UNIVERSIDAD DEL ISTMO

CAMPUS TEHUANTEPEC

MATERIA:

Redes de Computadoras II.

DOCENTE:

I.C. Carlos Mijangos Jimenez.

ALUMNO (A):

Karla Guadalupe Cordero Luna.

ACTIVIDAD: INVESTIGACIÓN MITM

SEMESTRE:

7°

PARCIAL:

1°

CARRERA:

Ingeniería En Computación.

FECHA DE ENTREGA: LUNES 27 DE OCTUBRE DE 2025.

Introducción

Un ataque *Man-in-the-Middle* (MITM) ocurre cuando un atacante logra situarse entre dos partes que se comunican (por ejemplo: un usuario y un servidor) de modo que puede escuchar, interceptar y, en muchos casos, modificar la información intercambiada sin que las víctimas lo detecten. Los MITM pueden dirigirse a credenciales, cookies de sesión, correos, información financiera y cualquier dato que viaje en la red. La gravedad varía según si la comunicación está cifrada o no y de las medidas de protección (TLS/HTTPS, HSTS, DNSSEC, etc.).

Desarrollo

1) Clasificación general

- Pasivos: el atacante solo escucha (eavesdropping) para recopilar información — por ejemplo capturar contraseñas o cookies en texto claro.
- Activos: el atacante altera el tráfico (reenvío, modificación de paquetes, suplantación) — por ejemplo insertando contenido malicioso, redirigiendo a páginas falsas o suprimiendo cifrado.

(Esta distinción importa porque las contramedidas y la detección son distintas: los pasivos son difíciles de detectar; los activos a menudo generan síntomas de red anómala).

2) Tipos y técnicas comunes de MITM (explicación + riesgo)

a) ARP spoofing / ARP poisoning

En redes LAN Ethernet, el protocolo ARP (Address Resolution Protocol) traduce IP → MAC. Un atacante envía respuestas ARP falsas para asociar su MAC con la IP del gateway, redirigiendo así el tráfico hacia sí mismo (MITM en la LAN). Muy usado en redes Wi-Fi públicas.

b) DNS spoofing / DNS cache poisoning

El atacante inserta respuestas DNS falsas en la caché de un resolutor o responde con direcciones IP equivocadas, de modo que las víctimas son dirigidas a servidores controlados por el atacante (phishing, falsificación de sitios). DNSSEC es una de las mitigaciones protocolarias.

c) Rogue Wi-Fi / Evil Twin / Rogue access point

El atacante crea un AP (punto de acceso) falso con un SSID legítimo; los usuarios se conectan y todo su tráfico pasa por el atacante, quien puede espiar o modificar las comunicaciones. Muy peligroso en cafeterías, aeropuertos, congresos, etc.

d) HTTPS / TLS interception por certificados fraudulentos o rotos

Si un atacante logra que el navegador confíe en un certificado fraudulento (por ejemplo mediante una CA comprometida o instalando un certificado raíz malicioso en el equipo), puede interceptar y descifrar tráfico HTTPS sin alertas. Este vector fue explotado en incidentes reales (ver "Casos famosos").

e) SSL/TLS downgrade y SSLStrip

Herramientas y técnicas (p. ej. *sslstrip* presentado por Moxie Marlinspike) convierten o fuerzan conexiones HTTPS a HTTP inseguro, permitiendo capturar credenciales cuando la web no fuerza siempre HTTPS. HSTS y listas de precarga ayudan a mitigar este riesgo.

f) Session hijacking y cookie theft (sidejacking)

Captura de cookies de sesión (por ejemplo en redes no cifradas) permite al atacante "tomar" sesiones activas sin conocer la contraseña. Herramientas demostrativas han probado la facilidad de esto en redes públicas.

g) BGP / IP hijacking (intercepción a gran escala)

Explotando la confianza del sistema de enrutamiento BGP, un actor (malicioso o erróneo) puede anunciar prefijos que no le pertenecen y desviar grandes volúmenes de tráfico a otras rutas donde puede inspeccionarlos o manipulados — potencial para espionaje a gran escala. Ejemplo famoso: el redireccionamiento global de tráfico de YouTube en 2008.

3) Casos famosos (estudio de incidentes)

Caso A — DigiNotar (2011)

En 2011 la autoridad de certificación neerlandesa DigiNotar fue comprometida y se emitieron cientos de certificados fraudulentos (incluido un certificado comodín para Google). Esos certificados se usaron para ataques MITM a usuarios iraníes, interceptando correo y tráfico web. La gravedad hizo que navegadores revocaran la confianza a DigiNotar y la compañía quebrara. Este caso muestra el riesgo de que una CA sea comprometida: confianza a gran escala y espionaje masivo.

Caso B — Superfish / Lenovo (2015)

Algunos portátiles Lenovo venían con un software publicitario (Superfish) que instalaba un certificado raíz común en el equipo y realizaba inspección de HTTPS para insertar anuncios. Ese certificado tenía una clave privada duplicada en muchos equipos, lo que permitió a atacantes

cualquiera crear certificados falsos y realizar MITM de conexiones HTTPS. El caso generó sanciones y retiradas del software; es un ejemplo de cómo software preinstalado o proveedores pueden debilitar la seguridad del usuario.

Caso C — Firesheep (2010) — demostración de sidejacking

Firesheep fue una extensión para Firefox que, al usar una red Wi-Fi compartida, capturaba cookies de sesión no cifradas y permitía a un atacante hacerse pasar por el usuario en servicios populares (Facebook, Twitter). Aunque no cifraba el tráfico, el impacto fue inmediato: impulsó a los grandes servicios a desplegar HTTPS por defecto. Es un caso pedagógico sobre por qué el cifrado end-to-end y la insistencia en HTTPS son críticos.

Caso D — BGP / YouTube hijack (2008)

En febrero de 2008, Pakistan Telecom anunció rutas para un bloque de IPs de YouTube para bloquear internamente el servicio; por error estas rutas se propagaron y redirigieron buena parte del tráfico de YouTube a proveedores paquistaníes, causando una interrupción global. Aunque inicialmente fue un intento de censura, el evento demostró la posibilidad de desviar tráfico a gran escala (vectores potenciales de MITM/espionaje).

Estos casos ilustran que los MITM pueden ser locales (Wi-Fi, ARP), de aplicación (cookies, software malicioso) o infraestructurales (CA comprometida, BGP), y que las consecuencias van desde robo de credenciales hasta espionaje masivo.

4) Contramedidas y buenas prácticas (resumen)

- Siempre HTTPS y HSTS: sitios bien configurados usan HTTPS en todo el sitio y HSTS para prevenir downgrade/sslstrip.
- Evitar Wi-Fi público o usar VPN: conexiones a redes no confiables deben usar túnel VPN para proteger tráfico.
- DNSSEC y resolutores confiables: para reducir DNS spoofing.
- Gestión segura de CAs y pinning: limitar confianza a CAs necesarias, usar pinning o transparencia de certificados cuando aplique (Certificate Transparency). El caso DigiNotar muestra por qué la gobernanza de CAs es crítica.
- Monitoreo y segmentación de red: proteger redes LAN contra ARP spoofing (snooping, inspección de ARP, uso de switch seguros), y aplicar autenticación en puntos de acceso.

- Actualizaciones y software de confianza: evitar software con privilegios (p. ej. roots) que pueda instalar certificados o modificar la pila TLS (lecciones del incidente Superfish).

Conclusión

Los ataques Man-in-the-Middle son una familia de técnicas con impacto muy variable: desde la captura de cookies en una cafetería hasta la interceptación masiva mediante certificados fraudulentos o la manipulación del enrutamiento global. La defensa es tanto técnica (TLS/HSTS, DNSSEC, VPN, monitoreo de red) como organizativa (gestión de CAs, control de software preinstalado, políticas de seguridad). Los incidentes históricos (DigiNotar, Superfish, Firesheep, los secuestros BGP) muestran dos lecciones clave: 1) la seguridad no es solo del servidor o del cliente, es de toda la cadena de confianza; 2) pequeñas debilidades (un CA comprometido, un certificado raíz instalado, una red Wi-Fi insegura) pueden provocar consecuencias a gran escala. Implementar medidas defendibles y asumir que el canal puede ser atacado (defensa en profundidad) es la mejor manera de mitigar el riesgo MITM.