12-4-2013

A 2013 Study of Wireless Network Security in New Zealand: Are We There Yet?

Alastair Nisbet
AUT University of Technology

DOI: 10.4225/75/57b567a3cd8e6
11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013

A 2013 STUDY OF WIRELESS NETWORK SECURITY IN NEW ZEALAND: ARE WE THERE YET?

Alastair Nisbet
AUT University of Technology, Digital Forensic Research Laboratories,
Auckland, New Zealand
anisbet@aut.ac.nz

Abstract
This research examines the current level of security in wireless networks in New Zealand. A comprehensive wardrive covering the length of the country was made in January 2013 to ensure accurate comparisons from two previous wardrives as well as comparisons between the four main cities and the suburbs can be made. With 16 years since the introduction of the original IEEE 802.11 wireless standard having passed, an examination is made of the current state of wireless security of networks throughout New Zealand and the Auckland suburbs, and where possible compares these results with similar studies undertaken in 2004 and 2011. Additionally, comparisons are made with growth of numbers of access points, security standards implementations and channel selections. This study looks at whether wireless network security has reached the levels hoped for in 1999 when security was built in to the IEEE 802.11a and 802.11b standards and concludes that whilst vastly improved, there is still some way to go. Finally, some recommendations are made as to what still needs to be addressed to ensure efficient and secure communications with wireless networks.

Keywords
Security, Wireless Networks, Privacy, Wardrive

INTRODUCTION

Wireless networks have been available to businesses, organisations and consumers for well over a decade. As costs have decreased and performance has increased, wireless device uptake have seen increasing growth. The initial security issues that surfaced after the introduction of the original IEEE 802.11 standards of 1997 and 1999 are now a distant memory. The considerable publicity over the security issues and potential attacks has had a significant influence on even the most technically unaware user. Whilst the original research in 2004 found significant numbers of networks open or poorly protected, by 2011 the percentage had increased from around 62% using encryption to around 85%. This 2013 wardrive seeks to achieve one significant goal, to see if the trend in increasing security in these networks has continued and whether it can be concluded that security has reached the point where wireless networks, at least in one small country, can now be considered secure. Further, the issues of channel selection leading to inefficiency in the networks is looked at to see whether the newer software assisting users during setup with effective channel selection are having the desired effect.

This paper is organized as follows. Security briefly examines the security of the networks from their introduction to the present day. Channels discusses the available channels and the importance of selecting the recommended channels. Data Collection outlines the method of data collection, and Results and Discussion analyses the results obtained from the data collection. Finally, Conclusions looks at the original question as to whether security of wireless networks at the levels we hoped it would be in 1999, and makes some recommendations for increased efficiency and further enhancements to security.

SECURITY

In 2001 a paper was published highlighting the problems with the implementation of the encryption algorithm used in WEP (Fluhrer, Mantin et al. 2001). Whilst the algorithm itself, RC4 was considered secure, the implementation in this standard caused the encryption to become insecure. Also that year, a paper was published describing described how the weaknesses in the way the algorithm had been implemented leads to practical attacks against the WEP symmetric key (Borisov, Goldberg et al. 2001). Finally in 2002, a practical attack against a WEP key was demonstrated proving that WEP could be relatively easily circumvented with approximately 5GB of data collected from a WEP secured network. (Stubblefield, Ioannidis et al. 2002). In 2004, a survey of New Zealand businesses found that a major reason for non-deployment of wireless networks in the workplace was fear of poor security (Houliston and Sarkar 2005). In 2003, manufacturers of wireless networking equipment, along with other interested industries together developed a new, temporary standard called WiFi Protected Access (WPA). Two versions were available, one using a pre-shared symmetric key suitable for home or small business users, and one using a separate server to handle encryption key creation and deployment. The extra equipment needed for this type of security setup, designated WPA2, meant that it was most likely that larger business would be the ones to adopt it. WPA and WPA2 were designed to fix all of the problems with WEP ensuring robust security and allaying fears from potential users of the network. The design of these new standards proved so successful that they were used as a basis for standards included with the wireless devices to replace WEP. With WPA still utilised and WPA2 now available in a simple pre-shared key version, robust security can simply be set up by all users.

