

Exploring Wireless Network Security in Auckland City through Warwalking Field Trials

Nurul I. Sarkar* and Abdul H. Abdullah**

*School of Computing and Mathematical Sciences, Auckland University of Technology, Auckland, New Zealand

**Faculty of Computer Science & Information Systems, Universiti Teknologi Malaysia, 81310 Skudai Johor, Malaysia

nurul.sarkar@aut.ac.nz, hanan@utm.my

Abstract— Security is a critical issue in wireless local area networks (WLANs) for many individuals and organizations worldwide, and is one of the main barriers to its adoption in organizations. This paper reports on the current status of WLAN security practices in Auckland's central business district (CBD) through war-walking field trials. It provides an in-depth analysis of field trial data collected since 2004. Our findings show that businesses are adopting more WLANs in recent years than a few years back and the overall growth of WLAN deployment in Auckland CBD is 406% since 2004. We also observed that about 88% of all WLANs detected in August 2010 utilized encryption technology. This shows that an overall 48% increase in the use of encryption protocols since 2004. Finally, we provide guidelines to help businesses in improving their wireless security practices in Auckland City.

Keywords—Wireless security, wired equivalent privacy (WEP), WLAN

I. INTRODUCTION

Wireless local area networks (WLANs) are gaining widespread popularity due to their simplicity in operation, low cost, well-defined standard (e.g. IEEE 802.11b/g) and user mobility offered by the technology. Despite this popularity, WLAN security is one of the main barriers to adoption of wireless technology in organizations. A good understanding of WLAN security issues is required for large scale deployment of such systems.

Detailed discussion of wireless security, in general, can be found in [1-3]. More specifically, Djenouri et. al. [4] provide a comprehensive survey of security issues in mobile ad hoc and sensor networks. Chen et. al. [5] examined WLAN security with a focus on the new IEEE 802.11i standard including security enhancements in encryption and authentication. Shridhar et. al. [6] investigated wireless security issues arising in IEEE 802.11x and 3G networks. A practical guide for deploying Wi-Fi Protected Access (WPA) and WPA2 in the enterprise can be found in [7]. Cai et. al. [8] proposes a set of technical and managerial solutions for organizations to protect their 802.11 WLANs.

Erten and Tomur [9] proposed a layered security architecture for enterprise level organizations deploying IEEE 802.11 WLANs. Lin et. al. [10] report on a field trial carried out to check the security status of wireless networks in

Auckland CBD. The results from the field trial show that, in most cases, the built-in security features of the IEEE 802.11b were not being configured and used properly, making the networks vulnerable to attacks. Hole et. al. [1] also assessed Wi-Fi network security in Bergen, Norway and suggested ways to secure such networks. The experimental results show that most of the 706 wireless networks revealed by war-driving did not use encryption at all. Curran and Smyth [11] investigated the weaknesses of Wired Equivalent Privacy (WEP) protocol in WLANs through field trials in Londonderry, United Kingdom. The authors have conferred on the weaknesses of default WLAN security settings such as WEP and service set identifier (SSID). Various wardriving results are also published in the web sites and open literature [12, 13].

There are various security measures that businesses can adopt to ensure the security of their wireless networks. The techniques that emphasizes in this paper are the enabling WPA/WPA2, 802.11x, MAC address filtering, virtual private network, intrusion detection system, and performing security risk assessment.

The remainder of this paper is structured as follows. Section II describes field trials activities in Auckland CBD. The data analysis and results are presented in Section III. The wireless security guidelines are outlined in Section IV, and Section V concludes the paper.

II. FIELD TRIALS

In 2007, we first conducted a war-walking exercise in Auckland CBD to get some insight into the WLAN security status around Queen Street at the heart of Auckland CBD where most of the retail shops and businesses are located. We repeat the same exercise in August 2010 for comparison and analysis purposes. Figure 1 shows the route of our war-walking field trials.

Using a wireless laptop (802.11b/g card) and a WLAN scanning software called NetStumbler (www.netstumbler.com) we walk along the footpaths from one end of the Queen Street to the other end covering both sides of the street (Fig. 1). The NetStumbler captured all variants of 802.11 networks (e.g. 802.11a/b/g/n) with details

about encryption, MAC address, network SSID, channel, data rate, vendors, and signal-to-noise ratio (SNR).

We looked at whether the detected networks are ad hoc or infrastructure, have used any encryption technology or not, vendor name, and the status of SSID and medium access control (MAC) addresses. These findings are systematically analysed in Section III.

To avoid legal and ethical issues in the field trials data collection, we followed guidelines suggested by Sathu [14, 15]. Basically, we did not examine the contents of the detected networks. No files have been added, deleted, or changed on the networks. We have not use their Internet connections for web surfing, email, chat, FTP, or other unauthorised access.

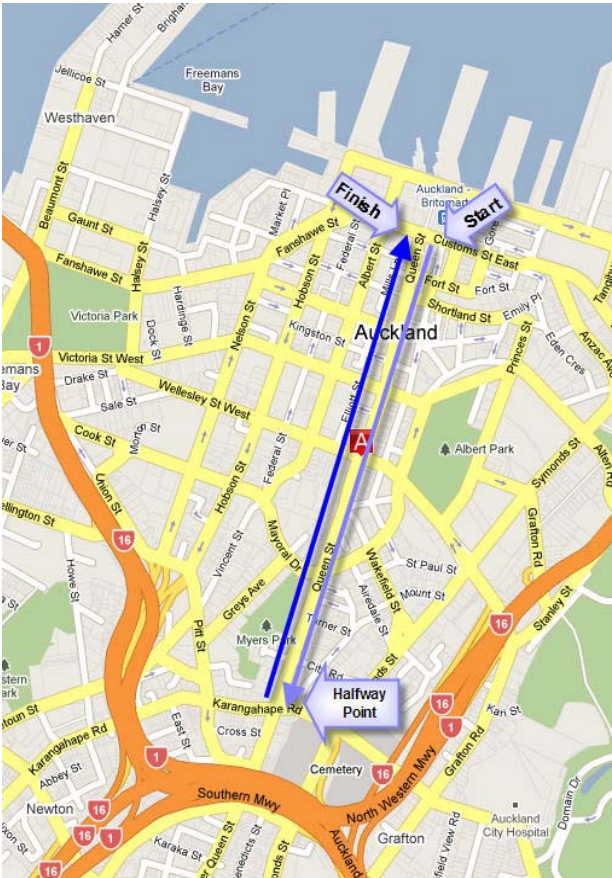


Figure 1. Warwalking field trials route along the Queen Street.

III. RESULTS AND ANALYSIS

A. Vendors

Table I lists the vendors (wireless cards and access points) identified in the field trials during daytime scan in August 2010. The highest number (218 out of 1194) was the Cisco systems followed by Thomson Telecom Belgium. D-Link Corporation was in the third position. However, it is interesting to observe that vendor popularity changes over time. For example, D-Link Corporation was the most popular

vendors followed by Netgear that we found in our previous field trials in 2007. Cisco was in the third position.

As shown in Table I, 82 vendors were not identified by NetStumbler. The rest 131 from various smaller vendors are categorized ‘others’.

B. Network types and deployment

The field trial discovers two types of networks namely, ad hoc and infrastructure (Infra). An ad hoc network consists of two or more Wi-Fi enabled computers that communicate with each other directly without using any access points (APs). An infrastructure network uses one or more APs to control data communications between stations in a centralized manner.

TABLE I. VENDORS IDENTIFIED IN THE FIELD TRIALS (DAY SCAN)

Vendor	Count	Percentage
Cisco systems	218	18.3
Thomson Telecom Belgium	184	15.4
D-Link Corporation	144	12.1
Netgear Inc.	143	12.0
Askey Computer Corporation	86	7.2
Belkin Corporation	50	4.2
Gigaset Communications	34	2.8
Apple Inc.	27	2.3
TP-Link Technology	24	2.0
Lumasense Technologies	16	1.3
Air Link Technologies	16	1.3
Senao Int. Co. Ltd.	15	1.3
3Com	12	1.0
NetComm Ltd.	12	1.0
Unidentified	82	6.9
Others	131	11
Total	1194	100

Table II summarizes network types identified during field trials in 2004, 2007 and 2010. The WLAN deployment growth (in %) since 2007 and 2004 are shown in column 5 and 6, respectively.

We observe that there is a huge growth of infrastructure network deployment in Auckland CBD since 2007. As shown in Table II, the growth of infrastructure networks since 2007 is 141%, and the overall network growth (combined ad hoc and infrastructure) is 136%. The deployment growth is even more significant if we look back to 2004 field trials where only 236 WLANs were detected, and the resulting growth is 406%.

TABLE II. NETWORK TYPES IDENTIFIED

Network type	2004	2007	2010	Growth (%) since:	
				2007	2004
Ad hoc	23	23	31	35	35
Infra	213	483	1163	141	446
Total	236	506	1194	136	406

C. Encryption

Figures 2(a) to (c) illustrate the encryption status of infrastructure networks detected during the field trials (Queen

Street) in 2004, 2007 and 2010, respectively. About 60% of Infrastructure WLANs in 2004, 26% in 2007 and 12% in 2010 have had no encryption enabled. This suggests that there is a gradual improvement in enabling WLAN encryption over the years.

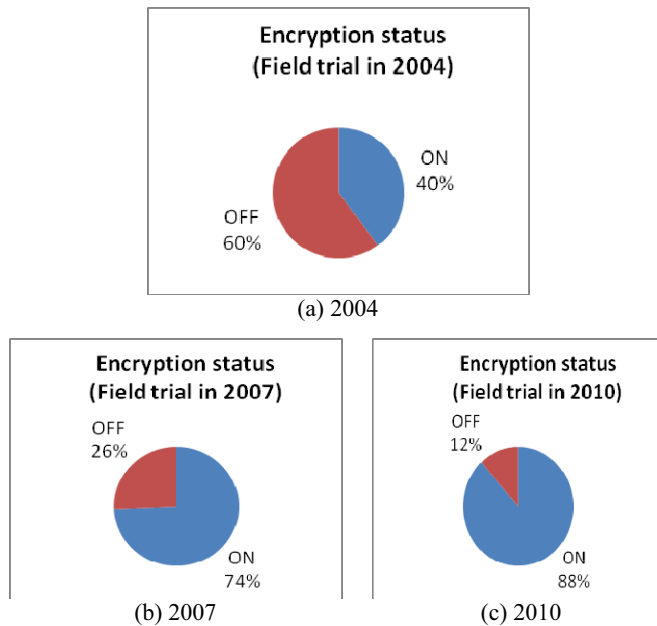


Figure 2. Encryption status of infrastructure networks detected in Auckland CBD

Figure 3 shows the types of encryption technologies identified during the field trials in 2010. About 88% of WLANs were found to have encryption enabled whereas the rest 12% did not use any encryption. Among the 88% encryption enabled WLANs, 71% have used WPA (including WPA2) while the remaining 17% used WEP. This suggests that there is an improvement in using better encryption protocol such as WPA2 in recent years.

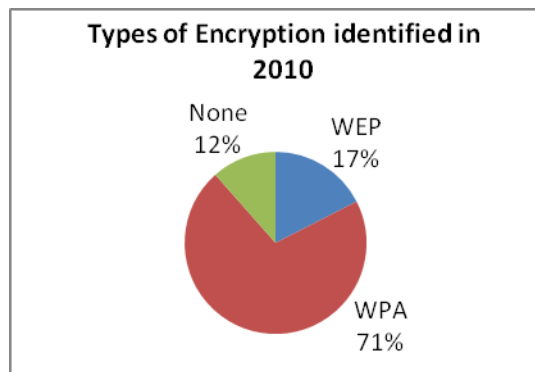


Figure 3. Encryption types identified in 2010

D. Different SSID settings with and without Encryption

The blank, broadcast and default SSIDs discovered during the field trials in 2007 and 2010 are summarized in Table III. The data 'count' shown in column 2 and 5 indicate the total number of SSIDs in each category identified in 2007 and 2010, respectively.

The 'En' (short for Encryption) shown in column 3 and 6 indicate the number of SSIDs count that had Encryption in 2007 and 2010, respectively. The 'No-En' shown in column 4 and 7 show the number of SSIDs that had no Encryption in 2007 and 2010, respectively.

TABLE III. DIFFERENT SSID SETTINGS WITH AND WITHOUT ENCRYPTION

SSID	2007			2010		
	Count	En	No-En	Count	En	No-En
Blank	24	16	8	7	6	1
Broad-cast	404	306	98	1187	1038	149
Default	1	1	0	2	2	0
Total	429	322	106	1196	1044	150
EN: Encryption No-En: No encryption						

We found that about 404 broadcast SSIDs were identified in 2007 in which 306 (i.e. 75.7%) had encryption enabled. In 2010, about 87.5% broadcast SSIDs had encryption. The blank SSIDs with encryption were 66.7% and 85.7% in 2007 and 2010, respectively. The default SSIDs identified in both 2007 and 2010 had encryption enabled. Overall, the wireless security practices in Auckland CBD improving greatly.

We now focus on the SSIDs identified that had no encryption at all. Table IV summarizes SSIDs identified with no encryption during field trials in 2004, 2007 and 2010.

TABLE IV. DIFFERENT SSIDS IDENTIFIED WITH NO ENCRYPTION

SSID	SSID count with No Encryption enabled (%)		
	2004	2007	2010
Blank	64.3	33.3	14.3%
Broadcast	57.5	24.3	12.5%
Default	74.2	0	0
2004: field trial data taken from Lin et al. [10]			

We observe that SSID count (both blank and broadcast) with no encryption enabled decreases significantly over the years. For example, the blank SSIDs identified with no encryption in 2010 is about 50% lower than 2004. There is also an improvement in terms of less number of default SSIDs identified in recent years. This suggests that there is a significant improvement in wireless security practices in Auckland CBD in recent years.

However, by looking at the last column of Table IV, one can observe that about 14.3% Blank SSIDs and 12.5% broadcast SSIDs had no encryption at all in 2010. Deploying WLANs without enabling any encryption technologies contribute to security risks for wireless networks.

E. Other Concerns

The data obtained during war-walking field trials could be intercepted by hackers equipped with a directional antenna to overcome the distance barriers and/or poor reception of radio signals. Such hackers could use a scanning system to launch a focused attack without being noticed. However, to mitigate the wireless security risks and to improve security practices, some guidelines for best security practices are highlighted next (Section IV).

IV. GUIDELINES FOR BEST SECURITY PRACTICES

No single security solution can offer protection against all possible attacks, so it is necessary to follow some guidelines for best security practices. In this section, we provide some recommendations and guidelines to improve wireless security awareness in Auckland CBD. These recommendations are also applicable to individuals and businesses using WLANs around the globe. The four recommendations are as follows:

i) Choose a better encryption technology for WLANs:

It is important for WLAN users and administrators (in case of corporate network) to make sure encryption is turn ON and set up a better encryption protocol such as WPA2. If APs are equipped with 802.11x security standards built-in, then they should also be used as they provide much better security and are well integrated with Windows XP, which has the features of the 802.11x wireless architecture. Network users should be aware of the risks and consequences of their insecure networks and use a better encryption technology to protect their data.

ii) Change the default SSID for improved security: A Service Set Identifier (SSID) is used to identify a network AP. Each AP transmits its own SSID (in the form of clear text) to let the other devices on the network know about its existence. Therefore, it is highly recommended to change the default SSID or disabling it altogether to make it a bit harder for active scanners (e.g. Netstumbler) to discover WLANs.

iii) Limit the MAC addresses to connect to the network: MAC addresses filtering can be used to authorize users to get access into the network. An AP can be configured to provide network access to those wireless nodes who are registered their MAC or IP addresses [11]. Although MAC address filtering might not be very effective for large WLANs containing a large number of APs, but certainly it would be a good protection for small WLANs. Wireless network users should use network monitoring tool such as AirMagnet (www.airmagnet.com) to check for any unusual activity that takes place across the network.

iv) Use a virtual private network for added security: A virtual private network (VPN) provides a secure data communication over the Internet. It is often difficult for a business to stop all users from accessing the network through Wi-Fi hotspots, especially when the users are behind the

company's firewall. VPN would be the best solution for this type of problem because VPN uses encrypted data all the way from wireless nodes to the network (e.g. malicious users would not be able to read VPN encrypted messages).

The organizations can take extra measures by developing and implementing security policy guidelines to protect their corporate WLANs. They can also hire wireless security experts to provide better protection.

V. CONCLUSIONS

By conducting field trials (war-walking) in Auckland CBD, we gain an insight into the current status of WLAN security practices in this area. The research findings are analyzed and compared with previous study conducted by Lin et al. [10]. Our findings show that businesses are using more WLANs in recent years and the overall growth of WLAN deployment in Auckland CBD is 406% since 2004. We also found that about 88% of all WLANs detected in August 2010 utilized encryption indicating that the overall 48% increase in using encryption protocols since 2004. Among the 88% encryption enabled WLANs, about 71% adopted WPA/WPA2 whereas the remaining 17% used WEP. This suggests that there is an improvement in using better encryption protocol such as WPA2 in recent years.

However, about 12% of all WLANs detected did not use any encryption at all. This suggests that there is a room for further improvement in wireless security awareness in Auckland City, especially in the CBD.

This paper provides four specific recommendations for best wireless security practices. Specifically, wireless network users should: (1) choose a better encryption technology for WLANs; (2) change the default SSID name into another name for improved security; (3) limit the MAC addresses to connect to the network; and (4) use a virtual private network for added security. Adopting these suggestions will help businesses to operate their WLANs more securely.

Further research in Auckland City and other major cities in New Zealand, is needed to monitor the security status of wireless networks.

ACKNOWLEDGMENT

We would like to thank Syafnidar, Fadi, and Marselius for carrying out field trials. The financial support provided by the UTM, Malaysia for the presentation of this work is greatly acknowledged.

REFERENCES

- [1] K. J. Hole, E. Dyrnes, and P. Thorsheim, "Securing Wi-Fi networks," *Computer*, vol. 38, no. 7, pp. 28-34, 2005.
- [2] W. A. Arbaugh, "Wireless security is different," *Computer*, vol. 36, no. 8, pp. 99-101, 2003.
- [3] J. W. Branch, N. L. Petroni, Jr., L. Van Doorn, and D. Safford, "Autonomic 802.11 wireless LAN security auditing," *IEEE Security & Privacy Magazine*, vol. 02, no. 3, pp. 56-65, 2004.
- [4] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2-28, 2005.
- [5] J. Chen, M. Jiang, and Y. Liu, "Wireless LAN security and IEEE 802.11i," *IEEE Wireless Communications [see also IEEE Personal Communications]*, vol. 12, no. 1, pp. 27-36, 2005.

- [6] A. Shridhar, D. Joyce, and S. Kolahi, "Security Issues that arise in IEEE 802.11x and 3G wireless networks," presented at the 18th Annual Conference of the National Advisory Committee on Computing Qualifications (NACCQ), Tauranga, New Zealand, July 11-13, 2005, pp. 97-101.
- [7] -----, *Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise*. Retrieved August 15, 2005, from http://www.wi-fi.org/membersonly/getfile.asp?f=WFA_02_27_05_WPA_WPA2_White_Paper.pdf
- [8] Y. Cai and J. Gutierrez, "Reviewing 802.11 wireless LANs security: a case study approach," presented at 18th annual Information Resources Management Association International Conference (IRMA 2007), Vancouver, B.C., Canada, May 19-23, 2007, pp. 324-328.
- [9] Y. M. Erten, "A layered security architecture for corporate 802.11 wireless networks," presented at Wireless Telecommunications Symposium, May 14-15, 2004, pp. 123-128.
- [10] C.-T. Lin, H. Sathu, and D. Joyce, "Wireless network security," presented at the 17th annual conference of the National Advisory Committee on Computing Qualifications (NACCQ), Christchurch, New Zealand, July 7-9, 2004, pp. 337-340.
- [11] K. Curran and E. Smyth, "Exploring the wired equivalent privacy protocol weaknesses in wireless networks," *International Journal of Business Data Communications and Networking*, vol. 1, no. 3, pp. 59-83, 2005.
- [12] *Wardriving results* Retrieved October 17, 2010, from <http://samsclass.info/wardrive/>
- [13] -----, (2010). *Hack Week: War-driving results*. Retrieved October 17, 2010, from <http://pzportal.net/main/2010/05/hack-week-war-driving-results/>
- [14] H. Sathu, "Wardriving dilemmas," presented at 19th Annual Conference of the National Advisory Committee on Computing Qualifications (NACCQ), Wellington, New Zealand, July 7-10, 2006, pp. 237-241.
- [15] E. Montcalm. (2002). *How to Avoid Ethical and Legal Issues In WLAN Discovery* Retrieved October 17, 2010, from http://www.sans.org/reading_room/whitepapers/wireless/