1-1-2007

User Security Behavior on Wireless Networks: An Empirical Study

Tim Chenoweth
Boise State University

Robert Minch
Boise State University

Sharon Tabor
Boise State University

User Security Behavior on Wireless Networks: An Empirical Study

Tim Chenoweth, Robert Minch, Sharon Tabor
Network, Operations, and Information Systems
College of Business and Economics
Boise State University
E-mail: {timchenoweth, rminch, stabor}@boisestate.edu

Abstract

Wireless networks are rapidly becoming ubiquitous but are often insecure and leave users responsible for their own security. We empirically study whether users are successfully securing their client computers when using wireless networks. Automated techniques are used that scan users' machines after they associate with a university wireless network. This determines whether a firewall is being used and what TCP ports are open. Results show that over 9% of 3,331 unique computers scanned were not using a properly configured firewall. In addition, almost 9% had at least one TCP port open, with almost 6% having open ports with significant security implications. We also found and discuss cases where connected computers were compromised by Trojan programs such as SubSeven and NetBus. We discuss the generalizability of our results to other potentially insecure wireless networks, and suggestions for further research.

1. Introduction

Analogous to the historic growth of the Internet, the number of wireless local area networks (hereafter referred to simply as wireless networks) is exploding with declining hardware prices and the rapid adoption of well-accepted standards. Using 802.11a/b/g standards (also known by the marketing name "Wi-Fi"), access points are increasingly acting as bridges for users of wireless devices to connect to wired local area networks and the Internet. Particularly significant are public access points, commonly known as hotspots, which are often located in heavily populated areas such as airports, coffee shops, hotel lobbies, and public areas, appealing to both business and casual users but offering little or no security [1].

By January 2006, public hotspots had already surpassed 100,000 worldwide, up from approximately 57,000 a year before [2]. About 8000 of these are free, and 92,000 charge for access (although approximately half of the latter are in hotels and restaurants, many of which offer access to customers at no added charge). These public hotspot numbers do not include large numbers of ostensibly private access points in homes and businesses or increasing numbers of free hotspots provided by municipalities and other entities. The growth in hotspots is expected to continue in part because they are inexpensive. For example, maintaining the Bryant Park Wireless Network in New York City and leasing its T1 backbone connection is said to cost less than the park spends on trash bags [3]. Additionally, the public in general and business users in particular are growing accustomed to the mobility and ubiquitous Internet access these networks provide.

A further impetus to wireless network use is the increasing proportion of mobile computers. In May of 2004 retail sales of notebook computers surpassed desktop computer sales for the first time [4]. Even with threats to data security on the rise, it is estimated that within the next three years 50% of all workers will be equipped with a laptop, even though only 10% of enterprises have a plan in place to manage and secure these devices [5]. While mobility has benefits in terms of employee productivity, managing this mobility and addressing security is an important requirement. Recommendations include using software solutions that track devices, enforce security policy, and synchronize data on the organization's terms. The software segment providing mobile security solutions is expected to grow to $400 million in sales by 2009, but with a cost of $50-$100 per user [5]. This added cost is often burdensome for individuals and organizations with limited budgets.

Computer and network security is consuming an increasingly larger amount of time, budgets, and other resources for individuals and organizations. The spiraling number of viruses and outsider attacks has driven this attention level, as has the shortened timeframe between vulnerability announcements and the appearance of global exploits. Despite this trend, many wireless networks and particularly public hotspots have little or no network security enabled. A recent survey conducted by Panda Software International determined that approximately 60% of all wireless networks do not use any form of

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

1530-1605/07 $20.00 © 2007 IEEE

encryption. Of wireless networks with encryption enabled, approximately 75% are using the wireless equivalence protocol (WEP), which has several well-documented security deficiencies [6][7][8]. The problem is even more acute with public hotspots because the users of these hotspots are interested in ease of use and not in the level of security employed [3]. Guests at hotels, for example, have reported theft of information from their computers while connected to the hotel's wireless network [9]. With the tendency of wireless users to access the Internet through many different public access points, the chance of picking up malicious code is high, and these threats are easily transferred to wired networks to which those users may later connect, thus extending the implications of user security to network security as well.

