Charles D. George

Wireless Security and Protection

ICTN 4040

Dr. Lunsford

As the world around us evolves and changes everyday it feels as though technology is always another step ahead. With technology advancing so much you see it all the time becoming more convenient to have a smaller handheld device more and more. This just makes it easier for someone to invade your privacy, because they can hack your network with ease just with a phone or laptop. Security is important at all times now whenever the transfer of information is ongoing on a live network with data. You have to prevent hackers from accessing your information, because it is so simple for you to be the next victim of account fraud or having everything as you know it taken from you. Wireless security flaws are common with users slipping and not being cautious enough when accessing a network.

Wireless Security is the prevention of unauthorized access or damage to computers on your wireless networks. Most people may connect to a public access point in a restaurant or business to use their internet for free to check their bank account or Facebook page not realizing what vulnerabilities exist. And usually these public networks that are available are not secured, so it is an open network that makes all of your information available to a hacker. Millions of wireless access points exist around the world and about 70% of them are not protected, so anyone can access them. The network doesn't have to have a password for you to connect to it but as long as it is secured with some type of authentication method then it may be safer to use. The convenience of having a mobile device with internet access and being able to connect to a free wireless connection, doesn't usually toggle the average person's mind to think about how

safe the network they are about to use is going to be or what they may be about to access.

Public attacks often happen when on these open networks where it is easy to steal data by eavesdropping and data snooping using packet sniffing programs. One of the most common programs that come to mind is Wireshark. Wireshark is a free, open-source network protocol analyzer. It is probably one of the most popular programs available that can capture and allow you to interactively browse the traffic running on a network (an image of Wireshark in capture mode is shown in Figure 1). It is used across many industries and educational establishments, but in the wrong hands can be a strong tool to grab just about any piece of information from networks like ethernet, IEEE 802.11, PPP, and loopback. Wireshark is available for download on Unix and Windows operating systems.

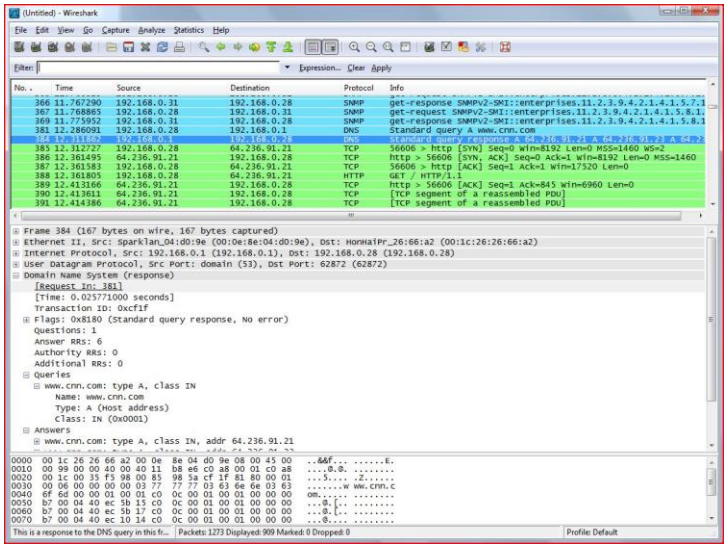

Figure 1: Shows Wireshark capturing packets from different protocols such as snmp, TCP, HTTP, and DNS on a Windows machine.

FaceNiff is an Android app that allows you to sniff and intercept web session profiles over a Wi-Fi network that your mobile device is connected to. In order for you to be able to hijack sessions you must use Wi-Fi that is not using

EAP. A rooted phone must be used, which means you have to have privileged control as an administrator-level permissions that a normal user cannot perform. If you are a SSL user then this application won't work and make sure you use the stock phone browser another might not work. You are then able to see profiles over any private network including open, WEP, WPA-PSK, and WPA2-PSK. If these previous steps are completed then you are available to gain access to and hijack profiles like FaceBook, Twitter, Youtube, Amazon, MySpace, Tumblr, etc. FaceNiff is available for download for free from their website. A screenshot of FaceNiff's interface is available in Figure 2.

