

**CIS 3660 Computer Networking**

**Fall Semester 2005**

**Research Paper:**

**“Developing an Effective  
Wireless Security Policy”**

**Randall S James**

**Signature:** \_\_\_\_\_

**Date: December 6, 2005**

**Professor: Dr. Mike Tarn**

# Table of Contents

<a href="#"><u>Abstract</u></a> .....	3
<a href="#"><u>Definitions</u></a> .....	4
<a href="#"><u>Introduction</u></a> .....	7
<a href="#"><u>Knowing the Enemy</u></a> .....	7
<a href="#"><u>Deciding What to Protect</u></a> .....	9
<a href="#"><u>Wireless Implementation</u></a> .....	10
<a href="#"><u>Securing the Network</u></a> .....	12
<a href="#"><u>Hardening the Network</u></a> .....	14
<a href="#"><u>Survey of a Local Business</u></a> .....	17
<a href="#"><u>Wireless Security Assessment</u></a> .....	18
<a href="#"><u>Conclusions</u></a> .....	19
<a href="#"><u>References</u></a> .....	21

## **Abstract**

Wireless networking is no longer the wave of the future; it has fast become common place in today's business world. Along with the presence of this new technology comes a whole new frontier of threats to company data. A surprising number of companies are unaware of these threats. They make common mistakes in the configuration of their networks, making it all too easy for someone to break in.

Some simple steps and techniques have been developed to prevent such security breaches. The use of tools such as firewalls, encryption, traffic filtering, and more can make your company network impenetrable. However, these steps are only helpful when you have an effective wireless security policy in place.

## **Definitions:**

(All definitions provided by [www.techweb.com](http://www.techweb.com))

**Denial of Service:** An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a denial of service attack interrupts network service for some period.

**Dictionary Attack:** A brute force attack that uses common words as possible passwords or decryption keys and may provide a more efficient way of discovering the user's code.

**Firewall:** The primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise.

**Hot Spot:** The geographic boundary covered by an 802.11 wireless access point. Typically set up for Internet access, anyone entering the hotspot with an 802.11-based laptop can connect to the Internet, providing the access point is configured to broadcast its presence (beaconing) and authorization is not required.

**IDS: (Intrusion Detection System)** Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

**IEEE: (Institute of Electrical and Electronics Engineers, New York, [www.ieee.org](http://www.ieee.org))** A membership organization that includes engineers, scientists and students in electronics and allied fields. Founded in 1963, it has more than 360,000 individual members in more than 150 countries and is involved with setting standards for computers and communications.

**IPSec: (IP SECURITY)** A security protocol from the IETF that provides authentication and encryption over the Internet. Unlike SSL, which provides services at layer 4 and secures two applications, IPSec works at layer 3 and secures everything in the network.

**PSK: Pre Shared Key**

**Router:** A network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it. To which interface on the router outgoing packets are sent may be determined by any combination of source and destination address as well as current traffic conditions (load, line costs, bad lines, etc.).

Social Engineering: A person who illegally enters computer systems by having persuaded an authorized person to reveal IDs, passwords and other confidential information. The social engineer is the "con man" of this business, taking the low-tech road rather than using programming skills and other cracker techniques.

SSL: (**S**ecure **S**ockets **L**ayer) The leading security protocol on the Internet. Developed by Netscape, SSL is widely used to do two things: to validate the identity of a Web site and to create an encrypted connection for sending credit card and other personal data. Look for a lock icon at the bottom of your browser when you order merchandise on the Web. If the lock is closed, you are on a secure SSL or TLS connection.

TKIP: (**T**emporal **K**ey **I**ntegrity **P**rotocol) uses the same RC4 algorithm as WEP for encryption, but adds sophisticated key management and effective message integrity checking. TKIP was designed to be efficient enough to work in older WEP devices by updating their firmware to WPA.

VPN: (**V**irtual **P**rivate **N**etwork) A private network that is configured within a public network (a carrier's network or the Internet) in order to take advantage of the economies of scale and management facilities of large networks.

