Ataques de intermediarios

¿Qué son, y cómo podemos evitarlos?

Cuando usamos Internet, esperamos que nuestras comunicaciones sean confidenciales y que no hayan sido modificadas o manipuladas en tránsito. Cuando ingresa su contraseña en la banca en línea, usted confía en el supuesto de que: a) su contraseña coincide con los registros del banco, b) el banco recibe la contraseña en su forma correcta, y c) los terceros no pueden ver, interceptar o cambiar su contraseña tal como se envía al banco. Este es un ejemplo simple, pero en resumen, un ataque de intermediario (man-in-the-middle, MITM) funciona cuando se frustra el segundo o tercero de esos supuestos.

Un ataque MITM no solo puede interrumpir las comunicaciones entre humanos, sino también impactar las comunicaciones de máquina a máquina que son críticas para las comunicaciones confiables en 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 a riesgos de seguridad como fraude, suplantación de identidad, malware y otros. Si sus dispositivos y objetos conectados no pueden comunicarse de manera segura y fiable, pueden ponerlo a usted y a su hogar en riesgo.

¿Qué es un ataque de intermediario?

Un ataque MITM es aquel en el cual un tercero intercepta una comunicación entre usuarios (o máquinas). Por lo general, esto se hace de manera encubierta, pero a veces el usuario puede tener conocimiento. Los ataques MITM suelen adoptar dos formas: la primera es cuando un adversario puede querer leer el contenido de un mensaje, y la segunda involucra a un adversario que cambia el contenido del mensaje o modifica la comunicación de otra manera, como por ejemplo al infectar a una víctima con malware. El primero es un ataque a la confidencialidad del mensaje; 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 que algunos gobiernos habían implementado importantes regímenes de recopilación de datos en Internet utilizando técnicas MITM. Agregar funcionalidades MITM a 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 amenazan la confidencialidad de las comunicaciones y reducen la confianza del usuario en que su comunicación no ha sido alterada en tránsito. Los ataques MITM socavan la confianza que sustenta las funciones centrales y la confiabilidad de Internet.[1]

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 al tapete del destinatario pueden, si así lo desean, leer el contenido.[2]

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 usar para ayudar al destinatario a asegurarse de que el mensaje original no haya sido alterado, de forma similar a un sello roto 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 crea un secreto directo obligatorio para el tráfico de Internet, asegurando que el tráfico interceptado no pueda ser descifrado incluso si un atacante tiene una clave privada en el futuro. Esto se debe a que cada sesión es cifrada con una nueva clave de sesión. Significa que un adversario tiene que descubrir las claves de cifrado para cada sesión, lo que aumenta enormemente la dificultad de los ataques MITM.

Ataques MITM para obtener acceso a contenido cifrado

Los gobiernos de todo el mundo han propuesto o implementado varias medidas para proporcionar acceso a comunicaciones o dispositivos cifrados a efectos de seguridad nacional o aplicación de la ley. Una categoría de dichos métodos son los ataques MITM.

Ejemplo: un ataque MITM sobre el tráfico HTTPS

Según Zdnet[3], en 2019 los usuarios de operadores móviles kazajos que intentaban acceder a Internet recibieron mensajes de texto que indicaban que necesitaban 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 ver, 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 críticos como electricidad, elecciones, hospitales y transporte. Una vez que se instalan estos certificados, los usuarios no tienen forma de saber si sus comunicaciones ya no son seguras. Los navegadores seguirán mostrando un símbolo de candado u otro indicador de que el tráfico "está cifrado y es seguro", pero el tráfico que parece

[1] https://datatracker.ietf.org/doc/rfc7258/

[2] https://www.internetsociety.org/resources/doc/2018/encryption-brief/

[3] https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/

seguro, no lo es. La introducción de esta debilidad socava la seguridad de Internet y erosiona la confianza en la infraestructura de clave pública global.

Los ataques MITM no solo quiebran la confidencialidad y la integridad, sino que también pueden interrumpir el acceso a Internet. Por ejemplo, en 2012 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.[4]

Conclusión

Los gobiernos deben abstenerse de utilizar ataques de intermediarios para permitir que las autoridades del orden público accedan a las comunicaciones privadas. La creación de estas capacidades socava en gran medida la seguridad para todos los usuarios y la infraestructura de Internet. Actores maliciosos podrían usar los mismos métodos creados por las fuerzas del orden para llevar a cabo sus propios ataques.[5] 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.

Referencias para conocer más:

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

[4] https://www.wired.com/2014/08/edward-snowden/

[5] https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal