Concise paper

Wireless network security

Chih-Ta Lin Hira Sathu Donald Joyce

Unitec New Zealand
Auckland, NZ
internetlin@yahoo.com

This paper discusses the security of the wireless networking standard IEEE 802.11b and describes a "war driving" field trial carried out to check the security of wireless networks in Auckland's Central Business District (CBD). The results showed that the built-in security features of the IEEE 802.11b standard were often not configured appropriately and in many cases not even used, making the networks vulnerable to attacks. A geographical positioning system (GPS) was used to record the location of the access points (APs) and could have been used by a hacker to launch specific attacks.

Keywords

Wireless local area network, IEEE 802.11b, war driving, access point, Wi-Fi Protected Access, Extensible Authentication Protocol, Message Integrity Code, Temporal Key Integrity Protocol, Service Set Identifier, Media Access Control, Wireless Equivalent Privacy encryption, IPSec.

1 . INTRODUCTION

In recent years, wireless local area network (WLAN) protocols or solutions have become much more affordable and user-friendly. As alternatives or extensions to wired networks they can provide more flexibility and mobility. However, there are serious concerns about the security of wireless networks, especially those which use the IEEE 802.11b wireless standard. This paper examines the features and security issues of IEEE 802.11b and the results of a "war-driving" field trial that highlighted some significant security loopholes, particularly involving WEP (Wireless Equivalent Privacy) encryption and SSID settings.

2. IEEE 802.11B FEATURES AND SECURITY ISSUES

The built-in security features of IEEE 802.11b include SSID (Service Set Identifier), MAC (Media Access Control) address filtering, and WEP encryption. Unfortunately, many organisations do not make use of the security features (usually to simplify the deployment of the network), which means their networks are unprotected.

2.1 Use of Default Settings

If the security features are left with their default settings, the network is still vulnerable. For example, many administrators use Web interfaces for system configuration via their built-in Web server, which means they only need a Web browser and the IP address of an access point (AP) to manage it. However, the default IP address will be easy for hackers to guess and thus gain access to the AP. Also many APs are set up with "admin" as the administrative login name and without a password, which is like leaving the door open for a burglar! Similarly a hacker could try using "WLAN", which is one of the common default SSIDs.

2.2 Jamming

A wireless network is also vulnerable to "jamming" by a high-powered radio signal generator, whether deliberately or otherwise. The equipment needed is readily available and does not need high-level expertise.

2.3 Lost Equipment

Many desktop computers, laptop computers and PDAs hold important network security information, including MAC addresses, security keys, SSIDs, user names and passwords. If such equipment is lost or stolen, a hacker can use the security information to access the network and create havoc.

2.4 Rogue Access Points

APs deployed by end users without the network administrator's knowledge are known as "Rogue Access Points". They can cause security problems because the end users may have used default settings when attaching the AP to the network (Gast, n.d.). Such an AP, with an easy-to-guess SSID and no WEP encryption or MAC filtering, is a great security risk, especially if fitted with an omni-directional antenna that can transmit sensitive information to any waiting hacker.

2.5 Weak WEP Protection

According to LaRocca & LaRocca (2002), WEP has two major weaknesses: the Initialisation Vector (IV) and the CRC-32 checksum algorithm. A hacker can easily extract information from a WLAN in order to create a "Decryption Dictionary". (Lin, 2003), especially since IVs are always transmitted unencrypted

3. FIELD TRIALS

The first author conducted a "war driving" exercise in Auckland's Central Business District (CBD) in order to establish the number and location of WLANs in the targeted area and find out how many were unprotected (WEP related) and/or insecure (SSID related). The exercise was conducted as follows (Lin, 2003):

- The vehicle (a car) used in this field trial was driven at the speed of no more than 50 Km/hr during the scanning.
- The scanning of WLANs was carried out on every road that was accessible to the vehicle within the defined area.
- The vehicle was driven along both sides of the road for better signal reception.
- All applications and services on the computer were terminated during the war driving except the wireless network scanning software, for technical, legal, and ethical reasons.
- The available wireless connectivity was not utilised in any way.
- The "auto save" function of the wireless network scanning software was enabled to retain collected information in case of system failure.

In order to avoid legal and ethical issues, the guidelines suggested by Duntemann (2003) were followed:

- Do not examine the contents of a network.
- Do not add, delete, or change anything on the network.
- Do not use the network's Internet connection for Web surfing, email, chat, FTP, or anything else.

The field trial had several limitations (Lin, 2003), including:

- Only IEEE 802.11b-based WLANs were scanned.
- WLANs located in high-rise buildings and/or far away from the road may not have been detected.
- Signals may have been absorbed or blocked by walls or other obstacles.
- A vehicle was used as the platform.

It may have been possible to obtain improvements by:

- Using an external high-gain omni-directional antenna mounted on the roof of the vehicle instead of a built-in one to extend the scanning range.
- Scanning on foot, using a MiniStumbler and a PDA, in order to go to places that are not accessible to the vehicle, such as footpaths, and are closer to, or even inside, buildings.

4 DATA ANALYSIS AND RESULTS

4.1 Vendors

Cisco's Aironet was the most widely used product in the scanned area (see Table 1).

4.2 Network Types

A BSS (Basic Service Set) uses an AP to centralise the data communication between stations while an IBSS (Independent Basic Service Set) consists of two or more Wi-Fi enabled computers that communicate with each other directly. The trial identified 212 BSS networks (89.8%) and 24 BSS networks (10.2%).

