2005

# Recommendations for wireless network security policy: An analysis and classification of current and emerging threats and solutions for different organisations

Andrew Woodward
*Edith Cowan University*

# Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations.

Andrew Woodward
School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
a.woodward@ecu.edu.au

## Abstract

*Since their inception, 802.11 wireless networks have been plagued by a wide range of security problems. These problems relate to both data security and denial of service attacks, and there have been many solutions created by different vendors address these problems. However, the number of different types of attack, and the many possible solutions, makes it a difficult task to put in place an appropriate wireless network security policy. Such a policy must address both the size and nature of the enterprise, and the resources available to it. Measures such as WEP and MAC filtering are only appropriate for home users, and WPA should be used instead. Larger organisations can benefit from using 802.1x/EAP, RADIUS authentication and AES encryption. However, the wireless segment of a network should always be considered unsafe.*

**Keywords**

802.11 wireless networks, security, WEP, WPA

## INTRODUCTION

One of the newer technologies being increasingly used in today's business is that of wireless networks. While this technology has the advantages of providing greater user mobility and temporary access, it does have the disadvantage of an intrinsic lack of security. The security risks are mostly the same as for wired networks, such as loss of intellectual property. However, the wireless medium, brings with it new risks, such as theft of Internet bandwidth (Coursey 2004), which can be a considerable amount of money, particularly for a small-business, or loss of intellectual property. Since their inception, the 802.11 wireless network protocols have been plagued by in-built security flaws. These flaws range from problems with the Wired Equivalent Privacy (WEP) encryption system, through to full-scale active denial of service attacks which aim to capture data from a victim. There are two aspects of wireless networks which lead to this insecurity.

The first aspect is that it is a broadcast medium, meaning that the information is effectively broadcast and propagated over a wide area with a suitably equipped entity within the signal locus capable of capturing this information.

The second is embedded vulnerabilities in the modus operandi of the actual 802.11 protocol. The inability to verify management and control frames is one such vulnerability, leaving the network susceptible to Denial of Service (DoS) and man-in-the-middle (MITM) attacks (Woodward 2004a). The most publicised of the wireless security problems is the implementation of WEP, allowing it to be compromised with relative ease (Walker 2000; Fluhrer et al 2001). Although there are a plethora of solutions available to these and other wireless security problems, the biggest problem facing IT security managers is which of these solutions are appropriate for their business. Many of the solutions proposed, or available, are not necessarily relevant to all levels of business. Basic solutions, such as MAC address filtering or SSID masking, are feasible to the home or possibly small-business user with limited numbers of wireless devices. On the other hand, the solutions which are more secure and appropriate for a larger enterprise are financially and technically cumbersome for the smaller business or home user. The problem then, is one of knowing which solution is right for the size of the organisation.

This paper will briefly look at the types of security threats that IS managers are likely to face, and then look at a range of available solutions. A brief analysis of the advantages and disadvantages of each solution will be provided and guidelines given as to where each of these countermeasures is appropriate to use. Finally, policies for appropriate use of the wireless network and equipment will be suggested for the spectrum of wireless users.

## SECURITY THREATS

There are a number of types of attack that wireless LANs are vulnerable to, based on different aspects of their operation and configuration. These will be briefly addressed here.

### Broadcast medium

The functionality of wireless network presents one of its biggest problems. Because wireless is a broadcast medium, there is no way to control where the information is sent and who therefore has access to it. By modifying the drivers used with the wireless client devices, many individuals and organisations have developed analysis tools, known as “sniffers”. When used within the broadcast range of a wireless network, these can be used to capture every packet travelling the wireless network. If an access point is set up and used in its default configuration, then the user of such a system is vulnerable to attack, because anyone running sniffer software can see and capture everything that a user does across that network. Another problem with the broadcast medium is that the range is not only dictated by the transmitter, but also by the receiver. Effective range of the wireless network is an intersection of where the two antenna coverage patterns overlap. An attacker can increase the distance at which they can perform an attack simply by using a larger antenna. Depending on the antenna type used, the range is only limited by the ability to obtain line of sight between attacker and victim.

### WEP Vulnerabilities.

One of the earliest security problems with 802.11 wireless networks is that relating to the problems with the WEP protocol. Although the system was never meant to absolutely protect data traversing the wireless network, there was the expectation that it would be more robust than it turned out to be. There were two problems with the original WEP encryption system.

Firstly, was the way in which it was implemented in the shared key authentication system. The shared key system requires the use of the WEP key to verify a user attempting to connect to the wireless network. The problem is that during the authentication process, the key is made vulnerable, due to both encrypted and unencrypted versions of the challenge text being transmitted. A malicious user can easily capture this information and use it to derive the WEP key in an offline mode. This key is the same one which is used to protect data as it travel the wireless network.

The second was the actual implementation of the encryption system itself. The use of a relatively small initialisation vector (IV) means that in a high traffic environment, the IV is likely to be repeated more than once during a day. This repetition of the IV, makes it easy for an attacker to bypass the encryption system. There are now many other systems and measures available to protect and encrypt data and some these will be discussed later in this work.

### Denial of Service

This type of attack can be perpetrated in one of two ways. It can either be conducted through the use of a jamming technique, or by exploiting the OSI Layer Two vulnerabilities that exist within that the 802.11 protocol suite. The first type of attack, that of jamming, is fairly easy to perpetrate, and also reasonably difficult to detect. A jamming attack can be either intentional or unintentional. An intentional attack is one in which the attacker broadcasts a very high-power signal at the same frequency that the wireless network is operating on, causing interference to the network (Hoad and Jones 2004). The likelihood of this type of attack being conducted is fairly low as there are no real benefits to an attacker. This type of attack may also occur unintentionally, through the action of placing a device which operates at the same frequency in the vicinity of the wireless network. For devices that operate in the 2.4GHz frequencies, this includes microwave ovens, some cordless phones and Bluetooth devices.

The second category of attack is that which exploits the lack of verification of control frames in the wireless network (Woodward 2004b). This control and management information is a broadcast in the clear by wireless networks, and can be captured by an attacker using a freely available packet capture tool, such as Kismet (Kershaw 2004). Once gathered this information can then be used against the wireless network that it was captured from and used to disassociate or deauthenticate a valid client from the network (Bellardo and Savage 2003). The point of launching this attack is that the user is forced to rejoin the network, and during the reassociation process, the user’s logon and authentication details can be captured. This information can then be used to further exploit the wireless network. This type of attack can also be used to launch a man in the middle attack against the wireless network, and can even be used to circumvent VPN systems. This type of attack is probably one of the most concerning to IS managers as there appears to be no adequate means to prevent it from occurring (Baird and Lynn 2002; Floeter 2003)

### Injection of traffic

A new tool has been released which allows a malicious user to inject or insert traffic at the application layer (Airpwn, 2004). The potential for misuse of this tool is great: the example used had pornographic images being displayed on the screen of wireless users. While an attack of this nature is disturbing enough, and would cause problems in most organisations with appropriate use policies, this is the least of what a tool such as this is capable of. As stated by the creators, it could even be used to wipe hard drives. Fortunately, this tool only works against open systems: implementation of WEP should be enough to prevent use of this tool against a wireless network.

### Rogue Access Points

These are access points that are set up using the MAC address and SSID of a valid AP. An attacker would firstly use a DoS attack against he wireless client to force it to dissociate from the valid AP. The attackers AP is run at higher power, and/or with a higher gain antenna so that when the client seeks to rejoin, it should go the AP with the higher power level. The attacker would typically run a program such as Airsnarf (Shmoo 2005) which allows such attacks to be carried out. Airsnarf is a simple rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hotspots.

There are some tools such as Hotspotter that also fool clients into associating with them (Remote-exploit 2005). Hotspotter passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names. If the probed network name matches a common hotspot name, Hotspotter will act as an access point to allow the client to authenticate and associate. Once associated, Hotspotter can be configured to run a command, possibly a script to kick off a DHCP daemon and other scanning against the new victim.

## THE SOLUTIONS

The security options available to protect the wireless network form the various types of measures listed above will be classified into two groups: data security, and user authentication

### Data security.

Data security addresses the problems with wireless networks that relate to encryption and protection of data on the network.  These include WEP with centralised encryption key servers, temporal key integrity protocol, advanced encryption standard and virtual private networks.

