INSTITUTO TECNOLOGICO DE CANCUN

ASIGNATURA: FUNDAMENTOS DE TELECOMM

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

PROFESOR: ISMAEL JIMENEZ SANCHEZ

ALUMNO: FERNANDO FLORES PRADO

Man in the midddle

En criptografía, un ataque de intermediario (en inglés, man-in-the-middle attack, MitM o Janus) es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando este se emplea sin autenticación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso wifi sin cifrar, donde este se puede insertar como intermediario.

Salvo en el protocolo de interbloqueo (interlock), todos los sistemas criptográficos seguros frente a ataques MitM requieren un intercambio adicional de datos o la transmisión de cierta información a través de algún tipo de canal seguro. En ese sentido, se han desarrollado muchos métodos de negociación de claves con diferentes exigencias de seguridad respecto al canal seguro.

Ejemplo de un ataque

Una ilustración de un ataque de intermediario

Suponga que Alice quiere comunicarse con Bob. Mientras tanto, Mallory quiere interceptar la conversación para escuchar y posiblemente alterar (aunque este paso no es necesario) el mensaje que recibe Bob.

En primer lugar, Alice le pregunta a Bob por su clave pública. Si Bob envía su clave pública a Alice, pero Mallory es capaz de interceptarla, un ataque de intermediario puede comenzar. Mallory envía un mensaje falsificado a Alice que dice ser de Bob, pero en cambio incluye la clave pública de Mallory. Alice, creyendo que esta clave pública sea de Bob, cifra su mensaje con la clave de Mallory y envía el mensaje cifrado de nuevo a Bob. Mallory intercepta otra vez, descifra el mensaje utilizando su clave privada, posiblemente altera si ella quiere, y vuelve a cifrar con la clave pública de Bob que fue enviada originalmente a Alice. Cuando Bob recibe el nuevo mensaje cifrado, él cree que vino de Alice.

Alice envía un mensaje a Bob, que es interceptado por Mallory:

Alice "Hola Bob, soy Alice. Dame tu clave." → Mallory Bob

Mallory reenvía este mensaje a Bob; Bob no puede decir que no es realmente de Alice:

Alice Mallory "Hola Bob, soy Alice. Dame tu clave." → Bob

Bob responde con su clave de cifrado:

Alice Mallory ← [clave de Bob] Bob

Mallory reemplaza la clave de Bob con la suya, y transmite esto a Alice, afirmando que es la clave de Bob:

Alice ← [clave de Mallory] Mallory Bob

Alicia encripta un mensaje con lo que ella cree que es la clave de Bob, pensando que sólo Bob puede leer:

Alice "¡Nos vemos en la parada de autobús!" [Cifrada con la clave de Mallory] → Mallory Bob

Sin embargo, debido a que en realidad estaba cifrada con la clave de Mallory, Mallory puede descifrarlo, leerlo, modificarlo (si se desea), volver a cifrar con la clave de Bob, y lo remitirá a Bob:

Alice Mallory "¡Nos vemos en la furgoneta de al lado del río!" [Cifrada con la clave de Bob] → Bob

Bob cree que este mensaje es una comunicación segura de Alice.

Bob va a la furgoneta sin ventanas y Mallory le atraca.

Este ejemplo muestra la necesidad de que Alice y Bob tengan alguna manera de asegurarse de que están realmente utilizando mutuamente claves públicas, en lugar de la clave pública de un atacante. De lo contrario, este tipo de ataques son generalmente posibles, en principio, contra cualquier mensaje enviado utilizando la tecnología de clave pública. Afortunadamente, hay una variedad de técnicas que ayudan a defenderse de los ataques MITM.

Posibles subataques

Debido al aumento en la cantidad de puntos de acceso inalámbrico gratuitos y en velocidades de banda ancha que han permitido una evolución en la comunicación que hace que vivamos más conectados, esto también han generado múltiples oportunidades para quienes desean espiar o interceptar nuestra actividad en línea.

El ataque MitM puede incluir algunos de los siguientes subataques:

Interceptación de la comunicación, incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos conocidos.

Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.

Ataques de sustitución.

Ataques de repetición.

Ataque por denegación de servicio. El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes. La defensa en ese caso pasa por el envío periódico de mensajes de status autenticados.

MitM se emplea típicamente para referirse a manipulaciones activas de los mensajes, más que para denotar interceptación pasiva de la comunicación.

Defensas contra el ataque

La posibilidad de un ataque de intermediario sigue siendo un problema potencial de seguridad serio, incluso para muchos criptosistemas basados en clave pública. Existen varios tipos de defensa contra estos ataques MitM que emplean técnicas de autenticación basadas en:

- Claves públicas.
- Autenticación mutua fuerte.
- Claves secretas (secretos con alta entropía).
- Contraseñas (secretos con baja entropía).
- Otros criterios, como el reconocimiento de voz u otras características biométricas.

Fijación de certificados

La integridad de las claves públicas debe asegurarse de alguna manera, pero éstas no exigen ser secretas, mientras que las contraseñas y las claves de secreto compartido tienen el requerimiento adicional de la confidencialidad. Las claves públicas pueden ser verificadas por una autoridad de certificación (CA), cuya clave pública sea distribuida a través de un canal seguro (por ejemplo, integrada en el navegador web o en la instalación del sistema operativo).

Características

En un ataque de MITM, el atacante tiene control total de la información entre dos o más socios de enlace. Esto permite al atacante leer, influir y manipular la

información. El atacante está reflejando la identidad del primero y del segundo interlocutor de comunicación, de modo que puede participar en el canal de comunicación. La información entre los dos hosts está cifrada, pero es descifrada por el atacante y transmitida.