A STUDY OF WIRELESS SECURITY PRIVACY AND FORENSICS

Studnets Demetrios Roubos; Shawn Casler ;James Hedigan; Ryan Shaw
demetrios.roubos@stockton.edu; stk28893@loki.stockton.edu;
stk32103@loki.stockton.edu; stk32166@loki.stockton.edu
The Richard Stockton State College of NJ Pomona, NJ 08240
Co- Advisors
Suvineetha. Herath, * Detective David Costantino, Vince Cicirello, Robert. Kachur,
*NJ Regional Computer Forensics Lab- Trenton NJ
Principal Advisor. Ajantha Herath
The Richard Stockton State College of NJ
Pomona, NJ 08240

ABSTRACT

Wireless networking has become an extremely common household technology in a matter of only a few years. Concerns for privacy have become more relevant than ever, with more cases of identity and data theft occurring everyday. Initially, consumer grade wireless technology was distributed without security being a major concern. Today, almost every consumer grade wireless router comes with either "out-of-the-box" encryption or with relatively easy to follow instructions on how to properly secure the household wireless infrastructure. In this paper we investigate wireless technology and the implications related to the privacy of the average user.

INTRODUCTION

We will focus this paper on a two tiered study including the geographic analysis of wireless networks within the city of Pomona NJ and an analysis of traffic sent through our own unencrypted wireless network. We feel that this is an ideal candidate for research because of the relative diversity in density, population demographics, and living conditions.

During the analysis phase of this project, an emphasis was put on mapping the wireless networks with a geographic mapping utility- in this case we used Google Earth as our mapping software. Collecting wireless access point information anonymously and without actually connecting to any networks was clearly paramount. There are several documents available regarding the ethics and legality of what is commonly referred to as war-driving. War-driving can be loosely defined as the act of scanning for networks with a device (such as a laptop computer) which is typically either carried or driven for the purposes of collecting information about wireless networks in a specific geographic region [9]. If done without malicious intent and without connecting to any of the scanned networks, this behavior can be likened to scanning for a radio station while in one's car. The Stumbler Code of Ethics points out several best practices to give researchers the heads up before they begin communicating with foreign networks and inadvertently breach the privacy of the owner. To accomplish the task of respecting laws and ethical

standards, we disabled the TCP/IP stack on our wireless network connection and used a freeware wireless utility known as Network Stumbler which synchronizes GPS data and can survey wireless access points for generic information. With the TCP/IP stack disabled, a connection to these wireless networks is never established.

PUBLIC WIFI TODAY

Wireless networking today is complicated for average computer users. In some cases, people have problems connecting to and configuring secure wireless networks and in other cases, people put themselves at risk by falling victim to one of several wireless attacks. Many exploits have been developed to compromise the security of wireless transmissions and in effect put the privacy of the end user at risk of being exploited.

Evil Twin networks create rogue access points that are named in a fashion that mimics the SSID of an already existing access point [5]. An evil twin access point acts as a middle man between the cloned access point and the end users wireless NIC. The evil twin is typically set up in a fashion whereby its signal strength often appears greater to the unsuspecting users than the strength of the cloned access point. Once a connection is established, the rogue access point begins routing traffic between the legitimate access point and the user and is thus capable of intercepting and even changing the user's traffic. Packet injection and promiscuous sniffing are serious threats to confidentiality, message integrity, and endpoint authentication [20]**.** In situations where multiple access points are in range, most users connect to the strongest signal. This is a typical example of a behavioral pattern that seems rational on the surface however, puts them at serious risk.

It's important to point out that it's not always the user which will instinctively connect to the strongest signal. The Microsoft Windows XP system will automatically connect to the strongest network in range when that particular SSID has been set to reconnect automatically; which will inadvertently put the user at risk, occasionally resulting in the user connecting to a malicious host [17]. This becomes more of a problem if the user fails to set a distinct SSID, resulting in the use of a default broadcast ID. Because there are so many wireless access points broadcasting SSID's of a default nature, this can result in the user preferentially connecting to a host of default networks unintentionally.

One of the greatest threats to user privacy with regard to the connection and use of non trusted, unencrypted wireless networks is that with relative ease, unskilled users can download and employ software that can sniff the traffic of those connected to public unencrypted wireless networks that are within range. Malicious users may operate in an environment where they provide the host connection and sniff the traffic of users connected to their access point, or they may not be hosting the connection, but simply are within range of the transmission and sniffing promiscuously.

