P. Wagenseller III, J. Cummings, R. Kolnicki
Faculty Advisor: Dr. Feng Wang
School of Mathematical and Natural Sciences

Network Forensic Analysis: Uncovering Attacks in Wireless Networks

Introduction

Computer hacking and data breaches are on the rise. During 2018 there was an estimated 1,231 data breaches. Even Facebook saw 87 million records stolen. Worse still there is now an estimated 23.14 billion internet of things devices connected to the internet. Many of these devices primary communication mechanism is wireless and do not undergo rigorous security testing before being sold to the public.

In this project we conducted a variety of wireless network-based attacks. The goal here is to educate future cyber defenders on how to anticipate, identify, mitigate, and defend against attacks of varying magnitudes. This is done by capturing an example of the attack to educate students whom may end up in positions responsible for cyber defense.

We looked at the following attacks:

- **Beacon and Probe Response Flooding** – a form of denial of service attack that prevents a user from selecting the correct access point in a series of possible choices. This attack can also sometimes break nearby devices or confuse wireless intrusion detection systems.
- **Wireless DNS Injection** – a sophisticated attack in which we monitor the data coming from connected clients and maliciously inject DNS responses into the communication before the access point has a chance to retrieve the DNS result.
- **Evil Twin Attack** – a common attack where you masquerade as a legitimate looking access point while simultaneously behaving as a man-in-the-middle attack against all connected clients.

Methodology

Research and Select Attack	First, we research common attacks within the 802.11 specification. Then select an attack we wish to reproduce.
Design Attack	This is done usually with scapy a python packet manipulation library. However, in some cases we design the attack using a Raspberry PI that has been maliciously configured.
Launch Attack and Capture	Next, we launch the attack in a lab environment to avoid affecting nearby devices. While doing this we capture the packets associated with the attack using Wireshark and a network card set to monitor mode.
Analyze the Captured Result	Finally, we do a detailed analysis of the attack we captured using Wireshark. This gives us insight into what the attack looks like, it also gives us an idea of what might be good questions to ask about the attack.
Produce Questions	During the last step we produce a series of questions to ask students. These can be answered from information contained within the data capture.

Beacon and Probe Response Flooding

Figure 1 – Attacker creates endless stream of fake access points colored in red. Amongst a single real access point.

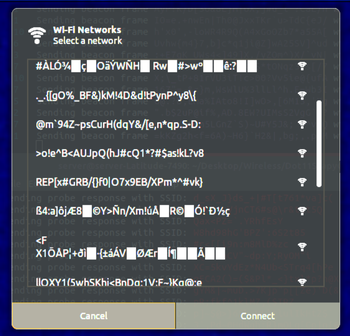


Figure 2 – Which network would you connect to?

- Beacon flooding is based upon the idea that wireless beacon frames are sent out periodically to tell your device that a wireless access point exist within the area. Beacon flooding abuses this by sending out fake beacon frames broadcasting access points that don't really exist. This is demonstrated in Figure 1.
- Probe response flooding is an extension of this type of attack. Periodically, your device sends out a probe request asking all nearby access points to notify it of their existence. When this happens, we send back several fake probe responses resulting in even more nonexistent access points appearing on your device. The result of this combined with beacon flooding can be seen in Figure 2.
- An attacker could even set the SSID names to be all the same as the organization they are targeting. For example, setting the name to be 'asu' for each fake access point. The user would be unable to determine which access point is real amongst all the fakes. This prevents the user from being able to connect to the access point.

