IT 125-41194

Alex Arnold

4-21-25

WLAN Threats  
  
The topic I chose to look into for the WLAN Threats chapter is the man in the middle attack. Let’s start by defining these two terms. According to The Cisco Network Academy

**Man in the Middle Attack** – “In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. There are many ways in which to create a MITM attack.”

I happen to like googles description a bit better “A man-in-the-middle (MITM) attack is a cyberattack where an attacker intercepts and relays communication between two parties, creating the illusion that they are directly communicating when, in reality, the attacker controls the entire conversation. This allows the attacker to eavesdrop on sensitive information, modify messages, or inject malicious code. “ due to it being a bit more descriptive about what the attacker is doing / has the ability to do.

One method of performing a man in the middle attack is to use an AP disguised as a legitimate AP to perform a man in the middle attack. This is referred to as an Evil Twin attack.

The danger in this attack is that the attacker has control over the access point that the victim is using and these will not have security measures in place to protect the victims data. This allows the attacker to capture packets and view information that the user is sending to the places they visit on the internet. This can allow them do things like having the users computer send unencrypted packets to them and then encrypting them to the server (the server wants encrypted info). In essence the server and the victim have no idea that there is an issue because both end up getting what is expected and in the expected way so there is no obvious “tell” that something is incorrect as things are functioning normally. The Attacker can also set up a captive portal to capture user information such as username and password or even payment information through such a method.

To avoid such a situation there are a few things that can be done.

* Be skeptical of public networks in general. The easier it is to connect to a wireless network the easier it is to spoof
* Use A VPN – the vpn will encrypt the data before it leaves your system helping to prevent the attacker from reading you data.
* Use a wireless hotspot. If you can connect through your own device the threat is mitigated.
* Ensure that the sites you use are using HTTPS to encrypt the data.