CHANNELS

One issue that arose with the 2.4 GHz frequency band that does not arise with the 5GHz band is that of channel bleed. The 2.4 GHz band gives 11 separate channels in most countries (14 in New Zealand) and the user selects a channel or one is automatically selected during initial setup. If there are other networks in the area on the same channel, interference will occur slowing down the network. The problem with the 2.4 GHz channels is that they 'bleed' onto other channels. That is, a selected channel will interfere with the 2 channels either side of it. If for example channel 6 is chosen, then channels 4,5,7 and 8 will also be affected. To counter this, it is recommended that only channels 1,6 or 11 should be used, preventing any radio signal 'bleeding' affecting the other channels. However, the user is free to choose any of the channels to use and if the device is configured to choose the least used channel it will do so at the time the device is configured. Whilst the automatically chosen channel may be least used when configured, it may not be so during normal operational hours. Both of these scenarios can lead to channels chosen that may become congested or may affect other channels chosen by other devices so that neighbouring devices slow each other down. In New Zealand there are 14 available channels but as there needs to be a gap of 5 channels, 16 would be required before channel 16 could be chosen and this would not interfere with channel 11. Therefore, choosing channels 12, 13 or 14 does not increase the efficiency of the network. Additionally most equipment does not provide for these extra channels in New Zealand so channels above 11 are rarely available and chosen.

In 2008, researches uncovered a minor problem with WPA using a pre-shared encryption key, called WPA-TKIP (Takahashi 2008). It is possible to mount a successful attack against the key during the initial login phase where an exchange of messages is taking place. However, if the devices are using keys greater than twenty characters then a brute force attack against the encryption key is not computationally realistic (Moskowitz 2003). It would simply take too long. Whilst WPA-TKIP, also called WPA-Personal utilises the RC4 algorithm, WPA-CCMP, known as WPA-Enterprise uses the AES algorithm. The AES standard was adopted by the United States Government in 2001 as its standard to replace 3DES and is presently considered entirely secure (United States Government 2003). The WPA2 standard which was ratified as the IEEE 802.11i standard was initially designed to utilise a separate RADIUS server for encryption key creation and distribution. This method has now become more commonly known as WPA2-CCMP or WPA2 Enterprise, with WPA2-TKIP, also

called WPA2-Personal available with a pre-shared symmetric key entered by the user manually or automatically generated by the device. The advantage of the Enterprise methods is that it supports the use of AES with a key up to 256 bits whilst TKIP uses the older RC4 algorithm (Lashkari, Danesh et al. 2009). AES gives comfort to those wanting an entirely unbreakable encryption but at the expense of more computation time and battery drain. However, the reality is that TKIP with a 20 character key or greater is extremely secure and suitable for most networks with the advantage that older, more basic wireless devices can generally utilise RC4 but cannot always implement AES. With these 4 methods of encryption available, the older WEP encryption is now considered obsolete and with newer software freely available that can crack a WEP key in less than a minute with less than a Gigabyte of captured data (Alkema 2013), WEP should not be used even for private use.

The high level of publicity of the insecurity of WEP when first discovered appeared to slow the adoption of wireless networking for some years. However, the development of WPA and WPA2, over time, significantly allayed the fears and wireless network in recent years has seen explosive growth. Whilst other attacks against wireless devices are possible, such as MAC address spoofing to circumvent an Access Control List, proper implementation of encryption can prevent unauthorized joining of the network and unauthorized reading of the messages. Recently, changes to the setup procedure for devices has meant that even very technically unskilled people are prompted to enter keys or have them automatically generated. Many devices now come with automatic setups where users need only enter a pin number, often found on a sticker on the wireless access point, to have the encryption keys generated and installed at the press of a button. This is very different from the earlier days where in 2006 a survey found that 44% of people who had wireless networks described activating security on them as moderately to very difficult. The same survey found that whilst 83% of people thought using someone else's WiFi network without their knowledge was stealing, about half of those surveyed admit that they have done so (WiFi Alliance 2007). The ease with which robust security can be implemented leads to an expectation that wireless security would have greatly improved over recent years. To test this theory, a comprehensive wardrive covering all four major cities throughout the length of New Zealand and a comprehensive war drive around the Auckland suburbs was undertaken. The following section describes the collection of data during mid-January 2013.

