Exploring Wireless Network Security in Auckland City through Warwalking

Syafnidar Abdul Halim

A dissertation submitted to
Auckland University of Technology
in partial fulfillment of the requirements for the degree of
Master of Computer and Information Sciences (MCIS)

2007

School of Computing and Mathematical Sciences

Primary supervisor: Nurul I. Sarkar

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. A good understanding of both the WLAN technology and the security issues is required to assist optimum planning and implementation of such systems. In this dissertation, an experimental investigation of the current status of WLAN security practices in Auckland CBD is reported. In the investigation, a warwalking (field trials) approach is considered.

It is observed that the use of WLANs in Auckland city has increased by 114.41% since 2004. It is also observed that about 74.31% of all WLANs detected on 26th June 2007 utilized encryption technology while the remaining 25.69% did not use encryption at all. This shows that overall 86.56% increase in the use of encryption compared to the data collected in 2004.

Another finding is that 25% of all access points detected are D-Links. There are various security measures that businesses can adopt to ensure the security of their wireless networks. The techniques that will be discussed further in this dissertation are the enabling WEP or WPA, MAC address filtering, virtual private network, intrusion detection system, running network simulation, and performing security risk assessment.

Attestation of Authorship

“I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning."

(Syafnidar Abdul Halim)

Acknowledgements

This dissertation would not be possible without the invaluable support and guidance from various people throughout my academic journey at the Auckland University of Technology. First and foremost, I would like to extend my deepest gratitude to my supervisor, Nurul I. Sarkar for his endless help, stimulating suggestions and valuable discussion in making this dissertation a reality. I would like also to express my hearty appreciation to Krassie Petrova for her appreciable guidance in academic affairs throughout my study and my stay in New Zealand.

I wish to acknowledge the financial support from Universiti Teknologi Mara (UiTM) and Ministry of Higher Education Malaysia through the Skim Latihan Akademik Bumiputera (SLAB).

I would also like to thank all my friends and colleagues in New Zealand for being very supportive and helpful through out my stay and study in this country. Finally, a special thank you to my beloved family, without their unconditional support this and many other accomplishments in my life would not be possible and would mean little.

Table of Contents

List of Figures

List of Tables

Abbreviations and Notations

AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CBD	Central Business District
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hop Spread Spectrum
GUI	Graphical User Interface
ICV	Integrity Check Value
IDS	Intrusion Detection System
ISM Band	Industrial, Scientific and Medical Band
LAN	Local Area network
IEEE	Institute of Electrical and Electronics Engineers
IPSec	Internet Protocol Security
IR	Infrared
IV	Initialization Vector
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
OUI	Organizational Unique Identifier)
P2P	Peer to Peer
RADIUS	Remote Authentication Dial-In User Server/Service
RC4	Ron’s Code 4
RF	Radio Frequency
SSID	Service Set Identifier

SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
UNII Band	Unlicensed National Information Infrastructure Band
VPN	Virtual private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Chapter 1

Introduction

Wireless network security is becoming an important issue for both individuals and organizations worldwide in recent years and is one of the main barriers to its adoption in organizations. A good understanding of both the wireless local area networks (WLANs) technology and the security issues is required to assist optimum planning, design, and deployment of such systems. In 2003, Lin et al. (2004) have conducted a wardriving experiment in Auckland's Central Business District (CBD) to see the security practices of organizations adopting WLANs. The authors reported that over 60% of WLANs have no wired equivalent privacy (WEP) enabled and at least 67% use identifiable default system set identifiers (SSIDs).

The aim of this research is to answer the following research question:
"What is the current status of WLAN security practices in Auckland City?"

By conducting field trials (warwalking) in Auckland's CBD, the current WLAN security practices of individuals and organisations adopting WLANs in this area is investigated. The research findings are analyzed and compared with that of Lin et al. (2004) on the differences that occurs between year 2004 and 2007. Then, based on the results, recommendations are made for further WLAN security improvements..

It is believed that this research findings will help both individuals and organisations in improving their WLAN security practices. In addition, this case study can also be used in the classroom as a real-world example when teaching WLAN security courses.

1.1 The structure of this dissertation

This dissertation consists of six chapters. The study starts with an introduction which outlines the purpose and importance of this research at an abstract level (Chapter 1). Chapter 2 discusses the IEEE 802.11 standards briefly from selected literatures as to understand the basis of this technology, the security measures that are available, the security issues that exist in current WLAN practices, and the researches that have been carried out in understanding the wireless security. Chapter 3 describes the research methodology adopted by this study, and Chapter 4 presents experimental results and analysis of the wireless LAN security status in Auckland CBD. In Chapter 5, the major findings from Chapter 4 are presented from the perspective of system deployment and recommendations are made for the improvement of security practices in businesses. The dissertation is summarized and concluded in Chapter 6.

Chapter 2

Literature Review

2.1 Introduction

In chapter 1, the aim and the structure of this dissertation is discussed. This chapter reviews selected literature in the area of WLANs in general and wireless security in particular. Firstly, this chapter provides an overview of the WLANs architecture. Then the 802.11 standards and the available security features are presented. Finally, the security issues concerning this technology as well researches that have been conducted for WLAN are discussed.

2.2 The WLANs architecture

In general the IEEE (Institute of Electrical and Electronics Engineers) 802.11 WLANs is a set of wireless end nodes (stations) that are positioned within a restricted physical area and are capable of establishing radio communication with each other or with the base stations (access points) (Housley & Arbaugh, 2003). The main characteristics of WLAN technology as often discussed in literatures are the physical layer used , radio band, operating range, data rates, security features, as well as the advantages and the disadvantages of those technologies. An overview of the characteristics mentioned previously is represented in Table 2.1.

The components in WLANs architecture consist of both physical and logical components. The physical components of the WLAN are the wireless end stations (or sometimes referred to as nodes), and the access points (AP). The wireless end stations which include PDAs, laptops, scanners, workstation, and printers are capable of communicating using the 802.11 standards (Gast, 2002). The access point (AP) in the other hand is a device that can function as a relay between nodes that are attached to it. Access Points can also function as a network bridge that connects WLANs to the wired LANs. The logical component of the WLANs includes the basic service set or also known as the BSS. As the logical components of the WLANs architecture, the basic service sets (BSS) will provide the management function to a group of wireless nodes (Housley & Arbaugh, 2003; Laet & Schauwers, 2005).

Characteristics	Description
Physical Layer	DSSS, FHSS, OFDM, IR
Radio Band	2.4 GHz (802.11b and 802.11g) 5GHz (802.11a)
Operating Range	Indoor : up to 150 feet (50m) Outdoor : up to 1500 feet (500m)
Data Rates	54 Mbps (802.11a and 802.11g); 11 Mbps (802.11b); 1 Mbps; 2 Mbps
Security	RC4, WEP, WPA, AES, TKIP
Advantages	Provides mobility; variety of products; wireless at Ethernet speed; cost effective
Disadvantages	Decreasing throughput with load and distance; security issues; vulnerability to attacks

Table 2.1 Overview of the main characteristics of WLANs

Adapted and simplified from original source Karygiannis and Owens (2002), and Panko (2004).

The available BSS configurations are the ad-hoc mode and the infrastructure mode (Laet & Schauwers, 2005). Ad hoc or peer-to-peer (P2P) mode is defined by the Institute of Electrical and Electronics Engineers (IEEE) as an independent basic service set (IBSS) (Curran & Smyth, 2005). This mode allows nodes to directly communicate with each other in a WLAN environment without having to go through access points (APs) (Park & Dicoi, 2003; Tyrrell, 2003). Ad hoc network is a collaborative set of nodes since each node is assumed to relay packets for each other (Farrel, Seigneur, & Jensen, 2004). Ad hoc WLANs can be formed when two or more nodes that wished to communicate are within transmission proximity of each other (Tyrrell, 2003). Each of the nodes in the Ad hoc WLANs are presumed to have equal rights to the network, are of equal importance, and may leave or join the network at any time (Curran & Smyth, 2005). The first advantage of this mode is the simplified, easy and quick WLANs formation by consenting nodes without having to rely on other medium such as AP. The second advantage is in the minimal hardware and network management requirements (Housley & Arbaugh, 2003). The main disadvantage of Ad hoc WLANs is the inability of wireless nodes to connect and communicate with other networks without applying additional routing protocols (Housley & Arbaugh, 2003; Tyrrell, 2003). Figure 2.1a represents the simplified Ad hoc WLANs architecture.

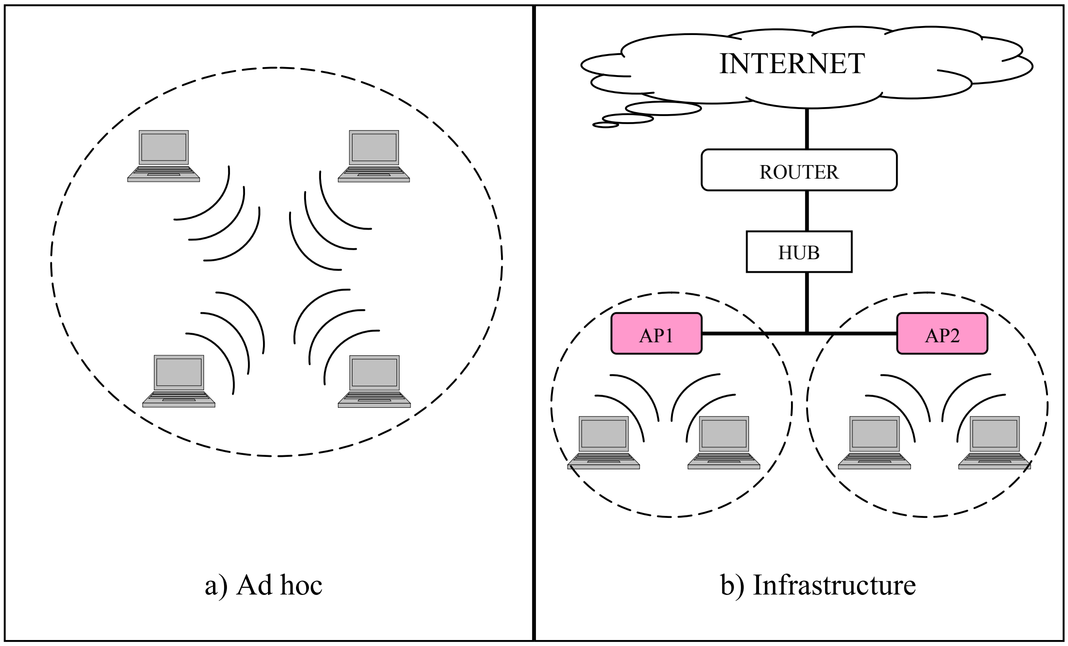


Figure 2.1 WLAN architecture a) Ad-hoc (IBSS) and b) Infrastructure (ESS)

The infrastructure BSS is more popular among the current WLAN users compared to the IBSS (Housley & Arbaugh, 2003). Infrastructure BSS can be used to create WLANs coverage in homes and small offices that have access to the wired LANs. In the infrastructure BSS, the WLANs will comprise of at least one access point (AP) that links to a group of wireless nodes and also to the wired LANs. In the infrastructure mode, the AP acts as an Ethernet bridge for all communications that occurs between the wireless nodes and also for communication that occurs between the wireless nodes and the distribution system (DS) located at the wired LANs (Tyrrell, 2003). The DS is defined as an interconnection networks that combines several BSS to form a single logical network (Schafer, 2003). In the infrastructure WLANs environment, there will exist at least one set of BSS (Arbaugh, 2003; Housley & Arbaugh, 2003). Figure 2.1b represents a simplified infrastructure WLAN configuration where BSS1 and BSS2 are in different background network and are connected to the DS through AP1 and AP2 in order to establish a communication with each other. When two or more BSSs are operating in the same logical network it is called an extended service set (ESS). The ESS configuration provides WLANs coverage at a much wider area, on multi-floors, and in between buildings. The aim of ESS is to provide seamless connection to the nodes when connecting to the network (Curran & Smyth, 2005; Panko, 2004). The main advantages of the infrastructure BSS is the connection redundancy offered by this technology and also a wider transmission coverage (Henning, 2003).

2.3 WLAN Networking Standards

The data rate standards offered by the 802.11 standards include the 802.11a, 802.11b, 802.11g, 802.11i, and 802.11n (Brown, 2003; Panko, 2004; Park & Dicoi, 2003). The following discussion attempts to provide an overview of the IEEE 802.11 standards.
For now, an overview of the IEEE 802.11 standards is presented in Table 2.

Standard	Released Date	Data Rates	Band	Transmission	Security Features	Range	Target Market
802.11 (legacy)	1997	0.5 Mbps	900 MHz ISM	FHSS, DSSS	-	indoor: depends outdoor: ~75m	
802.11a	1999	Up to 54 Mbps	5 - 6 GHz UNII	OFDM	WEP	indoor: ~30m outdoor:~100 m	Home
802.11b	1999	5.5 Mbps and 11 Mbps	2.4 GHz and 900 MHz ISM	DSSS	WEP	indoor: ~35m outdoor: ~110m	Office
802.11g	2003	Up to 54 Mbps	2.4 GHz ISM	OFDM, DSSS	WPA, WEP	indoor: ~35m outdoor:~110 m	Home, office
802.11i	2004	-	-	-	WPA	-	-
802.11n	2008	Max of 540 Mbps	2.4 GHz and/or 5 GHz UNII or ISM	MIMO	WPA, WPA2	indoor:~70m outdoor:~160 m	Home, office

Table 2.2 Overview of 802.11 standards

Adapted and enhanced from original source: (Brown, 2003; Elliot, 2007; Haskin, 2007; Jacobs, 2007; Laet & Schauwers, 2005; Stallings, 2004; Stanley, 2002; Varshney, 2003)

2.3.1 802.11a

The 802.11a was released in 1999 with the main target market being the home users offering possible data rates per channels of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (Stallings, 2004). Though the maximum data rates offered is at 54 Mbps, the actual data rate obtained are often less than that value due to the fact that data rate decreases as the distance between the user and the access point increases (Karygiannis & Owens, 2002). The 802.11a standard uses OFDM (orthogonal frequency-division multiplexing) scheme for transmission (J. Wong, 2003). The IEEE group selected the OFDM technology over DSSS (direct sequence spread spectrum) for its 802.11a standard because OFDM uses spectrum more efficiently than DSSS (Park & Dicoi, 2003). The frequency band for 802.11a standard is from 5 GHz to 6 GHz using the UNII (unlicensed national information infrastructure) band (Park & Dicoi, 2003) with twelve separate non-overlapping channels (Geier, 2002b). 802.11a also uses WEP for data confidentiality and security. One significant problem with 802.11a standards is its incompatibility with the 802.11b and 802.11g standards (Park & Dicoi, 2003).

2.3.2 802.11b

802.11b is actually the first official 802.11 standard introduced by the IEEE (McCullough, 2004). It was introduced in 1999; the same year 802.11a standard was released to the public. The 802.11b is also popular as wireless fidelity or Wi-Fi (Park & Dicoi, 2003). The target market for Wi-Fi is office applications and according to Stallings (2004), the 802.11b standard is the most commonly used wireless standard for commercial network products. In contrast to the 802.11a and 802.11g protocols, the 802.11b technology provides data rates at 5.5 Mbps and 11Mbps (Brown, 2003; Stallings, 2004). 802.11b standard is transmitted through the DSSS technology (Stallings, 2004) with the frequency of 2.4-GHz using the ISM (Industrial, Scientific, and Medical) band (Park & Dicoi, 2003). The usage of the ISM band in 802.11b creates interference problem with other devices that are also using the 2.4Ghz band such as the microwave ovens, cordless telephones, and Bluetooth products (McCullough, 2004).

2.3.3 802.11g

802.11g standard was released in 2003 and is also known as the "Wireless-G" (McCullough, 2004). The target market for 802.11g is the home appliances and office networks (Laet & Schauwers, 2005). 802.11g is also using the 2.4-GHz ISM frequency band as the 802.11b standard (Park & Dicoi, 2003). 802.11g is transmitted using both the OFDM and DSSS schemes and it is offered at data rates of 12 Mbps to 54 Mbps per channel (Stallings, 2004). Due to this, it is backward compatible to 802.11b standard (Park & Dicoi, 2003; Stallings, 2004). The utilization of the OFDM allows 802.11g to obtain a much higher data speed than the 802.11b. However, if a device with 802.11b standard connects to 802.11g access point, the lower 802.11b data rate will be used (Stallings, 2004). A concern with 802.11g as with the 802.11b is the substantial RF (radio frequency) interferences from other devices that are also operating at 2.4 GHz, such as the cordless phones (Geier, 2002b). For security mechanism, 802.11g is using both WPA and WEP protocols (Laet & Schauwers, 2005).

2.3.4 802.11i

The 802.11i was issued in 2004 and it was developed to improve the encryption processes for data transfer, to improve the user authentication methods, and also to improve the key management and distribution processes. These issues are a known problem with previous versions of 802.11 standards (McCullough, 2004). 802.11i standard outlines authentication and confidentiality as the main objective in building a secure and robust 802.11 network (Aime, Lioy, & Mazzocchi, 2004). In 802.11i project, a significant enhancement was implemented on the data transfer and authentication processes, while the key management has been totally redesigned. The new changes provided an added layer of security in the 802.11 wireless networks (Brown, 2003). 802.11i also introduces WPA (Wi-Fi protected access) to ensure a stronger message integrity check and user authentication (Brown, 2003). In addition to the WPA, 802.11i also uses advanced encryption standard or AES to replace the RC4 encryption algorithm (Fogarty, 2005). To make two-way authentication possible in 802.11i, several new keys have been introduced. The first key is the master key or MK which is a private and symmetric key that can assist the authentication between a host and the authentication server (Brown, 2003). The second key is the pair wise master key or PMK which is also a private and symmetric key that will be used by the host and AP to control access to the WLANs (Wexler, 2004).

2.3.5 802.11n

802.11n is still in the development and the expected release date is in 2008. The 802.11n standard is speculated to give WLANs more speed and range with the expected data rates of 100 Mbps to 140 Mbps (Haskin, 2007). Several new technologies and also enhancements to the current authentication and security processes will be introduced when 802.11n is released in 2008. An important technology called "multiple input multiple output" or simply referred to as MIMO will be used as well. MIMO depends on antennas to move multiple data streams, and its data rate increases as the number of antennas increases at both the receiving and sending end (Jacobs, 2007). The advantage of MIMO technology is that it can transmit three streams of data and also receive two streams of data simultaneously. This technique will allow more data to be transmitted at the same time and increases the range for transmitted data. Another technology incorporated into 802.11n is the channel bonding. This technique uses two separate non overlapping channels simultaneously to transmit data. Therefore this technique increases the size of data that can be transmitted at a given time. Payload optimization or packet aggregation is another technology that will be introduced in 802.11n, which allows more data to be stuffed into the transmitted packet (Haskin, 2007). 802.11n products will be compatible with the current 802.11g devices but unfortunately will perform at the lower 802.11g speed (Jacobs, 2007).

2.4 802.11 Security Features

The security requirements of any network is confidentiality, data integrity, authentication, access control, authorization, accountability, routing security, host security and also privacy (Farrel, Seigneur, & Jensen, 2004). In this dissertation, the security features in the 802.11 standards will be discussed in term of the authentication and access control processes that are offered. The techniques and protocols developed in data encryption to ensure confidentiality and integrity will also be discussed in more details.

2.4.1 Entity authentication and access control

Authentication can be performed between wireless nodes in ad hoc wireless networks and also between wireless nodes and the access point in infrastructure wireless networks. In other words, the authentication processes should always be mutual for it to be effective (S. Wong, 2003). A control mechanism to validate a wireless node credentials is also important to ensure the correct level of access can be granted to it by the access point (S. Wong, 2003). One such mechanism is the MAC address filtering. For authentication purposes, there are two schemes available for the 802.11 standard which are the open system authentication, and the shared key authentication (Schafer, 2003).

An easy way to control access to the WLAN is the MAC address filtering. Access points can be set up and configured to only accept connection request from wireless node that have registered its Ethernet MAC address (Varshney, 2003). The filtering can be done by the access point or by a RADIUS (remote authentication dial-in user server) server. By applying MAC address filtering, the access point will have control over wireless nodes access to the networks (Arbaugh, Shankar, & Wan, 2001). MAC address filtering is a useful tools but it may be impractical and difficult to manage if the number of wireless users is too many as in large enterprises.

The open system authentication is the default authentication scheme for 802.11 standards. Arbaugh, Shankar and Wan (2001) mentioned that even though the default authentication protocol for the 802.11 standard is the open system authentication, this protocol however provides absolutely zero security to the established WLANs since it is using a null authentication algorithm. To make it even more insecure, there are only two exchanges of authentication messages in the open system authentication process between the node (requester) and the AP (responder and authenticator). Both messages (the request and the respond) are also sent in clear text without even requiring the correct wired equivalent privacy (WEP) key (Chen, Jiang, & Liu, 2005). This therefore provide no security at all on the identity of the requestor and the authenticator (Schafer, 2003). Figure 2.2 illustrate the open system authentication process.

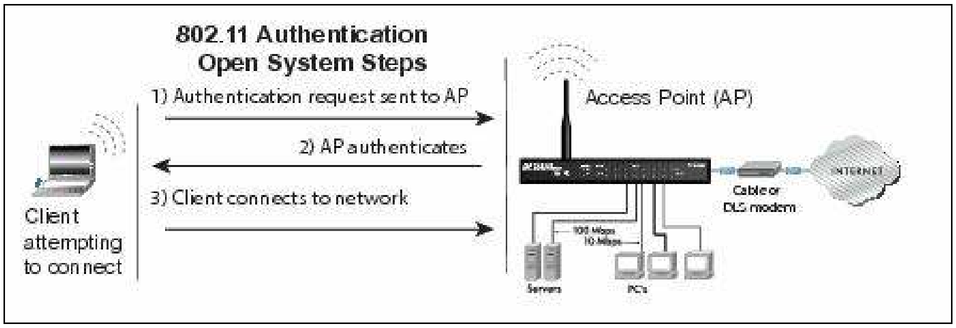


Figure 2.2 802.11 Open system authentication (Netgear Inc, 2005a)

The shared key authentication in contrast to the open systems authentication provides more security to the authentication and association processes in WLANs. In the shared key authentication, four messages will be exchanged between the node and the AP (Chen, Jiang, & Liu, 2005). The first message from the wireless node (requestor) to the AP (authenticator) will only contains the identity of the node. In the second message, the AP will send a challenge packet to the node. Then in the third message the node is expected to decrypt the challenge packet using the shared WEP protocol and send the encrypted file back to the AP. If the encrypted file is correct then the wireless node will be authenticated (Arbaugh, Shankar, & Wan, 2001; Chen, Jiang, & Liu, 2005; Schafer, 2003). To ensure mutual authentication the requestor and the authenticator will switch roles and repeat the process mentioned previously before the node is finally associated with the AP (Arbaugh, Shankar, & Wan, 2001). Though the shared key authentication seemed more secured than the open system authentication, Schafer (2003) argued that the process still provide no security to the identity of the requestor since the authentication data is still sent back and fro is clear text. The third authentication message can be easily eavesdropped by attackers due to the weaknesses of WEP protocol that is used in the process (Schafer, 2003). Figure 2.3 illustrates the shared key authentication process.

