *cada* dispositivo y *cada* cliente de la aplicación en el mundo para autenticar las firmas digitales. Esto resultaría altamente perjudicial para la innovación, puesto que los desarrolladores de todas partes del mundo se verían obligados a coordinar su desarrollo con los operadores de la base de datos central. Además, una firma digital obligatoria supondría mayores riesgos de privacidad y seguridad para los usuarios como un único punto de falla, o un único punto para que actores maliciosos ataquen o rastreen las actividades de un usuario.[11] Estas firmas digitales también tendrían que ser fácilmente revocables y reemitibles en caso de un ataque, lo que plantea la pregunta de cómo se protegen las claves privadas asociadas. Si esto depende de los datos biométricos de los usuarios, se introduce una capa adicional de complejidad técnica y operativa.

Metadatos

Varias entidades plantearon el uso de metadatos para posibilitar la trazabilidad en el debate sobre el cifrado. Los metadatos (que contienen información sobre la comunicación, pero no el contenido de la comunicación en sí) pueden usarse para determinar elementos como el origen, la hora, la fecha y el destino de una comunicación, posiblemente la ubicación del remitente, o incluso para estimar algunos atributos del contenido de la comunicación en sí.

Se ha señalado que los metadatos en torno al tamaño del mensaje, en especial un mensaje multimedia, podrían utilizarse para verificar la distribución descontrolada de mensajes específicos. Por ejemplo, WhatsApp mantiene un registro cifrado de los mensajes multimedia que se envían. No tiene acceso al contenido del archivo multimedia, sino que se ve como un fragmento de datos de un tamaño en particular. Cada vez que se reenvía este mensaje multimedia, el servidor tiene una estimación de cuántas veces se reenvía el fragmento de datos, el cual utiliza para combatir los mensajes no deseados en su plataforma. Puede ser posible inferir el historial del mensaje con acceso a una copia no cifrada del archivo multimedia, eliminando así la confidencialidad de la comunicación de manera efectiva.

Otros sostienen que los metadatos se pueden analizar para discernir patrones tales como quién habla con quién, con qué frecuencia y cuándo. Las plataformas pueden crear gráficos sociales básicos para construir redes de interacciones. Las estructuras de directorios, fundamentales para cualquier plataforma de comunicación, podrían aprovecharse con fines investigativos sin obtener acceso al contenido en sí. Estos directorios registran quién interactúa con quién sin interceptar el contenido en sí.

No obstante, los expertos, inclusive los que participan en los debates de Internet Society, resaltan inquietudes en torno al uso de metadatos para hacer posible la trazabilidad:

- **La atribución digital no es absoluta, en particular mediante los metadatos.** La responsabilidad penal en función de los metadatos, es incluso más difícil de determinar. Los cambios pequeños en el contenido de un mensaje podrían alterar los metadatos de un mensaje, inhibiendo la capacidad de seguir una cadena de metadatos similares hacia un originador. Asimismo, al igual que con las firmas digitales, es difícil unir un usuario a un mensaje cuando la suplantación de identidad en Internet es tan fácil y está tan generalizada. Aún más preocupante es la posibilidad de que un usuario inocente se vea implicado en conductas delictivas puramente en función de metadatos simulados.

- **Socavar los principios de minimización de datos y privacidad por diseño.** La dependencia de los metadatos perjudicaría el avance de las plataformas hacia la minimización de datos y la privacidad

11 https://www.internetsociety.org/policybriefs/identity

por diseño, que actualmente son requisitos de una cantidad de políticas de protección de datos cada vez mayor. Esto crea riesgos mucho más generalizados para la privacidad y la seguridad de las personas al reducir los estándares de seguridad para todos. La retención de metadatos para ayudar a posibilitar la trazabilidad sería un blanco valioso para los actores maliciosos. Los delincuentes y adversarios extranjeros podrían usar los metadatos almacenados para desarrollar gráficos sociales de usuarios o recopilar información que podría posibilitar ataques tales como extorsiones, ingeniería social o chantaje.

- **Riesgos de la creación del perfil social.** Cuando se utilizan metadatos para desarrollar gráficos sociales que ayudan a posibilitar la trazabilidad, estos gráficos sociales corren el riesgo de que delincuentes o adversarios extranjeros accedan a ellos. También existe el riesgo de que las plataformas mismas moneticen estos gráficos sociales, lo que podría exponer detalles sensibles de funcionarios gubernamentales, funcionarios elegidos, periodistas, activistas, abogados y disidentes a corredores de información y sus clientes.

- **Los periodos más prolongados de retención de datos crean riesgos de seguridad:** las normas sobre retención de metadatos suelen incluir requisitos para retener los metadatos por un período determinado. Si los gobiernos ordenan períodos de retención de metadatos más prolongados, se exacerban las inquietudes sobre privacidad y seguridad, ya que más metadatos se verían comprometidos en caso de una infracción de datos. Más datos retenidos significa mayor utilidad para los delincuentes y adversarios extranjeros, y un blanco más atractivo.

- **No todas las plataformas recopilan la misma cantidad de metadatos:** Por ejemplo, Signal recopila el mínimo esencial de metadatos que necesita para facilitar la comunicación y no recopila ningún dato adicional.[12] Los requisitos para retener mayores cantidades de metadatos podrían obligar a las plataformas a reconfigurar sus sistemas de manera significativa, lo que acarrearía costos y aumentaría los riesgos de crear nuevas vulnerabilidades de seguridad.

Ruptura del cifrado de extremo a extremo

Puesto que no es claro cuán útiles son las firmas digitales y los metadatos para posibilitar la trazabilidad, las plataformas pueden verse obligadas a usar métodos que permiten a terceros acceder al contenido de las comunicaciones, lo que a veces se conoce como acceso excepcional, para satisfacer los requisitos de trazabilidad. Al crear acceso al contenido de los mensajes de usuarios, una plataforma o entidad gubernamental podría revisar los mensajes enviados por los usuarios, lo que le permitiría marcar contenido objetable e identificar la cuenta que enviaba el mensaje.