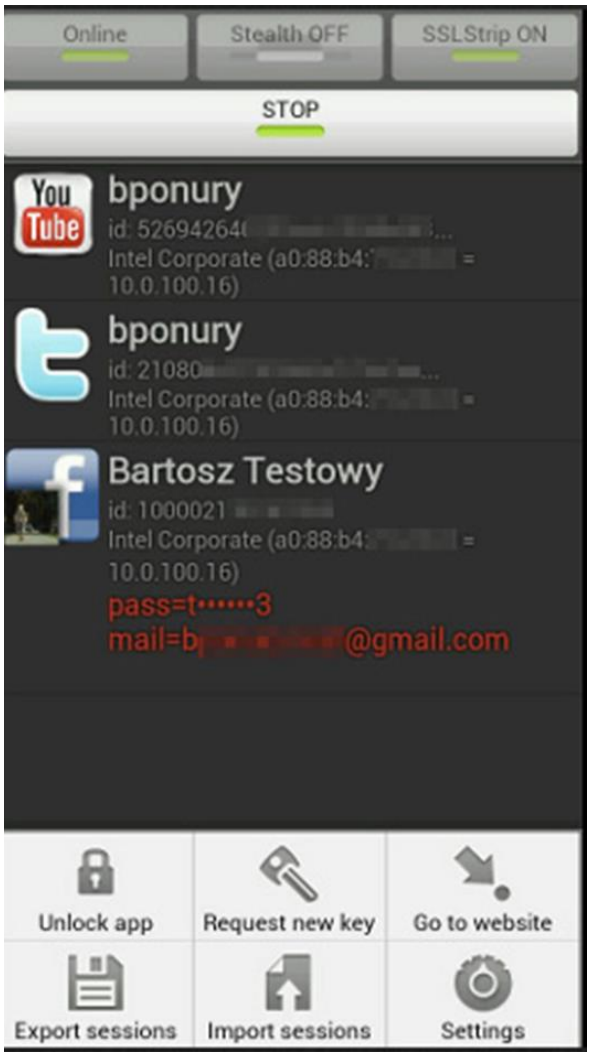

Figure 2: FaceNiff screenshot of the interface on an Android phone

Firesheep is a Firefox browser extension that uses cookies left behind to make a user vulnerable to attacks. Firesheep demonstrates HTTP session hijacking, which allows someone to do anything a user can on a website. A capturing image after Firesheep has accessed someone's user profile is available in Figure 3. When logging into a website that requires authentication you submit a username and password and the server checks them to see if it matches the existing information. It then replies back to you with a cookie which is used for all other requests. It is extremely common for websites to protect your password by encrypting the initial login, but surprisingly uncommon encrypt everything else. This entails a cookie being left making the user vulnerable to attacks. On an open wireless network, it makes it extremely easy to be attacked. It a widely known problem, yet many websites have fixed this issue with protecting their end users. The only effective fix of this problem is full end-to-end encryption with HTTPS or SSL. Firesheep reveals all flaws with security issues on popular websites such as Facebook and Google, by showing how easy it is to capture data from these insecure pages.

Figure 3: Firesheep capturing a Facebook profile by using a tracking cookie on an unsecure network

Protecting your information with wireless security is a simple step to take when setting up a network, but something some users don't take the time to do. One of the most common types of security is Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is one of the least secure forms of security. A network that is secured with WEP can be cracked in 3 minutes by the FBI. This is because WEP is an old outdate IEEE 802.11 standard developed in 1999. WPA then took over in 2003 as a quick alternative to improve security. The current standard is WPA2, but some hardware cannot support it without a firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256 bit key. Just as these standards have increased security so has the key length; the longer the key length, the stronger the security. Wireless security policies have been developed by industries to guard against unauthorized access to important resources. Wireless Intrusion Prevention systems (WIPS) or Wireless intrusion detection systems have been setup to

enforce these security policies, but that does not necessarily stop crackers from trying to gain access.

WPA provides stronger encryption than WEP through use of one of two standards temporal key integrity protocol (TKIP) and Advanced Encryption Standard (AES). Another plus for WPA over WEP is that it includes built-in authentication support. You can compare WPA security to VPN tunneling with WEP, with WPA giving the benefit of easier administration use. When setting up a home network WPA Pre Shared Key often referred to as WPA-PSK, which is simplified but still powerful. To use WPA-PSK, a static key or passphrase must be setup like with WEP. The benefit of using TKIP is that WPA-PSK automatically changes the keys at a preset time interval, which makes it more difficult for hackers to find them and gain access.

WPA2 replaced the original WPA technology on all certified Wi-Fi hardware since 2006. It is also based on the IEEE 802.11i standard for data encryption and like other standards was a designed to replace the older and less secure predecessor. WPA2 improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. WPA2 does not work with TKIP, because of the know security flaws and limitations that it had when first introduced with WPA. Several different forms of WPA2 security keys exist. WPA2 PSK (also known as Personal Mode) is the most common and found on home networks. WPA2 introduced CCMP, a new AES based encryption mode. The wireless network encrypts traffic with a 256 bit key that can be entered as 64 hexadecimal digits or a passphrase of 8 to 63 ASCII characters.

References

Geier , J. (n.d.). How to: Define Network Security Policies. Retrieved from http://www.wireless-nets.com/resources/tutorials/define_wireless_security_policies.html

Cheung, H. (2005, March 31). The Feds can own your WLAN too. Retrieved from http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100

Frisch, R. (2012, January 13). Your Encrypted Wi-Fi Signal is easily cracked. Retrieved from http://rhftech.com/blog/your-encrypted-wi-fi-signal-is-easily-cracked

Mitchell, B. (n.d.). WPA- Wi-Fi Protected Access. Retrieved from http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm

Mitchell, B (n.d.). What is WPA2? Retrieved from http://compnetworking.about.com/od/wirelesssecurity/f/what-is-wpa2.htm

N/A. (n.d.). Faceniff Facebook (and other services) Session Hijacker for Android. Retrieved from http://faceniff.ponury.net/

N/A. (n.d.). About Wireshark. Retrieved from http://www.wireshark.org/about.html

Butler, E. (2010, October 24). Firesheep. Retrieved from http://codebutler.com/firesheep/