

A FRAMEWORK FOR ENTERPRISE-WIDE WI-FI NETWORK ACCESS SECURITY MANAGEMENT

Janice Sipior, Burke Ward

Villanova University

Linda Volonino

Canisius College

Abstract

Corporate wireless fidelity (Wi-Fi) networks are at risk from internal and external roaming users who may gain access, either intentionally or unintentionally, subjecting corporations to economic costs, security risks, and legal liability for both the activities of unauthorized roaming users and for violating legally required security. As a result, wireless network security must explicitly be considered enterprise-wide in reengineering business processes and employee responsibilities. This paper addresses the necessity to formulate an enterprise-wide Wi-Fi network access security management plan. We first consider the growth of wireless hotspots and the security risks to which they are subject. The benefits of Wi-Fi connectivity are then discussed. The critical responsibility for corporations operating in industry sectors regulated by security provisions in laws is addressed. To understand the sources of wireless security threats, we present our typology of roaming users and identify the risks they present. We then provide recommendations to corporations for formulating a Wi-Fi network access security management plan. Roaming use is a concern for corporations across the world, requiring national policies, and ultimately a global solution.

Keywords: *Wi-Fi networks, security, roaming users, management.*

INTRODUCTION

To remain competitive, corporations have long recognized the value of using information technology (IT) to reengineer both their business processes and employee responsibilities (Brown, 1995). The introduction of wireless fidelity (Wi-Fi) local area networks (WLANs), to corporate-wide Information Systems (IS), represents a major change enabling reengineering opportunities. Integral in this reengineering is the strategic necessity to address security. As the use of corporate and employees' home WLANs continues to increase, security concerns have heightened. While, "companies are putting more and more money into security and the plain fact is, wireless security just doesn't exist," (Hytnen and Garcia, 2006)

subjecting corporations to economic costs, security risks, and legal liability for both the activities of unauthorized roaming users and for violating legally required security. As a result, WLAN security must explicitly be considered enterprise-wide in reengineering business processes and employee responsibilities.

This paper addresses the necessity to formulate an enterprise-wide Wi-Fi network access security management plan. We first consider the growth of wireless hotspots and the security risks to which they are subject. The benefits of Wi-Fi connectivity are then discussed. The critical responsibility for corporations operating in industry sectors regulated by security provisions in laws is addressed. To understand the sources of wireless security threats, we present our typology of roaming users and identify the risks they present. We then provide recommendations to corporations for formulating a Wi-Fi network access security management plan. Roaming use is a concern for corporations across the world, requiring national policies, and ultimately a global solution.

THE GROWTH OF WIRELESS HOTSPOTS

WLANs became a mass market technology as a result of the IEEE 802.11 open standard. As the number of Wi-Fi client devices and users grew during 2000–2002, commercial wireless carriers began a worldwide deployment of network infrastructure (Schmidt and Townsend, 2003). In recent years, Wireless Internet Service Providers (WISPs) have increasingly installed Wi-Fi access points, known as hotspots (Balachandran et al, 2003). In the United States (U.S.) for example, WISPs originally targeted mobile business users at locations frequented by these users, such as airport lounges, upscale hotels, and coffee-shops. Increasingly inexpensive Wi-Fi hardware drove the proliferation of no-fee Wi-Fi hotspots in universities and office buildings. As the popularity of fee-free hotspots grew, cooperative open wireless networks, located in outdoor public open spaces, began to proliferate.

The number of Wi-Fi users worldwide is projected to reach 707 million by 2008 (Pyramid Research, 2003) and the number of mobile office workers increases every year (Allen, 2006). Approximately 5% of all Americans have WLANs in their homes (Kapica, 2004). As the number of Wi-Fi users has increased, security concerns have increased. Access points do not necessarily include extensive security layers. Users may have to provide the desired level of security themselves by using tools such as Secure Shell Protocol (SSH), Transport Layer Security (TLS) and its predecessor Secure Socket Layer (SSL), Pretty Good Privacy (PGP), and Virtual Private Network (VPN). Given the current state of the technology, security at a hotspot is unachievable (Potter, 2006).

Wireless networks are subject to all of the security risks of wired networks, in addition to security challenges unique to wireless. Wireless communications that are not properly secured are vulnerable to threats such as eavesdropping, traffic analysis, masquerading, replay, message modification, and jamming (GAO, 2005), as summarized in Table 1.

Threat	Description
Eavesdropping	The attacker monitors transmissions for message content.
Traffic analysis	The attacker, in a more subtle way, gains intelligence by monitoring transmissions for patterns of communication.
Masquerading	The attacker impersonates an authorized user and exploits the user's privileges to gain unauthorized access in order to modify data.
Replay, Delay, or "Man-in-the-Middle"	The attacker places himself between communicating parties, intercepting their communications to delay and/or retransmit them.
Between-the-Lines	The attacker gains access to an authorized user's communication channel when the user is not using it, such as when he has remained logged on during a lunch break.
Message modification	The attacker alters a legitimate message by deleting or modifying it.
Jamming	Attackers flood a wireless network with stronger radio signals to prevent authorized users from accessing it.
Denial of Service	Attackers overload a wireless network with scripts capable of generating large volumes of traffic during a short period of time.

Table 1. Examples of Wi-Fi Security Threats (Based on GAO, 2005; Cabrera, 2002; and Patiyoot, 2002).

THE BENEFITS OF WI-FI CONNECTIVITY

Corporations are increasingly recognizing the benefits of Wi-Fi, including mobility, flexibility in connectivity, information access, improved efficiency, low cost, ease of use, and new applications which could change the way in which business is conducted. To achieve such benefits, both business processes and employee responsibilities must be reengineered. The U.S. federal government for example, enables employees to work in a variety of ways, such as collaboratively working on projects or developing products while in geographically separate locations. Corporations are using basic applications such as wireless email, web browsing, and intranets and are also beginning to take advantage of wireless connectivity for key applications, such as mobile supply chain management and enterprise resource planning applications (Webb, 2005).

Further expanding wireless connectivity could bring about a new ubiquitous economic environment. Mobile commerce (M-commerce) has emerged, resulting in changes in products and services themselves, their delivery, and how the processes underlying the completion of transactions are performed. Location-based marketers may direct advertising or promotions to roaming users. For example, customers in the test market of Boston Market, Donatos, and Starbucks can use the internet to find the nearest location, order, prepay, and avoid in-store lines when picking up their order. Wi-Fi connectivity has brought about a new consumer experience.

CORPORATE SECURITY CONTROL REQUIREMENTS

The security of proprietary information and systems can not be guaranteed should roaming employees use unsecured hotspots or uninvited roaming users enter unsecured corporate WLANs. Confidence, in the organization's ability to protect the privacy of proprietary data, can be lost. However, Wi-Fi security is especially critical for corporations operating in industry sectors regulated by security provisions in laws. In the U.S. for example, such laws include the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Sarbanes-Oxley Act of 2002. The results of a survey of organizations, in both the private and public sectors, indicate that Sarbanes-Oxley has had an impact on information security across several industries (Gordon, 2005).

SOURCES OF WIRELESS SECURITY THREATS

Corporations can centralize control over resources present within the physical perimeter of the facilities, including computers, servers, wired connectivity, and employees (Allen, 2006). The best tools and procedures for securing technological resources and related transmissions can be effectively applied. However, WLANs introduce the possibility of transmissions to extend beyond corporate walls, with each access point representing an ingress point into the internally protected network (Potter, 2006). A survey of private and public organizations, capturing responses for 7 years, shows that the frequency of security breaches has been steadily declining since 1999 in almost all categories (Gordon, 2005). A notable exception is an increase in the abuse of WLANs.

The majority of system intruders have been found to be hackers looking to steal credit card numbers and other financial data (Hanna, 2005), modify data, or harm the system (Lin, 2006). Employees may represent the biggest threat to computer security (Hanna, 2005). The claim that the majority of computer crimes are committed by insiders is not supported by the results of survey, of private and public sector organizations conducted for 10 years, which reveal that events perpetrated by insiders are detected about as often as those by outsiders (Gordon et al., 2005). To better understand the types of roaming users, we present our typology of them in the next section.

Topology of Roaming Wi-Fi Users

Roaming users can be characterized along two dimensions: the relationship of the roaming user with the corporate owner of the Wi-Fi network and the access authorization status of the user. A roaming user may be an internal employee of the corporation or may be external to the corporation. A roaming user may have authorized or unauthorized access to the Wi-Fi network. The four combinations result in Cells 1-4, as shown in

Figure 1, characterizing roaming users.

Relationship of User with Corporation	Internal to Corporation	Cell 1: Employees	Cell 2: Dishonest Employees
	External to Corporation	Cell 3: Business Partners	Cell 4: Intruders
		Authorized	Unauthorized
Access Authorization Status of User			

Figure 1. *Typology of Roaming Wi-Fi Users.***Cell 1. Employees: Internal with Authorized Access**

Employees, internal to the corporation with authorized access, are the intended roaming users, as shown in Cell 1. Employees represent a risk because they may not recognize or be aware of acceptable use practices, especially when utilizing Wi-Fi networks offsite. Employees accessing organizational information from hotspots or wireless home networks may not have security features enabled. The organization itself may have carefully implemented a secure VPN to protect organizational information from unauthorized access. A well-intentioned employee working from an unsecured wireless access point at home or while in transit, beyond the auspices of the organization's information systems division, subjects sensitive data to unauthorized access. A hacker could easily gain access to the organization's networks, through the VPN, using the identity of the employee with all of his user rights and privileges. A recent survey estimates that about 80% of U.S. residential wireless networks are unsecured (Hines, 2005). Organizations are thereby placed at risk by well-intended employees.

Cell 2. Dishonest or Intruding Employees: Internal but Unauthorized Access

Cell 2 represents employees who are internal to the corporation, but with no authorization to access WLANs in performing their corporate responsibilities. These unauthorized roaming users may access corporate WLANs either unintentionally, should the Wi-Fi network be left unsecured, or intentionally, through hacking activities or as a result of a security flaw. For example, Microsoft Windows XP operating system contains a "zero configuration" feature designed to facilitate connecting to Wi-Fi networks, which can cause a user to connect unintentionally.

An employee who intentionally accesses an unsecured network may be dishonest or disgruntled. This wireless hacker, or “w-hacker,” may apply his corporate knowledge in seeking personal gain or acting on behalf of a malevolent third party. Organizations could be held liable for such employee actions.

Cell 3. Business Partners: External with Authorized Access

Business partners, such as suppliers or customers, may be authorized to access corporate WLANs for the purpose of conducting business. Access should be restricted to only those facilities required to complete a transaction. In business transactions, the corporation has the responsibility to secure the transaction through user authentication and data encryption. User authentication ensures identification of an individual user, usually on the basis of a username and password. Data encryption is the translation of data into a form that is unintelligible without a deciphering capability, should an interception occur.

Cell 4. Intruders: External but Unauthorized Access

External roaming users may arrive uninvited, unintentionally or intentionally, to avail themselves of free internet connectivity or for malicious reasons. As previously discussed, unintentional, or accidental, roaming use may occur when the user is unaware of the source of wireless internet connectivity, should the corporation’s Wi-Fi network be left unsecured. Some organizations may leave their access points unsecured, intentionally allowing external roaming use. A report issued by the U.S. federal government revealed that a test of six federal agencies detected signal leakage at all six agencies and 13 of 24 major federal agencies do not require Wi-Fi networks be set up in a secure manner (GAO, 2005). Accidental intrusion is unlikely because a secure network would likely prompt a roaming user to enter a username and password as part of the user authentication process, alerting the user to the presence of security. Such access could, as previously mentioned, result from a security flaw.

Intentional roaming users, or “w-hackers,” may engage in activities for destructive, malicious, theft, espionage, or entertainment purposes. These include spamming; sharing copyrighted files; accessing pornography; port scanning for vulnerable services on an internet host; stealing, modifying, deleting, or simply viewing data; or otherwise causing harm to a computer, system, or data. Organizations could be held liable for unwittingly allowing their computers to partake in these illegal activities. Thus, it is essential that corporations formulate a Wi-Fi network access security management plan.

WI-FI NETWORK ACCESS SECURITY MANAGEMENT

“Security is the paramount concern in evaluating any ... wireless offering” (Zenel, 2005). To secure against unauthorized access, a formal comprehensive enterprise-wide Wi-Fi network access security plan should be formulated to provide standardization, allowing for improved implementation, management, and support.

Based on research addressing wireless network security (Fodil and Pujolle, 2005; Hanna, 2004; Siegel et al., 2004; Cabrera et al., 2002; Patiyoot, 2002), we formulate an approach to the plan, including both an audit and an assessment, as depicted in Figure 2. The audit includes the analysis of the Wi-Fi network. In addition, the audit encompasses an assessment of the risks, vulnerabilities, and threats to which the network is subject for the purpose of formulating countermeasures. Recommendations for a formal enterprise-wide Wi-Fi network access security management plan are summarized in Table 2.

Wi-Fi Network Access Audit

Our proposed Wi-Fi network access audit first entails a detailed analysis of the security features of the Wi-Fi network. For example, the IEEE 802.11i standard provides greater security features, including hardware based encryption, offering improved security. Enhanced authentication and encryption mechanisms are provided using an authentication mechanism called the Extensible Authentication Protocol (EAP). With EAP, the appropriate authentication, as desired by corporate management, may be used (Potter, 2006). Authentication may be a simple username and password or bidirectional certificate-based authentication, a primary method for securing wireless networks. However, bidirectional certificate-based authentication is difficult to assemble and maintain (Potter, 2006). At the time of installation, native security features are usually turned off by default, simplifying installation in the trend toward “plug-and-play.” Once the audit has identified the security features present, the risks, vulnerabilities, and threats are assessed to determine necessary countermeasures.

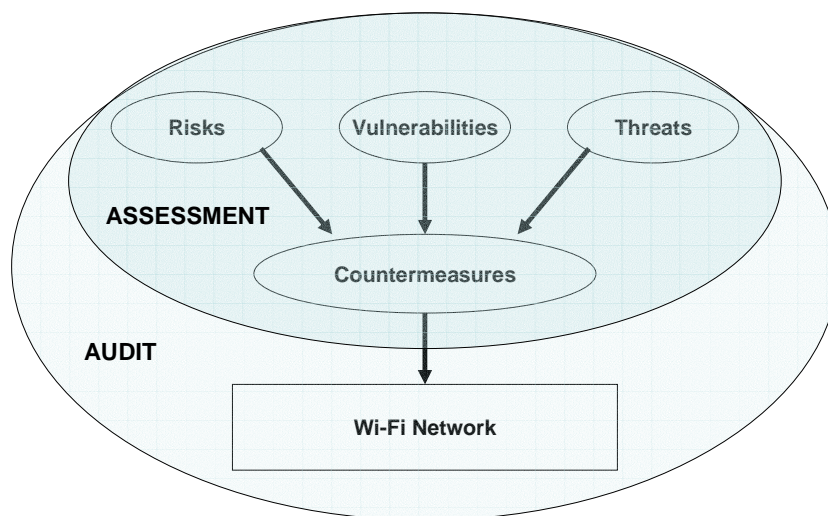


Figure 2. A Framework For Enterprise-Wide Wi-Fi Network Access Security Management (Based on Siegel et al., 2004 and Patiyoot, 2002).

Recommendations
Comply with ISP user agreement
Comply with security provisions in laws
Install standard encryption software
Authenticate approved user devices
Implement a virtual private network (VPN)
Monitor periodically to ensure security measures are functioning
Implement a proactive measures, such as an intrusion detection system
Formulate a formal written Wi-Fi Security Policy and train roaming employees to:
<ul style="list-style-type: none"> • Allow use of publicly accessible Wi-Fi only for specific purposes • Secure access of organizational systems and data • Use vigilance with physical access devices; provide guidelines to report losses

Table 2. Recommendations for WI-FI Network Access Security Management (Based on Sipior and Ward, in press).

Corporations are experiencing pressure to develop internal self-audits, as a result of the arrival of the Sarbanes-Oxley Act (Maurizio, 2007). To support compliance, a recent survey (May 2003) conducted by AMR, reported that 85 percent of companies surveyed indicated they were preparing for changes in their systems (Maurizio, 2007). The Wi-Fi network audit can include a detailed analysis of the security features of the network (Siegel, 2004), while identifying changes for compliance. For example, Sarbanes-Oxley requires as few interfaces as possible, which means reducing or eliminating any interfaces that would allow interruption of data flow between systems. Thus, any unnecessary use of wireless data transmission to portable user devices should be eliminated. System-to-system linkages that do not require such wireless data transmission should be established by fully integrated systems that process data and data flow consistently and with integrity (Maurizio, 2007).

Wi-Fi Network Access Assessment

In undertaking an assessment of Wi-Fi network access, risks, vulnerabilities, and threats must be evaluated. We do not take a strict interpretation of these terms, but rather we employ them to take a more comprehensive approach in the assessment. Risks arise because the network is vulnerable to unauthorized access which threatens the confidentiality and integrity of data transmissions and files. Example threats are presented in Table 1. Once recognized, appropriate countermeasures must be developed and implemented to eliminate the risks, vulnerabilities, and threats. For example, wireless transmissions can be intercepted within the

transmission radius. Once attached to the access point, the intruder may threaten the WLAN by eavesdropping or masquerading. In response, or proactively in advance, appropriate countermeasures, such as controls and procedures, must be developed.

Controls and procedures must meet the security requirements of applicable laws. Security considerations include the installation of standard encryption software, authentication of approved user devices to connect to the wireless network, implementation of a VPN for password protection, and implementation of firewalls to control the communication flow. For example, Wi-Fi Protected Access (WPA), the successor to WEP, and the 802.11i wireless standard manage encryption, while VPN authenticates the user's device and password. Wireless access should be restricted to only documented devices for which security has been approved. Periodic monitoring should be undertaken to assure security measures are functioning. For example, monitoring software may be used to undertake a site survey to detect signal leakage and unauthorized wireless-enabled devices. A wireless network intrusion detection system detects inappropriate communication activity, ensures configuration requirements are followed, and ensures that only approved wireless access devices are functioning.

Fundamental to the formal enterprise-wide plan is training and support for employees to ensure that wireless networks are configured, maintained, and used properly (GAO, 2005). Those authorized to use wireless connectivity should be identified. A policy for the use from home or while in transit should be formulated. Support for securing wireless networks at home should be provided. Acceptable use of publicly accessible Wi-Fi should clearly state what type of information may be communicated. Emphasize the necessity of vigilance in looking after physical access devices and provide guidelines for reporting losses.

CONCLUSION

The availability and use of Wi-Fi networks continue to increase. For users and corporations, Wi-Fi facilitates greater mobility, information access, flexibility in connectivity, improved efficiency, low cost, ease of use, and new applications which could change the way business is conducted. Proper management of this resource is the responsibility of the corporation which owns it and benefits from it. These obligations are premised upon, but are not limited to, those under an ISP user agreement and privacy and security provisions mandated by statutes such as HIPAA and Sarbanes-Oxley.

Network owners are exposed to potential system disruption and degradation, increased costs, security risks, and liability to third parties. Corporations have an ethical and legal obligation to reasonably manage their resources and protect against unauthorized use of their systems and access to data by managing Wi-Fi network access security. A formal written Wi-Fi Security Policy should be formulated and employees should be trained in appropriate Wi-Fi security practices, especially when remotely accessing the network. Although wireless network management is comprised of both technical and managerial considerations, most research focuses on technical considerations. As Wi-Fi use continues to increase, we call for additional research to respond to the need to develop best practices for Wi-Fi network management.

References

- Allen, M. 2006. 'An IT Manager's Insight into Mobile Security.' The British Journal of Administrative Management, April/May: 22-23.
- Bahl, P., Balachandran, A., Miu, A., Russell, W., Voelker, G.M. and Wang, Y.M. 2002. 'PAWNs: Satisfying the Need for Secure Ubiquitous Connectivity and Location Services.' IEEE Wireless Communications Magazine, Special Issue on Future Wireless Applications, February: 40-48.
- Balachandran, A., Voelker, G.M., Bahl, P. 2003. 'Wireless hotspots: current challenges and future directions.' Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots, San Diego, CA, USA: 1-9.
- Brown, A. 1995. 'Human factors: the problems of integrating people and technology in the workplace.' On the Horizon, April/May: 1-6.
- Cabrera, J.B.D., Lewis, L., Qin, W., Lee, W., Mehra, R.K. 2002. 'Proactive Intrusion Detection and Distributed Denial of Service Attacks--A Case Study in Security Management.' Journal of Network and Systems Management, 10(2): 225.
- Fodil, I. and Pujolle, G. 2005. 'Roaming and service management in public wireless networks using an innovative policy management architecture.' International Journal of Network Management, 15(2): 103-121.
- GAO (U.S. Government Accountability Office). 2005. 'Information Security: Federal Agencies Need to Improve Controls over Wireless Networks,' May: www.gao.gov/cgi-bin/getrpt?GAO-05-383.
- Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. 2005. 'CSI/FBI Computer Crime and Security Survey.' Computer Security Institute, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf
- Hanna, G. 2005. 'Securing Wireless Networks Against Intruders.' The CPA Journal, 75(4): 68-69.
- Hanna, G. 2004. 'Into Thin Air: Preventing Wireless Data Theft.' Risk Management, 51(12): 42.
- Hines, M. 2005. 'Worried about Wi-Fi Security?' CNET News.com, 19 January: http://news.com.com/Worried+about+Wi-Fi+security/2100-7347_3-5540969.html.
- Hytinen, R. and Garcia, M. 2006. 'An analysis of wireless security.' Journal of Computing Sciences in Colleges, 21(4): 210-216.
- Kapica, J. 2004. 'Consumers Still Hazy on Wi-Fi Facts: Study.' Globeandmail.com, February: <http://www.globetechnology.com/servlet/story/RTGAM.20040225.gtWi-ifeb25/BNSStory/Technology>
- Lin, P.P. 2006. 'System Security Threats and Controls.' The CPA Journal, 76(7): 58-66.
- Maurizio, A., Girolami L., and Jones, P. 2007. 'EAI and SOA: factors and methods influencing the integration of multiple ERP systems (in an SAP environment) to comply with the Sarbanes-Oxley Act.' Journal of Enterprise Information Management, 20(1): 14-31.
- Patiyoot, D. 2002. 'Security issues for wireless ATM networks.' ACM SIGOPS Operating Systems Review, 36(1): 31-57.
- Potter, B. 2006. 'Wireless hotspots; petri dish of wireless security.' Communications of the ACM, 49(6): 50-57. Pyramid Research, http://www.pyramidresearch.com/info/press/release_030721.asp
- Schmidt, T. and Townsend, A. 2003. 'Why Wi-Fi Wants To Be Free.' Communications of the ACM, 46(5): 47-52.
- Siegel, J.G., Levine, M.H., Siegel, R.M. 2004. 'Security Safeguards Over Wireless Networks.' The CPA Journal, 74(6): 68.
- Sipior, J.C. and Ward, B.T. in press. 'Unintended Invitation: Corporate Wi-Fi Use by Roaming Users.' Communications of the ACM.
- Webb, R. 2005. 'The untethered business.' Communication News, 42(3): 50.
- Zenel, B. and Toy, A. 2005. 'Enterprise-Grade Wireless.' Queue, 3(4): 30-37.