Unencrypted networks serve a dual purpose. Unencrypted access points act as wireless hotspots for passerby's allowing them a free and easy way to connect to the Internet. However, this comes with a significant tradeoff, in that there will exist a significant potential for the owner's privacy to be compromised by a malicious user.

This inherent duality makes today's wireless technology filled world complicated. It is often very nice to find an unencrypted public wireless hotspot if your goal is to simply connect to the Internet as quickly and as effortlessly as possible. Unfortunately, these unencrypted hot spots can fall victim to attacks by malicious users, rendering them a credible security risk.

OUR ANALYSIS

To better understand the risks of connecting to and using non trusted, publicly available wireless networks, we reset the factory defaults on a Linksys WRT54G (a common household wireless router) and connected it to the Internet. The router immediately began broadcasting a default SSID of "linksys" and provided client nodes the ability to connect and use its internet connection. We then connected a relatively new Dell laptop with a wireless card, running Microsoft Windows XP to the network. We installed Wireshark version 0.99.7, which is a freely available utility designed to analyze network traffic, and configured it to sniff the wireless connection promiscuously. We then attached a client node to the unencrypted network and began surfing and sniffing.

We started out by checking the Richard Stockton College of New Jersey loki e-mail system. *It uses https and SSL to encrypt both the initial handshake and the continued data transmission.* This is a big contrast to the other e-mail systems we tested. We tested yahoo mail (old and new versions) and g-mail. Both offered a secure authentication mechanism, but neither offered any encryption after you are logged in. It was easy to find pieces of text from e-mails just by scanning the contents of the packets we sniffed. Figure 1 illustrates the plain text capture of one of our member's address which was written in an email from Amazon regarding an order he had placed.

```
0a 53 68 61 77 6e 20 43  61 73 6c 65 72 3c 62 72   .Shawn C asler<br
20 2f 3e 3c 73 70 61 6e  20 63 6c 61 73 73 3d 22    /><span  class="
79 73 68 6f 72 74 63 75  74 73 22 20 69 64 3d 22   yshortcu ts" id="
6c 77 5f 31 32 30 30 32  35 37 31 39 33 5f 32 22   lw_12002 57193_2"
3e 32 38 33 20 48 6f 6f  76 65 72 20 41 76 65 3c   >283 Hoo ver Ave<
62 72 20 2f 3e 42 61 79  76 69 6c 6c 65 2c 20 4e   br />Bay ville, N
4a 20 30 38 37 32 31 2d  32 38 33 38 3c 62 72 20   J 08721- 2838<br
```

Figure 1 Plaintext capture from the "New" web-based Yahoo Mail system

The most surprising part of our test came next, when we checked the popular social networking site, MySpace. The login was not secure at all, as the user name and password were both transmitted in plaintext in a relatively distinct packet. This is relatively surprising for such a popular site. The data in Figure 2 was easily derived, as it came from the only HTTP POST command labeled login.process.

```
32 34 45 6d 61 69 6c 5f  54 65 78 74 62 6f 78 3d   24Email_ Textbox=
73 68 61 77 6e 69 65 63  61 73 25 34 30 79 61 68   shawniec as%40yah
6f 6f 2e 63 6f 6d 26 63  74 6c 30 30 25 32 34 4d   oo.com&c tl00%24M
61 69 6e 25 32 34 53 70  6c 61 73 68 44 69 73 70   ain%24Sp lashDisp
6c 61 79 25 32 34 63 74  6c 30 30 25 32 34 50 61   lay%24ct l00%24Pa
73 73 77 6f 72 64 5f 54  65 78 74 62 6f 78 3d 31   ssword_T extbox=1
77 69 6c 6c 69 61 6d 26  63 74 6c 30 30 25 32 34   william& ctl00%24
```

Figure 2 Plaintext capture of mySpace login packet

Our final test checked the security of AIM; which turned out to be similar to the security of gmail and yahoo. The login procedure featured encryption, however the messages, status updates, and buddy list information were all sent in plain text.