Given the open nature of public wireless networks, it is clear that it is the responsibility of the users of these networks to provide for their own security [3]. Therefore our study focuses on whether users of wireless networks are in fact securing their computers. There is surprisingly little quantifiable evidence that sheds light on this question, especially from the perspective of wireless users. For example, one study [10] examines users' *intention* to practice security (such as employing firewalls), but does not consider the wireless environment and does not quantify the subsequent *implementation* of user firewalls. Our study specifically explores the issue of wireless user vulnerabilities and security practices and quantifies the number of wireless users who are not achieving an adequate level of security.

Our goal is to directly investigate how well wireless users are securing their computers. Using a university campus wireless network, we perform a vulnerability scan of each wireless user shortly after they associate to one of the campus access points, using Nmap to perform the scan [11]. The results of the Nmap scans are used to determine the proportion of wireless users not using a firewall and the proportion of users with open ports. In particular, our study focuses on open ports with well known security implications [12] [13] [21] [22]. The specific research questions addressed are:

1. What is the percentage of wireless network users not using a firewall?

2. What is the percentage of wireless network users with detectable open ports?

3. Do open ports tend to be those with significant security issues?

The following section describes our methodology, including our subjects, the wireless network studied, data collection, firewall detection, and port-related vulnerabilities. Section 3 discusses our empirical results and relates these results to the research questions listed above. Finally, section 4 concludes by summarizing our findings, addressing the study's generalizability and limitations, and suggesting future research topics.

2. Methodology

2.1 Subjects

Subjects for the study are all authorized users of a campus wireless network. This potentially includes 18,599 students, approximately 1000 faculty and staff, and a variable number of visitors using the network. The university is a commuter campus with relatively non-traditional students and has 15,779 undergraduate students (average age 26) and 1663 graduate students (average age 36). The gender percentages are 54% female and 45% male (1% unspecified). Most students live off campus, and many have part-time jobs or full-time careers, often with one of several local high-tech firms. We view the non-traditional nature of the student subjects as a positive factor for the study as we believe it makes them more representative of the general public and workforce than traditional students would be.

It is possible that some wireless users on campus were not included in the study because they did not connect to an official campus access point, but instead connected to a "rogue" access point installed by a student in a dorm room, etc. While campus network administrators regularly detect and remove these rogue access points, they continue to come and go. From what can be observed over time, this is a very small minority of access points and users.

2.2 The Wireless Network

The wireless network uses approximately 80 Cisco 1200 wireless access points spread throughout a 175-acre campus. Most high-demand areas are covered, as evidenced by infrequent responses to a web form inviting users to report areas of missing coverage or poor signal strength.

Wireless user authentication is done using a web-based challenge-response system interfacing with the campus LDAP server and using the same single sign-on directory that authenticates users for the campus intranet and email systems. Once a user is authenticated, the MAC address for the network card installed on the user's computer is registered with the wireless network, allowing each authenticated machine to use the wireless network for a period of several days before the user is required to re-authenticate. This means that once a user has authenticated a computer with the wireless network, anyone with access to the authenticated machine has access to the wireless network until the authenticated period expires.

Wireless traffic on campus is segregated through the use of separate virtual local area network segments (VLANs) and IP subnets, and filtered through firewalls before reaching the campus internal network or the Internet. The wireless traffic is also managed through a traffic shaping device. However, other than the MAC-level access control described in the previous paragraph, there are no security measures in place on the wireless network itself. No encryption (e.g., WEP) is used over the wireless link, and users desiring additional security must use Virtual Private Networking (VPN), Secure Shell (SSH), or other measures not directly provided by the wireless network. While future plans call for automated vulnerability assessments that force users to prove that they have installed required operating system updates and anti-virus software, these security measures had not yet been implemented at the time of our study. We believe that this environment of minimal network-level security and heavy reliance on user security makes the campus wireless network reasonably representative of public hotspot-based wireless networks in general.

