A COMPARISON STUDY OF WIRELESS NETWORK SECURITY IN SEVERAL AUSTRALASIAN CITIES & SUBURBS

Alastair Nisbet,
School of Engineering, Computer
& Mathematical Sciences
Auckland University of Technology
Auckland, New Zealand
anisbet@aut.ac.nz

Andrew Woodward,
School of Computer and Security Science
SRI - Security Research Institute,
Edith Cowan University
Perth, Western Australia
a.woodward@ecu.edu.au

Abstract:

Wireless network technology has been available for public and private use for almost two decades. The casual approach to security with the early standards and channel selection began to cause issues when the initial security standard, WEP, was discovered to have serious flaws. The closer examination of security and efficiency that followed led to better security protocols, easier setup in quicker and more efficient methods and better guidelines for channel selection to ensure efficiency of radio communications. A survey of 5 areas throughout New Zealand was conducted and this is compared with a survey of 5 areas around Perth in Western Australia. The results indicate that whilst improvements continue to be made in security implementations, a small percentage of users do not implement their networks with the recommended settings. Whilst Australian users are slightly better at complying with recommendations, it is clear that some work still needs to be done in informing users and insuring compliance to the recommendations for deployment so that all users can utilise their networks efficiently and securely.

Keywords: wireless, network, security, privacy, bandwidth

INTRODUCTION

Wireless networks have been available for public use for almost two decades. Beginning in 1997 with the original IEEE 802.11-1997 standard, the uptake or wireless technology began to see a slow but steady rise. Whilst other wireless technology was available, it tended to be proprietary and enjoyed by relatively few users. The difference with the IEEE standards was that for the first time they could be utilised by all equipment manufacturers and relatively easily work with different computer manufacturers and operating systems. In 1999, the development and ratification of 2 new standards saw wireless acceptance begin to enjoy rapid growth. This was primarily for 3 reasons. Firstly, the new standards, IEEE 802.11a and 802.11b offered much greater bandwidth and the option of increased non-overlapping channels, especially in the case of 802.11a. This allowed for multiple wireless devices to communicate simultaneously without interfering with each other’s transmissions, something that greatly improved the use of multiple access points within radio range of each other. The second improvement was the inclusion of security within the standards, albeit to prove somewhat flawed at a later date. Finally, the Wireless Ethernet Compatibility Alliance (WECA) was established which tested the IEEE wireless devices from various manufacturers for compliance with the standards. If their testing found that devices were suitably designed to comply with the WECA’s standards, a stamp of approval was given and users could be assured that these ‘Wifi Certified’ devices would interoperate with all other similar Wifi Certified devices. In 2003, WECA changed its name to the Wifi Alliance and continues to certify products. By 2015 over 25000 different devices from hundreds of manufacturers have been WiFi Certified (Wifi.org).

Whilst the standards were seeing further developments at regular intervals that generally focussed on improved data transfer rates, the security issues with WEP began to surface in 2000 (Walker 2000). This became more serious in 2001, beginning with a theoretical attack against a WEP key published that year (Fluhrer, Mantin et al. 2001). This led to a series of articles highlighting possible weakness in the security of WEP (Arbaugh, Shankar et al. 2002) and was followed shortly afterwards by a practical implementation of the FMS attack in 2002 (Stubblefield, Ioannidis et al. 2002). This led to a period of uncertainty over the security of wireless networks (Cam-Winget, Housley et al. 2003) that lasted for several years, even after much improved security protocols were developed (Vibhuti 2005).

The effect was that wireless device sales slowed with the perception that wireless security was now a problem that was yet to be solved. In 2003, the 802.11G standard was ratified and incorporated into this standard were new security measures intended as an interim measure. WiFi Protected Access (WPA) utilising a pre-shared key between devices and the Temporal Key Integrity Protocol (TKIP) allowed for much greater security by updating keys at regular intervals without user intervention. A further development in security designed as an enterprise solution was IEEE 802.11i (Walker 2003). This new standard, also called WPA2 was initially designed to be implemented by a dedicated server attached to a corporate WLAN and utilising the AES encryption algorithm (Nechvatal, Barker et al. 2000). AES had been adopted by the United States Government as the official security standard because of its extremely high resilience to attack. The new standard would later be modified to utilise a pre-shared key allowing domestic users with a home access point to implement the much greater security offered by AES as an option. This left a range of security choices for users, from no security, often referred to as ‘open’ security, to the outdated and insecure WEP security, to WPA and the most robust security of WPA2.

Whilst WPA was designed by the WiFi Alliance as an interim standard until a more robust solution could be found, the design proved to provide high security with a relatively simple implementation. This ‘temporary’ standard is still utilised and for most home users tends to be the choice for security. However, as with WEP, WPA has been shown to suffer from several vulnerabilities. Firstly, during the authentication phase an attack is possible that can discover the PIN code used during the setup (WiFi Alliance 2007), and secondly encryption keys fewer than 20 characters are considered unsecure. Those keys approaching 20 characters are still possible to crack but it would take a determined attacker many months at least to crack the key (Lashkari, Danesh et al. 2009).

