# 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.

WLAN is a wireless local area network meaning that it is limited on the reach of the network like LAN while it does not have to be wired down. The other manner is WAP or wireless access point, which takes signals from a wired network and sends it out to the wireless connections.

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

WEP is the wired equivalent privacy protocol, it is considered too weak as the initialization vector is too small which leads to it being recycled a lot, the key management is not effective as most networks use a single key, and there are numerous tools out that can be used to crack the WEP key.

1. [2 points] How is WPA and WPA2 significantly different from WEP? How does it fix the problems that WEP had?

They are the wi-fi protected access protocols which were created to help fix the issues with the WEP. The key that is used for WPA, is a dynamically changing 128 bits key. It improves authentication and the keys are assigned to the user per session instead of the same key for everyone. WPA2 adds some more encryption and authentication protocols to help protect the network and solve some problems from WEP and WPA.

1. [2 points] What are the most notable threats to running a secure WLAN?

Some notable threats to WLAN are rogue access points, key cracking, wardriving, ARP poisoning, and DoS attacks.

1. [2 points] What are the recommended practices for running a secure WLAN?

Some recommended practices for a secure WLAN are to use WPA2 as it covers the other two and solves some problems they had, setup wireless IDS to spot rogue access points, use a VPN to ensure authentication for the wireless connections, and use mutual authentication methods.

1. [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?
   1. <http://www.youtube.com/watch?v=kTg1q5v3NMo> (WEP)

To crack the WEP they use a WLAN0 interface and then a dump to see everything like the mac address. Then the mac address is used to gather packets incoming and outgoing. It looks like it is using a dump to gather the starting information like the mac address and port number, then uses them to gather packets, the packets are then sent back to create an overwhelming amount of traffic. The packets can be found based on the length so it can pick up the encrypted packets. The data collected with the shared key can then be used to break it and crack the key.

* 1. <http://www.youtube.com/watch?v=GLO9HGDwOY0> (WPA)

The vulnerabilities for WPA were very specific and had to be cracked using man in the middle attacks while WEP could use brute force. WPA-Personal could be brute forced as it uses a shared key.

1. [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.

The first advantage is the encryption keys used in enterprise WLAN are not as vulnerable to cracking. The second advantage is that the dynamic key gives a better means of management and helps protect against lost devices. The third is that a captcha test can be added to stop robots from accessing the network through guests. The fourth advantage is that the network is scalable and can grow with the organization using it.

Citation:

/\* custom css \*/.tdb-post-meta{ margin-bottom: 16px; color: #444; font-family: 'Open Sans', Geier, E., /\* inline tdc\_css att \*/.tdi\_71{margin-top:10px !important;margin-bottom:0px !important;padding-top:24px !important;padding-right:24px !important;padding-bottom:24px !important;padding-left:24px !important;border-color:#dddddd !important;border-radius:8px, Eric GeierEric Geier is an eSecurity Planet contributor., Eric Geier is an eSecurity Planet contributor., 10, M., 17, D., 30, J., 8, O., 8, J., 30, J., & 22, J. (2022, May 3). *15 reasons to use enterprise WLAN security: Esecurity Planet*. eSecurityPlanet. Retrieved July 10, 2022, from https://www.esecurityplanet.com/trends/reasons-to-use-enterprise-wlan-security/

*Enterprise wlan*. Federated Service Solutions. (2022, July 7). Retrieved July 10, 2022, from https://www.federatedservice.com/enterprise-wlan/#architecture

1. [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 do not feel too comfortable doing this and the street I am on has regular cop patrols so it is likely that doing this could lead to problems with them.

* 1. 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).
  2. A screen shot of some of the output of your wardriving in VIstumbler.
  3. An analysis of how many people are running open or severely compromised security on their wireless networks.
  4. What manufacturers were represented among the SSIDs you saw?
  5. What was the distribution of channels used for the access points?

1. [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.

This week we looked at wireless network security. It talks about the number of problems that appear and the vulnerabilities with these networks. I knew that the wireless networks would be more vulnerable but seeing how fast someone can crack the keys is still surprising. This makes me think about how the average person would believe their network is safe but is quite vulnerable. This not taking into account the less tech savvy people who would be even more vulnerable as they may not understand how their network is unsafe.