Ataques Man-in-the-Middle

Grupo 1:

David Cabezas Berrido

dxabezas@correo.ugr.es

Patricia Córdoba Hidalgo

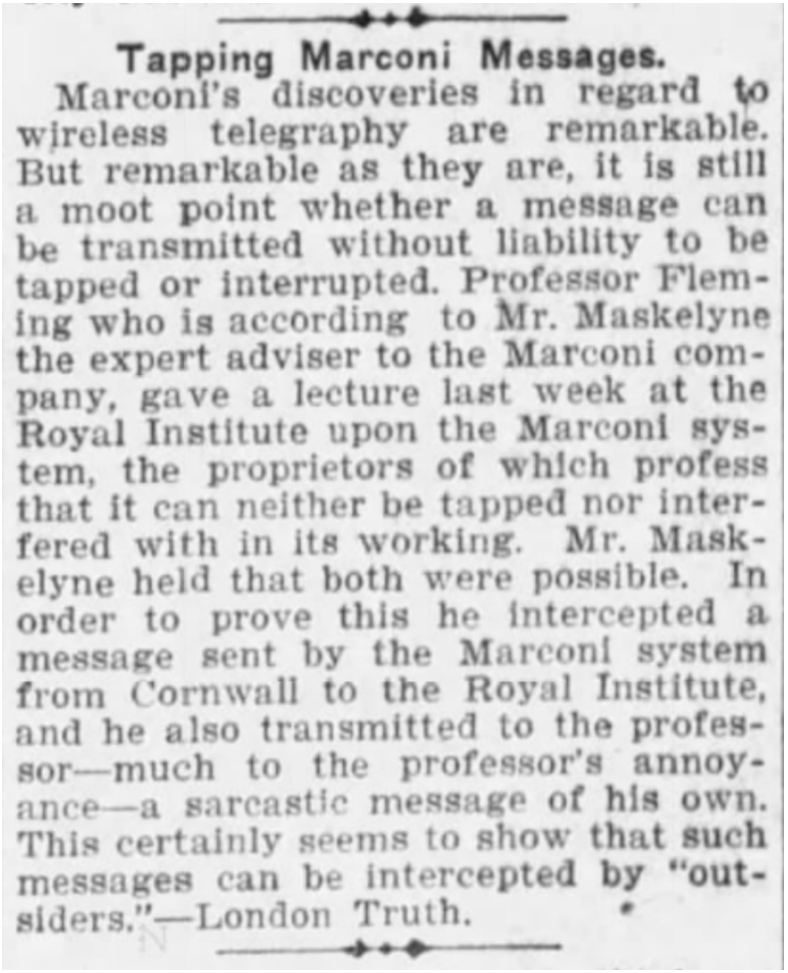
patriciacorhid@correo.ugr.es

Contenido

Contenido

Motivación

Vamos a presentar uno de los ciberataques más comunes en la historia y en la actualidad. Al igual que con otros tipos de ciberataques, conviene estar informado sobre las distintas formas en las que se manifiesta y saber cómo protegerse de él.



Tapping Marconi Messages.

Marconi's discoveries in regard to wireless telegraphy are remarkable. But remarkable as they are, it is still a moot point whether a message can be transmitted without liability to be tapped or interrupted. Professor Fleming who is according to Mr. Maskelyne the expert adviser to the Marconi company, gave a lecture last week at the Royal Institute upon the Marconi system, the proprietors of which profess that it can neither be tapped nor interfered with in its working. Mr. Maskelyne held that both were possible. In order to prove this he intercepted a message sent by the Marconi system from Cornwall to the Royal Institute, and he also transmitted to the professor—much to the professor's annoyance—a sarcastic message of his own. This certainly seems to show that such messages can be intercepted by "outsiders."—London Truth.

Figura: Recorte de periódico: Austin-American Statesman, 17 de julio de 1903.

NSA disguised itself as Google to spy, say reports

If a recently leaked document is any indication, the US National Security Agency -- or its UK counterpart -- appears to have put on a Google suit to gather intelligence.

Figura: Caso Snowden. Se descubrió que la NSA se hacía pasar por Google para robar información.

