# ISEC 325 Homework 08

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [1 point] Name and describe the two manners in which wireless networks are implemented.

   The first manner in which wireless networks are implemented uses Quadrature Amplitude Modulation (QAM) – In this method modulation technique data is encoded into radio signals. QAM combines both digital and analog signaling. It changes the amplitudes of two carrier waves using amplitude-shift keying or the amplitude modulation scheme. The second manner in which wireless networks are implemented is Quadrature Phase Shift Keying (QPSK)- QPSK provides multi bit carrying capability to encode digital data on an analog signal. QPSK is an enhancement of Binary Phase Shift Keying however QPSK uses four signal states instead of two.

2. [1 point] What is WEP, and why is it not considered at all secure for wireless networks?

   WEP is Wired Equivalent Privacy was an early attempt at wireless security it was too week cryptographically to provide protection against eavesdropping. It was too weak because it recycled IV initialization vectors which enabled attackers to use the RC4 cipher to reverse engineer the IV allowing them to decrypt packets and forge future packets the process could be accomplished in less than one minute. Key management was not effective because most networks used a single shared key value for each node. Hackers developed a host of tools to crack WEP taking advantage of its weaknesses. Tools like Aircrack-ng, WEPCrack, and Café Latte which capture network packets to reverse engineer the WEP key

   [2 points] How is WPA and WPA2 significantly different from WEP? How does it fix the problems that WEP had?

   WPA/WPA2 addresses and fixes the weaknesses of WEP by assigning dynamic keys which are assigned during each session in addition keys are calculated for each packet whereas WEP used a static key for everyone on the network. Once that key is reverse engineered you have unlocked the network. Dynamic keying makes that much more difficult. WEP uses 40-bit key encryption whereas WPA/WPA2 uses 128-bit key encryption, the length of the encryption increases the complexity making it very difficult to crack. WEP has very week authentication because it uses the same static key for authentication whereas WPA/WPA2 uses an improved user authentication taking advantage of Extensible Authentication Protocol (EAP). In addition WPA/WPA2 uses the Temporal Key Integrity Protocol (TKIP) which uses a cryptographic message integrity code called Michael to defeat forgeries, per packet key mixing which de correlates public IV's from weak keys, a rekeying mechanism that provides fresh encryption and integrity key that gets rid of attacks from key reuse, and IV sequencing that takes away replay attacks. WPA2 takes things a bit farther than WPA by providing a robust security network which follows a handshake method very similar to that of HTTPS.

3. [2 points] What are the most notable threats to running a secure WLAN?

Some of the big threats running a secure WLAN are Rogue Aps- A Rogue Access Point is when an employee or hacker sets up an access point of their own on a wireless network. If it is and employee, the danger may be that that access point may not have the same security. If it is a hacker, they will often try to mimic the SSID of the network to enact man in the middle attacks where innocent unknowing clients attach themselves to the rogue access point. The hacker then sets up a sniffer and collects all the data from the client. Key cracking- hacking tools like aircrack ng sniff packets and then use the data to crack encryption keys. Wardriving where a hacker will use wireless network cards many that have extensive range to place themselves on a network to key crack or an unprotected network to take make use of the wireless network. ARP poisoning- a hacker can spoof their mac address and map their ip and mac address to the ARP table of the target system once they have altered the ARP table, they are able to conduct man in the middle attacks effectively. DOS attacks- Denial of Service attacks are used to overwhelm the target systems by sending multiple handshake attempts, wireless access points are also susceptible to radio jamming which will deauthorize clients from the access point. Hackers often use this technique to capture the SSID of a target to try and gain access to a wireless network. The hacker deauthorizes a client from the wireless network and then acts as both the client and the server to conduct a man in the middle attack telling the client that they are the router and the router that they are the client. By using the SSID of the client they can then attempt to get a handshake from the router to try and capture the password to log into the network in encrypted form.

4. [2 points] What are the recommended practices for running a secure WLAN?

Make sure to use WPA2 and strong passkeys to encrypt communications and provide authentication at the wireless level. Use a wireless intrusion detection system to detect rogue access points and prevent wardriving. Use authentication methods such as EAP-TLS to provide authentication between the client and the server. Use a VPN so that transmittions to authenticate are encrypted to sniffers.

5. [4 points] Watch these two videos on cracking WEP and WPA-PSK. What are your observations about how this process works and the tools used to carry out the attack?

