Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Wireless Network Security in Hospitality SMEs

Mark Schmidt
Mississippi State University

Allen Johnston
Mississippi State University

Kirk Arnett
Mississippi State University

Wireless Network Security in Hospitality SMEs

Mark B. Schmidt
Mississippi State University
mbs87@msstate.edu

Allen C. Johnston
Mississippi State University
acj4@msstate.edu

Kirk P. Arnett
Mississippi State University
kpa1@msstate.edu

ABSTRACT

Wireless access provides ubiquitous connectivity to many different user environments. Some small businesses, in the early majority of technology adopters, establish public-use wireless networks as a source of competitive difference. In this study, representatives of five small organizations within the hospitality industry were identified, contacted, and interviewed regarding their decisions to adopt wireless networks for consumer use. These SME representatives believe they gained a competitive advantage from their early adoption, and consider the benefits of the wireless technology to outweigh any potential risks. Consequently, they regard issues of security as minimal factors in adoption.

Keywords

Wireless networks, case study, security, SME.

INTRODUCTION

SMEs that choose to embrace wireless networks as a source of competitive distinction are operating on the steep side of the technology adoption curve (Mason, 1998). These SMEs enjoy the benefits of attracting and serving an emerging form of clientele, the more mobile consumer. By providing wireless access to broadband network services, these SMEs have given customers the opportunity to extend their online work and social and entertainment activities to places that were historically more bricks than clicks. As owners and managers of SMEs deliberate the decision to adopt wireless technologies, many of them focus on the potential benefits while giving little attention to the risks inherent in this form of technology. This paper examines the perceptions of owners and managers of several SMEs within the hospitality industry with regard to their decisions to implement public-use wireless network service.

As the wireless community continues to expand and evolve, a clear and abundant need exists to establish wireless security standards to provide increased levels of assurance in the medium. In general wireless security implementations, in their current form, do not provide an adequate level of security. However, the SMEs that provide wireless service to their customers do not exhibit a sense of urgency when it comes to protecting their technology investment from malicious activities. Despite media reports of hackers, viruses, and intellectual sabotage, the SME's interest, in matters of security is vastly overshadowed by their interest in customer attraction, retention and service.

BACKGROUND

Wireless Security Issues

Threats to wireless environments exist regardless of industry type, business size, or locale (Attaway, 2003). These threats are significant and potentially harmful if adequate measures of protection are not implemented. Similar to threats against wired network typologies, wireless network security focuses on four essential assurance elements: confidentiality, availability, integrity, and accountability (Vaughn, 2003). Confidentiality refers to the process of protecting information from acquisition and/or exploitation by unintended parties. The confidentiality of data involved in a wireless transmission is maintained through the use of encryption technology. The most prevalent wireless standard in use today, IEEE 802.11b, provides the Wired Equivalent Privacy (WEP) encryption layer to handle data encryption needs. Many organizations are currently utilizing IEEE 802.11b as the standard of choice for providing wireless access in a local geographic area (Chen et al., 2003). Unfortunately, WEP only provides a thin layer of protection, as it is easily compromised by numerous hacking techniques (Phifer, 2003). Availability is the process of sustaining the technology in a form that is usable for its intended purposes. IEEE 802.11b is certainly adequate in terms of providing wireless services; however, because of its high-risk status, any guarantee of intended use of the technology is questionable at best. Integrity refers to the reliability of data. In a wireless environment, the integrity of data in transmission from one host to another is easily threatened. A proven method of mitigation is through the use of Virtual Private Network (VPN) technologies that allow for the secure transmission of data over wireless media by providing encryption and authentication services. Wireless traffic is isolated to a non-routable, private network where a VPN gateway isolates the routable network (Internet) in a typical VPN. Through the use of VPN client software (free), a user can be authenticated and provided an encrypted tunnel for data traffic. Accountability refers to the process by which purveyors of technology are able to hold individuals or parties responsible for their actions. The use of VPN technology in a wireless environment provides a mechanism by which routed traffic requires an authenticated, encrypted source. This requirement of authentication provides a mechanism to identify those persons responsible for improper activity on a network.

