Final Project

Warwalking

**Authors:**

**Dhal Wayne Lorenzo**

**Kristin Kogasaka**

**Brandon Chun**

Date: May 11, 2016

**1 Introduction**

Warwalking is the act of walking around in search of wireless network access points [3]. Modern access points have built-in encryption. Wired Equivalent Privacy (WEP) is considered easy to breach and thus insecure. Wi-Fi Protected Access (WPA and WPA2) are considered a secure version for wireless encryption depending on the type of coverage, business, personal, etc [1]. For this experiment, our group walked around the University of Hawaii at Manoa campus to discover possible open wireless network access points.

Section 2 will describe what how our group went about conducting the warwalking experiment and a discussion of our findings. Section 3 will discuss what kinds of policies a CISO could create to safeguard against wireless network vulnerabilities. Section 4 is the conclusion of this paper.

**2 Summary of Experiment**

There is a variety of software available for warwalking on different platforms. Our group was unable to use Netstumbler as specified since none of our wireless cards were compatible with Netstumbler. After looking at several alternatives we decided to use WiGle Wifi available on Android devices. This application allowed us to gather data on access points including their GPS coordinates, SSID, MAC address, and encryption type [4]. Figure 1 shows a map of our findings.

Below is a map of the experiment and as you can see we encountered many wireless access points (Figure 1). The green points on the map are extended service set known as ESS. The red points are WPA and WPA2 access points. The yellow points are WEP access points. We found a few WEP encryption access points around popular areas we surveyed.

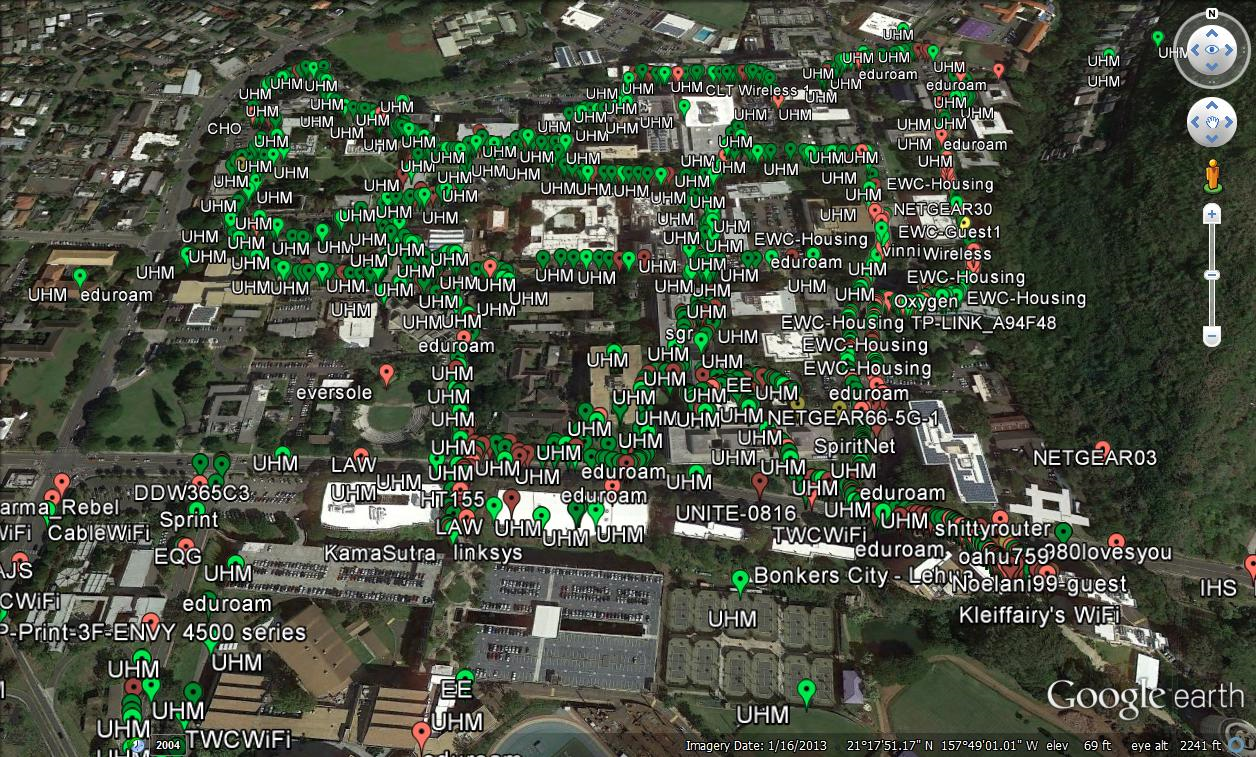


Figure 1: Warwalking Map

For this experiment we decided to target specific areas of UH Manoa where students and faculty would be most likely to access the network. We started our expedition at Hamilton Library since we know that is a popular area students use to study. Access points by Hamilton Library were secure. Most access points here were protected with Extended Service Set (ESS) or Wi-Fi Protected Access (WPA/WPA2). While searching around Hamilton Library we came up with the idea that the dorms may have an abundance of access points since there is a large student population residing there. We hypothesized that the dorm area would be the area with the most access points that are susceptible to attacks and vulnerabilities. When we walked through the dorms there were a few access points, not including the UHM network, that were unprotected and open to the public as shown in Figure 2.



Figure 2: Frear Hall

After visiting the student dorms, we went to the engineering building also known as Holmes Hall. Then we continued through POST building and we walked north on East-West Road next to international student housing. Next, we went West toward Webster hall and Shidler business college. Then we started walking down to the architecture school and then we past by sinclair library. After that, we went through campus center and walked to the Law buildings and ended at the parking structure.