2.3 Data Collection

Data collection was performed continuously during a 41-day period from April 27 to June 7, 2006. During that time 3,331 unique, non-university managed computers connected to the wireless network. The data collection process consisted of two main components:

1. **User/client machine detection:** A continuously running script polled the entire set of access points to retrieve a list of associated user machines.

2. **User vulnerability scans:** For each associated user machine that had not been previously scanned, a vulnerability scan was performed using Nmap.

User detection was performed with a Perl script using Net-SNMP [14] and SNMP (Simple Network Management Protocol) [15]. The script visited each access point in a continuous loop 24 hours a day, collecting a list of IP and MAC addresses of associated computers. After the set of associated computers is passed to the user vulnerability scan, the next set is collected. However, before a specific computer is scanned its MAC address is compared to the MAC addresses already stored in the database. If the MAC address is found, the computer is not scanned. In other words, each computer is scanned exactly one time, regardless of how often it connected to the wireless network during the data collection period. The study was constructed in this manner in part to minimize any additional load placed on the wireless network and its users by the study.

Where we were able to identify wireless client machines as university-owned and maintained devices, we removed these from the analysis because security precautions for these computers are largely outside the control of their users. The number of devices so identified was 30, which is less that 1% of the total number of machines studied. It is quite possible that we were unable to identify every university-owned machine, but we have reasonable confidence that any left mis-identified constitute a very small percentage of the total studied and thus would not significantly affect our results.

User vulnerability scans were performed using Nmap [11]. This tool has been used by other vulnerability analysis researchers, who note that port scanning has long been used by computer security analysts and Nmap is an efficient and effective tool for this purpose [16]. The output of the Nmap scan was parsed and relevant data was entered into MySQL database tables. This data was then used to determine the percentage of wireless network users who: (1) do not have a firewall; and (2) have open ports that may have security implications as discussed later.

Nmap was used in verbose and aggressive mode (*nmap –v –A <ip_add>*). This enables Nmap to provide additional information, including information concerning the service (application) listening to a port. In addition, we used Nmap's default port scanning settings, which is to scan the first 1024 TCP ports as well as the higher numbered ports listed in Nmap's nmap-services database. The nmap-services database includes contributions from Nmap users world wide and contains a reasonably complete list of services and the ports they use. This also enables Nmap to use its nmap-services-probe database, which contains probes Nmap can use to verify the identity of a specific service located at a specific port [17]. This resulted in a total of 1663 TCP ports being scanned for each connected computer.

2.4 Firewall Detection

For the TCP ports scanned in this study, Nmap reports the specific status of ports where a service was detected. Nmap then reports the status of all the remaining ports that were scanned but did not have a service present. The status of each remaining port is either closed, which means that the port is accessible, but there is no application listening to the port, or filtered, which means that Nmap could not determine if a port was open because packet filtering was preventing Nmap's probes from reaching the port. This provided the basis for our decision rule to determine if a specific computer was using a firewall. If the ports with no detectible application listening were closed, then the decision was that the computer was not using a properly configured firewall. If the ports with no detectible application were filtered, then the decision was that the computer was using a properly configured firewall. Note that we use firewall as a general term for a number of possible filtering mechanisms that could be present, including both hardware and software-based firewalls. These decision rules are summarized in Figure 1 below.

Status→	**open**	**closed**	**filtered**
All Ports with no detectable service present	N/A	Decision: no firewall present	Decision: firewall present
Any port with a detectable service present	Decision: Possible security vulnerability	N/A	N/A

Figure 1. Port scan interpretations

We validated our firewall detection methods by scanning machines with known security configurations. Using two software-based firewalls among the most popular with wireless laptop users (the Windows XP built-in firewall and the third-party Zone Alarm personal firewall), we turned firewall features on and off before associating to the wireless network, followed by scanning the machines to confirm that the firewall status was properly detected. In every test case the scanning process and our decision rules correctly determined the firewall status.

2.5 TCP Port-Related Vulnerabilities

Many user security vulnerabilities are related to TCP ports either left open inadvertently or deliberately enabled and used by insecure applications. Any open port is a potential security issue, and of particular interest is the set of ports with generally agreed-upon security implications. The following discussion of port vulnerabilities relies, to a large extent, on material provided by Berghel and Hoelzer in [12].

