Nombre de la materia:
Fundamento de telecomunicaciones

Nombre de la licenciatura:
SISTEMAS COMPUTACIONALES

Nombre del alumno(a):
ALAN GERARDO GIJON AGOSTO

Número de control:
18530390

Nombre de la tarea: Investigación MITM

Unidad #: nombre de la unidad:

Nombre del profesor(a):
ING. ISMAEL JIMENEZ SANCHEZ

Fecha:

Dicho de una forma sencilla, un MITM es un ataque en el que un tercero consigue acceder a las comunicaciones entre otras dos partes, sin que ninguna de ellas se dé cuenta de ello. Esa tercera parte puede leer el contenido de la comunicación o, en algunos casos, manipularlo. Así pues, por ejemplo, si Gerald le envía un mensaje a Leila supuestamente privado, y Max intercepta el mensaje, lo lee y se lo envía a Leila, eso sería un ataque MITM. Si Gerald quiere transferir 100 € a la cuenta bancaria de Leila y Max intercepta la transacción y cambia el número de cuenta de Leila por el suyo, eso también sería una ataque MITM (en este caso, Max está «intermediando» entre Gerald y su banco).

¿Por qué debo preocuparme?

En parte, porque los ataques MITM pueden socavar en gran medida nuestro estilo de vida moderno. En una vida conectada, dependemos de la fiabilidad y seguridad de todas las conexiones. Tampoco se trata solo de tus conversaciones, mensajes y correos electrónicos. Si no puedes confiar en las conexiones que estableces con los sitios web y servicios online, podrías exponerte al fraude y a la suplantación de identidad, y tus dispositivos y objetos conectados no pueden comunicarse de forma segura y fiable, cosa que podría poner tu casa en riesgo.

Los ejemplos de este blog están basados en el tráfico cifrado entre humanos, pero los ataques MITM pueden afectar a cualquier intercambio de comunicaciones, incluidas comunicaciones de dispositivo a dispositivo y objetos conectados (IoT). Los ataques MITM socavan la confidencialidad e integridad de las comunicaciones y al crear esta situación también pueden exponer los datos, los dispositivos y los objetos a un uso doloso.

Imagina el peligro que supondría que un pirata informático pudiese activar los airbags de un coche conectado o abrir a distancia una cerradura electrónica. El hecho de que ahora los objetos conectados puedan afectar al mundo físico introduce factores nuevos al análisis de riesgos, sobre todo en aquellos casos en los que la infraestructura física (transporte, energía, industria) está automatizada o se controla a distancia. Un ataque MITM a los protocolos de control de estos sistemas, en el que el atacante se interpone entre el controlador y el dispositivo, podría tener efectos devastadores.

¿Es esto algo nuevo?

En principio, no: los ataques MITM llevan existiendo desde que hemos tenido que recurrir a terceros para que envíen nuestros mensajes. Cuando la gente sellaba sus cartas con cera y un cuño personal, lo hacía para protegerse contra ataques MITM. El sello de cera no imposibilitaba que un tercero rompiese la cera y abriese la carta: se ponía para comprobar fácilmente si alguien lo había hecho, porque le resultaría bastante complicado cambiar la cera y falsificar la marca dejada por el cuño personal del remitente. Este tipo de protección se denomina “precinto de seguridad”, y también se puede ver en productos de consumo como, por ejemplo, el precinto de aluminio que lleva la tapa de un bote de pastillas o la tira de celofán que rodea un paquete de tabaco.

Si alguien no solo quisiera saber si su carta ha sido manipulada, sino también proteger la confidencialidad del contenido, normalmente tendría que escribir la carta en un código que solo pudiese descifrar el destinatario.

En el contexto digital, tenemos equivalentes para todos estos casos. Por ejemplo, si envías un correo electrónico sin cifrar, el contenido quedará a la vista de todos los intermediarios y nodos de red por los que pasa el tráfico. El correo electrónico no cifrado es como enviar una postal: el cartero, cualquier empleado de la oficina y cualquier persona con acceso al felpudo del destinatario puede leer el contenido, si así lo desea. Si quieres que el contenido de tu correo electrónico solo lo lea el destinatario, tendrás que cifrar el correo electrónico de forma que solo este pueda descifrarlo, y si quieres asegurarte de que nadie pueda modificar el contenido sin que el destinatario lo sepa, tendrás que realizar un monitoreo de integridad como, por ejemplo, con una firma digital, en el mensaje.

Así pues, en lo que al tráfico no cifrado respecta, un “ataque” MITM consiste en asegurarse de tener acceso al tráfico de mensajes entre Gerald y Leila.

En el caso del tráfico cifrado, esto no es suficiente; es probable que veas que Gerald le está escribiendo a Leila, porque la información tiene que ser clara para que el mensaje se redireccione correctamente. Pero no podrás ver el contenido del mensaje: para ello necesitarás la clave utilizada para cifrar el mensaje. En el tipo de cifrado que se emplea normalmente para proteger los mensajes, el mensaje se cifra y descifra usando dos copias de la misma clave, como si se enviara el mensaje en una caja fuerte cerrada. Para que eso funcione, Gerald y Leila tienen que intercambiar una copia de la clave.

Por lo tanto, en este caso, un ataque MITM empezaría por interceptar ese tráfico, lo que permitiría al atacante (Max) desbloquear el mensaje una vez enviado por Gerald, leerlo, volverlo a cifrar y enviárselo a Leila, sin que esta se entere.

He aquí los dos “frentes” de un ataque MITM. El primero se encarga de interceptar el contenido de los mensajes; el segundo tiene la finalidad de interceptar la clave utilizada para proteger el tráfico. En este sentido, la interceptación del mensaje sería simplemente cuestión de situarse entre las dos partes que se comunican y leer el tráfico; para interceptar la clave probablemente sea necesario suplantar activamente la identidad de las partes que se comunican. Por este motivo un ataque MITM exitoso podría exponerte al riesgo de ser engañado… porque para que funcione tienen que hacerte creer que estás hablando con el interlocutor seleccionado, aunque no sea así.

¿Qué puedo hacer al respecto?

Un ataque MITM exitoso pasará totalmente desapercibido para los usuarios, sobre todo si se realiza a la infraestructura. La seguridad general de este tipo de sistema depende de la seguridad de toda una serie de elementos que deben funcionar correctamente. Algunos de estos elementos están en manos del usuario, pero otros pertenecen y son gestionados por terceras partes (como el desarrollador del navegador y las autoridades de certificación).

Como usuario, es importante entender las pistas que indican si el sistema está funcionando según lo previsto:

- Distinguir una sesión de navegador segura de una no segura
- Reconocer una firma digital válida
- Saber cómo reaccionar adecuadamente a una advertencia de certificado

Bibliografía:

https://www.internetsociety.org/es/blog/2019/11/que-es-un-ataque-de-intermediario-mitm-por-sus-siglas-en-ingles/#:~:text=Dicho%20de%20una%20forma%20sencilla,%2C%20en%20algunos%20casos%2C%20manipularlo.