Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance

Young B. Choi*

Department of Computer Information Systems and Management Science
James Madison University
800 South Main Street
Harrisonburg, VA 22807-0001, USA
E-mail: choiyb@jmu.edu
*Corresponding author

Jeffrey Muller

Integrated Science and Technology and
School of Media Arts and Design
James Madison University
800 South Main Street
Harrisonburg, VA 22807-0001, USA
E-mail: mullerjx@jmu.edu

Christopher V. Kopek
and Jennifer M. Makarsky

James Madison University
800 South Main Street
Harrisonburg, VA 22807-0001, USA
E-mail: kopekcv@jmu.edu
E-mail: makarsjm@jmu.edu

Abstract: In this paper, we propose the necessary steps in implementing strong WLAN security for companies using our visual security assessment framework for wireless information assurance. Through real case studies on the organisations with various security measures and by showing complete execution paths of our framework, we suggest the importance of continual assessment of the WLAN for strong corporate security assurance using our Corporate WLAN Security Assessment Framework.

Keywords: Wireless Local Area Network (WLAN); corporate wireless LAN; wireless LAN security; security assessment framework; wireless information assurance; Wired Equivalency Privacy (WEP); WiFi Protected Access (WPA); Virtual Private Network (VPN); 802.11b; 802.11i.

Reference to this paper should be made as follows: Choi, Y.B., Muller, J., Kopek, C.V. and Makarsky, J.M. (2006) 'Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance', *Int. J. Mobile Communications*, Vol. 4, No. 3, pp.266–290.

Biographical notes: Dr. Young B. Choi is Assistant Professor of the Information Technology and Management Science Programme at James Madison University in Harrisonburg, Virginia. His current research interests are human factors in telecommunications, wireless telecommunications service management, security management in HIPAA, data mining and visualisation for telecommunications service delivery chain optimisation, and public healthcare. He has a diverse international experience of working in industry, research and academia in telecommunications and computer networking fields since 1978. He received his interdisciplinary PhD degree in Computer Networking and Telecommunications from the University of Missouri-Kansas City in 1995.

Jeffrey Muller is undergraduate scholar at James Madison University. He is double-majoring in Integrated Science and Technology with a concentration on information knowledge management and media arts and design and on digital interactive multimedia. His research interests are in telecommunications security, bioterrorism defense and education using multimedia.

Christopher V. Kopek is undergraduate student at James Madison University and graduated in May 2005 with a BS degree in Computer Science. His research interests are network technologies and database structures.

Jennifer M. Makarsky is a student at James Madison University.

1 Introduction

“Today, end users have an increasing selection of different terminals and devices that support wireless access, as well as support for new technologies like 802.11 based WLANs” (Maunuksela and Nieminen, 2005). Wireless Local Area Network (WLAN) technology is an important method of extending corporate networks, but the new technology brings greater security risks. An understanding of the types of security risks and attacks as well as the developing security standards and how to implement them will enable firms to stay protected.

WLANs have the same risks and vulnerabilities that exist in a conventional wired network and there are also numerous other types of threats specific to them. Some examples of particular WLAN threats are passive attacks, active attacks, loss of confidentiality, loss of integrity and loss of network availability.

As today’s technologies advance, so do the techniques and skills of hackers. New wireless security standards are now being created and released in order to stay one step ahead of hackers. The old Wired Equivalent Privacy (WEP) protocol has been proven to be insecure and does not protect WLANs efficiently. A new 802.11i protocol is being released in 2005 that will protect corporations from WLAN attacks. In conjunction with 802.11i, there are several other security standards that are being used such as WiFi Protected Access (WPA) and Virtual Private Network (VPN). With these new technologies, companies and firms can now have confidence that their WLANs are secure.

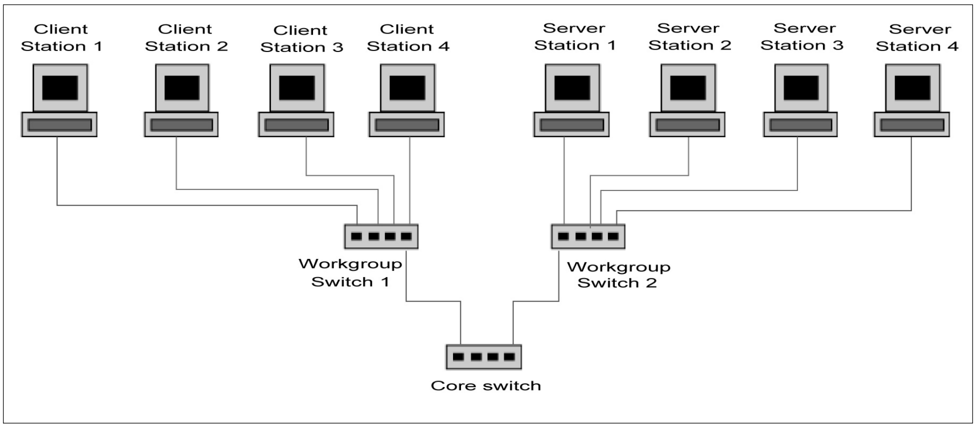
With wireless becoming such a mainstream technology, there is a growing interest in increasing its usage in the enterprise environment (Varshney, 2003). However, all the standards and security techniques under development will be in vain unless they are implemented vigilantly by companies. Companies developing a new wireless network need to design their network carefully, while those with existing wireless networks need to understand how to examine the costs and benefits of upgrading to more secure hardware and software.

The organisation of the paper is as follows. Section 2 introduces wired and wireless LAN architectures. In Sections 3 and 4, various threats and attacks in corporate wireless LAN and corresponding wireless LAN security standards and methods are described. In Section 5, emerging WLAN security technologies are introduced. In Sections 6 and 7, corporate vigilance efforts to protect the companies and continual assessment of WLAN are tackled. In Sections 8 and 9, our own Wireless LAN Security Framework and its applications on some real cases to verify its effectiveness and correctness in security assessment are explained in detail by showing all the possible execution paths of the framework. Finally, Section 10 provides the conclusion.

2 Wired and wireless LAN architectures

A Local Area Network (LAN) is a connection of multiple computers (called within a corporate site). The term 'Wired LAN' refers to the traditional LAN where stations are connected to a switch with a cable and the switch is connected to other stations using the same method. There is typically a switch on every floor of the site (called a 'workgroup switch') and a switch in the basement (called a 'core switch') that connects to all of the workgroup switches. This type of LAN uses the IEEE 802.3 protocol, also called 'Ethernet' and is sometimes referred to as 'Ethernet LANs' or '802.3 LANs'. The network topology for a corporate Ethernet LAN is usually hierarchical. Switches branch off other switches to extend connections to various stations. Using this topology, there is only one possible path between two stations. Figure 1 shows the structure of wired Ethernet LAN.

