



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Name: Matt Suozzo
GSEC Practical Assignment Version 1.4c
Option 1
Submitted: October 26, 2004

Rogue Wireless Access Points: An Emerging Threat to Corporate Networks

© SANS Institute 2005, Author retains full rights.

Abstract

There is a common analogy that securing a network is much like securing a medieval castle. There should be multiple lines of defenses, such as a moat, thick walls, and a drawbridge. An important thing to remember when securing a castle is to make sure that there are no alternative routes or backdoors to gain entry through. Much is the same when securing a corporate network. Rogue wireless access points can be just the backdoor that an attacker is looking for into a corporate network. With wireless technology becoming more widespread then ever, it is imperative that IT professionals be aware that they can appear on a network, and all of the time spent “securing the castle” will be negated.

This practical looks at the common causes of rogue access points. I will then discuss the dangers that are associated with these access points. Lastly I will discuss steps to detect rogue wireless access points on a network through the use of both freeware and commercial solutions.

Introduction

Wireless technology is spreading as rapidly as ever. “Wi-Fi Hotspots” are popping up all over the map in the most unlikely places. One can surf the Internet while ordering a hamburger at McDonald’s or while sipping their coffee at Starbucks. Wireless is becoming more and more common, which leads most people to believe that it is secure. The common user, more often then not, feels that wireless is just as secure as connecting to a wired network. The danger is that most users are not aware of the security holes that wireless can cause.

The goal of this paper is to discuss the emerging threat of rogue wireless access points, and the damage that they can cause to corporate networks. Whether it is placed by an employee who just wants the convenience of wireless, or an individual with malicious intent, a rogue access point that goes unnoticed can create a gaping hole in a secure corporate network. There are several methods to detect wireless access points that can be used to help secure a network

How Do Rogue Access Points Get In My Environment?

There are two common causes of rogue access points in the corporate environment today. The first is that it was placed there by an end-user. The second is that it was placed by an individual with malicious intent. To a security professional, the source is not always the most important thing. More often, they care concerned with the fact that the security of your network is being compromised by a simple piece of hardware. That may be true, but to truly understand the battle that is being fought you need to examine the source.

End-Users

Wireless LANs have become widespread in today's society. It has become commonplace for people to have their own wireless LANs set up in their homes. Many users also have wireless enabled devices such as laptops and PDAs, and desire to have the same freedom and conveniences in the workplace that they do at home, which may lead to them installing their own access points on the corporate network.

Prices are continually dropping on wireless hardware, which is another influence for end-users to install their own wireless LANs. Wireless access points can be found at local electronics stores or online for as little as \$35, and wireless cards for around \$30 (both depending on the model). To an end user, this is most likely a small price to pay for the vast benefits of wireless.

Ease of configuration is also a contributing factor for employees installing their own access points. Most wireless access points are ready "out of the box" or require minimal set-up. While this ease of configuration may be beneficial to the home user, it is usually detrimental to the corporate environment. The default configuration may work perfectly fine in an individual's house, but is most often lacking the security and configuration needed in a corporate environment. This ease of configuration can also make installing their own wireless access point an attractive option for the end-user. Users may feel that since there is minimal configuration or installation, there is no need for them to wait for the IT department to install an access point for them when they can do it themselves?

The default configuration of most access points does not address encryption; therefore even if an access point is being used by an employee for normal business they could still be transmitting sensitive information over the air. Such sensitive information can be recorded by an attacker running an easily obtainable wireless packet sniffer program. This is a risk especially for densely populated areas. If a company has a location in an office building that is shared with other companies, there is no telling who could be viewing the information contained in the packets that are traveling through the air.

The size of wireless access points can also contribute to the fact that they can be overlooked by IT. Access points are to the point where they can be very small and can be hard to find, even if they are not hidden well. With today's technology, most access points are fairly small and could be hidden behind a plant, books, or even attached under a desk. While a visual search can be done, it may not always yield results. A more thorough approach would be to perform a survey of the location using a wireless sniffer, which will be discussed later in this paper.

Attackers

The other main source of rogue access points is an individual with malicious intent. It is no secret that wireless access points can make entry into a corporate

network all too easy. If an attacker is trying to gain access to a company's network they will more than likely take the path of least resistance, which would be to place an access point on the company's network. In essence, they would be creating their own "back door" to your corporate network, negating the countless hours and dollars spent on hardening your network through firewalls.

There are several methods by which an attacker could connect a wireless AP to a corporate network. Most employees would be vulnerable to an approach utilizing social engineering. If an attacker could gain entry to an office building they could simply walk up to a user and say that they are from the Help Desk and that they need to check the wiring underneath their cubicle. It would only take a matter of minutes to install a small wireless access point underneath the desk, hidden from view. If the user questions this then there are many convincing explanations that could be used, such as "It's a switch which we're going to use in the future to connect additional workstations in the area". Most end users would never know the difference, and as long as they retained connectivity to the network, probably would not complain.

The physical security of a corporate office can also be a factor in defending from rogue access points. If security is lax and an attacker can gain entry, they might not even need to talk to an employee. It would be fairly easy to plant an access point in an empty conference room near the perimeter of the building. One thing to always be on the lookout for is suspicious individuals near the outside of a building. A dead give-away would be if someone is parked outside your building with an open laptop for several hours. Most attackers would be more clever than this, but if they aren't, one should definitely take note.

Dangers of Rogue Access Points

There are many ramifications of having a rogue access point on a corporate network. First and foremost, it can serve as a back door into a company's network. An attacker could gain access to sensitive material all without ever setting foot in the building or having to worry about external firewalls or other security mechanisms. This isn't saying that just because there is an access point on the network that anything and everything could be available. It all depends on the structure of the network and what types of internal security mechanisms are in place as well. Internal firewalls, access lists, intrusion detection systems, authentication systems will all help secure corporate information. The point that is being made is that depending on the configuration of the network, an attacker could by-pass firewalls and other security measures simply by walking or driving to within range of the transmitter.

In addition to being able to access sensitive information on a company's network, an attacker could engage in many other damaging activities. One such activity that could carry potential legal ramifications is if the attacker decided to launch

attacks from an unsuspecting company's wireless network. For instance, if an attacker launched a denial of service (DOS) attack from Company A's wireless LAN against Company B's web servers. Depending on Company A's service provider, there could be potential increase in costs from bandwidth usage during the attack. Not only would there be a financial impact, but it could also damage Company A's reputation. If Company A and Company B are competitors, one could imagine the types of accusations that would be publicized. Such negative publicity in the business world can lead to the loss of millions of dollars in sales or contracts.

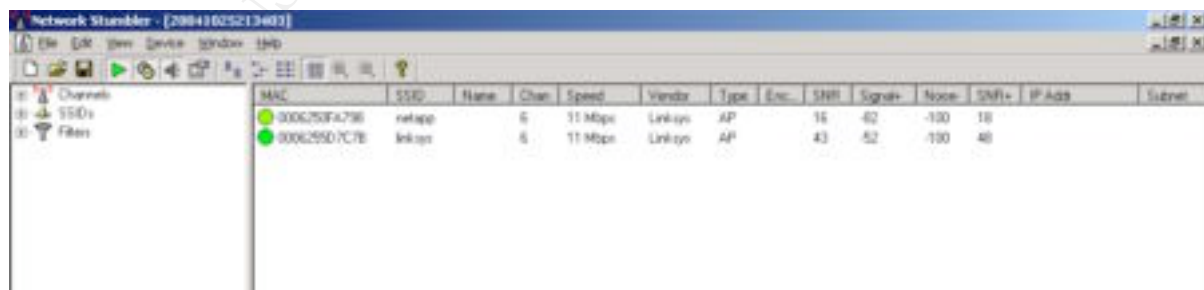
Prevention and Detection

Now that we have discussed what the potential damage is from rogue wireless access points, we will look at the different options for prevention and detection. There are many freeware programs available on the Internet that perform wireless network detection. For users that have a larger budget, there are also many good commercial solutions for detecting rogue access points on a network.

Wireless Sniffers

One of the simplest ways to detect wireless access points is through the use of "sniffer" programs. Sniffers are basically programs that detect the presence of wireless LANs. Depending on the program, information about each access point can be gathered to help identify the location or who the access point belongs to.

One very popular sniffer program is Netstumbler. Netstumbler is a tool that allows users to detect various types of wireless networks. It is a freeware tool that can be downloaded from <http://www.netstumbler.com>. The version tested by the author of this paper was able to detect 802.11a, 802.11b, and 802.11g networks. Below is a screenshot of the various types of information that Netstumbler can provide. It is an easily installable tool that can provide an enormous amount of information on the access points that it detects.



The screenshot shows the Network Stumbler application window. The title bar reads "Network Stumbler - [200410025213403]". The menu bar includes File, Edit, View, Device, Window, and Help. The left sidebar has a tree view with "Channels", "SSIDs", and "Filters". The main pane displays a table of detected access points.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.	SNR	Signal	Noise	SNR+	IP Addr	Subnet
000C75FA2790	netap0		6	11 Mbps	Linksys	AP		16	-62	-100	18		
000C295D7C7E	linksys		6	11 Mbps	Linksys	AP		43	-52	-100	40		

Fig 1: Network Stumbler screenshot, obtained using NetStumbler 0.4.0 (Build 554)

In addition to the full-size version of Network Stumbler, the same website also offers a PDA version, appropriately titled, “Mini Stumbler”. Mini Stumbler runs on the Windows CE platform, and offers most of the same functionality as it’s full-scale relative. The ability to run on a PDA is an added benefit which leads to a more discrete walkthrough.

```

+-----+-----+
| Networks                                     | Info |
+-----+-----+
| SSID                                         | T W Ch | Data | LLC | Crypt | Wk | Flags | | Nturks |
+-----+-----+
| noonian                                     | A Y 04 | 2     | 4146 | 0     | 0   |      | | 12     |
| default                                     | A N 06 | 0     | 49   | 0     | 0   |      | | Pckets |
| cvsretail                                   | A N 11 | 0     | 172  | 0     | 0   |      | | 20033  |
| cvsretail                                   | A N 11 | 22    | 3001 | 0     | 0   |      | | Cryptd |
| default                                     | A N 06 | 0     | 16   | 0     | 0   |      | | 196    |
| access01                                    | A N 06 | 10    | 4932 | 0     | 0   |      | | Weak   |
| default                                     | A N 06 | 29    | 6068 | 0     | 0   |      | | 0      |
| linksys                                     | A N 06 | 0     | 28   | 0     | 0   |      | | Noise  |
| gysealine                                   | A Y 06 | 1     | 860  | 0     | 0   |      | | 297    |
| Brian's Airport Network                    | A N 01 | 0     | 1     | 0     | 0   |      | | Discrd |
|                                             | A N 01 | 243   | 106  | 194   | 0   | A C   | | 328    |
|                                             | A N 01 | 9     | 10   | 2     | 0   | A C   | |        |
|                                             |        |        |      |      |      |      | |        |
|                                             |        |        |      |      |      |      | | Elapad |
|                                             |        |        |      |      |      |      | | 000641 |
|                                             |        |        |      |      |      |      | | H-M-S  |
+-----+-----+
| Status                                     |
+-----+-----+
| Found IP range for " " via ARP 172.25.20.0 |
| Detected new network " " bssid 00:02:2D:00:34:97 WEP N Ch 1 |
| Found IP range for " " via ARP 172.25.0.0  |
| Detected new network " " bssid 00:02:2D:0D:11:CE WEP N Ch 1 |
+-----+-----+

```

Kismet might be a little uncomfortable for Windows users, in that it does not have as easily navigable user interface. It is more of a menu-driven program, with most commands being listed when the 'H' key is pressed. Kismet provides the same useful information as NetStumbler about the access points that it detects.

Author retains full rights.

provide a more accurate picture of the corporate environment. Both tools offer the functionality of recording all of the access points that are found. The results can be output into a variety of different files for analysis after a walkthrough has been performed.

An added feature for both NetStumbler and Kismet is the capability to plot wireless LANs using Global Positioning System (GPS). This functionality requires a handheld GPS be attached to the laptop or PDA being used. As a wireless walkthrough is performed each time an access point is identified, GPS coordinates are input into the log file. After the walkthrough has been completed maps can be generated which will show the coverage areas of each access point that was seen. This can aid in determining whether an access point is physically located at the corporate location or whether it is in a nearby office or building and simply bleeding over.

Wireless Walkthrough

No matter whether you choose NetStumbler or Kismet, both have the capability of gathering the required information to perform a wireless walkthrough. The first step is to load the sniffer program of choice onto either a laptop, or PDA (Mini-Stumbler). It is a good idea to test the software to see if it detects a legitimate access point first. It would be a complete waste of time to walk around the entire location if the wireless card or sniffer program were incorrectly configured.

It is important to remember that the type of wireless card that is in your laptop or PDA will determine what types of access points can be found. If you are using an 802.11b card you will be able to see 802.11B and 802.11G access points, but it will not detect and 802.11A wireless access point (Posey). It is generally a good idea to invest in a combination A/B/G wireless card that can detect all access points running the most common wireless protocols.

An important thing to remember when conducting the walkthrough is to be discrete. Do not announce the fact that you are looking for rogue access points, otherwise employees could simply unplug them. The ideal situation would be to load Mini-Stumbler onto a PDA and perform the walkthrough because it is much less noticeable than an individual walking around with an open laptop.

The basic idea of a walkthrough is to walk throughout the entire corporate location looking for wireless access points that are broadcasting. The sniffer program will record or alert the user when it has detected a new access point. As access points are detected, each one should be analyzed to try and determine whether it is an authorized access point, rogue access point, or an outside source.

As you walk around with either Kismet or NetStumbler running, it will alert you when a new access point is detected. Once a new access point has been detected there are several things that one should look at. First, record the MAC address of the access point. This will allow you to trace it through your wired network if needed. Next, examine the SSID, if it is being broadcast. If it is the name of an access point vendor, such as Linksys, Netgear, etc, then there is a high probability that this access point is “out of the box” and might have been placed by an end-user. Another thing to consider is if your company has a wireless LAN already configured, does the found SSID match the existing SSID?

In addition to the SSID and MAC address, you should also look at several other things, such as the security settings. Does it have WEP or WPA enabled? Again, if there is an existing WLAN, does this access point conform to the company standards? Not only is a wireless walkthrough helpful at finding rogue access points, but it can also help find misconfigured ones as well (Geier, Identifying).

The next thing to look at for each access point detected is signal strength. Many things can affect signal strength. The materials used in a building can severely degrade signal strength, restricting the wireless coverage area. This is another reason why it is important to walk around your entire location and not just the perimeter of the building or office. For each suspicious access point found you should examine the signal strength. One way to try to locate a particular access point is to observe the signal strength as you move in different directions. If it decreases as you move north, try turning around and walking south. You can repeat this process in all directions to try to narrow down your search area. (Geir, Identifying). If it is not possible to identify the exact location of the access point, record the MAC address so that it can be searched from the wired network later.

Another helpful piece of information that both NetStumbler and Kismet provides is a “signal to noise ratio” (SNR) which can aid in determining if the wireless signal is one that is present in your corporate office or if it is originating from outside your location and merely “bleeding” through. SNR is basically a measurement of signal strength compared to the amount of “noise” on that same frequency. When it comes to detecting wireless LANs, the below table illustrates the comparison between SNR and the associated data transmission rates:

Windows Signal Level	Signal to Noise Ratio	Data Rates
Excellent	26 dBm and above	11Mbps
Very Good	25dBm to 21dBm	11Mbps
Good	20dBm to 16dBm	11Mbps
Low	15dBm to 11dBm	11Mbps
Very Low	10dBm to 8dBm	5.5Mbps

Very Low	8dBm to 6dBm	2Mbps
Very Low	6 dBm and under	1Mbps

Source: <http://is.med.ohio-state.edu/Wireless%20FAQ.htm>

Essentially what we are looking for in a wireless walkthrough is for each individual access point that is suspected as being “rogue”, does the it have a high or low SNR. If it has a low SNR throughout the walkthrough, then in all likelihood it is probably coming from an outside source.

While performing a walkthrough with a sniffer program may be the most comprehensive method of detecting a rogue access point, it does have its drawbacks. First, depending on the size of the location, a walkthrough can be very time consuming. As mentioned earlier, it is important that you cover the entire building and not just walk the perimeter. Second, using a sniffer only captures a specific point in time. If an individual were to connect an access point to the corporate network and then unplug it after a week, it would never be detected.

The use of freeware sniffers is a good start for detecting rogue access points. It may not be an accurate depiction of your environment at all times, but it will help detect any that are present at that point in time. Wireless walkthroughs are cheap, and relatively easy to perform. Any company that does not feel they are worth the time or effort better be willing to accept the risk that they might have access points on their network that they are not aware of.

Commercial Solutions

Using wireless sniffers is a good way to detect wireless access points for a given point in time, but for real-time detection and monitoring a commercial solution is something to consider. Not every company can afford to implement a commercial package, but those that can should seriously consider it. There are many packages available today, but for the purpose of this paper we will focus on the Airwave and AirDefense solutions.

AirDefense

The AirDefense RogueWatch solution is a combination of hardware and software that monitors all wireless traffic and detects rogue access points. It monitors wireless activity through the use of AirDefense Sensors which are placed in all of the locations of a corporate domain. The AirDefense Sensors gather information about any wireless activity that they detect, such as wireless access points within range. The sensors “have the capability to monitor 1,000 feet in all directions for most office buildings” (Wells). The sensors relay this information back to a central management console which in turn records all information about a suspicious signal by recording information such as MAC address, IP address, and SSID. The AirDefense system will then notify the appropriate IT individual

with an e-mail indicating that a rogue signal was detected. This type of solution is ideal for a company with multiple locations across great distances.

Below is a diagram which outlines the general setup of the AirDefense RogueWatch solution:

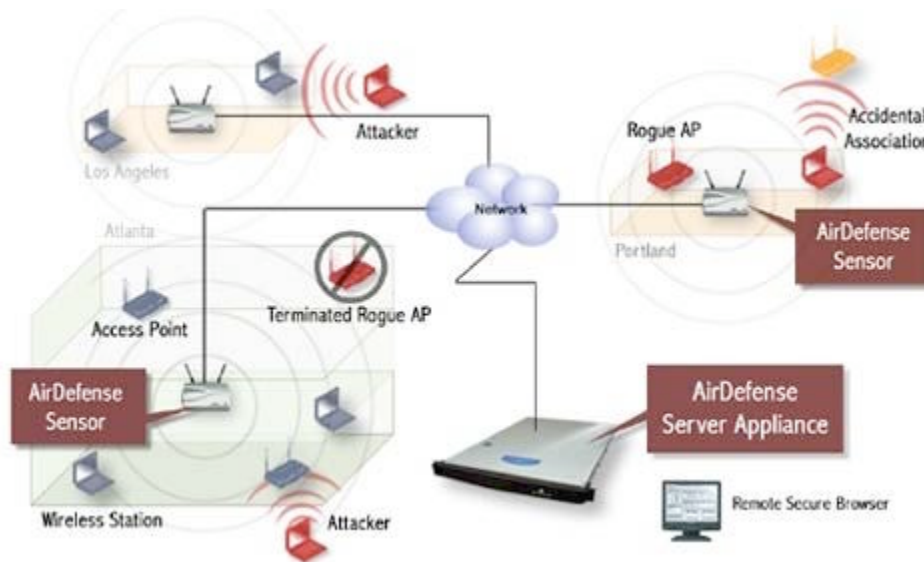


Fig 3: AirDefense RogueWatch, obtained from <http://www.airdefense.net/products/enterprise.html>

AirWave

The AirWave Rogue Access Point Intrusion Detection System (RAPIDS) is another leading commercial solution. The RAPIDS system is different from the AirDefense solution in the fact that RAPIDS uses existing wireless access points to detect rogue access points, rather than using specially designed “scanners”. The RAPIDS system uses existing access points to periodically scan the environment for any rogue signals. In addition to scanning, the RAPIDS system also employs a wired based network scan. It will scan the network looking for specific signatures of wireless devices. Upon discovery it reports information such as “the exact data port to which the rogue AP is connected” in order to help pinpoint its location (Airwave).

Both of these systems would be a valuable layer of defense in preventing and detecting rogue access points on a corporate network. The main difference between the two is in their use of hardware. The AirDefense solution uses specifically designed “scanners” which must be placed in specific locations, while the AirWave solution uses the existing access points. The drawback for the AirWave solution would be that if there is not currently a wireless LAN covering the entire environment, then there is a chance that an access point could go unnoticed by its periodic scans. The AirDefense solution would be a good choice for a company that does not intend to implement its own wireless LAN. Both of

these commercial solutions offer a type of “wired scanning” feature for determining if access points are on the network which combined with the other layers of defense will help detect rogue access points quickly.

Recommendations

The most effective way to detect rogue access points would be to implement a combination of wired and wireless detection. This would mean performing periodic wireless walkthroughs and also using some sort of software based detection methods (depending on budget). In addition to the software management packages listed above there are several steps that any network administrator can perform. Below is a list of steps that are recommended by Christopher Klaus of Internet Security Systems:

- From the wired network an organization could identify unknown and rogue base stations by searching for SNMP agents. The rogue base stations are identified as 802.11 devices through SNMP queries for host ID
- Some base stations have a web and telnet interface. By looking at these interfaces, this provides another method of identifying some 802.11 devices.
- Most TCP/IP implementations have a unique set of characteristics and many OS fingerprinting technologies use this method for identifying the OS type. This concept can be applied to the base stations (Author's Note: *In my personal experience, this can be misleading due to some access points being listed as running the Linux OS which could be confused with legitimate Linux devices*)

Source: http://www.iss.net/wireless/WLAN_FAQ.php

If your company cannot afford to implement a commercial solution, then it is recommended that frequent wireless walkthroughs be performed. One thing to consider when performing walkthroughs is what the extent of your network really is. If a large corporation has a corporate headquarters and also several remote locations, it would be a good idea to review each remote office as well. In an article by Matias Thurman, he discusses a common problem in today's larger organizations: remote offices. It is fairly easy to perform a walkthrough of one location, but if your corporation has multiple remote offices, it is very important that periodic checks of those offices occurs. A rogue access point in a remote location can be just as dangerous as one in the corporate headquarters (Thurman).

A less technical method for combating rogue access points, and one that should be combined with the other methods listed above is end user education. The company should have a clearly established policy on wireless devices. Specifically, it should indicate that wireless devices are not allowed unless approved and installed by a designated member of the IT department. Having a clearly defined policy is important, but just as important is to educate the end

user on why there is a need for such a policy in the first place. It should be made clear to the users that wireless access points can be dangerous if misconfigured and can lead to possible attacks on the corporate network itself. If the dangerous aspects of misconfigured access points are listed out then it can greatly decrease the chances of “user placed” access points popping up on your network.

Conclusion

As a last recommendation, if wireless LANs are implemented in your environment, all possible security precautions should be taken. The bottom line is that wireless is not as secure as wired networks simply because data is being transmitted and anyone can intercept it, even if encrypted. New specifications of 802.11, specifically the recently ratified 802.11i are said to address the security problems associated with 802.11a/b/g. If possible, the most secure standard should be used in the corporate environment, using the most advanced encryption available. Many corporations require the use of VPN to connect their wireless networks, which is also an added layer of security and encryption.

Rogue access points are an apparent threat to any corporate network’s security. Corporations should apply a “defense in depth” strategy when attempting to prevent access points from appearing on their network. Periodic wireless walkthroughs using sniffer applications, commercial solutions, and user education all used in combination should provide a good base for maintaining your existing wireless security and also for preventing rogue access points from appearing. In closing, when securing a corporate network it is always a good idea to fortify the castle so to speak, but the highest walls and best defenses are worthless if there is a backdoor is left wide open.

© SANS Institute

References

AirDefense. "AirDefense Enterprise 4.1" URL:

<http://www.airdefense.net/products/enterprise.html> (14 Oct. 2004).

Airwave. "Enhanced Security through Integrated Rogue Access Point Detection"

URL:http://www.airwave.com/docs/brochures/RAPIDS_070704.pdf (14 Oct. 2004).

Dragorn@Kismetwireless.net. "What is Kismet?" URL:

<http://www.kismetwireless.net/> (14 Oct. 2004).

Garfinkel, Simson. "Sweep Time for Rogue Access Points." URL:

<http://www.csoonline.com/read/100104/shop.html> (3 Oct. 2004).

Geir, Jim. "Identifying Rogue Access Points." June 6, 2003. URL:

<http://www.wi-fiplanet.com/tutorials/article.php/1564431> (9 Sept. 2004).

Geir, Jim. "The Guts of WLAN Security Policy." November 12, 2002. URL:

<http://www.wi-fiplanet.com/tutorials/article.php/1499151> (9 Sept. 2004).

Klaus, Christopher W. "Wireless LAN Security FAQ" October 6, 2002. URL:

http://www.iss.net/wireless/WLAN_FAQ.php (14 Oct. 2004).

Posey, Brien M. "Stop Rogue Access Points from Showing Up On Your

Network." August 6, 2003. URL: <http://techrepublic.com.com/5100-6313-5053779.html> (3 Oct. 2004).

Smith, Del. "Understanding Wireless LAN Protocols and Components" May 2,

2002. URL: <http://www.zdnet.com.au/insight/0,39023731,20265091,00.htm> (9 Sept. 2004).

Wells, Jim. "RogueWatch Does the Watching for You" April 4, 2004. URL:

http://techrepublic.com.com/5100-6263_11-5176405.html?tag=search (14 Oct. 2004).

Thurman, Matias. "Rogue Access Point Leads to Embarrassment." November 3, 2003.

URL:<http://www.computerworld.com/securitytopics/security/story/0,10801,86731,00.html> (27 Sept. 2004).

"Wireless Networking Technical FAQ." URL: [http://is.med.ohio-](http://is.med.ohio-state.edu/Wireless%20FAQ.htm)

[state.edu/Wireless%20FAQ.htm](http://is.med.ohio-state.edu/Wireless%20FAQ.htm) (14 Oct. 2004).