DATA COLLECTION

A laptop was placed on the front seat of a vehicle with Inssider software running on the laptop. In 2004 this software was not available and so for the first data collection a wireless laptop with Netstumbler was used. This involved a wireless PCMCIA card with external aerial attached which was placed on the roof of the vehicle. In 2011 a comparison was trialed where 1 laptop was set up as it was in 2004 using Netstumbler and a newer laptop was set up with Inssider. It was found that the newer laptop with internal wireless card found approximately 10% more of the wireless networks than the earlier style laptop.

The legality of performing this type of data collection was ascertained prior to the wardrive. In New Zealand, laws introduced in 2003 included specific sections on accessing computer systems illegally and being in possession of tools for doing so were examined. As the software involved did nothing more than log the details of the networks as they were found, no New Zealand laws were breached. In 2012, the Queensland Police intended to do similar activities to locate insecure networks (Kirk 2012). The purpose was to educate users who were not sufficiently securing their networks by providing owners of unsecure networks with an information pamphlet. However, the Police were criticized as some people objected to the Police spending resources on informing people of how to secure their networks when it is not against the law to have an insecure network. As a result, the Police cancelled their plans and instead provided information on their web site on how to secure wireless networks (Queensland Police 2012). This tends to show that many people do not take insecure wireless networks as being a serious threat when in reality an insecure network can expose

owners to theft of data, resources and expose them to liability if their networks are used for nefarious activity.

A wardrive around the Auckland and Wellington central business districts was conducted in April 2004 (Nisbet 2004). A further wardrive in April 2011 was conducted around the Auckland, Wellington, Christchurch and Dunedin CBDs (Nisbet 2012). For the 2013 wardrive, the same streets were covered at a similar time of day to the previous wardrives so that a fair comparison of security and the numbers of devices could be made. Christchurch and Dunedin, both large cities in the South Island were not covered in 2004 but were covered in 2011. Christchurch is the 3rd largest city in New Zealand but because of a devastating series of earthquakes in 2012, the CBD has been almost completely destroyed and is not open to the public. Therefore the data was collected by driving around the outside of the cordons. Dunedin is the 4th largest city in New Zealand and is situated the furthest large city south of the country, with Wellington, the capital city in the middle at the southern tip of the North Island and Auckland the most northern city. Together these 4 cities and their environs make up nearly half the population of New Zealand (Statistics New Zealand 2012).

The data collection followed the routes taken in 2011 and for Auckland and Wellington, those routes also taken in 2004. The total distance covered in Auckland was 7.5 kilometers and in Wellington was 6.5 kilometers. In Christchurch traveling around the cordoned off city center, a total of 7.5 kilometers was traveled, and in Dunedin the distance was 6.5 kilometers. The route taken was within the CBDs as much as possible. The suburban wardrive was added for 2013 and was made up of a number of separate wardrives covering different suburban areas of Auckland. The total distance for this wardrive was approximately 50 kilometers.

RESULTS AND DISCUSSION

With previous results available comparisons could be made in most areas with results from 2 years previously and 9 years previously. Whilst ad hoc networks only make up a minor portion of the networks, these were dealt with separately and the main data refers to infrastructure networks only. In 2011 there was a considerable increase in the number of wireless networks found. This continues in 2013 with Wellington having an explosive growth of 262%. Christchurch was the next biggest growth with 165%, Auckland a significant increase of over 50% and Dunedin with only a small increase of 18%. It should be noted that the CBD of Dunedin is comparatively small and is made up of commercial businesses but is a University city with a significant number of student flats that are mostly single of two level houses rather than apartment blocks. In comparison, Auckland and Wellington have seen considerable increases within their cities of large apartment blocks within the CBD.