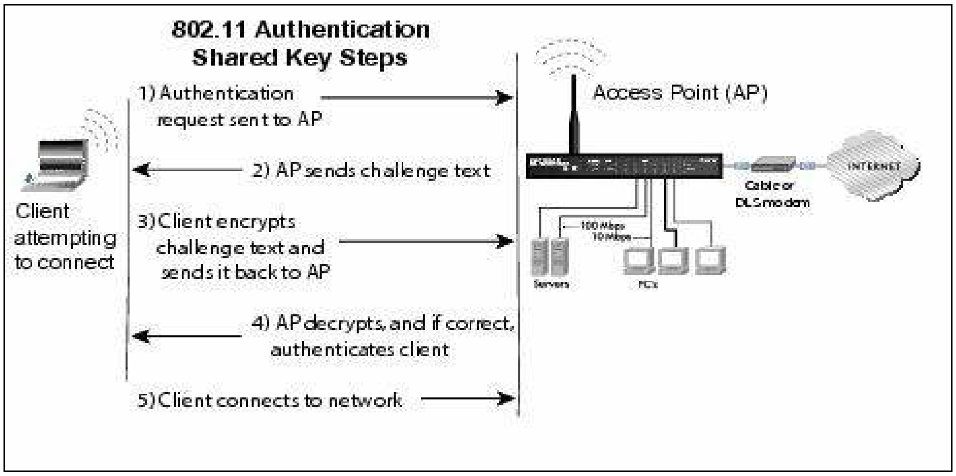

802.11 Authentication
Shared Key Steps
1) Authentication request sent to AP
2) AP sends challenge text
3) Client encrypts challenge text and sends it back to AP
4) AP decrypts, and if correct, authenticates client
5) Client connects to network
Client attempting to connect
Access Point (AP)
Cable or DSL modem
INTERNET
100 Mbps
10 Mbps
Servers
PCs

Figure 2.3 802.11 Shared key authentication (Netgear Inc, 2005b)

2.4.2 Encryption and Data Confidentiality

The implementation of encryption in WLANs is to ensure a security method that can provide both data integrity and privacy. The security method must ensure that all transmitted packets do originate from a real sender and that the data have not been decrypted while intransient by any unauthorized means. This security method must always impose the integrity of data at any given circumstances (S. Wong, 2003). In order to protect the confidentiality and integrity of data transmitted in WLANs, several techniques have been developed such as service set identifier (SSID), wired equivalent privacy (WEP), and also Wi-Fi protected access (WPA).

Every wireless device in WLAN would have a service set identifier (SSID) which is actually a "network name" that is used to identify each APs and wireless nodes in WLANs (Bhagyavati, Summers, & DeJoie, 2004). It is a unique string that is used to identify a network and all users associated with that network (Williams, 2001). By default, SSID is broadcasted in clear text by access points through their beacon messages therefore it is transparent to wireless nodes (Laet & Schauwers, 2005). Due to its nature, the SSID beacon messages from the AP can be easily be picked-up by eavesdropper through 802.11 WLANs active scanner and network analyser such as Netstumbler and Kismet (Hurley, Thornton, & Puchol, 2004; Laet & Schauwers, 2005). Though most access point came with a factory default SSID, it is still changeable. Tyrell (2003) suggested that the newly created SSID should avoid any descriptive and specific information such as the function and also the location of the access point to make it less vulnerable to attacks. Even though Hurley, Thornton and Puchol (2004) as well as Bhagyavati, Summers and DeJoie (2004) suggested that SSID should be disabled in beacon messages to ensure confidentiality and security of the network name, Laet and Schuawers (2005) argued that even though the SSID is disabled, eavesdroppers can still sniff the SSID through the probe response frames from the AP thus making SSID a weak mode for security and privacy.

Another protection to the WLAN is the wired equivalent privacy protocol or for short, the WEP protocol. WEP is developed to ensure data confidentiality, access control and data integrity at the link-level during 802.11 WLANs transmissions (Borisov, Goldberg, & Wagner, 2001; Laet & Schauwers, 2005). WEP development is to thwart eavesdropping, unauthorized and rogue access, and also data modification. The WEP protocol relies on a secret key that is used or shared by the clients and the APs. The function of the secret key is to encrypt packets before they are transmitted to the recipients (Tyrrell, 2003; Williams, 2001). Data confidentiality through WEP protocol is achieved by using the RC4 algorithm for data encryption (Housley & Arbaugh, 2003). RC4 algorithm is a stream cipher that expands the secret key into a long key streams of pseudorandom bits (Borisov, Goldberg, & Wagner, 2001). For data integrity, the CRC-32 algorithm is used by the wireless receiver (AP or nodes) to compute the integrity check value (ICV) of the transmitted data to ensure no tempering have been performed while that data is intransient (Geier, 2002a; Stubblefield, Ioannidis, & Rubin, 2004). The usage of RC4 and CRC-32 algorithm however are still insufficient to ensure the achievement of WEP security goals (Cam-Winget, Housley, Wagner, & Walker, 2003).

Borisov, Golberg and Wagner (2001) in their study mentioned that the inherent flaws in WEP protocol resulted from incorrectly using the RC4 stream cipher and also for choosing the CRC-32 as a data integrity algorithm thus renders WEP from providing the anticipated security goals. Agreeing to the mentioned WEP flaws, Stubblefield, Ioannidis and Rubin (2004) also added the specification of initialization vector (IV) selections, and the lack of key management as the main flaw of WEP protocol. In a high traffic WLAN environment, the usage of a relatively small IV would caused it to be repeated for more than once during a day which then makes it fairly easy for an attacker to evade the encryption process (Geier, 2002a; Woodward, 2005). Wi-Fi Alliance (2004) mentioned that an intruder or attacker with enough data can threaten a WEP protected network in three ways. The first way is by intercepting and decrypting the data while it is being transmitted. Secondly the network can be threatened by intruders modifying the data that is being communicated. Lastly, the intruder can deduced and forged the WEP key to gain unauthorized access to WLANs (Cam-Winget, Housley, Wagner, & Walker, 2003; Wi-Fi Alliance, 2004). Schafer (2003) explained that four other areas of security flaws in WEP which are the insufficiency of protection against messages that can be read by unauthorized users, the insecurity of data authentication and the lack of data integrity protection, the insufficient access control that validates user credentials, and finally the weakness of using key computation that is based on eavesdropped messages (Schafer, 2003). Despite all the flaws present it WEP protocol, WEP still provides a minimum level of security to WLAN (Geier, 2002a) and will discourage amateur attackers.

Another important security measure, WPA or Wi-Fi protected access addresses all known security issues of WEP therefore enhanced wireless security. WPA is not only providing stronger data encryption than WEP, it also added user authentication to the process (Loeb, 2005). WPA is developed to provide security to all versions of 802.11 devices which includes 802.11a, 802.11b, and 802.11g. WPA is both forward and backward-compatible with all 802.11 standard and is designed to run on the current available wireless devices as a software download (McCullough, 2004). WPA employs the 802.1X authentication, the extensible authentication protocol (EAP), and uses the temporal key integrity protocol (TKIP) for encryption (Wi-Fi Alliance, 2004). There are many security advantages of implementing WPA as compared to the WEP protocol. The first advantage of WPA is the mutual authentication mechanism which provides a much stronger network access control than WEP. Secondly, WPA protocol supports superior security technologies like EAP, RADIUS, 802.1X and pre-shared keys. WPA also implements the dynamic keys in TKIP in order to enhanced key management. The usage of "Michael Message Integrity Check" also enforces data integrity in WPA. However, there are still some possible security issues regarding WPA such as the probability of encryption weaknesses in TKIP and the decreasing WLANs performance due to a computational intensive of a more difficult encryption and authentication processes (S. Wong, 2003).

2.5 WLAN Security Issues

The WLANs technology has been around for more than ten years and during this period it has gone through tremendous advancement and growth. This however also open up the technology to various security attacks; for example, MAC address spoofing, rogue access point, denial of service (DoS), jamming attacks and also man-in-the-middle attacks (Curran & Smyth, 2005). The security problems associated with WLANs have become a barrier for some organization in implementing the WLANs technology (Erten & Tomur, 2004; Hole, Dyrnes, & Thorsheim, 2005). Developing a good understanding of both the technology and the possible security issues concerning WLANs deployment is essential to fully utilized and gain benefits from this evolving technology.

2.5.1 Security attacks on WLANs

There are many types of attacks targeted at WLANs which includes the passive attack, active attack, denial of service attack, man in the middle attack, and rogue access. These security attacks concerning WLANs will be discussed in more details.

2.5.1.1 Passive Attacks

Passive attack is described as the action of passively eavesdropping on the WLANs traffics (Xia & Brustoloni, 2005). This attack may be done fairly easily by using a few networks analysis tools that can be downloadable from the Internet such as the Netstumbler, Kismet, and Airsnort (Shimonski, 2003). Information that can be gathered through these software includes the MAC address, the IP address, the association ID for the station, and the SSID of the networks (Corbett, Beyah, & Copeland, 2006). Wong (2003) explained that passive attacks sometime could occur when someone unintentionally accessed a different network while trying to connect to an access point. Passive attacks could also be used to explain the activity of connecting to a network but without changing or using any resources in that network. This may include eavesdropping, traffic analysis and wardriving (Maple, Jacobs, & Reeve, 2006).

Passive attacks are mostly undetectable by network administrators and physical network devices due to the passiveness of this activity (Curran & Smyth, 2005; Welch & Lathrop, 2003).

2.5.1.2 Active Attack

Shimonski (2003) stated that the activity of passive attacks could accumulate enough information leading attackers to actively attack a wireless network. The main target of active attackers is usually to gain access to a network and then change or modify the resource's content (J. Wong, 2003). Two activities that can be categorized as active attacks are unauthorized access and spoofing (Shimonski, 2003). Active eavesdropping requires injection of data by the attacker into the communication session in order to decipher the payload. In this process, the attacker will listens to the wireless connection while actively injects messages into the communication session in order to determine the contents of the messages. Active attacks can happen in two ways, the first is when the attacker modifies a packet. Secondly is when the attackers inject completely new packets into the data stream (Welch & Lathrop, 2003). Actively attacking the network can caused the denial of service attack to the WLAN.

2.5.1.3 Denial of Service (DoS attack)

The denial of service attack or sometimes referred to as DoS attack is an effort by attackers to make a computer resource unavailable to its anticipated users. The seriousness of this attack is it can cause the network to slow down to a point of being unusable (Maple, Jacobs, & Reeve, 2006). Even though the motives for DoS attacks, the means to conduct it, and the targets of such attack varies, it still involves a rigorous and malicious efforts by the attacker (s) trying to prevent the WLANs services from functioning properly (Carli, Rosetti, & Neri, 2003). Woodward (2005) explained that the attack can be attempted in two ways. The first way to conduct the DoS attack is through the jamming technique which is quite easy to implement and not easily detected. This attack can cause serious interference to the WLAN when done intentionally or unintentionally such as placing a device that operates at the same frequency in the same area as the WLANs. The second way for DoS attack to be done is by exploiting the authentication and encryption weaknesses that exist within the 802.11 itself (Aime, Lioy, & Mazzocchi, 2004). In this attack the wireless node is forced to rejoin the WLANs where the logon and authentication details can be captured while the node is re-associating itself with the AP. The information gathered from this attacks can also lead to another problem, the man in the middle attack (Woodward, 2005).

2.5.1.4 Man in the middle attack

This man in the middle attack is achieved by inserting a malicious station in between the wireless node and the access point. By doing this, the attacker act as the man in the middle, impersonating the real AP to the node, and at the same time impersonating the real node to the AP (Maple, Jacobs, & Reeve, 2006). Man in the middle is a real-time attacks which occurs during a target device's session (Welch & Lathrop, 2003). The attacker passively monitors (passive attack) the packets sent between the station and the AP during the first association process using an 802.11 network analyzer. Information gathered through the network analyzer is enough to set up a rogue malicious station or AP between the real node and the AP to mimic the real device (Curran & Smyth, 2005). Once the attacker has successfully mimicked the real AP or the node, it can log every packet; it can modify the traffic and selectively forward or delete it completely. The attacker can also gain access and roam the network as a legitimate user (Curran & Smyth, 2005). The rogue access concept will be explained further in the next section.

2.5.1.5 Rogue Access Point

As explained previously, the man in the middle attack is achieved by setting up a rogue station between the targeted AP and node. Rogue access point are set up using the real MAC address and SSID of a valid AP (Woodward, 2005). This is a technical security issue since rogue station is an unauthorized imitation of the real AP and can connect to the WLANs (Lim, Schmoyer, Levine, & Owen, 2003). Without proper security procedures in place, an intruder can plant an unauthorized AP to the WLANs and use it as a medium to collect information such as nodes' login names and password (Lim, Schmoyer, Levine, & Owen, 2003; Zahur, 2004). Curran and Smyth (2005) conduct a real life attack on WLANs in their lab to show how easily rogue access can be created and manipulated. Rogue access point could also be created unintentionally by users since most consumer grade AP are configured user friendly and come with the security features turned off therefore allow everyone to access the network (Hole, Dyrnes, & Thorsheim, 2005). Rogue access is a great threat to the wireless network especially in business since the impact is on the sensitive corporate data.

2.5.2 Other Security Issues

This section will look into the security issues concerning WLANs from technical and social perspective. The first WLANs security issue that is often overlooked by users is the hardware's default configuration (Park & Dicoi, 2003). Park and Dicoi (2003) describe that most access points (AP) are manufactured with the WEP encryption disabled. User may not be aware of this default configuration therefore failed to turn on the WEP and become vulnerable to attacks. Other default configurations that came with the original setting of the device such as the password, the service set identifier (SSID), the dynamic host configuration protocol (DHCP) settings, and the simple network management protocol (SNMP) can also cause serious security problem to the WLAN if not modified by the user (Park & Dicoi, 2003).

The second 802.11 security issue is on how network access is controlled in WLANs. There are two ways to control access to WLANs which are the open network the close network access control (Arbaugh, Shankar, & Wan, 2001). The open system authentication has been discussed earlier in section 2.4. The open system architecture is the default authentication protocol for new 802.11 networks devices (Gao & Ansari, 2005; Zahur, 2004). Access points with open network authentication will advertise its existence and also respond to all authentication requests from any wireless nodes (Arbaugh, Shankar, & Wan, 2001). A close wireless network in the other hand will not respond to request from nodes with an “empty set” SSID (service set identifier). Due to this, access points with close network authentication will be invisible to sniffer program such as Netstumbler and Kismet (Arbaugh, Shankar, & Wan, 2001; Curran & Smyth, 2005) therefore provides some layer of security against attackers. Network access control needs to properly configured and managed by network administrator to prevent unauthorized and malicious access the network.

MAC address spoofing is another security problem with WLANs (Zahur, 2004). Park and Dicoi (2003) clarify that since MAC addresses are transmitted by WEP in clear text, it can be easily eavesdrop by malicious attackers. Network analyzer software such as Netstumbler can be used to detect MAC addresses as well (Hurley, Thornton, & Puchol, 2004). In worst case scenario, an intrusion through MAC address can also occur when a registered network card is stolen (Park & Dicoi, 2003).

Attackers can break into a wireless network only after gaining access to the AP signals. The access point’s service coverage may be beyond the desired and safe distance therefore can create a security concern (Park & Dicoi, 2003). The lack of control over the area and distances of WLANs coverage can also leads to serious security issues such as loss of data integrity, confidentiality, and denial of service attacks (DoS) (Park &

Dicoi, 2003). These attacks can be performed through a technique referred to as wardriving (Gao & Ansari, 2005). Park and Dicoi (2003) did not explain whether the signal distance and coverage can be controlled but the ability to control the network signal range will help in reducing the network vulnerability to attacks.

Hotspots at public area such as airports and coffee shops though convenience and provides flexibility and mobility to users can also contribute to security problem to corporate WLANs. Corporate users who are accessing the corporate network through the public WLANs may unintentionally provides an opportunity to attackers in gaining access to the corporate network (Park & Dicoi, 2003). Public and open WLANs are not usually configured with a very tight security procedures thus can be a threat to the private WLANs (Park & Dicoi, 2003).

2.6 Researches in WLAN Security

Several studies have been conducted by researches in order to understand the current WLAN implementation. One of the ways is to conduct a field trial survey to collect real life data on WLAN implementation and activity.

The studies conducted on WLAN security were not identical, but most of the researchers used the wardriving technique in order to collect real life WLANs data. Hurley et al. (2004) explained wardriving as the activity of driving and moving in a designated area while collecting WLAN access point's information. The information gathered is used for statistical analysis as well as to raise awareness on wireless security. Wardriving technique is not only limited to driving, it can be performed by flying (warflying) or by walking (warwalking) (Hurley, Thornton, & Puchol, 2004). Wardriving can be easily done using minimum tools. Having a laptop equipped with a wireless adapter and running a network analyzing software such as Netstumbler (for Windows) or Kismet (Linux) is sufficient to start a wardriving (Webb, 2003). Netstumbler is a popular wardriving software due to the ease of installation and the fact that it runs on Windows platform. However, advanced wardrivers might invest in more sophisticated hardware and software to expand the WLANs activities coverage (Hurley, Thornton, & Puchol, 2004).

The research conducted in Auckland CBD in 2004 by Lin et al. (2004) provided an analysis and report on two prominent WLANs security issues which are the WEP protocol, and the SSID. Lin et al. (2004) from their wardriving survey reported that a minimum of 60% of the WLAN devices identified in their study do not have the WEP encryption enabled while 67% of the WLAN devices are still using the factory default SSID. The study did not report on the number of ad-hoc and infrastructure WLAN detected in Auckland CBD which will show the growth of peer to peer wireless growth. Hole, Dyrnes and Thorsheim (2005) carried out a comparable study to Lin et al. (2004) by applying wardriving and warwalking methods to asses the security level of WLAN in Bergen, Norway. The focus of their study however is on the security issue of corporate employees connecting to the company network using wireless devices while at home or while on the road. From the study, the authors identified that a majority of the WLANs users in Bergen, both private users and businesses users, are only implementing WEP a security measure. The argument brought up by the authors is on the credibility and reliability of the WEP protocol alone in securing WLANs. The authors recommended WPA, virtual private network (VPN), and captive portal to replace WEP in WLAN (Hole, Dyrnes, & Thorsheim, 2005). Another similar experiment by Curran and Smyth (2005) was conducted in Londonderry in United Kingdom to investigate the number of wireless devices that are enabled with WEP. The authors confered on the weaknesses of default security mechanism such as WEP and SSID. WLANs attacks are listed out by the authors which includes the passive attacks, traffic analysis, man-in-the-middle attacks, session hijacking, MAC Spoofing (identity theft), IP redirection, and injecting traffic (Curran & Smyth, 2005).

The focus of the data gathered by all the researchers are on the WEP and SSID. It is arguable that eventhough the detected WLAN device is using WEP and the default SSID, those devices could also be secured through other more advanced security methods such as VPN and firewalls. However, a wardriving may not be able to detect such security features and thus require a more specific testing environment to do so.

2.7 Summary

The serious security hiccups that exist during WLAN earlier implementation such as the WEP and open system authentication will not render WLAN growth in the future. One the many reasons would be due to the benefit of network mobility and flexibility that is lacking in the existing wired LAN infrastructure. The increasing and affordable wireless devices are also a factor that generates WLAN future growth. Individuals and companies are currently using the wireless technology to conduct important communication such as sending and receiving emails, conducting mobile e-commerce transactions, and other data transmission which they expect will be kept as private as possible (Miller, 2001). The ongoing challenge of the WLAN development group is to ensure that those data will always be secured and private since hackers and intruders will not stop in finding ways to crack and attack the WLAN technology as well.

WLANs are vulnerable to various security threats such as the man in the middle attack and also the denial of service attack. The security attacks discussed in this chapter is to provide a preliminary understanding on the various attacks that can be attempted on WLANs technology. The discussion on the 802.11 security issues provides an overview of the problems not just from technological perspective but also from the social perspective. The researches that have been completed to understand the actual situation and position of WLANs security awareness at several locations have provided valuable information regarding the state of WLANs security not just to other researchers but also to organizations residing in those affected area. The information gathered in the Lin et al. (2004) will be used to identify and compare the progress of WLANs security status in Auckland CBD between 2004 and 2007.

The next chapter discusses the research methodology for this dissertation.

Chapter 3

Research Methodology

3.1 Introduction

In chapter 2, a review of literatures on WLAN architecture, standards, security issues, and researches are presented. This chapter explains the research methodology selected for this dissertation. Research methodology is defined as the general approach to the research processes, beginning from the hypothetical groundwork of the research approach to the gathering and analysis of data (Collis & Hussey, 2003). Therefore the methodologies selected for this project are literature reviews and field trials. The research guidelines are as follows:

- Review and report on current literatures on WLAN security, including field trips, observation, and security practices.
- Conduct field trials (warwalking) in Auckland CBD.
- Compare the research finding with a previous work by Lin et al. (2004) and then analyzed the differences.
- Provide recommendations and implications on methods to secured WLANs in businesses around Auckland CBD.

3.2 Purpose of Research

The main purpose of this research is to answer the following research question:

"What is the current status of WLAN security practices in Auckland City?"

In order to answer this question, literature reviews on the IEEE 802.11 technologies and a set of field trials in Auckland CBD are conducted. The purpose of the literature review is to investigate and identify the current security loopholes and vulnerabilities of WLAN technologies. Then, a set of field trials is performed using the wardriving technique to collect real life WLANs data in Auckland CBD. The research findings are analysed and compared with previous work (Jeffcoate, Chappell, & Feindt, 2002). The focus of the data analysis is to identify the differences and progresses with regard to WLAN security between the year 2004 and year 2007.

3.3 Goal

The goal of this research is to explore WLANs security and collect real-world data through field trials. The data accumulated from the field trials will be used to analysed and identify the current status of WLANs security in Auckland CBD.

3.4 The Hypothesis

The majority of WLANs in Auckland CBD are not implementing the minimum required security measures such as WEP encryption and are therefore vulnerable to network security attacks. The assumption is that the security awareness among users in Auckland CBD have increased but not to a satisfactory level since the last wardriving field trial conducted in 2004 (Jeffcoate, Chappell, & Feindt, 2002).

3.5 Research Design

3.5.1 Location

The location selected for this research is Auckland central business district (CBD). The exact area for the field trials is the stretch of road known as “Queen Street”. This area was selected by considering the centralized location and also the high concentration of small shops and businesses operating there (Hole, Dyrnes, & Thorsheim, 2005). The location and the paths selected for the field trials are as in Figure 3.1. The field trials started and ended at the corner of Custom Street and Queen Street. The direction taken during the study is as shown by the arrows in the map.