Previous research has established a considerably large set of threats to the confidentiality, integrity, availability, and accountability of wireless network environments (Phifer, 2003; Welch et al., 2003). As is the case with many emerging technologies, concerns of these threats are often an afterthought. Wireless environment threats can easily translate into risks because of known vulnerabilities in 802.11b. Insertion attacks, in which a wireless client is plugged directly into a wireless access point without authorization, represent well-known threats. Another form of insertion attack is the plugged-in unauthorized base station. In this situation, an end-user establishes a personal wireless access point within a wired network without authorization. Additionally, wireless environments are susceptible to wireless traffic analysis, eavesdropping (both active and passive), unauthorized access, man-in-the-middle attacks, replay attacks, denial-of-service attacks, and session hijacking (Welch et al., 2003).

Level of Protection

Figure 1 describes the situation whereby threats, countermeasures, and remediation are considered in light of a cost benefit analysis to develop a reasonable level of protection. The cost / benefit portion of the model suggests that for systems with relatively low levels of risk for confidentiality, availability, integrity, and accountability, a reasonable level of protection can be achieved without a high level of expenditure. In most cases protection level and expenses are directly related (e.g. a minimal level of protection typically requires a minimal level of expenditure to ensure that protection). Additionally, protection / expense levels have a direct relationship with IT Value. Put another way, if the value of the IT is high then the protection level and typically the expense of providing that protection will be high as well.

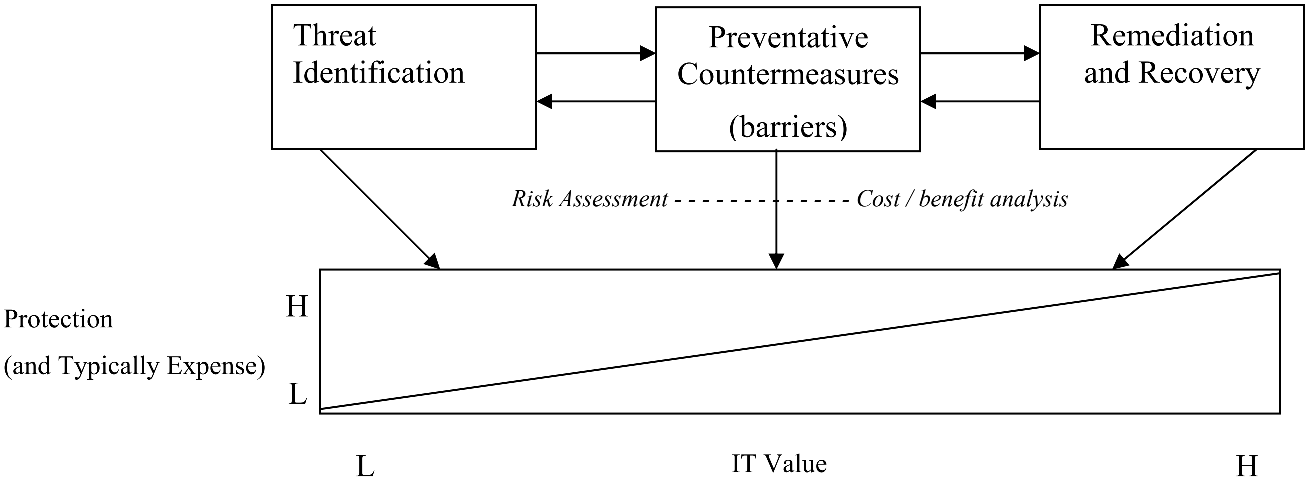

Threat Identification
Preventative Countermeasures (barriers)
Remediation and Recovery
Risk Assessment - - - - - - - - - - - - - Cost / benefit analysis
Protection
(and Typically Expense)
H
L
L
IT Value
H

Figure 1. IS Security Management Framework Adapted from (Warkentin et al., 2004)

It can be argued that the SMEs examined in this study employ wireless networks with low levels of risk to confidentiality, availability, integrity, and accountability. Further, their application environment is of low complexity. These wireless installations are vulnerable to a subset of threats that trouble most wireless networks. This is primarily due to the simplistic nature and intended use of the networks. As depicted in Figure 2, these wireless networks consist of a wireless access point (WAP) connected to a broadband router by Category 5 twisted pair cabling. Corporate clients and servers are not parts of the network.