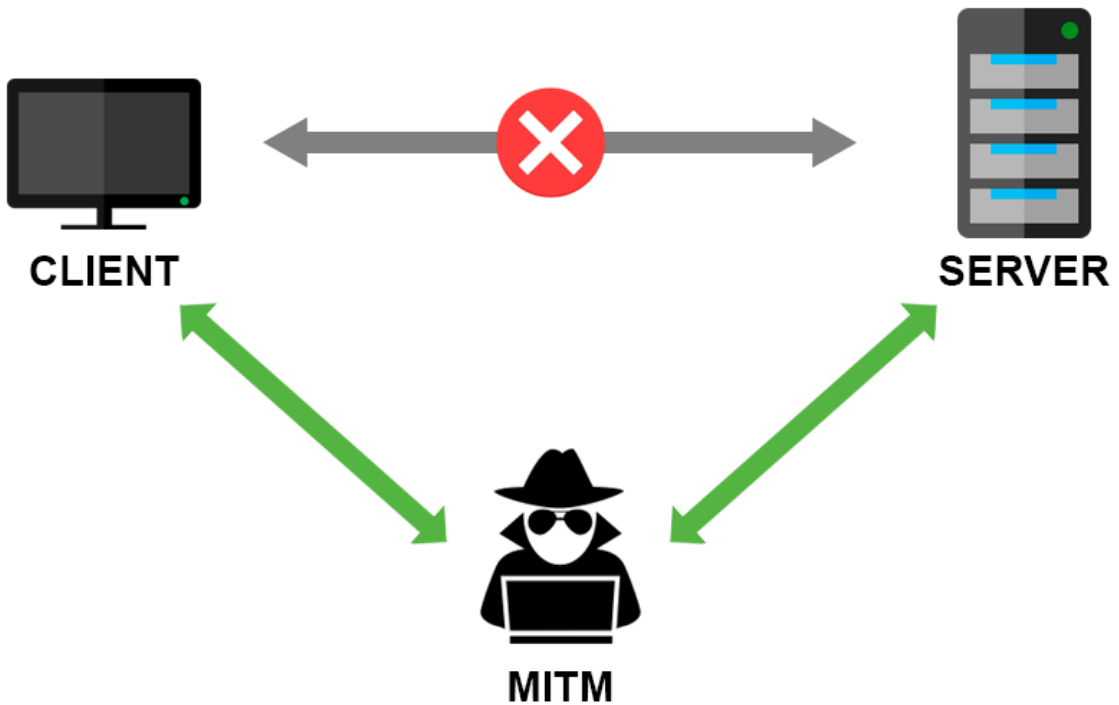
'Fraudsters hacked emails to my solicitor and stole £340,000 from my property sale'

Figura: Robo del pago de una vivienda.

Contenido

Descripción

Los ataques (MITM) son una clase de ciberataques en los que un individuo (el atacante) logra infiltrarse en una comunicación entre dos partes legítimas, de forma que ambas partes ignoran su presencia.



Ejemplo

1. Bob (cliente) quiere conectarse a la web del banco (servidor) para hacer una transferencia de 500€ a la cuenta XXX.

2. Alice (atacante) intercepta la conexión y conduce a Bob a una réplica de la web del banco creada por ella.

3. Bob intriduce sus credenciales, que son recibidos por Alice.

4. Alice se conecta a la aplicación del web con los credenciales de Bob.

5. Bob rellena el formulario (falso) para realizar la transferencia.

Ejemplo

6. Alice recibe el formulario y rellena uno (real) para enviar 5000€ a la cuenta YYY, registrada como Bob en la aplicación.

7. Cuando Alice recibe el siguiente mensaje del banco: “Hola Bob, para confirmar su transferencia de 5000€ al número de cuenta YYY, sume los dígitos 1, 2 y 7 de su código secreto e introduzca el resultado”.

8. Alice envía a Bob a través de la aplicación falsa el mensaje: “Hola Bob, para confirmar su transferencia de 500€ al número de cuenta XXX, sume los dígitos 1, 2 y 7 de su código secreto e introduzca el resultado”.

9. Bob envía a Alice la respuesta de seguridad, que Alice utilizará para robarle 5000€.

Inconveniente

Este ataque requiere de un papel muy activo del atacante para que las víctimas no se percaten del engaño.

Si sólo queremos acceder a la información, se puede reenviar a las víctimas de forma automática. Si queremos alterarla, el proceso es menos automatizable.

Inconveniente

Este ataque requiere de un papel muy activo del atacante para que las víctimas no se percaten del engaño.

Si sólo queremos acceder a la información, se puede reenviar a las víctimas de forma automática. Si queremos alterarla, el proceso es menos automatizable.

Contenido

ARP Cache Poisoning

Un atacante envía a los integrantes de la comunicación mensajes en los que indique que la dirección IP del otro integrante corresponde con la dirección física del atacante.

El atacante se infiltra en la conversación haciéndose pasar por ambas víctimas y recibiendo los mensajes que vayan destinados a cualquiera de las víctimas desde la otra.

