

Types of Threats

William H. Wolfe II (10 mins)

Some of the classifications of general wireless security threats are listed here for reference. On-Wire Attacks- that's basically where you can allow for a client-to-client backdoor access to the secured network.

We have Over-the-Air Attacks-that's our evil twin or honeypot APs, i.e. also rogue style APs fall into that category in some cases.

Reconnaissance basically looking for the network vulnerabilities that we have based upon our wireless environment.


Another type of security threat is denial-of-service attacks. Those denial-of-service attacks, we going to speak about a little bit later, but one of them is actually to intercept and crafts management frames and control frames that could otherwise disassociate or de-authenticate a user from the wireless environment.

We also have cracking tools such as packet sniffers, or something like a wireless pineapple, or the AirPcap tool. We'll speak about those a little bit later as well.

What's interesting about wireless security threats is that some of the threats are actually not related to either on-wire or over-the-air attacks using a technology. Things such as a microwave oven, or general RF radio-frequency jamming tools, even radar. In fact, there are some specific frequencies and channels in the 802.11ac wave 1 and wave 2 environment that are directly affected by radar. In the case of microwave ovens, if you are a 2.4GHz wireless environment and you are using channel 11, microwave ovens actually interfere specifically in the channel 11 frequency range.

So, what are some details behind some of these existing vulnerabilities and threats and some very specific examples? Well, we have wireless LAN sniffing, and war driving. We have encryption vulnerabilities. WEP, or Wired Equivalent Privacy, which was the first security used in wireless is extremely vulnerable We want to take a look at that in detail a little bit later on. But there are also vulnerabilities in its replacement, which is WPA and even WPA2.

Denial-of-Service attacks, again using the de-authentication and disassociation frame mechanism which by the way, the MFP or Management Frame Protection add-on that Cisco offers will help to mitigate some of that. We'll discuss that a little bit more in detail as well.



We also have authentication vulnerabilities that is the ability to using a dictionary attack infiltrates the wireless environment by authenticating to the SSID which will then allow you to associate to the access point.

Also MITM, otherwise known as Man-in-the-Middle attacks.

There's also address spoofing attacks. Address spoofing, primarily MAC address spoofing will allow an unauthorized wireless client to connect to the environment if, in fact, layer two MAC address filtering and security is enabled, We'll talk a little bit more about how and why you might want to use that and how that, along with other security mechanisms in combination, can help build more layered security approach.


How does a specific type of wireless exploit take place? Well, I could actually use a packet sniffing tool such as a wireless pineapple or AirPcap or others, and I can listen to the probed management frames coming from a client because those will have the Service Set Identifier (SSID) based upon what's stored in that wireless client's profile list of past SSIDs that have been connected to or even stored profiles.

Passive WEP key sniffing is another way that an exploit can take place. Now, if you're not using WEP, obviously Passive WEP sniffing isn't going to be of concern. WEP has been pretty much deprecated out of the industry and most client devices, for quite a number of years, even though there are still some devices that support WEP and some that actually still only will use WEP because they're very specific devices primarily used in inventory control and warehouse management but even those devices have since been updated and upgraded to newer versions by the companies that manufacture them.

The initial phases of a wireless LAN security exploit comes in the way of discovering the wireless networks that are around you. This is generally done by monitoring for the probes and the probe responses. This could also be done by sniffing the broadcast frames from the beacons from the access points. If you are failing to turn off your broadcast SSID, most data frames, as mentioned earlier, are going to be encrypted, and that will keep them from being infiltrated during a packet sniffing process. However, if it's a WEP encrypted frame, it can be processed offline, and you can get the WEP key and decrypt the packets. Hence, why WEP has been a deprecated security and encryption method.

Some of the ways that we can de-authenticate a user is by using the Kismac tool or other packet crafting tools or you could inject a de-authentication management frame into the RF environment and take the client off the network, and then continue to sniff as that client tries to re-authenticate to the SSID environment. This is mitigated as mentioned before using management frame protection.

Some wireless LAN sniffing and SSID broadcasting packet capture examples. As you can see, this is a Cisco Aironet wireless access point and we're looking at a probe response frame, and you can see that we see the Service Set Identifier listed as



'LINC5'. This is done because of the fact that the authentication is open authentication, which we'll discuss a little bit later as well. Even though the SSID broadcast has been disabled in this example, because this is a probe frame you're going to actually see the SSID listed.