	Year	A/P	Percentage Increase over Previous Study	Ad Hoc	SSID Broadcast	Encryption
Auckland	**2004**	**237**	**-**	**5**	**98.3%**	**52.9%**
	2011	**2077**	**776%**	**29**	**98.7%**	**84.6%**
	2013	**3255**	**56%**	**38**	**99.7%**	**77.6%**
Wellington	2004	35	-	2	100%	56.8%
	2011	953	2622%	12	95.1%	83.4%
	2013	3445	262%	25	99.8%	81.7%
Christchurch	**2011**	**418**	**-**	**5**	**86.3%**	**91.0%**
	2013	**1108**	**165%**	**7**	**99.8%**	**84.1%**
Dunedin	2011	1044	-	12	89.2%	84.2%
	2013	1232	18%	19	99.5%	80.4%
Suburbs	**2013**	**5069**	**-**	**33**	**99.3%**	**97.4%**
All	2013	14109	-	122	99.6%	88.6%

Table 1. Comparison of results

In 2004, just over half of the infrastructure networks discovered were using encryption. By 2011, this figure had increased significantly for all cities to over 80%, with Dunedin over 90%. In 2013, the number of networks had continued to increase yet the percentage of encrypted networks had reduced. Over 5000 private networks were found in the Auckland suburbs with encryption of those networks at 97%, significantly higher than in all four cities.

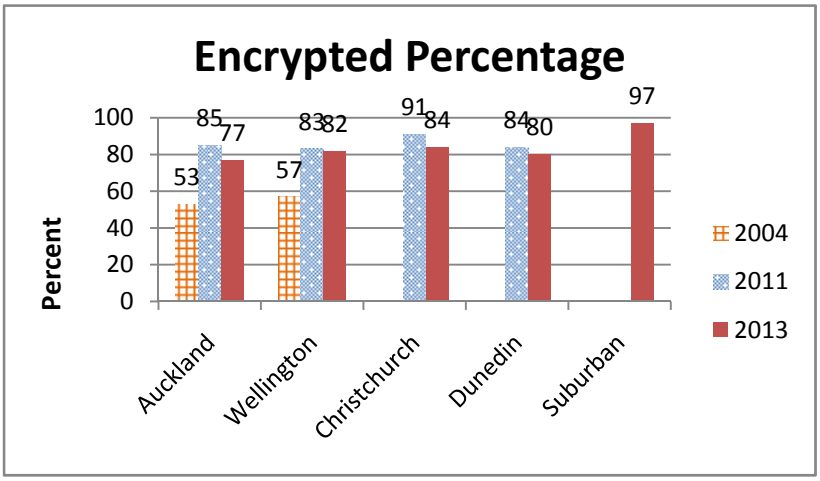

Figure 1. Encrypted Infrastructure Percentage

Some explanation for the reduction in the cities' encryption can be explained by the growth of free WiFi offered in hotels, cafes and throughout metropolitan areas. As technology has improved and the prices for equipment have reduced, free networks have grown considerably over the past 2 years. These networks are deliberately not encrypted to allow people to quickly and easily join and use the service. Any security such as encryption is left to the individual to organize through utilizing a VPN or similar, and so several percentage points can be attributed to access points that are deliberately unencrypted.

