UNIVERSIDAD FRANCISCO GAVIDIA

Docente:

JOSE WILFREDO ALEMAN ESPINOZA

Nombres:

JORGE ALBERTO CABRERA PONCE

Materia:

ESTRUCTURA DE DATOS

Tema:

CRIPTOGRAFIA E2EE

Fecha:

27/10/2021

OBJETIVOS

Objetivo General:

1. Conocer a profundidad las ventajas del cifrado de extremo a extremo o E2EE para lograr su implementación en futuros proyectos en clientes que necesiten este tipo de tecnología en sus empresas como de mensajería, bancos y así lograr su comprensión y correcto funcionamiento.

Objetivos específicos:

1. Conocer las características como veneficios, contras y diferencias del cifrado para su correcto funcionamiento.
2. Brindar información detallada de el E2EE al cliente para su beneficio y utilización.

INTRODUCCION:

La presente investigación sobre el encriptado de extremo a extremo o E2EE logrando conocer la forma de utilización para encriptado y desencriptado, logrando conocer como esto ayuda a poder envía información privada o importante por un medio público sin miedo a que esta sea intervenida y difundida públicamente, no sin antes aclarar que es un encriptado y como funciona.

También se lograra describir algunos ejemplos de empresas que utilizan este algoritmo y las ventajas, desventajas que puede traer.

Contenido

UFG

UNIVERSIDAD
FRANCISCO GAVIDIA

Tecnología, Innovación
y Calidad

¿Qué es la criptografía?

La criptografía es una técnica bastante antigua que busca cifrar un texto o una información, para que solo el emisor y el receptor puedan descifrarlos. Dentro de la informática, la criptografía se basa en complejos algoritmos matemáticos que se encargan de cifrar los mensajes.

criptología debe ofrecer:

- Privacidad o confidencialidad: solo pueden acceder a la información aquellas personas que estén autorizadas a obtenerla.

- Integridad: el receptor del mensaje debe ser capaz de comprobar que este no ha sido modificado durante su camino.

- Autenticación: cuando se establece una comunicación segura entre dos interlocutores, cada uno debe ser capaz de verificar la identidad de la otra parte de manera irrefutable.

- No repudio: ninguno de los interlocutores debe ser capaz de negar con posterioridad que ha realizado cierta acción o que ha transmitido determinada información.

¿Cómo se emplea el cifrado para proteger nuestra información en Internet?

Al entrar en webs cuya URL comienza por “HTTPS”: en la que una clave ‘pública’ y una clave ‘privada’ se emplean para encriptar los datos. Cuando un navegador inicia una sesión “HTTPS” con el servidor web, el mismo envía la clave pública al navegador y se lleva a cabo un “SSL Handshake”, también conocido como "saludo”, entre el navegador y el servidor.

Una vez que la conexión segura se ha iniciado y aceptado, el navegador reconoce el link y lo muestra como seguro, ya sea mediante una barra verde o un candado dependiendo del tipo de certificado que se use.

¿Qué es el cifrado de extremo a extremo o E2EE?

El E2EE el acto de aplicar un cifrado a los mensajes de un dispositivo de forma que solo el dispositivo al que se le envía pueda descifrarlo. El mensaje viaja desde el remitente al destinatario en forma cifrada.

¿Cuáles son las alternativas? Una alternativa es transferir los datos en texto plano, es decir, sin cifrar el mensaje. Esta es la opción menos segura. Por ejemplo, los datos enviados por SMS no se cifran, por lo que, en teoría, cualquiera podría interceptarlos. Afortunadamente, en la práctica se necesita un equipo especial, lo que limita en cierta forma la posibilidad de que alguien espíe tus mensajes.

Otra opción es el cifrado de datos en tránsito, mediante el cual los mensajes se cifran en el extremo del remitente, se envían al servidor, donde se descifran y vuelven a cifrar y, entonces, se envían al receptor y se descifran en su extremo. El cifrado en tránsito protege la información durante la transmisión, pero permite que un eslabón intermediario de la cadena, el servidor, vea el contenido. Y, dependiendo de la fiabilidad de los propietarios, esto puede llegar a ser un problema.

A su vez, el uso del cifrado en tránsito implica la aparición del servidor de la comunicación, lo que abre una amplia gama de servicios que van más allá de la simple transferencia de datos. Por ejemplo, un servidor puede almacenar el historial de mensajes, conectar participantes adicionales mediante el uso de canales alternativos a una conversación (como unirse a una videoconferencia por teléfono), usar la moderación automática, etc.

El cifrado en tránsito resuelve la mayoría de los problemas más importantes: la intercepción de datos en ruta desde el usuario al servidor y del servidor al usuario, que es la parte más peligrosa del viaje de un mensaje. Por ello no todos los servicios se han apresurado al cambio del cifrado de extremo a extremo: para los usuarios puede ser más importante hacerse con servicios más cómodos y adicionales, que añadir seguridad a los datos.

¿E2EE de que protege?