Whilst metropolitan wireless networks and local public areas such as cafes and restaurants may deliberately offer open networks for the public and customers, business organisations and home users should implement high security on their devices. This not only prevents unauthorised users utilising their network connections but ensures privacy of messages including emails, web browsing and user names and passwords utilised for sites that may have highly confidential information contained within them. The issues with wireless networks and the vulnerabilities have seen much publicity, both from academia and from more mainstream media. This began in 2001 with the FMS attack and has progressed over the years to expose security vulnerabilities in WPA. This should mean that both home and commercial premises are equipped with the highest level of security, with users aware of the dangers of no or low security and a corresponding increase in security of devices.

The following section examines the results of surveys taken in New Zealand cities from 2004 to 2011. This is discussed to show the progression of security over this period leading up to 2012. This is followed by the latest surveys conducted in 2013 in New Zealand’s four largest cities and a survey of several urban suburbs of Auckland. The results are used to compare the wireless security to that of several smaller suburbs of Perth as well as the Perth CBD. This comparison will serve to show whether or not security has progressed evenly within the two countries. Conclusions are then drawn examining the state of security and what if anything still needs to be done to increase security of wireless networks.

New Zealand Wireless Security Surveys

The first survey of wireless networks in New Zealand was conducted in Auckland City CBD. Inssider software was utilised with an external aerial to ensure the best possible detection of a wireless network operating. Approximately 12km was covered within the central city area and the results are shown in figure 1.

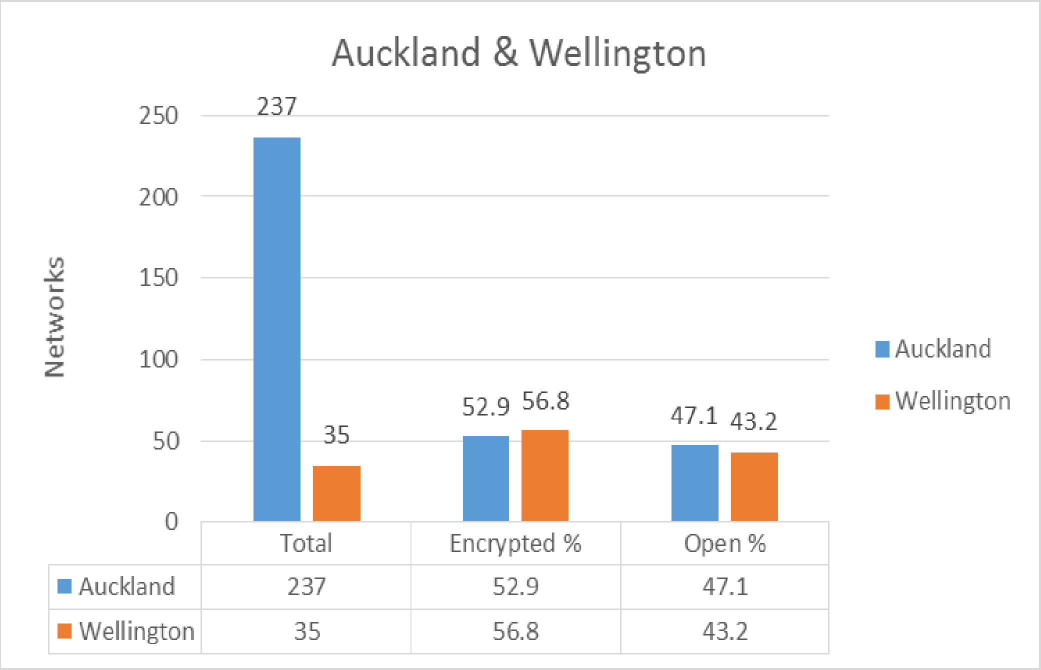
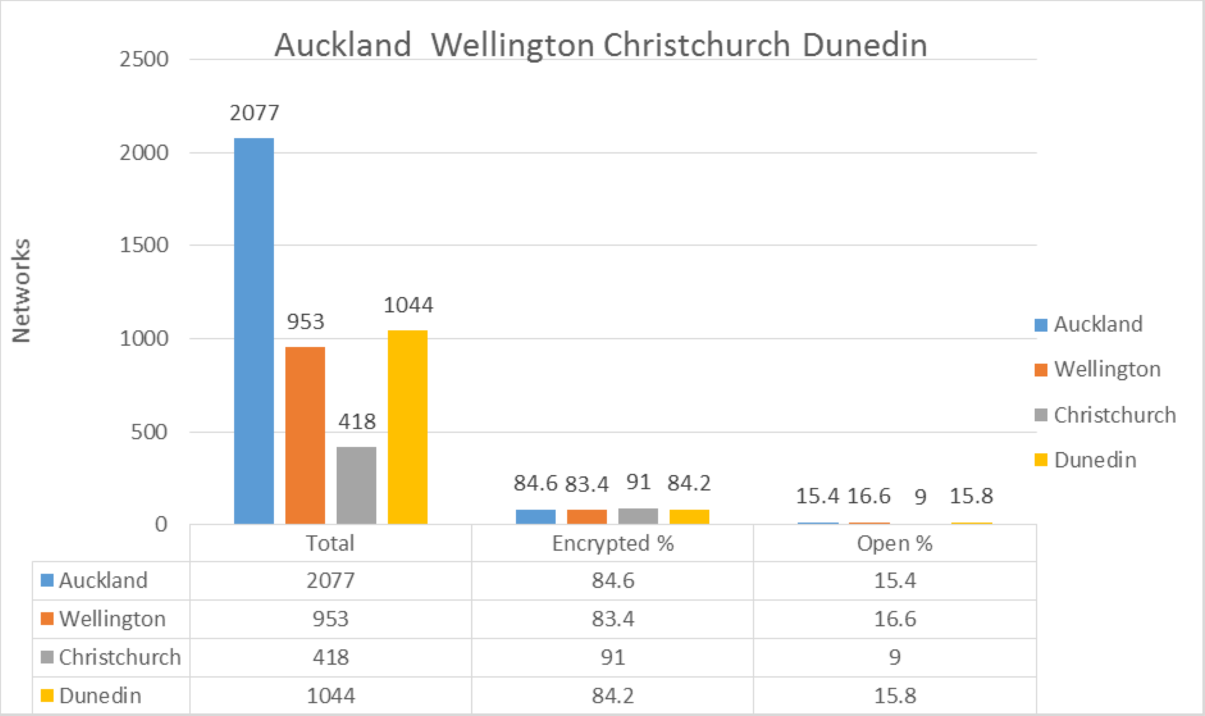