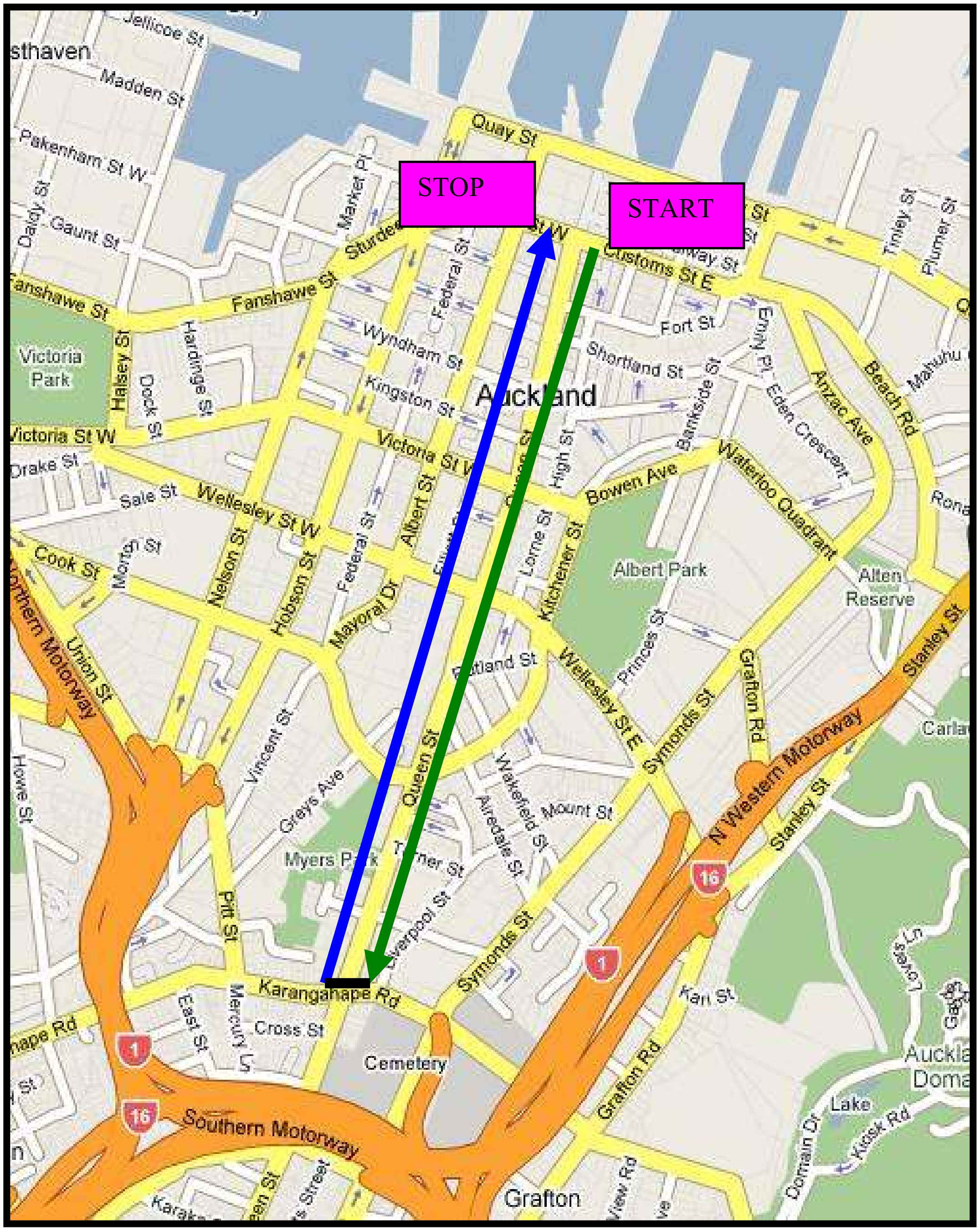


Figure 3.1 The location and path of field trials in Auckland CBD

3.5.2 Field Trials

A field trial is selected for this project since the goal is to evaluate the current wireless security level in Auckland CBD. To achieve this, experimental data collected through field trial are analysed and compared with previous research. A set of field trials is conducted in Auckland's CBD using the wardriving technique to gain an insight into the current status of WLANs security practices in the specified area. The first field trial is conducted during normal business hours between 1pm to 2pm and will be referred to as "Day Scan" throughout this paper. The second filed trial conducted after hours between 7pm to 8pm and is referred to as "Night Scan" throughout this report

3.5.3 Method

The method selected for the field trial is "warwalking". Warwalking is a variation of the wardriving which is conducted by walking in a specified area and collecting wireless data (Clincy & Sitaram, 2006; Hole, Dyrnes, & Thorsheim, 2005). Warwalking method is chosen for this research since it provides more flexibility while allowing greater access to the facilities located on the Queen Street. A network analyzing software, Network Stumbler, is selected for data gathering using warwalking method. The following guideline is followed during the field trials:

The automatic network attachment feature on the Netstumbler must be disabled. This is to ensure that the field trial complies with the legal and ethical requirements (Hurley, Thornton, & Puchol, 2004; Jeffcoate, Chappell, & Feindt, 2002; Sathu, 2006).

The content of the wireless network detected during the field trial should not be examined nor modified at any time (Jeffcoate, Chappell, & Feindt, 2002; Sathu, 2006).

The network resources detected during the field trial should not be used (Jeffcoate, Chappell, & Feindt, 2002; Sathu, 2006).

The field trial is conducted on both side of the Queen Street as shown in Fig. 3.1.

3.5.4 Resources Required

Tools that are used to conduct this experiment are as follows:

Hardware	: Dell Inspiron 5150 notebook; Cisco Aironet 350 NIC card
OS	: Windows XP
Software	: Netstumbler (http://www.netstumbler.com/downloads)

The tools used to conduct the experiment are shown in Figure 3.2. The software selected for the warwalking as mentioned previously is Network Stumbler or also known as Netstumbler (Netstumbler, 2007), is an open source software downloadable from http://www.netstumbler.com. Netstumbler operates in Windows environment to facilitate the detection of WLANs (802.11b, 802.11a and 802.11g standards) (Netstumbler, 2007). Netstumbler can dynamically sense wireless networks by sending probe requests roughly every second. Once a probe requests is sent, Netstumbler will listen for any responding probe response frame from node or access points (Clincy & Sitaram, 2006).

Network Stumbler Version 0.4.0 (Build 554)

Copyright © Marius Milner 2001-2004. All rights reserved.
NetStumbler® is a registered trade mark of Marius Milner.
mariusm@pacbell.net - http://stumbler.net
Please see Help menu for license information.

NDIS 5.1 card support by Marius Milner
U.S. Robotics Wireless MAXg PC Card (Microsoft's Packet Scheduler)
Driver Version: 868.46.0
MAC Address: 00:C0:49:57:A4:36
Additional: WPA

Figure 3.2 Tools used in the Wireless security filed trials

3.6 Data Analysis Considerations

Based on the previous study by Lin et al. in 2004, data analysis in this dissertation will mainly focus on the operation mode of the WLANs detected, the encryption status, and the service set identifier (SSID).

3.6.1 Operation Mode

WLANs can operate in either ad hoc or infrastructure mode. The data retrieved from the field trials on the distribution of the ad hoc (IBSS) and infrastructure mode (ESS) is used to determine the preferred architecture of the WLANs deployment in Auckland CBD (Yek & Bolan, 2004).

3.6.2 Encryption Status

If a device is encrypted, the Netstumbler software will report it as "WEP" regardless of whether the device is really using WEP (Clincy & Sitaram, 2006). Therefore the analysis will use "Encryption Status" instead of "WEP" during data analysis. The data collected on encryption status will be used to determine the level of wireless security awareness among users in Auckland CBD. WEP is assumed as the most basic security protocol that should be applied as the first defense against network attackers. The field trial conducted by Lin et al (2004) is used as a benchmark for this study. If the percentage of encryption detection on all AP and nodes is more than 40% of the total systems detected, it could mean an increase of user awareness on wireless network security.

3.6.3 SSID

Lin et al (2004) reported that 67% of the WLAN devices detected in their study are still using the default SSID. Therefore if the number of default SSID detected is higher than 67%, it could mean that there have been no significant changes on user awareness of wireless security.

3.7 Summary

This chapter describes the research methodology adapted in this dissertation. Real life WLAN data is collected by warwalking method using network analyzing software called Netstumbler. The field trials data on the status of WLAN security in Auckland CBD is presented in Chapter 4.

Chapter 4

Results and Analysis

4.1 Introduction

The previous chapter discusses the research methodology selected for this dissertation. This chapter presents experimental results and analysis. The wireless devices detected during the field trials, the encryption status of the WLANs, the network architecture and the SSID are discussed. The focus of the analysis in this chapter is based on the current WLAN practices in Auckland CBD.

4.2 Experimental Results

Overall, 428 wireless devices were detected during the day scan while 303 devices were detected during the night scan. The possible contributions to the 30% drop in WLAN usage between first scan and the second scan are that businesses are turning off the AP after office hours and users have relocated somewhere else. A brief comparison of the data collected is shown in Table 4.1.

Scans	Total	%
Day Scan	428	59
Night Scan	303	41

Table 4.1 Field Trial result

4.2.1 Device Manufacturer

From the data collected in the field trial in Auckland CBD using the Netstumbler software, the equipment manufacturers can be determined by comparing the first 6 alphanumerical value of the MAC address with the stored IEEE OUI (organizational unique identifier) data gained from this website http://standards.ieee.org/regauth/oui/oui.txt (IEEE, 2006). Below are the results for the day scan and night scan:

4.2.1.1 Day Scan

From the data collected during the day scan, the top five manufacturers are D-Link supplying 26.64% of the WLAN devices detected in Auckland CBD, second is Netgear with 14.72%, third is Cisco with 11.21%, fourth is Cisco-Linksys with 10.98%, and finally 3Com with 4.21% share. The rest of the device manufacturers detected in the day scan are listed in Table 4.2. A more comprehensive and detailed data can be viewed in Appendix 2.

Manufacturer	Detected	%
D-Link Corporation	114	26.64
Netgear Inc	63	14.72
Cisco	48	11.21
Cisco-Linksys	47	10.98
3Com Europe Ltd	18	4.21
Apple Computer	18	4.21
Askey Computer Corp.	15	3.50
Colubris Networks	14	3.27
Unidentified manufacturer in the OUI	14	3.27
Belkin Corporation	13	3.04
Others	64	14.95
Total	428	

Table 4.2 Device manufacturer detected in day scan

4.2.1.2 Night Scan

From the data collected during the night scan, the top five manufacturers still begins with D-Link leading at 22.44%, second is Netgear with 16.50%, however third is now Cisco-Linksys at 11.88%, Cisco is fourth with 11.55%, and finally 3Com with 5.28% share of the market. The rest of the device manufacturers detected in the night scan are listed in Table 4.3 below. A more detailed data can also be viewed in Appendix 1.

Manufacturer	Detected	%
D-Link Corporation	68	22.44
Netgear Inc	50	16.50
Cisco-Linksys	36	11.88
Cisco	35	11.55
3Com Europe Ltd	16	5.28
Unidentified Manufacturers	13	4.29
Apple Computer	12	3.96
Belkin Corporation	9	2.97
Colubris Networks	9	2.97
Airspan	6	1.98
Others	49	16.17
Total	303	

Table 4.3 Device manufacturer detected in night scan

Several conclusions can be derived from the data presented above. The first conclusion is that a majority of the wireless equipments used in the city are from D-Link with an average of 25% of the whole WLAN detected with Netgear following closely behind at an average of 15% of the market share. However in 2004, Lin, Sathu and Joyce reported that the main player in the WLAN in Auckland CBD was Cisco Aironet controlling 33% of the whole market (Jeffcoate, Chappell, & Feindt, 2002). The differences that have been observed shows that the data gained from the field trip can be used to analyze trends in WLAN equipment preference among users in a particular area by interested party such as equipment suppliers and vendors.

The second conclusion is that the origin of a wireless device can be easily determined by comparing the first six alphanumerical values of the device MAC address with the OUI data retrieved from the IEEE website mentioned previously. This process can be attempted by almost anyone with access to the internet or the OUI data. This information when combined with other data such as encryption status can be used my malicious users to launch attacks against the WLAN.

4.2.2 Encryption

The encryption status of the WLANs detected in the Auckland CBD is summarized in Table 4.4.

Encryption	Day Scan		Night Scan	
	Total	%	Total	%
On	322	75.23	229	75.58
Off	106	24.77	74	24.42
Total	428		303	

Table 4.4 WLAN Encryption Status in Auckland CBD

From the 428 WLANs detected during the day scan, 75.23% are encrypted while 24.77% are not encrypted. During the night scan, from the 303 WLANs detected, 75.58% were encrypted while 24.42% were not encrypted. From the data gathered, it can be concluded that the level of WLAN encryption in Auckland CBD were consistent on both day and night data with roughly 75% of WLANs detected were encrypted while only 25% were not.

4.2.3 Operation Mode

Two operation modes or network types are observed from the field trial, the first is the IBSS or the Ad hoc network, and the second is the ESS or the infrastructure network with access points (AP). The overview of the data collected is shown in 4.5.

Scan	Total	ESS		IBSS	
		Total	%	Total	%
Day Scan	428	415	96.96	13	3.04
Night Scan	303	291	96.04	12	3.96

Table 4.5 WLAN detected in Auckland CBD

4.2.3.1 IBSS (Ad Hoc)

Thirteen IBSSs were detected during the day scan while twelve are detected during the night scan. From the thirteen IBSS detected during the day scan, only four were encrypted while nine are without encryption. For the night scan, five were encrypted while seven other were not. Table 4.6 provides an overview of this information.

Encryption	Day Scan		Night Scan	
	Total	%	Total	%
On	4	30.77	5	41.67
Off	9	69.23	7	58.33
Total IBSS	13		12	

Table 4.6 IBSS detected and encryption status

4.2.3.2 ESS (AP)

In the day scan, 76.63% of the overall ESSs detected were encrypted while 24.10% were not. This information is almost consistent with the night scan result which showed that 76.98% of ESSs detected were encrypted while 23.02% were not. The Table 4.7 shows the result in more detail.

Encryption	Day Scan		Night Scan	
	Total	%	Total	%
On	318	76.63	224	76.98
Off	100	24.10	67	23.02
Total ESS	415		291	

Table 4.7 ESS detected and encryption status

4.2.4 SSID

Service Set identifier or SSID provides identification for access point to identify the local wireless networks. This section will be discussed SSID based on blank SSID and broadcasted SSID identified in the field trial.

4.2.4.1 Blank SSID

A "Blank SSID" is captured by Netstumbler's program when access points report their existence but not their SSID. From the data collected, there were 24 blank SSID detected in the day scan and 14 in the night scan. Even though not broadcasting the SSID could be a security measure, it is interesting to see that out of the 24 blank SSID identified in the day scan, eight were without encryption. In the night scan data, out of 14 identified bland SSID, five were without encryption. Table 4.8 shows the information discussed in more detail.

Encryption	Day Scan		Night Scan	
	Total	%	Total	%
On	16	66.67	9	64.29
Off	8	33.33	5	35.71
Total Blank SSID	24		14	

Table 4.8 Blank SSID detected and encryption status

4.2.4.2 Broadcasted SSID

There were 404 SSID broadcasted during the day scan and 289 during the night scan. For the day scan, a majority of the WLANs broadcasting their SSID were encrypted and only 23.61% were not. A similar result is observed during the night scan as shown in Table 4.9.

Encryption	Day Scan		Night Scan	
	Total	%	Total	%
On	306	73.73	220	75.60
Off	98	23.61	69	23.71
Total SSID	404		289	

Table 4.9 Broadcasted SSID detected and encryption status

4.2.4.3 Default SSID

Three usage of the default SSID were reported by Netstumbler during the day scan while only one was reported for the night scan. It was reported in 2004 that 13.1% of the WLAN detected are still using the default SSID value (Jeffcoate, Chappell, & Feindt, 2002). This show a sharp decrease in default SSID usage from 2004 to 2007.

4.2.5 Combined Day and Night data

The purpose of merging both day scan and night scan data is to evaluate the actual WLAN detected on 26 June 2007 and to confirm the analysis on both the day and night data previously. The merged data will be evaluated based on the actual number of WLAN detected during the day, the encryption status, operation mode, and SSID.

4.2.5.1 Total WLAN Detected

The actual WLAN distribution during the field trials can be determined by filtering the MAC address based on the time of its “first seen” and “last seen” fields in the report produced by the Netstumbler program. The total number of actual WLAN detected was 506, with 225 WLAN appearing on both scans, 204 appearing only in the day scan, and 78 appearing only in the night scan. Table 4.10 represents the data discussed earlier. The list of MAC addresses can be viewed in Appendix 2. This showed that the WLANs detected in Auckland CBD have increased 114%.

WLAN in Auckland CBD	Detected	%
WLAN appears in both scans	225	44
WLAN appears in day scan only	203	40
WLAN appears in night scan only	78	15
Total of actual WLAN detected	506	

Table 4.10 Actual MAC addresses detected in Auckland CBD

4.2.5.2 Encryption

It was identified that 74% of all WLAN detected on 26 June 2007 had some kind of encryption on while only 26% are without encryption. Table 4.11 provides a summary of this information. This data confirmed the speculated increment of encryption on the WLANs in Auckland CBD when compared with the data presented in 2004 by Lin, Sathu and Joyce. In 2004, Lin, Sathu, and Joyce (2004) discovered that only 40% of WLAN detected in 2004 applied some kind of encryption while 60% of all WLAN observed during their field trial in Auckland CBD were not encrypted. Comparing the result from 2004 with the current observation of WLAN encryption status in Auckland CBD, it can be concluded that the encryption enablement have increased by almost 85% from 2004 to 2007. This encouraging phenomenon could be due to an increase awareness of wireless security requirements among current wireless users.

Status	Total	%
Encryption On	376	74
Encryption Off	130	26

Table 4.11 Actual Auckland CBD encryption status

4.2.5.3 Operation Mode

The analysis on the merged data identified 95% of all the WLANs detected were ESS while less than 5% were IBSS. This data is summarized in Table 4.12. Comparing this data with the one from 2004, it is observed that there is a slight increase on the ESS detected. Based on this result, it can be assumed that the majority of WLAN implementers in Auckland CBD preferred the infrastructure mode.

Operation Mode	Total	%
IBSS (Ad hoc)	23	5
ESS (AP)	483	95

Table 4.12 Actual operation mode detected in Auckland CBD

4.2.5.4 SSID

From the 506 WLANs detected, 25 WLANs or 5% of the overall data were running with blank SSID, while 481 WLANs or 95% of the overall data broadcasted their SSID. From the 25 WLANs with blank SSID, only 17 applied encryption. For WLANs with broadcasted SSID, 359 WLANs applied encryption. This result is represented in Table 4.13. Applying blank SSID could be a security measure taken by the WLAN users in Auckland CBD. However, by not combining that technique with WEP or WPA encryption will still make the WLANs vulnerable to attacks unless other kinds of security measure are in place.

SSID	Blank SSID	Broadcasted SSID	Total encryption
Encryption On	17	359	376
Encryption Off	8	122	130
Total SSID detected	25	481	

Table 4.13 Actual SSID status in Auckland CBD

4.3 Summary

This research has identified that the number of WLANs detected in Auckland CBD has increased by 114.41% from 2004 to 2007. A total of 506 WLANs were detected in this research while only 236 WLANs were detected by Lin et al. in 2004. It was also identified that 74.31% of WLANs detected in this research had the encryption on while only 39.83% in 2004. This shows an increment of encryption implementation in Auckland CBD by 86.56% between 2004 and 2007. The data collected in this research also shows that WLANs without any encryption have drop by 57.30% between 2004 and 2007. The number of IBSS has also dropped by 55.30% in 2007 when compared to 2004 while ESS has increased by a mere 6.26%. The research findings are summarized in Table 4.14.

Field Trials Results	2004		2007		Increment	Decrement
	Total	%	Total	%		
Total WLANs	236	-	506	-	114.41	-
Encryption On	94	39.83	376	74.31	86.56	-
Encryption Off	142	60.17	130	25.69	-	57.30
IBSS	24	10.17	23	4.55	-	55.30
ESS	212	89.83	483	95.45	6.26	-

Table 4.14 Comparison of Field Trials Results on 2004 and 2007

The research also discovered that there were a total of 25 WLANs (5% of the total WLANs detected) running with blank SSID with 17 WLANs applied encryption. There were 481 WLANs (95% of the total WLANs detected) broadcasting their SSID with 359 WLANs applying encryption. The research also discovered the drop in the usage of default SSID. D-Link has become the main vendor for wireless devices in Auckland CBD with 25% of the market utilizing their product. The encouraging result indicates the growth of WLAN in Auckland CBD as well as the increase in security awareness among WLAN users as the technology matures. This could be due to more security training at corporate level, WLAN information communicated through multimedia, and the role played by academic institution in producing wireless security aware graduates or future work force.

The data collected in this research showed that the existence of WLANs can be easily detected and tracked by network analyzing software. The wireless network architecture as well as the parameter such as SSID, MAC addresses may also be identified. This information may be sufficient for attackers to gain unauthorized access to the network and manipulate sensitive data.

Chapter 5
Recommendations

5.1 Introduction

The result of the field trials conducted at Auckland CBD in 2007 is discussed in Chapter 4. This chapter now suggests techniques that can be employed by individuals and businesses to secure their WLAN in the future. The first part of this chapter is a discussion on the security techniques available for WLAN. There are many security techniques that businesses can execute to ensure the security of their WLAN. The techniques that are discussed in this chapter are the enabling of WEP or WPA, the MAC address filtering, the virtual private network (VPN), the intrusion detection system (IDS), network simulation, and the security risk assessment. The second part of this chapter is a discussion on the suitability of the techniques discussed for individual, small business, and enterprise users.

5.2 Recommendations

5.2.1 Enable WEP or WPA

Encryption can prevent malicious users from eavesdropping and stealing sensitive corporate information. Two major types of encryption protocol available on most wireless devices are WEP and WPA (McCullough, 2004). These protocols provide the first level of security to WLAN therefore it should be enabled in all wireless devices (Matsunaga, Merino, Suzuki, & Katz, 2003; Shridhar, Joyce, & Kolahi, 2005).

Network administrator should ensure that all wireless devices connecting to the WLAN are protected with either of the security protocols.

5.2.2 Change the Default SSID

Most new AP has a factory default Service Set Identifier (SSID) which is a unique network name for identification purposes (Bhagyavati, Summers, & DeJoie, 2004; Brown, 2003). In wireless environment, the SSID is transmitted in clear text by the AP as a way to inform other wireless devices of its existence (Bhagyavati, Summers, & DeJoie, 2004; Corbett, Beyah, & Copeland, 2006). Since this beacon message can be detected quite easily by active scanner such as Netstumbler, it is advisable to change the SSID or disable it (Bhagyavati, Summers, & DeJoie, 2004; Hole, Dyrnes, & Thorsheim, 2005; Hurley, Thornton, & Puchol, 2004). Though changing or disabling the SSID may not provide a significant impact on the overall security of the WLAN, it may provide a level of privacy to the network (Shridhar, Joyce, & Kolahi, 2005).

5.2.3 Implement MAC Address Filtering

Access Point (AP) can be set up and configured to only allow network connection from wireless nodes that have registered their MAC address with the WLAN (Curran & Smyth, 2005). The MAC address filtering technique can be applied either on the AP or at the RADIUS server. By applying this technique, the AP will have more control on wireless nodes that are accessing the network (Arbaugh, Shankar, & Wan, 2001). Hence, nodes that are not within the AP's allocated MAC address range will not be allowed to access the WLAN (Shridhar, Joyce, & Kolahi, 2005). This solution may be impractical in enterprises due to the huge number of users using the wireless devices in the WLAN but for a small WLAN, MAC address filtering may be useful in preventing unauthorized access to the WLAN.

5.2.4 Use Virtual Private Network

With the wireless technologies getting more and more ubiquitous, businesses also need to ensure that they are well prepared to protect their WLAN. An issue to consider is when an employee attempted a connection to the company's network via a Wi-Fi hotspot whose wired network and access points are beyond the control of the company's firewall? A solution to this problem is the virtual private network or VPN, that when utilized can help keep the data encrypted all the way from the wireless node to the network so that other malicious users cannot read the transmitted messages (Hole, Dyrnes, & Thorsheim, 2005).

VPN is a service that proposes a reliable and secure connection over a shared public infrastructure such as WLAN hotspot. It is also a security method that provides an encrypted connection between private networks and a public network. VPN used IPSec (IP Security) to provide confidentiality, data integrity, authentication and anti-replay protection (Laet & Schauwers, 2005). VPN works by creating a point-to-point connection between a user and a server that act as a tunnel to the public network. Various encryption techniques are being applied in this process which ensures that only the legitimate entity at each end of the VPN tunnels can read the transmitted messages (Hole, Dyrnes, & Thorsheim, 2005).

Virtual private network have been used in a wired LAN environment to protect remote users when dialing up into a corporate server or the intranet. It forces all traffic to go through an encrypted tunnel in order to access the corporate network which then provides an added security to the network (Woodward, 2005). How VPN works is by having one end of the tunnel with the VPN server software running on the company's computer and on the other end of the tunnel a VPN software client running on the employee's laptop. When an employee requests to connect to the network, the VPN server will then open a port in the firewall which allows intranet access for that employee through the VPN tunnel. However, VPN is still vulnerable to attacks if not implemented correctly. Hacking tools such as crackerjack can be utilize to evade a VPN and capture the network traffic via a man in the middle attack (Woodward, 2005).

5.2.5 Apply Wireless Intrusion Detection System (IDS)

Wireless intrusion detection system (IDS) is a network monitoring software that could be utilized in monitoring abnormal activity occurring in the WLAN as well as unauthorized devices presenting in the network (Laet & Schauwers, 2005; Shridhar, Joyce, & Kolahi, 2005; Woodward, 2005). Intrusion detection systems are developed to detect abnormal behaviors of networks and information systems, indicating infringement of the security policy. The analysis techniques implemented by most IDS are misuse-detection and anomaly detection. Misuse-detection analysis is to detect known security policy violation, while anomaly detection analysis is to detect divergence of normal systems behavior (Debar, 2004). Therefore IDS functions includes but not limited to the following, analyzing and monitoring user and system activities, identifying abnormal network activity, recognizing patterns of identified attacks, and discovering policy infringement for WLAN (Debar, 2004; Farshchi, 2003). However, IDS software are considered as reactive system which mean that attacks will not be prevented by this system but are only reported after they had occurred (Valli, 2004; Woodward, 2005). Hence, IDS provides accountability to the WLAN but does not protect the network from attacks (Debar, 2004).

The commercially available products such as AirMagnet, AirDefense, ActiveDefense, Surveyor Wireless, and AirSnare can be applied by businesses to perform intrusion detection for their WLAN infrastructure (AirDefense, 2007; AirSnare, 2007; Farshchi, 2003).Though the products mentioned previously may not be sufficient by itself to provide an adequate protection for the WLAN in organizations, utilizing this method is still beneficial in managing malicious attacks and intrusion (Lim, Schmoyer, Levine, & Owen, 2003). The main advantage of IDS is the separation of security enforcement and monitoring in the WLAN. Failure in WLAN security enforcement can now be detected by an independent technology which is the IDS (Debar, 2004).

5.2.6 Utilize Network Simulation

A way to evaluate the security level of a wireless network is through a simulation process. Network simulation or also referred to as networks modeling allows network administrators and designers to test and visualize new procedures or changes to a network topology before actually implementing it in a production network (Fritz, 2004). Simulation can be used to test wireless network coverage and security since building pilot labs and test beds are costly, while allocating and reconfiguring each of them is difficult and inflexible.

Simulation technique provides several benefits which includes but not limited to the isolation of network parameters, repeatable network scenarios, and detection of a range of metrics (Jardosh, Belding-Royer, Almeroth, & Suri, 2003). Other benefits would include a broader explanation of complex conditions and its associations, the usage of advanced graphical user interface (GUI) to represent simulated data and condition, the encouragement of new ideas, the promotion of system optimization, the ability to perform active evaluation of technical changes without causing disruption to the live system, and finally it is a cost efficient technique in evaluating and developing computer systems (Engelenhoven, 1998). Considering all the factor discussed previously, simulation is an important tool in the analysis, design and studies of WLAN (Bhatt, Fujimoto, Ogielski, & Perumalla, 1998; Breslau et al., 2000; Goktruk, 2006; Nieuwelaar & Hunt, 2004). A summary of the available network simulators is in Appendix 2.

5.2.7 Perform Security Risk Assessment

Security of information is of vital importance to organizations which use wireless local area networks. If these WLANs are left vulnerable, organizations are risking themselves of security threats that may caused severe damages to the company's operation (Dyce & Barrett, 2006). In spite of its size, a wireless network requires a through evaluation of its physical and operational security. Attackers can exploit the weaknesses that exist in WLAN to gain access to it. A way to protect the corporate WLAN is to reduce, mitigate or remove the threat risks. This can be achieved by having a good risk management program (Myerson, 2002).

In the long run, risk assessment can help organization avoids heavy financial losses due compromised security measures, protect against breaches of privacy, and finally protect the company from exposing themselves to cyber risks (Landoll, 2006). There are several benefits of conducting risk assessment to WLAN by organizations. The first benefit is the check and balance where the organization can review the current status of WLAN security measures implemented in the company. The second benefit of risk assessment is that it provides a periodic review on the effectiveness of security measures and threats that may occur as the WLAN technology advances and changes. The third benefit, organization can use the data gathered from risk assessment to plan and budget their spending on security implementation. The forth benefit is it creates security awareness among WLAN users and implementers (Landoll, 2006).

At an organizational level, risk assessments could be expected to be part of the normal security protocols to protect overall wireless network. Corporate users must be aware that the security requirement for wired and wireless network varies slightly. Implementing WLAN requires proper authentication of every network user, which is sometimes not required in wired LAN. WLANs also have to deal with providing and ensuring signals coverage and mobility to users. The confidentiality, authenticity, integrity and availability are the characteristics used in risk assessment to evaluate the security measures implemented and its effectiveness (Stanley, 2002).

5.3 Suitability of Applications to Businesses

The businesses in Auckland CBD compromise of small medium enterprises (SME) and enterprises. This section will discuss on the suitability of the applications mentioned previously to small businesses and the enterprise.

5.3.1 Small Businesses

SME could be a one-man operated or a company with less than 250 employees (Levy, Powell, & Worrall, 2005). SME usually have a small budget on IT implementation and maintenance. Considering this factor, it may be impractical for SME to implement all of the WLAN security recommendations suggested previously. However, SME should implement the WEP or WPA encryption, change or disable the SSID, and perform MAC address filtering immediately if they have not done so. Commercial simulation software can be very expensive and may be beyond the IT budget for most SME while an open source version may be hard to use, so this is a solution that may not be practical for SME with limited budget and IT knowledge. A company with IT staffs could start doing the risk assessment analysis to identify any loopholes in their current WLAN. The assessment data could further be used to evaluate whether implementing the IDS and VPN is necessary. For SME without IT staffs, it is advisable for them to hire a network consultant to evaluate the security level of WLAN in their company.

5.3.2 Enterprise

For the enterprises without any limitation on budget and IT staffs, they could implement all of the recommended security solutions except for MAC address filtering. MAC address filtering is impractical in company with a huge number of users due to extensive labor required to key in each of MAC address to the AP systems. Management of the MAC address is tedious therefore impractical for enterprises.

5.4 Summary

There are many ways to ensure the security of WLAN. This chapter provides seven recommendations that can be applied by business WLAN users to safeguard their network. The solutions suggested are enabling WEP or WPA encryption, changing the default SSID, implementing MAC address filtering, applying intrusion detection systems, utilizing the network simulation technique, and finally performing security assessment on the current and future WLAN infrastructure. This chapter also discusses the suitability of the security solutions to businesses.

Chapter 6
Conclusions

6.1 Introduction

In Chapter 5, various WLANs security solutions for improving security practices are discussed. This chapter concludes the whole research based on the results generated from the field trials. Then this chapter provides and discusses the implication of this research to the WLAN users in Auckland CBD. The limitations of this research are also discussed. Finally, this chapter recommends future researches in WLAN security.

6.2 Summary of Research findings

The number of WLANs detected in Auckland CBD has increased by 114.41% between 2004 and 2007 with a total of 506 WLANs detected in this research. It was also identified that 74.31% of all WLAN detected on 26 June 2007 utilized encryption technique while only 25.69% were without any encryption. This shows an increment of encryption utilization by 86.56% when compared to the data collected in 2004. It was also identified that 95% of all the WLANs detected were ESS while less than 5% were IBSS. The research also discovered that 5% of the total WLANs detected during the research had blank SSID while the other 95% broadcasted their SSID. The research also discovered a drop in the usage of default SSID by WLAN users in Auckland CBD. Another interesting finding is that 25% of the WLANs detected are sourced by D-Link.

6.3 Implication to WLAN users

From this research, users in Auckland CBD are made aware of the current security level of WLANs in their area. The literature analysis provides an overview of the WLANs in general and the security issues concerning its implementation. The field trial produces a result that shows the progress of WLAN security awareness among users in this area. The recommendations to improve the WLAN security can be referenced by users to enhanced and evaluate their current or future WLAN infrastructure.

6.4 Limitation of Research

This research was conducted using minimal equipments that may have not been very accurate in collecting WLAN data during the field trial. The research could be improve by applying the GPS scanning to capture the actual location of each WLANs detected during the study.

6.5 Recommendation for Future Research

It was assumed in this research that the user awareness on wireless security in Auckland CBD have increased based on the result obtained from the field trials. However, this assumption was not supported by evidence data from the users' side. A research to evaluate actual users' awareness and knowledge of wireless security would be beneficial to understand how wireless security could be further secured in the future. This will require conducting interviews or survey.

The adoption of WLAN in Auckland CBD is on the rise therefore it will also be practical to understand the actual procedures and steps taken by the corporate users in choosing, evaluating, implementing and securing WLAN in their organization. A research in this area would help other businesses in adopting WLAN in their organization.

The steps or procedure to help SME with limited IT staffs and budget conduct a risk assessment for WLAN can also be investigated. The current WLAN risk assessment procedures are mostly developed for enterprises and may be impractical for SMEs to follow.

6.6 Concluding remarks

The WLANs is gaining acceptance and popularity by home and business users worldwide. The main attraction of WLANs is in its architecture that provides a convenient, flexible and mobile alternative to the wired local area network (LAN) (Zahur, 2004). Another attraction is the installation and implementation cost of WLANs which is much lower when compared to the wired LAN (Housley & Arbaugh, 2003). However, the nature of wireless operation itself contributed to its vulnerability. Nevertheless, the security problem associated with WLANs should not become a barrier for its adoption in organizations. Understanding of the security issues surrounding this technology as well as the solutions to solve it is critical in assisting a successful deployment of WLAN anywhere.

References

Aime, M. D., Lioy, A., & Mazzocchi, D. (2004). On the security of 802.11 wireless network. In B. Jerman-Blazic, W. Schneider & T. Klobucar (Eds.), *Security and privacy in advanced networking technologies* (pp. 51-100). Amsterdam: IOS Press.

AirDefense. (2007). Anywhere, anytime wireless protection. Retrieved July 1, 2007, from http://www.airdefense.net/products/index.php

AirSnare. (2007). Air Snare. Retrieved July 1, 2007, from http://home.comcast.net/~jay.deboer/airsnare/index.html

Arbaugh, W. A. (2003). Wireless security is different. *Computer, 36*(8), 99-101.

Arbaugh, W. A., Shankar, N., & Wan, Y. C. J. (2001). Your 802.11 wireless network has no clothes. Retrieved 10 April, 2006, from http://www.cs.umd.edu/~waa/wireless.pdf.

Bethala, B., Joshi, A., Phatak, D., Avancha, S., & Goff, T. (2002). Design and Evaluation of a Common Access Point for Bluetooth, 802.11 and Wired LANs. Retrieved June 12, 2007, from http://ebiquity.umbc.edu/paper/html/id/106/Design-and-Evaluation-of-a-Common-Access-Point-for-Bluetooth-802-11-and-Wired-LANs

Bhagyavati, Summers, W. C., & DeJoie, A. (2004). *Wireless security techniques: an overview* Paper presented at the 1st annual conference on information security curriculum development Kennesaw, Georgia

Bhatt, S., Fujimoto, R., Ogielski, A., & Perumalla, K. (1998). Parallel simulation techniques for large-scale networks. *IEEE communication magazine,* 42-46.

Borisov, N., Goldberg, I., & Wagner, D. (2001). *Intercepting mobile communications: the insecurity of 802.11* Paper presented at the 7th annual international conference on mobile computing and networking, Rome, Italy

Breslau, L., Estrin, D., Fall, K., Floyd, S., Heidemann, J., Helmy, A., et al. (2000). Advances in Network Simulation. *IEEE Computer*(May), 59-67.

Brown, B. (2003). 802.11: The security difference between b and i. *IEEE Potentials, 22*(4), 23-27.

Cam-Winget, N., Housley, R., Wagner, D., & Walker, J. (2003). Security Flaws in 802.11 Data Link Protocols. *Communications of the ACM, 46*(5), 35-39.

Carli, M., Rosetti, A., & Neri, A. (2003, 23 Feb - 1 March). *Integrated security architecture for WLAN.* Paper presented at the 10th International Conference onTelecommunications, 2003. ICT 2003. .

Chang, T.-l. S., & Li, P. P. (2003). How to succeed in e-business by taking the Haier Road: Formulating e-business strategy through network building. *Competitiveness Review, 13*(2), 34-45.

Chen, J.-C., Jiang, M.-C., & Liu, Y.-w. (2005). Wireless LAN security and IEEE 802.11i. *IEEE Wireless Communications, 12*(1), 27- 36.

Clincy, V., & Sitaram, A. K. (2006). Evaluation and illustration of a free software (FS) tool for wireless network monitoring and security. *Journal of Computing Sciences in Colleges, 21*(3), 19-29.

Collis, J., & Hussey, R. (2003). *Business research: a practical guide for undergraduate and postgraduate students* (2nd ed.). New York: Palgrave Macmillan.

Corbett, C. L., Beyah, R. A., & Copeland, J. A. (2006). *Using active scanning to identify wireless NICs.* Paper presented at the 2006 IEEE Workshop on Information Assurance, New York.

Curran, K., & Smyth, E. (2005). Exposing the wired equivalent privacy protocol weaknesses in wireless network. *International Journal of Business Data Communications and Networking, 1*(3), 59-83.

Debar, H. (2004). Intrusion detection systems - introduction to intrusion detection and analysis. In B. Jerman-Blazic, W. Schneider & T. Klobucar (Eds.), *Security and privacy in advanced networking technologies* (pp. 161-177). Amsterdam: IOS Press.

Dyce, K., & Barrett, M. (2006). Taking Care of (E)-Business?: Australian IT Professionals' Views of Wireless Network Vulnerability Assessments. *Journal of Theoretical and Applied Electronic Commerce Research, 1*(2), 79-89.

Elliot, C. (2007). Why 802.11g should be your standard of choice. Retrieved June 10, 2007, from http://www.microsoft.com/smallbusiness/resources/technology/broadband_mobility/why_802_11g_should_be_your_standard_of_choice.mspx

Engelenhoven, J. V. (1998). Computer simulation and decision making. Retrieved May 10, 2007, from http://www.ciras.iastate.edu/publications/CIRASNews/CIRASatWork-2001Winter.pdf

Erten, Y. M., & Tomur, E. (2004). A layered security architecture for corporate 802.11 wireless network. *IEEE Wireless Telecommunication Symposium 2004*, 123-128.

Farrel, S., Seigneur, J.-M., & Jensen, C. D. (2004). Security in exotic wireless networks. In B. Jerman-Blazic, W. Schneider & T. Klobucar (Eds.), *Security and privacy in advanced networking technologies* (pp. 101-114). Amsterdam: IOS Press.

Farshchi, J. (2003). Wireless Intrusion Detection Systems. Retrieved June 30, 2007, from http://www.securityfocus.com/infocus/1742

Fogarty, K. (2005). Eye on 802.11i. Retrieved June 10, 2007, from http://www.networkworld.com/techinsider/2005/031405tiwireless2.html

Fritz, J. (2004). Network-modelling tools. *Network World* Retrieved May 10, 2006, from http://www.techworld.com/networking/features/index.cfm?featureid=938

Gao, Z., & Ansari, N. (2005). Tracing cyber attacks from the practical perspective. *IEEE Communication Magazine*, 123-131.

Gast, M. (2002). Wireless LAN Security: A Short History. Retrieved 10 April, 2006, from http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html

Geier, J. (2002a). 802.11 WEP: Concepts and vulnerability. Retrieved June 10, 2007, from http://www.wi-fiplanet.com/tutorials/article.php/1368661

Geier, J. (2002b). Making the Choice: 802.11a or 802.11g. Retrieved June 30, 2007, from http://www.wi-fiplanet.com/tutorials/article.php/1009431

GloMoSim. (2001). GloMoSim Manual. Retrieved 20 April, 2007, from http://pcl.cs.ucla.edu/projects/glomosim/GloMoSimManual.html

Goktruk, E. (2006). *Towards simulator interoperability and model interreplaceability in network simulation and emulation through AMINES-HLA* Paper presented at the 37th conference on Winter simulation Monterey, California

Haskin, D. (2007). FAQ: 802.11n wireless networking [Electronic Version]. *Computerworld* from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019472.

Henning, R. R. (2003). *Vulnerability assessment in wireless networks.* Paper presented at the Symposium on Applications and the Internet Workshops, 2003. .

Hole, K. J., Dyrnes, E., & Thorsheim, P. (2005). Securing Wi-Fi Networks. *Computer, July*, 28-34.

Housley, R., & Arbaugh, W. A. (2003). Security problems in 802.11-based networks. *Communication ACM, 46*(5), 31-34.

Hurley, C., Thornton, F., & Puchol, M. (2004). *Wardriving: drive, detect, defend a guide to wireless security*. Rockland: Syngress Publishing, Inc.

IEEE. (2006). IEEE OUI and Company_id Assignments. Retrieved July 22, 2007, from http://standards.ieee.org/regauth/oui/oui.txt

Jacobs, D. (2007). 802.11n creates systems integration opportunities. Retrieved June 30, 2007, from http://searchnetworkingchannel.techtarget.com/tip/0,289483,sid100_gci1255715,00.html

Jardosh, A., Belding-Royer, E. M., Almeroth, K. C., & Suri, S. (2003). *Towards realistic mobility models for mobile ad hoc networks* Paper presented at the 9th annual international conference on Mobile computing and networking San Diego, CA, USA

Jeffcoate, J., Chappell, C., & Feindt, S. (2002). Best practice in SME adoption of e-commerce. *Benchmarking: An International Journal, 9*(2).

Karygiannis, T., & Owens, L. (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices. Retrieved June 8, 2007, from http://cnscenter.future.co.kr/resource/crypto/standard/fips/NIST_SP_800-48.pdf

Kotilainen, N., Vapa, M., Keltanen, T., Auvinen, A., & Vuori, J. (2006, 8-9 June). *P2PRealm - Peer-to-peer network simulator.* Paper presented at the 11th Intenational Workshop on Computer-Aided Modeling, Analysis and Design of Communication Links and Networks.

Laet, G. D., & Schauwers, G. (2005). *Network security fundamentals*. Indianapolis: Cisco Press.

Landoll, D. J. (2006). *The security risk assessment handbook*. Boca Raton, FL: Auerbach Publication.

Levy, M., Powell, P., & Worrall, L. (2005). Strategic intent and e-business in SMEs: Enabler and inhibitors. *Information Resources Management Journal, 18*(4), 1-20.

Lim, Y. X., Schmoyer, T., Levine, J., & Owen, H. L. (2003, 18-20 June). *Wireless intrusion detection and response.* Paper presented at the 2003 IEEE Workshops on Information Assurance, West Point, USA.

Loeb, L. (2005). WPA: It's like WEP, but good. Retrieved 29 Mar, 2006, from http://www.security.ithub.com/article/WPA+Its+like+WEP+but+Good/163390_1.aspx

MANIACS. (n.d.). GTNETS. Retrieved 12 May, 2007, from http://www.ece.gatech.edu/research/labs/MANIACS/GTNetS/

Maple, C., Jacobs, H., & Reeve, M. (2006). *Choosing the right wireless LAN security protocol for home and business user.* Paper presented at the First international conference on availability, reliability and security.

Markus, B. (2004). Network modelling and evaluation tools for higher education. Retrieved June 30, 2007, from http://nsl.csie.nctu.edu.tw/NCTUnsReferences/Bernat_Markus.pdf

Matsunaga, Y., Merino, A. S., Suzuki, T., & Katz, R. H. (2003). *Secure authentication system for public WLAN roaming* Paper presented at the 1st ACM international workshop on wireless mobile applications and services on WLAN hotspots San Diego, CA, USA.

McCullough, J. (2004). *Caution! Wireless networking: Preventing a data disaster.* Hoboken: Wiley Publishing Inc.

Miller, S. K. (2001). Facing the challenge of wireless security. *Computer, 34*(7), 16-18.

Myerson, J. M. (2002). Identifying enterprise network vulnerabilities. *International Journal of Network Management, 12*, 135-144.

Netgear Inc. (2005a). WEP Open System Authentication. Retrieved June 30, 2007, from http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-08.html

Netgear Inc. (2005b). WEP Shared Key Authentication. Retrieved June 30, 2007, from http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-09.html

Netstumbler. (2007). About. Retrieved March 10, 2007, from http://www.netstumbler.com/about/

Nieuwelaar, M. v. d., & Hunt, R. (2004). Real-time carrier network traffic measurement, visualisation and topology modelling. *Computer Communications, 27*(1), 128-140.

Opnet. (2007). Modeler wireless suite. Retrieved 20 April, 2007, from http://www.opnet.com/products/modeler/home-1.html

Panko, R. R. (2004). *Corporate computer and network security*. New Jersey: Pearson Prentice Hall.

Park, J. S., & Dicoi, D. (2003). WLAN security: current and future. *IEEE Internet Computing, 7*(5), 60-65.

Pawlikowski, K., Jeong, H.-D. J., & Lee, J.-S. R. (2002). On credibility of simulation studies of telecommunication networks. *IEEE Communication,* 132-139.

Perrone, L. F., Yuan, Y., & Nicol, D. M. (2003). *Simulation of large scale networks II: modeling and simulation best practices for wireless ad hoc networks* Paper presented at the 35th conference on winter simulation: driving innovation New Orleans, Louisiana

Riley, G. F. (2003). *The Georgia Tech network simulator.* Paper presented at the ACM SIGCOMM 2003 workshop.

Sathu, H. (2006). *Wardriving dilemmas.* Paper presented at the 19th Annual Conference of the National Advisory Committee on Computing Qualifications, Wellington, NZ.

Scalable Network Technologies. (2007). QualNet Developer. Retrieved 20 April, 2007, from http://www.qualnet.com/products/developer.php

Schafer, G. (2003). *Security in fixed and wireless network* (H. J. v. Schmoeger, Trans.). Berlin: John Wiley and Sons.

Shimonski, R. J. (2003). Wireless Attacks Primer. Retrieved May 1, 2006, from http://www.windowsecurity.com/pages/article_p.asp?id=1133

Shridhar, A., Joyce, D., & Kolahi, S. (2005). *Security issues that arise in IEEE 802.11x and 3G wireless Networks.* Paper presented at the Eighteenth Annual Conference of the National Advisory Committee on Computing Qualification, Bay of Plenty.

Shunra. (2007). Shunra Virtual Enterprise (Shunra VE) 5.0. Retrieved 20 April, 2007, from http://www.shunra.com/content.aspx?pageId=69

Stallings, W. (2004, Sept-Oct). IEEE 802.11: Wireless LANs from a to n. *IT Pro, 6,* 32-37.

Stanley, R. A. (2002). Wireless LAN risks and vulnerabilities. Retrieved July 1, 2007, from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=6774

Stubblefield, A., Ioannidis, J., & Rubin, A. D. (2004). A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Trans. Inf. Syst. Secur. , 7*(2), 319-332

Tetcos. (2007). Products. Retrieved 20 April, 2007, from http://www.tetcos.com/software.html

Tyrrell, K. (2003). An Overview Of Wireless Security Issues. Retrieved 15 May, 2006, from http://www.sans.org/rr/whitepapers/wireless/943.php

Valli, C. (2004). *WITS - wireless intrusion tracking system.* Paper presented at the 3rd European conference on information warfare and security, Royal Holloway, UK.

Varshney, U. (2003). The status and future of 802.11-based WLANs. *Computer, 36*(6), 102-105.

Vernez, J., Ehrensberger, J., & Robert, S. (2006, 8-9 June). *Nessi: A Phython network simulator for fast protocol development.* Paper presented at the 11th International Workshop on Computer-Aided and Design of Communication Links and Networks (CAMAD), Trento, Italy.

Walsh, K., & Sirer, E. G. (2004). Staged simulation: A general technique for improving simulation scale and performance. *ACM Trans. Model. Comput. Simul., 14*(2), 170-195.

Webb, S. (2003). *Identifying trends in the deployment and security of 802.11b wireless technology in Perth, W.A.* Paper presented at the 4th Australian Information Warfare and Security Conference, Adelaide, Australia.

Welch, D., & Lathrop, S. (2003). *Wireless security threat taxonomy.* Paper presented at the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.

Wexler, J. (2004). 802.11i security standard goes on the books. Retrieved June12, 2007

Wi-Fi Alliance. (2004). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. Retrieved June10, 2007, from http://www.wi-fi.org/files/wp_8_WPA%20Security_4-29-03.pdf

Williams, J. (2001, Nov-Dec). The IEEE 802.11b security problem, part 1. *IT Pro,* 91-96.

Wong, J. (2003). *Performance investigation of secure 802.11 wireless LANs: Raising the security bar to which level?* Unpublished Dissertation, University of Canterbury.

Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. Retrieved June 12, 2007, from http://www.sans.org/reading_room/whitepapers/wireless/1109.php

Woodward, A. (2005). *Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations.* Paper presented at the 3rd Australian Information Security Management Conference, Perth, Western Australia.

Xia, H., & Brustoloni, J. C. (2005). *Hardening Web browsers against man-in-the-middle and eavesdropping attacks.* Paper presented at the 14th international conference on World Wide Web, Chiba, Japan.

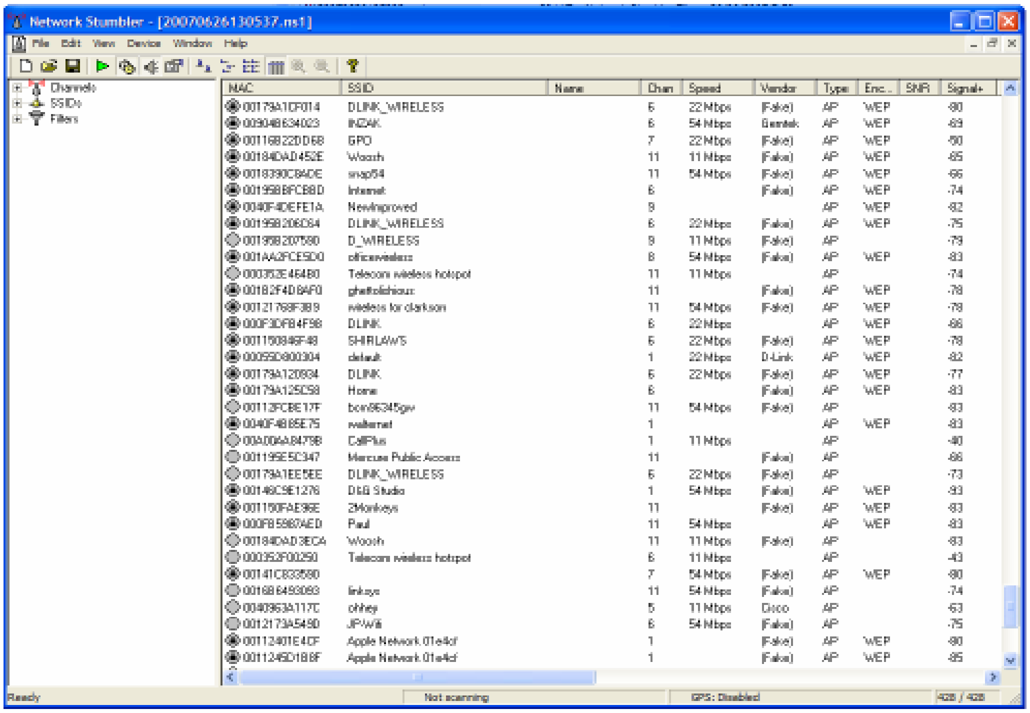
Ye, Q., & MacGregor, M. H. (2006). *Combining Petri Nets and ns-2: A hybrid method for analysis and simulation.* Paper presented at the Proceedings of the 4th annual communication Networks and services research conference.

Yek, S., & Bolan, C. (2004). *An analysis of security in 802.11b and 802.11g wireless networks in Perth, W.A.* Paper presented at the 5th Annual Information Warfare and Security Conference, Perth, Western Australia.

Zahur, Y. (2004). *Wireless Local Area Network - Security and Performance.* Unpublished Thesis, University of Houston - Clear Lake, Houston.

Appendices

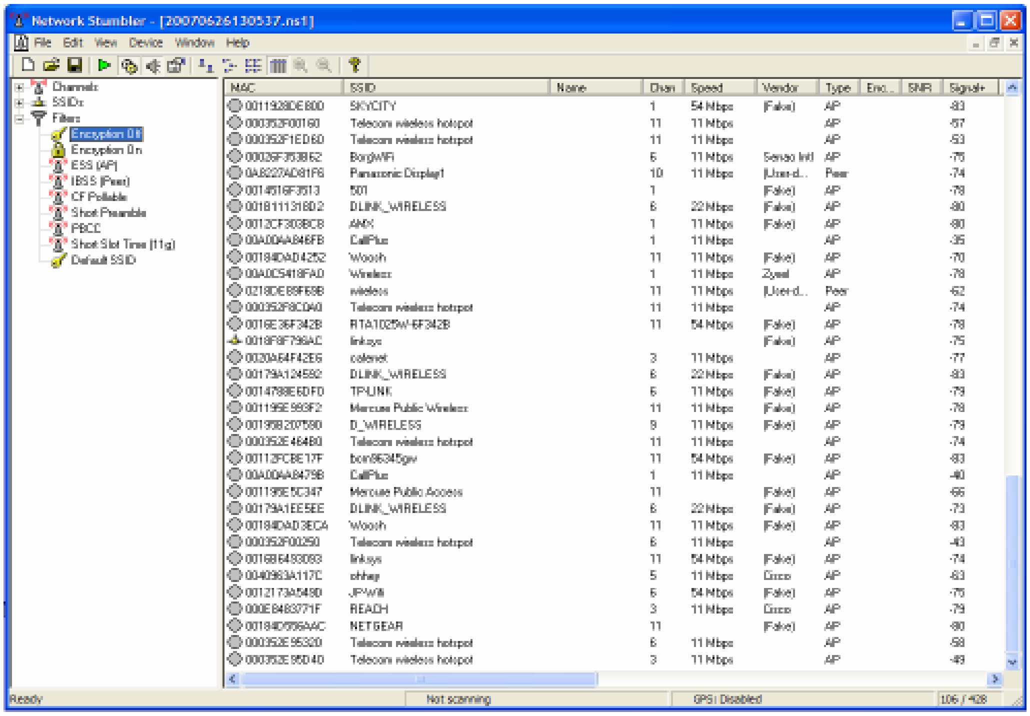
Appendix 1: Example of Data and Results



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00179A1CF014	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP	WEP		-80
00904B634023	INZAK		6	54 Mbps	Gemtek	AP	WEP		-69
001168220D68	GPO		7	22 Mbps	(Fake)	AP	WEP		-90
00184DAD452E	Woosh		11	11 Mbps	(Fake)	AP	WEP		-65
0018390C8ADE	snap54		11	54 Mbps	(Fake)	AP	WEP		-66
00195BBFCB8D	Internet		6		(Fake)	AP	WEP		-74
0040F4DEFE1A	NewImproved		9			AP	WEP		-82
00195B206D84	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP	WEP		-75
00195B207580	D_WIRELESS		9	11 Mbps	(Fake)	AP			-79
001AA2FCE5D0	officewireless		8	54 Mbps	(Fake)	AP	WEP		-83
000352E464B0	Telecom wireless hotspot		11	11 Mbps		AP			-74
00182F4D8AF0	ghettolicious		11		(Fake)	AP	WEP		-78
00121768F3B9	wireless for clarkson		11	54 Mbps	(Fake)	AP	WEP		-78
000F3DFB4F98	DLINK		6	22 Mbps		AP	WEP		-86
00115084 6F48	SHIRLAWS		6	22 Mbps	(Fake)	AP	WEP		-78
00055D800304	default		1	22 Mbps	D-Link	AP	WEP		-82
00179A120934	DLINK		6	22 Mbps	(Fake)	AP	WEP		-77
00179A125C58	Home		6		(Fake)	AP	WEP		-83
00112FCBE17F	bcm96345gw		11	54 Mbps	(Fake)	AP			-83
0040F4B85E75	walkernet		1			AP	WEP		-83
00A0D4AB479B	CallPlus		1	11 Mbps		AP			-40
001195E5C347	Marcus Public Access		11		(Fake)	AP			-66
00179A1EE5EE	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-73
00146C9E1276	D&G Studio		1	54 Mbps	(Fake)	AP	WEP		-93
001150FAE96E	2Monkeys		11		(Fake)	AP	WEP		-83
000FB5987AED	Paul		11	54 Mbps		AP	WEP		-83
00184DAD3ECA	Woosh		11	11 Mbps	(Fake)	AP			-83
000352F00250	Telecom wireless hotspot		6	11 Mbps		AP			-43
00141C833590			7	54 Mbps	(Fake)	AP	WEP		-90
00168B493083	linksys		11	54 Mbps	(Fake)	AP			-74
0040963A117C	ohhey		5	11 Mbps	Cisco	AP			-63
0012173A549D	JP-Wifi		6	54 Mbps	(Fake)	AP			-75
00112401E4CF	Apple Network 01e4cf		1		(Fake)	AP	WEP		-80
0011245D1B8F	Apple Network 01e4cf		1		(Fake)	AP	WEP		-85

Ready | Not scanning | GPS: Disabled | 428 / 428

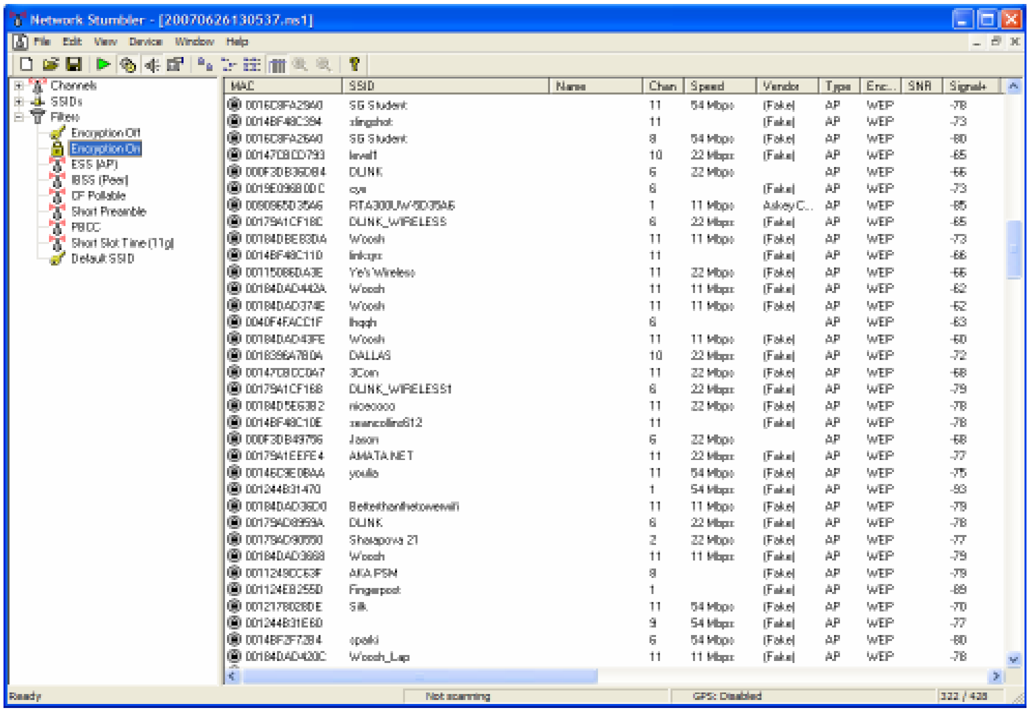
Figure A 1 WLANs (Day Scan)



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
0011928DE800	SKYCITY		1	54 Mbps	(Fake)	AP			-83
000352F00160	Telecom wireless hotspot		11	11 Mbps		AP			-57
000352F1ED60	Telecom wireless hotspot		11	11 Mbps		AP			-53
00026F353B62	BorgWiFi		6	11 Mbps	Senao Intl	AP			-75
0A8227AD81F6	Panasonic Display1		10	11 Mbps	(User-d...	Peer			-74
0014516F3513	501		1		(Fake)	AP			-78
0018111318D2	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-80
0012CF303BC8	AMX		1	11 Mbps	(Fake)	AP			-80
00A0D4AB46FB	CallPlus		1	11 Mbps		AP			-35
00184DAD4252	Woosh		11	11 Mbps	(Fake)	AP			-70
00A0C5418FA0	Wireless		1	11 Mbps	Zyxel	AP			-78
0218DE89F69B	wireless		11	11 Mbps	(User-d...	Peer			-62
000352F8C0A0	Telecom wireless hotspot		11	11 Mbps		AP			-74
0016E36F342B	RTA1025W-6F342B		11	54 Mbps	(Fake)	AP			-78
0018F8F798AC	linksys				(Fake)	AP			-75
0020A64F42E6	calenet		3	11 Mbps		AP			-77
00179A124592	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-83
0014788E6DF0	TP-LINK		6	11 Mbps	(Fake)	AP			-79
001195E993F2	Marcus Public Wireless		11	11 Mbps	(Fake)	AP			-78
00195B207580	D_WIRELESS		9	11 Mbps	(Fake)	AP			-79
000352E464B0	Telecom wireless hotspot		11	11 Mbps		AP			-74
00112FCBE17F	bcm96345gw		11	54 Mbps	(Fake)	AP			-83
00A0D4AB479B	CallPlus		1	11 Mbps		AP			-40
001195E5C347	Marcus Public Access		11		(Fake)	AP			-66
00179A1EE5EE	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-73
00184DAD3ECA	Woosh		11	11 Mbps	(Fake)	AP			-83
000352F00250	Telecom wireless hotspot		6	11 Mbps		AP			-43
00168B493083	linksys		11	54 Mbps	(Fake)	AP			-74
0040963A117C	ohhey		5	11 Mbps	Cisco	AP			-63
0012173A549D	JP-Wifi		6	54 Mbps	(Fake)	AP			-75
000E8483771F	REACH		3	11 Mbps	Cisco	AP			-79
00184D596AAC	NETGEAR		11		(Fake)	AP			-80
000352E95320	Telecom wireless hotspot		6	11 Mbps		AP			-58
000352E95D40	Telecom wireless hotspot		3	11 Mbps		AP			-49

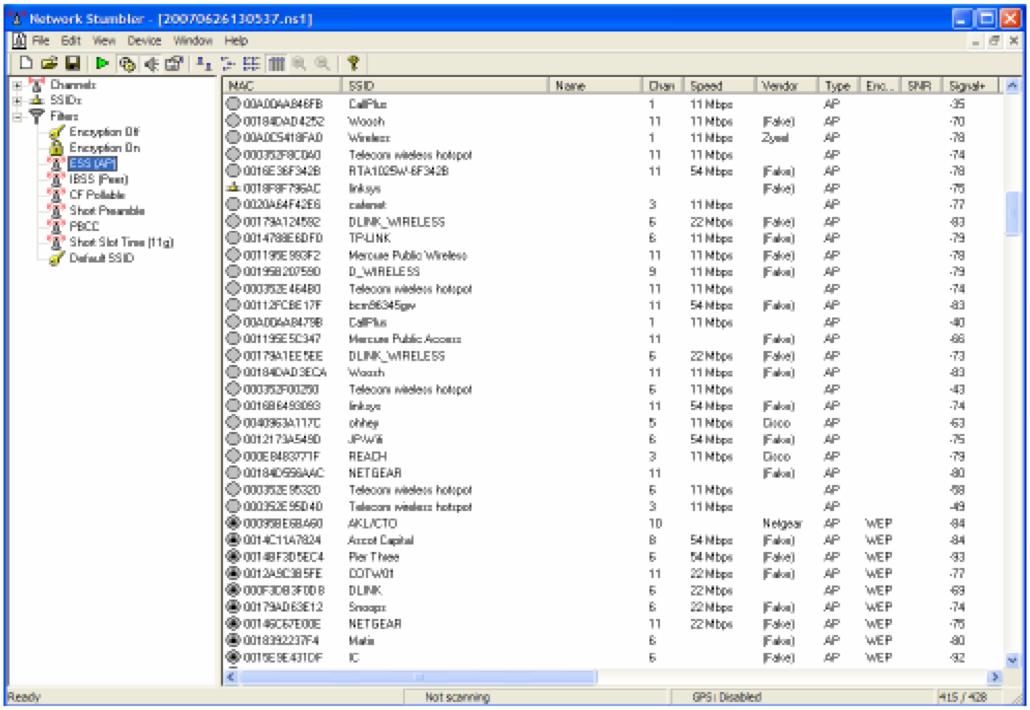
Ready | Not scanning | GPS: Disabled | 106 / 428

Figure A 2 WLANs (Day Scan) with encryption off



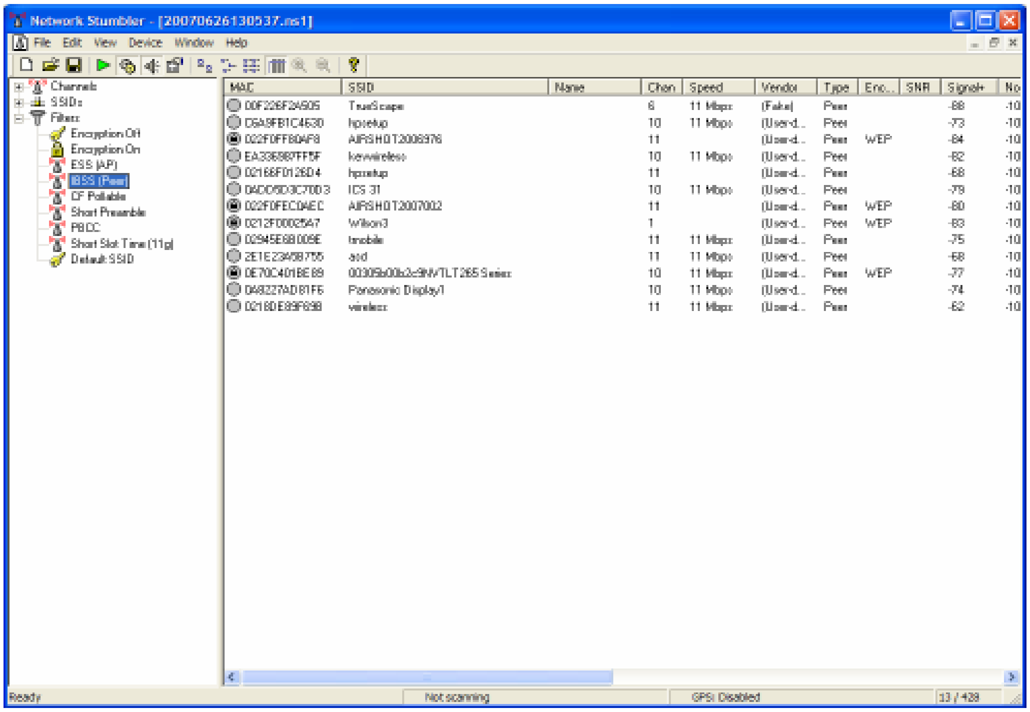
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
0016C8FA2960	SG Student		11	54 Mbps	(Fake)	AP	WEP		-78
0014BF48C394	slingshot		11		(Fake)	AP	WEP		-73
0016C8FA2640	SG Student		8	54 Mbps	(Fake)	AP	WEP		-80
00147DBDD793	level1		10	22 Mbps	(Fake)	AP	WEP		-65
000F3DB36D84	DLINK		6	22 Mbps		AP	WEP		-66
0019E0968D0C	cyx		6		(Fake)	AP	WEP		-73
0080965D3546	RTA300UW-5D35A6		1	11 Mbps	Askey C...	AP	WEP		-85
00179A1CF18C	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP	WEP		-65
00184DBE83DA	Woosh		11	11 Mbps	(Fake)	AP	WEP		-73
0014BF48C110	linksys		11		(Fake)	AP	WEP		-66
00115086DA3E	Ye's Wireless		11	22 Mbps	(Fake)	AP	WEP		-66
00184DAD442A	Woosh		11	11 Mbps	(Fake)	AP	WEP		-62
00184DAD374E	Woosh		11	11 Mbps	(Fake)	AP	WEP		-62
0040F4FACC1F	lhqqh		6			AP	WEP		-63
00184DAD43FE	Woosh		11	11 Mbps	(Fake)	AP	WEP		-60
0018396A7B0A	DALLAS		10	22 Mbps	(Fake)	AP	WEP		-72
00147DBDC0A7	3Com		11	22 Mbps	(Fake)	AP	WEP		-68
00179A1CF168	DLINK_WIRELESS1		6	22 Mbps	(Fake)	AP	WEP		-79
00184D5E63B2	niceoooo		11	22 Mbps	(Fake)	AP	WEP		-78
0014BF48C10E	seancollins612		11		(Fake)	AP	WEP		-78
000F3DB49756	Jason		6	22 Mbps		AP	WEP		-68
00179A1EEFE4	AMATA.NET		11	22 Mbps	(Fake)	AP	WEP		-77
00146C9E0BAA	youlis		11	54 Mbps	(Fake)	AP	WEP		-75
001244B31470			1	54 Mbps	(Fake)	AP	WEP		-93
00184DAD36D0	Betterthanthetowerwifi		11	11 Mbps	(Fake)	AP	WEP		-79
00179AD8959A	DLINK		6	22 Mbps	(Fake)	AP	WEP		-78
00179AD90990	Sharapova 21		2	22 Mbps	(Fake)	AP	WEP		-77
00184DAD3668	Woosh		11	11 Mbps	(Fake)	AP	WEP		-79
0011249DC63F	AKA.PSN		8		(Fake)	AP	WEP		-79
001124EB255D	Fingerpost		1		(Fake)	AP	WEP		-89
001217B0280E	Silk		11	54 Mbps	(Fake)	AP	WEP		-70
001244B31E60			9	54 Mbps	(Fake)	AP	WEP		-77
0014BF2F72B4	spaki		6	54 Mbps	(Fake)	AP	WEP		-80
00184DAD420C	Woosh_Lap		11	11 Mbps	(Fake)	AP	WEP		-78

Figure A 3 WLANs (Day Scan) with encryption on



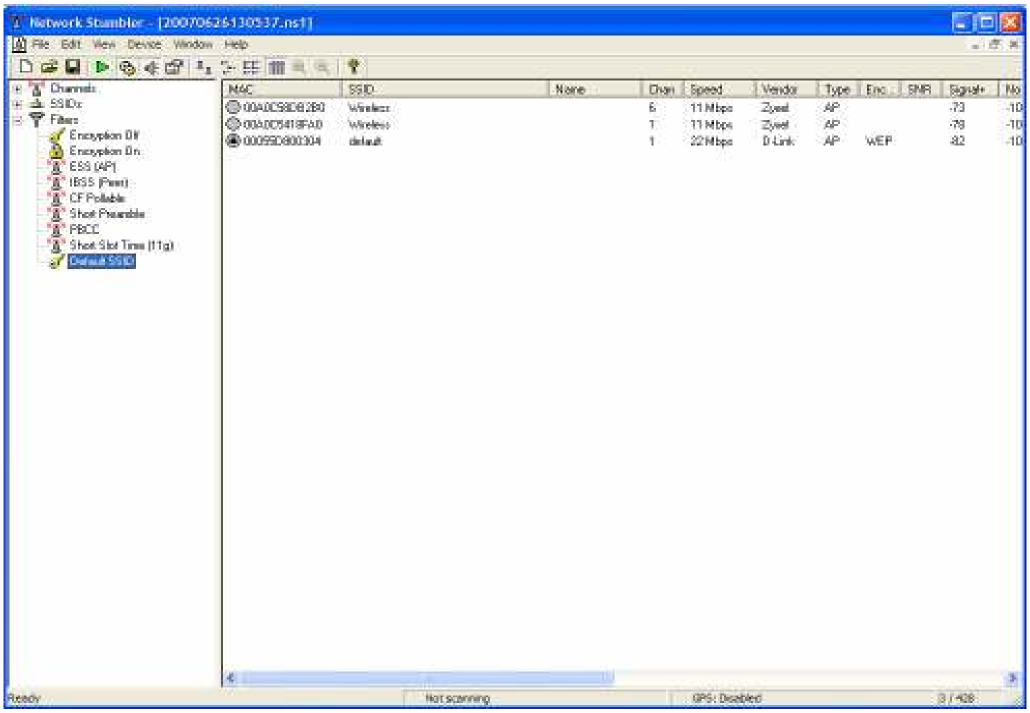
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00A0DAA846FB	CallPlus		1	11 Mbps		AP			-35
00184DAD4252	Woosh		11	11 Mbps	(Fake)	AP			-70
00A0C5418FAD	Wireless		1	11 Mbps	Zyxel	AP			-78
000352F8CDA0	Telecom wireless hotspot		11	11 Mbps		AP			-74
0016E36F342B	RTA1025W-6F342B		11	54 Mbps	(Fake)	AP			-78
0018F8F796AC	linksys				(Fake)	AP			-75
0020A64F42E6	calamet		3	11 Mbps		AP			-77
00179A124592	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-83
00147BBE6DF0	TP-LINK		6	11 Mbps	(Fake)	AP			-79
00119BE993F2	Mercure Public Wireless		11	11 Mbps	(Fake)	AP			-78
001958207590	D_WIRELESS		9	11 Mbps	(Fake)	AP			-79
000352E464B0	Telecom wireless hotspot		11	11 Mbps		AP			-74
00112FCBE17F	bcm96345gw		11	54 Mbps	(Fake)	AP			-83
00A0DAA8479B	CallPlus		1	11 Mbps		AP			-40
00119BE5C347	Mercure Public Access		11		(Fake)	AP			-66
00179A1EE5EE	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-73
00184DAD3ECA	Woosh		11	11 Mbps	(Fake)	AP			-83
000352F00290	Telecom wireless hotspot		6	11 Mbps		AP			-43
0016B6493093	linksys		11	54 Mbps	(Fake)	AP			-74
0040963A117C	ohhey		5	11 Mbps	Cisco	AP			-63
0012173A549D	JP-Wifi		6	54 Mbps	(Fake)	AP			-75
000E8483771F	REACH		3	11 Mbps	Cisco	AP			-79
00184D59BAAC	NETGEAR		11		(Fake)	AP			-80
000352E95320	Telecom wireless hotspot		6	11 Mbps		AP			-58
000352E95D40	Telecom wireless hotspot		3	11 Mbps		AP			-49
00095BE6BA60	AKL/CTO		10		Netgear	AP	WEP		-84
0014C1147824	Ascot Capital		8	54 Mbps	(Fake)	AP	WEP		-84
0014BF305EC4	Pier Three		6	54 Mbps	(Fake)	AP	WEP		-93
0012A9C3B5FE	COTW01		11	22 Mbps	(Fake)	AP	WEP		-77
000F3D83F008	DLINK		6	22 Mbps		AP	WEP		-69
00179AD63E12	Snoops		6	22 Mbps	(Fake)	AP	WEP		-74
00146C67E00E	NETGEAR		11	22 Mbps	(Fake)	AP	WEP		-75
0018392237F4	Matis		6		(Fake)	AP	WEP		-80
0015E9E431DF	IC		6		(Fake)	AP	WEP		-92

Figure A 4 WLANs (Day Scan) that are ESS/AP



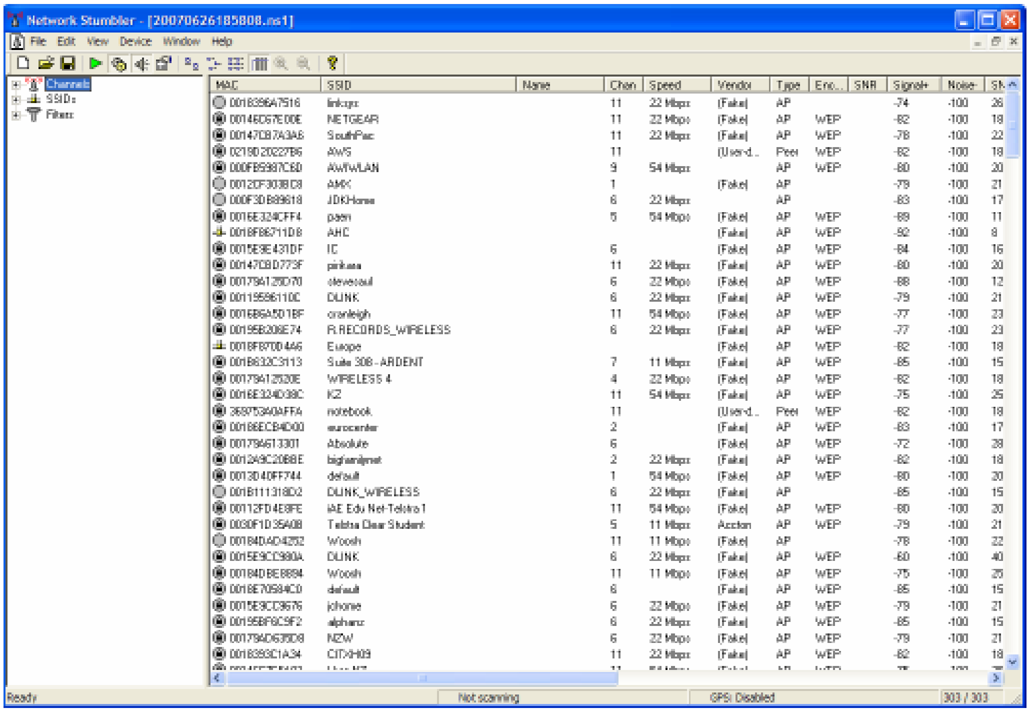
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	No
00F226F2A505	TrueScape		6	11 Mbps	(Fake)	Peer			-88	-10
D6A9FB1C4630	hpsetup		10	11 Mbps	(User-d...	Peer			-73	-10
022F0FF80AF8	AIRSHOT2006976		11		(User-d...	Peer	WEP		-84	-10
EA336987FF5F	kevwireless		10	11 Mbps	(User-d...	Peer			-82	-10
02166F0126D4	hpsetup		11		(User-d...	Peer			-68	-10
0ADD5D3C70D3	ICS 31		10	11 Mbps	(User-d...	Peer			-79	-10
022F0FEC0AEC	AIRSHOT2007002		11		(User-d...	Peer	WEP		-80	-10
0212F00025A7	Wilson3		1		(User-d...	Peer	WEP		-83	-10
02945E6B009E	tmobile		11	11 Mbps	(User-d...	Peer			-75	-10
2E1E23458755	asd		11	11 Mbps	(User-d...	Peer			-68	-10
0E70C401BE89	00305b00b2c9NVTLT265 Series		10	11 Mbps	(User-d...	Peer	WEP		-77	-10
0A8227AD81F6	Panasonic Display1		10	11 Mbps	(User-d...	Peer			-74	-10
0218DE89F698	wireless		11	11 Mbps	(User-d...	Peer			-62	-10

Figure A 5 WLAN (Day Scan) that are IBSS/Peer



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	No
00A0C58DB2B0	Wireless		6	11 Mbps	Zyxel	AP			-73	-10
00A0C5418FA0	Wireless		1	11 Mbps	Zyxel	AP			-78	-10
00095D800304	default		1	22 Mbps	D-Link	AP	WEP		-82	-10

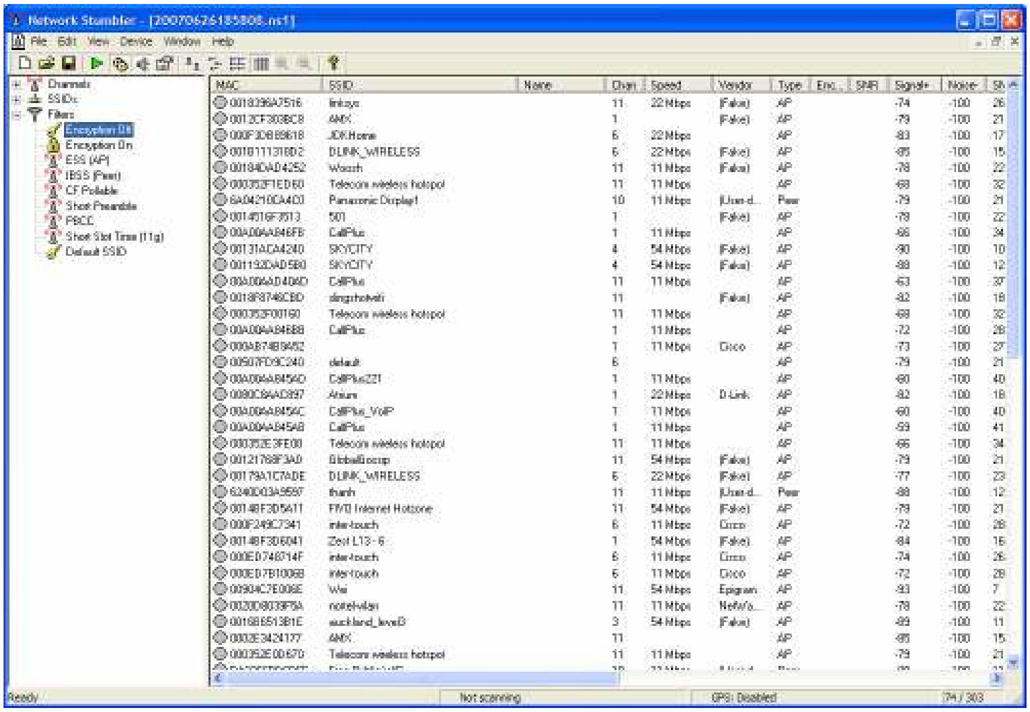
Figure A 6 WLAN (Day Scan) with default SSID


Network Stumbler - [20070626185808.ns1]
File Edit View Device Window Help
Channels
SSIDs
Filters

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SN
0018396A7516	linksys		11	22 Mbps	[Fake]	AP			-74	-100	26
00146D67E00E	NETGEAR		11	22 Mbps	[Fake]	AP	WEP		-82	-100	18
00147CB7A3A6	SouthPac		11	22 Mbps	[Fake]	AP	WEP		-78	-100	22
0219D20227B6	AWS		11		[User-d...	Peer	WEP		-82	-100	18
000FB5987C6D	AWfWLAN		9	54 Mbps		AP	WEP		-80	-100	20
0012CF303BC8	AMX		1		[Fake]	AP			-79	-100	21
000F3DB89618	JDKHome		6	22 Mbps		AP			-83	-100	17
0016E324CFF4	paem		5	54 Mbps	[Fake]	AP	WEP		-89	-100	11
0018F86711D8	AHC				[Fake]	AP	WEP		-92	-100	8
0015E9E431DF	IC		6		[Fake]	AP	WEP		-84	-100	16
00147CBD773F	pinkasa		11	22 Mbps	[Fake]	AP	WEP		-80	-100	20
00179A129D70	stevesaul		6	22 Mbps	[Fake]	AP	WEP		-88	-100	12
00119596110C	DLINK		6	22 Mbps	[Fake]	AP	WEP		-79	-100	21
0016B6A5D1BF	cranleigh		11	54 Mbps	[Fake]	AP	WEP		-77	-100	23
00195B208E74	R.RECORDS_WIRELESS		6	22 Mbps	[Fake]	AP	WEP		-77	-100	23
0018F87DD446	Europe				[Fake]	AP	WEP		-82	-100	18
001B632C3113	Suite 308 - ARDENT		7	11 Mbps	[Fake]	AP	WEP		-85	-100	15
00179412520E	WIRELESS 4		4	22 Mbps	[Fake]	AP	WEP		-82	-100	18
0016E324D38C	KZ		11	54 Mbps	[Fake]	AP	WEP		-75	-100	25
36975340AFFA	notebook		11		[User-d...	Peer	WEP		-82	-100	18
0018BECB4D00	eurocenter		2		[Fake]	AP	WEP		-83	-100	17
00179A613301	Absolute		6		[Fake]	AP	WEP		-72	-100	28
001249C20B8E	bigfamjnet		2	22 Mbps	[Fake]	AP	WEP		-82	-100	18
0013D40FF744	default		1	54 Mbps	[Fake]	AP	WEP		-80	-100	20
001B111318D2	DLINK_WIRELESS		6	22 Mbps	[Fake]	AP			-85	-100	15
00112FD4E8FE	IAE Edu Net-Telstra 1		11	54 Mbps	[Fake]	AP	WEP		-80	-100	20
0030F1D35A0B	Telstra Clear Student		5	11 Mbps	Accton	AP	WEP		-79	-100	21
00184DAD4252	Woosh		11	11 Mbps	[Fake]	AP			-78	-100	22
0015E9CC980A	DLINK		6	22 Mbps	[Fake]	AP	WEP		-60	-100	40
00184DBE8894	Woosh		11	11 Mbps	[Fake]	AP	WEP		-75	-100	25
0018E70584C0	default		6		[Fake]	AP	WEP		-85	-100	15
0015E9CC3676	jchome		6	22 Mbps	[Fake]	AP	WEP		-79	-100	21
00195BF6C9F2	alphanz		6	22 Mbps	[Fake]	AP	WEP		-85	-100	15
00179AD639D8	NZW		6	22 Mbps	[Fake]	AP	WEP		-79	-100	21
0018393C1A34	CITXH09		11	22 Mbps	[Fake]	AP	WEP		-82	-100	18

Ready | Not scanning | GPS: Disabled | 303 / 303

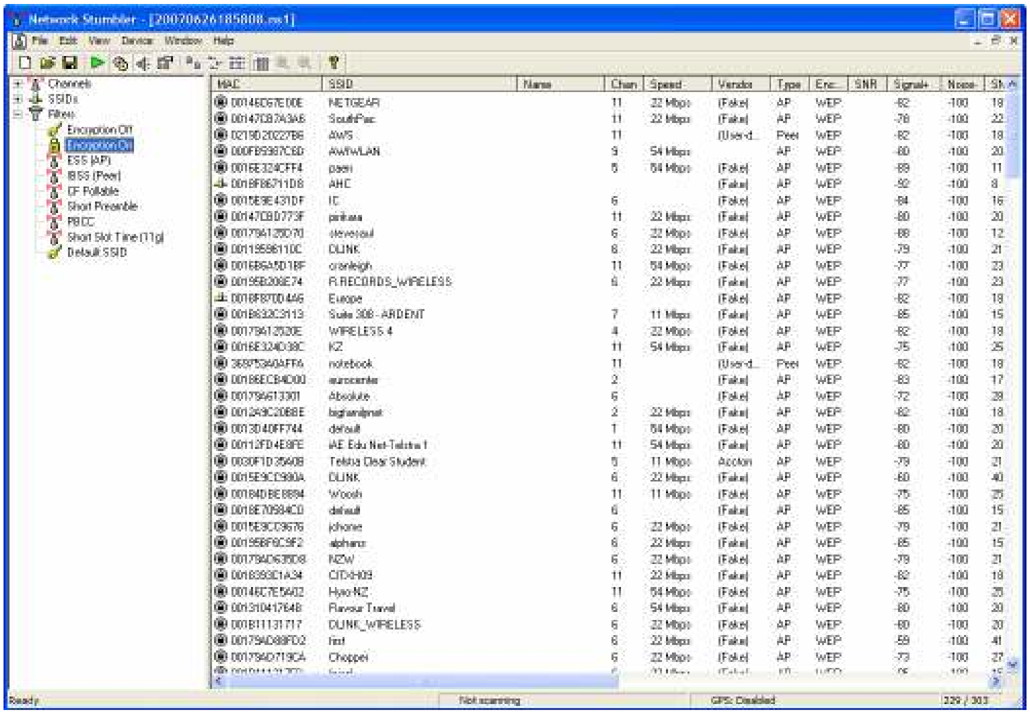
Figure A 7   WLAN (Night Scan)



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SN
0018396A7516	linksys		11	22 Mbps	[Fake]	AP			-74	-100	26
0012CF303BC8	AMX		1		[Fake]	AP			-79	-100	21
000F3DB89618	JDKHome		6	22 Mbps		AP			-83	-100	17
001B111318D2	DLINK_WIRELESS		6	22 Mbps	[Fake]	AP			-85	-100	15
00184DAD4252	Woosh		11	11 Mbps	[Fake]	AP			-78	-100	22
000352F1ED60	Telecom wireless hotspot		11	11 Mbps		AP			-68	-100	32
6A04210CA4C0	Panasonic Display1		10	11 Mbps	[User-d...	Peer			-79	-100	21
0014516F3513	501		1		[Fake]	AP			-78	-100	22
00A00AAB46FB	CellPlus		1	11 Mbps		AP			-66	-100	34
00131ACA4240	SKYCITY		4	54 Mbps	[Fake]	AP			-90	-100	10
001132DAD5B0	SKYCITY		4	54 Mbps	[Fake]	AP			-88	-100	12
00A00AAD404D	CellPlus		11	11 Mbps		AP			-63	-100	37
0018F8746CBD	dingzhotels		11		[Fake]	AP			-82	-100	18
000352F00160	Telecom wireless hotspot		11	11 Mbps		AP			-68	-100	32
00A00AAB46BB	CellPlus		1	11 Mbps		AP			-72	-100	28
000AB74B9452			1	11 Mbps	Cisco	AP			-73	-100	27
00507FD9C240	default		6			AP			-79	-100	21
00A00AAB454D	CellPlus221		1	11 Mbps		AP			-60	-100	40
0080C8AAD897	Atrium		1	22 Mbps	D-Link	AP			-82	-100	18
00A00AAB454C	CellPlus_VoIP		1	11 Mbps		AP			-60	-100	40
00A00AAB45AB	CellPlus		1	11 Mbps		AP			-59	-100	41
000352E3FE00	Telecom wireless hotspot		11	11 Mbps		AP			-66	-100	34
0012178BF3A0	GlobalGcorp		11	54 Mbps	[Fake]	AP			-79	-100	21
00179A1C7ADE	DLINK_WIRELESS		6	22 Mbps	[Fake]	AP			-77	-100	23
6240D03A9597	thanh		11	11 Mbps	[User-d...	Peer			-88	-100	12
0014BF3D5A11	FIVO Internet Hotzone		11	54 Mbps	[Fake]	AP			-79	-100	21
000F249C7341	inter-touch		6	11 Mbps	Cisco	AP			-72	-100	28
0014BF3D6041	Zest L13 - 6		1	54 Mbps	[Fake]	AP			-84	-100	16
000ED748714F	inter-touch		6	11 Mbps	Cisco	AP			-74	-100	26
000ED7B1006B	intertouch		6	11 Mbps	Cisco	AP			-72	-100	28
00904C7E006E	Wei		11	54 Mbps	Epigram	AP			-93	-100	7
0020D8039F6A	notelwlan		11	11 Mbps	NetWa...	AP			-78	-100	22
00168B513B1E	auckland_level3		3	54 Mbps	[Fake]	AP			-89	-100	11
0002E3424177	AMX		11			AP			-85	-100	15
000352E00670	Telecom wireless hotspot		11	11 Mbps		AP			-79	-100	21

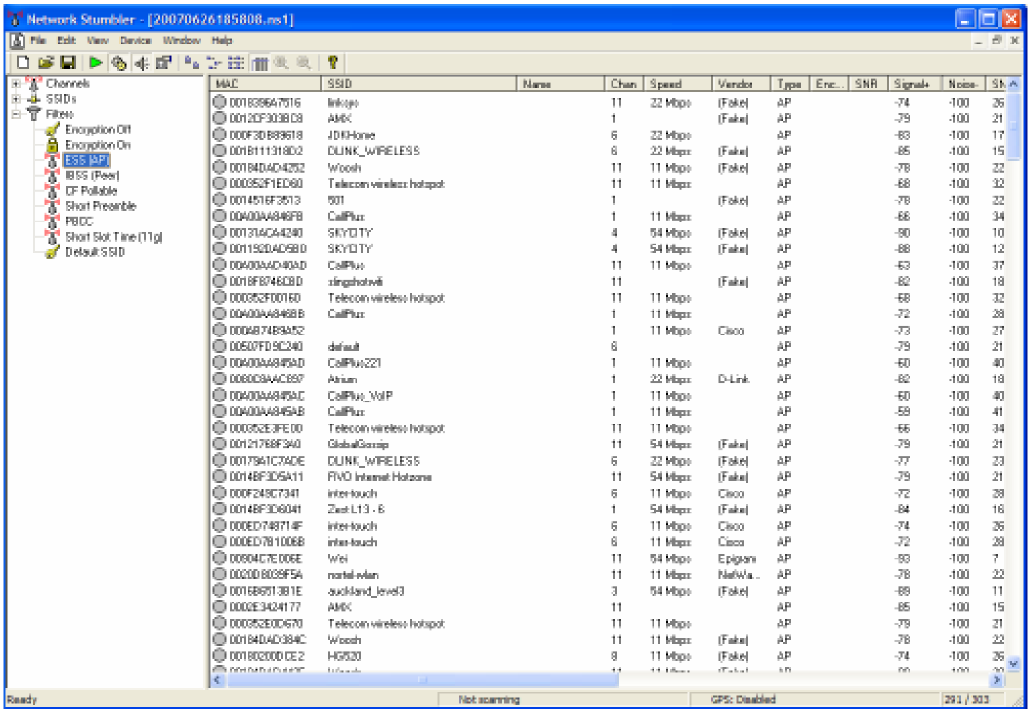
Ready | Not scanning | GPS: Disabled | 74 / 303

Figure A 8 WLAN (Night Scan) with encryption off



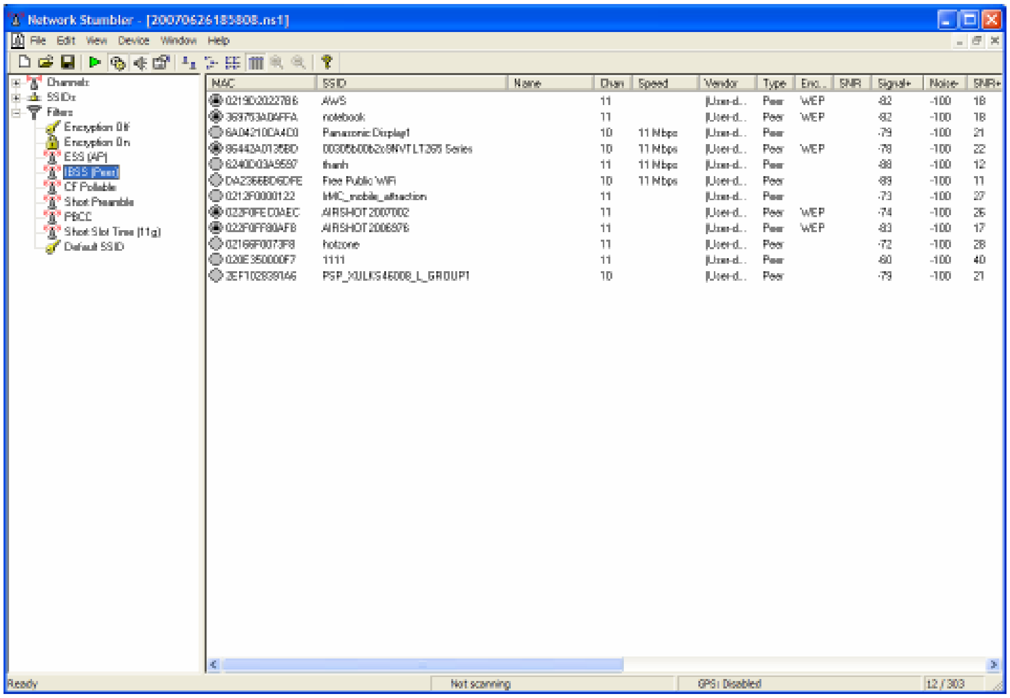
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SN
00146D67E00E	NETGEAR		11	22 Mbps	(Fake)	AP	WEP		-82	-100	18
00147CB7A3A6	SouthPac		11	22 Mbps	(Fake)	AP	WEP		-78	-100	22
02190D2027B6	AWS		11		(User-d...	Peer	WEP		-82	-100	18
000FB5987C6D	AWNWLAN		9	54 Mbps		AP	WEP		-80	-100	20
0016E324CFF4	paeri		5	54 Mbps	(Fake)	AP	WEP		-89	-100	11
0018F86711D8	AHC				(Fake)	AP	WEP		-92	-100	8
0015E9E431DF	IC		6		(Fake)	AP	WEP		-84	-100	16
00147CBD773F	pirikawa		11	22 Mbps	(Fake)	AP	WEP		-80	-100	20
0017961 28D70	steveraul		6	22 Mbps	(Fake)	AP	WEP		-88	-100	12
00119596110C	DLINK		6	22 Mbps	(Fake)	AP	WEP		-79	-100	21
0016B6A5D18F	cranleigh		11	54 Mbps	(Fake)	AP	WEP		-77	-100	23
00195B208E74	R.RECORDS_WIRELESS		6	22 Mbps	(Fake)	AP	WEP		-77	-100	23
0018F870D4A6	Europe				(Fake)	AP	WEP		-82	-100	18
0018632C3113	Suite 308 - ARDENT		7	11 Mbps	(Fake)	AP	WEP		-85	-100	15
00179612520E	WIRELESS 4		4	22 Mbps	(Fake)	AP	WEP		-82	-100	18
0016E324D38C	KZ		11	54 Mbps	(Fake)	AP	WEP		-75	-100	25
3697534 0AFFA	notebook		11		(User-d...	Peer	WEP		-82	-100	18
00186ECB4D00	eurocenter		2		(Fake)	AP	WEP		-83	-100	17
001796613301	Absolute		6		(Fake)	AP	WEP		-72	-100	28
001249C20B8E	bighandjnet		2	22 Mbps	(Fake)	AP	WEP		-82	-100	18
00130 40FF744	default		1	54 Mbps	(Fake)	AP	WEP		-80	-100	20
00112FD4E8FE	IAE Edu Net-Telstra 1		11	54 Mbps	(Fake)	AP	WEP		-80	-100	20
0030F1D35408	Telstra Clear Student		5	11 Mbps	Accton	AP	WEP		-79	-100	21
0015E9CC990A	DLINK		6	22 Mbps	(Fake)	AP	WEP		-60	-100	40
00184DBE8884	Woosh		11	11 Mbps	(Fake)	AP	WEP		-75	-100	25
0018E70984CD	default		6		(Fake)	AP	WEP		-85	-100	15
0015E9CC9676	jphone		6	22 Mbps	(Fake)	AP	WEP		-79	-100	21
00195BF6C9F2	alphanz		6	22 Mbps	(Fake)	AP	WEP		-85	-100	15
00179AD635D8	NZW		6	22 Mbps	(Fake)	AP	WEP		-79	-100	21
0018393C1A34	CITXH03		11	22 Mbps	(Fake)	AP	WEP		-82	-100	18
00146C7E5A02	HyaoNZ		11	54 Mbps	(Fake)	AP	WEP		-75	-100	25
0013104176 4B	Flavour Travel		6	54 Mbps	(Fake)	AP	WEP		-80	-100	20
001B11131717	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP	WEP		-80	-100	20
00179AD88FD2	first		6	22 Mbps	(Fake)	AP	WEP		-59	-100	41
00179AD719CA	Chopper		6	22 Mbps	(Fake)	AP	WEP		-73	-100	27

Figure A 9 Wireless (Night Scan) with encryption on



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SN
001839647516	linksys		11	22 Mbps	(Fake)	AP			-74	-100	26
0012CF3038D8	AMX		1		(Fake)	AP			-79	-100	21
000F3DB89618	JDKHome		6	22 Mbps		AP			-83	-100	17
001B111318D2	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-85	-100	15
00184DAD4252	Woosh		11	11 Mbps	(Fake)	AP			-78	-100	22
000352F1ED60	Telecom wireless hotspot		11	11 Mbps		AP			-68	-100	32
0014516F3513	501		1		(Fake)	AP			-78	-100	22
00A00AA846FB	CallPlus		1	11 Mbps		AP			-66	-100	34
00131ACA4240	SKYCITY		4	54 Mbps	(Fake)	AP			-90	-100	10
001192DAD5BD	SKYCITY		4	54 Mbps	(Fake)	AP			-88	-100	12
00A00AAD40AD	CallPlus		11	11 Mbps		AP			-63	-100	37
0018F8746C8D	slingshotwifi		11		(Fake)	AP			-82	-100	18
000352F00160	Telecom wireless hotspot		11	11 Mbps		AP			-68	-100	32
00A00AA846BB	CallPlus		1	11 Mbps		AP			-72	-100	28
000AB74B9A52			1	11 Mbps	Cisco	AP			-73	-100	27
00507FD9C240	default		6			AP			-79	-100	21
00A00AA845AD	CallPlus221		1	11 Mbps		AP			-60	-100	40
0080C8AAC897	Atrium		1	22 Mbps	D-Link	AP			-82	-100	18
00A00AA845AC	CallPlus_VoIP		1	11 Mbps		AP			-60	-100	40
00A00AA845AB	CallPlus		1	11 Mbps		AP			-59	-100	41
000352E3FE00	Telecom wireless hotspot		11	11 Mbps		AP			-66	-100	34
0012176BF3A0	GlobalGossip		11	54 Mbps	(Fake)	AP			-79	-100	21
0017941C7ADE	DLINK_WIRELESS		6	22 Mbps	(Fake)	AP			-77	-100	23
0014BF3D5A11	FIVO Internet Hotzone		11	54 Mbps	(Fake)	AP			-79	-100	21
000F248C7341	inter-touch		6	11 Mbps	Cisco	AP			-72	-100	28
0014BF3D6041	Zest L13 - 6		1	54 Mbps	(Fake)	AP			-84	-100	16
000ED748714F	inter-touch		6	11 Mbps	Cisco	AP			-74	-100	26
000ED781006B	inter-touch		6	11 Mbps	Cisco	AP			-72	-100	28
00904C7E006E	Wei		11	54 Mbps	Epigram	AP			-93	-100	7
00200B039F5A	nortel-wlan		11	11 Mbps	NetWa...	AP			-78	-100	22
0016B6513B1E	auckland_level3		3	54 Mbps	(Fake)	AP			-89	-100	11
0002E3424177	AMX		11			AP			-85	-100	15
000352E0D670	Telecom wireless hotspot		11	11 Mbps		AP			-79	-100	21
00184DAD384C	Woosh		11	11 Mbps	(Fake)	AP			-78	-100	22
001802000DE2	HG520		8	11 Mbps	(Fake)	AP			-74	-100	26

Figure A 10 WLAN (Night Scan) that are ESS/AP

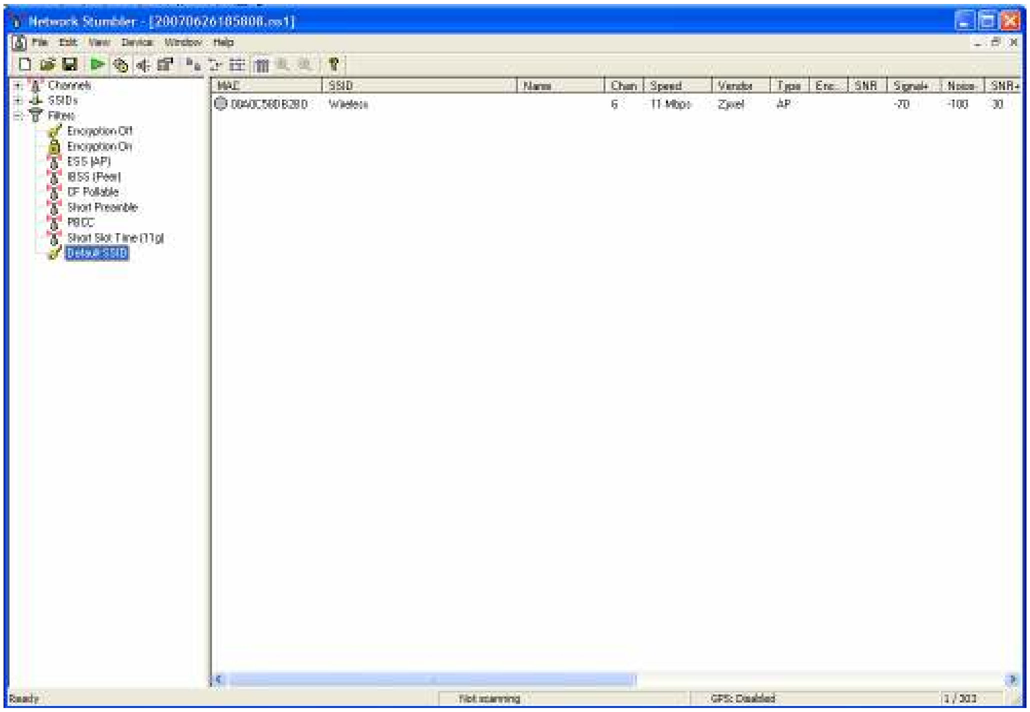


Network Stumbler - [20070626185808.ns1]

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+
0219D20227B6	AWS		11		(User-d...	Peer	WEP		-82	-100	18
369753A04FFA	notebook		11		(User-d...	Peer	WEP		-82	-100	18
6A04210CA4D0	Panasonic Display1		10	11 Mbps	(User-d...	Peer			-79	-100	21
86442A01358D	00305b00b2c9NVT LT265 Series		10	11 Mbps	(User-d...	Peer	WEP		-78	-100	22
6240D03A5597	thanh		11	11 Mbps	(User-d...	Peer			-88	-100	12
DA2366BD6DFE	Free Public WiFi		10	11 Mbps	(User-d...	Peer			-89	-100	11
0212F0000122	IMIC_mobile_attraction		11		(User-d...	Peer			-73	-100	27
022F0FEC0AEC	AIRSHOT 2007002		11		(User-d...	Peer	WEP		-74	-100	26
022F0FF80AF8	AIRSHOT 2006976		11		(User-d...	Peer	WEP		-83	-100	17
02166F0073F8	hotzone		11		(User-d...	Peer			-72	-100	28
020E350000F7	1111		11		(User-d...	Peer			-60	-100	40
2EF102839146	PSP_XULKS46008_L_GROUP1		10		(User-d...	Peer			-79	-100	21

Ready | Not scanning | GPS: Disabled | 12 / 303

Figure A 11 WLAN (Night Scan) that are IBSS/Peer



Network Stumbler - [20070626185808.ns1]

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+
00A0C580B28D	Wireless		6	11 Mbps	Zyxel	AP			-70	-100	30

Ready | Not scanning | GPS: Disabled | 1 / 303

Figure A 12 WLAN (Night Scan) with default SSID

Table A 1 Device Manufacturer (Day Scan)

NIC and AP Manufacturer	Detected	%
D-Link Corporation	114	26.64
NETGEAR Inc	63	14.72
Cisco	48	11.21
Cisco-Linksys	47	10.98
3Com Europe Ltd	18	4.21
Apple Computer	18	4.21
ASKEY COMPUTER CORP.	15	3.50
Colubris Networks	14	3.27
Unidentified Manufacturers	14	3.27
Belkin Corporation	13	3.04
CAMEO COMMUNICATIONS, INC.	6	1.40
ASUSTEK COMPUTER INC.	5	1.17
ShenZhen TP-LINK Technologies Co., Ltd.	5	1.17
Airspan	4	0.93
Accton Technology Corp.	3	0.70
Airespace, Inc.	3	0.70
ZYXEL COMMUNICATION	3	0.70
Digital Data Communications Asia Co.,Ltd	2	0.47
EPIGRAM, INC.	2	0.47
GemTek Technology Co., Ltd.	2	0.47
Giga-Byte	2	0.47
SMC Networks, Inc.	2	0.47
The Linksys Group, Inc.	2	0.47
TP-LINK Technologies Co., Ltd.	2	0.47
U.S. Robotics Corporation	2	0.47
Agere Systems	1	0.23
AirVast Technology Inc.	1	0.23
Ambit Microsystems Corporation	1	0.23
CC&C Technologies, Inc.	1	0.23
DELTA NETWORKS, INC.	1	0.23
DrayTek Corp.	1	0.23
Edimax Technology Co., Ltd.	1	0.23
Hon Hai Precision Ind. Co., Ltd.	1	0.23
KeunYoung Electronics & Communication Co., Ltd.	1	0.23
Nortel Networks	1	0.23
PROXIM, INC.	1	0.23
QTelNet, Inc.	1	0.23
REMOTEK CORPORATION	1	0.23
Routerboard.com	1	0.23
Senao International Co., Ltd.	1	0.23
SONIC SYSTEMS, INC.	1	0.23
SparkLAN Communications, Inc.	1	0.23
SYMBOL TECHNOLOGIES, INC.	1	0.23
TurboComm Tech Inc.	1	0.23
Total	428	100.00

Table A 2 Device Manufacturer (Night Scan)

NIC and AP Manufacturer	Detected	%
D-Link Corporation	68	22.44
NETGEAR Inc	50	16.50
Cisco-Linksys	36	11.88
Cisco	35	11.55
3Com Europe Ltd	16	5.28
Unidentified Manufacturers	13	4.29
Apple Computer	12	3.96
Belkin Corporation	9	2.97
Colubris Networks	9	2.97
Airspan	6	1.98
ASKEY COMPUTER CORP.	6	1.98
Cameo Communications, INC.	6	1.98
ASUSTek Computer Inc.	5	1.65
Airespace, Inc.	3	0.99
ShenZhen TP-LINK Technologies Co., Ltd.	3	0.99
The Linksys Group, Inc.	3	0.99
Accton Technology Corp.	2	0.66
Edimax Technology Co., Ltd.	2	0.66
Agere Systems	1	0.33
Alpha Networks Inc.	1	0.33
CABLETRON - NETLINK, INC.	1	0.33
CC&C Technologies, Inc.	1	0.33
DELTA NETWORKS, INC.	1	0.33
DrayTek Corp.	1	0.33
EPIGRAM, INC.	1	0.33
GemTek Technology Co., Ltd.	1	0.33
Hon Hai Precision Ind. Co., Ltd.	1	0.33
LIBIT SIGNAL PROCESSING, LTD.	1	0.33
LITE-ON Communications, Inc.	1	0.33
Nortel Networks	1	0.33
PROXIM, INC.	1	0.33
REMOTEK CORPORATION	1	0.33
SMC Networks, Inc.	1	0.33
SparkLAN Communications, Inc.	1	0.33
SYMBOL TECHNOLOGIES, INC.	1	0.33
TP-LINK Technologies Co., Ltd.	1	0.33
ZYXEL COMMUNICATION	1	0.33
Total	303	100.00

Table A 3 MAC addresses detected in both day and night scans

Total detected: 225

(00:02:2d:01:1f:10)
(00:03:52:d7:2a:40)
(00:03:52:e0:d6:70)
(00:03:52:e1:82:20)
(00:03:52:e3:fe:00)
(00:03:52:eb:32:e0)
(00:03:52:ef:fc:10)
(00:03:52:f0:01:60)
(00:03:52:f1:0e:a0)
(00:03:52:f1:ed:60)
(00:09:5b:95:ae:9c)
(00:09:5b:d9:a2:ba)
(00:0a:50:00:1c:92)
(00:0a:b7:4b:9a:52)
(00:0b:85:0c:76:fd)
(00:0b:85:0c:76:fe)
(00:0b:85:0c:76:ff)
(00:0c:41:66:8a:a1)
(00:0c:41:c1:b9:1d)
(00:0d:54:fb:e4:e8)
(00:0e:6a:d3:a9:27)
(00:0e:8e:7a:d4:d1)
(00:0e:d7:48:71:4f)
(00:0f:24:9c:73:41)
(00:0f:3d:3d:27:7c)
(00:0f:3d:9e:5b:ce)
(00:0f:3d:b4:97:56)
(00:0f:3d:b8:91:22)
(00:0f:66:4b:cf:c3)
(00:0f:b5:3a:16:17)
(00:0f:b5:98:7c:6d)
(00:11:24:9c:c6:3f)
(00:11:24:eb:25:5d)
(00:11:2f:d4:e8:fe)
(00:11:50:60:20:74)
(00:11:50:86:da:3e)
(00:11:50:c9:54:57)
(00:11:50:e8:ee:28)
(00:11:50:eb:b6:a8)
(00:11:92:a9:68:d0)
(00:11:92:da:d5:b0)
(00:11:95:0a:3c:0f)
(00:11:95:7e:6c:c2)
(00:11:95:96:11:0c)
(00:11:95:9f:fc:14)
(00:11:95:a0:09:74)
(00:11:95:bf:6e:e1)
(00:11:f5:10:c2:c0)
(00:12:17:68:f3:a0)
(00:12:17:75:04:b5)
(00:12:17:80:28:de)
(00:12:17:b9:ee:1f)
(00:12:44:b3:14:70)
(00:12:44:b3:15:60)
(00:12:44:b3:1e:60)
(00:12:a9:c2:0a:7a)
(00:12:a9:c2:0b:be)
(00:12:a9:d4:26:d6)
(00:12:cf:30:3b:c8)
(00:13:10:41:76:4b)
(00:13:10:41:78:c7)
(00:13:1a:ca:42:40)
(00:13:46:0c:c4:3a)
(00:13:d4:0f:f7:44)
(00:13:f7:09:b1:49)
(00:14:51:6f:35:13)
(00:14:51:71:9d:69)
(00:14:6c:12:f2:02)
(00:14:6c:67:e0:0e)
(00:14:6c:7e:5a:02)
(00:14:6c:9c:17:50)
(00:14:6c:9e:0b:aa)
(00:14:6c:b1:73:c6)
(00:14:6c:d0:28:3c)
(00:14:6c:f5:a3:1a)
(00:14:78:8e:5f:88)
(00:14:78:e4:85:6e)
(00:14:7c:ad:3c:5c)
(00:14:7c:b7:a3:a6)
(00:14:7c:bc:c0:a7)
(00:14:7c:bc:d7:93)
(00:14:7c:bd:77:3f)
(00:14:7c:bd:9d:a5)
(00:14:a4:10:4f:70)
(00:14:bf:2f:72:b4)
(00:14:bf:3d:5a:11)
(00:14:bf:3d:63:da)
(00:14:bf:48:c1:0e)
(00:14:f2:8f:84:b0)
(00:15:e9:0b:70:58)
(00:15:e9:25:07:48)
(00:15:e9:25:0f:b4)
(00:15:e9:cc:09:b4)
(00:15:e9:cc:96:76)
(00:15:e9:cc:98:0a)
(00:15:e9:cd:bc:92)
(00:15:e9:e4:31:df)
(00:16:46:9b:c5:30)
(00:16:46:aa:cc:50)
(00:16:b6:13:d0:bb)
(00:16:b6:1d:f0:87)
(00:16:b6:51:3b:1e)
(00:16:b6:51:3b:e2)
(00:16:b6:52:d6:7b)
(00:16:b6:a5:d1:bf)
(00:16:b6:b4:9f:74)
(00:16:c7:7f:a6:00)
(00:16:e3:24:cf:f4)
(00:16:e3:24:d3:8c)
(00:16:e3:64:8a:9c)
(00:16:e3:6f:0e:77)
(00:17:3f:0b:ff:74)
(00:17:3f:81:7b:58)
(00:17:94:3b:e8:30)
(00:17:94:3b:e8:90)
(00:17:94:3b:f9:50)
(00:17:94:3b:f9:70)
(00:17:95:81:9f:c0)
(00:17:9a:11:fb:a4)
(00:17:9a:11:fd:3c)
(00:17:9a:12:03:8c)
(00:17:9a:12:5c:24)
(00:17:9a:12:5d:70)
(00:17:9a:13:88:a6)
(00:17:9a:1c:19:8c)
(00:17:9a:1c:4f:38)
(00:17:9a:1c:7a:de)
(00:17:9a:1d:8c:ee)
(00:17:9a:1e:e4:76)
(00:17:9a:1e:ef:e4)
(00:17:9a:1f:f6:f0)
(00:17:9a:61:33:01)
(00:17:9a:61:37:51)
(00:17:9a:d6:33:52)
(00:17:9a:d6:35:78)
(00:17:9a:d6:35:d8)
(00:17:9a:d6:38:0a)
(00:17:9a:d8:8a:ea)
(00:17:9a:d8:8d:9c)
(00:17:9a:d8:8f:d2)
(00:17:9a:d8:95:9a)
(00:17:df:11:3f:e0)
(00:18:39:22:59:b8)
(00:18:39:23:b5:86)
(00:18:39:3c:1a:34)
(00:18:39:6a:7b:0a)
(00:18:4d:ad:36:68)
(00:18:4d:ad:36:d0)
(00:18:4d:ad:37:56)
(00:18:4d:ad:38:4c)
(00:18:4d:ad:42:0c)
(00:18:4d:ad:42:14)
(00:18:4d:ad:42:52)
(00:18:4d:ad:43:48)
(00:18:4d:ad:44:2a)
(00:18:4d:ad:44:3e)
(00:18:4d:be:81:9e)
(00:18:4d:be:81:dc)
(00:18:4d:be:83:2c)
(00:18:4d:be:86:4a)
(00:18:4d:be:88:94)
(00:18:4d:be:8a:0c)
(00:18:4d:be:8b:cc)
(00:18:4d:f9:34:ca)
(00:18:4d:f9:35:e6)
(00:18:6e:06:70:a6)
(00:18:6e:09:0b:77)
(00:18:f8:36:7f:57)
(00:18:f8:67:11:d8)
(00:18:f8:70:d4:a6)
(00:18:f8:74:6c:bd)
(00:18:f8:f9:7b:ad)
(00:19:5b:02:f0:aa)
(00:19:5b:1f:1f:d2)
(00:19:5b:20:4c:da)
(00:19:5b:20:63:b4)
(00:19:5b:20:65:fe)
(00:19:5b:20:6e:74)
(00:19:5b:20:72:76)
(00:19:5b:8d:0c:90)
(00:19:5b:9b:0e:04)
(00:19:5b:f6:c9:f2)
(00:19:e0:97:e9:95)
(00:19:e3:e3:47:f7)
(00:1a:30:30:83:90)
(00:1a:70:5b:d4:f3)
(00:1a:a1:69:6c:50)
(00:1b:11:13:17:17)
(00:1b:11:13:18:d2)
(00:1b:11:13:1d:ea)
(00:1b:11:87:61:5c)
(00:1b:2a:23:5c:30)
(00:1b:2f:47:bb:28)
(00:1b:2f:4d:7b:e0)
(00:1b:63:22:74:f5)
(00:1b:63:2c:31:13)

MAC addresses detected in both day and night scans (continue)

```
( 00:1c:0e:26:e2:30 )
( 00:1c:10:1a:3b:36 )
( 00:20:a6:4f:42:e6 )
( 00:20:d8:03:9f:5a )
( 00:30:ab:1e:08:fa )
( 00:30:f1:d3:5a:0b )
( 00:40:96:25:90:f3 )
( 00:40:96:25:98:29 )
( 00:40:f4:e0:23:47 )
( 00:40:f4:e0:24:6f )
( 00:40:f4:fa:cc:1f )
( 00:40:f4:fd:cb:fa )
( 00:50:7f:d9:c2:40 )
( 00:60:b3:19:8c:34 )
( 00:80:c8:aa:c8:97 )
( 00:90:4b:63:43:20 )
( 00:90:4c:7e:00:6e )
( 00:a0:0a:a8:46:bb )
( 00:a0:0a:a8:46:fb )
( 00:a0:0a:ad:40:ad )
( 00:a0:c5:8d:b2:b0 )
( 00:a0:f8:db:fa:cc )
( 02:2f:0f:ec:0a:ec )
( 02:2f:0f:f8:0a:f8 )
( 08:10:73:09:cc:f0 )
( 00:0e:2e:6f:12:2c )
( 00:11:24:08:51:e9 )
( 00:17:9a:d9:05:88 )
( 00:18:4d:5e:63:b2 )
```

Table A 4 MAC addresses detected in day scan only

Total Detected: 203

(00:02:6f:35:3b:62)
(00:02:72:59:ee:75)
(00:02:8a:9e:4c:65)
(00:03:52:e4:64:b0)
(00:03:52:e9:53:20)
(00:03:52:e9:5d:40)
(00:03:52:f0:02:50)
(00:03:52:f8:c0:a0)
(00:03:93:ea:b8:3f)
(00:04:e2:d6:e0:c9)
(00:05:5d:80:03:04)
(00:09:5b:85:b6:6e)
(00:09:5b:de:2e:ee)
(00:09:5b:e6:ba:60)
(00:0a:b7:4b:9c:3a)
(00:0a:e9:0f:f1:4b)
(00:0c:42:0c:22:3f)
(00:0d:54:9b:7d:9e)
(00:0d:88:93:8f:52)
(00:0d:93:eb:a8:cc)
(00:0e:84:83:77:1f)
(00:0e:a6:c0:49:17)
(00:0f:3d:09:6f:ab)
(00:0f:3d:28:1c:1f)
(00:0f:3d:b3:6d:b4)
(00:0f:3d:b3:ee:74)
(00:0f:3d:b3:f0:d8)
(00:0f:3d:b4:00:20)
(00:0f:3d:b4:07:f2)
(00:0f:3d:b6:9d:2a)
(00:0f:3d:fb:4f:98)
(00:0f:3d:fb:50:7e)
(00:0f:b5:98:7a:ed)
(00:0f:b5:9d:89:a3)
(00:11:24:01:e4:cf)
(00:11:24:0b:0b:11)
(00:11:24:24:19:06)
(00:11:24:5d:1b:8f)
(00:11:24:5d:43:2f)
(00:11:2f:cb:e1:7f)
(00:11:2f:cb:e1:82)
(00:11:50:26:cc:da)
(00:11:50:61:3f:62)
(00:11:50:84:6f:48)
(00:11:50:e9:b8:8d)
(00:11:50:f0:e0:0e)
(00:11:50:fa:e9:6e)
(00:11:6b:22:dd:68)
(00:11:6b:30:81:cb)
(00:11:92:8d:e8:00)
(00:11:92:da:f3:d0)
(00:11:93:3d:7b:c0)
(00:11:95:64:d4:04)
(00:11:95:95:d3:86)
(00:11:95:e5:c3:47)
(00:11:95:e9:93:f2)
(00:11:f5:8d:28:f5)
(00:12:17:3a:54:9d)
(00:12:17:68:f3:b9)
(00:12:17:7a:e1:e8)
(00:12:17:b4:a6:0e)
(00:12:a9:55:0f:82)
(00:12:a9:c3:b5:fe)
(00:12:cf:13:52:c0)
(00:13:10:41:72:d9)
(00:13:10:7d:d4:88)
(00:13:10:d9:e8:90)
(00:13:46:27:01:b3)
(00:13:46:27:05:f0)
(00:13:46:3e:6a:3e)
(00:13:46:c8:83:96)
(00:13:49:2f:67:8b)
(00:14:1c:83:35:90)
(00:14:1c:83:38:90)
(00:14:51:6c:da:6d)
(00:14:51:70:c5:93)
(00:14:51:78:ad:fd)
(00:14:69:f2:cc:70)
(00:14:6c:9e:12:76)
(00:14:6c:da:af:78)
(00:14:78:8e:6d:f0)
(00:14:78:eb:24:02)
(00:14:78:f7:22:be)
(00:14:7c:b7:93:64)
(00:14:85:bd:51:5b)
(00:14:bf:3d:5e:c4)
(00:14:bf:3d:62:33)
(00:14:bf:48:c1:10)
(00:14:bf:48:c3:94)
(00:14:bf:7f:c8:99)
(00:14:c1:1a:78:24)
(00:14:f1:61:63:c0)
(00:14:f2:fc:31:50)
(00:15:2c:48:70:40)
(00:15:e9:0a:c4:b8)
(00:15:e9:a9:0d:9c)
(00:15:e9:cd:bd:94)
(00:16:b6:49:30:93)
(00:16:b6:5f:db:eb)
(00:16:c8:fa:26:a0)
(00:16:c8:fa:29:a0)
(00:16:c8:fa:29:f0)
(00:16:c8:fa:30:b0)
(00:16:e3:2a:56:e0)
(00:16:e3:48:61:83)
(00:16:e3:64:8a:e4)
(00:16:e3:6f:29:7f)
(00:16:e3:6f:34:2b)
(00:16:e3:6f:39:9f)
(00:17:0f:83:38:a0)
(00:17:94:3b:fa:b0)
(00:17:9a:11:fd:58)
(00:17:9a:12:09:34)
(00:17:9a:12:45:92)
(00:17:9a:12:5c:58)
(00:17:9a:1c:7e:ce)
(00:17:9a:1c:f0:14)
(00:17:9a:1c:f1:68)
(00:17:9a:1c:f1:8c)
(00:17:9a:1d:8b:40)
(00:17:9a:1e:e0:64)
(00:17:9a:1e:e3:64)
(00:17:9a:1e:e5:ee)
(00:17:9a:1f:0c:f0)
(00:17:9a:5b:d9:8d)
(00:17:9a:66:94:7f)
(00:17:9a:d6:35:ca)
(00:17:9a:d6:3e:12)
(00:17:9a:d8:9a:1e)
(00:17:9a:d9:05:50)
(00:18:39:0c:8a:de)
(00:18:39:22:37:f4)
(00:18:39:6a:79:f4)
(00:18:4d:55:6a:ac)
(00:18:4d:55:6e:28)
(00:18:4d:5e:40:6e)
(00:18:4d:5e:65:76)
(00:18:4d:9c:09:96)
(00:18:4d:ad:37:4e)
(00:18:4d:ad:39:66)
(00:18:4d:ad:3c:26)
(00:18:4d:ad:3c:dc)
(00:18:4d:ad:3e:ca)
(00:18:4d:ad:3f:60)
(00:18:4d:ad:43:fe)
(00:18:4d:ad:45:2e)
(00:18:4d:be:83:da)
(00:18:4d:be:85:94)
(00:18:4d:be:8a:5e)
(00:18:4d:f9:3b:e0)
(00:18:6e:ca:9b:d0)
(00:18:b9:b3:d2:d0)
(00:18:f8:f7:96:ac)
(00:19:07:35:42:e0)
(00:19:5b:20:50:ba)
(00:19:5b:20:53:1c)
(00:19:5b:20:54:e2)
(00:19:5b:20:5f:54)
(00:19:5b:20:64:68)
(00:19:5b:20:6c:64)
(00:19:5b:20:6f:4c)
(00:19:5b:20:74:d6)
(00:19:5b:20:75:90)
(00:19:5b:9a:ea:d0)
(00:19:5b:9a:ef:28)
(00:19:5b:9a:f8:72)
(00:19:5b:9c:3f:b8)
(00:19:5b:bf:c5:cd)
(00:19:5b:bf:cb:bd)
(00:19:e0:96:b0:dc)
(00:1a:a2:fc:e5:d0)
(00:1b:2f:07:54:ec)
(00:1b:2f:07:55:00)
(00:1b:2f:4d:86:56)
(00:1b:2f:4d:8a:f0)
(00:1b:2f:4d:8b:40)
(00:20:ed:0f:ff:e3)
(00:30:3f:51:bc:a0)
(00:30:4f:3f:38:2e)
(00:40:10:10:00:03)
(00:40:96:25:9e:f2)
(00:40:96:3a:11:7c)
(00:40:96:44:50:95)
(00:40:f4:b8:5e:75)
(00:40:f4:de:fe:1a)
(00:90:4b:63:40:23)
(00:90:4c:91:00:01)
(00:90:96:5d:35:a6)
(00:90:96:cf:44:b4)
(00:90:96:fb:aa:52)
(00:a0:0a:a8:47:9b)
(00:a0:c5:41:8f:a0)
(00:c0:49:e7:e4:a5)
(00:f2:26:f2:a5:05)
(02:12:f0:00:25:a7)
(02:16:6f:01:26:d4)

MAC addresses detected in day scan only (continue)

```
( 02:18:de:89:f6:9b )
( 02:94:5e:6b:00:9e )
( 0a:82:27:ad:81:f6 )
( 0a:dd:5d:3c:70:d3 )
( 0e:70:c4:01:be:89 )
( 2e:1e:23:a5:b7:55 )
( c6:a9:fb:1c:46:30 )
( ea:33:69:87:ff:5f )
```

Table A 5 MAC addresses detected in night scan only

Total Detected: 78

(00:02:72:63:30:b4)
(00:02:e3:42:41:77)
(00:0c:41:8a:a7:56)
(00:0e:2e:6a:58:02)
(00:0e:d7:b1:00:6b)
(00:0f:3d:b8:96:18)
(00:0f:90:13:61:39)
(00:11:24:08:af:27)
(00:11:24:0b:0c:1f)
(00:11:24:ec:da:f3)
(00:11:2f:61:48:ee)
(00:11:2f:d4:e8:2b)
(00:11:50:fa:38:6e)
(00:11:d8:b7:fb:7a)
(00:12:17:3b:f6:4b)
(00:12:17:68:f1:2e)
(00:14:6c:62:c4:48)
(00:14:6c:97:d2:5a)
(00:14:6c:d0:33:62)
(00:14:78:eb:f0:8c)
(00:14:7c:bd:4a:5a)
(00:14:7c:be:19:92)
(00:14:bf:3d:60:41)
(00:14:bf:c3:88:86)
(00:15:c6:82:9d:b0)
(00:16:46:a9:e7:30)
(00:16:e3:6f:20:13)
(00:17:3f:5a:ff:1f)
(00:17:9a:12:52:0e)
(00:17:9a:66:97:1f)
(00:17:9a:d7:19:ca)
(00:18:02:00:dc:e2)
(00:18:39:6a:75:16)
(00:18:39:a2:e7:b9)
(00:18:4d:5e:3f:02)
(00:18:4d:5e:40:a0)
(00:18:4d:ad:3d:28)
(00:18:4d:be:85:7e)
(00:18:4d:be:8a:24)
(00:18:6e:cb:4d:00)
(00:18:e7:05:84:c0)
(00:18:f8:70:d4:a8)
(00:19:5b:20:53:1c)
(00:19:5b:20:6e:ac)
(00:19:e3:0e:3c:d2)
(00:1b:11:0a:30:1a)
(00:1b:11:13:17:fb)
(00:1b:11:13:17:fd)
(00:1b:11:15:69:ee)
(00:1b:2f:07:72:2e)
(00:1b:2f:07:74:d4)
(00:1b:2f:47:bd:e4)
(00:1b:2f:4d:7f:52)
(00:1b:2f:4d:82:32)
(00:1b:2f:4d:8e:8a)
(00:1b:2f:57:58:48)
(00:1c:0e:26:a1:00)
(00:1c:0e:26:da:70)
(00:1c:0e:27:48:40)
(00:1c:0e:d4:b7:a0)
(00:1c:0e:d6:36:90)
(00:1c:57:89:17:f0)
(00:20:a6:62:dc:ca)
(00:40:f4:b8:68:b8)
(00:50:f1:12:12:10)
(00:a0:0a:a8:45:ab)
(00:a0:0a:a8:45:ac)
(00:a0:0a:a8:45:ad)
(02:0e:35:00:00:f7)
(02:12:f0:00:01:22)
(02:16:6f:00:73:f8)
(02:19:d2:02:27:b6)
(2e:f1:02:83:91:a6)
(36:97:53:a0:af:fa)
(62:40:d0:3a:95:97)
(6a:04:21:0c:a4:c0)
(86:44:2a:01:35:bd)
(da:23:66:bd:6d:fe)
(6a:04:21:0c:a4:c0)
(86:44:2a:01:35:bd)
(da:23:66:bd:6d:fe)

Appendix 2: Network Simulation Software

Computer network simulators are essential in the evaluation and designing of networking protocols and distributed networking systems (Walsh & Sirer, 2004). In the area of wireless ad hoc and sensor networks, simulators can be used to evaluate new systems and protocols based on various deployment scenarios (Jardosh, Belding-Royer, Almeroth, & Suri, 2003; Walsh & Sirer, 2004). Simulator can also be used to test other ubiquitous devices such as Bluetooth that may need to co-exist with 802.11 devices (Bethala, Joshi, Phatak, Avancha, & Goff, 2002). As in wired LAN, it is also very important that a well-established simulation technique is followed when evaluating a WLAN. This would include a descriptive WLAN experimental study scenarios (Perrone, Yuan, & Nicol, 2003).

However, choosing a suitable wireless network simulator for a business and its application requires a thorough assessment of the available simulation software in term of its performance, scalability and reliability. The current wireless network simulation software are available both as commercial and open source products. The most important aspect of a network simulator or model is in its ability to correctly match the generated network model to the real life WLAN topology. The network simulator must be able to modeled scenarios such as link failure, device failure, load change, route change, link change, and link overloading (Fritz, 2004). The rule to accurately assess the performance of a wireless network, is to develop and implement a valid network simulation model that will therefore ensure a valid and repeatable network simulation experiment (Pawlikowski, Jeong, & Lee, 2002).

The network simulators that are available both commercially and open source which can be utilized by the businesses in Auckland CBD or anywhere else to evaluate their current or future wireless network are as follow.

Shunra Virtual Enterprise (Shunra VE) 5.0: This application will provides an accurate modeling and analyzing of network performance (Shunra, 2007). Shunra is a hardware-based application therefore provide more advantage in terms of performance when compared to a software-based simulation application (Fritz, 2004; Markus, 2004).

QualNet Developer: QualNet offers distributed and parallel network simulator that can model large scale LAN and WLAN with heavy traffic (Scalable Network Technologies, 2007).

NetSim: Tetcos (2007) mentioned that NetSim software is capable to provide network simulation to various protocols such as the WLAN, Ethernet, TCP / IP, and ATM as well as wireless devices such as routers and AP (Tetcos, 2007).

OPNET (Optimized Network Engineering Tools): This tool was developed by MIL3 Inc. for simulation of communications protocols, devices and networks, which specializes in discrete-event simulation (Chang & Li, 2003). Opnet developed the "Modeler Wireless Suite" specifically to support wireless network simulation (Opnet, 2007).

P2PRealm: This is a peer-to-peer simulator. P2PRealm is an efficient peer-to-peer network simulator that can be used to study algorithms based on neural networks (Kotilainen, Vapa, Keltanen, Auvinen, & Vuori, 2006).

The Georgia Tech Network Simulator: The design of the GTNetS strongly matches that of real network protocol hardware, therefore anyone with an understanding of networking can quickly understand the construction of this simulator (MANIACS, n.d.; Riley, 2003).

Nessi: Nessi attempts to minimize the development time and the difficulties of implementing simulation (Vernez, Ehrensberger, & Robert, 2006). It can be used to visualize and observe the behaviors of networks protocol (Vernez, Ehrensberger, & Robert, 2006).

NS-2: NS-2 provides sufficient support for simulation of routing, multicast and TCP protocols over wired and wireless networks (Ye & MacGregor, 2006).

GloMoSim: GloMoSim is a library-based parallel and sequential simulator developed to support both wireless and wired network systems which provides evaluation of various wireless network protocols (GloMoSim, 2001).

A summary of these network simulators are as in Table A 6.

Simulator	Web Address	Type	Scale	Network Impairments	Network Topologies	Advantages	Disadvantages
Shunra VE	http://www.shunra.com	Commercial	Enterprise	Latency, bandwidth, jitter and packet loss, bandwidth congestion and utilization.	Point-to-point, NTier, hub and spoke, fully meshed networks.	Hardware based simulator, technical support, empirical model that uses real-life appliances provides better accuracy.	Needs networks infrastructure to be available before running Shunra.
QualNet Developer	http://www.qualnet.com	Commercial	Enterprise	Evaluation of various protocols.	Wired and WLAN and WAN	Support thousands of nodes. Run on variety of OS an also on both 32 & 64 bit computing environment, offers technical support, downloadable from the web.	Lack of predefined model constructs. Lack of parameter documentation. The process is time consuming due to missing modularity and reusability.
Netsim	http://www.tetcos.com/software.html	Commercial and Academic	Large scale	Relative positions of stations, realistic modeling of signal propagation, collision handling and detection process	WLAN, Ethernet, TCP / IP, and ATM	Compatible with both Windows and Linux environment.	More of an educational network simulator.
Opnet	http://www.opnet.com	Commercial	Enterprise	Link models such as bus and point-to-point, queuing service	ATM, TCP, FDDI, IP, Ethernet, Frame Relay, and WLAN	High level of modeling detail. The result parameters are comprehensive. Customizable Presentation of result diagrams is customizable. Easy to use GUI.	The parameter categorization is not transparent and confusing. There is insufficient documentation of attributes.
P2PRealm	Developer site: http://www.mit.jyu.fi/cheesefactory/	Open source	Small scale	Verify P2P network requirements, resource discovery	Wireless peer to peer (P2P)	Developed for optimizing neural networks used in P2P networks.	Still in research. Only for P2P.
GTNetS	http://www.ece.gatech.edu/research/labs/MANIACS/GTNetS/	Open source	Large scale	Packet tracing, queuing methods, statistical methods, random number generator etc.	Point-to-Point, Shared and switched Ethernet, and Wireless links.	The design of the GTNetS closely matches the design of real network protocol hardware and stacks.	No support available. Ongoing development.
Nessi	Information not available	Open source	Small scale	Evaluation of new protocols.	Wired and WLAN	Developed to minimize the development time and ease of implementation.	Only suitable for academic purposes.
NS-2	http://www.isi.edu/nsnam/ns/ns-build.html	Open source	Small scale	Congestion control, transport protocols, queuing and routing algorithms, and multicast work.	Routing, multicast and TCP protocols over wired and WLAN	Free for research and teaching. Downloadable through website.	No support available. Poor usability
GloMoSim	http://pcl.cs.ucla.edu/projects/glomosim/GloMoSimManual.html	Open source	Large scale	Evaluation of various wireless network protocols includes models for the channel, transport, radio, MAC networks etc.	WLAN	Scalable simulator that support thousand of network nodes.	Only for wireless networks

Table A 6 Summary of Network Simulators