La principal ventaja del cifrado de extremo a extremo es su restricción de los datos transmitidos de cualquiera al receptor, el cifrado de extremo a extremo garantiza la privacidad de tu comunicación.

1. Miradas indiscretas. E2EE evita que cualquier persona que no sea el remitente y el destinatario previsto lea la información del mensaje en tránsito porque solo el remitente y el destinatario tienen las claves para descifrar el mensaje. Aunque el mensaje puede ser visible para un servidor intermediario que está ayudando a mover el mensaje, no será legible.
2. Manipulación. E2EE también protege contra la manipulación de mensajes cifrados. No hay forma de alterar de forma predecible un mensaje cifrado de esta manera, por lo que cualquier intento de alteración sería obvio.

¿De qué no te protege el cifrado de extremo a extremo?

Después de conocer los beneficios del cifrado de extremo a extremo, es probable que los lectores se hayan hecho a la idea de que es la solución a todos los problemas de la transferencia de información. Pero no lo es, el cifrado de extremo a extremo también tiene sus limitaciones.

En primer lugar, aunque el uso del cifrado de extremo a extremo te permite ocultar el contenido de tu mensaje, el hecho de que estás enviando un mensaje a cierta persona (o recibiendo) sigue quedando patente. El servidor no podrá leer los mensajes, pero sí es consciente de que has intercambiado mensajes cierto día y a cierta hora. En algunos casos, el mero hecho de comunicarse con determinadas personas puede llamar una atención no deseada.

En segundo lugar, si alguien consigue acceder al dispositivo que usas para comunicarte, podrán leer todos tus mensajes, además de escribir y enviar otros nuevos en tu nombre. Por tanto, para proteger el cifrado de extremo a extremo, necesitas proteger también los dispositivos y el acceso a las aplicaciones, aunque solo sea con un código PIN. De esta forma, si pierdes o alguien te roba tu dispositivo, tu correspondencia, junto con la capacidad de hacerse pasar por ti, no caerá en las manos equivocadas.

Por ello, necesitas proteger tus dispositivos con un software antivirus. Si el malware llega a tu smartphone, cualquiera podría leer la correspondencia que

mantienes en él, como si lo tuviera físicamente. Esto es así independientemente del tipo de cifrado que utilices para enviar y recibir mensajes.

En tercer y último lugar, aunque lleves mucho cuidado con la protección de todos tus dispositivos y estés completamente seguro de que nadie tiene acceso a tus mensajes, no puedes estar tan seguro del dispositivo de tu interlocutor. Y el cifrado de extremo a extremo tampoco podrá ayudarte con eso.

Igualmente, a pesar de sus limitaciones, el cifrado de extremo a extremo es la forma actual más segura de transferir datos confidenciales y por ello cada vez más servicios de comunicación están apostando por este sistema. Y eso es una buena noticia.

1. Metadatos. Si bien E2EE protege la información dentro de un mensaje, no oculta información sobre el mensaje, como la fecha y hora en que se envió o los participantes en el intercambio. Estos metadatos podrían dar a los actores malintencionados interesados en la información cifrada pistas sobre dónde pueden interceptar la información una vez que se haya desencriptado.
2. Puntos finales comprometidos. Si alguno de los extremos se ha visto comprometido, un atacante puede ver un mensaje antes de que se cifre o después de que se descifre. Los atacantes también podrían recuperar claves de puntos finales comprometidos y ejecutar un ataque de intermediario con una clave pública robada.
3. Intermediarios vulnerables. A veces, los proveedores afirman ofrecer cifrado de extremo a extremo cuando lo que realmente ofrecen está más cerca del cifrado en tránsito. Los datos pueden almacenarse en un servidor intermediario donde se puede acceder a ellos.

¿Cuáles son las diferencias del E2EE de otros tipos de cifrado?

Lo que hace que el cifrado de un extremo a otro sea único en comparación con otros sistemas de cifrado es que solo los puntos finales, el remitente y el receptor, son capaces de descifrar y leer el mensaje. El cifrado de clave simétrica, que también se conoce como cifrado de clave única o clave secreta , también proporciona una capa ininterrumpida de cifrado del remitente al destinatario, pero utiliza solo una clave para cifrar mensajes.

La clave utilizada en el cifrado de clave única puede ser una contraseña, código o cadena de números generados aleatoriamente y se envía al destinatario del mensaje, lo que le permite desencriptar el mensaje. Puede ser complejo y hacer que el mensaje parezca un galimatías para los intermediarios que lo pasan del remitente al receptor. Sin embargo, el mensaje puede ser interceptado, descifrado y leído, sin importar cuán drásticamente la clave lo cambie si un intermediario obtiene la clave. E2EE, con sus dos claves , evita que los intermediarios accedan a la clave y descifren el mensaje.

El cifrado de extremo a extremo utiliza un enfoque asimétrico. Vea cómo se compara con la metodología de cifrado simétrico.

