Robert Fink
INFOTC2910
Research Report

Wireless Network Security

1. Source: https://www.owasp.org/index.php/Man-in-the-middle_attack

This source gives a description of Man in the Middle (MiM) attacks and the basics of how a MiM attack works. Firstly an attacker must intercept a communication link between two systems. Http transactions happen over the TCP connection between the client and server, so that is the target. The attacker must then split the TCP connection into 2 TCP connections and act as a proxy between the victim and server. This can easily be done over https as well with 2 SSL connections. A warning will be issued to the user in most cases because the attacker will likely not have a valid digital certificate, but it is very possible for the user to ignore this warning and fall victim the MiM attack. After the TCP connection is intercepted the attacker can read, insert, and modify data in the intercepted communication.

2. Source: http://www.csoonline.com/article/2997241/advanced-persistent-threats/meet-the-man-in-the-middle-of-your-next-security-crisis.html

This source gives more information on Man in the Middle attacks. It quotes Michael H. Davis, CISO, American Bureau of Shipping, saying, "Any communication path can have it's own form and methods to exploit Man in the Middle attacks." One of the more common MiM attacks out there deal with fake Wi-Fi access points. Commonly available tools like Kali Linux, Aircrack-ng, Wireshark, Ettercap, etc. can be used to accomplish setting up fake Wi-Fi access points. It is also possible to infect a victim with a Trojan horse that infects the web browser and taps communications between the server and browser. From there an attacker can sniff http traffic for the session ID, from there an attacker can hijack a session, enabling them to access the web server, the user, or both. Also, with the increasing use of cloud platforms it is important to mention that it is possible for attackers to steal all the data stored in their cloud account. This is called a Man-in-the-Cloud attack. It is accomplished by stealing an OAuth token. Common tools like Box, Dropbox, Google Drive, and OneDrive use OAuth tokens. If an attacker steals an OAuth token they just place the token on their own device, and the tool with synchronize all your stored data on the attackers device.

3. Source: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html

ARP cache poisoning is an older MiM attack. It is easy to execute and highly effective. It allows an attacker to eavesdrop on all network traffic of the victims as long as they are on the same subnet. When a device sends and receives and ARP request and reply, respectively, the transmitting device will update its ARP cache table and this allows the devices to communicate wit each other. ARP is an insecure protocol and because of that, devices using ARP will accept updates at any time. This means that any device can send an ARP reply packet to some host and it will force an update on the hosts ARP cache. After that an attacker can intercept communications from the victim.

4. Source: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html

DNS spoofing is another MiM technique. This technique is called DNS ID spoofing. A simple model of DNS is that a client sends a query containing a web address like www.google.com and the DNS server responds with an IP that can be used to connect to Google's homepage. Every DNS query sent over the network contains a unique ID that ties queries and responses together. So if an attacker sends a fake response packet containing that unique ID, the victim will accept the packet and think it is the real response to its request. This means an attacker could reroute a user trying to access the bank account online to a fake website that looks like their online banking site, where a user could unknowingly enter their private banking information. This is accomplished by first ARP cache poisoning the target device to reroute traffic through the attacker's device to intercept the DNS request, then the attacker just sends the fake response packet and the victim is redirected to the malicious site.

5. Source: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html

Yet another MiM attack is SSL Hijacking. Secure Sockets Layer is a modern means of encryption over network communications. Secure services use SSL over HTTP known as HTTPS. This MiM attack is especially effective for malicious attackers because the information being transmitted over communications with these services is highly private information and definitely not for the eyes of attackers with bad intent. In order to defeat SSL the concept is to block a request from HTTP to HTTPS, meaning the encrypted SSL connection does not take place. A well-known security researcher whose name is Moxie Marlinspike developed a tool called SSLstrip, which is used to accomplish this.

6. Source: http://searchsecurity.techtarget.com/answer/Defense-best-practices-for-a-man-in-the-middle-attack

Protecting oneself from MiM attacks should be considered pretty important. ARP is an insecure protocol by nature but there are some steps a user can take to help protect themselves. A browser should force https wherever possible to enable SSL encryption, so if an attacker does try a MiM attack, the information they see will at least be encrypted. Also, when communicating over HTTPS, web servers use trusted certificates, and an attacker would not have that certificate. Another layer of security a user should implement is a Virtual Private Network.

7. Source: https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

HTTP Strict Transport Security (HSTS) is a web security policy that allows web servers to declare that a web browser should only interact with it using HTTPS and never via HTTP. This can fix the SSL-stripping MiM attacks.

8. Source: https://www.us-cert.gov/ncas/alerts/TA15-120A

This is a US government alert describing some dangers of MiM attacks and ways to protect oneself. US-CERT recommends upgrading to the most recent Transport Layer Security (TLS/SSL). They also recommend Certificate Pinning. This means a user can be configured to "only trust this certificate" effectively blocking fake certificates. Additionally it is recommended to implement DNS-based Authentication of Named Entities (DANE). Dane is bound to DNS, which used Domain Name System Security Extensions. It allows the domain to sign statements by itself about which entities are authorized to represent it.

9. Source: http://news.mit.edu/2011/secure-wifi-0822

Fake Wi-Fi access points rely on broadcasting a stronger signal strength with the same SSID of a legitimate network, booting a user off a network, and then relying on that user's auto-reconnect to known networks feature to steal the connection from the user and act as a proxy to the intended server, without the user knowing the attacker is really in control of the connection. Security researchers Douglas Ross along with the help of Dina Katabi have come up with a Wi-Fi security scheme that blocks this attack. It deals with transmitting a second sequence of numbers after transmitting the encryption key. The attacker will not be able to match this sequence, so the legitimate access point can be found and connected to directly.

10. Source: http://searchmidmarketsecurity.techtarget.com/tip/Avoid-security-risks-of-Free-Public-WiFi-wireless-ad-hocs

Free Wi-Fi is often unprotected. Unprotected networks are the ideal place for MiM attacks. An attacker can easily setup a spoofed access point and launch a Man in the Middle attack. From there they could monitor any of the victim's traffic, which could contain information like SSN, legal name, email, passwords, bank info, etc. Free unprotected Wi-Fi and Wi-Fi in places like hotels where all users connect with the same password are hotbeds for MiM attacks. Unprotected Wi-Fi is very bad.