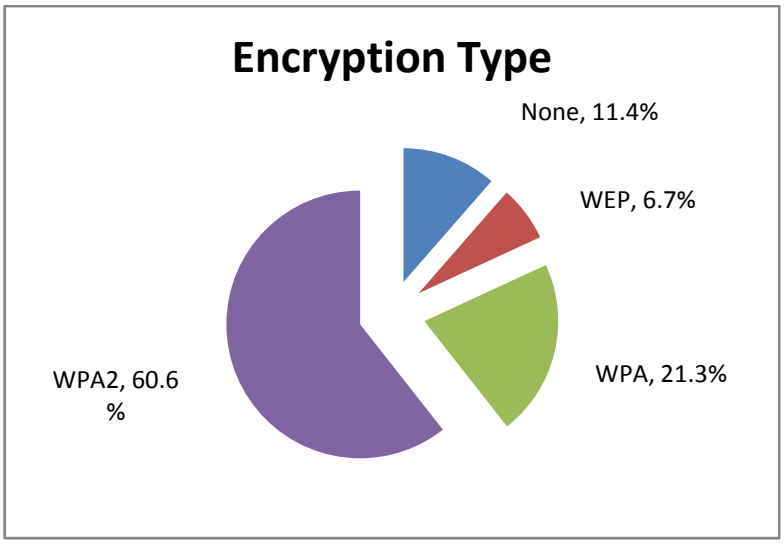

Figure 2. Summary of encryption percentages

The type of encryption used has a significant effect on the security of the network. Whilst over 11% of the infrastructure networks use no encryption it is estimated by examining the Service Set Identities of those networks that approximately half of those unsecured are deliberately unsecured. What is of more concern is that 6.7% of networks are using WEP. Whilst some level of encryption may be considered better than nothing, using outdated and easily breakable encryption may give users a false sense of security. At least if there is no security the user knows there is no security, but if insecure technology is used, are your communications being monitored or not? WEP is insecure and should not be used, especially in commercial enterprises where breaking encryption keys may lead to leaked information and unauthorized use of resources. Table 3 shows a break-down of this information by city, showing that Auckland and Dunedin lead the way with the most secure encryption percentages for WPA and WPA2.

Encryption	Auck	Well	Christ	Dun	Sub
None	22.4%	18.3%	15.9%	19.6%	2.6%
WEP	5.2%	3.1%	10.8%	4.2%	9.7%
WPA	30%	19.0%	18.1%	22.1%	24.1%
WPA2	64.7%	59.5%	71%	73.6%	66.1%

Table 2. Types of encryption 2013

One difficulty for network administrators can be catering to legacy equipment that only uses WEP encryption. In this case, allowing WEP compromises the rest of the network so that other access points on the same network set to use WPA or WPA2 no longer assure users that robust security is being utilised.

An important factor that significantly affects the efficiency of the network is channel selection. Interference from other wireless devices can severely slow throughput on the network. The necessity of choosing the best channel to operate on is one factor that many users may not be aware of. Default channels exist for many access points and the user does not need to consciously choose a channel. Others will automatically choose a channel with the least interference, at least at the moment of setup. However, figure 3 shows that if users choose the recommended channels of 1,6 or 11, they will often select channels used by neighbouring networks causing both networks to run slower because of interference.