Wireless DNS Injection

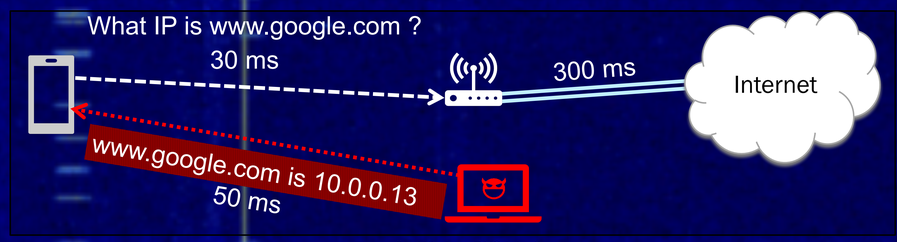
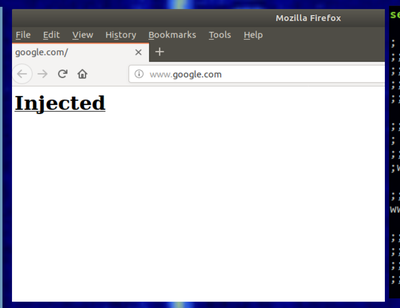


Figure 3 – Wireless DNS Injection

- Wireless DNS Injection is a timing-based attack whereby the attacker is closer to you than you are to the DNS server. An attacker can exploit this timing differences by monitoring the wireless channel for any DNS queries you submit. Upon seeing such a request, the attacker immediately responds with a fraudulent IP address claiming to be the authoritative answer.
- This causes your computer to be redirected to an attacker-controlled IP address, but your browser website would still claim to be at the requested site e.g. www.google.com. The basic concept of this is illustrated in Figure 3. Next, in Figure 4 we see this attack in action. Whereby a user has been redirected to a website not controlled by Google, and a dig request which returns a spoofed IP address for Google.



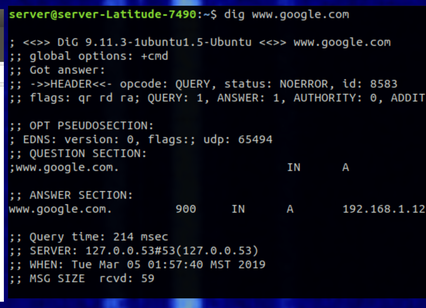


Figure 4 – Wireless DNS Injection

Evil Twin Attack

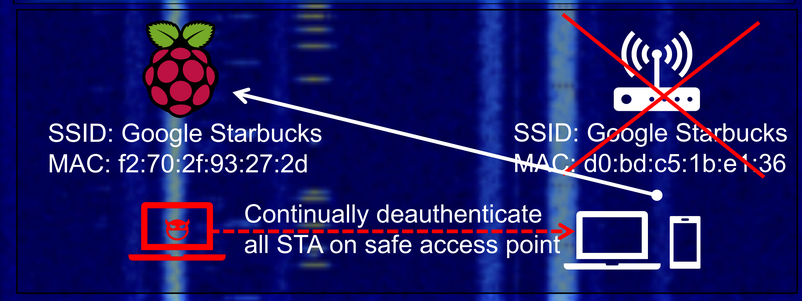


Figure 5 – Evil Twin Attack

- The concept of an evil twin attack is that an attacker sets up a nearby access point using the same SSID as that used by the enterprise or business. Once a user joins the evil twin functions as a man-in-the-middle device for all data flowing through it.
- In order to intercept user devices more rapidly an attacker may attempt to deauthenticate all user devices from the real access point. The user's devices then attempt to reconnect to an access point of the same SSID and channel. However, the only access point allowing reconnection is the evil twin.
- After a device connects to the evil twin the attacker gains control over all data streams coming from the device(s). This allows the attacker to perform any type of man-the-middle style attacks against the user.
- This could include SSL stripping, DNS spoofing, manipulation received website data, replacing entered online forum data while you perform an online purchase, injecting malware in place of downloaded documents, credential harvesting, phishing attacks, etc.

Conclusion

While this presentation shows some attacks that we conducted and analyzed. Many others were investigated which we did not show. The goal of this project is to educate students with real world attack examples. By doing so, we hope to improve student's ability to forensically analyze unknown attacks of increasing complexity.