Hack Boston:
Monitoring Wireless Security Awareness in an Urban Setting

Matthew B. Kowalski
ECE Department
Northeastern University
Boston, MA, U.S.A.
E-mail: mkowalsk@ece.neu.edu

Keith D. Bertolino
ECE Department
Northeastern University
Boston, MA, U.S.A.
E-mail: kbertoli@coe.neu.edu

Stefano Basagni
ECE Department
Northeastern University
Boston, MA, U.S.A.
E-mail: basagni@ece.neu.edu

Abstract

This paper describes "Hack Boston," a project carried out by members of the IEEE student chapter at Northeastern University (NU) in Boston, MA. Our purpose was to identify the presence of wireless networks in order to determine qualitatively and quantitatively how secure these networks are, thus monitoring the security awareness of the wireless community around NU. Our study goes beyond common "war driving/war walking." We present statistical results over a range of metrics that go from the number of wireless signals in the scanned areas to the specific encryption method they use (if any). Experiments have been performed in 2004 and 2005, which indicate an increased awareness of the need for securing in-home wireless Internet connections. Our results are analyzed and compared with national statistics. We finally describe the activities that the NU IEEE student chapter is proposing for educating the community about the proper, secure use of wireless technologies.

Keywords — *Security awareness; wireless networks.*

1 Introduction

IEEE 802.11b/g (a.k.a. WiFi) networks have become the standard *de facto* for high-speed wireless networking in the home. Given their low cost, simple deployment and increasing reliability, WiFi devices are now commonplace in many homes and apartments. Due to the broadcast nature of such networks, the wireless signal goes beyond private boundaries into public areas (parks, streets, etc.), where it is often easily detectable. In fact, it is so usual to find wireless signals anywhere in cities and suburban areas that it is nowadays highly likely to pop one's laptop open and get connected to the Internet for free.

In this paper we describe "Hack Boston," a project carried out by members of the IEEE student chapter at Northeastern University (NU) in Boston, MA. Our study aims at checking the wireless presence (mostly IEEE 802.11b/g signals) in and around the NU Boston campus. Our purpose is to scan for wireless networks (without accessing them), for determining qualitatively and quantitatively how secure these networks are, i.e., how the community around Northeastern is aware of potential security threats that come with unsecured networks.

Differently from previous studies on war driving/war walking (the act of scanning or searching for wireless networks while driving/walking), our aim is to *monitor* and *promote* security awareness among wireless users. We are motivated by the host of serious security risks of leaving wireless networks open. Typical security threats include viruses spreading through the local network (which is different from common "Internet infection" because of the lack of firewalls), anonymous mass-mailing of unsolicited e-mail (spam), and illegal access to remote systems. Most wireless network users are unaware of these risks. Although legislation is still mostly unsettled in terms of who is liable when a wireless network is accessed and used for illegal purposes, there is a trend to hold the owner of the wireless access point liable if the network is not sufficiently protected. We created a "security map" of the area around our campus, with the final aim of educating the community to security and its implementation.

We have performed two wireless networks searches in 2004 and 2005. In both searches, IEEE team members scanned an area within a mile radius around the NU campus, equipped with laptops with wireless cards and extended wireless antennas. Also using GPS transceivers and armed with a recording program called NetStumbler, we could passively find wireless networks, record their position, and determine if these networks were WEP encrypted. The Wired Equivalent Privacy (WEP) [1] protocol is a method of securing wireless data. It is relatively simple to configure, and it provides an effective, first wall to block "prying eyes" from private data. When WEP is enabled, a bystander passing by with a wireless laptop might be able to see the network but would have to enter a secret key before s/he is allowed to see any data on the network, and also to access the network itself. Although this technology comes by default on almost every network router and card, it is never enabled by many wireless network owners. More specifically, our 2004 findings show that 58% of the networks we found were not encrypted and 42% were encrypted using either WEP or WPA (WiFi Protected Access, the security protocol that superseded WEP in 2003 [2]). The following year, the data collected in the same area showed an opposite trend: 60% of access points were encrypted with either WEP or WPA and 40% were unencrypted. This paper discusses the details of our project, compares the findings in the two years, gives some possible reasons for the observed changes, and compares the findings with the national trend.

Section 2 below describes war driving and war walking, and Section 3 deals with to the possible legal implications of leaving wireless access points unsecured. The experiments we performed and the equipment we used are described in Section 4. Our findings are also illustrated in Section 4. Section 5 briefly describes related activities organized by

1-4244-0038-4 2006
IEEE CCECE/CCGEI, Ottawa, May 2006

the NU student chapters of the IEEE, and Section 6 concludes the paper.

2 War Walking and War Driving

War walking and *war driving* both refer to the process of covering terrain on foot or by car in search of wireless access points. This involves some wireless enabled device, such as a laptop or PDA, and the incorporation of some data collection software. Publicly available free software is usually deployed in combination with extended range antennas. In addition, in order to record access point locations, GPS receivers are usually used. Available software is not only capable of recording access points and their signals' GPS coordinates, but it can also determine if the network requires security authentication.

The findings of war walking/driving activities are collected and posted on the Internet for other users. Alternatively, war walking is also connected to *war chalking*, i.e., the drawing of symbols like those depicted in Figure 1 below in public places to advertise the presence of a wireless signal, and whether it is accessible or secured.

Because of the nature of wireless routers and access points—designed with simplicity and ease of use in mind—there is no easy way to accomplish authentication before a signal is sent out. Therefore, routers are set by default to broadcast their network names or SSID as well as additional information to all users. If encryption is enabled, users will not be able to access any information other than this standard "handshake" information without a key. However, in either case it is not necessary to join a network to obtain information. By simply recording the public information sent to a wireless device, and moving that wireless device around to different areas, one can learn a great deal about networks in a given area.

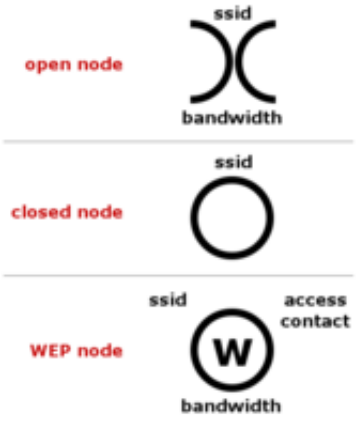

Figure 1: War chalking symbols

3 Legal Implications

When dealing with wireless communication, two major legal implications arise. The first concerns legal expectation of network owners. The second deals with the responsibility of users acquiring information about, or connecting to, any given wireless network to which they have not been specifically granted access. As with most emerging technology, laws governing operation or practice in relation to that technology are generally vague or initially non-existent. Sometimes old laws are required to be interpreted in new ways, and other times it may be necessary to produce a new set of laws specifically tailored to the technology at hand. Both of these processes are slow. The process of enacting new legislation to keep pace with technology is a protracted endeavor. Old laws that are re-interpreted to encompass new technology are often not effective until the first cases have reached appellate courts where the decisions set the precedents for future cases. According to recent reports, no cases on this issue have reached federal appellate courts [3]. However, because of the latest push for information security and customer/patient confidentiality, there have been some directives that impact the handling of legally sensitive information. These directives can be directly applied to the expectation of wireless network owners, although the law does not specifically mention wireless technology. These directives include GLBA for financial institution, HIPAA for health care, Sarbanes-Oxley for all U.S. public organizations, and Department of Defense directive DoD 8100.2 for government agencies. These laws and directives mandate the protection of information concerning customer health, financial status, personal information, and in general all information deemed sensitive by nature or explicitly classified [4]. Assuming that this type of information resides on an unsecured network, and that it is accessed without permission, it appears that these regulations would subject network owners to liability.

The second area of concern for network owners is criminal activity conducted on their own network by users gaining unauthorized access. If a wireless network is insecure and an unauthorized user connects and proceeds to launch attacks from this network, it is possible that the wireless network owner could be held legally accountable for the resulting damage. Wireless users are also bound by certain legal requirements. Originally, regardless of intent, any unauthorized connection to a network was illegal. However, because of the rapid growth of the technology, and the vendors' quest for increased simplicity, many devices that are wirelessly enabled automatically look for, and connect to, insecure networks within range, without direct user intervention. This caused the legislators to rethink the wireless communication laws. The focus shifted to the owner of the wireless network, removing most of the accountability from network users. This, however, does not indemnify users from intentional malicious or misuse of open networks.

Our identification of wireless signals was unobtrusive, in that we never used a discovered (unencrypted) wireless network access point to actually gain access to computers or the Internet. In this, we comply with the advisory warning posted by the FBI stating that "Identifying the pres-

ence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations" [5].

4 Description of the Experiments

Wireless security presence and security information was collected regarding access points in a one mile radius of the Northeastern University campus. All covered areas are depicted in Figure 2. The areas for which we are reporting our findings are those with the highest density of "dots"), i.e., the residences closer to campus for which we have enough data to draw statistically meaningful results.

To cover each area, cars were used with external antennas as well as walking down streets and through alleys. To accomplish this task, multiple groups were formed to cover small sections around campus. Results were then compiled. Each wireless access point Medium Access Control (MAC) address was counted only once to prevent duplicate data points. Two questions needed answers: What time of day should the data be collected, and how many times should the same areas be covered? We decided to collect all data during normal business hours and 9am to 5pm on the weekends. Given that most of the area covered in the one mile radius was student/residential, we felt daytime collection would be an accurate representation of average use. Walking through the streets of Boston required that our equipment must be portable and light to maximize our efficiency. The length of the data acquisitions was limited by battery power of the laptop. All peripherals were USB powered. We also utilized backpacks to maintain a low profile thus ensuring that users would not change their wireless habits as a direct result of our data collection. After the data was collected, it was exported into a NetStumbler [6] summary file that we uploaded to a website for data points parsing. The parsing generated a simpler CSV (comma separated value) file that was imported into "Microsoft Streets and Trips" [7]. The access point mapping was used to offer a visual to the project leaders to ensure that a one mile radius was covered as well as the entire area inside the radius. The experiments may easily be repeated because the software we used, NetStumbler, prevents duplicate MAC entries during a data merge.

4.1 Equipment

The hardware used includes an Orinoco Gold wireless card with an external 5dbi antenna and a NAVMAN GPS e Series USB GPS receiver [8]. This hardware was chosen because of its portability, which was critical in order to cover the "hidden" areas of Boston. NetStumbler [6] software was used to collect all of the data. After the data was collected and merged into a single "summary file," it was exported into a standard CSV file. This file was then

Figure 2: Visited Areas and Wireless Access Points

translated into a format suitable for importing into a mapping product that supports importing of data files, which also parsed the encrypted networks out from unencrypted networks [9]. Finally, "Microsoft Streets and Trips" [7] was used to plot each access point into a Boston map (Figure 2).

The wireless card was chosen for its ability to attach an external antenna which allows data to be collected from a car. The card also works in any standard installation of Windows XP or Linux. The GPS receiver was inexpensive; no special equipment was required because GPS waypoints were automatically updated in NetStumbler when a new network was detected.

4.2 Findings

Figure 3 shows the number of networks found in 2004 and 2005.

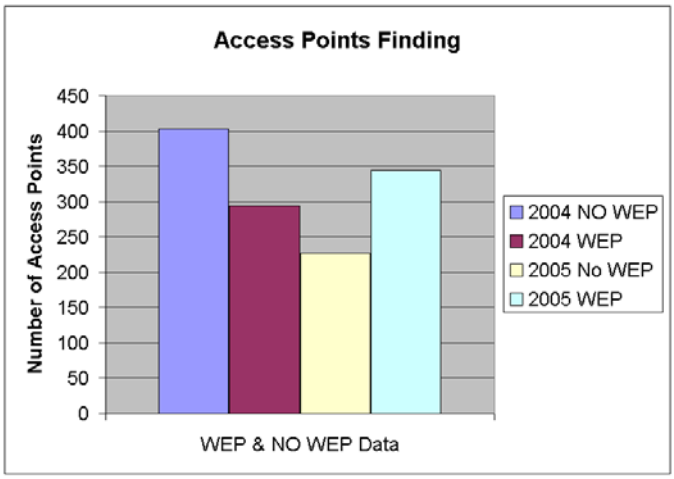

Figure 3: Wireless Access Points, 2004 and 2005

The bar graph shows the data collected in 2004 and 2005 grouped by WEP status. The graph shows that, for the same area, the number of protected access points versus the unprotected ones has almost reversed year to year. In 2004, 58% of the access points were not encrypted, while in 2005, 60% of them were. (The 2004 data set was slightly bigger than that collected in 2005.)