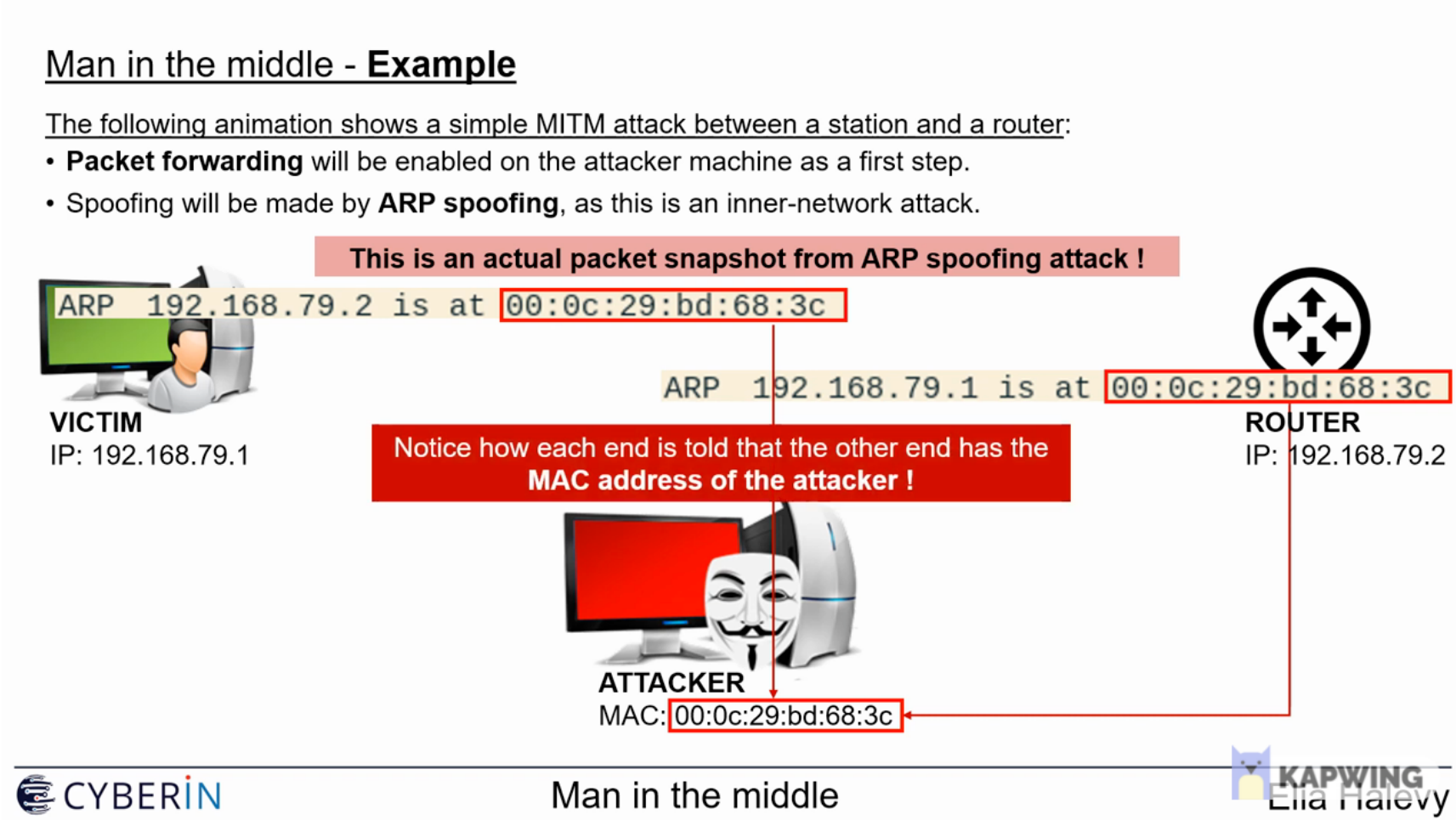


Figura: Esquema de ARP Cache Poisoning. Fotograma extraído del tutorial https://www.youtube.com/watch?v=fbXu8EX0hsI.

DNS Cache Poisoning

Un atacante se infiltra en la comunicación entre un usuario y un servidor DNS, para proporcionarle al usuario una entrada DNS falsa que conduce a una página creada por el atacante.

Figura: Esquema de DNS Cache Poisoning. Artículo "A Review of Man-in-the-Middle Attacks", Figura 5.

HTTPS Spoofing

El atacante elabora un página HTTPS con dominio similar y contenido idéntico al de otra página a la que quiere acceder una de sus víctimas.