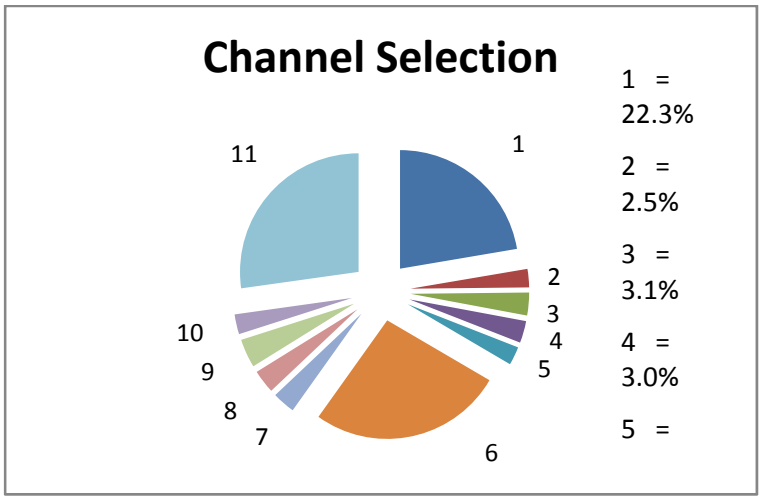

Figure 3. Channel selection percentages

Figure 3 shows that the three recommended channels of 1, 6 and 11 are used by over 75% of the infrastructure access points. This adherence to the recommended channels is pleasing, but with almost ¼ of the networks using other channels, significant inefficiency on the networks is occurring. It is interesting to note that for suburban networks, 79% of access points are using the 3 recommended channels. This follows the trend of private networks being more securely configured than commercial networks. With even a small percentage of neighboring networks being on overlapping channels, all users should do a simple site survey with appropriate software to assist them with selecting the most appropriate channel. Clearly, surveys should be done several times at varying times of day as one survey may give spurious results. Broadcasting the SSID makes the access point easier to find for users and potential attackers. By broadcasting the SSID the access point SSID name is not only visible, but the parameters such as whether encryption is implemented or not and if so, what type of encryption is used is also disclosed. A malicious attacker may therefore search for access points that are either unencrypted or encrypted with WEP. By not broadcasting this information an attacker must either probe for replies from hidden access points, or monitor traffic to infer the existence of an access point. In 2013 almost all networks, both commercial and private, are broadcasting their SSIDs. This is something that for many networks is not necessary and switching off the broadcast adds another layer of security that is simple to implement.

CONCLUSION

With the user-friendly interfaces on the devices, step by step setup where usually encryption needs to be turned off rather than selected, and with push button WiFi Protected Setup available on many devices, non-expert users can simply and easily configure their networks for robust security. The suburban figures show that security is better deployed on private networks than it currently is on commercial networks. Whilst there are a number of reasons for this, clearly encryption is still not utilised as much as it should be. Additionally, WEP is long since passed its usefulness and there is still some education for users to be had as to the type of encryption that should be implemented. Finally, channel selection remains a problem and users should both be aware of the importance of adhering to the recommended channels, and additionally site survey tools should be made readily available during setup and maintenance for all users so that the best channels can be chosen. This 2013 wardrive covering an entire country shows that the publicity, education and better design of installation software along with other factors has had the desired effect of increasing security. In 1997 when IEEE 802.11 was ratified, security was not part of the original standard. Two years later this changed with the ‘a’ and ‘b’ modifications to the protocol but serious security flaws in

WEP highlighted within a few years of their introduction made consumers nervous. Now, fourteen years on from those protocols, this research shows that security has finally reached acceptable levels. Users should now be aware that they should use the available security and when joining a network check what method of encryption is used and ensure they have robust passwords of acceptable lengths, generally at least 20 characters to be certain of robust encryption. The focus can now be on using WiFi to enhance our use of technology without always questioning whether it is really safe to use. Are we there yet? This research shows that if not quite there, the destination is just around the next corner.

REFERENCES

Alkema, P. (2013, 8th September 2013). "Automatically Crack All Wi-Fi Routers' WEP Keys With Only 30 Seconds Worth of Work." Retrieved 8th September 2013, from http://paulalkema.com/post.cfm/automatically-crack-wifi-with-only-30-seconds.

Borisov, N., I. Goldberg and D. Wagner (2001). Intercepting mobile communications: the insecurity of 802.11. Proceedings of the 7th annual international conference on Mobile computing and networking. Rome, Italy, ACM.

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

Houliston, B. and N. I. Sarkar (2005). "Wi-Fi Deployment: A Survey of Large New Zealand Organisations." International Journal of Business Data Communications and Networking 1(3): 37-58.

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

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

Moskowitz, R. (2003) "Weakness in Passphrase Choice in WPA Interface."

Nisbet, A. J. (2004). Wireless Network Security, A Tale of Two Cities. Auckland, New Zealand, IIMS Post Graduate Conference, Massey University.

Nisbet, A. J. (2012). A Tale of Four Cities: Wireless Security Growth in New Zealand. Computing, Networking and Communications (ICNC), 2012 International Conference on.

Queensland Police. (2012). "Secure your wireless network at home." Retrieved 22nd December 2012, 2012, from http://www.police.qld.gov.au/programs/cscp/eCrime/wireless.htm.

Statistics New Zealand (2012). National Population Estimates. Statistics New Zealand. Wellington, NZ Government.

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

Takahashi, T. (2008) "WPA Passive Dictionary Attack Overview."

United States Government (2003). CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information.

WiFi Alliance (2007) "Introducing WiFi Protected Setup."