Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2004 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 2004

Wireless Network Security in Australia: A Study of 7 Australian Capital Cities

Mathew Hannan
University of South Australia

Benjamin Turnbull
University of South Australia

WIRELESS NETWORK SECURITY IN AUSTRALIA: A STUDY OF 7 AUSTRALIAN CAPITAL CITIES

Mat Hannan
School of Accounting and Information Systems
University of South Australia
Mathew.Hannan@unisa.edu.au

Benjamin Turnbull
B.IT (Hons)
University of South Australia
Benjamin.Turnbull@unisa.edu.au

Abstract

Wireless network technology is rapidly being adopted by individuals and organizations as an alternative to existing 'wired' networking solutions. This research was undertaken to provide a foundation study of 802.11b wireless network security in Australian capital cities. The study employs Wardriving using the Network Stumbler program to collect sample data upon which results are based. The same methodology was replicated across the central business districts of Adelaide, Brisbane, Canberra, Hobart, Melbourne, Perth and Sydney. The research discovered that 729 wireless networks were in operation in 7 Australian Capital Cities and 14.6% have failed to implement even rudimentary security practices. Further the research demonstrated the ease with which the level of security of wireless networks can be evaluated.

It is anticipated that this research will provide the foundation for a time-series analysis of Australian Wireless Network security, as well as provide a basis for international comparative work in this area.

Keywords: Wireless, Networking, 802.11b, Australia, Wardriving

1. Introduction

Wireless network technology is rapidly being adopted by individuals and organizations as an alternative to existing 'wired' networking solutions. Using Radio-Frequency gives enormous flexibility, but may open a seemingly secure network to new threats of network intrusion. This paper details a study of the security level of wireless networks in the central business district (CBD) of 7 Australian Capital cities.

This research was undertaken to provide a foundation study of 802.11b wireless network security in Australia. The study determines current basic wireless security levels and to provide a basis upon which future research can be conducted and compared.

The purpose of the research was to demonstrate the ease and relative low-cost with which the security features of wireless networks can be perimeter tested both internally or by malicious users for the purpose of mounting an attack on the network.

Although there has been previous research in this area in Australia targeting individual cities (Webb 2003; Turnbull, Nicholson and Slay 2003), there has been no previous comparison of the level of wireless network security across multiple cities.

The methodology employed to collect data upon which results are based was replicated across the central business districts of Adelaide, Brisbane, Canberra, Hobart, Melbourne, Perth and Sydney.

The research discovered that 729 wireless networks were in operation in Australian Capital Cities and 15.3% of them have failed to implement even the most rudimentary security practices. Further the research demonstrated the ease with which the level of security of wireless networks can be evaluated.

The study identifies the need for vigilance by individuals and organizations adopting this increasingly popular networking technology.
It is anticipated that this research will provide the foundation for a time-series analysis of Australian Wireless Network security, as well as provide a basis for international comparative work in this area.

2. Background Information

This section of the paper provides an overview of important topics and issues that are associated with this research.

2.1 Wardriving

Wardriving is the act of locating wireless networks through trawling a large area by car operating a wireless network detection device. This can be as simple as a notebook computer, a wireless network card and some freely available software. At a more advanced level, extra equipment such as external antennae, multi-protocol wireless network cards and GPS locators can add to the number of wireless networks detected as well as pinpointing geographical location more precisely (Shipley 2001). This study used wardriving as the method employed for data collection.

2.2 Legal Issues

The legality internationally of wardriving has not been challenged. In Australia, the radio frequency used by wireless networks (i.e 802.11a, 802.11b and 802.11g protocol) is regulated; however it is not licensed and therefore is open for use for individuals and organizations. A Telecommunication Carrier License is required should an organization or individual attempt to sell access to a wireless network (Radio Communications Act 1992).
Internationally, the United States Federal Bureau of Investigation has stated "Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations" (Shore 2002).
In Australia, there is no legislation in place that specifically prevents listening to Wireless networks. However, the Radio Communications Act itself dates from 1992, before the invention of wireless networking and subsequent security concerns (Radio Communications Act 1992). The Cybercrime Bill does not specifically mention the monitoring of wireless networks, and becomes relevant in the event that the communication medium is deliberately made unusable or intentionally impaired (Cybercrime Bill 2001).
However, under State Law, all individual states have provisions against computer crime (Crimes Act, 1900 (Australian Capital Territory Legislation); Crimes Act, 1900 (New South Wales Legislation); Crimes Act, 1958 (Victoria Legislation); Criminal Code Act, 1913 (Western Australia Legislation); Criminal Code Act, 1924 (Tasmania Legislation); Criminal Code Act, 1995 (Queensland Legislation). For example, South Australian State Law dictates "A person who, without proper authorization, operates a restricted-access computer system is guilty of an offence" (South Australian Consolidated Acts 1953), and other states have similar laws in place. This law would be violated if a person entered (or attempted to enter) a network without specific approval to do so.
Given this information, it seems there is no law specifically governing wardriving, provided no wireless network is accessed. Assessment of Australian shows that a distinction exists

between monitoring wireless networks, deemed to be legal, and attempting to access them as illegal.

2.3Wireless Networks and SSIDs

Wireless networks provide the ability to connect computers much in the same manner as an Ethernet network but utilizes radio frequencies for linkage instead of physical cabling. Wireless networks typically utilize access points to provide the connection between the wireless network and a conventional 'wired' network. Currently there are 3 commonly used protocols in which wireless devices communicate over significant distance, IEEE 802.11a, 802.11b and 802.11g. The most widely used protocol is 802.11b due to the low cost of equipment and the relatively good transfer speeds (Kapp, 2002). All the results in this paper are based on wireless networks that operate on the 802.11b protocol and the 802.11g protocol which is backward compatible, and hence will appear within this study as an 802.11b network. An access point makes itself known to other devices by broadcasting a Service Set Identifier (SSID). An SSID is a 32 character unique identifier that allows for distinction between wireless networks. All access points by default broadcast their SSIDs to inform wireless nodes of their presence (Gomes 2001). This provides enough information to allow wireless network users to connect to the network. All access points come pre-configured with a default SSID that is set by the manufacturer. This SSID can later be changed when configuring the wireless network. Table 2.3.1 provides the manufacturer's default SSIDs.

Table 2.3.1 – Default SSIDs

Manufacturer	SSID
3COM	3COM
Apple	' '
Apple	Apple Network ******
Belkin	belkin54g
Cisco	tsunami
D-Link	default
Enterasys	' '
GST	AP******
Linksys	linksys
Netgear	Wireless
Netgear	NETGEAR
SMC	SMC
Generic Manufacturer	default
Generic Manufacturer	wireless
Generic Manufacturer	WLAN
Note: ' ' Denotes a single white space ****** Denotes the final 6 digits of the AP MAC address	

(List of vendors and default SSIDs adapted from: Wireless 2600, 2003; Lleida Wireless (2003)

2.4 Wired Equivalent Privacy (WEP)

There has been a great deal of research focusing on Wired Equivalent Privacy (WEP), the security mechanism defined in the 802.11b standard (Fluhrer, Mantin & Shamir 2001, Housley & Arbaugh 2003). WEP provides an encryption standard under the 802.11b protocol, and utilizes a shared secret-key algorithm that is an implementation of the RC4 algorithm (IEEE, 1999). Several researchers have proven that WEP is flawed and susceptible to decryption (Fluhrer, Mantin & Shamir 2001, Housley & Arbaugh 2003). WEP operates at the two lowest levels of the Open System Interconnection model; the data-link and physical layers (Housley, Arbaugh 2003). Access points by default have WEP disabled to allow for initial connections and testing.

Despite its flaws, WEP is still functional in securing wireless networks, as it serves to deter 'casual' network attacks. In order to determine the WEP key of a network, approximately 4,000,000 packets are required (Shipley 2001). This is a time consuming and resource intensive process, and is based entirely on the amount of traffic that is being produced by the target network. This lowers the likelihood of wireless network attacks, potentially restricting it to those attackers seeking to access specific networks.

Virtual Private Networks (VPN) are third party security mechanisms that can be used for security over wireless networks. The details of these depend upon the implementation, but VPN's offer higher levels of security than WEP. The presence of a VPN was unable to be detected in this study due to legal and ethical considerations (discussed in Section 3.4 of this paper) and the desire of the researchers to maintain simplicity in the method employed.

