Wireless networks operate on both the 2.4 and 5.0 GHz frequencies under the 802.11 a/b/g/n standard. Each one of these ranges has a number of channels based on the frequency. Of the frames that exist there are three types. Those types under the 802.11 MAC frames are: data, control, and management which each, of course, utilized for different processes. Like in the disassociation and deauthentication lab we utilized the management frames to disconnect a device on an access point.

Instead of broadcasting and SSID to all surrounding devices there is a way to hid the SSID to make so that the user trying to connect essentially must have a ‘username’ (SSID) and the password to authenticate. Making it a ‘hidden’ device. A packet sniffer, usually utilized with a wireless card in monitor mode, can procure information about ESSID and BSSID and channel information by searching all frequencies and channels. In addition to these devices ‘hidden’ features being easily trumped the other problem is that most of these devices come with default credentials. Depending on the brand the default might be static across the access points or some do have a variation on passwords, but not by much.

One other issue with most access points is that their security features age out and don’t receive updates to ensure the users utilizing those access points are safe. Since there is still a large percentage of users on the WPA2 standard there are several exploits one can conduct against it. Denial-of-service attacks such as deauthentication, authentication flood, access point overloaded, and disassociation attacks make users vulnerable to service interruptions or even the evil twin attacks. This then can be used for Man-in-the-middle attacks.

Cracking the encryption using something called KRACK has been released to the world and can make it possible to eventually crack the password and then access the network. Another flaw that makes the WPA2 standards an antiquated technology.

There is a plethora of tools out there right now for anyone to download and use. Of course, there are consequences to using these tools and depending on the region some use them in even sniffing for networks and BSSIDs can get someone in trouble. There is something called Aircrack-ng which is a package full of different utilities under the -ng name. These all work together in creating a way to sniff packets, enable monitoring mode, attack a target, and even virtualize a network.

One way to test something like a man-in-the-middle attack is by using the airbase-ng tols to create a soft access point which then can be used to create a bridge to a consist a wireless and wired interface. Then by forcing a deauthentication and leveraging the soft access point an attacker could get a user’s device to attach to the rouge access point making it a way to monitor their network traffic and steal information from the access point on or anything coming in from the internet back to the user’s device.

In my opinion this is why we should not let vendors get away with either not updating older devices and ensuring that IoT and other wireless devices security is truly tested before being shipped to someone’s front door.

References

<https://www.researchgate.net/publication/310662676_Wireless_Network_Penetration_Testing_and_Security_Auditing>