Se han propuesto varias técnicas para brindar acceso a comunicaciones cifradas a terceros.
Esto incluye:

- *El depósito de claves*, mediante el cual las claves utilizadas para descifrar mensajes son almacenadas (de manera total o parcial) por un tercero (como el proveedor de la plataforma) para permitir el acceso al contenido de las comunicaciones cifradas.
- *La propuesta fantasma*, mediante la cual se añade un tercero silencioso como participante en una conversación.
- *El escaneo del lado del cliente,* mediante el cual se examinan comunicaciones o particiones[13] creadas a partir de las comunicaciones para encontrar coincidencias con una base de datos de contenido antes de que el mensaje se envíe al destinatario previsto.

12 https://signal.org/blog/sealed-sender/

13 Una partición es una "huella digital" de contenido de usuario funcionalmente única

No obstante, el consenso entre los expertos, inclusive los que participan en los debates de Internet Society, es que los métodos de acceso de terceros romperían el cifrado de extremo a extremo al posibilitar el acceso de terceros al contenido y debilitaría las protecciones de seguridad y la privacidad de los usuarios.

- **Acceso para uno es acceso para todos.** Al crear una vía para que un tercero acceda a las comunicaciones cifradas de los usuarios se crean, efectivamente, nuevas vulnerabilidades en el sistema. Una vez que los actores maliciosos los encuentran, los mismos métodos utilizados para brindar acceso a las fuerzas de seguridad o las plataformas podrían usarse para actividades malévolas. Por ejemplo, si un actor malicioso obtuviera acceso a las claves de descifrado en custodia, podría descifrar todas las comunicaciones enviadas en un sistema de comunicaciones. No hay manera de asegurar que las vulnerabilidades creadas por un método de acceso excepcional no caerían en manos equivocadas.[14]

- **El acceso excepcional no puede ser selectivo y perjudica la seguridad de todos los usuarios.** Cuando un sistema se modifica para habilitar el acceso excepcional, todos los usuarios quedan expuestos a un riesgo mayor. No hay manera de brindar acceso excepcional a un usuario sin crear vulnerabilidad para todos los usuarios. Por ejemplo, a fin de implementar la propuesta fantasma, se debe alterar el proceso de distribución de claves mediante la distribución secreta de claves a personas que no están en el chat grupal y los proveedores deben suprimir los avisos a los usuarios de que terceros no autorizados tienen acceso a sus comunicaciones. Al alterar la distribución de claves y la notificación en un servicio de comunicaciones, la plataforma introduce nuevas vulnerabilidades que podrían utilizarse sobre todos los usuarios.[15]

- **El escaneo del lado del cliente introduce vulnerabilidades.** Algunas personas alegan que el escaneo del lado del cliente es seguro, en especial cuando las comunicaciones se particionan antes de compararlas con una base de datos de contenido objetable. No obstante, el escaneo del lado del cliente aun introduce vulnerabilidades que ponen en riesgo la seguridad y la privacidad de los usuarios. Los actores maliciosos que obtienen acceso a una base de datos de contenido podrían agregar contenido nuevo para crear falsos positivos o monitorear a quién, cuándo y dónde se comunicó cierto contenido.[16] Los sistemas de escaneo del lado del cliente en los que el contenido de un mensaje se envía a un tercero para su revisión manual tras la correspondencia con una base de datos son particularmente peligrosos ya que crean una nueva forma que los actores maliciosos pueden aprovechar para obtener acceso a comunicaciones no cifradas.

- **Preocupaciones en materia de seguridad nacional.** Si un gobierno o agencia del orden público pudiera acceder a las comunicaciones de un usuario, la misma capacidad estaría disponible a cualquier otro país del mundo, inclusive países adversarios. Los funcionarios gubernamentales y las agencias del orden público tampoco tendrían acceso a canales de comunicación segura y correrían el riesgo de ser blancos de vigilancia por parte de adversarios. Muchas entidades gubernamentales, inclusive la Comisión Europea[17] y el ejército de los Estados Unidos,[18] han encomendado a sus empleados el uso de servicios de comunicaciones con cifrado de extremo a extremo de mercado masivo a fin de proteger sus comunicaciones.

Conclusión

Es probable que la trazabilidad continúe siendo un asunto prominente en el debate de la India sobre las normas de las plataformas digitales y los proveedores de servicios de comunicaciones. No obstante, hay inquietudes razonables en torno a la seguridad, la privacidad y la efectividad de los dos métodos propuestos

14 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf
15 https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/
16 https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/
17 https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/
18 https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/

con más frecuencia para posibilitar la trazabilidad, el **uso de firmas digitales** y el **uso de metadatos.** Para cumplir los requisitos de la trazabilidad, los proveedores de servicios de comunicaciones se verían obligados a acceder al contenido de las comunicaciones de los usuarios, lo que reduciría en gran medida la seguridad y la privacidad de un sistema para todos los usuarios y pondría en un mayor riesgo la seguridad nacional.

Cuando los formuladores de políticas, legisladores y funcionarios judiciales consideran las acciones que crearían requisitos de trazabilidad, deben considerar las graves consecuencias de hacer que los proveedores de servicios y contenidos cumplan estas normas.

Agradecimiento

Agradecemos la participación de más de 50 expertos técnicos y en políticas de la región de Asia-Pacifico, África, Europa, Latinoamérica y Norteamérica en la serie de Reuniones de expertos técnicos mundiales llevadas a cabo de junio a agosto de 2020.