Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security and the 802.11b Wireless LAN

Wireless networking is quickly spreading across the country and around the globe. Individuals and organizations are finding the simplicity of installation and ease of use to be major benefits. Unfortunately, there is a dark side to the technology. Wireless networking has inherent flaws from a security perspective that places sensitive and private data at risk. This paper seeks to review these issues and make recommendations regarding ways to mitigate the risk and reduce network vulnerabilities.

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Security and the 802.11b Wireless LAN

Sean Griffin
September 16, 2001
GSEC Assignment 1.2f

Wireless networking is quickly spreading across the country and around the globe. Individuals and organizations are finding the simplicity of installation and ease of use to be major benefits. Unfortunately, there is a dark side to the technology. Wireless networking has inherent flaws from a security perspective that places sensitive and private data at risk. This paper seeks to review these issues and make recommendations regarding ways to mitigate the risk and reduce network vulnerabilities.

Wireless Networking Overview

No matter what research organization one chooses to believe, the annual market potential of wireless networking is incredibly huge. Manufacturers are looking at revenues increasing from $771 million in 2000 to as much as $5 billion by 2005.[1] [2] According to Gartner Inc., by 2005, there will be 137 million wireless network users most of whom will be working on corporate systems.[3]

The most common standard for wireless networking and the one with the most momentum uses the IEEE 802.11b protocol. Other standards such as Bluetooth are in the works but 802.11b is enjoying the most commercial success.

Wireless networks can be configured as *ad hoc* peer-to-peer networks where clients communicate directly with each other to share data or as more complex networks that involve the installation of one or more access points acting as bridges that connect the wireless network to the wired Ethernet network. Wireless LAN cards are installed in client workstations, laptops or PDAs that allow the clients to communicate through the access point to the wired network and it's resources.[4]

802.11b uses Direct Sequence Spread Spectrum (DSSS) technology operating in the 2.400 GHz to 2.4835 GHz range and provides theoretical data throughput of 11Mbps though 4-6Mbps is more typical. Nominal range under normal office conditions is from 75 to 150 feet.[5]

It only takes a quick review of the benefits wireless networking via 802.11b provides to understand it's appeal:

- **Reduced infrastructure costs**. Wireless allows for the easy implementation of local area networks without the associated expense of physically installing wires throughout a facility and into areas traditionally difficult to reach such as open areas and conference rooms. The same savings are available to homeowners unwilling to retrofit their homes with network cabling as well as those in homes where retrofits are impossible.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **Roaming ability**. Wireless provides employees with laptops or PDAs the ability to move about a facility while always maintaining connection to the network.
- **Low cost**. Wireless equipment costs are falling quickly as more vendors enter the marketplace. There are nearly 100 vendors of wireless network cards and prices have dropped below $100/card for notebook cards. Wireless access point equipment currently sells for as low as $150.[6]

Flies in the Ointment

Unfortunately, as with any new technology, wireless networking using the 802.11b standard is not without its flaws. Though 802.11b does include built-in security, research has shown that these measures are ineffective and put any organization's data at risk. In addition, there are vulnerabilities associated with the inherent nature of wireless networking that systems administrators must be concerned with and against which preventive measures must be taken. Consider the following:

San Francisco, CA – Matt Peterson, founder of the Bay Area Wireless Users Group, walks around a four-block area of San Francisco with his laptop equipped with a 802.11b wireless card. He finds that he can access six wireless LAN networks that are not his own. In another area he locates eleven additional networks and is able to access one of them in less than ten seconds.[7]

New York, NY – Journalists on a "War Driving" expedition log 481 wireless LAN access points over a period of several weeks.[8]

Auckland, New Zealand – PC World journalist Juha Saarinen spends thirty minutes using a laptop equipped with wireless technology and maps out 18 vulnerable wireless networks.[9]

Silicon Valley, CA – Computer security researcher and consultant Peter Shipley combines GPS equipment, an external antenna, his laptop and his car to map wireless networks throughout the San Francisco Bay Area and Silicon Valley. In less than an hour he has collected vital information on nearly eighty wireless networks. He knows their network names, signal strengths, latitude and longitude and a host of other data. Shipley plans to map the entire area and expects to have information on thousands of networks when he is done.[10]

These activities were all undertaken as experiments to illustrate the inherent dangers associated with the widespread deployment of wireless networks without a comprehensive and clear understanding of the security risks involved. Unfortunately, there are those with less than innocent intentions who can and are taking similar steps to identify and access wireless networks worldwide.

One of the first problems with wireless is that as the name implies, broadcast waves are used to connect network devices. These waves do not simply stop once they reach a wall or the boundary of a business but rather they keep traveling into parking lots and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

other businesses in an expanding circle from the broadcast point. This introduces a risk of unintended parties eavesdropping on network traffic from parking areas or any other place where a laptop can be set up to intercept the signals. While 802.11b standards specify that the range of a broadcast is only 150 - 300', in reality the signal travels much further. Beyond these distances signals are weakened to the point that normal wireless cards cannot detect them with their small antennas. This does not, however, prevent the use of high-gain antennas to detect and analyze these weak signals far beyond the 300' range (vertically as well as horizontally). This is a serious consideration in multi-story buildings. One test in Manhattan led to the detection of 802.11b signals from a business nearly six blocks distant.[11]

With wireless signals clearly not limited by walls or legal boundaries, wireless networks lend themselves to a host of attack possibilities and risks. These can include any or all of the following[12]:

Insertion Attacks – This type of attack involves unauthorized devices being deployed in order to gain access to an existing network. Laptops or PDA's can be configured to attempt access to networks simply by installing wireless network cards and setting up near a target network. If password authentication is not enabled on the network, connection to an access point and network resources is simplified.

Another type of insertion attack is the deployment of rogue access points either by a hacker or by well-meaning internal employees seeking to enhance wireless coverage. Hacker controlled access points can be used to entice authorized wireless clients to connect to a hacker's access point rather than the network's intended access points. In addition, access points not authorized by the network administrator have the potential to be improperly configured and vulnerable to outside attack. This presents the risk of the interception of login ID's and passwords for future direct attacks on a network. The risk can be magnified if rogue access points are deployed behind the corporate firewall.

Denial of Service – The 2.4 GHz frequency range, within which 802.11b operates, is shared with other wireless devices such as cordless telephones, baby monitors and Bluetooth based devices. All of these devices can serve to degrade and interrupt wireless signals. In addition, a determined and resourceful attacker with the proper equipment can flood the frequency with artificial noise and completely disrupt wireless network operation.

Client-to-Client Attacks – A wireless access point is not necessary for two wireless enabled clients to communicate. As such, each client is at risk from the same file sharing and TCP/IP attacks as clients on a wired LAN.

Brute Force Password Attacks – Even when password authentication is implemented on wireless network access points, unauthorized access is still possible through the use of brute force dictionary attacks. Password cracking applications can methodically test passwords in an attempt to break-in to a network access point.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Wired Equivalent Privacy (WEP) Weaknesses – WEP, the built in security mechanism of 802.11b has well known flaws in the encryption algorithms used to secure wireless transmissions. The details of these flaws is beyond the scope of this paper but full details can be found in the following publications: Intercepting Mobile Communications: The Insecurity of 802.11, Your 802.11 Network Has No Clothes and Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.

Misconfiguration – Another problem with 802.11b networks is that the equipment used is designed to allow for ease of installation. For this reason, even though security features may be present, in most cases the default settings are for the features to be turned off in order to allow a network to be up and running as quickly as possible. Network administrators who leave their equipment with the default settings intact are particularly vulnerable as hackers are likely to try known passwords and settings when attempting to penetrate wireless networks.

Interception and Monitoring – An attacker can passively intercept wireless network traffic and through packet analysis determine login ID's and passwords as well as collect other sensitive data using wireless packet sniffers such as those noted below.

Wireless Packet Sniffers – The ease with which intruders can penetrate a wireless network is now being made easier with the release of several software applications that allow intruders to passively collect data for real time or later analysis. Such analysis can lead to the compromise the network. Examples include Airopeek, AirSnort, NetStumbler and WEPCrack.[13] [14] AirSnort is an application that utilizes known WEP flaws to extract the WEP key and allow unauthorized network access. NetStumbler is a full-featured wireless sniffer that logs an extensive array of information about any wireless network it happens to encounter: MAC address of the access point, network name, SSID, manufacturer, channel in use, signal strength, and whether or not WEP is enabled.[15] An intruder looking to attack a target wireless network can make use of all of this information.

Hardware Theft – Should a wireless network device be lost or stolen the person in control of the device could potentially access the network without authorization without the knowledge of network and security administrators. In the event of a theft, the entire network will in some cases need to be reconfigured to eliminate this vulnerability.

What Can Be Done?

Despite the risks and vulnerabilities associated with wireless networking there are certainly circumstances that demand their use. As such there are steps that can be taken to minimize the risks and make hacking a more difficult exercise for potential intruders. Measures that can be taken include any or all of the following:

Changing Default Settings (SSID, etc) – Wireless equipment manufacturers use a default Service Set ID (SSID) in order to identify the network to wireless clients. All access points often broadcast the SSID in order to provide clients a list of networks to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

be accessed. Unfortunately, this serves to let potential intruders identify the network they wish to attack. If the SSID is set to the default manufacturer setting it often means that the additional configuration settings (such as passwords) are at their defaults as well. Good security policy is to disable SSID broadcasting entirely. If a network listing is a requirement for network users then changing the SSID to something other than the default that does not identify the company or location is a must. Be sure to change all other default settings as well to reduce the risk of a successful attack.

Establishing Access Lists – By creating access lists of MAC addresses with permission to access the network an organization can limit the ability of unauthorized clients to connect to the network at will. Unfortunately, if the number of wireless clients is large this has the potential to create significant administration overhead. In addition, since MAC addresses of wireless NICs are transmitted in clear text a sniffer would have little difficulty identifying a known good address that can be spoofed as part of an attack.

Utilize a RADIUS Server – User-based authentication provides a centrally managed method of authenticating users attempting to access the wireless network. A RADIUS (Remote Authentication Dial-in User Service) server provides this functionality and has the ability to handle VPN client authentication as well.

Enable WEP – As mentioned previously, WEP is disabled by default on wireless network equipment. Despite it's known flaws enabling WEP is better protection that nothing at all. It adds an additional barrier to access against the casual "War Driver".

Use VPNs – Many organizations use Virtual Private Networks (VPNs) to allow access to the corporate LAN via the Internet while providing security against unauthorized users. Wireless LANs present another opportunity for VPN use. The wireless portion of the network can be separated from the wired network by a firewall. By configuring the firewall to only pass VPN traffic all other network activity would be stopped thus preventing unauthorized clients from gaining access to the main network. All traffic between the wired and wireless network would take place through the VPN tunnel and would benefit from encryption via the IPSec protocol. IPSec has the advantage of thwarting sniffer attacks utilizing applications such as AirSnort.

Access Point Placement – As part of the initial site survey to determine placement of wireless access points give consideration to placing the equipment towards the center of the building to minimize the strength of wireless signals emanating to the outside world. Avoid placing equipment near windows, which will allow the signal to travel farther and possibly reach unintended receivers.

Proactive Network Sniffing – It is a good practice to deploy network sniffers on a regular basis in order to identify rogue access points that may be providing unauthorized access to the network. Rogue access points might be deployed by employees within the organization or by outside intruders wishing to penetrate the system. As an additional precaution, it is good practice to take measurements external to a facility in areas an intruder might be likely to attempt an attack. It is helpful to know

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

just how far wireless network signals are traveling outside the intended boundaries of a building.

In Summary

Wireless networking is an appealing technology. It is imperative, however, that security and network professionals treat the potential of intrusion and data theft from wireless networks as seriously as they would a wired network. Many of the same precautions and security measures used in the wired world are also applicable in a wireless environment. The deployment of firewalls, VPNs, encryption and hardware security as well as the development of comprehensive security policies and regular network monitoring are all part of an effective wireless security program.

References/Endnotes

[1] Zeller, Tom. "Security Still Up in the Air." Network Computing. February 5, 2001. URL: http://www.networkcomputing.com/1203/1203ws1.html (September 16, 2001).
[2] Manion, Patrick. "Cipher attack delivers heavy blow to WLAN security." EETimes.Com. August 6, 2001. URL: http://www.eetimes.com/story/OEG20010806S0006 (September 16, 2001).
[3] Boulton, Clint. "IBM Ripples Security Waves with 802.11 Wireless Auditing Tool." InternetNews.Com. July 12, 2001. URL: http://www.internetnews.com/infra/article/0,,10693_800221,00.html (September 16, 2001).
[4] Schenk, Rob. Et al. "Wireless LAN Deployment and Security Basics." ExtremeTech. August 29, 2001. URL: http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13521,00.asp (September 16, 2001).
[5] Schenk, Rob. Et al. "Wireless LAN Deployment and Security Basics." ExtremeTech. August 29, 2001. URL: http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13521,00.asp (September 16, 2001).
[6] Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks." ExtremeTech. September 4, 2001. URL: http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13880,00.asp (September 16, 2001).
[7] Albright, Peggy. "With Popularity Comes Security Concerns." Wireless Week. April 16, 2001. URL: http://www.wirelessweek.com/index.asp?layout=print_page&articleID=CA72302 (September 16, 2001).
[8] Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks." ExtremeTech. September 4, 2001. URL: http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13880,00.asp (September 16, 2001).
[9] Saarinen, Juha. "Cracked by PC World." New Zealand PC World. September 3, 2001. URL: http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/D613EE06F6D98222CC256AB5000913CE?OpenDocument (September 16, 2001).
[10] Poulsen, Kevin. "War driving by the Bay." SecurityFocus.Com. April 12, 2001. URL: http://www.securityfocus.com/frames/?content=/templates/article.html%3Fid%3D192 (September 16, 2001).
[11] Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks." ExtremeTech. September 4, 2001. URL: http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13880,00.asp (September 16, 2001).
[12] "Wireless LAN Security, 802.11b and Corporate Networks." Internet Security Systems. 2001. URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf (September 16, 2001).
[13] Mullen, Tim. "In the air tonight." SecurityFocus.Com. August 26, 2001. URL: http://www.securityfocus.com/frames/?content=/templates/column.html%3Fid%3D19%26_ref%3D1081477708%26_ref%3D1564390234 (September 16, 2001).
[14] Associated Press. "Users of wireless beware: electronic eavesdropping is easier than ever." MSNBC. August 24, 2001. URL: http://www.msnbc.com/local/rtroa/m83951.asp (September 16, 2001).
[15] Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks." ExtremeTech. September 4, 2001. URL: http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13880,00.asp (September 16, 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**