Figure 1: Auckland & Wellington results 2004

In 2004, WPA had just began to be implemented. The software utilised at that time did not differentiate between WEP and WPA, so the results simply show whether encryption is utilised or not. Also at that time, free to use wireless networks were fairly uncommon meaning that encryption would be expected to be used on almost all networks. However, results showed that little over half the networks were implemented with security. This appears to be for a number reasons. Firstly, users were far less aware in 2004 of the issues that arose when security was not implemented and secondly the wireless equipment had no security switched on by default. This combination meant that many networks had no security implemented and users were often unaware that this was the case. By 2011 this had changed significantly. In the seven years since 2004, wireless technology had received much more attention from media and manufacturers meaning that when installing their networks, users were more likely to switch security on. The 2011 survey of Auckland and Wellington was conducted and two further cities were added. Christchurch is the third largest city in New Zealand and Dunedin is the fourth largest. These surveys gave not only a good geographical spread of New Zealand but all four cities are diverse in their makeup. Wellington is the capital city and has many government agencies including military agencies and Dunedin has a small centralised CBD with a number of student houses and flats within the central city servicing Otago University and Otago Polytechnic. Christchurch has a much more spread out CBD with older buildings of generally 4 stories at most. By adding the two south island cities, a comparison could be made within New Zealand of how information regarding security settings and technological expertise may have had an impact on wireless network security settings. The results of the 2011 survey are shown in figure 2.

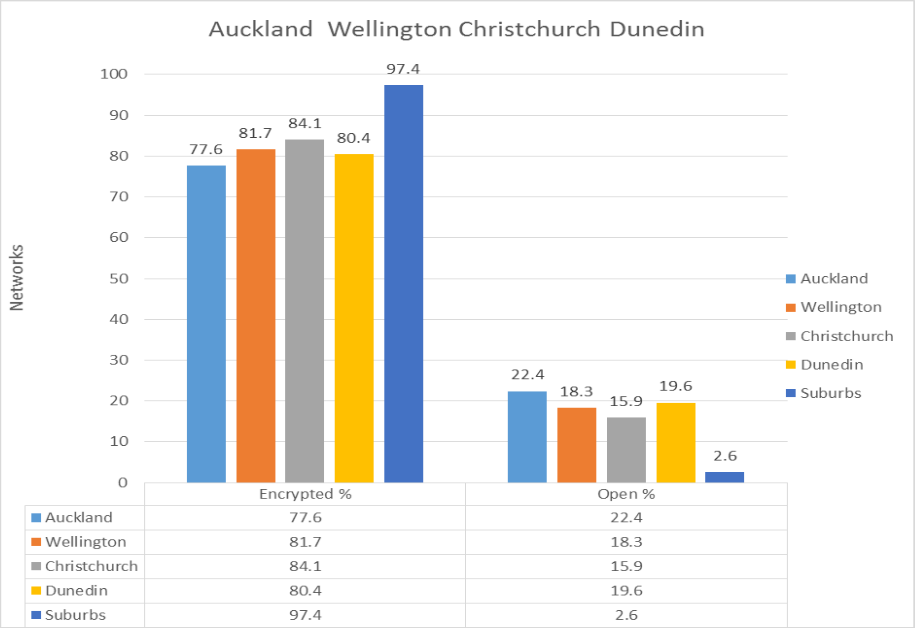


	Total	Encrypted %	Open %
🟦 Auckland	2077	84.6	15.4
🟧 Wellington	953	83.4	16.6
◼ Christchurch	418	91	9
🟨 Dunedin	1044	84.2	15.8