2.5 Levels of Wireless Network Security

This study attempted to assess the levels of wireless network security being deployed by organization and individuals operating wireless networks in the CBD of 7 Australian Capital cities. In order to assess the level of security in place to protect the networks, the methodology was designed to detect whether the network had:

- A default SSID setting
- WEP not enabled
- A default SSID setting and no WEP enabled

Whilst utilizing a default SSID does not impact security in itself, it serves as an indication that there has been little or no effort to edit the default settings that were provided with the device. If an access point has both a default SSID and does not utilize any security protection such as WEP encryption, it is highly unlikely that a high-level third party protection such as a Virtual Private Network (VPN) is in place. It is more probable that the access point has been installed as a 'plug and play' device and that no security measures have been taken to protect the wireless network. Based upon this assumption this study assumed that access points detect with default SSID settings and WEP not enabled are most vulnerable to intrusion.

The next section of this paper will discuss the method used to gain data to address the objectives of this paper.

3. Method

The methodology chosen to undertake this research was specifically designed to be simple, require little technical knowledge and make use of basic Computing equipment.

The method was developed to provide valid and reliable data using a technique that was robust and easily replicated across the seven Australian capital cities that were used for data collection.

This section of the paper will discuss the hardware and software used to collect data, the procedure which was employed in each of the seven Australian Capital cities, and the analysis of the data.

3.1 Hardware/Software

To maintain consistency with the objectives of this research the researcher sought to minimize the cost and technical knowledge required to undertake similar wireless network surveys.

The hardware utilized for the data collection was representative of a low cost 'hacking system' that could be acquired relatively easily and cheaply if desired by a malicious individual to serve as a platform for network intrusion. It also provided a relatively robust and mobile system upon which to collect the data required for this research.

The machine used for this experiment was a DELL Latitude laptop computer utilizing an Intel Celeron processor running Windows 2000 Professional and using a Cisco Systems Aironet 340 Series Wireless Network Interface Adaptor. No external antenna was utilized. This system serves as a demonstration of what is required as a minimum, and this by no means represents any device that is not commercial off-the-shelf.

For the collection of data, the freeware software Network Stumbler (NetStumbler) was used. NetStumbler is possibly the most 'user friendly' of wireless Access Point locators. It is relatively simple to install onto a computer and provides an easy to use graphical interface to guide the user on how to operate the program. Other alternatives, such as the Linux-based Kismet were considered however the degree of expertise both in initial configuration and in operation was considered too high when one primary objective of this paper is to show the technical ease of which wireless networks may be found.

NetStumbler relies upon the wireless Access Point broadcasting information of itself in response to a request probe sent along the 802.11b frequency.

Whilst the majority of wireless Access Points will respond to a request for information, some systems are able to disable this broadcast of information, making them effectively invisible to programs such as NetStumbler.

3.2 Technical Limitations of Research

The technical limits of this research are found in the equipment that was used; the system was designed to demonstrate that low cost and readily available equipment can be used to evaluate the security level of a wireless network. More advanced equipment, such as external antennae and wireless network cards that operate on a multitude of network protocols, are also available for advanced users.

In addition, the software program used for the collection of this information, NetStumbler, is considered the most 'user friendly' of wireless Access Point locators, but does not detect all access points. NetStumbler relies upon the wireless Access Point broadcasting information of itself to all users, something an increasing number of Wireless Network Administrators are opting not to do.

The researchers recognized that the use of an external antenna would have increased the sensitivity of the test equipment which may have resulted in an increase in the ability to detect wireless networks. However, to maintain consistency with minimizing the cost of test equipment it researchers decided to use a simple wireless card without external antenna.

3.3 Procedure

This research was undertaken by operating the testing equipment (notebook computer, Wireless Network Interface Card and NetStumbler) whilst driving a vehicle through a search pattern of the test cities' Central Business District. The research focused on all Australian State and Territory Capitals (except Darwin) including:

- Adelaide
- Brisbane
- Canberra
- Hobart
- Melbourne
- Perth
- Sydney

Darwin was excluded from this study due to the relative small population and financial constraints of this research.

In the absence of defining information on what constituted the CBD in each city, the researchers chose to use landmark buildings and pronounced geographical features of each city to determine the border of the CBD in each of the test cities. Table 3.3.1 provides the extremities of each city tested and a brief description of the feature utilized to define the area of the test.