One reason for the increase in wireless security is education. Many articles have been published in several newspapers, which include the authoritative New York Times [10]. These articles discuss the "dangers" associated with not securing wireless networks.

Another speculation is that, until recently, wireless devices were shipped without security enabled. Therefore, security would have to be manually enabled by the user. Devices now come with "One-Touch Secure System (AOSS)." This allows the end user to press a button on the device and configure security through a simple interface.

Our finding are similar to those in a study recently performed were businesses and home networks were surveyed. The study revealed consistent results with our 2005 findings: Around 62% of the home networks were secured [11].

5 NU IEEE Activities

Since the inception and execution of "Hack Boston," promoting security awareness has become one of the proposed activities within the NU student chapter of the IEEE. More particularly, one of the services to the community surrounding our campus is going to be the creation of the "NU IEEE Wireless Clinic." This idea is going to be implemented by both a media campaign and by offering technical help to assist people in securing their wireless networks. More precisely, we will be involved in informing the population of Boston, especially that around campus, about the threats of leaving their wireless network unsecured. In addition, we will have students who are experts in wireless security volunteer to help those who are interested in learning more about wireless security and want to set up WEP/WPA for their wireless access points.

6 Conclusions

This paper presents the findings of a two-year experiment about monitoring the wireless security awareness of the community around the Northeastern University urban campus, in Boston, MA. Designed as a project for the NU student chapter of the IEEE, "Hack Boston" has exposed undergraduate students to a host of problems—from legal to technical—concerning the use of wireless access points (WiFi technology) for Internet connectivity and information exchange, and the need for securing this kind of communication. The study confirms that although progress is being made, most of the population in private housing surrounding the NU campus, is still unaware of the potential threats of unauthorized wireless access. The NU IEEE section is now committed to increasing the public's awareness of the risks of wireless networks, and assisting in the implementation of measures to make wireless networks secure.

7 Acknowledgments

The authors wish to thank the Department of Electrical and Computer Engineering at Northeastern University for support and encouragement throughout the project. Thanks also go to Professor Bruce McDonalds, who shared the initial idea for this project. Finally, data collection and data managements would not have been possible without the help of the NU IEEE crew, and especially of Carolyn Andrews, Neil Gupta, Zachary Johnson, Michael Mazzello, Andrew Medico, Daniel Quigley and Vishal Sunak: Thanks guys!

References

[1] A. S. Tanenbaum. *Computer Networks*. Prentice Hall PTR, Upper Saddle River, NJ, fourth edition, 2003.

[2] WiFi Alliance. Wpa2 (wi-fi protected access 2). http://www.wi-fi.org/OpenSection/knowledge_center/wpa2/, February 6 2006.

[3] E. Lawrence and J. Lawrence. Threats to the mobile enterprise: Jurisprudence analysis of wardriving and warchalking. In *Proceedings of the IEEE International Conference on Information Technology: Coding and Computing, ITCC 2004*, volume 2, pages 268–273, Las Vegas, NV, April 5–7 2004.

[4] A. Kathod. Questions on wireless security, December 2004. http://www2.cio.com/ask/expert/2004/ questions/question1981.html.

[5] A. Gaffin. Use an open wireless port; go to jail? http://www.networkworld.com/compendium/archive/001072.html, August 14 2002.

[6] http://www.netstumbler.com/.

[7] http://www.microsoft.com/streets/default.mspx.

[8] http://www.navman.com/land/products/eseries/.

[9] http://kb3ipd.com/phpStumblerParser/index.php.

[10] STANDARDS AND PRACTICES; to be safer, turn on the security. http://select.nytimes.com/gstabstract.htmlres=F00B13F93F590C778CDDAC0894DC%404482, 2004.

[11] E. Geier. A war driving experience–part i: The results. http://www.wi-fiplanet.com/tutorials/article.php/3581946, January 2006.