Figure 2: Four cities throughout New Zealand in 2011

The final survey in the series of New Zealand cities was conducted in 2013. This covered all four cities and was conducted on a weekday at the same time of day as the previous surveys. The number of networks detected had increased significantly over this time. A devastating earthquake in 2012 had destroyed many of the inner city buildings of Christchurch and this necessitated the survey taking place around the perimeter of the CBD area. Despite this, a significant increase in the number of networks was detected and a similar drop in the percentage utilising encryption to the other cities was also apparent. For 2013, many of the suburbs surrounding Auckland City were added to the survey. Over 5000 networks were discovered over a distance around the suburban roads of approximately 60km. This is a 20% greater distance covered driving around the CBD's of the four cities. The number of networks discovered in the 50km drive through the CBD's totals 9040, indicating that approximately twice as many networks are present in business areas as in the suburbs. However, encryption is implemented in 97.4 % of suburban networks compared to an average of 88.6 % for inner city networks. Whilst the possible reasons for the lower encryption have been briefly discussed, the very high implementation of encryption in the suburbs is encouraging. It would appear that a combination of publicity and media attention regarding the dangers of unsecured networks and the greater ease with which encryption can be set up on home networks, including WiFi Protected Setup

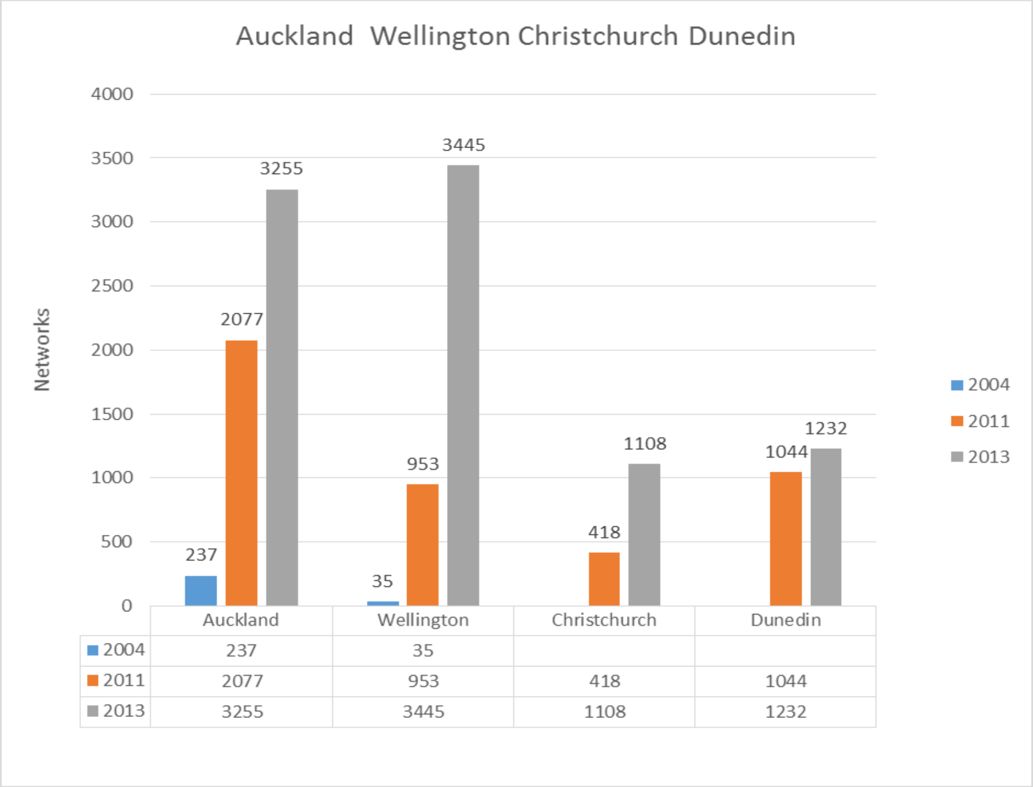
(WPS) available at the touch of a button, is having a positive effect in ensuring these networks are secure (WiFi Alliance 2007). The encryption percentage results of this survey are shown in figure 3.



	Encrypted %	Open %
■ Auckland	77.6	22.4
■ Wellington	81.7	18.3
■ Christchurch	84.1	15.9
■ Dunedin	80.4	19.6
■ Suburbs	97.4	2.6

Figure 3: Encryption percentage in 2013 for four cities throughout New Zealand

The increase in the number of networks detected over the eight years is one interesting factor from the survey. The greatest increase is in the capital city with an almost 10 000% increase from 35 networks to 3445. Christchurch and Dunedin's surveys cover a 3 year period only and both show increases but with Dunedin showing a very modest increase. These results are shown in figure 4.



	Auckland	Wellington	Christchurch	Dunedin
■ 2004	237	35		
■ 2011	2077	953	418	1044
■ 2013	3255	3445	1108	1232

Figure 4: Comparison of CBD wireless network numbers over 9 years

Overall, the increase in networks indicates a significant adoption of wireless technology both in business organisations and for home users. The increase in encryption utilised and allowing for the many free and deliberately unsecured networks indicates that confidence in wireless network security has reached a point where it is a trusted technology. Something that may well have occurred much earlier if the original security standard, WEP, had proven to be as secure as promised. The wireless network growth seen up to 2013 may well have occurred much earlier. The following section discusses a similar survey of suburban and semi-industrial areas near the city of Perth in Australia.

AUSTRALIA WIRELESS SECURITY SURVEYS

In 2012 a survey of 4 suburbs near Perth and the Perth CBD was conducted. These areas are a mixture of suburban and light industrial organisations. Perth, like Auckland is a city spread over a large area with multiple outer suburbs. Unlike the New Zealand surveys, the Australian surveys were all conducted within the general area of one, large city. However, the population of Perth at Approximately 1.8 million is fairly close to the total population of cities surveyed in New Zealand at 2 million. This and the fact that the cities share many of the same features and qualities of the New Zealand cities make for many comparisons between the two. The research question was whether these similar areas would share similar qualities with their wireless network security. The first of these surveys involved the CBD of Perth where 2142 networks were discovered. The encryption percentages are shown in figure 5.

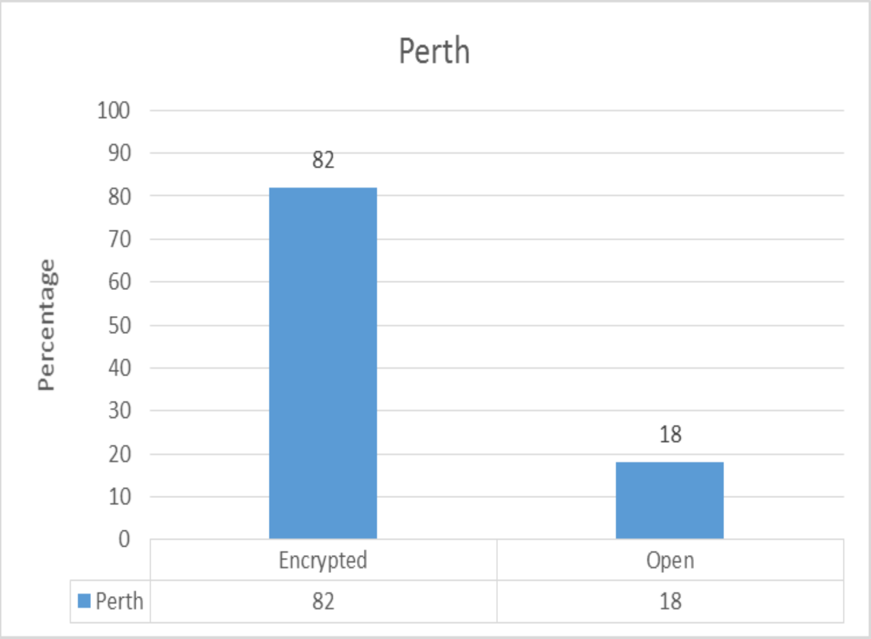
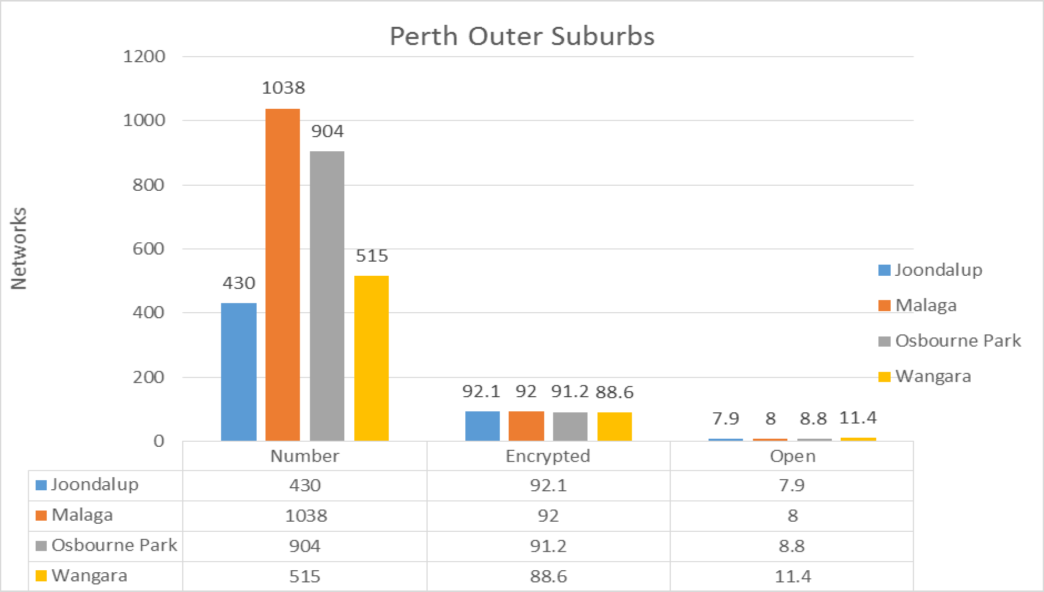


Figure 5: Encryption percentage in 2013 for Perth CBD

The results show that this compares fairly closely with an average of the results from Auckland for 2011 and 2013, both in numbers of networks and with the encryption utilised. The implication being that similar influences as regards the necessity of encrypting business networks are working in Perth and New Zealand. Next, the outer suburbs of Perth were compared to see how well the results matched with New Zealand's smaller cities. The results of these surveys are shown in figure 6.