Table 1: Vendors Identified in the Field Trial

Vendor	Count	Percentage
Cisco (Aironet)	78	33.0%
D-Link	13	5.5%
Agere (Lucent) Orinoco	10	4.2%
Linksys	9	3.8%
Apple	8	3.4%
Askey Computer Corp	7	3.0%
GST (Linksys)	6	2.5%
Compaq	5	2.1%
Enterasys (Cabletron)	5	2.1%
Nokia	5	2.1%
Netgear	3	1.3%
Agere (Lucent) WaveLAN	2	0.8%
Delta (Netgear)	2	0.8%
Gemtek (D-Link)	2	0.8%
3Com	1	0.4%
Accton	1	0.4%
Acer	1	0.4%
Unknown	78	33.0%
Total	236	100%

4.3 WEP Encryption

Slightly more than 60% of WLANs were found to have no WEP encryption enabled - similar to proportion (67.7%) in the third Worldwide War Driving Results (n. d.). Perhaps other security solutions were being used, such as IPSec or Cisco's Lightweight Extensible Authentication Protocol?

4.4 SSID Settings

Using Google and Telecom's online yellow pages we were able to identify 127 SSIDs (53.8%). Another 31 SSIDs (13.1%) were default values and 8 SSIDs (3.4%) were not specified or not broadcast. The remaining 70 SSIDs (29.7%) could not be identified, being either an apparently meaningless series of characters or very general (e.g. "home" or "my_network"). The default SSIDs were identified using Network Stumbler's filtering function and information obtained from http://lleidawireless.net/space/Default+Config about the default settings of access points.

4.5 Different SSID Settings without WEP Encryption

The data under "SSID Count" in Table 2 is taken from section 4.4. The data under "No WEP" is the number of WLANs without WEP out of the "SSID Count". The "No WEP / SSID Count" column shows the percentage of "SSID Count" that had "No WEP". The "Percentage" column shows the percentage of all detected APs and WNICs that had "No WEP".

Table 2: Different SSID Settings without WEP Encryption

SSID	SSID Count	No WEP	No WEP / SSID Count	Percentage
Identifiable SSID	127	73	57.5%	30.9%
Default SSID	31	23	74.2%	9.7%
No SSID	8	1	12.5%	0.4%
Unidentifiable SSID	70	45	64.3%	19.1%
Total	236	142		60.2%

Deploying WLANs without enabling WEP and using default or identifiable SSIDs each contribute to security problems on wireless networks. Doing both compounds the risk. Yet 74.2% of the WLANs that were using the default SSID and 57.5%of those using identifiable SSID had not enabled WEP. Conversely, all but one of the eight WLAN administrators who had concealed the SSIDs had also enabled WEP encryption.

4.6 Other Concerns

The positional data gathered during the field trials could be used by a hacker equipped with a directional antenna to overcome barriers of distance and/or poor reception of RF signal. Such a hacker could use a PDA based scanning system to launch a focussed attack without being noticed.

5 CONCLUSION

Even when its built-in security features are deployed to their full potential, the IEEE 802.11b standard can be broken into by a hacker, using tools that are freely available on the Web. All too often, these security features are not configured appropriately or not even used. Other possible sources of security problems include rogue access points, lost devices, and signal jamming. No single solution can offer protection against all possible attacks, so it is necessary to "fight on several fronts".

The basic protections discussed above would suit individuals and small businesses, being relatively cheap and easy to implement and applicable to most wireless networks. More advanced solutions are available for organisations that have higher security requirements but are more expensive and complex to deploy, usually requiring additional hardware and software. Products designed to secure the new IEEE

802.11i standard should be available in the second quarter of 2004. Meanwhile the The Wi-Fi Alliance has developed a subset of IEEE 802.11i called Wi-Fi Protected Access (WPA) in order to strengthen wireless network security. According to Phifer (2002), The Cable Guy (2003) and Wi-Fi Alliance (2002, 2003), WPA uses EAP (Extensible Authentication Protocol), MIC (Message Integrity Code), TKIP (Temporal Key Integrity Protocol) and a port-based network access control.

The war driving exercise described above showed that more than 60% of WLANs had not enabled WEP encryption and 67% used default or identifiable SSIDs, both of which create significant security risks. These results may not be entirely accurate (because of limitations in the hardware and software used in the exercise) but it is hoped that they will alert businesses in the Auckland CBD and the business community in general to these risks. Further research, in Auckland and other major centres, is needed to monitor the security of WLANs.

REFERENCES:

Duntemann, J. (2003) “Jeff Duntemann’s wardriving FAQ”. Accessed October. 13, 2003, http://www.duntemann.com/wifi/wardrivingfaq.htm

Gast, M. (n.d.) “Seven security problems of 802.11 wireless”. Accessed Jul. 1, 2003, http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html

LaRocca, J. & LaRocca, R. (2002) “802.11 demystified”. U.S.A: McGraw-Hill, p. 158

Lin, C-T. (2003) “IEEE 802.11b-based Wireless Network Security”, Master of Computing Dissertation, Unitec New Zealand.

Worldwide War Driving Results (n. d.) Accessed October. 23, 2003, http://www.worldwidewardrive.org/stats.html

Wwi-Fi Alliance (2002) “Wi-Fi protected access”. Accessed July 11, 2003, http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_ Protected _Access_Overview.pdf

Wi-Fi Alliance (2003) “Securing Wi-Fi wireless networks with today’s technologies”. Accessed August 17, 2003, http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Networks2-6-03.pdf

Phifer, L. (2002) “Understanding wireless LAN vulnerabilities”. Business Communications Review, pp. 26-32

The Cable Guy (2003) “Wi-Fi protected access (WPA) overview”. Accessed September 7, 2003 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0303.asp