The process is basically the same until the step of using airreplay ng which I will talk about at the end. Cracking WEP the attacker must posses a wireless network card that enables monitor mode and packet injection it is an important part that the creator of the video left out. You first use airmon ng to put the wireless adapter into monitor mode. Then the attacker uses airodump ng to see the BSSID's of the wireless networks in range. Airodump ng will also show what type of encryption the wireless networks are using WEP or WPA. The attacker then uses airodump ng in conjunction with the BSSID of the selected network and the channel that network is on to sniff and dump packets into a file that they create on their machine. The attacker then uses aireplay

ng to inject ARP packets at the target machine in an attempt to get a handshake and capture the encrypted wireless key. Then the attacker uses aircrack ng to attempt to crack the web key and write it to the previously set up folder. The process is identical with WPA until the third step in which the attacker uses the BSSID of the network that they are attempting to crack and the BSSID of a client on that network. The attacker then injects deauthorization packets into the target router which breaks the connection. The attacker then uses the BSSID of the client to try and capture the four-way handshake between the client and the router, this is a man in the middle attack. The video then shows the attacker using Wireshark to see that the handshake has been captured but this is no longer necessary the airodump ng tool used to deauthorize will show if the handshake is made. The attacker then takes the handshake(password) and runs it through dictionary attacks in order to try and crack it. The creator of the video uses a very poor password to show it is working had he used a 12-character upper and lowercase alphanumeric password with special characters he would not have been able to crack the password. Attackers are using packet sniffing in conjunction with dictionary attacks to crack passwords. Strong passwords and password policy are key to protecting your wireless network.

a. http://www.youtube.com/watch?v=kTg1q5v3NMo (WEP)

b. http://www.youtube.com/watch?v=GLO9HGDwOY0 (WPA)

6. [5 points] A consistent tradeoff in the security field is security versus complexity/usability. WEP and WPA-PSK use "pre-shared keys" to conveniently secure small networks. These keys rarely ever change, making them susceptible to offline dictionary attacks against the passphrase. On the other hand, WPA2 Enterprise overcomes the issue of PSK. Research enterprise WLAN security and describe at least 4 significant advantages. Cite your sources.

Four significant advantages of enterprise WLAN security are: clients get dynamic unique encryption keys which make dictionary attacks almost ineffective, the dynamic keys are not kept on personal devices like pre shared keys are so that if a device is stolen or lost your network will not be compromised, you can use enterprise WLAN security to authenticate both wireless and wired clients, you can regulate the access t the network with usernames and passwords that are familiar to the clients. The biggest take away is that dynamic keying is essential however enterprise WLAN security also offers more granular level of control.

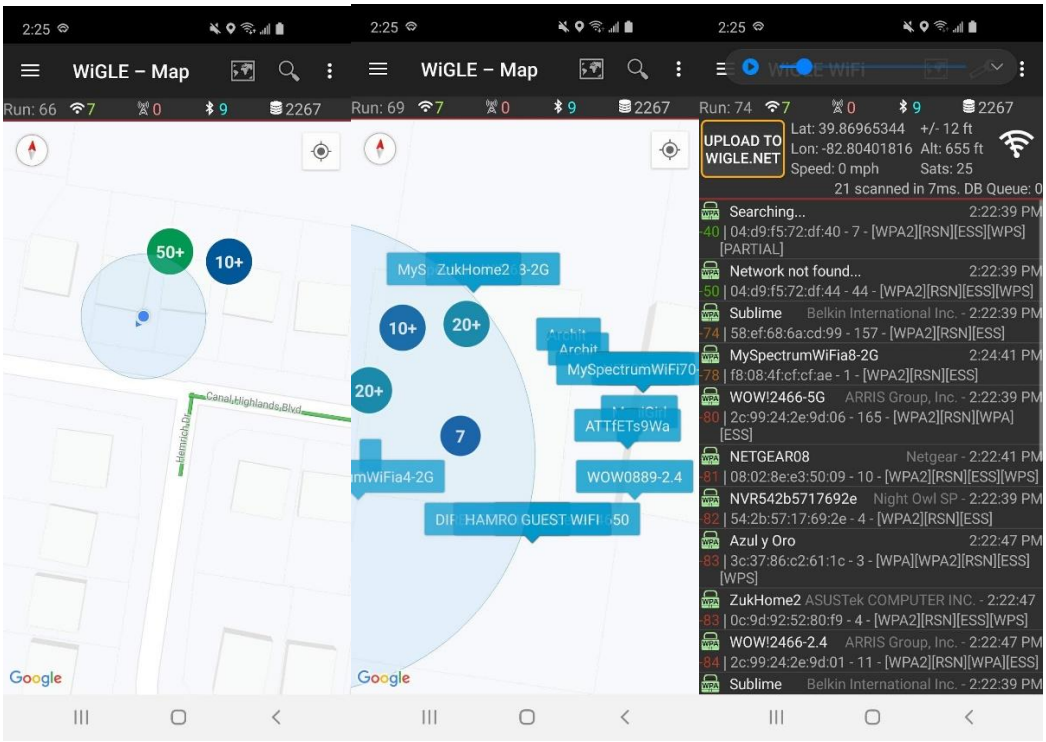
7. [8 points] Download and install VIStumbler (http://sourceforge.net/projects/vistumbler/) on a laptop machine. Drive slowly around your neighborhood for 15 to 20 minutes to locate as many access points as possible. Using some screen shots and data analysis, show:

I had previously used a mobile app to do this I am interested in all aspects of internet security and experiment with a lot of legal activities on my own. I used the mobile app WIGLE WiFI which is awesome. I have downloaded screenshot so that you may look at them.

a. The map of your driving route and the income level of the neighborhood (Google Maps is a good source for the former and Zillow is a good source for the latter).

The average income level of the people in the neighborhood is around $40,000

b. A screen shot of some of the output of your wardriving in VIstumbler.




The first photo is a general out view of networks the first and second screen shots are using google maps. The second photo is a closer view showing the networks. The third is a list of the networks that can be sorted by channel, signal state and encryption.

c. An analysis of how many people are running open or severely compromised security on their wireless networks.

I found no networks running open or severely compromised security however I have seen open networks from time to time for visitors to use. All networks showed up as robust security networks.

d. What manufacturers were represented among the SSIDs you saw?

Belkin, Asus and Arris are the primary manufacturers that came up in the scan.

e. What was the distribution of channels used for the access points?

The distribution of channels was channel 7 through 11 for 2.4 networks and 44 through 165 for 5ghz networks.

8. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

I feel like a broken record when I say that I found the reading and MEET session to be very informative and interesting to me. I hope that my answers to the questions convey my level of interest in the topics every week. I think it is interesting and important to have the MEET sessions. You had mentioned that the peer to peer and the mesh wifi networks and topologies being inherently insecure. The book doesn't really talk a lot about that. That is why it is so important to hold classes with someone who knows the material personally. The book covers a lot of wifi technologies that I don't see for the most part I am assuming that is the case because technology is always improving and becoming more affordable.

In a previous course that I completed research writing I researched cyber security jobs throughout the course and one of the things that hiring managers had to say was that people that held degrees were great but didn't have the practical experience and didn't know the tools. I took that to heart and have done my own research on many security topics. I was initially interested in penetration testing, I met with a bunch of penn testers and I fit in very well with them. I am not interested in a stigma however or being looked at like a hacker. Even though I would probably find that job interesting I don't have any interest using the tools for personal reasons or gain of any kind. Before I knew that the penetration testing job would put a stigma on me I started practicing with the kali Linux and the hacking tools out there that were available on my home lab that I was instructed to set up by penetration testers. I used Aircrack ng and the other tools to try and capture the password to a network with a decent password and had no success. It gets to be dodgy because the password would not show up on wordlists however hacking groups with accept payment to crack the password. I didn't have to time to research that or how they do it but inherently the takeaway that I had was that WPA2 is next to impossible to break if you use a strong password or at least not worth your time at all.

I also talked with a security official at the hacker's convention that told me he used to work for PNC. We hit it off and I asked him if he had any funny stories. He told me about then catching an employee on the company wifi that would sit in the same bathroom stall and watch granny porn at the same time every day. We both had a big laugh. I asked him why the guy wasn't using a personal VPN while using the company

wifi and he told that people were stupid. The reason I bring this up is that it makes me think about the part in the book where it tells you to use VPN to authenticate for security and that makes sense.

When I used Aircrack I fumbled through it will YouTube tutorials and didn't understand much on how it works, after this chapter I see how it works. At very least understanding the hacking tools gives you great insight on how to protect against them.

## References

Geier, E. (2010, October 11). *15 Reasons to Use Enterprise WLAN Security*. Retrieved from eSecurity Planet: https://www.esecurityplanet.com/views/article.php/3907721/15-Reasons-to-Use-Enterprise-WLAN-Security.htm

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.