### WEP key servers.

The major problem with the use of WEP is that the private key is static. Because, the key is not changed regularly, if at all, this makes it much easier for an attacker to derive or capture the private key. These are centralised key encryption server makes it possible to have the key changed regularly, thereby reducing or eliminating some of the risks of using the WEP system. Keys can be changed on a per packet, or per session basis. Changing the key on a per packet basis adds significant overhead to the wireless network, and would reduce throughput markedly. In most cases, the use of per session keys is sufficient.

### Virtual private networks (VPN)

VPNs have long been used in a wired environment, usually to protect remote users dialling into a corporate server. The added security of having all traffic pass through an encrypted tunnel makes provide access to the corporate network, a viable option.  When the problems with WEP become public, VPNs were widely adopted as a means of securing wireless network traffic.  However, if not implemented correctly, a tool such as crackerjack from the air jack suite can be used to circumvent a VPN and the capture traffic via a man in the middle attack. Due to recent additional security measures, added via WPA, the use of VPNs is on the decline.

### Temporal key integrity protocol (TKIP)

Due to the perceived problems with wireless, and WEP in particular, a new system of security measures for wireless networks was developed called Wi-Fi protected access (WPA).  This system incorporated several elements of the draft 802.11i security, the most notable feature being that of an inbuilt key rotation system, TKIP. The use of this meant that the installation of additional servers to manage the task of key rotation became unnecessary. It also means that it is an extremely difficult task for an attacker to crack or derive the key. All wireless hardware built from the beginning of 2004 was required to support WPA if it wished to achieve Wi-Fi certification. Many vendors have also released firmware updates for hardware built previous to this in order to add support for WPA.

### AES/CCMP

To further increase the security of wireless networks, an updated version of WPA was announced in September 2004, known as WPA2.  This increases the security of wireless networks by incorporating additional features of the IEEE 802.11i security protocol. In particular, it incorporated the use of the advanced encryption standard to protect data. The AES/CCMP encryption system is generally acknowledged to be virtually unbreakable. There are however, some drawbacks to the AES system. Most notable is the additional overhead required for encryption and decryption. If the wireless device does not have the hardware capability to run the AES and is forced to do it in software, then the wireless network would become unusable. Fortunately, most hardware devices built in the last year does have hardware support for AES.

### User authentication.

This second category of security measures includes MAC address filtering, SSID masking, and 802.1x / EAP. These are means of verifying and establishing the identity of both client and access point, for the purposes of creating and/or maintaining a valid connection.

### MAC address filtering and SSID masking

MAC address filtering involves entering a list of MAC addresses, which are unique to every network device, into the AP, or to a server (Maufer 2004). This means that only users with a MAC address on this list can connect to the network. Additionally, the same MAC address cannot be used on the same network more than once. This means that if someone was to capture a valid MAC address, they would not able to use it until such time as that address isn't being used on the network. However, MAC addresses can be cloned or spoofed by a malicious user, and valid users can be forcibly disconnected from the network because of the layer two vulnerabilities. MAC address filtering is not intended to be a strong solution, but is one which should be used in most defence systems.

SSID masking makes it harder, but not impossible, for a malicious user to discover the AP. The term masking refers to the process of removing the SSID from the beacon frames broadcast by the access point (Barken 2004). The idea is that if an attacker does not have the SSID, then they cannot connect to the network. This solution is not recommended to be used as much more than a basic deterrent, because the use of a tool such as Airjack (Abaddon, 2003) makes it an easy task to discover a masked SSID. These measures will not stop a dedicated attacker; they are simply intended to make an attempt to break into the wireless network more difficult.

### RADIUS

This is a system of authentication which has been used for many years with wired systems. Originally developed to authenticate dial up users to a corporate network, this authentication system has been adopted by wireless network users, and is required for 802.1x authentication. It is a service which can run on an existing server, or a dedicated server depending on user load. The level of technical expertise required and hardware costs mean that this system is only likely to be appropriate for medium to large enterprise. However, there are some software solutions that provide RADIUS like authentication which require very little user setup or even knowledge of how the system works (Lucidlink 2005). The utility offered by Lucidlink can be obtained for no cost for a small amount of users, making it a good solution of SOHO.

### 802.1x and EAP

The IEEE802.1x authentication system is a means for authenticating and controlling user access to a protected network, as well as dynamically varying encryption keys. 802.1X works in conjunction with an extensible authentication protocol (EAP) to both the wired and wireless LAN media (Edney and Arbaugh 2004). It supports multiple authentication methods including Kerberos, one-time passwords, certificates, and public key authentication. Client authentication with 802.1x works in the following manner (Wong 2003). Firstly, an authenticated client attempts to connect to an access point. The access point opens a port which only allows EAP packets to pass from client to an upstream authentication server. All other traffic is blocked until the client is authenticated. If the client does success of dedicated there is allowed to pass traffic as per normal. There are many different types of EAP, which can be used in conjunction with the 802.1x system. These include: protected EAP (PEAP), lightweight EAP (LEAP), EAP with transport layer security (EAP-TLS), tunnelled transport layer security (EAP-TTLS), and EAP message digest (EAP-MD-5) (Intel 2003). While each of these methods provides additional security and compatibility, they do all have potential weaknesses, and provide different strength (Barken 2004). The proprietary Cisco LEAP is probably the most vulnerable, as it is subject to offline dictionary attack (Wright 2004). Whilst all Cisco wireless equipment incorporates LEAP, its use is not recommended. The newest of the methods mentioned is that of protected EAP, which was developed by both Microsoft and Cisco. This PEAP system is recommended to be used with 802.1x to provide for user authentication in a wireless network. It should also be noted that Windows XP provides native support for 802.1x and EAP.

## RECOMMENDATIONS FOR A WIRELESS SECURITY POLICY

Listed here are some specific as to what procedures and policy should be put in place for different wireless users. This is not exhaustive, but should allow for a wireless security policy to be put in place that protects the organisation. Wireless security recommendations are provided for home, small business and enterprise, with additional general recommendations provided for enterprise IS managers.

### Home

The greatest danger to a home user is that of theft: leaving an AP open can allow someone to steal their internet bandwidth. While not a major concern from a liability point, it is one of financial concern. The recommended option for a home user is to implement shared key authentication at the very least. This is not recommended for anyone concerned about data security because it does leave the WEP key vulnerable to discovery. However, if the equipment being used has WPA equipped, then it will have a rolling key, making it very difficult for someone to derive the WEP key (Wi-fi Alliance, 2003). What it does do is prevent a passer-by from being able to immediately connect to, and use, the internet connection. In the majority of cases, this is enough to deter someone who is likely to try this type of attack. However, in reality, all users should implement WPA security. If the wireless equipment being used does not support WPA, then serious consideration should be given to replacing it with WPA approved equipment. Other basic measures that should be taken by a home user include masking the SSID (where possible), and also making use of MAC address filtering (Maufer 2004).

### Small Business

In addition to bandwidth theft, small users such as real estate agents, medical professionals and small retailers are exposing themselves to a potentially greater risk. If the signal from an AP that this type of business has setup is accessible from a distance, then their data is not secure. Any sensitive data travelling the wireless segment is available to anyone within range. If this data is of a sensitive nature, and it very likely is, then the person operating the AP may be in breach of information privacy laws. Recommendation for this type of wireless user is to implement the methods listed in the home section (above) provided that a rolling key is used. The use of a VPN or even some sort of segregation of the network is also recommended. These last two measures may not always be possible, as the technical and financial resources required may not be available.

### Enterprise

Large organisations are less likely to have bandwidth stolen because they usually have the infrastructure in place to ensure that users are authenticated before being allowed access to the internet. Authenticating to a RADIUS or proxy server to gain access to network resources would normally be in place as part of their wired network, and this can be extended to cover the WLAN. What larger organisations are at greater risk of is people stealing their data. There are several recommendations for protecting the network for an enterprise. MAC address filtering can still be of use even for enterprise, and is recommended. Strong mutual authentication, such as that provided by 802.1x / EAP, should be put in place. A VPN server may or may not be implemented, depending on what other methods are in place. To further aid in the development of a wireless security policy for enterprise, the additional recommendations are provided. They are summarised as: AP configuration; scanning for rogue APs and intrusion detection systems; firewalls, segregation and wireless DMZs.

#### AP configuration

By connecting wireless equipment in default configuration, the individual or organisation leaves themselves open to a number of risks. These include having traffic intercepted, which has a number of significant consequences, injection of malicious traffic and denial of service (DoS) attacks. There is evidence that organisations, both large and small, are in fact leaving themselves vulnerable by having unsecured WLANs. A survey of the Perth CBD in 2003 (Webb 2004) found a large number of APs installed by organisations with both the default SSID and no WEP encryption being used. A more recent survey of the same area found that the total number of APs had increased, with the number of unprotected APs being roughly the same (Yek and Bolan 2004). This gives information to an attacker, and leaves the owner of that equipment vulnerable. It informs a malicious individual that the rest of the configuration of the AP is likely to be default, and it indicates the manufacturer of the equipment, which may also expose other flaws of that particular device. A large number of the APs detected had no WEP authentication, meaning anyone would be able to connect to that network. The recommendation is to change the SSID from the default, and to make it something which doesn’t easily identify the name or nature of the business to an attacker.

#### Intrusion detection systems (IDS) and Scanning for Rogue APs

One major problem for large enterprise is the risk of staff attaching unauthorised APs to the company network. The first step is to create policy which outlaws the use of wireless equipment unless it is setup by the organisations IS staff. If not configured properly, this gives an attacker easy access to the network, allowing them to bypass most security features that may be in place. Although a policy may be put in place, prohibiting the connection of such a device to the network, this of course does not mean that employees will not do so. The recommendation is that routine wireless scans be conducted in order to detect any devices in operation that should not be present.

One way of making sure that rogue or unauthorised access points are discovered early is to use a wireless intrusion detection system, or WIDS (Lim et al 2003). There are both commercial and freeware WIDS available, but their effectiveness in protecting wireless networks is questionable (Valli 2004). They work by monitoring wireless traffic and alerting system administrators to any unauthorised traffic or devices. However, these systems do have drawbacks, and are only as good as the rules that determine what traffic is classified as legitimate or unauthorised (Farshchi, 2003). If the rules are not strictly defined, then legitimate traffic can be classed as a potential attack, particularly when clients signal strength is low. Another problem with these systems is that they are a reactive system rather than an active, meaning that attacks are not prevented, but are reported after they occur.

Firewalls, segregation and wireless DMZs

In the event that the access point or wireless network segment is compromised, it is important that this breach not be allowed to expose the wired network. A basic level, this simply means connecting the access point to a gateway to segregate it from the rest of the network. Another way to make sure this doesn't occur is to place the access point behind a firewall, and only allow connection to the wired network through the use of a VPN. This allows for additional monitoring of traffic passing from wireless to wired. The wireless demilitarised zone, or WDMZ, is a means of totally compartmentalising and segregating the wireless portion of the network from the wired (Planet3 Wireless 2002). Such a system would involve creating a separate network either physically, or through the use of a VLAN, with all wireless equipment connected to this subnet. A separate DHCP server should be used for this segment, and a user authentication method, such as 802.1x with EAP should also be included.

## CONCLUSION

Early adopters of wireless networks faced significant security threats, with little on offer to protect the network from attacks. The last few years have seen many new security features and solutions offered by various vendors, including WPA, WPA2 and 802.11i. Although there are now many security solutions on offer for wireless networks, the difficulty can lie in deciding which of the available measures is appropriate for the Information Security manager to implement. In addition to having to secure and monitor an IT infrastructure, IS managers now face the additional task of having to secure a part of the network which is inherently vulnerable. The initial security measures available to users of wireless networks, such as MAC address filtering and SSID masking, are only appropriate for small business or home users. More advanced means of protecting wireless network, such as a VPN, TKIP, and strong mutual authentication, are recommended for medium to large enterprise. This paper has attempted to aid in the task of developing and implementing an appropriate wireless network security policy, by analysing current threats and solutions, and providing recommendations based on those aspects.

Whilst the solutions and recommendations given in this paper will aid IS managers in developing policy to secure the network, none of the solutions are absolute. Each of the measures given here still has a flaw of one sort or another. Although the risk associated with some of the more robust solutions, such as 802.1x / EAP, is extremely small, it is important to note that in certain circumstances its security can be compromised.

## REFERENCES

Abaddon (2003) Airjack. http://802.11ninja.net/airjack/. Retrieved 13 March, 2005

Barken, L. (2004) *How secure is your wireless network? Safeguarding your wi-fi LAN*. Prentice Hall, New Jersey

Baird, R. and M. Lynn (2002) Advanced 802.11b Attack. Blackhat Briefings 2002, Caesars Palace, Las Vegas, Nevada. URL: http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt, Retrieved 17 March, 2005

Bellardo, J. and S. Savage (2003) Disassociation and De-auth attack. 2003 USENIX Security Symposium, USENIX.

Coursey, D. (2004). Is it wrong to steal wireless bandwidth?, URL http://reviews-zdnet.com.com/AnchorDesk/4520-7296_16-5121168.html, Retrieved 4th Aug 2005

Edney, J. & Arbaugh, W.A. (2004) *Real 802.11 security: Wi-Fi protected access and 802.11i*. Pearson, Boston

Farschi, J. (2003) Wireless Intrusion Detection Systems. URL: http://www.securityfocus.com/infocus/1742 Retrieved 5/7/05

Floeter, R. (2003) Void11, URL: http://www.wlsec.net/void11/. Retrieved 17 March, 2005

Fluhrer, S., Mantin, I. & Shamir, A. (2001) Weaknesses in the key scheduling algorithm of RC4. URL: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf Retreived 27/7/05

Hoad, R. & Jones, A. (2004) Electromagnetic (EM) threats to information security – Applicability of the EMC directive and information security guidelines. 3rd European conference on Information Warfare and Security, Royal Holloway, UK June 2004

Intel (2003) Wireless Security - 802.1x and EAP Types. URL: http://support.intel.com/support/wireless/wlan/sb/CS-008413.htm Retrieved 28/7/05

Kershaw, M (2004) Kismet readme. URL: http://www.kismetwireless.net/documentation.shtml Retrieved 28/7/05

Lim YX., Schmoyer, T., Levine, J. & Owen, H.L. (2003) *Wireless intrusion detection and response*. Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003

LucidLink (2005). *LucidLink makes it easy to secure your wireless network*. URL: http://www.lucidlink.com/ Retrieved 28/7/05

Maufer, T. (2004). *A field guide to wireless LAN's for administrators and power users*. New Jersey: Prentice Hall.

Planet 3 Wireless. (2002). Certified Wireless Network Administrator: Official CWNA Study Guide. Planet3 Wireless, Georgia

Remote-exploit (2005). Hotspotter. URL: http://www.remote-exploit.org/index.php/Hotspotter_main Retrieved 29/7/05

Shmoo (2005). Airsnarf - A rogue AP setup utility. URL: http://www.macsecurity.org/ Retrieved 28/7/05

Valli, C. (2004) WITS – Wireless Intrusion Tracking System. 3rd European conference on Information Warfare and Security, Royal Holloway, UK June 2004

Webb, S. (2004). Growth in the Deployment and Security of 802.11b Wireless Local Area Networks in Perth, Western Australia. Perth, Western Australia.

Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. URL: http://www.sans.org/rr/whitepapers/wireless/1109.php Retrieved 28/7/05

Woodward, A. (2004a). Wireless Jacks - An analysis of 802.11 wireless denial of service attacks and hijacks. 3rd European conference on Information Warfare and Security, Royal Holloway, UK June 2004

Woodward, A. (2004b) An analysis of current 802.11 wireless network layer one and two attacks and possible preventative measures. *Journal of Information Warfare*. **3(3):** pp37-47

Wright, J. (2004). Asleap. URL: http://asleap.sourceforge.net/ Retrieved 8/04/05

Yek, S. & Bolan, C. (2004). An analysis of security in 802.11b and 802.11g wireless networks in Perth, W.A. 5th Annual Information Warfare and Security Conference, Perth, Western Australia 2004

## COPYRIGHT