Figure 1 Structure of Ethernet LAN

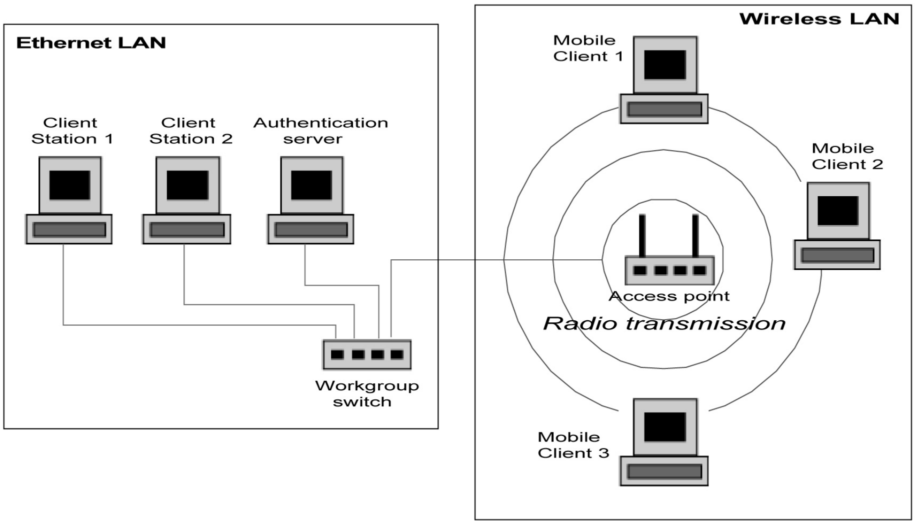


Wireless LAN (WLAN) uses the air to transmit data between stations. It uses access points to connect to the existing Wired LAN and to broadcast to stations with Wireless Network Interface Card (NIC). In contrast to Wired LANs, Wireless LANs use a bus topology where one station broadcasts to all other stations. "Mobile devices in the IEEE

802.11 Wireless Local Area Network (WLAN) have the ability to transmit data frames at one of four transmission rates 1Mb/s, 2Mb/s, 5.5Mb/s and 11Mb/s" (Sheu *et al.*, 2003). Each transmission rate is dependant on which version of 802.11 the system is using.

Wireless LANs are not competing with traditional Ethernet LANs. They are used to extend the existing corporate network to mobile clients. Therefore, if the security is lax on a company's wireless LAN, it compromises the security of the wired LAN. Figure 2 shows how the wireless network connects to the existing wired LAN using an access point.

Figure 2 Wireless LAN extending Ethernet LAN



3 Threats and attacks in corporate wireless LAN

Wireless LANs have the same risks and vulnerabilities that exist in a conventional wired network. There are numerous other types of WLAN threats and attacks that need to be taken into consideration if a WLAN is to be kept free of hackers and crackers. Some of these threats and attacks are passive attacks, active attacks, loss of confidentiality, loss of integrity and loss of network availability.

3.1 Passive attacks

A passive attack occurs when an unauthorised party gains access within the network but does not modify the content. There are two types of passive attacks: *eavesdropping* and *traffic analysis* or monitoring.

Eavesdropping is when an attacker, usually from within the perimeter of the business, monitors transmissions for message content by listening to the transmission between two workstations. Nothing is touched physically, but information and privacy is invaded. On the other hand, traffic analysis is typically performed by an intruder that is outside the perimeter of the business, monitoring the transmissions for patterns of communication, just like a traffic cop. The intruder typically observes and makes assessments about the nature of traffic, amount of traffic and the load on the network, but again, he/she does not physically alter the information.

3.2 Active attacks

An active attack is where an unauthorised party makes changes and alters information to a message or file. These types of attacks can be detected but may not be preventable. Four types of active attacks are *masquerading*, *replay*, *message modification* and *Denial-of-Service* (DoS).

Masquerading is when an attacker impersonates an authorised user and gains access to the network. The authorised user's identity is compromised and the attacker has full access to the authorised user's network information. These attacks can range from very simple to complex based on the security in effect. When an attacker monitors transactions then retransmits the information as the authorised user, replay has occurred. The attack starts off as a passive attack, but it eventually becomes an active attack when the attacker replies to the transmission. Meanwhile, message modification occurs when the attacker modifies a message by deleting, adding, changing or reordering the message. Any tampering of the message would be considered message modification. A Denial-of-Service (DoS) attack, on the other hand, is an assault that can cripple or disable a WLAN. It occurs when an attacker prevents or prohibits use of the network. The attacker blocks the service or transmission and can slow the network to crawling speeds or actually force it to quit working. There are multiple DoS attacks, one of which is the 'brute force' method. This can come in one of two forms: either a huge flood of packets that uses up all of the network's resources and forces it to shut down, or a very strong radio signal that totally dominates the airwaves and makes access points and radio cards useless.

3.3 Loss of confidentiality

Confidentiality is a major concern when dealing with any network. An organisation does not want its company's private information and investments open to competitors. With WLANs, an attacker does not need to tap into a network cable to access the network; they can go through radio and broadcast waves which make traditional security for LANs less effective. Passive attacks assault confidentiality just by listening to the transmissions; and due to the extended range of WLANs, attackers can listen to transmissions outside of the organisation without the users knowing it. If the user has a hub, the chance of being attacked increases as hubs broadcast to the entire network and leaves traffic vulnerable.

3.4 Loss of integrity

In connection with loss of confidentiality, losses of integrity in WLANs are the same as those in LANs. Unfortunately, most companies do not have adequate protection, thus, integrity is difficult to achieve. If an attacker message modifies data, data integrity is lost through the alterations of the attacker. This can be devastating to an organisation if important information is lost or modified.

3.5 Loss of network ability

Loss of network ability goes along the same line as DoS attacks, since loss of network is usually a result of a DoS attack like 'jamming'. Jamming occurs when an attacker creates a signal that blocks the wireless signals, causing the entire network to be jammed – no information can go in or come out and users are unable to communicate on the network. A user can inadvertently cause a jam by downloading a large file, thus causing everyone else on the network to be without access. Table 1 shows a summary of the types of attacks and risks in corporate WLANs.

Table 1 Summary of types of attacks and risks in corporate wireless LAN

Attack type	*Description*
Passive attacks	Access to WLAN, but no modification to content
	Eavesdropping – attacker monitors transmissions for message content
	Traffic analysis or monitoring – intruder monitors the transmissions for patterns of communication
	The risk of passive attacks
	Loss of confidentiality – attacker listens to transmissions and compromises private information
Active attacks	Makes changes and alters information to a message or file
	Masquerading – attacker impersonates an authorised user and gains access to the network
	Message modification – attacker modifies a message by deleting, adding, changing or reordering the message
	A Denial-of-Service (DoS) – attacker prevents or prohibits use of the network
	Jamming – attacker creates a signal that blocks the wireless signals and causes the entire network to be jammed with no information going in or coming out
	The risks of active attacks
	Loss of integrity – attacker modifies data to the point where data integrity is lost
	Loss of network ability – network is no longer available to users because of attacks

4 Wireless LAN security standards and methods

> "Security remains one of the biggest challenges in wireless enterprise. Many incidents (such as 250,000 devices in airports, most of which carried sensitive corporate data without even password protection), perceived and real wireless infrastructure attacks, and the lack of strong security in wireless technologies could adversely affect the wireless enterprise." (Varshney *et al.*, 2004)

Currently, there are several security standards that are being used in wireless networks to help combat this security problem. These standards include: 802.11b, 802.11i, Wi-Fi Protected Access (WPA) and Virtual Private Network (VPN). Each of these standards has different levels and methods of protection, and this section describes the features of each.

