Global Information Assurance Certification Paper

Isolating and Securing Wireless LANs

Overview:

Wireless LAN technology (hereafter referred to as 802.11b for 802.11b and 802.11a standards) is one of the more talked about technologies available and thus one of the most wanted. Chances are that some executive in your organization has read about it in some glossy magazine and is hot to have it implemented. It is important to stress to management to move slowly and implement this technology carefully. Wireless technology is not secure and may open a big can of worms. In fact it touches all three fundamental pillars of Information Security:

> *Confidentiality:* are you the only one who is viewing information specific to you?
>
> *Integrity:* are you communicating with whom you think? Is the data you are looking at correct or has it been tampered with?
>
> *Availability:* are the required resources there when you need them?

Administrators and IT security professionals are challenged to build secure foundations for the above pillars when using 802.11b wireless technologies without limiting the beneficial functionality it provides. This paper intends to expand upon some of the concepts already put forth by Lee Elmendorf's paper, "Wireless Networks: Panacea or Next Hacker's Playground" [1] and show how you may create a secure wireless Ethernet network.

802.11b: A Laymen's View

The description in the Cisco Aironet 340 release notes states the 802.11b base station acts “as the center point of a standalone wireless network and as a connection between the wireless devices and the wired LAN network. Wireless devices communicate with a network infrastructure through the base station.”

802.11b is a Radio Frequency (RF) broadcast technology that has a potential data transfer speed of 11Mbs. It is similar to a traditional radio station in the sense that anyone with a radio receiver who is in range of the transmitter / radio broadcast tower will be able to pick up the radio signal.

This is in fact how 802.11b-networking technology works. For our purposes the wireless base station is the transmitter / radio broadcast tower and any 802.11b network card in a PC is a radio receiver (more accurately they are both transceivers which means that they both transmit and receive data).

What does this mean to you're wireless 802.11b network? It means that anyone

with a receiver (wireless network card) within range of your transmitter (wireless base station) is able to potentially compromise your network, use it to attack a remote network or both.

The Dangers:

There are tools today, such as Netstumbler [2], that will not only detect wireless networks within range but will also map exactly where you encountered that network via Global Positioning Systems (GPS). The tactics using these tools are known as warwalking or wardriving. [3] "The concept of "wardriving" is simple: You need a device capable of receiving an 802.11b signal, a device capable of locating itself on a map, and software that will log data from the second when a network is detected by the first. You then move these devices from place to place, letting them do their job. Over time, you build up a database comprised of the network name, signal strength, location, and ip/namespace in use. You may even log packet samples and probe the access point for data available via SNMP." [4]

Going back to the radio analogy, this is similar to the observation of what happens on long car trips. As you leave an area the signal strength of the radio station to which you are listening begins to weaken and get static filled. Eventually the signal is dropped because it is no longer in range. The inverse of this is, as you get closer to a transmitter / radio tower the signal comes in clear as you get closer and the signal strength increases. Eventually you have a perfectly clear signal. Warwalking or Wardriving is simply traveling around and looking for 802.11b RF signals to come into range.

When testing my own wireless Access Point (AP) with Netstumbler, I was able to walk over one city block away and still receive a signal. It wasn't until I lost site of my building that the signal dropped. While doing this test I also picked up signals from four other wireless networks.

What did Netstumbler tell me about these networks? It told me the signal strength, noise level, Service Set Identifier (SSID), Basic Service Set Identifier (BSSID), if it were an Access Point (AP) or set to serve DHCP and if the site was using Wired Equivalent Privacy (WEP) encryption or not. Three of these networks were using default installations and no encryption. All of them were Access Points, which has the potential of exposing the wired Local Area Network (LAN) to my probing. The problems with this are multiple:

A. A hacker could use these networks for attacking a third parties network. Anything traced back would be to the unsuspecting company whose network I was using.

B. Because there was no encryption being used, any traffic being sent via the wireless LAN could be sniffed, allowing an attacker to view any data

being passed on the network.

C. An attacker could easily use the wireless network to compromise computers on the Local Area Network of the host company.

You can now see how Netstumbler is a valuable tool for network administrators and hackers alike.

Another problem inherent with 802.11b technology is that the WEP encryption algorithm is a relatively weak one. AirSnort is a free Open Source program that collects encrypted network traffic then “breaks” the encryption so that data on the wireless network can be viewed. The AirSnort website claims that “AirSnort requires approximately 100M-1GB of data to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second.”[5] This is trivial to the determined hacker.

In addition, the wireless AP is essentially a hub, with all the security risks associated with a hub. All traffic is exposed to easy to monitoring, interception or worse when connected to a wireless LAN.

Defensive Measures

Security best practices and “Defense in Depth” is critical when implementing 802.11b for private networking. The wireless LAN should be considered a hostile Network with unknown, and possibly hostile elements attached. Thus, access should be restricted as much as possible.

Policy should always come first. Think about what people are trying to do when they use the 802.11b network. Do they need Internet access? Do they need access to services on the local wired LAN? In short, plan your implementation and be as restrictive as possible without interfering with your user’s requirements. In addition, educate your users about the possible dangers of using wireless network technology.

Finally, never rely on the basic configuration of the base station if you are connecting to a wired LAN. Default installations and configurations are the security professional’s worst nightmare. Below are some basic areas to give some thought too when implementing your 802.11b network.

1. The MAC addresses of all NICs should be registered with the LAN administrator and the base stations should be set to accept only those MAC addresses. However, because MAC addresses can be spoofed this is an unreliable method on its own. It is just a precaution. Filtering MAC addresses will stop the casual "snooper" but not the skilled cracker.

2. Virtual Private Network (VPN) software should be deployed on the hosts

connecting to the unrestricted LAN segments as well as host based Firewall software. However, because VPN depends on trusting the IP address of the connecting host alone, a compromised machine on the restricted network would be given access to the unrestricted network as well. Thus, username and password authentication should be required to gain access to the unrestricted LAN. In addition to an IPSec based VPN I would also use PGP to encrypt messaging and any text that contains sensitive information if compromised.

3. Access Points should be placed on their own segment or Virtual LAN (VLAN) with a stateful IP filtering firewall separating the restricted wireless LAN and unrestricted "internal" wired LAN.

4. Finally, extensive logging of both the restricted and unrestricted LAN access should be maintained. The network administrators should always know the five "Ws" of their network; who accessed it, when they accessed it, why they accessed it and from where they accessed it. These logs are critical when tracing back malicious activity on your network.

NASA has published a White Paper explaining their solution to almost all of the above problems. [6] They leveraged Open Source Operating Systems and software to develop what they call a Wireless Firewall Gateway (WFG). It is easy enough that anyone with a familiarity with free UNIX systems such as OpenBSD or Linux should be able to implement one using free Open Source code.

Brief Overview of NASA White Paper

NASA's solution is inspired enough for a brief overview here. NASA used OpenBSD as their OS but this could easily be replaced with Linux. Of course the SANS consensus paper, "Securing Linux Step-by-Step," should be followed before deploying this system.

The process works as follows:

1. DHCP is configured on the Wireless Firewall Gateway (WFG). It provides the usual subnet mask, default gateway and name server information. DHCP is configured only to listen on the wireless network. If lease is released for any reason the host is dynamically removed from the Firewall access list.

2. The user is required to authenticate on a Web authentication page. This session uses SSL encryption and provides a front-end to RADIUS authentication server.

3. Stateful IP filtering using OpenBSD's IPF or Linux 2.4.x IPTables/Netfilter. The script that provides web authentication updates the IP filters dynamically upon successful login, thus allowing the provided IP address to access the unrestricted LAN.

4. Further security implemented was to block "clear text" applications, such as telnet, and use ssh for system administration.

Additional Security Considerations

When setting up an Access Point near an exterior wall try turning down the gain. Gain is what controls the signal strength and how far that signal will travel. Unless you are unconcerned about a stranger using your network while sitting in their car at the curb or in the park across the street you should always take this precaution.

Use Netstumbler to test your Network. Know what potential risks there are to your wireless network and where they may come from. This is an easy and fun step to take.

Finally, implement port security on your switch. 802.11b access points are relatively inexpensive now. You don't want just anyone buying a base station and plugging into your network. This is certainly a recipe for disaster.

Summary

How restrictive you make your wireless LAN depends on you're your requirements. Perhaps the idea of a wireless network should not even be entertained. That really depends on the security posture of your organization.

In many senses it is like adding a miniature Internet to your network in the sense that there is an opening for potentially hostile elements. On the plus side you are in control of your wireless network. With proper planning, diligent implementation and vigilant monitoring you can provide a relatively safe wireless LAN for your users without sacrificing the benefits.

1. http://www.sans.org/infosecFAQ/wireless/wireless_net.htm
2. http://www.netstumbler.com
3. http://www.bitshift.org/wardriving.shtml
4. http://www.wardriving.com/
5. http://airsnort.sourceforge.net/
6. http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/index.html

Additional Links

http://wepcrack.sourceforge.net/

http://www.practicallynetworked.com/tools/wireless_articles_security.htm

http://www.byte.com/documents/s=1436/byt20010926s0003/1001_bar.html

http://www.cs.berkeley.edu/~mikechen/classes/fa00_cs294-1_mobile_computing/reverse-firewall.html

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