	Number	Encrypted	Open
Joondalup	430	92.1	7.9
Malaga	1038	92	8
Osbourne Park	904	91.2	8.8
Wangara	515	88.6	11.4

Figure 6: Encryption percentage in 2012 for Perth's outer suburbs

With almost 3000 networks discovered in the outer suburbs and over 2000 within the Perth CBD, a good comparison between the suburbs and the city can be made. As with the New Zealand results, the city shows a reasonably predictable number of wireless networks detected based on the population and as with New Zealand, encryption implementation is more common for the outer suburbs than for the central city. This would appear to be for similar reasons as with New Zealand cities where free and deliberately unsecured wireless networks are common in the central CBD. Whilst the message about implementing security and the manufacturers' assistance with ease of setup for encryption is proving to be successful, an examination of the type of encryption utilised and the channel selections shows a deeper examination of the implications of utilising wireless networks both in a secure and efficient manner.

ENCRYPTION PROTOCOLS & CHANNEL SELECTIONS

Whilst a survey such as these gives a good overview of wireless security at a given time, the reasons for the results are often necessarily left largely to speculation. One change that is apparent in the results is that in all four cities in New Zealand, the implementation of encryption has decreased from 2011 to 2013. This appears to signify a problem with security but this would seem to be unlikely. It is far more likely that the growth in free wireless networks within the CBD's of these cities, which are provided free of charge but with no security, is the reason for the drop in security. The free and unencrypted networks appear to be growing at a faster rate than the networks overall and therefore whilst security in networks in businesses is increasing, the overall percentage is dropping. Therefore, there should be no expectation of a 100% encryption uptake but rather something less than this should be expected. The problem from a research point of view is that there is simply no way to be sure which networks are deliberately left open, as the Service Set ID of the network does not always permit an assumption of open security. In Auckland, names such as "Auckland Metro WiFi" and in Perth many use the term "Guest" may indicate a deliberately open wireless network, other names are not so clear that the intention is for them to be available to the public unencrypted. However, it would appear that security has reached a point where most business networks in the CBDs are secured with encryption while most of those that are unencrypted are intentionally so. No doubt there are still some networks that are unintentionally unencrypted but it is simply not possible to be sure which ones or how many there are. What is more of a concern is those networks that are utilising WEP. This type of encryption is insecure and utilising WEP gives a false sense of security, something that is worse than users knowing that there is no security.

An examination in both countries of the type of encryption utilised highlights several issues. Firstly, WEP is still available on most newer models of wireless equipment but is provided to support legacy equipment that does not support later encryption protocols such as WPA and WPA2. Additionally, utilising features of some network equipment may have the undesirable side effect of having to downgrade the encryption implemented to WEP. One example of this is using a wireless access point as a hopping point to extend the range of the main access point. In some equipment that is only a few years old, the encryption utilised for this feature is WEP only, and so the user implementing this feature has no choice but to significantly compromise the security of their network by effectively leaving a side door partially open. Figure 7 shows the security implementations of all New Zealand networks surveyed in 2013.

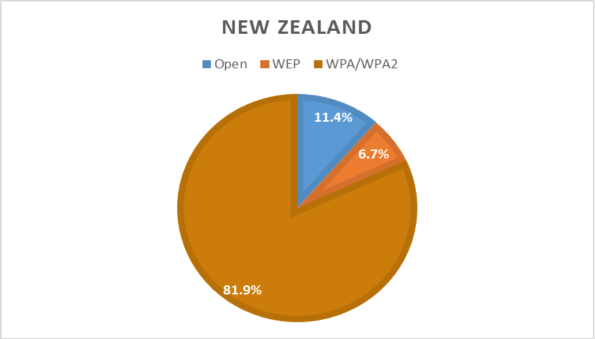


Figure 7: Encryption protocols for New Zealand in 2013

The breakdown of security protocols implemented shows that WPA and WPA2 account for 81.9% of the encryption implemented in New Zealand. WPA has had some criticisms regarding its security unless implemented in the recommended way. However, it has proven to be generally secure. WPA2 has not suffered from any criticisms for its security and is therefore generally the recommended best practice. However, WPA and WPA2 are considered to provide sufficient security whereas WEP is considered to give a false sense of security because of the ease with which the encryption key can be recovered by someone with even fairly limited technical skills. From the New Zealand results we can see that 6.7% of networks are utilising WEP and therefore the conclusion is that 6.7% of networks are desired to be secure but are failing in this goal.

For the Australian survey, very similar results were obtained as shown in figure 8.

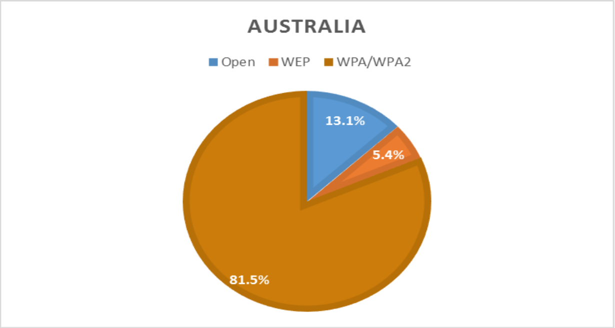


Figure 8: Encryption protocols for Australia in 2012

The networks utilising WPA or WPA2 are almost identical in value at 81.5%. The open networks have a slight difference with more in Perth which may be accounted for with more ‘free to use’ networks being publicly available. There is a slight improvement over the New Zealand results with 1.3% fewer networks using WEP, something that indicates that the Australians are slightly better at securing their networks than the New Zealanders.

Finally, the selection of channels is compared to indicate how efficiently the networks are being utilised as regards data throughput. Recommendations are that channels 1, 6 and 11 only should be used as the channels ‘bleed’ over into neighbouring channels affecting the throughput of the neighbouring channels. This channel bleed affects the two neighbouring channels so that if only the recommended channels are utilised there will be no interference from the other channels giving 3 non-overlapping channels that can be used at the same time. If a network is using channel 3 for example, it will affect both channels 1 and 6, slowing their throughput. Channel 3’s throughput will be affected by networks using channels 1 and 6, so the effect is much slower throughput for all users. Figure 9 shows the channel selection for the New Zealand survey.

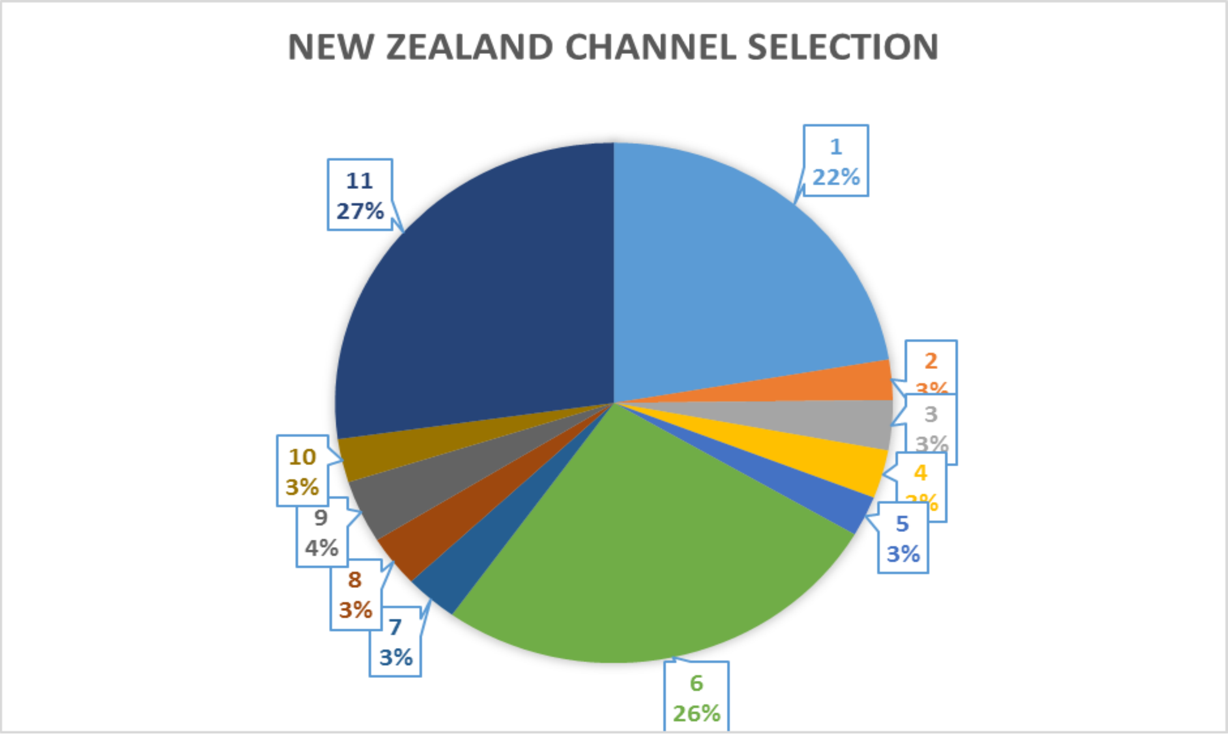


Figure 9: Channel selection in New Zealand in 2013

Usage of channels 1, 6 and 11 account for 75% of the networks surveyed. Whilst this shows that most users are aware that these channels should be used for efficient running of their networks, ¼ of the networks are being implemented inefficiently, and worse affecting those networks that have been installed correctly. Figure 10 shows the results for the Australia survey which compare closely with that of New Zealand.

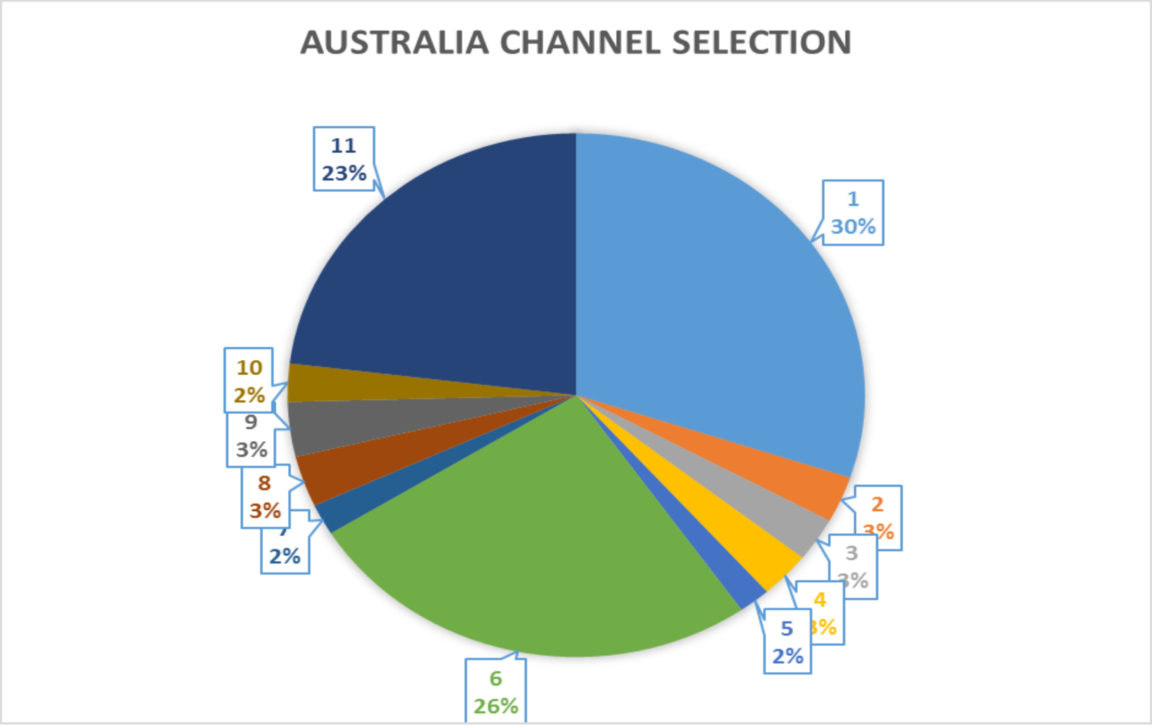


Figure 10: Channel selection in Australia in 2012

The total percentage of networks using channels 1,6 and 11 is 79%, again slightly higher than New Zealand's total. This indicates that users in the Perth area are complying with the recommended channels better than their counterparts in New Zealand. From these results it appears that as the Australian users are using their networks with better encryption and by complying more closely with the recommended channels, they are being better informed of the recommendations and are complying with the information more closely than those in New Zealand. It is interesting to note that in 2012 the Australian Police in Queensland planned to survey wireless networks to identify insecure deployments and inform their owners where possible of their insecurity and how best to deploy them safely (Kirk 2012). The publicity generated with the best of intentions led to criticism that the Police should not be snooping on networks as it was described as 'none of their business' if users did not secure networks securely. Whilst this odd stance by the media and some of the public led to the information campaign being cancelled, the publicity generated may well have assisted in educating readers at least of the vulnerabilities, perhaps leading to some increase in security of the networks.

CONCLUSION

Wireless networks have been available as an IEEE standard since 1997. Security in the form of WEP was provided with the wireless equipment when IEEE 802.11 was extended to the 'a' and 'b' versions in 1999. The initial issues with this security standard were much publicised and in 2003 WPA and later WPA2 became available. Wireless devices very quickly became available at cheaper and cheaper prices that incorporated these later security standards, yet the surveys show that some networks are still being deployed with WEP. This is worrying considering that replacement equipment is cheap and the benefits from secure networks are many, especially with privacy of data and protection of assets. The poor channel selections that account for 25% of networks in New Zealand and 21% of networks in Australia indicate that there is still work to be done to educate and assist users in how most effectively to deploy their networks. Whilst these studies are now 3 and 4 years old respectively, later casual surveys indicate that only slight improvements have been made. There still needs to be work from manufacturers, retailers and network administrators to continue improvements to ensure all users are utilising their wireless networks as securely and as efficiently as possible.

REFERENCES

Arbaugh, W. A., N. Shankar, et al. (2002). "Your 80211 Wireless Network has no Clothes." IEEE Wireless Communications 9(6): 44-51.

Cam-Winget, N., R. Housley, et al. (2003). "Security flaws in 802.11 data link protocols " Commun. ACM 46 (5): 35-39

Fluhrer, S., I. Mantin, et al. (2001). Weaknesses in the key scheduling algorithm of RC4. Eighth Annual Workshop on Selected Areas in Cryptography. Toronto, Canada.

Kirk, J. (2012) In Australia Secure Your Wi-Fi or Face a Visit From the Police.

Lashkari, A. H., M. M. S. Danesh, et al. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009. .

Nechvatal, J., E. Barker, et al. (2000, 2nd October 2000). "Report on the Development of the Advanced Encryption Standard (AES)."

Stubblefield, A., J. Ioannidis, et al. (2002). Using the Fluhrer, Mantin, and Shamir attack to break WEP. Network and Distributed Systems Security Symposium (2002).

Vibhuti, S. (2005) IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability.

Walker, J. (2000). "Unsafe at any key size, An analysis of the WEP encapsulation." http://www.dis.org/wl/pdf/unsafe.pdf

Walker, J. (2003). "802.11 Security Series Part III: AES Based Encapsulations of 802.11 Data." from http://jcbserver.uwaterloo.ca/cs436/handouts/miscellaneous/Intel_Wireless_1.pdf.

WiFi Alliance (2007) Introducing WiFi Protected Setup.