ugr | Universidad de Granada

GRADO EN INGENIERÍA INFORMÁTICA

Trabajo Final

Man-in-The-Middle

Autores

Adrián Sánchez Cerrillo

Sixto Coca Cruz

Servidores Web de Altas Prestaciones

Dpto. de Arquitectura y Tecnología de los Computadores

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

—

Indice

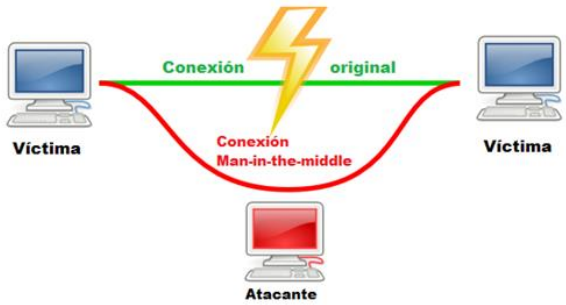
Introducción

En la era de la información, cifrar las comunicaciones es algo imprescindible para asegurar el correcto funcionamiento de un servicio cualquiera. Man-in-The-Middle es un tipo de ataque informático que permite, no solo la lectura de la información, si no también añadir y/o modificar la información ya existente. Este tipo de ataques es muy usado en la actualidad para modificar la información que un usuario visualiza en una página web, o con la finalidad de robar credenciales.

Los ataques de este tipo suelen desempeñarse en multitud de escenarios, siendo las redes Wi-Fi públicas el principal medio de actuación, aunque su uso se ha visto reducido en los últimos años con la llegada de tarifas de itinerancia de datos, especialmente en dispositivos móviles, sigue siendo un ataque difícil de detectar.

¿Cómo funciona Man-In-The-Middle?

El ataque Man-in-The-Middle consiste en interceptar el tráfico consecuente de la comunicación entre dos equipos, pudiendo así desviar y/o controlar las comunicaciones.



Por un lado, para llevar a cabo este tipo de ataque, el cual puede utilizarse contra muchos protocolos criptográficos, es necesario comentar el protocolo que disponen las máquinas para comunicarse entre sí, denominado *ARP* o protocolo de resolución de direcciones. Cuando un dispositivo quiere establecer comunicación con otro, siempre y cuando ambos se encuentren en la misma red, se realizará una petición *ARP* a la dirección de difusión de red para conocer dónde se encuentra la dirección IP del dispositivo destinatario de la comunicación. Una de las máquinas en la red (dependiendo del tipo de estructura de red) responderán con la dirección requerida, la cual quedará registrada en la memoria caché de la primera máquina.

Uno de los métodos más comunes de ataque a redes utiliza el protocolo anteriormente mencionado, *ARP Caché Poisoning* busca manipular las tablas ARP de los ordenadores en la red por medio de respuestas ARP falsas haciendo que la dirección MAC e IP del atacante y

víctima sean iguales, de tal forma que el tráfico que se dirige a la víctima pasará también por el atacante. Este ataque necesita que el atacante se encuentre en la misma red que la víctima.

De forma similar, en un ataque basado en un servidor DHCP o *DHCP Spoofing*, con el atacante en la misma red que la víctima, se utiliza el propio equipo para configurarlo como servidor DHCP, el cual es un componente de las redes que se encarga de asignar las configuraciones locales a los equipos conectados, teniendo así el atacante .

Con la llegada de los protocolos de conexión seguros como HTTPS o *"Hypertext Transfer Protocol Secure"* se dificultó la obtención de información interceptada mediante ataques MiTM, sin embargo, una técnica introducida por Moxie Marlinspike denominada 'SSL Stripping' permitió modificar cada enlace HTTPS de páginas por las que la víctima estaba navegando, por enlaces HTTP.

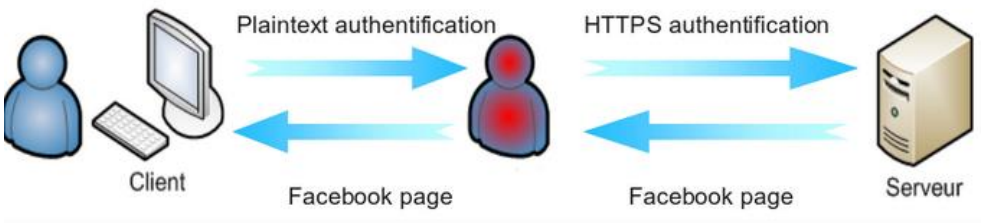
Hasta el año 2010, SSL Stripping funcionó correctamente, fué entonces cuando, con la llegada del mecanismo HSTS o *"HTTP Strict Transport Security"*, se garantizó la seguridad ante estos ataques, ayudando a proteger la degradación del protocolo y secuestro de cookies, además de permitir a los servidores web declarar a los navegadores que sólo deben interactuar con él mediante conexiones HTTPS. Este mecanismo se incorporó a los navegadores que utilizamos hoy en día.

En el año 2014, Leonardo Nve Egea presentó SSL Srip 2, herramienta mejorada de su antecesor que permitía eludir las políticas de HSTS, rebajando los enlaces HTTPS a HTTP y, a su vez, añadiendo un nombre de dominio secundario personalizado. Los enlaces resultantes no eran válidos para ningún servidor DNS, pero gracias a la interceptación de paquetes, es el propio intruso quien resuelve los nombres de host. Por lo tanto, una página web accedida de la siguiente forma:

> https://www.facebook.com/

Durante un ataque de derivación HSTS lo cambiaría a:

> http://wwww.facebook.com/



Tipos de ataque

- **Simulación de punto de acceso inalámbrico**. Un modelo de ataque dirigido sobre todo a los usuarios de dispositivos móviles. Se basa en la simulación de un punto de acceso inalámbrico de una red inalámbrica pública, como las de las cafeterías o las de los aeropuertos. En ello, un atacante configura su ordenador de tal manera que este se convierta en una vía adicional para acceder a Internet (probablemente una con una calidad de señal mejor que el propio punto de acceso). De esta manera, si el atacante consigue engañar a los usuarios más ingenuos, este puede acceder y manipular la totalidad de los datos de su sistema antes de que estos se transmitan al verdadero access point o punto de acceso. Si este requiere autenticación, el atacante recibe para ello los nombres de usuario y contraseñas que se utilizan en el registro. El peligro de convertirse en el blanco de estos ataques man-in-the-middle se da particularmente cuando los dispositivos de salida se configuran de tal manera que se pueden comunicar automáticamente con los puntos de acceso con mayor potencia de señal.

- **Escucha activa.** En este caso, el atacante logra acceder a la red en la que se encuentra la víctima interceptando sus comunicaciones, obteniendo y/o modificando información.

- **Man-in-the-browser .** En él, el atacante instala malware en el navegador de los usuarios de Internet con el objetivo de interceptar sus datos. Si se introducen programas en el navegador de un usuario de forma clandestina, estos registran en un segundo plano todos los datos que se intercambian entre el sistema de la persona que ha sido víctima del ataque y las diferentes páginas web. De esta manera, esta modalidad de ataque hace que los hackers puedan intervenir en una gran cantidad de sistemas con relativamente poco esfuerzo.

Casos reales

- La Agencia de Seguridad Nacional de EE. UU. Se hizo pasar por Google y se reveló en 2013 cuando Edward Snowden filtró al público los documentos de la NSA. Al usar su capacidad para interceptar el tráfico y falsificar los certificados SSL, la NSA pudo mantener un registro de las búsquedas de Google potencialmente de cualquiera.
- Comcast fue capturado al inyectar JavaScript en su tráfico web para mostrar sus propios anuncios en lugar de los alojados en sitios de terceros.
- Se encontró que Superfish , un programa de adware, estaba escaneando el tráfico SSL e instalando certificados que le permitían interceptar y redirigir el tráfico seguro.
- Una falla importante en las aplicaciones bancarias en los teléfonos con Android abrió docenas de aplicaciones a los ataques MITM.

Formas de protegernos ante ellos

Las formas más efectivas para proteger nuestro equipo o nuestra red ante estos ataques son las siguientes:

- **Tablas ARP estáticas**: Los MITM existen gracias al ARP Poisoning, y éste gracias a que el caché ARP se actualiza dinámicamente. Poniendo la tabla de caché estática se solucionaría este problema, pero cualquier cambio de dirección de cualquier pc tiene que ser actualizado a mano en los demás, por eso solo se usa en redes pequeñas que sean fácilmente operables.

- **DHCP snooping**: El caché ARP no tiene sentido debido al protocolo de configuración dinámica ya que, este protocolo ofrece dinámicamente una configuración para cada terminal. Este tipo de arquitectura es más segura y cómoda , ya que un nuevo terminal es fácilmente reconocible, aunque facilita otro tipo de ataque como el de la clonación de DHCP, se monta un DHCP falso para que asigne dinámicamente la configuración de terminales, el primero que conteste será el que configure los terminales.

- **Redes VPN**. De esta manera la conexión quedaría cifrada entre el cliente y el proveedor de servicios VPN, haciendo más dificultosa la tarea de acceder a la información interceptada.