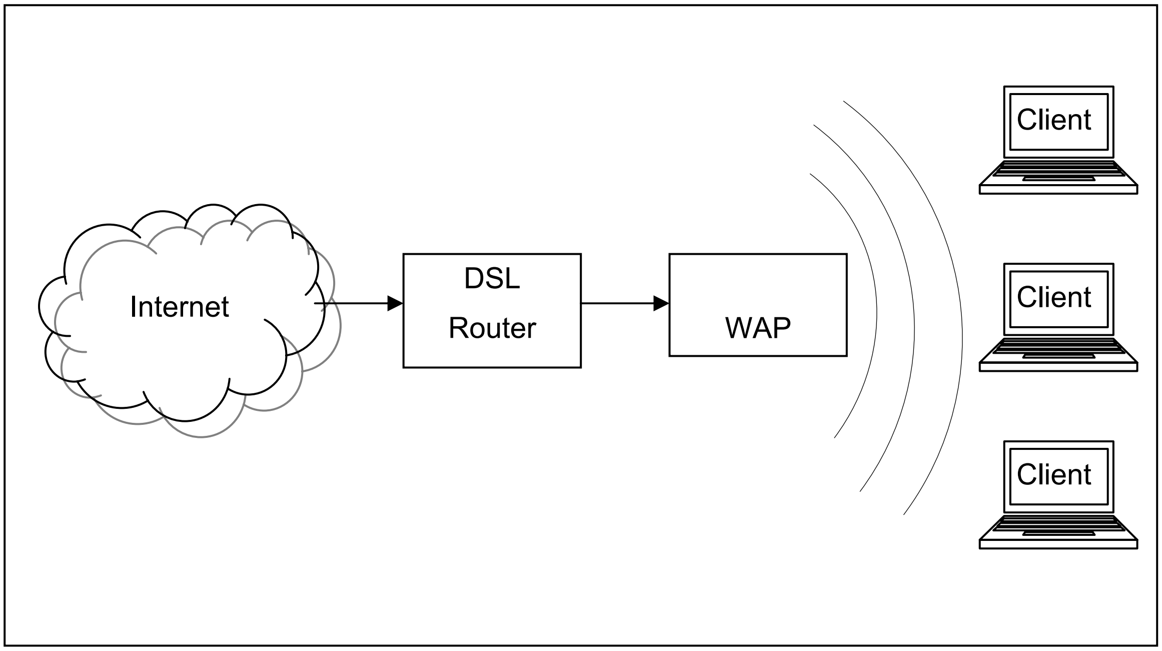


Figure 2. Simplistic Network Diagram

METHODOLOGY

The case study method was used to examine the security rationale of five organizations, located in the Southeastern United States, which incorporated wireless networks into their existing infrastructures and business plans. Case studies are appropriate when an in-depth understanding of a contemporary event is desired (Babbie, 2001). Further, qualitative methods, such as case studies, when properly utilized, can provide a great deal of knowledge and information for MIS researchers who are investigating phenomena in which organizational context and depth of knowledge are important (Goldstein, 1986). Wireless network implementation and security is an area that can be effectively examined with the case study method.

Five businesses were eventually selected for the case studies. The details of the selection are covered later. Each SME manager or owner was contacted in person and requested to spend approximately one hour in a face-to-face interview regarding their wireless network. Once permission was obtained, and the interview schedules were confirmed, at least two of the three researchers visited each business. The use of two or more researchers proved valuable for follow-up discussions to insure that more than the person asking the questions during each interview agreed with the interpretation of the interviewees' responses. Each respondent was given the required consent forms and a copy of the questions. Then the standard script of questions was discussed with all present. Typically, the SME owners/managers would ask questions of the researchers regarding our thoughts as to security measures that should be taken, and regarding the extent of reach of their signal. We were able to accommodate the latter request by using NetStumbler at the interview premises.