TCP ports 135, 137, 138, and 139 in the Windows environment are used by the legacy NetBIOS API for Remote Procedure Call (RPC) communication, while TCP port 445 is the Server Message Block (SMB) port. These ports allow file and print sharing in the windows environment (among other things). They also allow file and print sharing with Unix/Linux platforms through SAMBA. All of these ports can allow null session connections by remote machines, in effect opening up the computer's hard disk to external access.

RPC vulnerabilities also extend to other ports. With many Internet service providers filtering port 135, ports 1026 through 1029 are being targeted with Windows Messenger pop-up spam, which is an RPC service. It is generally suggested that if Windows Messenger is not needed, ports 1026 through 1029 should be blocked.

Another Windows based vulnerable port related to NetBIOS is TCP port 42, which is the Windows Internet Naming Service (WINS). WINS maintains translation tables from NetBIOS Names to IP addresses for computers that share resources. It is possible for hackers to insert a corrupted table into the system, thereby directing computers to hacker controlled computers in a manner similar to ARP poisoning. In the latter case, a false MAC addresses is inserted into a frame to impersonate trusted network devices.

The Windows Remote Desktop Protocol (RDP) port (TCP port 3389) is also of note. This protocol provides remote access to Windows based computers. RDP has been shown to be susceptible to denial-of-service attacks. While this particular vulnerability has been patched, RDP has been prone to attack for several years and most security exports suggest that the port be blocked.

In both the Windows and Unix/Linux environments, ports 20 and 21 (FTP), port 23 (Telnet), and port 25 (SMTP) should all be blocked. All of these ports have well known security issues and are prone to stack overflow attacks and brute force authentication and password guessing attempts. In addition, port 22 (SSH) has the same vulnerabilities as the previously mentioned ports and has the potential for an attacker to create an encrypted session.

The Rlogin service (port 513) and the finger service (port 79) should also be blocked. Rlogin is used for remote access in the Unix/Linux environment. Most security experts suggest that SSH be used instead because of its encryption and stronger authentication. The finger service allows remote querying of a system for the usernames of individuals currently logged on. This gives potential hackers half of the username/password equation.

The LDAP service ports (TCP ports 389, 636, 3268, and 3269) should also be blocked. LDAP is a directory service used to lookup information such as usernames, passwords, email addresses, etc. It is possible, depending on how the information is stored, for a hacker to query the LDAP services and recover information.

A problematic windows service is UPnP (Universal Plug and Play), which is located on port 5000. This service has been plagued by buffer overflow and denial of service attacks for several years. In December 2001 the FBI urged consumers to disable the UPnP service because the threat was so significant [13]. Since then, Microsoft has patched UPnP several times, mitigating the threat. However, many security experts still consider UPnP to be a security threat and suggest disabling the service and/or blocking port 5000 [13].

It is also interesting to note the presence of ports 427 and 548. Port 427 is the port that the slp daemon listens to on Apple systems. The slp daemon advertises local services to the network, and is known to have security issues [21]. Port 548 is the port afpovertcp listens to. The afpovertcp service implements the Apple Filing Protocol, which enables file sharing on an Apple system over TCP connections. This service has many of the same security issues that plague the windows file sharing services and is very dangerous to leave unblocked [22].

3. Results and Discussion

In general, security experts agree that the most important step users of wireless networks can take to protect themselves from other wireless users is to use a properly configured firewall. This is relatively easy and inexpensive to do because of firewall software built into Windows XP [18] or available free from third parties [19], including open source alternatives for Linux [20]. To address research question 1, "*What is the percentage of wireless network users not using a firewall?,*" we looked at the status reported by Nmap for the TCP ports that did not have a detectible service installed, as described in Figure 1. We found that 9.13% of the 3,331 computers scanned were not using a properly configured firewall, as shown in Table 1.