4.1 802.11b

Security threats and attacks have compromised WLANs for the past several years. However, new emerging technologies allow WLANs to be secure and protected from most attacks. One recent step toward reducing WLAN attacks and threats is the security added to the 802.11b standard. The 802.11b uses the Wired Equivalent Privacy (WEP) protocol. WEP was designed to ensure both encryption and ease of use among wireless users. WEP encrypts the network packet with an encryption key. The encrypted packet is then sent to its destination and the destination must decrypt the packet to retrieve its contents. In theory, this sounds like a perfect way to encrypt packets and keep hackers from seeing the data, because no person or device knows the encryption key except the source and the destination. However, there is one inherent flaw in WEP that compromises its real security to any true hacker. With each packet, the WEP protocol sends a portion of the key in plain text, which hackers can use with a software to steal the encryption key and see the contents of the packets. The best and only way to ensure protection using the WEP protocol is to frequently change the key so that hackers cannot collect data on packets long enough to crack the key. Since WEP has widely known weaknesses, most major companies and firms have not implemented or have even abandoned the 802.11b wireless LAN. Another major problem with the 802.11b standard is that the WEP protection can be turned off. Most firms and companies know about WEP and they make sure they have it turned on. However, many home users are not educated enough to realise its benefits, leaving the WEP turned off. Since WEP is not even used by most home users, and firms have abandoned it for its lack of security features, the 802.11b wireless security is a failure. Nonetheless, even though security in the 802.11b protocol is basically a failed method, it has started a wireless security revolution and has helped advance more current and future security methods. Table 2 describes a time line of the 802.11b WEP security standard.

Table 2 802.11b WEP security timeline

Date	*Event*
1st half, 2000	802.11b and WEP introduced.
2nd half, 2000	No one turns on WEP protection for their wireless network.
1st quarter, 2001	WEP flaws are discovered.
2nd quarter, 2001	More WEP flaws are discovered.
3rd quarter, 2001	Terrorist attacks cause fear.
1st quarter, 2002	Mainstream press decides to brand WLAN security as a hot story.

4.2 802.11i

With the failure of 802.11b WEP security, one of the newest technologies was developed – the 802.11i, which adds protection using more secure keys and encryption. On June 24, 2004, the IEEE approved 802.11i security standard for use in WLANs (Dulaney *et al.*, 2004). However, even though 802.11i has been approved for use, it has not been released to the public yet. Hardware and software are currently being made and released to the public in anticipation of its release.

The 802.11i standard uses one of two different security protocols: the 'Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)' and the 'Temporary Key Integrity Protocol (TKIP)'. CCMP is the main method used for protecting wireless packets in the 802.11i standard. One great feature is that CCMP always has to be active, and this means protection will always be enabled even if the user does not know how to operate it or how it works. The CCMP uses a variation of the Advanced Encryption Standard (AES) encryption algorithm, which is a very secure and nearly impenetrable method. Protection begins by using a 128-bit key, and the packet is encrypted with this key. Not only is the message data encrypted, but the source, destination and other data are encrypted as well. Since all this data is encrypted, a hacker cannot spoof a packet because he/she does not even know where to send the packet. Another important feature of CCMP is that a key does not need to be included in the packet. One fallback of WEP is that a portion of the key is included in the packet. This resulted in more packets being sent than were needed; and with each extra packet, a hacker has a higher chance of cracking the key. With CCMP, 802.11i is secure against all known hacking attacks and will insure near flawless security protection. The only problem with CCMP is that it uses all new technology, which means that new hardware and software will have to be created and purchased for this method to work. Nonetheless, it is a necessary step to ensure security protection in wireless networks.

The other encryption method used with the 802.11i protocol is TKIP, and it is beneficial because it was designed as a wrapper around the old WEP protocol. Compared with CCMP protocol where it is necessary to buy new hardware, old hardware and software that use WEP can be reused to comply with TKIP. The TKIP works similar to CCMP, except that it uses two more keys to encrypt the data and headers of the packet, and it includes the keys in the packet. Each packet is initially encrypted with a changing 64-bit encryption key, and then the packet is sent through a process and is encrypted by another 64-bit intermediate key. These keys encrypt the header and data of each packet, and since these keys change with every packet, it is necessary to add these keys to the packet. Finally, the final 128-bit encryption key is used to encrypt the entire packet including the 64-bit keys. The entire TKIP encryption method works just as well as the CCMP, and both of these methods are part of the 802.11i standard.

4.3 Wi-Fi Protected Access (WPA)

Since 802.11i requires new hardware and software, there is going to be a long crossover period where firms need to buy equipment to support the new technology. WPA was developed by the Wi-Fi Alliance as an interim technology to support wireless security until 802.11i is released. WPA is not a protocol like 802.11i, TKIP or CCMP. "[It] is a specification of standards-based, interoperable security enhancements, which strongly increase the level of data protection (encryption) and access control (authentication) for existing and future Wi-Fi wireless LAN systems" (Grimm, 2003). This specification was released in 2003 and is in use today. The WPA specification uses TKIP (like the 802.11i) to ensure data encryption, and it uses Extensible Authentication Protocol (EAP) to ensure user authentication. EAP consists of three parts: the user, the access point and the authentication server. In order for the user to access the network, he/she must first authenticate himself/herself. Once the user has entered his/her authentication data, that data will be transmitted to the access point. The access point in return transmits the data to the authentication server; if that data is valid or invalid, the authentication server will accept or deny the user trying to access the system. Table 3 shows the steps of EAP connection.

Table 3 EAP authentication in Wi-Fi Protocol Access (WPA)

Step	*Process*
1	Client associates their computer with the local access point.
2	Access point blocks all user requests to access LAN.
3	User then authenticates an EAP server via a digital certificate.
4	EAP server authenticates user via a digital certificate.
5	Once both user and server are authenticated, they derive a unicast WEP key.
6	EAP server delivers unicast WEP key to the access point.
7	Access point delivers broadcast WEP key, encrypted with the unicast WEP key, to the client.
8	Client and access point activate WEP key and use unicast and broadcast WEP keys for transmission.

There are also various EAP Authentication Protocols, which include:

- Lightweight Extensible Authentication Protocol (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Tunneled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

Due to the security weaknesses that exist in EAP, several companies formed to create a stronger and more secure variation. Cisco Systems, RSA Security and Microsoft developed the standard known as PEAP (Protected Extensible Authentication Protocol). PEAP uses Transaction Layer Security, which is a proven security method, to wrap EAP. PEAP has been a successful protocol; but since the IEEE takes long periods of time to approve a new protocol, some companies decided to create their own so they could immediately implement it. Cisco decided to create the Lightweight Extensible Authentication Protocol (LEAP) and Microsoft proceeded to create EAP-TLS. The two protocols are basically the same except for one major difference: LEAP uses passwords to ensure device authentication, while EAP-TLS uses digital certificates (Pescatore *et al.*, 2002). The next version of EAP, called Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS), was created to ensure better flexibility and integration with servers. EAP-TTLS adds an extra layer of security by ensuring protection before the exchange of keys begins (Girard *et al.*, 2003). The final type of EAP is Extensible Authentication Protocol-Subscriber Identity Module (EAP-SIM). This method enables the user to gain access to the wireless network by using a SIM card to be authenticated through EAP. The card contains the key and/or passwords, granting access to the user once the card has been entered. Overall, each variation of EAP has its benefits; however, the only newly approved standard is PEAP. It is likely that in the near future, each company will have to either convert to PEAP or enable their variation of EAP to work with other variations.

WPA was intended for short intermediate use. However, the 802.11i release was delayed so a newer intermediate security method, called WPA2, is being released. The next edition of WPA is identical to the old version in every way, except that it uses AES encryption to ensure protection for firms where encryption is a must. Overall, WPA/WPA2 is a temporary yet very secure solution for individuals and companies who cannot wait for the release of 802.11i and need immediate security.

4.4 Virtual Private Networks (VPN)

"A Virtual Private Network is a private network that uses a public network to connect remote users or sites together" (Tyson, 2001). VPNs, having extra security features, were created to make a way for users to connect to a network. There are four parts that make a VPN secure: "Firewalls, Encryption, IPSec, and AAA Server" (Tyson, 2001).

A VPN firewall is the same as any other firewall – it is setup to block and allow only certain ports, and it is also designed to allow only packets which it does not think are malicious. This may sound trivial, but a firewall is a necessary entity in the VPN so that viruses and Trojan horses cannot compromise the VPN server.

There is no specific encryption technique that is required in a VPN; however, three main techniques are used. The first technique is Symmetric Key Encryption, where each computer on the network has the key, enabling them to decrypt the packet when it arrives. An identical symmetric key is used on each computer, which means that the key needs to be changed frequently so hackers will not be able to analyse packets and break into the network. The next method is Public Key Encryption, which uses a public key and a private key. The sender encrypts the packet with their private key (which they only know), and the receiver decrypts the packet with the sender's public key. This system is similar to the Symmetric key, except that two different keys are used instead of only one. In order for this method to work, each user must have some way to securely get the public key from each sender. The last way to encrypt is with Pretty Good Privacy (PGP), which uses session keys to ensure protection. A new session key is created for one session per user, and with each new session or new user, a different session key is produced. The PGP system then becomes a public key system as it encrypts the packet and the session key to the user's public key. These new encrypted packets and keys are sent to the receiver, who in turn uses his/her private key in decryption. These are the three widely used techniques; but because there is no encryption standard in VPN, any other type of encryption can be used or adopted to fit a VPN system.

Internet Protocol Security Protocol (IPSec) is another secure method used in VPNs to ensure privacy protection. IPSec is a simple system using two techniques to encrypt messages across the network. The first method is *tunnel*, which means that the entire packet is encrypted with a key, including the header. The second method is *transport*, which only encrypts the data section of the packet and not the header. Both of these methods require that the user and the access point have the same key so that the message can be decrypted when it arrives. The final security method in a VPN is an Authenticating, Authorising and Accounting (AAA) server. When a user requests a session, the request is forwarded to a proxy server and that server determines who the user is, what the user is allowed to do, and what the user is actually doing (Tyson, 2001). This system has extra security because it monitors what the user is doing. By monitoring activity, the system has the ability to predict if an attack is about to happen based on certain user's habits. Overall, a VPN is not as secure as the soon to-be-released 802.11i, but it allows a firm to be more flexible and secure until 802.11i is released. Table 4 shows a summary of security protocols for wireless LANs.

Table 4 Major security protocols for wireless LANs

Protocol	*Description*
WEP	Oldest security method, extremely weak and easy for hackers to crack
802.11i	Strongest security possible, approved by IEEE, but not yet released to the public
WPA/WPA2	Stop-gap Wi-Fi Alliance specification that uses elements of 802.11i, strong encryption and authentication
VPN	Technology developed for WAN and Wired LAN, not as secure as 802.11i, but features different possible encryption techniques

5 Emerging technologies

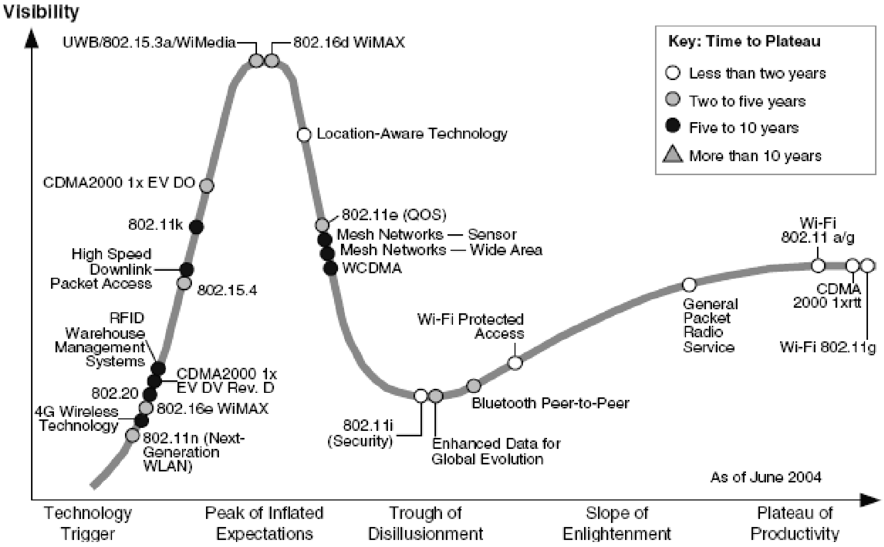
The newest technology that is being produced is the 802.11n protocol. The protocol is still in its early developmental stages; however, it is going to be a great advance as 802.11n will increase the bandwidth used in today's wireless networks. Currently, there is a limit on bandwidth depending on which protocol the firms are using, and this restricts the amount of flexibility a firm can have with the wireless network. An official speed specification on 802.11n is not yet available, but the goal is to have it reach speeds of up to 500 Mbps. According to the WiFi Alliance, "802.11n offers at least four times, and perhaps eight times, the user data rate of any current available IEEE 802.11 product" (Hanley, 2004). A data rate speed of four times the current rate would leave 802.11n at a speed of more than 200 Mbps, and this is a substantial speed increase. Another good feature of 802.11n is that it will be backwards compatible with 802.11g and 802.11b. This means that users do not need to buy new equipment or software to support the protocol. No word is released as to 802.11n's security features; however, if 802.11n does not implement the 802.11i security, this protocol will probably be used only as a stepping stone into another faster and more secure protocol.

Another technology that is being developed and tested is Voice over IP (VoIP) in WLANs. Many companies have decided to do research in VoIP for their WLAN because they want more control over the telephone network. By using VoIP, they can control where the coverage is, who gets that coverage as well as the security features. Not only does VoIP add more control but it also reduces costs. The estimated cost for a cellular call is $0.14, whereas the cost for a VoIP call is approximately $0.015 (Redmond, 2004). Even with all these advantages, VoIP has yet to take off because of quality issues. The data network was designed for the bursting of data; however, voice is continuous and this causes large problems for the network. The continuity of voice travelling through the network results in the loss of some voice, and/or it makes the voice sound extremely choppy. This problem was mainly resolved by the IEEE when they formed the 802.11e standard. 802.11e adds the Hybrid Coordination Function (HCD) and the Enhanced Distributed Coordination Function (EDCF) to the Media Access Control (MAC) layer. These two additions fixed the VoIP problem by reducing the delay of the voice over the network. Still, there are few other problems such as roaming, handoff, and security that also pose a threat to the use of VoIP in WLANs. These issues are currently being addressed by the IEEE in their 802.11e standard. The 802.11e standard is scheduled to be released in two to five years. Once this standard is released, it should provide enormous savings, increased flexibility and great control to the corporations who implement it (Redmond, 2004).

Worldwide Interoperability for Microwave Access (WiMAX) is a new, highly hyped developing technology. WiMAX is highly known because through the media, it claims that it will eventually achieve 70-Mbps mobility and 50 km range. According to Simpson and Keene (2004), "despite the hype, WiMAX will never deliver 70-Mbps mobility and 50 km range at the same time, and considerable challenges are ahead in developing a mobile version". WiMAX may not achieve those specifications but it is being developed to reach them. Currently, WiMAX can only be used as a Wi-Fi hot spot backhaul because it has not been fully developed and the necessary infrastructure features have not been built. However, by 2009, WiMAX plans to be fully operational by having a large array of products that support it. Currently, IBM is developing mobile WiMAX chipsets that will complement its Centrino technology.

Overall, WiMAX is an alternative solution to Wi-Fi, but it is predicted that WiMAX will not take over the latter; instead, they will compliment each other. There are many other developing technologies that are planned for release, and Figure 3 shows the hype cycle of developing WLAN technologies in the near future.

Figure 3 WLAN hype cycle



Source: Redmond *et al.* (2004)

6 Corporate vigilance

All the standards, hardware and software under development will be in vain unless they are implemented vigilantly by companies. Developing strong wireless security is an active process. First, companies need to have the right attitude about wireless security. There are typical false assumptions that many companies make, leading to poor wireless security. Next, companies need to plan their wireless network security methods, while those developing a new wireless network need to design carefully. Also, companies with existing wireless networks need to understand how to examine the costs and benefits of upgrading to a more secure hardware and security mechanisms. The last step is the ongoing process of assessment of the WLAN.

6.1 Corporate attitude

The first step to implementing strong wireless security is having the right attitude. According to Gartner Group (Girard, 2004), many organisations and corporations have false assumptions such as:

- They have no unauthorised remote access.
- They have control of their wireless LANs.
- They do not have to worry because their information is not worth stealing.

'War-dialing' is typically overlooked by companies, but is a surprisingly common method for unauthorised access to a corporate wireless network. The term traditionally refers to "dialing many phone numbers looking for computers to access", while wireless networks can also mean "scanning for various access points" (Klaus, 2002). This method, although old-fashioned, is "easy for users to set up and hard for IT managers to discover" (Girard, 2004). Companies can use the very same 'war-dialing' method to detect unauthorised access.

Companies assume that all of the access points in the site are legitimate access points they have set up. However, according to Gartner (Girard, 2004), many companies are discovering rogue access points (access points that have been set up but are not part of the company's wireless network). They are a huge security risk because they expose the corporate network and neutralise any security that the company implements. They are usually set up by employees for convenience without the intention of harming the network, but in some cases, they are maliciously set up.

Many small companies and charitable organisations believe that since they do not 'have any information worth stealing' they have minimal risks of attack. This is a dangerous misconception, because even seemingly unimportant information can severely damage the company. For example, the hacker can steal information from an employee database and commit identity fraud. Also, hackers break into the network for more reasons than stealing. They can also use the corporate network to launch an attack on another party. The bottom line is that "no one in the enterprise is too unimportant to follow security best practices" (Girard, 2004).

6.2 Risk analysis

A typically overlooked step for companies developing a new corporate WLAN is risk analysis (von Solms and Marais, 2004). Since wireless networks are cheap and easy to set up, many companies are rushing to set them up around their sites. Once the company has developed the proper attitude (*i.e.*, that security is a necessary component of a WLAN), they can perform an in-depth risk analysis to determine whether a WLAN is necessary. They should also determine whether they have the time and budget to invest in strong security. If they have not, the numerous risks of an insecure wireless network outweigh the benefits.

6.3 Initiating a Wireless Network Security Policy

Every company, even if they choose not to install a WLAN, needs to draft a Wireless Network Security Policy. This can be incorporated into the existing Network Security Policy or it can stand on its own as a separate policy. All employees must be notified of the policy and measures that need to be observed in order to strictly enforce them.

If the company does not install a wireless network, they need to state in their Network Security Policy that the installation of any type of wireless network in the company is prohibited (von Solms and Marais, 2004). This will hold employees accountable if they set up an insecure personal wireless network.

On the other hand, if the company has an existing WLAN or is developing a new one, their Wireless Network Security Policy must prohibit the use of unauthorised access points and ad hoc peer-to-peer networks. It should also "supply a procedure which must be followed in applying and getting approval for the installation of any access point or peer-to-peer network" (von Solms and Marais, 2004). Below are additional regulations to be observed:

- [Company] access points are only operational during specific hours (*e.g.*, office hours).
- The workstations and laptops, which may get access to a specific access point, must be preregistered at the access point (MAC addresses).
- The installation of any wireless access point must be based on a proper risk analysis performed for that specific installation.
- All installed access points, wireless cards and operating systems must be configured according to set company security standards.
- The installation of any wireless equipment can be done only by the company's IT Department (von Solms and Marais, 2004).

6.4 Designing the WLAN

Once the company has outlined their Wireless Network Security Policy, they need to carefully plan their wireless network. If they already have an existing wireless LAN, they need to reevaluate it and make changes where necessary. Careful planning is essential to strong wireless network security.

"A poorly designed lawn sprinkler system suffers from 'overspray' — that is, it drenches the sidewalk and street. By rearranging the sprinklers and adjusting the water pressure, water spillage can be reduced" (Girard, 2003). This same theory should be applied to the placement of wireless access points to prevent 'overspraying' of wireless signals. By default, access points transmit in a circular pattern, but buildings are typically shaped in rectangular patterns. Therefore, before installing access points, a site survey needs to be conducted to precisely determine the shape of the building. The company can then estimate how much overspray will occur when setting up access points at certain locations. Gartner Group suggests only purchasing access points whose signal strength can be adjusted programmatically to further increase the precision of wireless signal emission (Girard, 2003).

6.5 Implementing wireless LAN security technology

Once the wireless network has been physically set up, the company needs to implement wireless security standards. They should use the most current security techniques that are feasible depending on their hardware. Typically, companies with older WLANs will not be able to use security techniques as strongly as companies with newly set up WLANs, but they can make decisions to increase their current security.

Many small companies do not use any security at all. In this case, they should at least turn on WEP. This protocol is available on all WLANs and is very easy to implement. However, it offers very weak security and at best will 'keep honest people honest' (Reynolds *et al.*, 2003).

If the company has doubts on security and the use of WEP, they should upgrade to WPA. Although this method is more involved than simply turning on WEP, it is usually feasible since many older WEP products can be upgraded to WPA. Companies should make sure to configure access points so as to "disable legacy WEP security because the access points may still accept WEP client connections" (Reynolds *et al.*, 2003). They also need to make sure that they have a server on the wired network for EAP authentication. However, not all types of EAP can defend against the same types of attacks. All forms of EAP can protect against MITM (Man-in-the-Middle) active attacks, authentication forging, passive attacks, rogue access points and brute-force dictionary attacks (but Cisco LEAP with TKIP is vulnerable to a brute-force dictionary attack).

If the company is setting up a new wireless network, they should purchase hardware that complies fully with the 802.11i standard (Dulaney *et al.*, 2004). This will allow the company to implement WPA (for the time being) and also 802.11i when it is released. Since the standard has been approved by IEEE in June 2004, companies can be assured that it is legitimate. There are, however, hardware vendor interoperability problems that make it harder for companies with existing wireless networks to upgrade. Most likely, this will not affect companies developing a new wireless network unless they have a definite need to use multiple hardware vendors.

Another approach for companies in any of the previous cases is the use of VPN for WLAN security. VPN provides much stronger security than WEP, and it is comparable to WPA. If the company already uses VPN on the wired network, they already have the necessary components to set it up for the WLAN. VPN could be a more feasible option than WPA because companies do not have to set up new components such as a Redundant Array of Inexpensive Disks (RAID) server on their wired network. On the other hand, companies that do not currently use VPN on their wired network could set it up for security on their wireless network. By using VPN, they can also enhance their wired network security.

The problem is that VPN is still not as secure as 802.11i. Using VPN as opposed to WPA will make the transition to 802.11i much more difficult since WPA uses some of the features of 802.11i, while VPN is an entirely different technology. If the full 802.11i is not feasible for companies, they should use VPN instead and if companies plan to implement the full 802.11i when it is released, they should use WPA.

6.6 Monitoring the WLAN

A major concern in monitoring the wireless LAN is the detection and prevention of rogue access points. The traditionally recommended detection method involves walking "through the facilities with sniffing tools, such as AirMagnet or AiroPeek" (Geier, 2002). Cornell University and Microsoft researchers proposed an "architecture for detecting and diagnosing faults in IEEE 802.11 infrastructure wireless networks" that can also be used for rogue access point detection (Adya *et al.*, 2004). It involves a novel technique called 'Client Conduit' that uses the following:

- Diagnostic Client module (DC) – runs on clients to monitor radio frequency environment and transmits information to other two components
- Diagnostic Access Point module (DAP) – runs on access points to receive messages from DCs and combines them with the information it collects then sends it to the last component, DS
- Diagnostic Server module (DS) – receives data from DCs and DAPs and analyses it to detect and diagnose faults. The DS has access to a database that stores each access point's location.

This method provides a low cost and a steady way of detecting rogue access points. When data about access points is sent from the DCs and DAPs to the DS, the latter checks if the access point is registered in the database. If not, it is considered a rogue access point. Figure 4 shows a pseudo-code representation of the software process taken to determine if there is a rogue access point.

Figure 4 Rogue access point detection using the ‘Client Conduit’ method

```
Start:
Boolean isRogue;
/* the access point is not a rogue point if the MAC address is registered, if the access point is
in the expected location, if the access point is advertising the expected SSID, and the access
point is on the expected channel */
IF MAC is registered THEN
{
        IF AP is in expected location THEN
        {
                IF AP is advertising expected SSID THEN
                {
                        IF AP is on expected channel THEN
                                isRogue is false;
                        Else
                                isRogue is true;
                }
                Else
                        isRogue is true;
         }
         Else
                isRogue is true;
}
Else
        isRogue is true;
End.
```

Source: Adya *et al.* (2004)

7 Continual assessment of WLAN

The last recommendation in developing a strong WLAN is that the process should continue even after the security methods are implemented. Continual assessment of the WLAN is necessary for the success of the security. Even if a company takes great efforts in implementing wireless security, it can fail if this security is not consistently monitored after its creation. Jim Geier of Wi-Fi Planet recommends a ten-step WLAN assessment plan that will ensure continued WLAN security and includes many of the methods described for initialising wireless LAN security (Geier, 2002):

1 Review existing security policies.

2 Review the system architecture and configurations.

3 Review operational support tools and procedures.

4 Interview users to see if they know the Wireless Network Security Policy and are following it.

5 Verify configurations of wireless devices.

6 Investigate physical installations of access points.

7 Identify rogue access points.

8 Perform penetration tests.

9 Analyse security gaps.

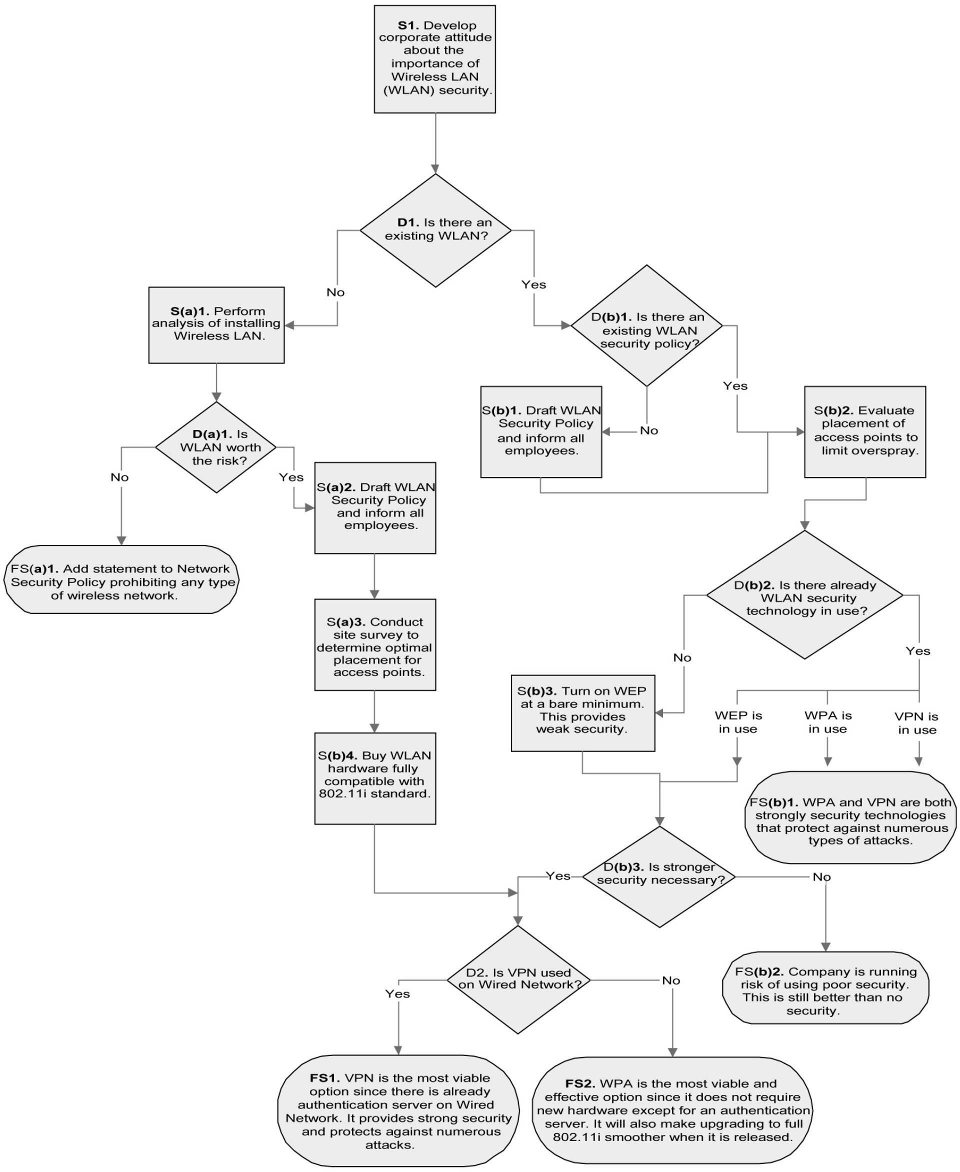
10 Recommend improvements.

8 Wireless LAN security assessment framework

Figure 5 summarises our complete analysis result, showing all the steps to implementing strong wireless LAN security and providing companies with a visual security assessment framework. The rectangles represent Steps (S) the company must undertake and the diamonds represent Decisions (D). Meanwhile, the circles represent Final Suggestions (FS) and the box represents ongoing security measures. The diagram splits into two sections, which are based on whether the company has an existing WLAN: Section (a) is the path a company follows if they do not have an existing WLAN and Section (b) is the path the company follows if they already have an existing WLAN. The paths merge after S(a)4 and D(b)3.

Table 5 shows all of the possible execution paths for the security assessment framework.

Figure 5 Corporate wireless LAN security assessment framework


S1. Develop corporate attitude about the importance of Wireless LAN (WLAN) security.
D1. Is there an existing WLAN?
No
Yes
S(a)1. Perform analysis of installing Wireless LAN.
D(b)1. Is there an existing WLAN security policy?
Yes
No
S(b)1. Draft WLAN Security Policy and inform all employees.
S(b)2. Evaluate placement of access points to limit overspray.
D(a)1. Is WLAN worth the risk?
No
Yes
S(a)2. Draft WLAN Security Policy and inform all employees.
FS(a)1. Add statement to Network Security Policy prohibiting any type of wireless network.
D(b)2. Is there already WLAN security technology in use?
No
Yes
S(a)3. Conduct site survey to determine optimal placement for access points.
S(b)3. Turn on WEP at a bare minimum. This provides weak security.
WEP is in use
WPA is in use
VPN is in use
S(b)4. Buy WLAN hardware fully compatible with 802.11i standard.
FS(b)1. WPA and VPN are both strongly security technologies that protect against numerous types of attacks.
D(b)3. Is stronger security necessary?
Yes
No
D2. Is VPN used on Wired Network?
Yes
No
FS(b)2. Company is running risk of using poor security. This is still better than no security.
FS1. VPN is the most viable option since there is already authentication server on Wired Network. It provides strong security and protects against numerous attacks.
FS2. WPA is the most viable and effective option since it does not require new hardware except for an authentication server. It will also make upgrading to full 802.11i smoother when it is released.

Continually monitor the wireless network, especially looking for 'rogue' access points (access points that are not part of the official WLAN). AirMagnet or AiroPeek are useful for this. There is also a technique called 'Client Conduit' that is being developed for diagnosing WLAN faults, but can also be used to continually look for 'rogue' access points.

Continually assess WLAN security. Review existing policies and interview users to see if they know what they are. Performing penetration tests is also important for finding security gaps. Improvements should be recommended during each assessment.

Table 5 Corporate WLAN security assessment framework execution paths

Chain of Steps (S) and Decisions (D)	*Final suggestion*
Case Set 1: No existing WLAN	
[S(a)1]Risk analysis →[D(a)1]Not worth risk	[FS(a)1] Add statement to network security policy prohibiting any type of wireless network.
[S(a)1]Risk analysis →[D(a)1]Worth risk→ [S(a)2]WLAN security policy→[S(a)3]Site survey→[S(a)4]802.11i hardware→[D2]VPN is on wired LAN	[FS1] VPN is suggested. It provides strong security and protects against numerous attacks.
[S(a)1]Risk analysis→[D(a)1]Worth risk→ [S(a)2]WLAN security policy→[S(a)3]Site survey→[S(a)4]802.11i hardware→[D2]VPN not on wired LAN	[FS2] WPA is suggested. It does not require new hardware except for authentication server. It will make upgrading to 802.11i smoother when released.
Case Set 2: Existing WLAN, no existing WLAN security policy	
[S(b)1]Draft WLAN security policy→ [S(b)2]Evaluate access point placement→ [D(b)2]WPA or VPN in use	[FS(b)1] WPA and VPN are both strong security technologies that protect against numerous types of attacks.
[S(b)1]Draft WLAN security policy→ [S(b)2]Evaluate access point placement→ [D(b)2]WEP in use→[D(b)3]Stronger security not necessary	[FS(b)2] Company is running risk of using poor security. This is sill better than no security.
[S(b)1]Draft WLAN security policy→[S(b)2]Evaluate access point placement→ [D(b)2]WEP in use→[D(b)3]Stronger security is necessary→[D2]VPN is on wired LAN	[FS1] VPN is suggested. It provides strong security and protects against numerous attacks.
[S(b)1]Draft WLAN security policy→ [S(b)2]Evaluate access point placement→ [D(b)2]WEP in use→[D(b)3]Stronger security is necessary→[D2]VPN not on wired LAN	[FS2] WPA is suggested. It does not require new hardware except for authentication server. It will make upgrading to 802.11i smoother when released.
Case Set 3: Existing WLAN and existing WLAN security policy	
[S(b)2]Evaluate access point placement→ [D(b)2]WPA or VPN in use	[FS(b)1] WPA and VPN are both strong security technologies that protect against numerous types of attacks.
[S(b)2]Evaluate access point placement→ [D(b)2]WEP in use→[D(b)3]Stronger security not necessary	[FS(b)2] Company is running risk of using poor security. This is sill better than no security.
[S(b)2]Evaluate access point placement→ [D(b)2]WEP in use→[D(b)3]Stronger security is necessary→[D2]VPN is on wired LAN	[FS1] VPN is suggested. It provides strong security and protects against numerous attacks.
[S(b)2]Evaluate access point placement→ [D(b)2]WEP in use→[D(b)3]Stronger security is necessary→[D2]VPN not on wired LAN	[FS2] WPA is suggested. It does not require new hardware except for authentication server. It will make upgrading to 802.11i smoother when released.

9 Case studies

9.1 Palo Alto School District: dangerously weak WLAN security makes sensitive files available to anyone

The Palo Alto School District (PAUSD) set up their wireless network in the same haphazard manner that many companies do. From the beginning, they did not develop the proper attitude about wireless security, as advised in Step 1 (S1) of the decision framework. Furthermore, they did not analyse the risks associated with installing a WLAN (S(a)1), nor did they develop any type of WLAN Security Policy (S(a)2).

"Andrew Hannah, a Network Administrator for the district, admitted security was an afterthought when the first open wireless networks were installed…" (Metz, 2003). He also commented that "the district was more interested in equipment issues than [in] securing information" (Metz, 2003). This lax WLAN security policy led to a security breach where a local newspaper, *Palo Alto Weekly*, was able to gain access to sensitive student information such as grades, home phone numbers and addresses, emergency medical information complete with full-colour photos of students, and a psychological evaluation. The *Weekly* simply went outside of the school district's main office with a laptop that had a wireless network card. There was no authentication process. The files were not even password-protected, although the district does password-protect other files. Any user could view the files, copy them to their computers and upload the files to a server used by the district.

Even more unbelievable is the fact that the district knew about the WLAN vulnerability for about nine months, but did nothing about it until they were notified by the *Weekly*. Once they recognised the problem, they should have enhanced the security of their WLAN. It could have been as easy as MAC address filtering or turning on WEP. Continually assessing the security of the WLAN is a critical process of wireless security. Once a weakness is identified, swift action is necessary.

The PAUSD failed on the many critical components of WLAN security. They not only had a lax attitude about wireless security, but they also did not even take swift corrective action when a security gap was identified.

9.2 University of Tennessee: effort to implement strong security without consistent wireless security policy

In 2002, the University of Tennessee made an unsuccessful attempt to implement security for their wireless LAN. Instead of using a standards-based security technique, they used a proprietary authentication method that would only work with certain operating systems such as Windows 2000 and Mac OS 9 and below (Higgins, 2004). The method was not compatible with the emerging operating systems Windows XP and Mac OS 10. After "[WLAN] usage dropped by 10% and the helpdesk was flooded with complaints", the university abandoned the authentication method and reverted to MAC address filtering. The incompatibility concern influenced the university's attitude when they again tried to implement WLAN security in 2004.

The university developed the right attitude about wireless security as advised in Step 1 (S1) of the decision framework. Philippe Hanset, a Senior Network Engineer, said that "with the WLAN now an integral part of campus life, security awareness has become a hot button" (Higgins, 2004). Because of the concern for compatibility, the university's

WLAN Security Policy and implementation was uneven. They decided to divide the network into a secure segment and an unsecured segment. The secure segment uses 802.1 × with a Radius server using TTLS authentication. However, the university uses only MAC address filtering and traffic analysis on the unsecured segment.

Wireless security is only as strong as the weakest link. It is unfortunate that the university made a great effort implementing strong wireless security but still left the WLAN at risk with the unsecured segment. For a university, this tradeoff might be acceptable to please the large number of students who want to use the WLAN for convenience. However, if this were a company, a better decision would be to draft a WLAN Policy (S(b)1) that requires all users to upgrade their laptops with wireless NICs that support 802.1 ×. Universities might feel the need to balance security and convenience, but since companies have more critical data at stake, security should be the top priority.

9.3 Randy Hensel: an impeccable WLAN security strategy

Randy Hensel was an early adopter of Wireless LAN technology in the office, but he always kept security in mind. In 2001 and 2002, he implemented an 802.11b wireless network using WEP encryption, but kept it limited because he was aware of the protocol's weaknesses (Hansel, 2003).

Demand for the WLAN grew so he needed to expand it to a much larger network. He also knew that at such a large scale, he would need to improve WLAN security; so in 2003, he upgraded to WPA. Not only did he use the strong security of TKIP encryption and PEAP authentication, but he also used additional features such as IP address filtering.

He also implemented a policy that requires users of the WLAN to use compatible Network Interface Cards. If users have old cards that do not support WPA, they must be upgraded before using the WLAN. He even suggested further WLAN security improvements such as additional authentication measures and upgrade to the full 802.11i when it is released.

10 Conclusion

It is important for companies to understand the current security threats to wireless networks and how to implement strong protection against these attacks. Several new security standards are being developed and used such as 802.11i, WPA/WPA2 and VPN. These standards provide varying degrees of protection, so companies need to understand which standard is most feasible for them. Using methods beyond the security standards (such as using a firewall and monitoring) and a continual assessment of the WLAN ensures that the corporate WLAN stays secure.

To achieve that goal, we proposed the steps to implement strong wireless LAN security for companies using a visual security assessment framework. Through case studies, we verified how the continual assessment of the WLAN can be accomplished systematically using our corporate WLAN security assessment framework for seamless wireless information assurance.

References

Adya, A., Bahl, P., Chandra, R. and Qiu, L. (2004) 'Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks', *International Conference on Mobile Computing and Networking*, pp.30–44.

Dulaney, K. *et al.* (2004) 'New 802.11i standard will advance wireless networking', *Gartner*, Note Number: FT-23-3273.

Geier, J. (2002) 'Wireless LAN security assessments steps', *Wi-Fi Planet*, http://www.wi-fiplanet.com/tutorials/article.php/1545731

Girard, J. (2003) 'Secure the enterprise against WLAN attacks', *Gartner,* Note Number: TG-20-8777.

Girard, J. (2004) 'Three false remote-access security assumptions', *Gartner*, Note Number: TG-16-1454.

Girard, J., Pescatore, J. and Dulaney, K. (2003) 'Wireless LAN authentication choices', *Gartner*, Note Number: QA-20-6834.

Grimm, B. (2003) 'Wi-Fi protected access', *Wi-Fi Alliance*.

Hansel, R. (2003) *Case Study: Implementing a Secure Wireless Network using WPA*, GSEC Version: 1.4 b Option: 2.

Hanley, K. (2004) 'IEEE 802.11n', *WiFi Alliance*, http://www.wi-fi.org.opensection/pdf/802.11n_q_a.pdf

Higgins, K. (2004) 'Case study: University of Tennessee implements 802.11i', *Mobile Pipeline*.

Klaus, C.W. (2002) 'Wireless LAN security FAQ', *Internet Security Systems (ISS)*, http://www.iss.net/wireless/WLAN_FAQ.php

Maunuksela, A.J. and Nieminen, M. (2005) 'Micromobility supported WLAN networks: an empirical study of new IP protocol to support mobility and connection handovers', *International Journal of Mobile Communications*, Vol. 3, No. 2.

Metz, R. (2003) 'Security breach', *Palo Alto Weekly.*

Pescatore J. *et al.* (2002) 'Wireless LAN security Q&A', *Gartner*, Note Number: QA-18-7478.

Redmond, P. (2004) 'Voice over WLAN remains niche for now', *Gartner*, Note Number: T-22-7994.

Redmond, P. *et al.* (2004) 'Hype cycle for wireless networking', *Gartner*, Note Number: G00120922.

Reynolds, M., Girard, J., Pescatore, J. and Dulaney, K. (2003) 'Wireless LAN security decision framework', *Gartner*, Note Number: DF-20-6636.

Sheu, S-T. *et al.* (2003) 'Adaptive rate controller for mobile ad hoc networks', *International Journal of Mobile Communications*, Vol. 1, No. 3, pp.312–328.

Simpson, R. and Keene, I. (2004) 'WiMAX will complement, not kill, wireless fidelity', *Gartner*, Note Number: COM-23-0196.

von Solms, B. and Marais, E. (2004) 'From secure wired networks to secure wireless networks – what are the extra risks?', *Computers and Security*, Vol. 23, pp.633–637.

Tyson, J. (2001) *How Virtual Private Networks Work*, http://computer.howstuffworks.com/vpn.htm

Varshney, U. (2003) 'Location management for wireless networks: issues and directions', *International Journal of Mobile Communications*, Vol. 1. Nos. 1–2, pp.91–118.

Varshney, U. *et al.* (2004) 'Wireless in the enterprise: requirements, solutions and research directions', *International Journal of Mobile Communications*, Vol. 2, No. 4.

Bibliographies

Convery, S., Miller, D. and Sundaralingam, S. (2003) 'Cisco SAFE: Wireless LAN security in depth', *Cisco Systems*.

Dulaney, K. (2004) 'Technological advances change WLAN recommendations', *Gartner*, Note Number: G00123755.

Girard, J. *et al.* (2004) 'WPA, WPA2 and 802.11i don't meet interoperability needs', *Gartner*, Note Number: T-22-8594.

Girard, J., Pescatore, J. and Dulaney, K. (2004) 'How to implement secure WLANs while you wait for 802.11i', *Gartner*, Note Number: QA-22-9136.

Karygiannis, T. and Owens, L. (2002) *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, National Institute of Standards and Technologist, Gaithersburg, MD.

Lu, J. *et al.* (2004) 'Wireless trust: conceptual and operational definition', *International Journal of Mobile Communications*, Vol. 2, No. 1, pp.38–50.

Novell (2005) *Novell's Networking Primer*, http://www.novell.com/info/primer/prim08.html

Panko, R. (2005) *Business Data Networks and Telecommunications*, 5th edition, Upper Saddle River, New Jersey: Prentice Hall Publishers.

Pescatore J. (2002) 'Wireless LANs move toward 'safe enough'', *Gartner*, Note Number: TG-15-5414.

Vaughan-Nichols, S. (2003) 'Making the most from WEP', *Wi-Fi Planet*, http://www.wi-fiplanet.com/tutorials/article.php/2106281

Walker, J. (2003) '802.11i overview Part 1', *Intel Corporation*, http://www.ocate.edu/wireless_4.ppt

Appendix: Acronyms

AAA	Authenticating, Authorising, and Accounting
AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
DAP	Diagnostic Access Point module
DC	Diagnostic Client module
DoS	Denial-of-Service
DS	Diagnostic Server module
EAP	Extensible Authentication Protocol
EAP-SIM	Extensible Authentication Protocol-Subscriber Identity Module
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunnel Transport Layer Security
EDCF	Enhanced Distributed Coordination Function
FMS	Fluhrer, Mantin, and Shamir
HCD	Hybrid Coordination Function
IPSec	Internet Protocol Security Protocol
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MITM	Man-in-the-Middle
NIC	Network Interface Card
OTP	One-Time Password
PEAP	Protected Extensible Authentication Protocol
PGP	Pretty Good Privacy
RAID	Redundant Array of Inexpensive Disks
RSA	Rivest, Shamir, and Adelman
TKIP	Temporary Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access