The standard script of questions was used in a pilot interview before being administered to the SME owner/managers. The pilot interview was given to the technology officer at a local church that had recently implemented a wireless network. After making some minor modifications to the script, interviews were conducted with representatives of five organizations over the next week. The same researcher asked the questions of all the interviewees while the other researcher(s) took detailed notes during the process. After each interview, all the authors met to compare notes and recap the important findings from the session. Table 1 presents an overview of the interview structure.

Establishment:	Interviewee(s):	Date:	Length:
Church (pilot interview)	Technology manger	1/16/04	1 ½ hours
Restaurant 1	Both owners (husband and wife)	1/20/04	1 ½ hours
Restaurant 2	Owner	1/23/04	1 hour
Hotel 1	Manager	1/22/04	1 hour
Hotel 2	Manager	1/22/04	1 hour
Hotel 3	Manager	1/22/04	1 hour

Table 1. Interview Structure

In order to determine the location of wireless networks, the researchers utilized word of mouth, company promotions, and NetStumbler software. Word of mouth and company promotions were used to find wireless networks that were somewhat established and popular in the community. However, there was not a comprehensive listing of public-use wireless networks available. As such, NetStumbler was employed to locate networks that were not promoted. NetStumbler software, when used in conjunction with a wireless network interface card (NIC), can detect the presence of wireless access points. The primary uses of NetStumbler are to locate rogue wireless access points which may pose a security threat and to "war drive." War driving is the practice of driving around to locate, map, and perhaps illegally steal the services offered by wireless networks (Tyler, 2003). Appendix A shows an example of a NetStumbler log produced during the research period. Three of the wireless networks were located with word of mouth / promotions and the others with NetStumbler. Table 2 provides an overview of the SMEs examined in this study.

Establishment:	Size:	Primary Reason for Wireless:	Location Method:
Restaurant 1	25 tables	Free / provide service to patrons.	Word of mouth.
Restaurant 2	15 tables	Installed free / provide service to patrons.	NetStumbler.
Hotel 1	69 rooms	Corporate mandate / provide service to travelers.	Word of mouth.
Hotel 2	76 rooms	Corporate mandate / provide service to travelers.	Word of mouth.
Hotel 3	105 rooms	Point of difference / provide service to travelers.	NetStumbler.

Table 2. Organizations, Rationale and Location Method

Two of the WAPs were initially implemented by technology-savvy friends or acquaintances, whereas the other were installed by a professional systems installer under contract with the companies corporate management consequently, the business owners and mangers typically did not put a great deal of effort into their decisions to adopt wireless networking. Table 3 provides an overview of the installation and costs of to the wireless networks. As stakeholders, the managers and owners of the SMEs have the most concern for the integrity of the wireless networks. However, many informed users may be concerned in regard to the security procedures employed on the network. One such concern relates to the fact that one user on the wireless network could potentially hack into another user's system.

Establishment:	Cost:	Installation / maintenance provided by:
Restaurant 1	$0	Local vendor (to promote his business).
Restaurant 2	$100 (equipment)	Owner's son and his friend (college students).
Hotel 1	Not specified	Regional consulting company.
Hotel 2	Not specified	Regional consulting company.
Hotel 3	Not specified	Regional consulting company.

Table 3. Overview of installation Issues

DISCUSSION

The majority of the SMEs involved in this study utilized their wireless networks in an atypical fashion. Specifically, most of the participants chose to provide wireless access to their patrons as a matter of differentiating themselves from competitors. They did so by providing a service as opposed to a more traditional use of wireless networks, such as interconnecting several components of an information system. Three of the participants indicated that their decision to incorporate wireless was voluntary. However, two of the participants indicated that their corporate management required a wireless networks to be installed.

The different perspective from which these particular SMEs in the hospitality industry view wireless networks in general and specifically wireless security, requires a depth of knowledge that can be effectively obtained from the case study method. The two-way communication afforded by the personal interviews was paramount in discovering the underling reasons for incorporating wireless, and understanding their approach to security.