Table 3.3.1 Australian Capital City Central Business District Borders

	Directional Border			
City	North	East	South	West
Adelaide	North Tce	East Tce/Hutt St	South Tce	West Tce
Brisbane	Turbot St	Queens St/ Eagle St/ Felix St/ Brisbane River	Alice St/Botanic Gardens	North Quay/William St/Brisbane River
Canberra	Barry Drv/ Cooyong St	Ballumbir St/ Coranderrk St	Parkes Way/Lake Burley Griffin	Marcus Clarke St/ Australian National Museum
Hobart	Brooker Highway	Davey St/Derwent River	Molle St	Bathurst St
Melbourne	La Trobe St/ Flag Staff Gardens	Nicholson St/ Parliament House/Treasury Gardens	Flinders St/ Flinders St Station	Spencer St/Spencer St Station
Perth	Wellington St	Nelson Ave/ Swan River	Riverside Drv/ Swan River	Mitchell Freeway
Sydney	Cahill Express	Macquarie St/ Elizabeth St/ Botanical Gardens /Hyde Park	Hay St/Rawson Plc/Eddy St/Central Station	Western Distributor/Harbor St/George St

In an attempt to maximize the similarities between this research and potential clandestine attempts to access wireless networks the researchers chose to collect data on weekdays in the late afternoon/ early evening in all cities. This time was chosen as it:
Minimized traffic interruptions
Lessened the likelihood of arousing suspicion as each city still had sufficient traffic and people to obscure testing
Offered the cover of twilight or darkness

The procedure used to collect data was to activate the test equipment at an outside corner of the CBD area and drive at 40kph or less, the driver attempted to maintain 20kph and only deviated from this speed when traffic conditions necessitated. A search pattern was devised for data collection based on the perimeters shown in table 3.3.1.
The same driver and test equipment was used on all cities in order to ensure consistency in the search pattern and driving manner employed to capture data.

3.4 Limitations of Procedure
In the assessment of wireless network security the procedure use to perform the assessment is limited by legal and ethical considerations (See Section 2.2 of this paper). Whilst it is legally permissible to locate wireless networks that are broadcasting information on a public spectrum and query them for information, it would not be legal nor ethical to attempt to associate with these networks. This limits the amount of security reconnaissance that can be conducted; as only the very outer perimeter of network security can be tested for. The result of this is that whilst WEP (Wired Equivalent Privacy) can be tested for, proprietary and advanced solutions, such as VPN cannot be discovered. As a result this study only identified whether WEP encryption was operational, as network association must be made before any further analysis can be made.

3.5 Analysis
All of the data collected by the NetStumbler was transferred to MiniTab statistical package. At the completion of data entry, all data fields were checked by the researchers to ensure data integrity.
The analysis of the data was undertaken using MiniTab.
The data was analysed using a variety of statistical methods, consistent with the descriptive and inferential nature of this study. The purpose of the analysis was to achieve the objective of this research through the provision of an understanding of the content of the data and to form the basis of findings of the study (Neuman 2000).
Principally, this Section provided a clear insight into data collection, processing and analysis as it relates to this research study. This has been accompanied to provide a sound methodology upon which this research was conducted. The next section of this paper presents the results obtained from the employment of the techniques detailed within section.

4. Results
The section of the paper presents the result of the analysis performed upon the data collected using the procedure discussed in the previous section. The following results are provided:
Data Collection Factors
Information relating to the number wireless networks detected
The level of security employed on wireless networks
Correlation and regression testing of wireless network security

4.1 Data Collection Factors

Table 4.1.1 sets out the start and completion time for each city, as well as the vehicle used and the atmospheric conditions for each test. This table is included to provide details of factors that varied between the data collection procedures in each city.

Table 4.1.1 Data collection Factors

City	Start Time	End Time	Vehicle	Atmospheric conditions
Adelaide	8:45pm Thurs 8Jan04	10:45pm Thurs 8Jan04	1995 Peugeot 306 Hatch	Clear
Brisbane	4:11pm Thurs 15Jan04	5:45pm Thurs 15Jan04	2003 Toyota Avalon Sedan	Drizzle
Canberra	7:47pm Mon 12Jan04	9:12pm Mon 12Jan04	2003 Toyota Avalon Sedan	Clear
Hobart	7:33pm Thurs 4Dec03	8:46pm Thurs 4Dec03	2001 Holden Commodore Sedan	Clear
Melbourne	9:07pm 16Oct03	12:15am 17Oct03	2003 Nissan X-Trail Wagon	Clear
Perth	7:18am Thurs 27Nov03	8:20pm Thurs 27Nov03	2003 Nissan Lancer Hatch	Clear
Sydney	7:23pm Tues 13Jan04	9:23pm Tues 13Jan04	2003 Toyota Avalon Sedan	Clear
Note: All times stated are local time i.e Brisbane, Sydney, Canberra, Melbourne and Hobart AEST; Adelaide ACST; Perth WST.				