Por ejemplo, si visitamos el enlace https://www.xn–80ak6aa92e.com veremos que el dominio que aparece en la barra de navegación se asemeja a https://www.apple.com, mientras que el contenido es totalmente distinto y ambas páginas utilizan HTTPS.

Normalmente se utiliza el Phishing para hacer que la víctima haga click en uno de estos enlaces engañosos.

Wi-Fi Eavesdropping

Los atacantes pueden interceptar el tráfico en redes públicas o inseguras, o incluso crear una red WiFi para ver todo el tráfico que circula por ella. Si un usuario escribe sus credenciales, contraseñas, cuentas bancarias o cualquier tipo de información sensible en esa red, el atacante puede robarlas y usarlas en su beneficio.

Session Hijacking

El atacante puede hacerse con la cookie que contiene información relativa a la sesión que se crea al iniciar la comunicación con un servidor web. Así, éste será capaz de navegar por dicha web haciéndose pasar por el usuario.

Contenido

Cifrado con clave asimétrica

Bajo el supuesto de que el intercambio de claves públicas pueda producirse en un canal seguro (lo que no siempre ocurre), el sistema de cifrado asímetrico permite establecer un canal de comunicación libre de este tipo de ataques.

Estas claves son utilizadas tanto para descifrar los mensajes como para identificar al emisor, por lo que ningún atacante podría acceder a la información cifrada ni suplantar a sus víctimas sin conocer sus claves privadas.

Contenido

Simulación de ataque

Vídeo simulando un ataque MITM con ARP Cache Poisoning.

Seguimos el tutorial de: https://www.youtube.com/watch?v=fbXu8EX0hsI.

Contenido

Consejos y buenas prácticas

- Evitar el uso de redes Wi-Fi públicas y sin contraseña.
- Evitar hacer logins desde redes públicas como las de cafeterías o bibliotecas.
- Evitar navegar en sitios web que no utilicen protocolo HTTPS.
- Usar varios factores de autenticación.

Consejos y buenas prácticas

- Utilizar algún protocolo de cifrado y firma para intercambiar mensajes importantes.
- Cerrar la sesión en páginas antes de cerrarlas.
- Seguir el principio de confianza cero: No aceptar conexiones hasta verificar su procedencia.

Indicios de que estamos siendo víctimas de un ataque MITM

- Experimentamos retrasos en la comunicación, o desconexiones inesperadas.
- Aparecen direcciones extrañas en nuestra barra de navegación.
- Tenemos conexiones a sitios desconocidos.

Cómo actuar caso de sospecha

- Monitorizar la actividad de red con Wireshark o similares.
- Inspeccionar las conexiones actuales.
- Usar un network sniffer (una herramienta para espiar tráfico) de forma defensiva.
- Buscar software malicioso en nuestro equipo.

Contenido

Bibliografía

Ataque MTIM en demostración de Marconi.

1. https://havocshield.com/2020/07/cybersecurity-history-the-very-first-man-in-the-middle-attack.
2. https://www.bbc.com/mundo/noticias/2016/05/160523_primer_hacker_caballero_victoriano_marconi_fleming_maskelyne_finde_dv.

Ejemplos notables.

4. Escándalo de la NSA: https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports.
5. Estafa a la familia Lupton: https://www.conveyancingassociation.org.uk/fraudsters-hacked-emails-to-my-solicitor-and-stole-340000-from-my-property-sale-a-case-study-from-ca-affiliate-members-lawyer-checker.

Bibliografía

Ataque MITM: Explicación y tipos.

6. What is a MITM Attack, Detection and Prevention Tips: https://www.varonis.com/blog/man-in-the-middle-attack.
7. A Review of Man-in-the-Middle Attacks: https://arxiv.org/pdf/1504.02115.pdf.
8. Punycode alert: https://github.com/yabirgb/punycodeAlert.

Cifrado y firma para evitar ataques MITM.

9. Asignatura Seguridad y Protección de Sistemas Informáticos. Apuntes del profesor Francisco Miguel García Olmedo.

Bibliografía

Simulación.

10. Redirección de paquetes: https://www.garron.me/es/gnu-linux/habilitar-ip-forward-linux-ubuntu.html.
11. Tutorial YouTube: https://www.youtube.com/watch?v=fbXu8EX0hsI.

Consejos para evitar ser víctimas del ataque.

12. What is a MITM Attack, Detection and Prevention Tips: https://www.varonis.com/blog/man-in-the-middle-attack.
13. Zero Trust: https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.