Global Information Assurance Certification Paper

802.11b - Wireless Security Issues and Risks
Richard Rampolla
September 18, 2002

1 Abstract

The proliferation of wireless networks is increasing at an astonishing rate given all of the security risks that are associated with this technology. It seems inconceivable that so much wireless connectivity has been implemented in corporate networks without an understanding of the security risks associated with the technology. Given all of the effort to secure networks connected to the Internet via Intrusion Detection Systems (IDSs), Firewalls, and DMZs, it is quite ironic that this technology is providing the ultimate back door to corporate networks.

This paper will provide the reader with a background on 802.11b technology, focusing on the associated security issues and risks. To understand the security flaws, topics such as factory default settings, SNMP management, WEP and SSIDs will be discussed. The reader will be presented with wireless software tools as a means of auditing a network. In addition, the paper will briefly discuss the next wireless standard - 802.1x - that attempts to address some of the security issues that are related to 802.11b. Finally, the paper concludes with recommendations to help eliminate or minimize the security risks found in 802.11b networks.

2 The Technology

2.1 802.11

The Institute of Electrical and Electronics Engineers (IEEE) working group for wireless standards, adopted the first standard in 1997. 802.11 in this case, provided a common standard, which allowed vendors to interoperate.

The current standard that is implemented in most corporate networks is 802.11b. The bandwidth of 802.11b is 11 mbits and operates in the 2.4 GHz Frequency, the same frequency as wireless phones and microwave ovens. Wireless LANs operate on the same principal as wired LANs only they transmit via RF as opposed to electrically. In this case, the RF is the leading problem with security due to the fact the signal cannot be controlled or confined. "The signal is transmitted to anyone who is in proximity to intercept it", (National Infrastructure Protection Center). In the case of wired networks, the transmissions are contained to the copper wires and controlled to subnets and networks with routing protocols and access lists. This is not the case in the wireless networks, since there is no means to keep the RF signal in the corporate building from being propagated outside. Typically, users are located

in all types of office space, from offices with windows on the top floor to users located in sub basement floors. Therefore, to provide wireless access the entire interior of the building needs to have adequate signal strength to reach all offices. In order to provide this coverage to the offices with windows, access points are located in nearby hallways. By locating the access point near windows, the signal will go beyond the window or corporate property, by up to 2,000 feet (Blackwell 2002).

To address the security issues in 802.11b, WEP (wired equivalent privacy) was adopted. WEP is the optional encryption standard implemented in the MAC Layer that virtually all client cards and access points support. After the WEP standard was adopted it was discovered that there was an easy method to crack the encryption and break into the network or client PC, but more on this later.

2.2 Wireless Hardware

There are two pieces of equipment that are found in a wireless network the Access Point (AP) and the client card. The AP, which is also referred to, as a base station is the wireless station that, acts as the gateway between the wired network and the wireless network. The AP is usually configured to run in bridged mode but can also act as a router. "The AP typically, has an IP address assigned to provide remote management and configuration of the device" (Klaus). The AP may have remote management via an SNMP agent, telnet or a web interface.

The client card is typically a PCMCIA card that can be installed into a laptop, PDA or other mobile device. The client card will require software to update the drivers necessary to communicate with the AP. In newer versions of laptops the chips are integrated into the mobile device, thereby eliminating the need for the PCMCIA card. The antenna in this case is built into the device and not visible on the outside as is the card.

2.3 Configurations

There are two types of configurations for 802.11b networks: Peer-to-Peer and Client-Server. For the Peer-to-Peer network there is no need for an Access Point or base station. The typical configuration is two clients communicating with each other with no connectivity to a wired network.

For the client-server topology the Access Point is used to provide connectivity between wireless users and the wired network. The Access Point is the bridge between the corporate wired network and the wireless users. The Access Point is typically connected on the wired side via a 100mbps Ethernet connection. On the RF side of the access point, the device provides 11 mbits to the users on a first come first serve basis. In areas with a high concentration of users it may be necessary to install multiple access points to handle the bandwidth requirements.

3 Security risks found with 802.11b

There are security risks in wireless networking due to the installation of unauthorized equipment factory default settings, and hacking software. This section details the security issues and risks found when implementing or installing wireless equipment.

3.1 Unauthorized Devices

Installing unauthorized devices on the wireless network without going through a security review poses the greatest threat. There are cases of departments and individuals adding access points to the network to provide wireless access. The risk here is that the base station has not been correctly configured or is using default settings, and thereby poses a backdoor to the corporate network. The second case is the unauthorized client that accesses the corporate network. Wireless users have the ability to connect to nearby networks that they are not supposed to have access. For the administrator the best method to mitigate this risk is to perform periodic audits using a freeware tool such as NetStumbler.

3.2 Intercepting traffic

Any wireless client is capable of intercepting and capturing 802.11b traffic. Capturing the traffic only requires the hacker to be within range of the traffic. Utilizing freeware tools such as WEPCrack, Airsnort and NetStumbler makes identifying wireless networks, cracking encryption codes and intercepting traffic quite easy.

The administrator is left with limited options to reduce a hacker's ability to view the wireless traffic. The initial approach should be to reduce the wireless traffic that is propagated outside of the building. To do this, the access points transmitting the signals outside the building need to be identified. Once the access points have been identified the administrator should try relocating them to a different location to minimize the signal strength leaving the building. Implementing a VPN solution is another option but will require a greater undertaking.

3.3 Peer-to-Peer

Since Peer-to-Peer networking is one of the architectures supported in 802.11b there exists the possibility of being attacked by a client. A client must protect itself from another client. The greatest exposure of this threat comes when a mobile user is located in a public location such as an airport. The ability of a hacker to get within close proximity of a mobile device and to gain access to any service on the individuals PC that has sharing enabled is possible. To eliminate this security issue, the laptop should not have the 802.11b client software running when the wireless network is not being used. Also installing intrusion detection software on the laptop such as Zone Alarm or Black Ice would

eliminate exposure to this type of attack.

3.4 Default Configuration

In order to provide a quick and easy installation vendors provide the least secure mode available on the equipment. Leaving the default settings only makes it that much easier for the attacker to gain access to the network. Three major manufactures of base stations all fall into this profile; Agere, 3COM, and Cisco. The three major areas that require the default setting to be changed are in the SSID, the WEP key and the SNMP community strings.

3.5 Blocking

Blocking refers to a user not being able to connect to the network due to congestion. An example of blocking would be the home user that is getting poor throughput because of unauthorized traffic on the broadband connection. Most home wireless networks are installed with factory settings making them vulnerable to unauthorized users – fellow neighbors. The neighbors end up using more bandwidth than the homeowner who gets blocked or has to share the bandwidth with the other neighbors. To eliminate this issue, the home user needs to configure the access point to block connections using MAC address filtering. This would eliminate most neighbors but not the more sophisticated hackers. The manufacturer of the particular device may have additional settings that can be applied to eliminate unauthorized access, please refer to the hardware manual. It should be noted that access points for the home do not always contain all of the security settings that are found in the higher end devices.

3.6 WEP (Wireless Equivalent Privacy)

3.6.1 Background

WEP is the standard adopted by the 802.11 standards body to provide security between wireless nodes, i.e. base stations and NIC cards. WEP is implemented at the MAC layer, Layer 2, to protect the link-level transmission, and relies on a shared secret key. The same key needs to be configured in all base stations and NIC cards in order for the protocol to work. Basically, the transmitting station encrypts the payload of each frame before transmitting using an RC4 cipher. The receiving wireless station decrypts the frame before sending the packet onto the wired side of the network. Therefore, the encryption only takes place on the wireless portion of the network.

WEP is typically disabled by default from the manufacturer. However, if WEP is enabled it has the option of being set to either 40 bit or 128 bit encryption. In most cases public wireless networks leave WEP disabled, whereas in home and corporate networks, WEP may be enabled, but the keys are not frequently changed. Keys are not regularly changed because every access point and NIC

card would have to be reconfigured with the new key. Performing this in a large organization would be a major undertaking.

The WEP protocol was intended to provide three security goals: (Borisov)

1. **Confidentiality** – preventing unauthorized individuals from intercepting the information.
2. **Access Control** – ability to discard improperly encrypted packets, thereby controlling access to the network. Nodes that try to connect to the access point with incorrect WEP keys are rejected.
3. **Data Integrity** – by using an integrity checksum, tampering with data packets is prevented.

3.6.2 WEP Process

1. WEP builds a key schedule or seed by using the shared secret key, (40 or 104bits) and appending a 24-bit initialization vector (IV). This produces the 64 or 128-bit key. The user or administrator of the network configures the shared secret key, and the transmitting node randomly generates the initialization vector. The transmitting node will generate a new key schedule or seed for each frame being transmitted. Thereby ensuring that each packet has a different RC4 key.
2. The seed is then put into a random number generator that produces a key stream the same length as the initial frames payload
3. The data is run through an integrity-checking algorithm to produce a 32-bit integrity check value (ICV).
    a. The receiving station uses this to determine if the data has been tampered.
4. WEP combines the keystream with the payload/ICV through a bitwise XOR process, which produces the encrypted data that gets transmitted.

3.6.3 WEP Vulnerabilities

WEP is vulnerable because of the short initialization vectors and static keys. As mentioned earlier, the key needs to be the same in every device that belongs to the wireless network. For a large corporation, changing the keys in every access point and NIC card environment this is a major undertaking. The flaws with the small IV and the static key in the protocol leave the network vulnerable to passive and active hacking.

Even with WEP enabled, hackers still have the ability to decrypt the

transmissions being sent – confidentiality - and still have the ability to break into the network – access control. Using tools like Airsnort and WEPCrack on a laptop or a handheld makes it very easy to break into a network.

Some manufacturers ship the access points with factory default WEP Keys. This makes it important to change the KEY when first installing the device on the network. There are three important steps to take with regards to WEP:

1. Make sure that it is enabled. Enabling the protocol will deny the casual intruder from accessing the network or intercepting the traffic.
2. Change the WEP key to remove any factory setting.
3. Make sure to periodically change the keys. This will make it harder for the hacker.

3.7 Problems with SNMP

Simple Network Management Protocol (SNMP) is the management protocol that is implemented on most access points and may be enabled on wireless clients. The security issues associated with SNMP are similar to those found on wired network devices. The protocol is vulnerable since it is configured with a default community string from the factory. Knowing the manufacturer of the access point allows a hacker to gain access using the default setting. Most of the major 802.11 equipment vendors ship with a default community string of "public" for read only access. Having access to the management interface of the access point could potentially allow a hacker to gain access to the network.

For the SNMP write community strings, some manufacturers set community string and others require the string to be configured during installation. Table 3.7 represents the factory default settings for the three major manufacturers (Klaus).

Manufacturer	SNMP Read Community String	SNMP Write Community String	Default SSID
Cisco	Public	Configured during setup	tsunami
Lucent/Agere	Public	Configured during setup	RoamAboutDefual t NetworkName
3Com	Public	comcomco m	101

Table 3.7 – Factory Default SNMP Community Strings

3.8 Server Set ID (SSID)

The Server Set ID (SSID) is the ID that allows the wireless user to communicate with the correct base station. The SSID is a configurable parameter that will allow all of the same devices to communicate with one another. For example this could be used to separate different companies where wireless networks overlap. The SSID is configured in both the client and the access point or base station, and acts as a password between both devices.

One of the major security issues regarding the SSID is that the ID is not encrypted even if WEP is enabled. Therefore, the SSID is easily obtained by sniffing the wireless traffic with freeware such as AirSnort. Once the SSID is captured the attacker is that much closer to gaining access to the network.

The other security issue has to due with the factory default setting of the SSID beacon packet. The access point is shipped with SSID beaconing enabled. Having the SSID in the broadcast beacon packets and broadcasting them periodically is a security issue. Freeware tools will be able to passively listen for the beacons and pull the SSID out of the packet. Turning this off eliminates the tools ability to grab the SSID. However, the SSID can still be pull out when a wireless user connects to the access point for the first time. Turning the beaconing off does not eliminate a hacker from gaining access to the SSID, but does slow them down.

Like the SNMP community string the SSID also comes configured with a default setting. Table 3.7 contains the factory default settings for the three major manufactures of wireless equipment.

3.9 802.1x

802.1x is the newer version of the wireless standard passed in 2001 to address the security issues found in 802.11b. The technology tries to incorporate authentication and encryption into the wireless LAN. The 802.1x standard is designed to enhance the security for both wired and wireless networks. The standard is not tied to a particular network scheme, but rather to a technology that defines a means for authenticating a user to a physical network (Connolly).

The standard uses EAP (Extensible Authentication protocol), which is based on PPP. 802.1x maps the EAP to the physical medium, regardless of whether it is Ethernet or a wireless LAN. The protocol working at layer 2 does not let any node onto the network that is not authenticated. The protocol is designed to easily change the wireless encryption keys. This eliminates two of the major problems found in WEP, static keys, and difficulty in updating the keys in all wireless equipment. The standard unlike 802.11b requires the use of authentication servers (Snyder).

802.1x is not as widely deployed due to the availability of products supporting the new standard. In addition, upgrades to access points, client software and authentication servers are required, thus making this a major upgrade.

4 How to improve security with freeware tools

Using the same software that is available to a hacker provides a good approach to auditing a wireless network. Software is available that is capable of locating access points in both passive and active mode, sniffing the wireless transmission to compute the WEP keys, and to grab the SSID all in an effort to gain unauthorized access to wireless networks. Using these same tools to audit the wireless network will reveal it vulnerabilities. Three of the most widely used tools are WEPCrack, AIRSnort and Network Stumbler.

4.1.1 WEPCrack

WEPCrack is a tool that is used to crack the WEP encryption keys of 802.11b networks. The tool is available from http://sourceforge.net/projects/wepcrack, which can be loaded on a Linux box.

4.1.2 AIRSNORT

Airsnort is a tool that recovers encryption keys. It passively monitors transmissions until enough packets have been captured to compute the encryption keys. The tool along with documentation is available from http://airsnort.shmoo.com/ .

4.1.3 Network Stumbler

Network Stumbler Is a tool that is used to actively probe for wireless networks. The tool has the ability to use GPS to visualize the equipment on a map. The tools along with other documentation can be found at http://www.netstumbler.com . In addition to Network Stumbler, there is a new software product out called Mini Stumbler designed for the pocket PC.

5 Conclusion

802.11b networks present the same security risks that are found when corporations connect their private network to the Internet. Yet in many cases, the security policies and architecture defined for the Internet is not applied to the wireless network. Therefore, companies should treat the wireless network similar to the Internet connection. In fact, architecting the wireless network to mirror the Internet connectivity would eliminate many of the issues that were discuss in this paper, especially the issue of confidentiality. Bringing the connection outside the DMZ or firewall and Intrusion Detection Systems leverages the security systems and controls access to the corporate network. In addition, the same VPN technology used to protect connection over the Internet can be utilized in the wireless network.

Finally, regardless of the architecture, both users and administrators must take the responsibility to understand the risk associated with wireless networks,

develop policies and procedures, and regularly audit their networks.

The following recommendation are made to eliminate or mitigate security risks:

- WEP
    - Enable WEP
    - Change any factory default WEP key
    - Regularly change the WEP key
- SSID
    - Change the default SSID to something not associated with you personally or with your company
    - Disable SSID beacon broadcasts
- SNMP
    - Change the default password for the read community string
    - Change the default write community string
- Auditing
    - Engineer the network so that Access Points are in the center of the building and not near the windows
    - Periodically use the tools listed above to audit your network for new access points
- Security
    - Develop an overall security plan for this network architecture
    - Use MAC address filtering
    - Leverage existing security equipment by moving the wireless traffic outside the firewall
    - Leverage Existing authentication servers and VPN
    - Install client intrusion detection software on all mobile devices.

6 References

Blackwell, Gerry. 2002 "Assessing WLAN Security Threats: Part1"
http://www.80211-planet.com/tutorials/article/0,,10724_953481,00.html

Borisov, Nikitia; Goldberg, Ian; Wagner, David. 2002 "Intercepting Mobile Communications: The Insecurity of 802.11 – Draft
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Cigital. 2002 "Wireless Vulnerability FAQ"
http://www.citigal.com/news/wireless/faq.html

Connolly, PJ. March 2002 "The Trouble with 802.1x"
http://www.infoworld.com/articles/fe/xml/02/03/11/020311fe8021x.xml

Extreme Tech. August 2002 "Exploiting and Protecting 802.11b Wireless Networks"
http://www.extremetech.com/article2/0,3973,34635,00.asp

Geier, Jim. 2002 "802.11 WEP: Concepts and Vulnerability"
http://www.80211-planet.com/tutorials/print/0,,10724_1368661,00.html

Janszen, Eric. 2002 "Understanding Basic WLAN Security Issues"
http://www.80211-planet.com/tutorials/article/0,,10724_953561,00.html

Klaus, Christopher. April 2002 "Wireless LAN Security"
http://www.iss.net/wireless/WLAN_FAQ.php

National Infrastructure Protection Center. 2002 "Best Practices for Wireless Fidelity (802.11b) Network Vulnerabilities"
http://www.nipc.gov/publications/nipcpub/bestpract.html

Phifer, Lisa. 2002 "Improving WLAN Security"
http://www.80211-planet.com/columns/article/0,,1781_928471,00.html

Schwartz, Ephraim. February 2002"Researchers crack new wireless security spec"
http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml

Snyder Joel. September 2002, "Wireless Security Options" Network World, Volume19 Number 36, page 51