4.2 Information relating to the number of Wireless Networks Detected

Prior to the commencement of this study, no comprehensive research had been undertaken across 7 Australian Capital cities. Table 4.2.1 sets out the number of wireless networks detected in each Australia Capital city and each city as a percentage of the overall sample population detected and various security levels of the cities.

Table 4.2.1 Number of Wireless Networks detected

	Wireless Networks		Default SSID		WEP Not Enabled		Default SSID and WEP Not Enabled	
		% of Total		% of City Networks		% of City Networks		% of City Networks
Adelaide	109	15%	20	18%	71	65%	16	15%
Brisbane	72	10%	13	18%	52	72%	11	15%
Canberra	41	6%	12	29%	17	41%	1	2%
Hobart	29	4%	10	34%	11	38%	7	24%
Melbourne	176	24%	33	19%	102	58%	24	14%
Perth	58	8%	15	26%	30	52%	7	12%
Sydney	244	33%	83	34%	108	44%	41	17%
Total	729	100%	186	25.5%	391	54%	107	15%

This research detected a total of 729 wireless networks operative in the CBD of the 7 Australian Capital cities. From Table 4.2.1 it can be observed that Sydney (244 wireless networks) recorded the highest number of wireless networks detected, with Hobart (29 wireless networks) recording the least. It also shows that Melbourne and Sydney combined

possess over half (57%) of the number of wireless networks currently operating in the CBD's of the Australia capital cities studied.
Further 26% of wireless networks detected were using default SSID settings and 54% of wireless networks did not have WEP activated. Hobart had the highest level of default SSID settings (about 24%) and Canberra had the lowest (about 2%).
Of the 729 wireless networks detected in this research 54% had not activated WEP (As identified in the Section 2.4 and Section 3.4 of this paper, this figure does not take into account the use of Virtual Private Networks). The results show that Brisbane has the lowest level of wireless encryption use with 72% of networks choosing not to activate WEP (or using alternative methods) and Hobart with the highest level of WEP use at 38% of wireless networks with WEP enabled.
Default SSID (as identified in Section 2.3 of this paper) setting are another indication of levels of wireless security with 25.5% of wireless networks detected operating within the surveyed Australian capital cities using default SSID settings. Sydney and Hobart recorded the highest use of default SSID setting with approximately 34% of Wireless networks detected using default SSID settings. Adelaide and Brisbane had the lowest incident of wireless networks detected with default SSID settings at 18%.
Wireless networks using default SSID settings without WEP enabled are likely to be the most insecure wireless networks (as discussed previously in Section 2.4 of this paper). A regression analysis was undertaken in the next section of this paper in order to more closely examine the results obtained.

4.3 The Level of Security Employed on Wireless Networks

One primary objective of this research was to determine the vulnerability of wireless networks in 7 Australian capital cities. The results shown in Table 4.3.1 provide an indication of the level of security employed by users of the wireless networks identified in this research.

Table 4.3.1 Level of security employed on Wireless Networks

Variable	N	Mean	Median	StDev	SE Mean
Total Wireless Networks	7	104.1	72.0	79.1	29.9
Default SSID	7	26.57	15.00	26.06	9.85
No WEP	7	55.6	51.0	39.1	14.8
Default SSID + No WEP*	7	15.29	11.00	13.52	5.11

Variable	Minimum	Maximum
Total Wireless Networks	29.0	244.0
Default SSID	10.00	83.00
No WEP	11.0	107.0
Default SSID + No WEP*	1.00	41.00

*Default SSID + No WEP was calculated based upon a count of Wireless Networks that had not enabled WEP and had not changed the default SSID settings as discussed in the Background section of this paper.

The mean number of Wireless Networks in existence in the 7 Australian Capital cities studied was approximately 104 wireless networks per city (at a standard deviation of approximately 79 indicating a large variance across cities).

4.4 Correlation and Regression Analysis of Wireless Network Security

Regression analysis was undertaken in order to determine whether a correlation existed between the number of wireless networks detected in each Australian Capital city and the number of wireless networks operating with default SSID's and without WEP enabled. Details of this analysis are provided in Table 4.4.1

Table 4.4.1 Details of regression analysis

The regression equation is:Combined No WEP + Default SSID = 0.153 Total networks

Predictor	Coef	StDev	T	P
Noconstant				
Total ne	0.153477	0.009415	16.30	0.000
S = 3.171				
Analysis of Variance				

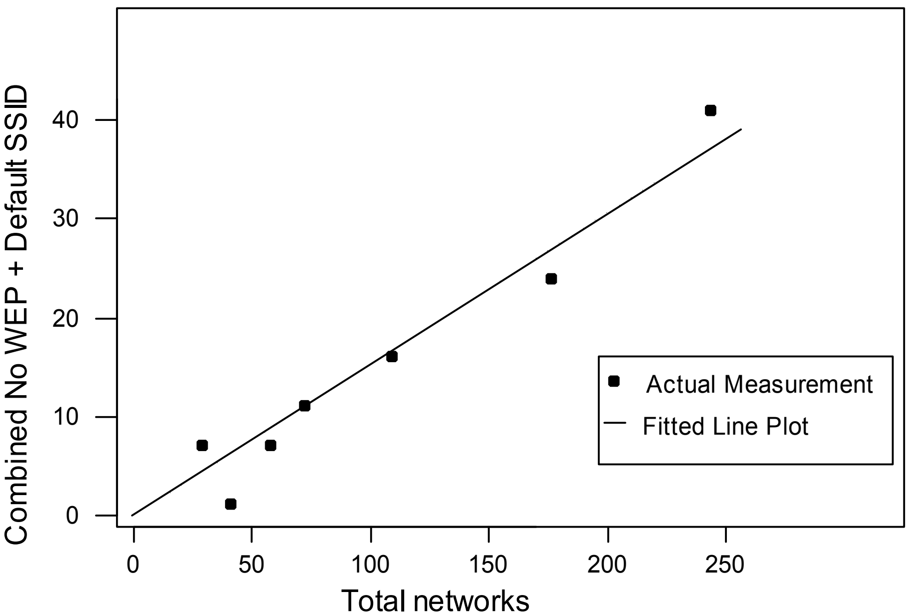
Source	DF	SS	MS	F	P
Regression	1	2672.7	2672.7	265.74	0.000
Residual Error	6	60.3	10.1		
Total	7	2733.0			

Note: It was assumed during the regression analysis that a plot of the variables would pass through the origin i.e. At 0 Wireless Networks there would not be a negative number of Wireless Networks without WEP enabled and with default settings.

The relationship between the predictor, the number of wireless networks operating in the CBD of 7 Australian Capital Cities, and the response, the number of wireless networks without WEP enabled and with default SSID settings, is demonstrated with the fitted line plot in Figure 4.4.2.

Figure 4.4.2

The number of wireless networks in Australian Capital Cities V number of wireless networks without WEP enabled and with default settings.



R-Squared was calculated to measure the strength of the correlation depicted in Figure 4.4.2.

$$\frac{S_r^2}{S_y^2} = 1 - R^2$$

$$1 - R^2 = \frac{6 \times 3.171^2}{2733.00} = 0.22, \qquad R^2 = 97.8\%$$

R-sq at 97.8% indicated a strong linear association existed between the number of wireless networks detected in each the CBD of the 7 Australian Capital cities and the number of wireless networks with default SSID settings and WEP not enabled.

To summarise the following results have been provided:
Approximately 25.5% of all wireless networks found were operating using default SSID.
Hobart is considered the most insecure of all Australian capital cities surveyed with 24.1% of wireless networks found operating using default SSID and with no WEP encryption.
Canberra is considered the most secure of all Australian capital cities surveyed with 2.4% of all wireless networks found operating using default SSID and not enabling WEP encryption.

The regression equation for wireless networks within the CBD of the 7 Australian Capital Cities with WEP not enabled and default SSID for Total Networks is:
Combined No WEP + Default SSID = 0.153 Total networks

This section has provided the results from the data collected and presents them in a manner that allows discussion specifically relating to the research objectives.
The next section provides a discussion of the research objectives in light of the results presented in this chapter. The Section also discusses the benefits and limitations of this research and its application within both practical and theoretical environments. Suggested areas for future research in the field of Forensic Computing will conclude Section 5.

5. Discussion

Of the 729 wireless networks detected in this research 54% had not activated Wired Equivalent Privacy encryption. Whilst this figure does not take into account the use of Virtual Private Networks (as discussed in section 2.5), it does identify a substantial number of wireless network users in the 7 Australian Capital cities are not employing rudimentary encryption. This absence of security allows both unauthorized users from accessing a private wireless network and passive eavesdropping on the wireless network. Without any form of encryption, even if other security measures are in place, all data transmitted through the network is considered publicly available.
The number of wireless networks identifiable by default SSID's were high and infers little in isolation of other data as the use of a default SSID does not affect security. However, it can be used as a marker to determine insecure networks as an inexperienced installation of a wireless Access Point will not change the default SSID, as the installer would lack sufficient knowledge.
Of the most interest in the results were the number of wireless networks detected that have the default SSID and have also not enabled WEP encryption. Whilst further perimeter testing would be both unethical and illegal, there is a strong likelihood that these networks are

vulnerable to attack, and likely have no security enabled to prevent unauthorized access. The aggregated results indicate that this particularly vulnerable group is a relatively high percentage of the total wireless networks – above 15%. When put into context, about 15% of wireless networks in Australia are vulnerable to infiltration, and have no security mechanism in place at all.

The regression analysis formulated the equation for wireless networks within the CBD of the 7 Australian Capital Cities with WEP not enabled and default SSID for Total Networks as:

Combined No WEP + Default SSID = 0.153 Total networks with an R-squared value of 97.8.

The high R-squared value suggests a very strong linear association between the number of wireless networks and the number of wireless networks with WEP not enabled and default SSID. This equation may be useful in predicting or identifying changes to levels of wireless network security in future research within Australia Capital cities as the prevalence of wireless network technology increase.

Using the regression analysis formula from this study Figure 5.1 provides a visual representation of possible future trends in wireless network security levels.

Figure 5.1

Future trends in wireless network security levels

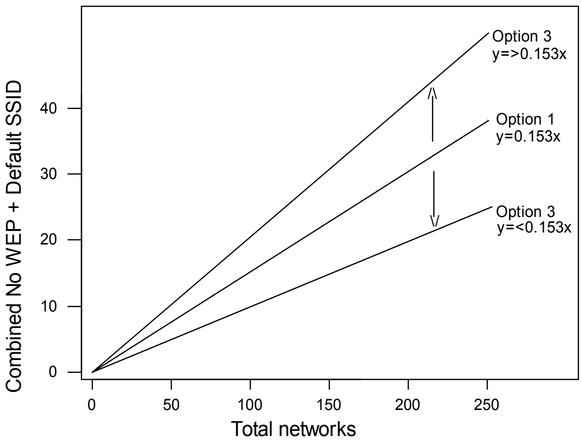


Figure 5.1 depicts three future scenarios for wireless security within Australia based upon the results of this study;

Option 1 The portion of insecure networks remains the same

Option 2 The portion of insecure networks increases

Option 3 The portion of insecure networks decreases

Option 1

The regression equation describing the relationship between wireless networks and default SSID and WEP not enabled will remain the same. This can potentially be explained by assuming that as wireless network increase in use a consistent percentage of users will fail to implement rudimentary security precautions.

Option 2

The relationship between wireless networks and default SSID and WEP not enabled will change reflecting a increase in insecure networks. This change could possibly be explained through changes in the user profile of wireless networks as the technology becomes cheaper and more accepted by users with lower technical knowledge. One consideration is that Wireless network hardware vendors may choose to market their products to home and small business users advertising ease-of-use and installation. If users without technical expertise were to install wireless hardware without understanding the security implications, the system would still be operational, and many would not consider the potential security threat that this system could result in. As vendors look to increase the sales of Wireless Networking devices, the incidence of users on plug-and-play systems that do not incorporate any security measures will increase.

Option 3
The equation describing the relationship between wireless networks and default SSID and WEP not enabled with change to reflect a lower incidence of insecure networks. Potentially this change could be explain through an increase in user awareness of the security risks associated with wireless network use and how to implement rudimentary security procedures.
The regression equation for wireless networks within the CBD of the 7 Australian Capital Cities with WEP not enabled and default for Total Networks is:
Combined No WEP + Default SSID = 0.153 Total networks
No prior data exists that can be used for comparative purposes for this paper however, given the infancy of wireless networking technology it is highly probable that the number of wireless networks is increasing. How this uptake will affect the regression equation identified in Section 4.4 can only be determined by conducting a time series study of using the methodology outlined in Section 3.

5.1 Application of Results outside Australia
Whilst this study was solely undertaken within Australia the results serve as a prediction of wireless network security in other countries. In the absence of international data this cannot be tested however, at least on a base level this study may provide international researchers with the ability to compare future studies with current trends in Australia capital cities.

6. Conclusion
After careful analysis it can be concluded that within Australia there is a noteworthy percentage of wireless networks that are highly vulnerable to intrusion. Whilst the majority of wireless networks have some level of security there is still a large number that fail to have even rudimentary protection against external intrusion.
The chief factor is user awareness; those installing wireless networks must consider the security implications of the network and understand that whilst authorized wireless users are able to access internal networks via wireless technology, low security measures also allow entry to any users within broadcast range.
Further, this research has demonstrated that the equipment required to either detect or exploit these vulnerabilities is easily commercially available, and relatively inexpensive. Whilst external antennae, GPS and other third party additions may provide increased sensitivity, wireless network vulnerability can be assess remarkably effectively with the use of even an outdated notebook PC and 802.11b Wi-Fi card.
Overall this research has demonstrated the need to maintain vigilance over security risks as wireless networks become increasingly popular among commercial and private users throughout Australia.

7. Further Work
This paper raises a number of intriguing issues, many of which may warrant further investigation. Whilst some of the legal and ethical considerations discussed in this report may hinder potential research in the field, is anticipated that this research will provide the

foundation for a time-series analysis of Australian Wireless Network security to provide information on how this is changing over time and the long-term consequences that are caused by this. Another area of further work would use the results of this study as provide a basis for international comparative work in this area.

References

Crimes Act 1900. Australian Capital Territory Legislation. Available www.legislation.act.gov.au , Accessed 1 March 2004.

Crimes Act 1900 No 40. New South Wales Legislation. Available www.legislation.nsw.gov.au , Accessed March 1, 2004.

Crimes Act 1958. Victoria Legislation. Available http://www.dms.dpc.vic.gov.au . Accessed 27 February 2004.

Criminal Code 1913. Western Australia Legislation. Available http://www.slp.wa.gov.au . Accessed March 4 2004.

Criminal Code Act 1924. Tasmania Legislation. Available http://www.thelaw.tas.gov.au . Accessed 1 March 2004.

Criminal Code 1995 No 37. Queensland Legislation. Available http://www.legislation.qld.gov.au . Accessed 2 March 2004.

Cybercrime Bill 2001. Commonwealth of Australia Legislation. Available: http://scaleplus.law.gov.au/, accessed 23 February, 2004.

Institute of Electrical and Electronics Engineers, Inc (IEEE), (1999), 802.11b Standard, available http://www.standards.ieee.org, accessed 19 February 2004

Fluhrer, S., Mantin, I. and Shamir, A. (2001). Weakness in the Key Scheduling Algorithm of RC4.

Available www.drizzle.com, accessed 12 July 2003.

Gomes, L. (2001). Many wireless networks open to attack. The Wall Street Journal Online, April 26, 2001. Available www.zdnet.com, accessed 23 February, 2004.

Housley, R. and Arbaugh, W. (2003). Security Problems in 802.11-based networks, Communications of the ACM, ACM Press New York USA.

Kapp, S, (2002) 802.11: Leaving the wires Behind, Internet Computing Vol. 6, issue 1, Jan-Feb 2002, IEEE, USA.

Lleida Wireless (2003). Default Config. Available: http://lleidawireless.net/space/Default+Config, accessed 20 July 2003.

Neuman, W. L. (2000). Social Research Methods. Boston, Allyn and Bacon.

Radio ommunications Act 1992. Commonwealth of Australia Legislation. Available: http://scaleplus.law.gov.au/, accessed 23 February, 2004.

Shipley, P. (2001). Open WLAN's: The early results of wardriving, Avilable: www.dis.org-filez-openlans.pdf, accessed 20 July 2003.

Shore, B. (2002). FBI releases advisory about 802.11-spotting "wardriving". Available: www.politechbot.com, accessed 20 July 2003.

Summary Offences Act 1953. South Australian Legislation. Available: www.austlii.edu.au, accessed 14 July, 2003.

Turnbull, B., Nicholson, D. and Slay, J. (2003). "Wireless Networking Security- A practical summary 802.11b in Adelaide, Australia". Proceeding of the 4th Australian Information Warfare and IT Security Conference. 20-21 November 2003. Adelaide:Australia.

Webb, S. (2003). The role of Wireless Network Technology in Network Centric Warfare, 4th Australian Information Warfare and IT Security Conference, 2003, Adelaide, Australia.

Wireless 2600 (2003). Default AP Vendors and SSIDs. Available: www.wi2600.org , accessed 23 November 2003