Otra estrategia de cifrado estándar es el cifrado en tránsito. En esta estrategia, los mensajes son encriptados por el remitente, desencriptados intencionalmente en un punto intermedio, un servidor de terceros propiedad del proveedor de servicios de mensajería, y luego reencriptados y enviados al destinatario. El mensaje es ilegible en tránsito y puede utilizar cifrado de dos claves, pero no utiliza cifrado de extremo a extremo porque el mensaje se ha descifrado antes de llegar a su destinatario final.

El cifrado en tránsito, como E2EE, evita que los mensajes sean interceptados en su viaje, pero crea vulnerabilidades potenciales en ese punto medio donde se descifran. El protocolo de cifrado de seguridad de la capa de transporte es un ejemplo de cifrado en tránsito.

Ventajas del cifrado de un extremo a otro

La principal ventaja del cifrado de extremo a extremo es un alto nivel de privacidad de los datos, proporcionado por las siguientes características:

1. Seguridad en tránsito. El cifrado de extremo a extremo utiliza criptografía de clave pública, que almacena claves privadas en los dispositivos terminales. Los mensajes solo se pueden descifrar con estas claves, por lo que solo las personas con acceso a los dispositivos terminales pueden leer el mensaje.
2. A prueba de manipulaciones. Con E2EE, no es necesario transmitir la clave de descifrado; el destinatario ya lo tendrá. Si un mensaje cifrado con una clave pública se modifica o manipula en tránsito, el destinatario no podrá descifrarlo, por lo que el contenido manipulado no se podrá ver.
3. Cumplimiento. Muchas industrias están sujetas a leyes de cumplimiento normativo que requieren seguridad de datos a nivel de cifrado. El cifrado de

un extremo a otro puede ayudar a las organizaciones a proteger esos datos haciéndolos ilegibles.

¿Desventajas del cifrado de un extremo a otro?

Aunque E2EE generalmente hace un buen trabajo al proteger las comunicaciones digitales, no garantiza la seguridad de los datos. Las deficiencias de E2EE incluyen las siguientes:

1. Complejidad en la definición de los puntos finales. Algunas implementaciones de E2EE permiten que los datos cifrados se descifren y se vuelvan a cifrar en determinados puntos durante la transmisión. Esto hace que sea importante definir y distinguir claramente los puntos finales del circuito de comunicación.

2. Demasiada privacidad. Los organismos gubernamentales y de aplicación de la ley expresan su preocupación de que el cifrado de extremo a extremo pueda proteger a las personas que comparten contenido ilícito porque los proveedores de servicios no pueden proporcionar acceso al contenido a las fuerzas del orden.

3. Metadatos visibles. Aunque los mensajes en tránsito están encriptados y son imposibles de leer, la información sobre el mensaje (la fecha de envío y el destinatario, por ejemplo) sigue siendo visible, lo que puede proporcionar información útil a un intruso.

4. Seguridad de endpoints . Si los puntos finales están comprometidos, es posible que se revelen datos cifrados.

5. No está preparado para el futuro. Aunque el cifrado de extremo a extremo es una tecnología sólida en la actualidad, se especula que eventualmente la computación cuántica hará que la criptografía sea obsoleta .

Aplicaciones que utilizan E2EE

El primer software de mensajería E2EE ampliamente utilizado fue Pretty Good Privacy , que protegía el correo electrónico y almacenaba archivos y firmas digitales. Las aplicaciones de mensajería de texto utilizan con frecuencia cifrado de extremo a extremo, incluido iMessage, Jabber y Signal Protocol de Apple (anteriormente, TextSecure Protocol).

Los proveedores de POS, como Square, también utilizan protocolos E2EE para ayudar a mantener el cumplimiento de PCI.

En 2019, Facebook anunció que sus tres servicios de mensajería comenzarían a usar E2EE. Sin embargo, las fuerzas del orden y las agencias de inteligencia argumentan que el cifrado limita la capacidad de Facebook para controlar la actividad ilegal en sus plataformas. El debate a menudo se centra en cómo E2EE puede dificultar la identificación y la interrupción del abuso infantil en plataformas de mensajería privadas.

El cifrado es solo una pieza de la seguridad de los datos en la empresa. Obtenga más información sobre todos los aspectos de la seguridad y el cumplimiento de los datos en nuestra guía completa.Esto se actualizó por última vez en junio de 2021

Bibliografía

Echenique García, J. A. (2001). *Auditoria en informática.* México: McGraw-Hill.

Gomez Vieites, Á. (2007). *Enciclopedia de la seguridad informática.* México: Alfaomega.

Hernández Encinas, L. (2016). *La criptografía.* Editorial CSIC Consejo Superior de Investigaciones Científicas.

Ibarra Quevedo, R. (2010). *Teoría de la información y encriptamiento de datos.* ebook SS.

Nichols, R. K., & Lekkas, P. C. (2003). *Seguridad para comunicaciones inalámbricas : redes, protocolos, criptografía y soluciones.* SPANA: FANCE .

profesionales, C. :. (2009). *Maiorano, Ariel Horacio.* Alfaomega.