The business owners and managers within this particular market segment view the threat horizon through a unique lens as illustrated in figure 3. From their perspective, the customer service benefits of wireless technology significantly outweigh the costs. From the mangers' perspective, the number one benefit involves providing a service to customers. The benefits are the underlying factors that guide the practices of the business owners and managers when faced with security issues.

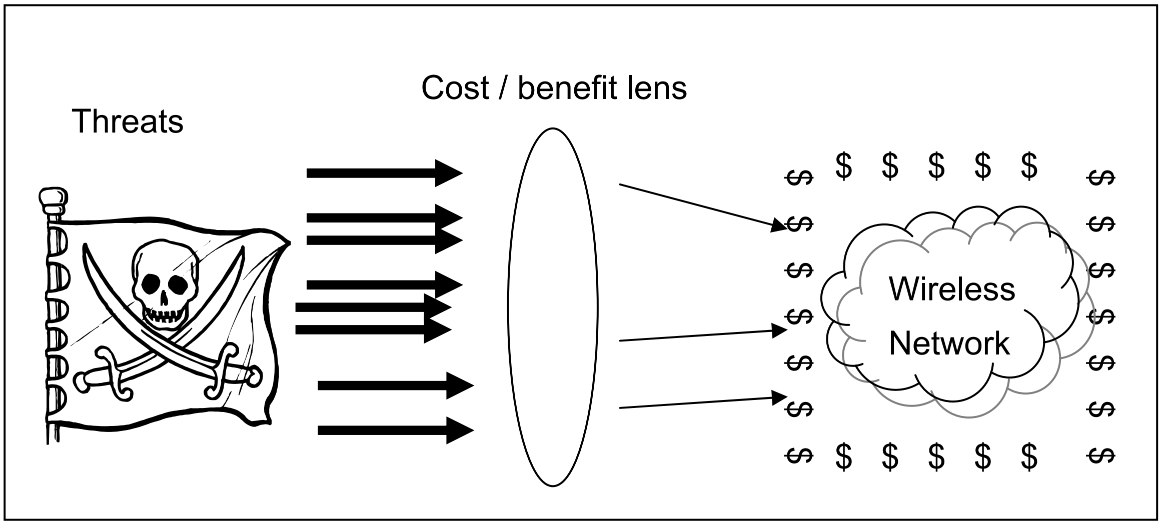


Figure 3. The Unique Threat Perspective of the Participating SMEs

It is estimated that 85% of wireless access points incorporate no security (Pfleeger et al., 2003). In fact, none of the five SMEs utilized WEP. Additionally, they made no efforts to manage data transmission security via a VPN. As a matter of ease of use and convenience to customers, clients, guests, and patrons, the restaurants do not even require a username or password to connect. All three hotels required a password to gain access. It is interesting to note that two of the hotels, although under different franchises, outsourced network management to the same company. Consequently, they used identical usernames and passwords for customer authentication. Table 4 presents an overview of the security concerns.

Establishment	WEP	UN / PW	Concerned?
Restaurant 1	No	None	No
Restaurant 2	No	None	No
Hotel 1	No	Never expire / same across the management organization	No
Hotel 2	No	Never expire / same across the management organization	No
Hotel 3	No	1. 24 hours use or 2. Never expires	Somewhat

Table 4. Security Concerns

When asked if anyone has ever broken into their wireless networks, four of the participants responded in the negative (at least to their knowledge). The manager of Hotel 1 indicated that a non-guest "broke in" to the network to check email. When asked what the non-guest was doing in the hotel with a computer, he responded that he was staying at another hotel that did not have access to the web. On the way back from dinner the non-guest noticed Hotel 1's wireless advertisement on the marquee and stopped to check his email. The manager added, "… the same (non-guest) person stayed at my hotel three weeks later when he was the area." The manger of Hotel 2 remarked that a non-guest noticed the marquee that mentioned wireless access. The non-guest asked the manger how much it would cost to get access to the wireless network. The manager replied, "The service is only for guests." Hotel 3's management indicated that the nature of the building construction and deployment of WAPs mitigates the risk of service theft. These responses provide clear indication that the managers of all three hotels are concerned about providing the service to guests only.

Neither restaurant provides wireless network security. Minimal security is provided by a third party at all three hotels. Utilizing NetStumbler, we provided the participants with the perimeters of their WAPs. In response to the perimeter information, the manager at Hotel 3 plans to be more vigilant in looking for non-guests in the parking lot who may be stealing service. The other two were less concerned.

Wireless networking is relatively new in the organizations under study. As such, it is not currently used to capacity. However, as the owner of restaurant 1 remarked "as more people get laptops with wireless cards, the system will be used more and more." Table 5 presents a summary of the usage levels in our study.

Establishment	Equipment for patrons:	Users per day	How long the service has been in place
Restaurant 1	None	5	1 ½ months
Restaurant 2	None	3	3 months
Hotel 1	10 bridges / free	15	2 months
Hotel 2	8 bridges / 8 cards / free	20	1 month
Hotel 3	5 wireless cards / $10 per day	25	6 months

Table 5. Usage Levels of Wireless Networks

IMPLICATIONS

It is clear that the Internet and e-commerce have reshaped the nature of the relationship between customers and businesses and have impacted entire industries (Daniel et al., 2002). It remains to be seen if broadband wireless access will have such an impact. According to Tom Higgins, president and CEO of Best Western Hotels, "[High speed Internet access / wireless is] the No. 1 amenity requested by virtually everyone, especially businesspeople" (Veiga, 2004). Wireless access is by no means is a new technology. In fact, wireless access points have been available since the early 1990s. Wireless access points have even been pushed by computer bellwethers such as Gateway and Dell since the late 1990s. According to a 2003 study which included a representative U.S. sample of age 18 and over respondents, 38% of the people are at least somewhat familiar with the technology (Laver, 2003).

It took 38 years for radio to attract 50 million users (Gabay, 2000). It is commonly accepted that Internet-related technologies have exceeded the adoption rates of earlier mass communications technologies by several magnitudes (Hannemyr, 2003). In fact, the Internet attracted 50 million surfers in only four years (Gabay, 2000). The combination of portable computing and communications is changing the manner in which casual computer users and professionals alike think about computing (Kleinrock, 2001). Popular press would lead us to believe that due to increase bandwidth and better security, wireless adoption will occur with similar speed (Coffee, 2002; Scheraga, 2002). Our findings indicate that usage of wireless is catching on with up to 25 users per day in Hotel 3. Time will tell when and if the use of wireless becomes as widespread as the use of the Internet itself. As the manager of Hotel 3 remarked, "Once a couple more national chains require access – then all hotels will require it".

These cases represent a distinctive culture of early majority participants. These business owners and managers are not technology focused, nor inclined to take technology risks; however, they do recognize trends in technology and are willing to implement technology as a means to establish a competitive advantage (Carr, 2000). For example, as a college student gets up to leave one of the restaurants, both owners (husband and wife) said, "Bye Kristen – good luck on your test – see you later." One owner then made the following statement that epitomizes his feelings toward the use of their network, "Even if people just come in to use wireless, they will probably make a purchase – if they don't, then hopefully they will come back and purchase something soon."

CONCLUSION

Much current literature focuses on the security of wireless networks, and indeed this focus is justified because of the inherent weaknesses of this technology. Little attention has been given to wireless network implementations where security is not a major concern. These SME cases represent the hospitality industry where wireless security has received minimal attention. Although, speculation suggests that the lack of technology acumen might be the reason, our cases present stronger reasons for the dearth of concern.

Competition in hospitality obviously centers on customer focus. This often translates to differentiation. For example, a hotel might consider a shoeshine shop, a turn down service, or a no-cost continental breakfast. Similarly, a restaurant might consider live entertainment, menu specials, or discount pricing, etc. These activities would be directed to differentiation to attract and retain customers. The five cases profiled here used wireless technology to differentiate their service and to attract and retain customers. Clearly from the interviews these owners and mangers believe their efforts are successful. Network security was never a primary focus; customer service always was. Table 5 shows that these SMEs had only adopted the technologies within the last six months. Yet every participant believed the investment to be cost effective and to hold high promise for the future.

ACKNOWLEDGEMENTS

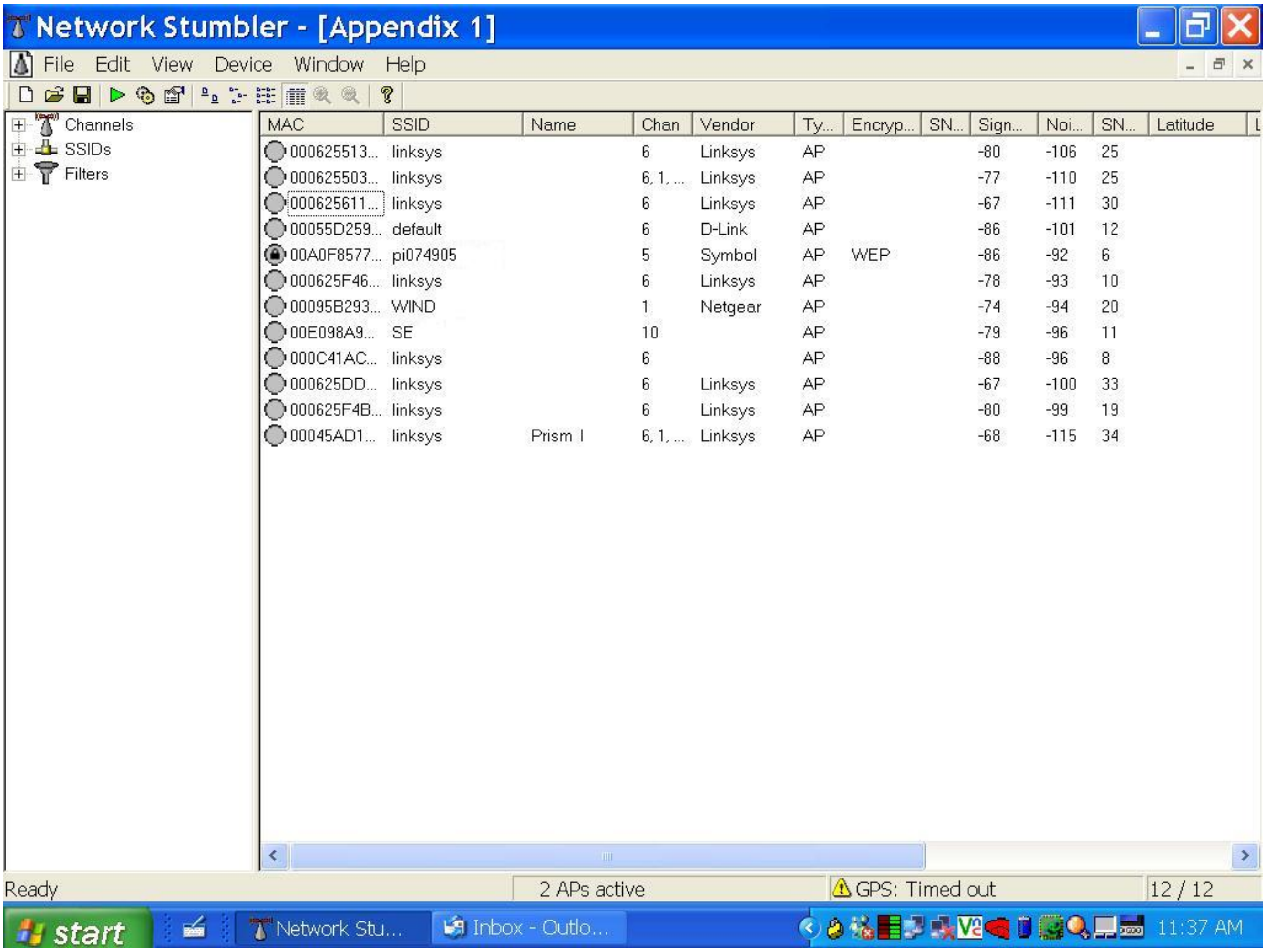
This research is supported by the Mississippi State University Center for Computer Security Research, and is funded by the National Security Agency, grant number DUE-0209869. The authors would like to thank the SME owners and managers for their time and thoughts during the interview process. Additionally, the authors thank the reviewers for the detailed feedback provided to improve this work as well as future work in this area.

REFERENCES

1. Attaway, M. "Protecting Against Wireless Threats," in: *Internal Auditor*, 2003, pp. 26-29.
2. Babbie, E. *The Practice of Social Research*, (9th ed.) Wadsworth / Thomson Learning, Belmont, 2001.
3. Carr, V.H.J. "Technology Adoption and Diffusion," 2000.
4. Chen, L., and Nath, R. "Implementing and Managing Wireless LAN: An Empirical Study," Ninth Americas Conference on Information Systems, Tampa, FL, 2003, pp. 73-76.

5. Coffee, P. "Innovation Still Thrives," in: *eWeek*, 2002, pp. 37-39.
6. Daniel, E.M., and Grimshaw, D.J. "An Exploratory Comparison of Electronic Commerce Adoption in Large and Small Enterprises," *Journal of Information Technology* (17:3), Sep 2002, pp 133-147.
7. Gabay, J. *Successful Cybermarketing in a Week,* Hodder & Stoughton, London, 2000.
8. Goldstein, D.K. "The Use of Qualitative Methods in MIS Research," ICIS, 1986, pp. 338-339.
9. Hannemyr, G. "The Internet as Hyperbole: A Critical Examination of Adoption Rates," *Information Society* (19:2), Apr-Jun 2003, pp 111-121.
10. Kleinrock, L. "Breaking Loose," *Communications of the ACM* (44:9), September 2001, pp 41-45.
11. Laver, M. "Awareness of Wireless Fidelity Taking Off," IPSOS New Center, 2003.
12. Mason, C. "Bursting at the Seams," in: *America's Network*, 1998, pp. 14 -18.
13. Pfleeger, C.P., and Pfleeger, S.L. *Security in Computing*, (Third ed.) Prentice Hall, Upper Saddle River, NJ, 2003.
14. Phifer, L. "Securing Wireless Access to Mobile Applications," *Business Communications Review* (33:9) 2003, pp 47-51.
15. Scheraga, D. "Retailers Go Mobile with Wireless.," in: *Chain Store Age*, 2002, pp. 104-106.
16. Tyler, G. "Go on a War Drive," *Management Services* (47:11), November 2003, pp 20-23.
17. Vaughn, R.B. "Advances in the Provision of System and Software Security -Thirty Years of Progress," in: *Advances in Computers*, Elsevier Science, 2003, pp. 287-340.
18. Veiga, A. "Best Western to Offer Free High-speed Internet," Associated Press, Chicago, 2004.
19. Warkentin, M., Schmidt, M.B., Johnston, A.C., and Boren, M. "IS Security Management Framework: A Comprehensive Life Cycle Perspective," Proceedings of the 2004 Information Resources Management Association (IRMA), New Orleans, LA, 2004.
20. Welch, D., and Lathrop, S. "Wireless Security Threat Taxonomy," 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, 2003.

Appendix A: NetStumbler log.



MAC	SSID	Name	Chan	Vendor	Ty...	Encryp...	SN...	Sign...	Noi...	SN...	Latitude	L
000625513...	linksys		6	Linksys	AP			-80	-106	25		
000625503...	linksys		6, 1, ...	Linksys	AP			-77	-110	25		
000625611...	linksys		6	Linksys	AP			-67	-111	30		
00055D259...	default		6	D-Link	AP			-86	-101	12		
00A0F8577...	pi074905		5	Symbol	AP	WEP		-86	-92	6		
000625F46...	linksys		6	Linksys	AP			-78	-93	10		
00095B293...	WIND		1	Netgear	AP			-74	-94	20		
00E098A9...	SE		10		AP			-79	-96	11		
000C41AC...	linksys		6		AP			-88	-96	8		
000625DD...	linksys		6	Linksys	AP			-67	-100	33		
000625F4B...	linksys		6	Linksys	AP			-80	-99	19		
00045AD1...	linksys	Prism I	6, 1, ...	Linksys	AP			-68	-115	34		