Table1. Summary of Results

Research Question	*Results*
1. What is the percentage of wireless network users not using a firewall?	9.13% of the wireless network users were *not* using a properly configured firewall (304 out of 3,331 total users).
	90.87% of the wireless network users were using a properly configured firewall (3,027 out of 3,331 total users).
2. What is the percentage of wireless network users with detectable open ports?	8.62% of the wireless network users did have detectable open ports (287 out of 3,331 total users).
	91.38% of the wireless network users did *not* have detectable open ports (3,044 out of 3,331 total users).
3. Do open ports tend to be those with significant security issues?	Of the 287 users with detectable open ports, 189 (or 65.85%) had at least one open port with significant security implications.
	Of the 287 users with detectable open ports, 98 (or 34.15%) had *no* open ports with significant security implications.

Even with a firewall, wireless network users can have detectable open ports. An open port means that Nmap was able to determine that an application is accepting TCP packets from that port. Since any open port is a potential security risk, the second research question we examined was "*What is the percentage of wireless network users with detectable open ports?.*" In our study, 8.62% of the 3,331 computers scanned had at least one detectable open port, as shown in Table 1.

Table 2 shows the frequency of open ports found in our scans, ordered by decreasing frequency. As discussed in the previous section, some ports are more dangerous than others to leave open. This leads to the third research question "*Do open ports tend to be those with significant security issues?.*" Table 2 shows, in the second column, ports having a notable security issue. Shaded rows indicate a port with notable security issues *and* where we found at least one client with that port open. We found that 5.67% of the wireless users had at least one of these dangerous ports open and accepting TCP packets (see Table 1). See section 2.5 above for a discussion of each port's significance.

Table 2. Results from Nmap port scans

TCP Port Number(s)	*Notable Security Issue*	*Common Services*	*Percent Open*
139	Yes	Microsoft File and Print Sharing; Unix SAMBA	4.0%
135	Yes	Microsoft RPC Server	3.3%

445	Yes	Microsoft File and Print Sharing; Unix SAMBA	3.3%
3689		Rendezvous (Apple iTunes)	2.2%
427	Yes	Apple slpd	1.6%
1025		msrpc	1.3%
548	Yes	Apple afpovertcp	1.1%
5000	Yes	Universal Plug and Play	0.8%
80	Yes	HTTP Web Server	0.8%
1761		landesk-rc	0.7%
22	Yes	Secure Shell	0.5%
3389	Yes	Windows Remote Desktop Protocol (RDP)	0.4%
21	Yes	FTP	0.4%
25	Yes	SMTP	0.1%
1026	Yes	Microsoft RPC Server	0.1%
389	Yes	LDAP Service	0.06%
1027, 1028, 1029	Yes	Microsoft RPC Server	0%
20	Yes	FTP	0%
23	Yes	Telnet	0%
42	Yes	WINS Server	0%
79	Yes	Finger Server	0%
137	Yes	Microsoft File and Print Sharing; Unix SAMBA	0%
138	Yes	Microsoft File and Print Sharing; Unix SAMBA	0%
513	Yes	Rlogin	0%
636	Yes	LDAP Service	0%
3268	Yes	LDAP Service	0%
3269	Yes	LDAP Service	0%
8080	Yes	HTTP Proxy	0%

As can be seen in Table 2, the most frequently open ports are also some of the most dangerous. The top three open ports (in order 139, 445, and 135) are all dangerous and were discussed in section 2.5.

We also noticed the presence on the wireless network of several computers that were infected with various malware applications. A total of 17 computers (0.5% of the computers scanned) had at least one malware application installed. Although a small number relative to the total number of wireless users, the existence of malware is an important finding because such infected machines may be used to launch attacks against the much larger client population. A complete list of the malware found and the number of infected computers detected is presented in Table 3.

