Ataques de máquina en medio

Qué son y cómo podemos prevenirlos

Agosto de 2022

Cuando usamos Internet, esperamos que nuestras comunicaciones sean confidenciales y que no hayan sido modificadas o manipuladas en tránsito. Cuando ingresa su contraseña para usar la banca en línea, usted confía en la suposición de que, a) su contraseña coincide con los registros bancarios, b) el banco recibe la contraseña en su forma correcta y c) los terceros no pueden ver, cambiar, falsificar o reutilizar su contraseña. Este es un ejemplo simple, pero en esencia, un "ataque de máquina en medio" (MITM) funciona rompiendo la segunda y/o tercera de esas suposiciones.

Un ataque MITM no solo puede interrumpir las comunicaciones digitales entre humanos, sino también afectar los tipos de comunicación de máquina a máquina que son vitales para confiar en los productos conectados y los servicios de Internet. Por ejemplo, un dispositivo de IoT, como un asistente virtual, habitualmente comparte información con un servidor central que aloja contenido.

Si no puede confiar en las conexiones que realiza a sitios web y servicios en línea, podría ser vulnerable al fraude, la suplantación de identidad, el malware y otros riesgos. Si sus dispositivos y objetos conectados no pueden comunicarse de manera segura y confiable, pueden ponerlo a usted y a su hogar en peligro físico.

¿Qué es un ataque de máquina en medio?

Un ataque MITM es aquel en el cual un tercero intercepta una comunicación entre usuarios (o máquinas). Los ataques MITM suelen adoptar dos formas. La primera es esencialmente escuchar a escondidas: un adversario monitorea pasivamente una conversación o lee el contenido de un mensaje; la segunda, un ataque "activo", implica que el adversario cambie el contenido del mensaje o modifique la comunicación (por ejemplo, infectando a una víctima con malware). El primero es un ataque a la confidencialidad de la comunicación, el segundo un ataque a su integridad. Si bien algunos ataques MITM se realizan sin el conocimiento de los proveedores de servicios de comunicaciones, otros están diseñados en la infraestructura de los servicios de comunicaciones.

En 2013, los medios informaron[1] que algunos gobiernos habían implementado importantes regímenes de recopilación de datos en Internet utilizando técnicas MITM. Agregar funcionalidades MITM a

1 https://www.amnesty.org/en/latest/news/2013/06/usa-revelations-about-government-surveillance-raise-red-flags/

partes de la infraestructura de Internet, a veces con la ayuda de proveedores de servicios de Internet, permitió a las agencias de seguridad nacional interceptar y leer el tráfico masivo de Internet. Si se hubiera cifrado todo el tráfico, acceder al contenido habría sido más difícil para las agencias. Después de conocer estas actividades de vigilancia, los principales proveedores de servicios adoptaron medidas para cifrar sus servicios, agregar cifrado de extremo a extremo y activar el cifrado de forma predeterminada.

Los ataques MITM son una amenaza real para Internet, independientemente de cuál sea la entidad que los utiliza. Los ataques MITM reducen la confianza de los usuarios en que su comunicación es privada y no ha sido alterada en tránsito. Los ataques MITM socavan la confianza que subyace las funciones fundamentales y la fiabilidad de Internet.[2]

El cifrado ayuda a proteger contra ataques MITM

El cifrado es una forma en que las personas pueden protegerse contra un ataque MITM. Puede ayudar a evitar que terceros lean o modifiquen los contenidos de sus comunicaciones. Por ejemplo, si envía un correo electrónico sin cifrar, el contenido será visible para todos los intermediarios y nodos de red a través de los cuales pasa el tráfico. El correo electrónico sin cifrar es como enviar una postal: el cartero, cualquier persona en la oficina de clasificación y cualquier persona con acceso a la alfombrilla de entrada del destinatario puede, si lo desea, leer el contenido.[3]

Cifrar el mensaje protege su confidencialidad: puede que no evite que un adversario vea el contenido, pero lo que leen será incomprensible, porque está codificado.

Usar el cifrado para firmar datos, un documento o una comunicación de manera digital, ayuda a garantizar que si un adversario logra modificar el contenido, la manipulación será evidente. Con la mayoría de los algoritmos de cifrado, cambiar cualquier parte del mensaje inicial da como resultado una versión cifrada completamente diferente del mensaje. Esta propiedad se puede utilizar para ayudar al destinatario a comprobar que el mensaje original no ha sido manipulado, como un sello en un sobre.

Transport Layer Security 1.3 (TLS 1.3) es un importante protocolo de seguridad de Internet que proporciona una capa adicional de defensa contra los ataques MITM. TLS 1.3 hace que la confidencialidad directa[4] sea obligatoria para las sesiones de TLS. Esto garantiza que se use una clave separada para cada sesión cifrada, lo que significa que descifrar una clave de sesión no da acceso a los datos cifrados de sesiones anteriores ni ayuda a descubrir claves de sesión posteriores. Significa

2 https://datatracker.ietf.org/doc/rfc7258/

3 https://www.internetsociety.org/resources/doc/2018/encryption-brief/

4 https://blogs.cisco.com/security/tls-1-3-and-forward-secrecy-count-us-in-and-heres-why

que un adversario tiene que descubrir la clave de cifrado específica para cada sesión, lo que aumenta la dificultad de los ataques MITM.

Ataques MITM para obtener acceso a contenido cifrado

Los gobiernos de todo el mundo han propuesto o implementado varios métodos para proporcionar acceso a comunicaciones o dispositivos cifrados a efectos de seguridad nacional o aplicación de la ley. Uno de esos métodos es el ataque MITM. Ciertos tipos de ataques MITM, como el ejemplo a continuación, pueden incluso socavar la protección de confidencialidad directa de protocolos como TLS 1.3, porque potencialmente subvierten todo el mecanismo de intercambio seguro de claves en el que se basa la confidencialidad directa.

Ejemplo: un ataque MITM sobre el tráfico HTTPS

Según ZDnet[5], en 2019, los usuarios de operadores móviles kazajos que intentaban acceder a Internet recibieron mensajes de texto que indicaban que debían instalar certificados raíz emitidos por el gobierno en sus dispositivos móviles y de escritorio. Exigir a los usuarios de Internet que instalen certificados raíz que pertenecen al gobierno podría darle al gobierno la capacidad de interceptar el tráfico HTTPS encriptado y realizar un ataque MITM para romper la comunicación segura. Esto significa que el gobierno podía monitorear, registrar e incluso bloquear las interacciones entre los usuarios de Kazajistán y cualquier sitio web, incluidos bancos, proveedores de correo electrónico, redes sociales y servicios públicos fundamentales como electricidad, hospitales, transporte y votación. Una vez que se instalan estos certificados, los usuarios no tienen forma de saber si sus comunicaciones ya no son seguras. Es posible que los navegadores sigan mostrando un símbolo de candado u otro indicador de que el tráfico "está cifrado y es seguro", pero el tráfico que parece seguro, no lo es. La introducción de esta debilidad socava la seguridad de la infraestructura de clave pública global y erosiona la confianza en la información y los servicios a los que se accede a través de Internet.

Los ataques MITM no solo quiebran la confidencialidad y la integridad, sino que también pueden interrumpir el acceso a Internet. Por ejemplo, en 2012, se informa que el intento de ataque MITM de una agencia de seguridad en Siria rompió una parte central de la infraestructura de Internet del país, dejando a los sirios sin acceso a Internet global.[6]

5 https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/
6 https://www.wired.com/2014/08/edward-snowden/

Conclusión

Los gobiernos deben abstenerse de utilizar ataques de máquina en medio para permitir el acceso de las fuerzas del orden público a las comunicaciones privadas. La creación de estas capacidades compromete la seguridad de todos los usuarios y socava la infraestructura de Internet. Los mismos métodos creados para las fuerzas del orden pueden utilizarse como medio de ataque, tanto por parte de usuarios autorizados como de terceros malintencionados[7]. Los ataques MITM presentan una amenaza real, no solo para la confianza que los usuarios tienen en la confidencialidad e integridad de las comunicaciones en línea, sino también para la seguridad y fiabilidad de Internet global.

Información adicional:

"Keys Under Doormats" – Technical Report, MIT Computer Science and Artificial Intelligence Laboratory, 2015

7 https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal