Reviewing 802.11 Wireless LANs Security: A Case Study Approach

Yue Cai, The University of Auckland, Private Bag 92019, Auckland, New Zealand; E-mail: ycai015@auckland.ac.nz
Jairo A. Gutiérrez, The University of Auckland, Private Bag 92019, Auckland, New Zealand; E-mail: j.gutierrez@auckland.ac.nz

ABSTRACT
This paper proposes a set of technical and managerial solutions which can be adopted by organizations to protect their 802.11 wireless LANs. A case study methodology was carried out by selecting five individual cases, including two wireless vendor cases and three organizational user cases. The primary source of data was face-to-face interviews. Another portion of the data came from extensive secondary materials. Findings from the case study were integrated with the ones from the existing literature to shape the final conclusions and recommendations of this research.

Keywords: 802.11 Wireless LANs; security; guidelines; case study

1. INTRODUCTION
Compared with wired networks, wireless networks may be more vulnerable and easy to attack. In a wired network, an attacker must penetrate some physical security perimeter to gain network access. In a wireless environment, attackers can easily gain access to the wireless network without getting into the building. The broadcast nature of wireless networks also makes traditional link-layer attacks readily available to anyone (Arbaugh 2003). According to a survey conducted by Computer Weekly's InfoSecurity User Group (CWIUG), more than four companies in five are worried about the security of wireless mobile products and services (O'Halloran 2004).

This research aims to present a set of security solutions, from both the technical and managerial perspectives, which can be adopted by organizations to protect their 802.11 wireless LANs. The paper is organized as follows: the next section discusses the literature review. After that, the research method employed in this work is described. Thirdly, a case study analysis is carried out to further improve the research findings. Lastly, based on the findings from the literature review and the case studies, a set of operational guidelines is proposed.

2. LITERATURE REVIEW
The solutions to address different aspects of 802.11 wireless LANs security fall into two main categories: technical solutions and managerial solutions, which mainly concentrate on the theory and practice of sound security management processes.

2.1 Technical Solutions
2.1.1 Authentication and Encryption
Mishra & Arbaugh (2002) argued that, due to the broadcast nature of wireless LANs, strong access control must be a feature of the security solutions used to protect wireless LANs from various attacks. Mutual authentication should also be implemented because access points are untrusted. Moreover, they emphasized that strong confidentiality should be addressed and dynamic rekeying is needed as an inherent part of the design. Williams (2004) also stated that authentication and encryption are the basic requirements of wireless LANs security.

2.1.2 Detection
Several authors (Karygiannis and Owens 2003; Rittinghouse and Ransome 2004) believe that if organizations require high levels of security, they should implement an Intrusion Detection System (IDS) because it provides an added layer of wireless LANs security. Rittinghouse & Ransome (2004) also pointed out that, network design, projected transactional load, the depth of security policy desired, the real and future costs, implementation, and management overhead are critical factors that should be considered when organizations configure a wireless IDS security product. Other authors (Gast 2004; Solms and Marais 2004; Williams 2004) highlight that organizations need to have a solution in place to combat rogue access points, which is a serious problem with 802.11 wireless LANs.

2.1.3 Additional technical enhancements
Researchers (Wong 2003; Mateti 2004; Rittinghouse and Ransome 2004) have argued that wireless LANs security can be enhanced by using firewalls, antivirus software and application layer security technologies such as Secure Shell (SSH) and Kerberos. They also suggest installing personal firewall and antivirus software on each client.

2.1.4 Segmentation between the Wireless LAN and the Wired LAN
Rittinghouse (2004) pointed out that, in order to reduce the chances of the wired network being attacked via a wireless LAN, organizations need to separate wireless LANs from the wired network using segmentation devices, such as routers, layer 3 switches, VPN concentrators, firewalls, enterprise encryption gateways and enterprise wireless gateways.

2.2 Managerial Solutions
Current research suggests that wireless security is not solely a technical issue. "There is also a human element that must be addressed by appropriate employee awareness of the issues, user education, and a clear statement of acceptable organization policies, procedures, and practices by management" (Pike 2002, p.2). As pointed out by Potter (2004), relying on technology itself can't solve the problems created by wireless security. "Without users, a secure wireless network is simply an expensive atmospheric heater" (Potter 2004, p.5). Therefore, Karygiannis & Owens (2003, p.ES-3) commented, "security management practices and controls are especially critical to maintaining and operating a secure wireless network".

In summary, current research suggested seven categories of management practices for deploying and maintaining a secure wireless LAN. These practices include:

- Control wireless LANs coverage area and reduce RF leaking
- Management of access points, including proper configuration of access points, controlling reset functions, access points inventory and proper placement of access points.
- Establish security policies
- Regularly check patches and upgrades
- Regularly conduct security audits
- Provide user education
- Control physical security regarding wireless network facilities

2.2.1 Control Wireless LANs Coverage Area and Reduce RF Leaking
A number of researchers (Hassick 2002; Maxim and Pollino 2002) argued that, the chances of attacks resulting from the broadcasting nature of the wireless networks can be reduced by controlling the coverage area and reducing RF leakings. These measures can be accomplished by using site surveys, appropriate access point placement and RF containment.

Generally, a site survey involves evaluating the building, including surrounding areas and the obstacles that need to be overcome. Outer and inner wall construction, window treatments and window glass material must all be identified and considered. Access points and roaming wireless clients should also be used to decide the network coverage with optimal performance and security. (Maxim and Pollino 2002). The objective of RF containment is to limit the scope of the wireless networks within the known boundaries. Although coverage control provides certain level of security, it is not an absolute solution. Karygiannis & Owens (2003) argued that attackers still can use high-gain antennas to eavesdrop on the wireless network traffic.

2.2.2 Management of Access Points

Proper Configuration of Access Points

Many authors (Karygiannis and Owens 2003; Wong 2003; Mateti 2004; Rittinghouse and Ransome 2004) suggested that the default settings of an access point should be changed before its deployment. They also described some guidelines on access point configuration:

- Update the default administrator password
- Use the MAC access control list function
- Change the default SSID
- Change the default shared keys
- Establish proper encryption settings
- Change SNMP parameters
- Change default Channels
- Disable DHCP and use static IPs if feasible. If using a static IP is not feasible and offers little value, two solutions can be adopted by organizations. One solution is to implement a DHCP server behind the wired network's firewall, which grants access to a wireless network located outside of the wired network's firewall. Another solution is to use access points with an integrated firewall, moving authentication and access control to the link layer

Rittinghouse & Ransome (2004) suggested using a local serial port interface to configure the access points in order to minimize the exposure of sensitive management. They also suggested enabling a user authentication mechanism for the management interfaces of the access points.

Control the Reset Functions

A reset function may return the access point to its default settings. If an access point is placed in an insecure place and the attacker has gained physical access to the access point, he/she may reset the access point and cancel all the security settings. Therefore several researchers (Karygiannis and Owens 2003; Rittinghouse and Ransome 2004) suggested that the reset functions should be used only when needed and should be only invoked by an authorized group of people.

Access Point Inventory

Williams (2002) suggests that organizations keep the access point infrastructure current by tracking the locations of all access points and recording the configuration of all access points to ensure each access point follows corporate standards and uses the latest software patches and firmware upgrades.

2.2.3 Establish Security Policies

Several authors (Maxim and Pollino 2002; Karygiannis and Owens 2003; Potter 2003; Regan 2003; Rittinghouse and Ransome 2004) made the point that security policies are a critical and essential part of wireless security and they should cover the following areas:

- Issues of wireless devices
- Wireless users configuration and activity
- Link level security
- Network and application level security
- Level of security protection
- Patches upgrade
- Offsite use of wireless devices
- Security audit

2.2.4 Regularly Check Patches and Upgrades

A number of researchers (Karygiannis and Owens 2003; Wong 2003) suggested that network administrators need to check with the vendor the availability of security patches and upgrades regularly, and apply them as needed.

2.2.5 Regularly Conduct Security Audits

Karygiannis & Owens (2003) argued that security audits are essential tools for organizations to check the security of a wireless network and determine corrective action to make sure it remains secure. They argued that the security assessment approach should be holistic and two methods can be adopted by organizations to perform security audits:

- Use wireless network analyzers and other tools, such as ***Netstumbler***, to check whether access points transmit data correctly and operate on the correct channels.
- Conduct third party audits. Organizations providing audit services are usually more up-to-date on security vulnerabilities, better trained on security solutions, and well equipped to assess the security of a wireless LAN.

2.2.6 Provide User Education

Keenan (2004) argued that every organization deploying a wireless LAN needs to develop a serious user training program to assure that users understand they each have a personal responsibility to keep their wireless network safe from intrusion. In addition, the user training should not only let users know about security protocols and how to follow them, but also let them know why these protocols exist. He also stated that, although wireless security protocols are set by the IT department, education and enforcement are best implemented by the Human Resources department. Karygiannis & Owens (2003) held a similar opinion on the importance of training users and making them aware of wireless risks. Moreover, they pointed out that network administrators also need to be fully aware of the security risks associated with wireless LANs. The administrators must work to ensure security policy compliance and to know what steps they need to take if an attack occurs.

2.2.7 Control Physical Security

Karygiannis & Owens (2003) argued that physical security is the most fundamental step to ensure that only authorized users have access to wireless network facilities. Two measures can be adopted by organizations to ensure physical security of the wireless network facilities:

- Conduct physical access control, such as photo identification, card badge readers or biometric devices, to minimize the risk of improper penetration of wireless network facilities.
- Deploy external boundary protection, including locking doors and installing video cameras around the perimeter to discourage unauthorized access to wireless network facilities such as access points.

3. RESEARCH METHOD

Multiple-case design is chosen instead of single-case because the evidence from multiple cases is often considered as "being more compelling and the overall study is therefore regarded as more robust" (Yin 1994, p.45).

Two cases were selected from wireless vendors and three organizational user cases were respectively selected from the education sector and the commercial sector. These cases include:

- ***Vendor A***: a leading wireless infrastructure provider. Its main wireless products include access points, wireless bridges, wireless security servers and intrusion detection systems.
- ***Vendor B***: a leading wireless management system provider. Its main wireless products include wireless gateways and wireless intrusion detection systems.
- ***User C***: a New Zealand secondary school
- ***User D***: an international real estate company
- ***User E***: a New Zealand university

Two data collection techniques are adopted: interviews and documentation. Six face-to-face interviews were conducted with IT directors, network administrators

and security consultants coming from vendors and users. All the interviews were audio-taped. When interviewing the vendors, two main topics were discussed:

- Technical products they provide or security technologies they recommend to protect 802.11 wireless LANs .
- Network management practices they perceive to be the must-use practices for organizations.

When interviewing the users, three main topics were covered:

- Motivation for deploying their wireless LANs
- Perception of the main risks associated with their wireless LANs
- Technical and managerial solutions they have adopted to secure their wireless LANs

4. ANALYSIS OF THE CASE STUDY FINDINGS

This section contains a summary description of the five cases. A detailed description can be found in [eliminated for blind peer-review].

4.1 Technical Solutions

As revealed in the case studies, all the technical solutions compiled from the literature review are either provided by the vendors in their wireless products or adopted by the organizational users. The case study also revealed some findings which were not discussed in the literature.

4.1.1 Finding 1: Evaluation of Technical Solutions

As discovered in the case study, both the vendors and organizational users agree on the following issues which need to be considered to evaluate the technical solutions:

- Network infrastructure and security requirements
- Interoperability of the different technical solutions
- Secure roaming across the subnets
- Administration burden
- Ease of use
- Transparency to the users
- Cost

4.1.2 Finding 2: Current Authentication and Encryption Technologies in the Industry

With regards to the technologies that provide authentication and encryption, the two vendors pointed out that SSID, MAC access control lists and WEP are not sufficient for enterprise-level security, because a MAC address is easy to forge and WEP has many fatal flaws. The two vendors suggested that organizations use 802.1x/EAP+TKIP (or AES) or IPsec VPN to provide strong authentication and encryption. As revealed in the case studies, three users are currently using these two technologies. Moreover, the case studies revealed that 802.1x/EAP+TKIP (or AES) can be used when an organization wants both reasonable assurance of confidentiality and a transparent user security experience, while IPsec can be chosen when organizations have utmost concern for the sensitivity of the transported data.

Furthermore, guidelines are suggested by the wireless vendors for choosing the authentication and encryption technologies. Firstly, it is recommended that the authentication should be user-specific not device-specific. Ideally, strong authentication should be tied to the use of multiple factors of information, including something you know (a password), something you have (a hardware token card, a digital certificate) and something you are (biometrics). Secondly, it is recommended that, when evaluating encryption technologies, organizations need to consider ease of use, administration load, CPU/battery load and support for mobility across subnets.

4.1.3 Finding 3: Current Intrusion Detection Technologies in the Industry

As revealed in the case studies, intrusion detection systems and rogue access point detection are already available in current wireless products. Intrusion detection is built into Vendor B's wireless gateway. Vendor A's access point is also capable of detecting rogue access points. Moreover, current wireless products also provide the capability of detecting unassociated clients, ad-hoc networks and interference. Except the detection functions provided by Vendor A and Vendor B, the three organizational users also rely on a third party product. User C utilizes *AirMagnet*, User D relies on *Snort*, and User E uses *Argus*.

Furthermore, it is identified from the case studies that traditional ways of detecting intrusions which are used in wired networks could also be utilized in the wireless environment. For example, in the case of User D, they rely on some traditional ways, such as monitoring log files, to detect wireless intrusions.

4.1.4 Finding 4: Bandwidth Management

As revealed in the case studies, bandwidth management is suggested by Vendor B as one component of the wireless security solution. This solution is available in Vendor B's wireless gateways, enabling network administrator to assign a maximum bandwidth to each user. Two organizational users, User C and D are also running bandwidth management tools to carry out bandwidth management, such as bandwidth differentiation based on the roles of the users.

4.1.5 Finding 5: Authorization

Authorization is another new component of the solutions, which is discovered in the case studies. As a wireless management system provider, Vendor B points out that organizations need to differentiate access to network resources based on each user's role. Therefore, Vendor B has developed role-based access control to provide the correct level of access for each user.

4.2 Managerial Solutions

The solutions found in the literature review suggest seven management practices for organizations to deploy and maintain a secure wireless LAN. Furthermore, the cases studies indicated that the technical solutions and managerial solutions should not be separated from each other. Technologies can assist in some management practices, such as management of access points and security audits. There are plenty of tools available in the market for assisting in the inventory of access points. For example, Vendor A's wireless management solution offers the functions of displaying the location and configuration of each access point. All the three organizational users also use Vendor A's wireless management solution to control the access point reset function.

5. FORMULATION OF THE GUIDELINES

Based on the information gathered from the literature review and the case studies, a set of operational guidelines are proposed to assist organizations in protecting their 802.11 wireless LANs. The proposed guidelines are divided into two parts: technical and managerial.

5.1 Technical Guidelines

Guideline 1: Choose the technical solutions that are suitable for your network infrastructure and security requirements. When evaluating technical solutions, you need to consider interoperability, administration burden, ease of use, transparency to the users, secure roaming across the subnets and cost.

Guideline 2: Have an authentication and encryption solution in place.

- The authentication solution should be user-based, not device-based. Consider deploying authentication that is tied to multiple factors of information, i.e. something you know (username/password), something you have (digital certificate) and something you are (biometrics). Consider user-friendliness when choosing the authentication solution, for instance, the authentication process needs to avoid multiple user steps.
- When evaluating the encryption solution, consider ease of use, administration burden, CPU battery load and support for mobility across the subnets.
- Recommend two solutions: 802.1x/EAP+TKIP (or AES) and IPsec. 802.1x/EAP can be adopted when you want both reasonable assurance of confidentiality and transparent user security experience. IPsec can be adopted when you have utmost concern for the sensitivity of the transported data.

Guideline 3: Have an intrusion detection solution in place. The solution is at least capable of detecting general network intrusions, rogue access points, unassociated clients, ad-hoc networks and interferences.

Guideline 4: Have a solution in place to manage the bandwidth.
- Bandwidth differentiation based on the roles of the users.
- Monitor bandwidth usage of each user.
- Block unneeded applications, such as video.

Guideline 5: Have a solution in place to enable differentiating users' access to your network resources.

Guideline 6: Have a worm-protection solution in place. Install antivirus software on each wireless client if it is feasible. If not, have a solution in place to detect the virus and prevent the virus-infected client from accessing the wireless LAN.

Guideline 7: Separate your wireless LAN from your wired network by using segmentation devices, such as routers, layer 3 switches, VPN concentrators, firewalls, enterprise encryption gateways and wireless gateways.

5.2 Managerial Guidelines

Guideline 1: Control the coverage of your wireless LAN and reduce the leaking of radio frequencies. For doing this, you can adopt the following three approaches:

Approach 1: Conduct a site survey

Approach 2: Place the access points strategically to reduce the radio frequency leakage and focus the majority of the coverage within the building.

Approach 3: Implement radio frequency containment. This can be achieved by:
- Minimizing the transmission power of the access points.
- Modifying the building by installing metallic film or foil under the drywall, applying metallic paint to walls to add layer of attenuation and using metallic window blinds to provide better attenuation.

Guideline 2: Change the default settings of the access points and configure the access points properly. The followings are some guidelines:
- Disable any insecure and nonessential settings.
- Update the default administrator password. Recommend implementing strong passwords with both alphanumeric and special characters and a minimum password length of eight characters. In addition, passwords should be changed regularly.
- Change default SSID.
- Choose strong community strings for SNMP and change them often. Consider using ***SNMP Read Only*** if the management infrastructure allows it.
- Ensure the access points have at least three channels different from any other nearby wireless networks to prevent interference.
- Utilize secure management protocols, such as SSH for web and SSL for telnet, to configure the access points.
- Limit management traffic to a dedicated wired subnet.
- Isolate management traffic from user traffic and encrypt all management traffic where possible.

Guideline 3: Control the reset function of the access points.
- Make sure that only an authorized group of people can reset the access points.
- Have a solution in place that allows the reset access points to restore themselves to the latest security settings.

Guideline 4: Track the locations of all the access points and record the configuration of all the access points to ensure each access point follows the security standards and uses the latest patches. Recommend using vendor-specific tools to do this.

Guideline 5: Establish security policies regarding wireless security. The security policies need to be expressed in a way that everyone can easily understand. Moreover, the security policies are recommended to address the following issues:
- **Wireless users**: Identify who may use the wireless LAN in the organization and specify the acceptable and unacceptable behavior of the wireless users.
- **Wireless communications**: Identify what type of information may be sent over the wireless network and define the security level of the information.
- **Use of wireless devices**: Specify who is authorized to install wireless equipments, such as the access points, the acceptable and unacceptable offsite use of the corporate wireless devices, and the procedures on reporting losses of the wireless devices and security incidents.
- **Network configuration**: Define standard security configurations of network devices, such as access points. Provide guidelines on the use of encryption and other security technologies.
- **Security management**: Define procedures of network security management, including virus control, password management, security upgrades and security audit.

Guideline 6: Regularly check the security patches and only apply the ***needed*** ones. Make sure that the antivirus software has the latest virus definition.

Guideline 7: Conduct a security audit regularly. You may choose the following two approaches to do this:

Approach 1: Use public tools (such as ***NetStumbler***) or vendor-specific tools (such as ***AirMagnet***) to check if access points are transmitting correctly and are deployed on the correct/authorized channel and to check for rogue access points and other unauthorized access.

Approach 2: Ask professional companies to conduct a security audit of your wireless LAN. Usually these companies provide audit services that are more up-to-date on security vulnerabilities than most organisation's IT departments.

Guideline 8: Provide user training for those who operate and manage your wireless LAN. The training at least covers the following areas:
- Make sure the relevant people understand that they have personal responsibility to keep the wireless LAN safe from intrusion.
- Let the relevant people know about the risks associated with the wireless LAN.
- Let the relevant people know about security protocols, why these protocols exist, and how to follow them.

Guideline 9: Cultivate good communication between your IT staff and end users. Encourage the users to consult IT staff if they are uncertain about some computer or network operations.

Guideline 10: Protect your wireless network facilities physically, especially the access points.
- Conduct physical access controls, such as using security cards, to minimize the risk of improper penetration of wireless network facilities.
- Install access points out of the normal reach of people. If possible, conceal the access points from sight.
- Deploy external boundary protection, including locking doors and installing video cameras around the perimeter to discourage unauthorized access to wireless network facilities, such as access points.

6. CONCLUSIONS AND LIMITATIONS

As revealed in this research, 802.11 wireless LANs security must be achieved by the integration of security technologies and good management practices. On one hand, technologies can secure the wireless LANs only when they meet the organizational security requirements, are applied to an appropriate network environment, and are implemented properly. This is actually associated with an organization's security management practices. On the other hand, technologies can assist in good security management practices. With the help of the adequate technology it is easy to carry out good management practices.

This research has three main limitations. Firstly, the findings are only applicable to 802.11 wireless LANs, not to the other types of wireless networks. Secondly, the findings are only suitable for organizational users, not for home users. Finally, the technical solutions proposed in this research do not consider the issue of network performance, which is also an important factor that organizations need to consider when evaluating the possible technical solutions.

REFERENCES

Arbaugh, W. A. (2003). "Wireless security is different." *Computer* 36(8): 99-101.

Benbasat, I., D. K. Goldstein, et al. (1987). "The case research strategy in studies of Information Systems." *MIS Quarterly* 11(3): 369-385.

Cai, Y. (2005). *How to secure your 802.11 wireless LAN.* MCom Thesis, Department of Information Systems and Operations Management, University of Auckland, Auckland, New Zealand,

Gast, M. (2004). The top seven security problems of 802.11 wireless. Retrieved 9 December, 2004, from http://www.airmagnet.com/bitpipe/assets/AirMagnet.Security.WhitePaper25.pdf.

Hassick, B. (2002). "Simple wireless exposures in traditional networks." *Secure business quarterly* 2(1): 2-5.

Karygiannis, T. and L. Owens (2003). Wireless network security 802.11, Bluetooth and handheld devices. Retrieved 09 Nov, 2004, from http://www.netsys.com/library/papers/draft-sp800-48.pdf.

Keenan, K. (2004). What hackers don't want you to know about your WLAN. Retrieved 9 December, 2004, from http://www.airmagnet.com/bitpipe/assets/WLAN_Hacker_White_Paper.pdf.

Mateti, P. (2004). Hacking techniques in wireless networks. Retrieved 5 January, 2005, from http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524648.

Maxim, M. and D. Pollino (2002). *Wireless security*. Berkeley, Calif. ; London, McGraw-Hill/Osborne.

Mishra, A. and W. Arbaugh (2002). An initial security analysis of the IEEE 802.1X standard. Retrieved 4 February, 2005, from http://www.cs.umd.edu/~waa/pubs/1x.pdf.

O'Halloran, J. (2004). "Fashion sharpens wireless risk." *Network Security* 2004(8): 2.

Pike, J. (2002). *Cisco network security*. Upper Saddle River, N.J. ; London, Prentice Hall PTR.

Potter, B. (2003). "Wireless security policies." *Network Security* 2003(10): 10-12.

Potter, B. (2004). "Fixing wireless security." *Network Security* 2004(6): 4-5.

Regan, K. (2003). "Wireless LAN Security: Things You Should Know about WLAN Security." *Network Security* 2003(1): 7-9.

Rittinghouse, J. W. and J. F. Ransome (2004). *Wireless operational security*. Burlington, MA, Digital Press.

Solms, v. B. and E. Marais (2004). "From secure wired networks to secure wireless networks - what are the extra risks?" *Computers & Security* 23(8): 633-637.

Walsham, G. (1995). "Interpretive case studies in IS research, nature and method." *European Journal of Information Systems* 4(2): 74-81.

Williams, A. (2004). WLAN security best practices. Retrieved 9 December, 2004, from http://www.airmagnet.com/bitpipe/assets/WLAN_Security_Best_Practices.pdf.

Williams, J. (2002). "Providing for wireless LAN security. 2." *IT Professional* 4(6): 48, 44-47.

Wong, J. (2003). Performance investigation of secure 802.11 wireless LANs: raising the security bar to which level? Retrieved 5th August, 2004, from www.cosc.canterbury.ac.nz/research/reports/MastTheses/2003/mast_0301.pdf.

Yin, R. K. (1994). *Case study research : design and methods*. Thousand Oaks, Sage Publications.