Access points at the student dorms (Frear Hall), near Holmes hall, Jefferson hall, and the Architectural building had vulnerable wireless access points as shown in Figures 2, 3, 4, and 5 respectively. These access points are vulnerable because they have a weak WEP encryption that can easily be exploited [2]. Our experimental guesses on these targeted areas were right as these are areas that students most likely would use a wireless access point. This is a security issue for students since these areas would have high wireless access traffic.



Figure 3: Holmes Hall

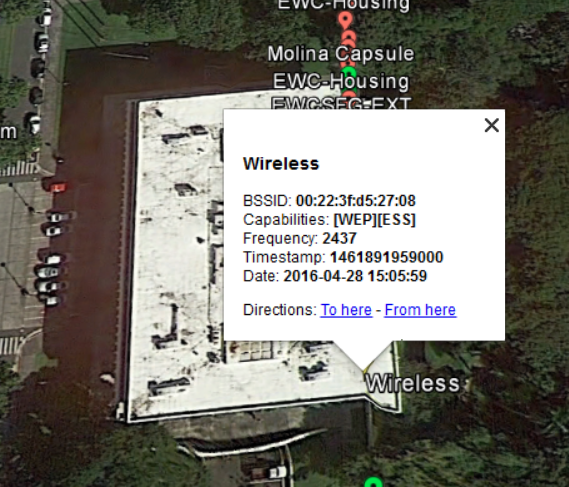


Figure 4: Jefferson Hall

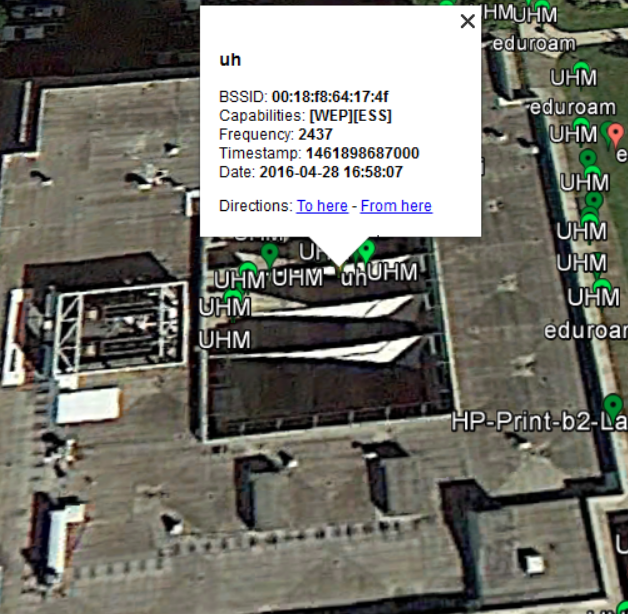


Figure 5: Architecture School

**3 Policies to Safeguard Against Wireless Network Vulnerabilities**

One type of policy a CISO could create to safeguard against wireless network vulnerabilities could be to make sure all wireless access points are encrypted with WPA2. WPA2 is the newest form of encryption and makes it harder for attackers to obtain access to the network.

Majority of the open access points were located in the student residence areas. A CISO could implement a policy that requires students to secure their personal wireless networks. Having open access to wireless networks can lead to major vulnerabilities for the network.

Another policy that is important to include is to make sure that the staff and employees do not write down the passwords to the already secured wireless networks. By not writing down the passwords the risk of vulnerability is decreased because it removes the possibility of a breach from a notepad or a stray sticky-note.

To add to the protection of password information, a policy of not sharing passwords between users would also be useful to implement. When multiple people share passwords it narrows down the possibilities of what the password might be and removes individual responsibility to protect the passwords. This encourages attackers to target specific people to obtain passwords that are used for multiple reasons.

In the workplace it can be very tempting to use a personal device such as a cell phone or iPad and connect to the internet through the University’s network. But storing passwords on personal devices can lead to leaks of the passwords to protected networks if the device is lost or stolen. In order to prevent possible intrusion into the network, a policy that bans the use of personal devices in the workplace might be necessary.

**4 Conclusion**

In conclusion, our group did not find any vulnerabilities in the University of Hawaii at Manoa ESS access points. The vulnerable access points that we located were personal student access points or access points for certain departments within the college.

A policy ensuring that all access points within the University of Hawaii at Manoa campus are secure would keep all access points from being unnecessarily vulnerable to attacks. It would also give the campus a good reputation for having secure networks and thus deter attention from potential hackers. For example, if hackers thought there were an abundance of vulnerable access points at the University of Hawaii at Manoa campus dormitories, they would target that area more. They may even decide to place malware on removable drives such as USB drives, and students and faculty may unknowingly spread the malware to other computers on campus or their workplaces off campus. Also, the target area at the dormitories may spread in the assumption that there may be more vulnerable access points nearby. If hackers knew that the University of Hawaii at Manoa is known for its secure access points and enforces a policy ensuring that all access points remain secure, hackers will divert their attention elsewhere.

**References**

1. Cisco. (2012 Mar 28). *Understanding the Difference Between Wireless Encryption Protocols*. [Online]. Available: https://blogs.cisco.com/smallbusiness/understanding-the-difference-between-wireless-encryption-protocols
2. How-to-Geek. (2013 July 16). *HTG:Explains The Difference Between WEP, WPA, WPA2 Wireless Encryption(and Why it Matters)*. [Online]. Available: <http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/>
3. NETGEAR. (2014 Feb). *What is a wireless access point*. [Online]. Available: http://kb.netgear.com/app/answers/detail/a\_id/235/~/what-is-a-wireless-access-point%3F
4. Wigle. (2016). *Wigle.net*. [Online]. Available: https://wigle.net/