Table 3. Malware found

Name	*Description*	*Number of Users Infected*
NetBus	Very similar to Back Orifice. Allows for a computer to be controlled remotely without a client (from IRC). Online keystroke logging	9
qaz	A worm application that provides a backdoor into a system.	6
Kuang2	Provides a backdoor into a system. Also captures passwords.	5
Back Orifice 2000 (bo2k)	Allows for a computer to be controlled remotely without a client (from IRC). Online keystroke logging.	4
Elite on port 31337	Nmap uses Elite for anything it finds running on port 31337, which is a well known Trojan port. Most likely Trojan is Back Orifice	4
Trinoo Master	Server application used to simultaneously control many compromised computers. Most often used to begin and manage denial of service attacks.	2
SubSeven	Allows for a computer to be controlled remotely without a client (from IRC). Online keystroke logging.	2

A more detailed description of each malware application can be found at [23]. Note that many of the infected computers had multiple malware applications present. Of particular interest (and somewhat alarming) is the presence on many of the compromised computers of network monitoring and packet sniffing applications. Of the 17 infected computers, 12 also had at least one network monitoring/packet sniffing application. The most common network monitoring tools found were nessus, bigbrother, and netsaint.

4. Conclusions

4.1 Summary of findings

Our results indicate that a small but significant number of wireless network users are not using a firewall (9.13%) and/or have detectable open ports (8.62%), some of which have important security implications. The study also found that the ports most often left open were also the ports with the most serious security implications (see Table 1). When a machine had any ports open, there was a greater than 65% chance that one or more of those ports had significant security implications.

Of additional note are the 17 computers that have been compromised by various forms of malware. Also disturbing was the presence on these compromised machines of network monitoring tools such as nessus. This opens up the possibility of these infected computers not only being used to infect other unprotected computers on the network, but to also act as packet sniffers and to launch other forms of attack such as ARP poisoning and man-in-the-middle attacks. Wireless users are particularly vulnerable to man-in-the-middle attacks in which a hacker, using a computer, emulates a rogue access point with the specific intent of capturing log-in credentials.

4.2 Generalizability

The campus wireless network we studied shares many similarities with public hotspots—both free and fee-based. The network employs no form of security other than simple authentication and subsequent MAC-level access control. There were no enforced policies requiring users to employ security measures such as firewalls. Therefore, this study provides insight into the behavior of open wireless network users concerning their security precautions.

The campus user population is reasonably similar to the general public because of the large number of part-time and non-traditional students. These users connect to the wireless network with a variety of personal and employer-owned laptop computers, and perform a variety of tasks including personal, school-related, and work-related activities. If anything, because of security awareness and guidance provided by the university and their employers, they may be somewhat more security conscious than the general public, possibly understating the average wireless network user's vulnerability.

The methods we used may be replicated in a number of different wireless environments. As long as wireless access points support the SNMP protocol (as do most) and can be queried for information about associated users, user/client machine detection is feasible. Similarly, our user vulnerability scans rely only on the ability to probe client machines by IP address—a capability that should be available on any network with appropriate security permissions. Thus the same basic methodology can be applied to study additional wireless networks, whether they be open or closed, public or private. Our methodology also provides a reasonably general method for conducting wireless security audits.

4.3 Limitations

Although we scanned every client computer that accessed the campus wireless network during a 41-day period, there might be a small number of users undetected by this process. The majority of these are expected to be users who deliberately or inadvertently associated with ephemeral and unauthorized rogue access points. We estimate this number to be a very small percentage of the total users.

The vulnerability analysis we conducted is heavily dependent on TCP port scans. There are a lesser number of vulnerabilities associated with UDP ports, such as SNMP port 161, which we did not test. We also did not probe deeper than the port response level—e.g., if port 80 responded we did not then issue HTTP requests to that port to determine whether application-level authentication was in place that could provide some protection to the user. Of course, there are a host of other security-related issues that affect users and are outside the scope of this research, including privacy/anonymity, viruses, and spyware.

4.4 Future research

This study quantified a small but significant number of wireless network users not properly protecting themselves by using a properly configured firewall. It similarly identified a number of important vulnerabilities at the TCP port level that significantly compromises user security. Additional research is needed in other public and private wireless networks to confirm the broader applicability of these findings.