In our analysis of random geographic locations within the State of New Jersey, we found that the overall percentage of encrypted networks has grown significantly in just one year. The highest density of encrypted networks is seen in the most densely populated areas of North and Central Jersey. Conversely, the lowest density of encrypted networks is seen in the Southern and Eastern areas of New Jersey. In an analysis of the SSID's we happened across, we found that a significant portion of networks surveyed were using what looked to be default broadcast ID's. In a statistical analysis conducted based on information derived from figures posted on wigle.net (The Wireless Geographic Logging Engine), it has been shown that approximately 5 in 10 wireless networks in rural areas are unencrypted. Currently, wigle.net is reporting that 45.5% of the total number of wireless networks logged use WEP based encryption. They're also reporting 38.7% of the wireless networks logged are unencrypted. This figure seems rational and is generally representative of other similar studies. It is becoming increasingly clear that the overall percentage of encrypted networks is increasing dramatically.

TOOLS AND METHODS

A freeware program called Network Stumbler can be used in conjunction with a GPS receiver and a wireless network card to survey wireless access points that are in range. The information obtained by Network Stumbler can be exported to another freeware program, Earth Stumbler, which converts the exported data into an XML based format which Google Earth can parse. When this data is loaded into Google Earth, the location of every access point that was found is marked with one of two unique markings. One of which is a green symbol, which represents unencrypted networks, the other, a red symbol, which represents encrypted networks. With the mapping features of Google Earth, one can analyze the concentration of access points in different regions and what percentage of them is encrypted.

There are many freeware programs that can be used to analyze network traffic. In this section, we'll look at several tools that can be used to analyze wireless networks. WireShark is a very useful freeware utility for collecting data from a specific network. It is a packet sniffer that is used to analyze traffic being transmitted over a network in real time. This tool can be used to analyze both wired and wireless traffic. Snort is also a freeware program that is an intrusion detection and prevention system. It is widely used by IT professionals working in the information security industry to analyze large networks. Although the learning curve associated with this software is steep, its use is a must in the modern day technologically oriented enterprise. Kismet is another program used for network analysis; it differs by working completely promiscuously, or without transmission, so that its use cannot be detected without special detection software. Kismet can also be used to detect other active sniffing programs, provided that those programs

aren't promiscuously sniffing in the same fashion that Kismet does. All of these software packages are easily obtainable via the Internet.

WEB BASED ROUTER CONFIGURATION UTILITIES

There are a variety of methods to secure your home router from intruders. The most secure home networks utilize all of the security suggestions provided with the documentation for the equipment being used. Regardless the age of or level of encryption used on your router, there exist common vulnerabilities which plague wireless home configurations.

A major vulnerability can occur if the user isn't steadfast in reading the documentation and implementing the recommendations contained therein. It thus follows that the end user plays an extremely significant role in configuring a secure network. One common mistake, which may appear virtually insignificant to the untrained user, but is a serious security threat, is related to the remote access utility built into most wireless routers. Almost every consumer grade wireless router available today offers remote administration to the end user through a web client. This web client is often secured by a username and password combination, which is typically set to a manufacturer's default setting. The impact rating associated with accessing a router by using the default administrative account is high. What's more, several websites have appeared that list the default credentials for virtually every consumer grade product on the market. Some of these lists also include information like what the default SSID of each specific product is. This information can be particularly useful to an attacker trying to gain unauthorized access to a network. The combination of users not securing their remote access utilities, coupled with the advent of easily accessible documentation related to default login credentials, ultimately leads to affording malicious users the chance to wreak serious havoc on any network. As it stands however, the end user is ultimately responsible for the initial setup procedure, and in the face of saving effort and time, security tends to take a back seat.

BEST PRACTICES

There are however several ways to mitigate attacks by unsophisticated sniffers. The use of a Virtual Private Network can be employed to securely connect to a trusted host through a non trusted access point, rendering traffic transmitted through the non trusted gateway illegible to the eavesdropper [19].

The concept of onion routing provides the potential to eliminate some of the risks associated with connecting to and using non trusted networks. Tor is the Second Generation Onion Router. It offers free anonymous routing services to users [16]. While Onion Routing isn't a cure-all for wireless security threats, it offers significant protection from the unsophisticated eavesdropper.

Home users are primarily concerned with ease of implementation and most importantly, whether or not the product works within their existing infrastructure. Security is seldom the major focus of any typical utilitarian consumer. This of course is a problem that only education can realistically solve. People need to become more aware of the importance of security and the impact a lack of security may have on their own personal privacy. The commercial manufacturers of routers have lots of useful information on their websites regarding how to properly secure your network while using their specific product.

CONCLUSION AND FUTURTE WORK

Wireless technology is an amazing addition to the everyday lives of ordinary individuals. Everyday, people enjoy the benefits of using wireless computers and technology. It is for this purpose that we investigated current trends related to the security of wireless networks. We've found that although significant progress has been made in moving users toward encryption proactive configurations, there is still much research work to be done in terms of educating the public and working towards correcting some of the age old problems associated with the inherent tradeoff between ease of use and security. More studies needed in future to work with privacy and computer forensic areas.

SPECIAL ACKNOWLEDGEMENTS

We greatly appreciate the NJ Regional Computer Forensics Lab and Richard Stockton student senate for their continued support. This project was funded by the Richard Stockton College Board of Trustees Fellowships for Distinguished Students program and motivated by computer Science and Information Systems faculty.

REFERENCES

1. A. Back, U. Möller, and A. Stiglic. Traffic Analysis Attacks and Trade-offs in Anonymity Providing Systems. In I. S. Moskowitz, editor, *Information Hiding (IH 2001)*, pages 245-257. Springer-Verlag, LNCS 2137, 2001.
2. Aharoni, Mati, EtterCap – ARP Spoofing And Beyond. Jun 23 2006. http://www.securitypronews.com/securitypronews-24-20030623EtterCapARPSpoofing andBeyond.html
3. Arbaugh, William. An Initial Security Analysis of the IEEE 802.1X Standard. Feb 6, 2002. http://www.cs.umd.edu/%7Ewaa/1x.pdf
4. Atheros Communications. Jumpstart for Wireless. Jan 4 2005. http://www.atheros.com/pt/whitepapers/atheros_JumpStart_for_wireless_whitepaper.pdf
5. Crossman, Craig. Beware Hotspot Hacker Attacks. Aug 24 2005. http://proquest.umi.com/pqdweb?did=886418531&sid=1&Fmt=3&clientId=44884&RQT=309&VName=PQD
6. Goldsmith, Andrea. Wireless Communications. Aug 2005. http://www.cambridge.org/ us/catalogue/catalogue.asp?isbn=0521837162&ss=exc

7. Intel Technology Journal. Bringing Security Proactively into the Enterprise. Vol8 Issue4, 2004. ftp://download.intel.com/technology/itj/2004/volume08issue04/ art05_security/ vol8_art05.pdf
8. John's Hopkins Institute. History of Wireless. Jun 8 2002. http://www.jhsph.edu / wireless/history.html
9. Kern, Benjamin D, Gordon, Glickson. Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. http://www.abanet.org/buslaw /committees/CL320010pub/newsletter/0009/. December 2005
10. Muts. ARP Spoofing and DSniff. Feb 18 2003. http://www.illmob.org/files/text/ ARP_SPOOFING_WIN.pdf
11. M. Wright, M. Adler, B. N. Levine, and C. Shields. Defending anonymous communication against passive logging attacks. In *IEEE Symposium on Security and Privacy*, pages 28-41. IEEE CS, May 2003.
12. Nair, Sajeev. Information Security – Tools of the Trade. Nov 30 2006. http://www.infosecwriters.com/text_resources/pdf/SNair_Tools.pdf
13. Oudot, Laurent, et. al. Defeating Honeypots: Network Issues, Part 2. Oct 7, 2004. http://www.securityfocus.com/infocus/1805
14. Renderman. Stumbler Code of Ethics. Nov 26 2007. http://www.renderlab.net/ projects/wardrive/ethics.html
15. SmartComputing. Wireless Woes. Aug 2006. http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/r1005/42r05/42r05.asp
16. SSL and TLS: Designing and Building Secure Systems, Addison-Wesley, 2001
17. T. Dierks and C. Allen. The TLS Protocol - Version 1.0. IETF RFC 2246, January 1999.
18. The Tor Project. Updated January, 2008. http://www.torproject.org/
19. Virtual Private Network Consortium. http://www.vpnc.org/. January 2008.
20. Walker, Jesse. Unsafe at any size; An analysis of the WEP encapsulation. Oct 27, 2000. http://md.hudora.de/archiv/wireless/unsafew.pdf
21. Welcher, Peter. Troubleshooting Poor Performance, and DSniff Woes. Aug 7 2006. http://www.netcraftsmen.net/welcher/papers/perf-dsniff.pdf
22. Wi-Fi Alliance. WIFI Protected Access. April 29, 2003.http://www.wi-fi.org/ files/wp_8_WPA%20Security_4-29-03.pdf