War Driving: Driving around an area with a laptop computer and an 802.11 wireless LAN adapter in order to find unsecured wireless LANs. When the laptop's wireless adapter (NIC) is set to promiscuous mode, it will receive any packets within its range. The goal is to find vulnerable sites either to obtain free Internet service or to potentially gain illegal access to the organization's data.

WEP: (**W**ired **E**quivalent **P**rivacy) An IEEE standard security protocol for wireless 802.11 networks. Introduced in 1997, WEP was found to be very inadequate and was superseded by WPA, WPA2 and 802.11i. Its authentication method was extremely weak and even helped an attacker decipher the secret encryption key. As a result, WEP authentication was dropped from the Wi-Fi specification.

Wi-Fi: (**W**ireless-**F**idelity) A logo from the Wi-Fi Alliance that certifies that Ethernet devices comply with the IEEE 802.11 wireless standard. In the early 2000s, Wi-Fi/802.11 became widely used.

Wi-Fi Alliance: A membership organization founded in 1999 devoted to certifying 802.11 wireless Ethernet devices for interoperability. The Wi-Fi CERTIFIED logo on a wireless radio (PC card, access point, etc.) means that it has passed a thorough interoperability test and will work with any other Wi-Fi CERTIFIED product.

WLAN: **W**ireless **L**ocal **A**rea **N**etwork

WPA: (**Wi-Fi Protected Access**) A security protocol for wireless 802.11 networks from the Wi-Fi Alliance that was developed to provide a migration from WEP. The WPA logo certifies that devices are compliant with a subset of the IEEE 802.11i protocol. WPA2 certifies full support for 802.11i.

# **Developing an Effective Wireless Security Policy**

## **By: Randall S James**

The definition of a network has evolved over the years since the inception of the internet. Today, networks are common place in all types of business, ranging in size from a handful of employees to thousands of people. So what happens when companies introduce wireless networking into their company network? How do they ensure that the network is safe from attack and that company data remains company data? What threats do companies need to prepare for? In this paper we will examine the steps that should be taken to secure your wireless network, and develop an effective wireless security policy.

Several techniques have been developed over the years to secure a wireless network. It is hard to say exactly what every network needs to be secure, but when you follow some commonly used techniques to develop a thorough wireless security policy you can be reasonably sure that your network is safe. Some of the ways to secure a wireless network include use of a firewall, encryption, MAC address restriction, password authentication, and more. We will examine each of these in detail later. First, let's get to know the enemy of the wireless network.

### **Knowing the Enemy**

There are many threats to a network. Natural disasters such as earthquakes impact people, facilities, and equipment. These risks must be considered by managers as part of the larger picture of disaster planning. In information systems security however, we use the word threat to describe a narrower, more limited component of risk (Lekkas, 2002).

When preparing for your wireless network it is important to keep security in mind, and with that you must know what to defend against. Running a risk assessment can help with this. Microsoft offers a free application called ITASecur that will guide you through the process.

There are two basic types of threats; passive attacks (eavesdropping), and active attacks (penetrating the network) (Sikora, 2003). One technique used to find your network is called “war driving”. In this technique, a person would drive around with a laptop and a wireless card, “listening” for wireless network activity. When a signal is found, they capture packets and use the information they contain to steal data from your network. An unsecured network might even be hijacked and controlled by the hacker (Vines, 2002).

Other threats a network face include, but are not limited to: Denial of Service, where a hacker floods a server with requests that go unanswered in an attempt to overburden the system; man in the middle attacks, where a hacker poses as the intended recipient in order to obtain encryption and other network information; MAC spoofing, where a known MAC address is copied in order to obtain access to the system; port scanning, where hackers look for open doors in your network; virus attacks, Trojans, worms, and more.

Also be aware of some other threats to a WLAN:

- Brute force password attacks on Access Points: Use strong password policies such as minimum characters length, alpha and numeric, capitalization and punctuation, and frequent changes, to prevent dictionary attacks.

- Incorrectly configured network equipment: This is a common problem among wireless networks as misconfiguration leaves doors open to hackers.
- Monitoring of network traffic: A passive approach to obtaining network configuration information. A hacker can capture packets and use the data in them to break into your network.
- Encryption attacks (WEP weakness): With the weakness in the WEP encryption standards it is relatively easy for a hacker to extract the encryption key from captured packets.

A network must be protected not only from external threats, but also internal threats. A key component to bear in mind when setting up a wireless network is the fact that anyone who has access to the equipment in use can pose a threat to the integrity of the system. All companies must guard against Social Engineering.

The problem with most wireless networks in place today is that no one is taking the hacking threat seriously. “In real life we see again and again that these identified risks are ignored and that even existing security mechanisms are not used effectively, making it even easier for attacks to take place. No-one has yet disagreed with this assessment!” (Sikora, 2003, pg 153). These threats are relatively simple to protect against. The fact that most people are not paying them much attention is what makes them so dangerous.

### **Deciding What to Protect**

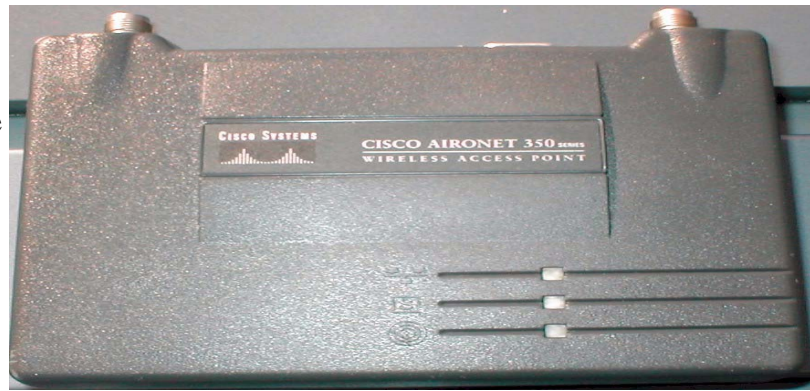
Often when drafting a wireless security policy it is handy to look at things from an “acceptable loss” perspective. That is to say, how much is too much to lose, and what steps need to be taken to prevent that. A six step approach to this technique has been laid out by Randall K. Nichols and Panos C. Lekkas:

1. Assess the impact of loss of or damage to the potential target. How badly will the organization be hurt from loss of the data you are trying to protect?
2. Specify the level of risk of damage or destruction that is acceptable. This can be the most difficult part of the process, as it may seem unnatural to put a level of acceptability on the loss of that which you are assigned to protect. The reality is that some loss is acceptable, and the total cost of preventing any and all loss is often quite high.
3. Identify and characterize the threat. Knowing what you are protecting against is half the battle.
4. Analyze vulnerabilities. Know how, when, and where your attackers will hit your network. If you are not looking for vulnerabilities, it is guaranteed that some one else is.
5. Specify countermeasures. How do you plan on dealing with these vulnerabilities? If you don't plug the holes some one will get in.
6. Allow for uncertainties. It is not logical to say that we can foresee and plan for all attacks. Allow a margin for error so that unforeseen threats do not cripple your network (Lekkas, 2002).

### **Wireless Implementation**

The design of your wireless network plays a role in your ability to protect it. When choosing equipment, look for features that allow you to lock the system down. Cisco Systems Aironet 350 series of wireless access points are a nice choice. They are the best on the market for features and security. They can be used as the center point of a standalone network, or to connect wireless to wired networks. It also offers RADIUS

support, WPA encryption, MAC restriction, and can be configured via browser based management as well as telnet (Vines, 2003).



Some companies cannot afford to spend enough to get all of these nice features. In that case,



identify the top priority options and purchase equipment that gives you the most features for the money that you have to invest. Other vendors to look at include 3com, NetGear, Proxim, and D-Link to name a few.

Before installing your network perform a site survey (with security in mind of course). There are five basic steps to setting up a wireless network:

1. Identify specific goals for wireless deployment: Is the payback measurable? Will it result in lower operating costs? Will it help your company provide better customer service?
2. Determine device types to be supported: Desktop and notebook PC's, handheld devices, VoIP phones.
3. Draft a site plan: Determine where to place the wireless access points by looking at factors that affect range, considerations for antennas, and access point considerations. Avoid bleed over into off campus areas.

AP Range Chart	Indoors	Outdoors
<b>802.11b</b>		
@11 Mbps	30 m (100 ft)	150 m (500 ft)
@1 Mbps	100 m (300 ft)	500 m (1500 ft)
<b>802.11a</b>		
@54 Mbps	20 m (60 ft)	30 m (100 ft)

4. Perform a site survey: Determine if the access point locations are feasible, power requirements, range factors and more. This is the most critical step.

5. Commission the network: Once you have completed steps one through four, implement your network. Check to make sure that nothing has changed since the original site survey, make sure security is enabled, and test for latency.

After deciding what to protect and implementing your network, you can begin work on securing your network.

### Securing the Network

When securing the wireless network, keep in mind the AAE and A method: Authentication, Authorization, Encryption, and Accounting. This plan is often referred to as the “Triple A” method, encryption is implied, but not stated (Held, 2003).

Authentication: This is the process of challenging a client and verifying permissions to enter the network. This can be done in several ways, including the use of WEP<sup>1</sup> authentication which is built in to most wireless routers. The IEE 802.11 specification for WEP (Wired Equivalent Privacy) issues a challenge to the client, the client then responds with a pre-shared encryption key, and access is granted after verification of that key. WEP however has a weakness, it is easy to passively monitor

---

<sup>1</sup> Since the release and subsequent failure of WEP, a new encryption specification has been launched called WPA (Wi-Fi Protected Access). WPA is a more robust and secure policy.

network traffic and obtain the WEP key in use. Other methods of authentication have been implemented including MAC (Media Access Control) authentication. However, it is also easy to passively monitor network traffic to obtain the MAC address in use, spoof it, and gain access to the system. Some proprietary systems have been developed to combat this weakness including RADIUS servers and Secure ID cards for password/username authentication. The use of a server and passwords are the recommended solution to authenticating users (Held, 2003).

Authorization: This is the process of granting permission or denying access to the user. Various network and computer functions can be restricted based on user identity. This is not addressed in the IEE 802.11 standards. A variety of techniques are available for authorization such as the aforementioned RADIUS servers, firewalls, router access limitations, Operating System functionality, third party products such as Cisco Systems Clean Access software, and more (Held, 2003).

Encryption: As stated before, WEP is the encryption protocol defined by the IEEE 802.11 specification. When the holes in WEP were discovered, the Wi-Fi Alliance wrote WPA as an upgrade, making WEP obsolete. Also, it is common to use layer 3 defenses against unauthorized viewing of network traffic. Some of the more popular choices include SSL and IPSec, or the creation of a VPN (Held, 2003).

Accounting: Accounting is not required to secure a network, but can be beneficial in tracking down successful thieves after the fact. This is the process of setting rules and recording usage data so that law enforcement can prosecute offending individuals if the need arises. Servers can be used to log access requests and create a database of successful and unsuccessful login attempts. Using this database, the system can be configured to

enable or disable future login attempts based upon historical data. This tactic is referred to as “lockout”. In addition, MAC information can be used to identify equipment used to break into your network (Held, 2003).

### **Hardening the Network**

After you have designed the network, implemented the wireless, and accounted for the “Triple A” protection plan, it is time to harden the network from attack. This can be done using several methods, the best protection coming from the combination of all of the following techniques:

- WPE/WPA: Enabling encryption will prevent passive listening attacks, and make it extremely difficult to obtain access to the company data (Robinson, 2005).
- SSID: Wireless equipment comes with a default name for the network that it broadcasts. Most companies make the mistake of not changing this name to something unique to their network, making it easy for would be hackers to guess the name of the network and monitor its traffic.
- Disable broadcast: By default, wireless networking equipment is set to broadcast the SSID. Turning off this broadcast will make it even harder for hackers to find your network, let alone break into it. Combined with a unique SSID, this will make your network virtually invisible to hackers.
- Periodically change encryption key: Even the tightest security can be breached from time to time. Changing your encryption key is one step to prevent hackers from having unlimited access to your system forever. It is recommended to change the key once per month, although this can be a cumbersome process in the absence of an automated process.

- MAC restriction: In the router for the wireless network is a table where the administrator can specify which MAC addresses are authorized to operate on the network. Restricting this list to only hardware in the possession of your company can help prevent a hacker from using their own equipment to break into your network. This is also handy in the event that equipment is lost, stolen, or put out of commission, as you can remove the MAC address from the routing table, preventing that equipment from accessing your network in the future (Robinson, 2005).<sup>2</sup>
- Positioning of AP's and antennas: Making sure that your company and your company only, will have sufficient coverage in your wireless network is a crucial part of planning your network. Excess broadcast of wireless into neighboring business, streets, or parking lots will just invite people to attempt accessing your system.
- DHCP limiting: Another handy setting in your router that will allow you to control how many devices can access your network at once. If you restrict the number of IP addresses issued, you can prevent rouge equipment from obtaining an IP address.
- Firewall: This can be either software or hardware, and is an essential part of protecting your networks sensitive data. On an open network, the firewall is placed between the wireless network and the company wire line network. This will allow users to obtain access to wireless internet in a "hot spot", while preventing them from surfing the files and resources on the company network. If

---

<sup>2</sup> The first five steps should not be implemented when using an "open" wireless network for public access. Always make sure that an open network is outside of the company firewall.

you do not desire an open network, place the firewall before all company networking to prevent unauthorized access. Scott Robinson of Tech Republic says, "...you've done yourself no good if your configuration doesn't place your wireless system's access points outside the firewall. Make sure it does—otherwise, you're not only failing to create a necessary barrier, you're creating a convenient tunnel through one that was already there (Robinson, 2005, pg 1).”

- Limit social engineering: One of the hardest vulnerabilities to prevent, social engineering is also one of the most dangerous. Educate your employees on security policies and procedures and instruct them to never give out any information with regard to the company network or passwords.
- White hat hackers: It helps to pay a third party company to assess your networks security by analyzing and attempting to “break” your network. This will give you insight into the realities of your network from an unbiased professional. One of the recommended sites to obtain such a service is [www.tigertesting.com](http://www.tigertesting.com) (Vines, 2003).
- Intrusion Detection System: Using IDS can detect and help you prevent future attacks on your network. (Vines, 2003)
- Change the channel: Another one of those default settings on the wireless router, changing the channel which you broadcast on serves two purposes; making it harder for hackers to find your network, and avoiding interference with other common wireless devices around the office such as wireless phone systems.
- Don't allow unauthorized access points: Using free monitoring software available for download on the internet, such as Netstumbler, an administrator can scan and

detect all access points on a network. When someone adds a new device not sanctioned by your company it should be taken down, as it will not be configured to your specifications and could be the hole that a hacker needs to gain access to the whole system (Robinson, 2005).

Even though you are done hardening your network you must always review and test your security to keep it in good working order. It is also a good idea to benchmark your network and compare it to industry trends. Mimicking other successful networks will help to ensure that your network is safe.

### **Survey of a Local Business**

To get an idea of what techniques are being used in local business networks I asked a few questions to Larry Sauer, a network administrator for Schupan & Sons, Inc., a local business here in Kalamazoo.

- 1) What threats to the integrity of your wireless network does your company consider highest priority?

Physical proximity to streets from our wireless stations (wardriving), ability of others to find/decode packets, access to wireless network (wireless AND domain authentication)

- 2) What steps have been taken to secure your network (i.e.; encryption, firewall, etc.)?

We use WPA-PSK authentication with TKIP encryption, turn off SSID broadcast, and use MAC address filtering. Our domain already has a firewall.

- 3) How often does your company review its wireless security policy?

About once a year, or when changes to the wireless network need to be made.

- 4) Does your company have a preference on equipment for wireless networking?

3Com

You can see from Larry's response that hackers are a threat that needs to be taken seriously. Wardriving is just one of the techniques used to gain access to your system, but the use of encryption and authentication techniques will slow down hackers, if not stop them all together. Reviewing your wireless security policy is essential to keeping it up to date, and the industry average seems to be approximately one year reviews, or as Larry points out, as needed when changes are implemented.

### **Wireless Security Assessment**

A wireless security assessment will help you to make sure that your WLAN security is effective. It is not wise to trust that your system is free from flaws, and reviewing this assessment will help to expose any problems that exist on your network.

Jim Grier from Wi-Fiplanet.com wrote the following steps for assessing a network. For more information on Wireless Security Assessments please see the whole article at <http://www.wi-fiplanet.com/tutorials/article.php/1545731>.

1. Review existing security policies: This will allow you to benchmark and ensure that your company is following its own security policies.
2. Review the system architecture and configurations: Knowing the design and layout of your network in detail will help you to define any weaknesses in the system.
3. Review operational support tools and procedures: Weaknesses can appear over time. Use support tools to monitor and fix these procedure breaches.
4. Interview users: Don't take for granted that all employees are aware of your security policy.

5. Verify configurations of wireless devices: Use tools such as AirMagnet or AiroPeek to capture and verify the configuration of your wireless devices. Identify and fix any abnormalities found during this exercise.
6. Investigate physical installations of access points: Observe the location and proximity to other users of all access points. They should be installed such that no one can handle them without being seen.
7. Identify rogue access points: Find and eliminate all non sanctioned access points. They may not be configured properly and represent a security hole.
8. Perform penetration tests: If you can not penetrate your network using tools available to hackers, then you can be reasonably sure that your network is safe. If you can, find the problem and plug the hole.
9. Analyze security gaps: During your assessment of the network gather all relevant information to gain a clear picture of how your organization is complying with security policies.
10. Recommend improvements.

### **Conclusions**

Wireless networking has a huge upside when implemented properly. Companies can gain productivity, provide better customer service, create work environments in places where no network connection was previously available, and more. However, improperly configured networks can lead to more trouble than they are worth.

When designing a wireless addition to an existing network an organization should proceed with caution. Paying strict attention to security concerns from the very beginning of your network will make the fusion of wireless and wire line networks seamless. Not all

companies can afford a full time IT staff, which makes having a well thought out security policy that much more important.

To make a wireless security policy effective it takes a team effort, careful planning, testing, and reviews. An effective security policy is a living breathing document. It needs to be cultivated over time, and constantly updated.

If an organization follows the steps that I have outlined, they can feel comfortable with the security of their company data. Having an effective wireless security policy in place is paramount to a successful business. Feel free to take advantage of the gains to be made from making your network wireless, but never take that freedom for granted!

## References

Held, G. (2003) *Securing Wireless LANs: A Practical Guide for Network Managers, LAN Administrators, and the Home Office User* Antony Rowe Limited, Chippenham, Wiltshire. Wiley Publishing Incorporated, Indianapolis, Indiana.

Lekkas, P. C., & Nichols, R. K. (2002) *Wireless Security: Models, Threats, and Solutions* McGraw – Hill. New York: New York.

Robinson, S. (2005) *Top Five Don'ts in Wireless Security* Tech Republic.

<http://techrepublic.com>

Sikora, A. (2003) *Wireless Personal and Local Area Networks* TJ International Limited Padstow, Cornwall. Wiley Publishing Incorporated, Indianapolis, Indiana.

Vines, R. D. (2002) *Wireless Security Essentials: Defending Mobile Systems from Data Piracy* Eds. Eldridge, Margaret. Wiley Publishing Incorporated, Indianapolis, Indiana.

Other sources:

<http://www.techweb.com>

<http://www.cisco.com>

<http://techrepublic.com>

<http://www.wi-fiplanet.com>

Special thanks to Larry Sauer and Schupan & Sons, Inc. for their participation in my wireless networking survey.