Global Information Assurance Certification Paper

The Difficulty of Detecting Rogue Wireless Access Points on a University or Organization Campus

Anna Grace Zapata
February 5, 2003 (final date of submission)
GSEC Version 1.4b

Abstract:
Wireless Local Area Networks (wireless LAN or WLANs) have become the standards for mobile users around the world. People have found that deploying a wireless LAN is relatively easy and inexpensive either on a personal level or for public or private use (corporate or education).

In theory, deploying a wireless LAN is a great idea. A wireless LAN allows a user all the wonderful features of a typical LAN, minus all the wires and connection hassles. A wireless LAN allows a user to work and play from just about anywhere, just as long as they are within proximity of a wireless access point (wireless AP). This paper will discuss the serious security implications of installing rogue wireless access points, the process of detecting such access points, and the need for prevention and policy as many organization move towards a wireless environment.

Introduction:
An individual may have a couple hundred dollars and wants to be wireless throughout their home or small business. They can go to their local electronic store carrying a few wireless products and purchase them with ease. Once they get their new wireless system home, all they need to do is make the necessary installations and the wireless LAN is up and ready to go (possible rogue wireless access points). Now this is probably just fine for the individual home or small office user, but when a wireless LAN is implemented on a personal level, there are still security implications that must be taken into account.

For the public and private sector (i.e. government, corporate, university, etc…), employees have taken it upon themselves to purchase wireless LAN equipment, bring it to work, and install it on the company network. Many employees feel that there is nothing wrong with installing their own wireless LAN on the corporate network (rogue wireless access points). They are able to be mobile throughout parts of the building without having to be attached to their desk for connectivity. Although there are security implications with the typical home/small office user, the security implications increase vastly when an employee randomly connects his/her wireless equipment to the corporate network.

Unfortunately, many people, including those in Information Technology (IT) departments (both in the public and private sectors), do not understand the grave security issues involving the deployment of wireless LANs. This then brings us to answer the following questions:

- What are the real security implications involved with rogue wireless access points?
- How do IT professionals detect rogue wireless access points on the network?
- Once the rogue access points have been found, what do you do?
- How do you prevent any further rogue wireless access points from being installed on the network?
- How does policy play a role in reducing the number of rogue wireless access points on the network?

Basics:
What is a wireless LAN? What does the term "wireless" mean in the world of technology? A wireless LAN is part of the 802.X family that has been defined by the Institute of Electrical and Electronics Engineers (IEEE). IEEE has categorized wireless technology into the 802.11 family, where the transmission of data will take place over the air "between a wireless client and a base station or between two wireless clients" (webopedia.com). In 1997, the IEEE accepted the specifications for the 802.11 family.

Wireless technology as deemed by the IEEE has been broken into several categories:

- 802.11 – uses 2.4 GHz radio frequencies to transmit data at a rate of 1 to 2 megabytes per second (Mbps).
- 802.11a – uses 5 GHz radio frequencies to transmit data up to 54 Mbps.
- 802.11b – also known as Wi-Fi, is the most readily used wireless technology. 802.11b can provide a transmission rate up to 11 Mbps on a radio frequency of 2.4 GHz. In 1999, the IEEE accepted 802.11b as an Ethernet equivalent.
- 802.11g – uses 2.4 GHz radio frequencies to transmit data at a rate of 20 or more Mbps.

For the purposes of this paper, I will be focusing on the 802.11b wireless technology and it's impact on the public and private sector.

The 2.4 GHz radio frequency for 802.11b works on the same principal as the radio stations we listen to in our car or home stereo. When you listen to the stereo, the receiver in your stereo is able to "pick up" or receive the signals that are being broadcasted from the station's radio tower. The same idea works with your mobile computing device (i.e. laptop, PDA, tablet pc) and a wireless network interface card (NIC). The wireless card you have in your mobile computing device is similar to the receiver in your car radio or home stereo. The access points are similar to the radio towers that are broadcasting the radio signals, thus allowing for your wireless NIC to receive the signal that is being broadcasted and allowing for connectivity.

Problem:
The idea of everyone being able to listen to the same radio station is great. However, this same idea is not such a good one when everyone is able to have access to your wireless access points and obtain connectivity to your network. Unfortunately, without the proper security restrictions being implemented on your wireless LAN, you could be setting yourself up for major problems. Like a radio tower, your access point is broadcasting signals that any passer-by could pick up on by simply using a laptop and wireless NIC to obtain connectivity. Now, this individual may be a harmless person simply looking for a connection to check their email or surf the web. Perhaps they are the students on your campus or an out-of-state businessperson in need of connectivity. However, what do you do about the person who is maliciously looking for an open access point in order to hack your network and wreck havoc on your organization? This leads to the question of how do you supply secure wireless connectivity to those who legitimately need it and how do you keep those who want to cause problems, out?