The present study addresses only one element in a larger constellation of wireless user security awareness and behavior questions, i.e., user security measures actually implemented at one point in time. Several other questions concerning knowledge, beliefs, and education/training effects need to be studied. Examples of specific questions include:

1. How knowledgeable are users about the specific vulnerabilities that exist on their computers?
2. How important do users believe firewalls and other security measures are to them personally?
3. If users are educated about wireless network vulnerabilities and offered training in how to mitigate them, how will their behaviors change over time?

Further research in this stream will investigate questions such as those above, as well as study emerging wireless networking threats.

5. References

[1] Poole, C. "Wireless Information Security," in *Information Technology Security, Advice from Experts*, Lawrence Oliva (ed). CyberTech Publishing, (Idea Group Inc.), London, 2004, pp. 110-143.

[2] Hamblen, M. "Wi-Fi hot spots top 100,000", Computerworld, accessed June 8, 2006 at http://www.computerworld.com/mobiletopics/mobile/story/0,10801,107991,00.html.

[3] Schmidt, T. and Townsend, A. "Why Wi-Fi Wants to be Free", *Communications of the ACM* 46:5, May 2003, 47-52.

[4] Gonsalves, A. "Retail Notebook Sales Top Desktops," TechWeb, accessed June 8, 2006 at http://www.techweb.com/wire/26805132.

[5] Chickowski, E. "Well-Managed Mobile Devices", *Processor* 27:49, December 9, 2005, pp. 1-10.

[6] PANDA Software International, "Security in Wireless Networks," accessed June 15, 2006 at http://vocuspr.vocus.com/VocusPR30/Temp/Sites/2631/28d2f2c9bfeb4c808531a849e150d810/WP%20Wifi.pdf

[7] Housley, R., Arbaugh, W. Security Problems In 802.11-Based Networks. *Communications of the ACM* 46:5, May 2003, 31-34.

[8] Borisov, N., Goldberg, I., and Wagner, D. Intercepting mobile communications: The insecurity of 802.11. *In Proceedings of the International Conference on Mobile Computing and Networking*, July 2001, 180–189.

[9] Dutton, A. "Hackers are sneaky threats for wireless-network users", Arkansas Democrat Gazette, May 4 2006. Accessed June 10, /2006 at http://www.nwanews.com/adg/Style/153726/

[10] Ng, B.Y. and Rahim, M.A., "A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security", *The Ninth Pacific Asia Conference on Information Systems*, 7-10 July 2005, Bangkok, Thailand. Accessed June 10, 2006 at http://www.pacis-net.org/file/2005/255.pdf.

[11] http://www.insecure.org/nmap

[12] Berghel, H. and Hoelzer, D. "Pernicious Ports", *Communications of the ACM* 48:12, December 2005, pp. 23-30.

[13] Gibson, S, "UnPlug n' Pray", accessed June 13, 2006 at http://www.grc.com/unpnp/unpnp.htm

[14] Net-SNMP, accessed June 14, 2006 at http://www.net-snmp.com.

[15] Mauro, D. and Schmidt, K. *Essential SNMP* (2nd ed.). O'Reilly, 2005.

[16] Lee, A.J., Koenig, G.A., Meng, X and Yurcik, W. Searching for open windows and unlocked doors: port scanning in large-scale commodity clusters. *IEEE International Symposium on Cluster Computing and the Grid*, May 2005.

[17] Insecure.org, accessed June 14, 2006 at http://www.insecure.org/nmap/man/man-version-detection.html

[18] Microsoft, "*Understanding Windows Firewall*", accessed June 9, 2006 at http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx.

[19] Zone Labs, "Zone Labs Free Downloads", accessed June 9, 2006 at http://www.zonelabs.com

[20] Smoothwall, "The SmoothWall Open Source Project", accessed June 9, 2006 at http://www.smoothwall.org/.

[21] Mac OS X slpd daemon temporary file creation vulnerability, accessed June 14, 2006 at https://www3.ca.com/securityadvisor/vulninfo/Vuln.aspx?ID=26466.

[22] SANS Institute, accessed June 15, 2006 at http://isc.sans.org/port_details.php?port=548

[23] CA Security Advisor, accessed June 14, 2006 at http://www3.ca.com/securityadvisor

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE