Propuestas fantasma

¿Cuáles son, cuál es su impacto y pueden lograr sus objetivos?

¿Qué son las propuestas "fantasma" y por qué debería importarnos?

Al menos un gobierno ha propuesto recientemente que para facilitar el acceso a los mensajes cifrados de extremo a extremo, la tecnología debe modificarse de forma que un oyente externo pueda agregarse en silencio a las conversaciones cifradas. Dicen que esto puede cumplir los requisitos del orden público o seguridad nacional sin debilitar el cifrado utilizado para cifrar los mensajes. Sin embargo, la propuesta fantasma introduciría vulnerabilidades de seguridad sistémica en los servicios de comunicación confidenciales y cambiaría fundamentalmente la relación de confianza entre los usuarios y los proveedores de servicios.

¿Qué es una propuesta "fantasma" y cómo afecta la seguridad y la confidencialidad?

El término "propuesta fantasma" se refiere a una propuesta en la que los proveedores de aplicaciones de mensajería de extremo a extremo tienen una forma de agregar un tercero a un intercambio de comunicaciones cifradas sin que las otras partes lo sepan. Esto solo se puede hacer con la cooperación del proveedor de servicios de comunicación. Aprovechando las funciones de mensajería grupal de muchos servicios, un usuario se agregaría "en silencio" a una conversación al suprimir las notificaciones habituales que avisan que se ha agregado un nuevo usuario al grupo.

La seguridad de un servicio de comunicaciones cifradas se basa en una gestión de claves de cifrado efectiva y transparente (garantizando que solo los destinatarios tengan las claves que decodifican los mensajes). Para que el cifrado proporcione la confidencialidad que espera un usuario, todo el sistema debe garantizar que solo los destinatarios previstos puedan acceder a las claves necesarias (que permiten cifrar y descifrar el contenido).

Los defensores de la propuesta fantasma argumentan que la inclusión de un tercero secreto es preferible a otras formas técnicas de lograr un acceso excepcional porque el mecanismo de cifrado no se tocaría. Pero si bien la criptografía utilizada para cifrar el contenido de los mensajes puede no verse afectada, introduciría una falla de seguridad en el software de la aplicación de mensajería que utiliza cada usuario; es decir, una gestión de claves de cifrado comprometida que podría permitir el acceso de usuarios no previstos al contenido de las comunicaciones cifradas.

Además, desde la perspectiva de la confianza en un servicio, si un sistema de mensajería promete confidencialidad y no puede brindarla, no importa qué elemento específico de los servicios ha cambiado. El sistema no brinda la protección que los usuarios esperan.

Propuestas fantasma en la práctica: Oyentes silenciosos en grupos de chat

En un sistema de mensajería grupal cifrado de extremo a extremo (E2E), el proveedor de servicios gestiona la distribución segura de claves a los usuarios. Este servicio se oculta en gran medida a los usuarios finales para permitir una experiencia de usuario simplificada, pero a los usuarios se les avisa cuando se agrega a alguien a un chat grupal. La mensajería grupal E2E se fía de este servicio para garantizar que los usuarios previstos se incorporen a un mensaje grupal y que ningún usuario no previsto o desconocido pueda descifrar las comunicaciones, inclusive los propios proveedores de servicios.

La distribución de claves el compleja. Por ejemplo, un servicio de chat cifrado también debe actualizar de forma segura las claves de un usuario cuando reinstala la aplicación o cambia de dispositivo, pero desea permanecer en los mismos grupos.

La propuesta fantasma altera el proceso de distribución de claves al distribuir secretamente claves a personas que no están en el chat grupal, lo que permite a los miembros fraudulentos del grupo escuchar la conversación a escondidas. La propuesta fantasma también requeriría que los proveedores de servicios supriman los avisos a los usuarios de que nuevos terceros no autorizados tienen acceso a sus comunicaciones.

Problemas con la propuesta fantasma

Socava la finalidad del cifrado E2E: Los sistemas de comunicación "seguros" se componen de múltiples partes entrelazadas, de las cuales el cifrado es una pieza esencial pero no la única importante. La gestión de claves de cifrado y la fiabilidad general del sistema son elementos críticos de un sistema de comunicaciones E2E seguro. Incluso si la propuesta fantasma no modificara los algoritmos de cifrado utilizados por las aplicaciones de mensajería de extremo a extremo para cifrar y descifrar los mensajes, introducirían una vulnerabilidad de seguridad sistémica en esos servicios que afectaría negativamente a todos los usuarios, inclusive los usuarios comerciales y gubernamentales. Estas propuestas socavan la gestión de claves y la fiabilidad del sistema, con el resultado de que las comunicaciones supuestamente confidenciales entre el remitente y el destinatario pueden dejar ser confidenciales y serán menos seguras.

Crea vulnerabilidades para que los delincuentes aprovechen: A fin de que terceros se incorporen silenciosamente a las comunicaciones incluso para un solo objetivo, sería necesario que un proveedor de servicios altere el servicio respecto de todos los usuarios para habilitar esta capacidad. Esto introduce una vulnerabilidad intencional en el sistema que, si se descubre, aprovecha o replica, podría ser utilizada indebidamente por terceros no deseados (como delincuentes, empleados deshonestos o gobiernos hostiles) para espiar las comunicaciones.[1] Dado que las comunicaciones con cifrado E2E son esenciales para todos los aspectos de nuestra sociedad, inclusive la seguridad nacional, el orden público y los negocios, esto crea un riesgo inaceptable e innecesario.

Crea nuevos desafíos técnicos y de procesos: Agregar más complejidad técnica a un proceso de gestión segura de claves ya complejo conlleva el riesgo de crear vulnerabilidades involuntarias que actores maliciosos podrían explotar. La gestión efectiva y segura del acceso silencioso autorizado a las comunicaciones es una tarea intimidante y potencialmente problemática. Las organizaciones, inclusive los gobiernos, han tenido dificultades para asegurarse de que los datos sensibles permanezcan seguros y confidenciales. Estas capacidades tendrían que protegerse, no solo de los delincuentes que desean aprovecharlas, sino de empleados deshonestos y adversarios extranjeros.

Los delincuentes migrarán a otro servicio: Los sistemas de comunicaciones con cifrado E2E existen fuera de la jurisdicción de cualquier gobierno. Para evitar que lo atrapen, un delincuente verdaderamente determinado podría dejar de usar los servicios que, según se sabe o se sospecha, implementan la propuesta fantasma, para utilizar otros.

1 "The Athens Affair" es solo un ejemplo. https://spectrum.ieee.org/telecom/security/the-athens-affair

Ampliación de la misión (podría utilizarse para muchas cosas): La propuesta **fantasma** no es selectiva por diseño. Introduce vulnerabilidades en los protocolos de intercambio de claves y notificaciones, y podría utilizarse de maneras no previstas por sus partidarios (por ejemplo, para monitorear a miembros de la prensa, partidos políticos u otros).

Conclusiones

La propuesta fantasma insta a que las fallas sistémicas se diseñen en protocolos para el mercado masivo que utilizan consumidores, empresas y gobiernos. Aumentan la vulnerabilidad y la complejidad de los sistemas resultantes, lo que, a su vez, también aumenta el riesgo de que los desarrolladores introduzcan más fallas por accidente. Los gobiernos deberían abandonar la propuesta fantasma como método de acceso a las comunicaciones cifradas: el riesgo es demasiado grande.

Referencias para conocer más:

- Sharon Bradford Franklin, Andi Wilson Thompson. Mayo de 2018. *Open Letter to GCHQ on the Threats Posed by the Ghost Proposal* (Carta abierta al GCHQ sobre las amenazas planteadas por la propuesta fantasma). https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal
- Matthew Green. Diciembre de 2018. *Sobre usuarios fantasma y puertas traseras de mensajería* (Sobre usuarios fantasma y puertas traseras de mensajería) https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/