Unfortunately, this is just half of the problem. The other half has to do with the people within your organization who want wireless and have taken it upon themselves to set up their own wireless LAN on the company network. They go out to the local computer or electronic store and purchase a wireless system, go back to the office and connect the equipment to the network. At this point, you now have what is called a "rogue" access point that could open the door to a whole host of problems. What is worse is that these individuals do not even deploy the simplest security measurements available to them with a wireless access point, called WEP.

WEP stands for Wired Equivalent Privacy, which is a security protocol design for wireless local area networks. In theory, WEP is supposed to provide the same security features that you would see in a wired local area network. WEP strives to provide security by encrypting the data you send, from point A to point B, over radio waves. Unfortunately, WEP is not as secure as once thought since it works at the data link and physical layers of the Open System Interconnection (OSI) model.

The security issue with WEP is that by having such a short initialization vector (IV) (24-bits), which remains constant, WEP will be able to use the same IV for other packets in a short amount of time. Due to this problem, the keystreams begin to look alike, thus giving a hacker enough information to discover the key and decrypt any information over the wire.

Although WEP is not the best security measure for a wireless LAN, it still provides some security by not allowing the SSID of the access point and the MAC address of your laptop to be broadcasted in the open. WEP will also

provide some security against a passer-by picking up on account numbers, passwords, IP addresses, and the like, thus trying to keep out malicious users.

Design of wireless LAN:
The topology for our wireless network, at the University, includes the installation and deployment of Lucent/Orinoco wireless access points around the campus and placing them in strategic locations for maximum connectivity. Along with the wireless access points, high gain antennas are also strategically placed around the campus. These high gain antennas will provide for good wireless reception and connectivity and are an essential part of our wireless network. All of the access points are connected into a single VLAN (virtual local area network), thus sectioning the wireless network off on it's own, from other VLAN's and the network as a whole. By putting the wireless network on a VLAN of it's own, we have implemented one level of security. Should someone gain unauthorized access to the network via the wireless network, it will be more difficult for that individual to navigate through the rest of the network.

Another level of security that was put in place was the use of a Virtual Private Network (VPN). A Cisco VPN Concentrator 3000 was put on this VLAN for further protection. The VPN contains access lists of all those who can gain access to the network via the wireless network. Students, staff, and faculty can gain network access by typing in their identification (ID) number and password. The VPN will then act as a tunnel and help transmit this ID number and password in an encrypted manner from the client to the Remote Authentication Dial-in User Service (RADIUS) to the database that will allow for authentication if the ID number and password are correct. Once authentication has taken place, a secure connection between the user and the VPN has been established and the user now has access to the network.

Wireless AP kit set-up:
Over the past year, there have been several hardware/software tools that have come onto the market in order to help detect rogue wireless access points. Some of these products include Sniffer Technologies by Network Associates, AiroPeek and AiroPeek NX by Cisco, the Distributed Wireless Security Advisor by IBM, and the like. The main objective of these tools is to help your network services and network security team identify that rogue wireless access points do exists on your network and to pinpoint exactly where the access point physically is, on your campus.

For our purposes, we decided to use a shareware program that is free to the public called Netstumbler. Netstumbler easily installs on your laptop or handheld computer. Along with Netstumbler, you also need to equip your laptop or handheld pc with a wireless network interface card (NIC) and some sort of antenna that will provide for better reception of all access points on and around your organization's campus.

I have equipped a laptop with the Netstumbler software that easily installs on any machine with Windows 2000 or Windows XP. Other "stumbling" shareware like Kismet can be used for those with Unix/Linux operating systems, but for this discussion, I primarily focused on Netstumbler and a Windows 2000 based laptop. Along with the Netstumbler software, a "stumbling kit" was purchased for this project. The kit includes an Orinoco Gold wireless card that easily fits into the PCMCIA slot of the laptop, the drivers for the wireless card, and a low-profile antenna with a 5 dB gain that easily attaches to your vehicle for "war-driving" (this will be further discussed as part of my research later in this paper). I also found that www.netstumbler.com to be a useful site with a great deal of helpful information. However, I found the Netstumbler forum to be of the greatest value as I could ask questions and get immediate, informative answers to just about any question.

Detection of Rogue AP's:

On foot:
My first experience was taking the "stumbling" setup out, around the campus. I simply turned on Netstumbler (*note: in order to find rogue access points, make sure your SSID is set to ANY so you have the ability to pick up "any" SSID's being broadcasted in the area) and walked around the campus with laptop and antenna in hand. As I began walking around, I immediately began seeing different wireless names or Service Set Identifiers (SSID) come up on the screen, thus informing me that the relative location I was in, had rogue wireless access points connected to the University network. Unfortunately, walking around with the laptop and antenna was a bit cumbersome. I constantly kept losing the wireless signal and found the laptop difficult to use (and read) outdoors with the sun.

Another downfall from carrying the stumbling kit across campus is weather. The only good time to be on foot with the kit is when it is relatively warm, yet not too sunny. Unfortunately, this does not happen too often. Overall, I would not recommend that you use a laptop-based stumbling kit if you plan on walking around your campus searching for rogue access points. It would be best to have a handheld pc with the appropriate equipment in order to do a more efficient job on foot.

On the Road:
For my second adventure, I decided to go "war-driving". The term war driving means to get in a vehicle and drive around an area looking for wireless connectivity for your personal computing device (laptop or PDA). Your laptop or PDA must be equipped with a wireless card in order to receive a signal for connectivity. Unfortunately, war driving can be very dangerous for an organization who has deployed wireless and is not secure and/or who has rogue access point on the network without prior knowledge.

I placed my laptop in the passenger seat of my car and mounted the antenna on top of the car roof. Within minutes of starting Netstumbler and began driving around the perimeter of the campus, I quickly began picking up a numerous amount of access points that were not associated with the University's wireless network. As I drove around, I consistently picked up rogue access points. After a period of thirty minutes, I had gathered approximately 75 rogue access points, all coming from various parts of the campus and the surrounding area.

Unfortunately, war driving and detecting rogue wireless access points is not an exact science, there is no black and white about the process. When looking for rogue access points, much of the area is grey, especially when it comes to seeing what access points appear on the screen of your laptop. When you are driving around, you know what access points belong to your network and with the help of Netstumbler, you know that rogue access points are also present. However, another problem arises with a University campus that is located in close proximity of various business and homes. How can you tell which access points are rogue on your network and which access points are legitimate points that belong to a nearby business or home. This is where mapping comes into play.

Homing in to the Rogue Access Point(s):
Along with your typical stumbling kit of a laptop or handheld pc, wireless network interface card, antenna, and software, it is essential to have a Global Positioning System (GPS) in conjunction with the rest of your kit. A handheld GPS can be picked up at any local electronic store and can be easily found on the Internet for comparable prices.

A GPS will allow you to pinpoint exactly where the rogue access point is, on your campus. Along with a GPS, you also need mapping software that will assist you in finding various access points, in a particular area. The mapping software allows you and others to view the area you went war driving around and get a good look at the area as a whole, where the access points are located, and how many access points are present. Along with this information, each access point you see on the map also has very specific details associated with that particular point. These details include the name of the access point, if WEP encryption is enabled, the MAC level address, the signal that the access point in coming in on, in dB, and what mode the access point is in.

There are various types of mapping software on the market used for this purpose. Some of the most popular include Microsoft's Map Point, StumbVerter by Sonar Security, GPSMAP that comes with Kismet (the Linux version of Netstumbler). There are also a few web-based logging tools that a war driver or war chalker can use to pinpoint open wireless access points, in a more global manner. These sites include www.wifimaps.com and www.wigle.net; however, there are more web sites being developed that will allow individuals to log their findings.

Unfortunately, these websites open up yet another security hole to a wireless network. If your organization has not fully secured their wireless network, anyone looking for an open access point can easily go to one of these web sites, look for a specific area they want access to, and the next thing you know, they are driving around your campus trying to gain access to your network. You do not want your organization to be compromised in any fashion because a previous war driver found your wireless network to be wide open and put your location on a web site that everyone can see.

You can also use Netstumbler for help in mapping your points. In order to map what you have found, you must export your data and save your findings on your machine. After this, go to the Netstumbler website and use the MapPoint Converter tool that is available to you. Next, put the results that Netstumbler gave you, into a Microsoft Excel spreadsheet so that you can easily transfer your data into MapPoint. You now can import your findings into MapPoint and watch how each access point is placed on a map of the area you were driving in.

Methods of tracking:
There are two main methods used when tracking (and finding) a rogue wireless access point, triangulation and using relative signal strength. In order for triangulation to work properly, a directional antenna, with a narrow range and receiver, is needed. Find an area and scan that region for the strongest signal possible, once that first signal has been found, record it. Next, move your antenna set up and rescan that same area for another signal and record. Using some basic trigonometry, you can find the final position.

Unfortunately, the above method is not fool proof and does not take certain things like obstructions, terrain, temperature, and other factors into consideration. You may see the strongest signal on the screen of your laptop or handheld pc, but that may not be the exact location of the transmission.

A second method for tracking the transmission of an access point is by using the relative signal strength in the area you are scanning. There are two ways to go about finding the transmitter. First, you will need to know the power of the transmitter, the gain of each antenna that is transmitting and receiving a signal, where the power begins to diminish, and the strength of the incoming signal, you should be able to locate the transmitter with to other locations in you sample area.

Prevention and Policy:
The final key to this puzzle of reducing (and hopefully riding) your network of rogue wireless access points is by implementing written policy clearing stating that the private use of wireless access points on the company or university network is strictly prohibited. Through written policy, your Information Technology department has the ability to control what wireless equipment goes

on the network and has a better understanding of the protocols involved when an employee or student violates the policy. A policy of such magnitude should be constructed by a group of knowledgeable people coming from every department within your organization. By including one or two people from every department, you are getting input from every side and making this a well-known policy so that no one is in the dark about the situation.

It is essential that everyone in the organization is aware and has a clear understanding of the implications that rogue wireless access points have on the network. If you do not educate the employees (and/or students) of your organization about the hazards of such devices, they will never fully understand that what they are doing can cause great danger to not only them, as individuals, but to the company/university as a whole. By educating and informing the members of your organization about the potential security implications unsecured wireless equipment can have, you are adding yet another (possibly one of the most important) layers of security to your wireless network.

Conclusion:

Wireless technology is on the forefront of mobile computing. Wireless is providing everyone, from the beginner to the advanced user, an opportunity to have connectivity just about anywhere. In theory and possibly in practice, it is a great idea to have an Internet connection at your fingertips. If you are the typical user who simply wants to connect to the web to check your email or do some surfing, then you really don't pose a risk to any organization's wireless network.

However, what does an organization do about a wireless LAN that they recently implemented and is not sure how secure they really are. What does an organization do about potential hackers that are war driving, war chalking, and such around their campus, looking for an open door into their network to perform malicious activities? With simple tools like Netstumbler, Kismet, Airomagnet, and the like, it has become relatively easy for any malicious user to tap into your organization's wireless network. Although these tools can be used for malevolent purposes, on the same token, they can also be used to safeguard your wireless network.

By having equipment to detect and locate rogue wireless access points, as well as assessing your known access points currently on your network, you are able to safeguard your wireless investment. Not only is it important to implement equipment that helps you detect rogue wireless access points, it is also imperative to have written policy and an educated organization that has a full understanding of the wireless network and the possible security implications the network can face if there are rogue wireless access points present.

Implementing a wireless network is not easy, in fact, it can be a daunting task. However, securing it, is even more complex. Nevertheless, with the proper

strategies in place, a wireless network can be so much more beneficial than ever conceived.

Works cited:

Brewin, Bob. "Sniffing, war-chalking and more: A wireless vocabulary evolves." 17 September 2002.
URL:http://www.computerworld.com/networkingtopics/networking/lanwan/story/0,10801,74321,00.html (13 Jan. 2002)

Chen, Anne. "Sniffing Out Rogue Wireless Lans." 6 May 2002.
URL: http://www.eweek.com/article2/0,3959,7744,00.asp (13 Jan. 2002)

Etter, Andrew. "A Guide to Wardriving and Detecting Wardrivers." 3 September 2002. URL: http://www.sans.org/rr/wireless/wardriving.php (13 Jan. 2002)

Fred. "Wardriving HOWTO (Un-official)." 4 September 2002.
URL: http://www.wardriving.com/doc/Wardriving-HOWTO.txt (13 Jan. 2002)

Geier, Jim. "802.11 WEP: Concepts and Vulnerability." 2002.
URL: http://www.80211-planet.com/tutorials/article.php/1368661 (13 Jan. 2002)

Huey, Benjamin. "Penetration Testing on 802.11b Networks." 24 February 2002.
URL: http://www.sans.org/rr/wireless/test_80211b.php (13 Jan. 2002)

Interlink Networks. "A Practical Approach to Identifying and Tracking Unauthorized 802.11 Cards and Access Points." 2002.
URL: http://www.netsys.com/library/papers/wireless_detection_and_tracking.pdf (13 Jan. 2002)

Netstumbler.com
URL: http://forums.netstumbler.com (13 Jan. 2002)

Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy." 23 January 2002. URL: http://www.sans.org/rr/wireless/netsec.php (13 Jan. 2002)

Webopedia. Wireless Computing. 2002.
URL: http://webopedia.com/Mobile_Computing/Wirelsess_Computing/ (13 Jan. 2002)

Weiss, Jonathan. "Wireless Networks: Security Problems and Solutions." 30 August 2002.
URL: http://www.sans.org/rr/wireless/solutions.php (13 Jan. 2002)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS