AUCKLAND UNIVERSITY OF TECHNOLOGY

WarDriving: Auckland Case Study

Has the security of wireless networks improved in Auckland's CBD in the past 5 years?

Thomas Laurenson

0958095

Abstract

This research report discusses the 802.11 wireless networking standard and the associated security issues in regards to the assessment of Auckland's Central Business District (CBD) wireless infrastructure. The field trial method of WarDriving was proposed to gather data on WLANs, which were analysed to determine if the security features of the 802.11 standard have been implemented.

The field trails methodologies have been evaluated and tested prior to the field trial being conducted. The final field trial method utilises the Kismet WarDriving application as the method to collect the data using an Apple MacBook with an AirPort Extreme wireless network adaptor as the testing machine.

The results have been analysed, discussed and compared with a similar study previously conducted by Lin (2003) to attempt to answer the research question: Has the security of wireless networks improved in Auckland's CBD in the past 5 years?

The results show that the security features implemented, in particular the use of encryption, on WLANs has improved in the last 5 years. The previous study by Lin (2003) concluded that 39.8% of WLANs discovered had implemented encryption on their networks. This study discovered a total of 3572 APs, of which 2495, or 69.85% were actively implemented with encryption. This shows a distinct rise in the number of encrypted WLANs in the Auckland CBD area, and proves that the security of wireless networks in Auckland's CBD has indeed improved in the last 5 years.

1.0 Introduction

The topic for this research project is to assess the security of Wireless Local Area Networks (WLANs) in the CBD of Auckland City and compare the results to a similar study previously conducted by Lin (2003).

This research project is of great interest to me because I am fascinated by both wireless technology and the security issues related to computer systems. Wireless security presence and associated problems were first introduced to me by a lecturer, Hira Sathu during my under-graduate studies at UNITEC in Auckland.

In the 5 years since the dissertation was written by Lin in 2003, there have been many advances in the standards and technology of WLANs. The introduction of a new specification 802.11n and standardization of WPA, means that better infrastructure and security options are now available.

The topic has significant and current relevance mainly because wireless networking technology has become a major aspect of the infrastructure of both commercial and household computer networks.

These issues have become well known to both the commercial and household users. Media coverage has emphasised the importance of wireless networks and also highlighted the concerns relating to network security, plus the related legal and technical aspects. Commercial as well as household users of wireless technology should be made aware of the security aspects of the technology and this research project is aimed at identifying those areas of concern.

2.0 Ethics and Legality of Field Trials

Ethics

After writing the research proposal and receiving feedback there were ethical issues regarding this research project. I outlined in the research proposal to attempt to gain approval to conduct the study from AUT, which bought about ethical issues regarding AUT taking legal responsibility for the research being conducted.

For specialist information regarding the legality and ethical issues surrounding this I contacted Professor Noel Cox a Professor of Law and Chair of Department of Law at AUT University. Noel had previously been a guest lecturer for the eCrime and Governance paper I had taken. Given his background and his specialisation in public law and law and technology he was the perfect person to consult regarding the issues I was facing.

After explaining my situation to Noel he personally contacted the Ethics Committee at AUT and discussed my intended research methodologies querying if there would be any issues conducting the research. The feedback provided was that no ethics approval was needed as the research did not involve human participation. However, getting ethics approval for AUT to take responsibility for the study was beyond the scope of this research project.

The AUT website also provided valuable information regarding ethical approval for the research project from the AUT Ethics Knowledge Base (AUT KB, 2009). A PowerPoint presentation provided by the knowledge base, entitled 'Getting Ethics Approval' also indicated that ethics approval was not needed as the other people would not be participating in the research (AUTEC, 2008, pp. 5).

Legality

The issue of legality was still important as it was now my responsibility to ensure that precautions were taken to mitigate any potential legal risks while conducting the research.

I also queried Professor Noel Cox regarding the legality of the WarDriving methodology to be used to gather data. Due to the specialised nature of the method he was unable to provide any more solid information regarding laws that could possibly hinder the process. After discussing the method, outlining precautions to be taken and research I had previously conducted in the research proposal he agreed that the WarDriving method was located in the 'likely legal' or maybe 'gray' area of the WarDriving legal continuum displayed in Figure 3 below.

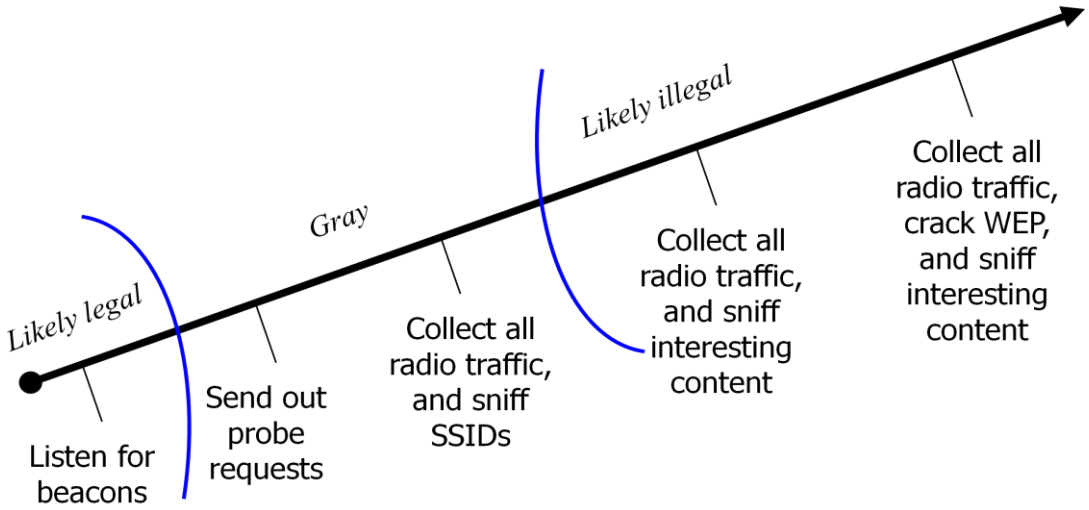

Figure 1: Legal WarDriving Continuum (Hoar, 2006)

As it was my own personal decision whether or not to continue with the research, I concluded that the research I had conducted into the legal issues provided enough information to ensure that the method was legal and that any legal issues confronted would be held personally accountable by me as an individual party.

Professor Noel Cox also made the following recommendations to me regarding my study from a legal perspective:

- Conduct the field trials from public places
- Aggregate the data found into statistics

Precautions

As outlined in the research proposal TCP/IP addressing was turned off on the laptop used in the field trials. Figure 2 below shows a screenshot of the AirPort network preferences on the test machine.

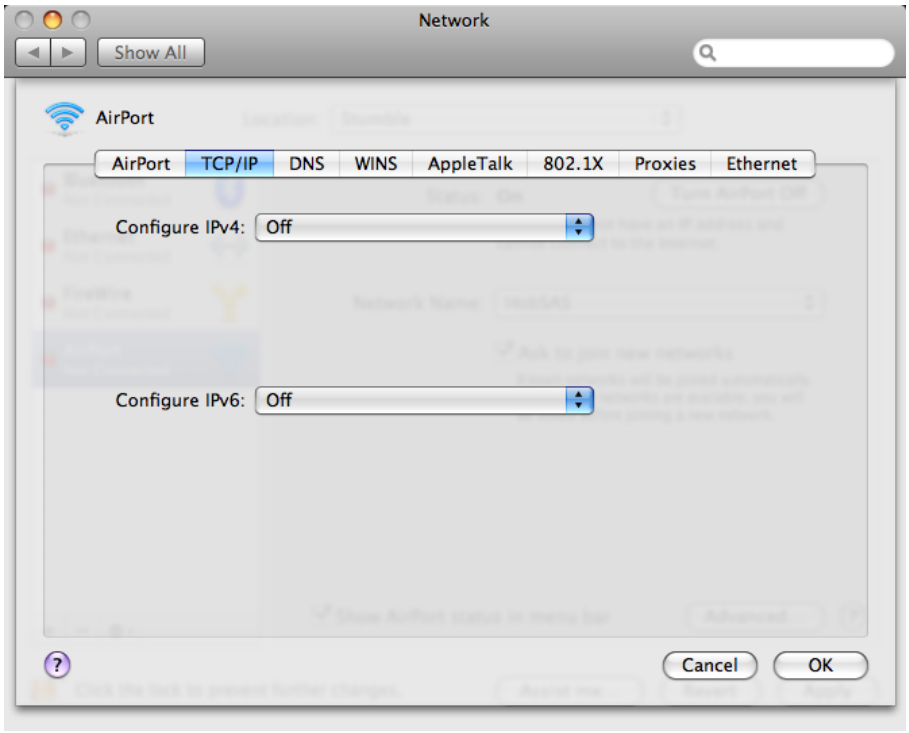

Figure 2: OS X Network Properties: TCP/IP

It can be seen that both the IPv4 and IPv6 service has been turned off. This precaution has been taken as it completely removes the ability of the test machine to automatically connect to an AP.

A further precaution of spoofing the MAC address of the test machine was also implemented. This was done to hide the actually physical addressing of the testing machines MAC address. Figure 3 below shows the MAC address of the testing machine has been spoofed by replacing the 3rd and 6th octet with other information providing a different MAC address.

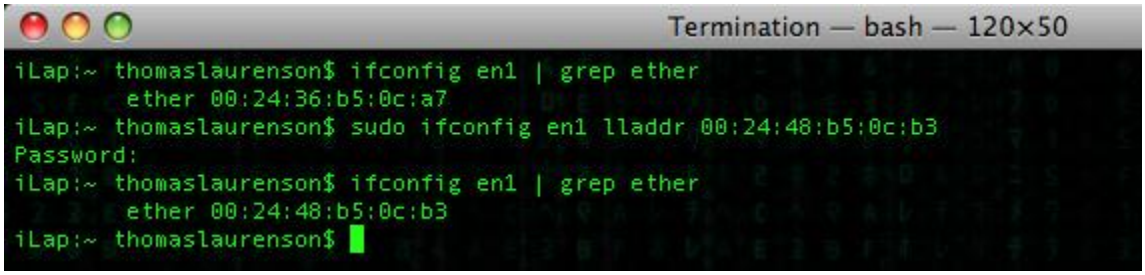

Figure 3: Wireless Card Configuration in Bash Shell

4.0 Research Design Evolution

The information addressed and discussed in the research proposal outlined the research design that was to be attempted in the field trials. The only firm conclusion that was 'set-in-stone' in the research proposal was the use of the Kismet application to gather the data. Information now covered in this section was the continuation of an ongoing design and has hence been labelled 'design evolution'.

The various methods and applications will be discussed and evaluated through the use of testing and experimental field trials.

4.1 Hardware Method

The hardware method needed to be in the form of a mobile computer system. The mobile computing system was to be configured with an operating system able to run the chosen WarDriving software, Kismet.

The proposed hardware to be used in the field trials has been outlined and discussed in sections 4 and 6 of the research proposal. The following list was the original proposed method:

- Toshiba Laptop Computer.
- Buffalo OEM PCMCIA wireless network adaptor card with SMA connector. This card uses the correct chipset (Hermes) for compatibility with Kismet.
- iPaq 3975 with expansion pack to attach a PCMCIA wireless network adaptor card.
- Proxim omni-directional high-gain antenna (+ 7dbi) with SMA connector to attach to PCMCIA network adaptor.
- Garmin eTrex GPS unit that can be connected to either the laptop or iPaq PDA via a serial port to map the waypoints (latitude and longitudinal co-ordinates) of discovered WLANs.

The intention to use an iPaq Pocket PC was quickly eliminated from my initial proposal. The iPaq model 3975 is an outdated Pocket PC and caused a range of issues including lack of availability of software, hardware accessories and current information. As the iPaq could not function correctly with the default operating system the likelihood that it would run with a third-party operating system of a different platform was slim.

This was a major drawback as the iPaq provided an excellent solution for a mobile device to conduct the field trials.

The original research proposal included the use of a GPS unit to connect to the testing machine. The Kismet application supports GPS data input and was to be used to map the longitude and latitude co-ordinates of discovered APs. The main reason for this was to attempt to analyse trends of WLAN security based on mapped locations in the CBD. For example, is there inferior WLAN security implemented in the outlying perimeter sector of the CBD?

Based on advice offered by Professor Noel Cox it was decided to abandon the use of GPS from the research project. It was realised that it would be superfluous to the study as the data gained

from the GPS waypoints could not be used to identify ad further answer other research questions. Instead, the intention now was the data gathered was to be aggregated into a statistical report.

With both the iPaq and GPS unit removed from the proposed method, the end result was that a much simpler hardware and software design package was possible that could be cohesively tested and evaluated.

This left the following items in the proposed hardware method:

- Toshiba Laptop Computer.
- Buffalo OEM PCMCIA wireless network adaptor card with SMA connector. This card uses the correct chipset (Hermes) for compatibility with Kismet.
- Proxim omni-directional high-gain antenna (+ 7dbi) with SMA connector to attach to PCMCIA network adaptor.

At this stage I started testing with the Toshiba Laptop and Buffalo PCMCIA wireless network adaptor. Testing discussion and analysis is further covered in the Field Trials Method (Section 4.3) in this report.

4.2 Software Method

"Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system" (Kismet, 2009), and was proposed to be used due to the following features:

- Passive scanning method
- Hidden network SSID decloaking
- Manufacturer and model identification of access points and clients
- XML output
- CSV output
- Dump file output

The use of the Kismet application has already been identified as the preferred WarDriving software to use in the field trials. During the testing phase (Section 4.3) the application proved to be the superior choice to other wireless sniffers tested including Network Stumbler on Windows, iStumbler and KisMAC on Mac OS X and airodump-ng on Linux.

Kismet saves the output of information gathered into different file types including xml, csv and dump. The main file used for this study was the csv format that separates values gathered by semi-colons which can then be imported into an appropriate viewer for analysis.

The main issue found with the csv file format was that it was difficult and impractical to combine Kismet output files. This was due to the large amount of data that was gathered and the fact that no application had been devised to simplify this process of the combination of files. This information showed that a single Kismet output file was needed to simplify the analysis of data gathered. A single output file can only be achieved if the entire field trial was conducted in a single sweep of the target area, without closing or restarting the Kismet application.

4.3 Field Trials Method

Preliminary field trials were conducted to test the hardware and software solutions discussed in the above section. The preliminary field trial was first carried out in a testing environment on my own HAN (Home Area Network), and secondly by conducting experimental runs based on the field trial method.

HAN Testing Phase

Testing on my own network was a perfect way to analyse the method needed to collect the data and also to interpret the information that was collected.

For interpretive reasons the topology of my HAN is displayed in Figure X below:

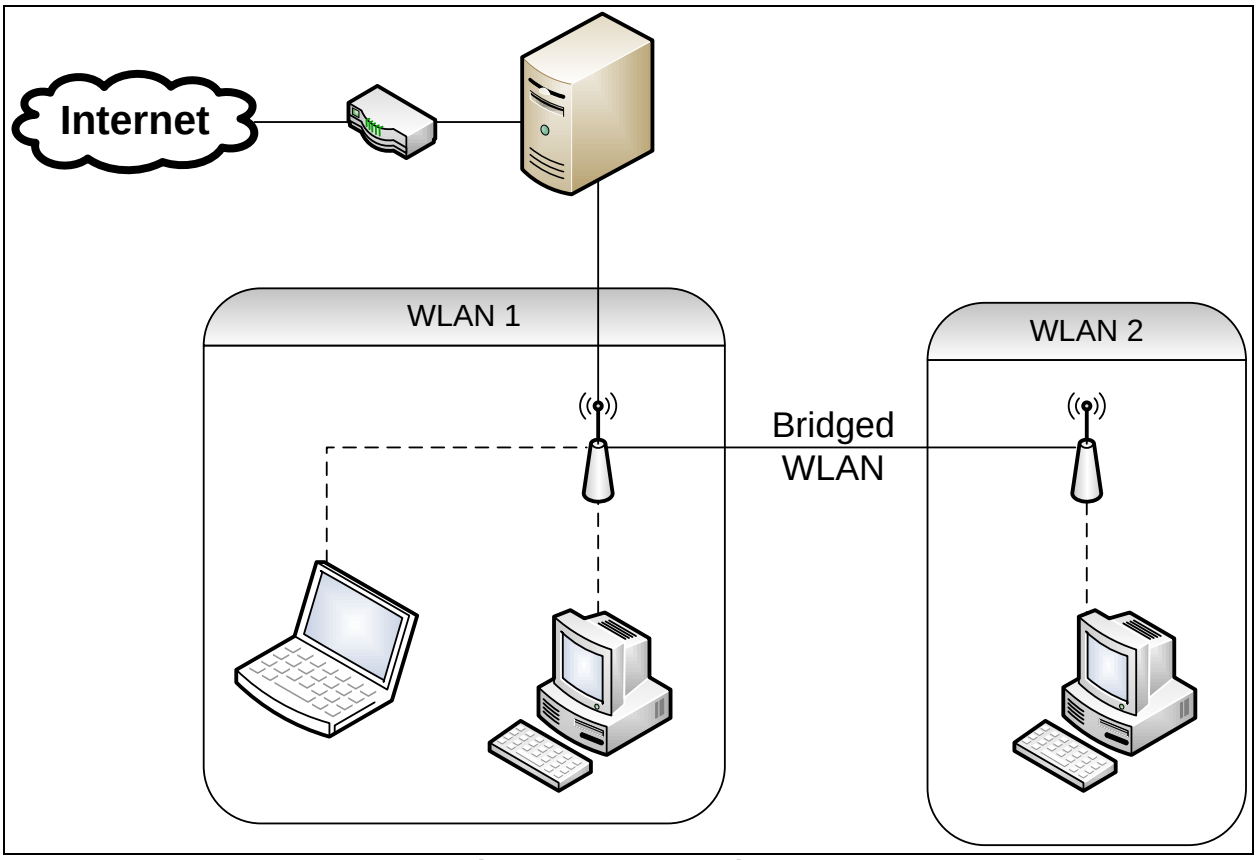

Figure 4: HAN Topology

The network includes two separate Access Points (AP) that are bridged into one WLAN. The two APs are located in separated buildings and are approximately 25 meters apart. The APs are TP-LINK Wireless routers (model TL WR642G) set to operate on 802.11g mode. WLAN 1 especially is a good test area as there is a very small amount of coverage lost due to no other devices using the 2.4GHz frequency, for example, cordless phones and microwave ovens.

After receiving the Buffalo PCMCIA card which was bought especially for this study, I tested it on the Toshiba laptop for the first time. Although the field trial specifies that Kismet be the

preferred software to be used, NetStumbler (Milner, 2004) was used initially to test the signal strength of the PCMCIA wireless card.

Figure 5 shows a test conducted using NetStumbler version 0.4.0. It can be seen that there are two distinct trends in the data gathered. The average signal, measured in decibels (dBm), is around 50 for the first 3 minutes of the test. The signal then increases to about 65dBm once the omni-directional antenna is connected.

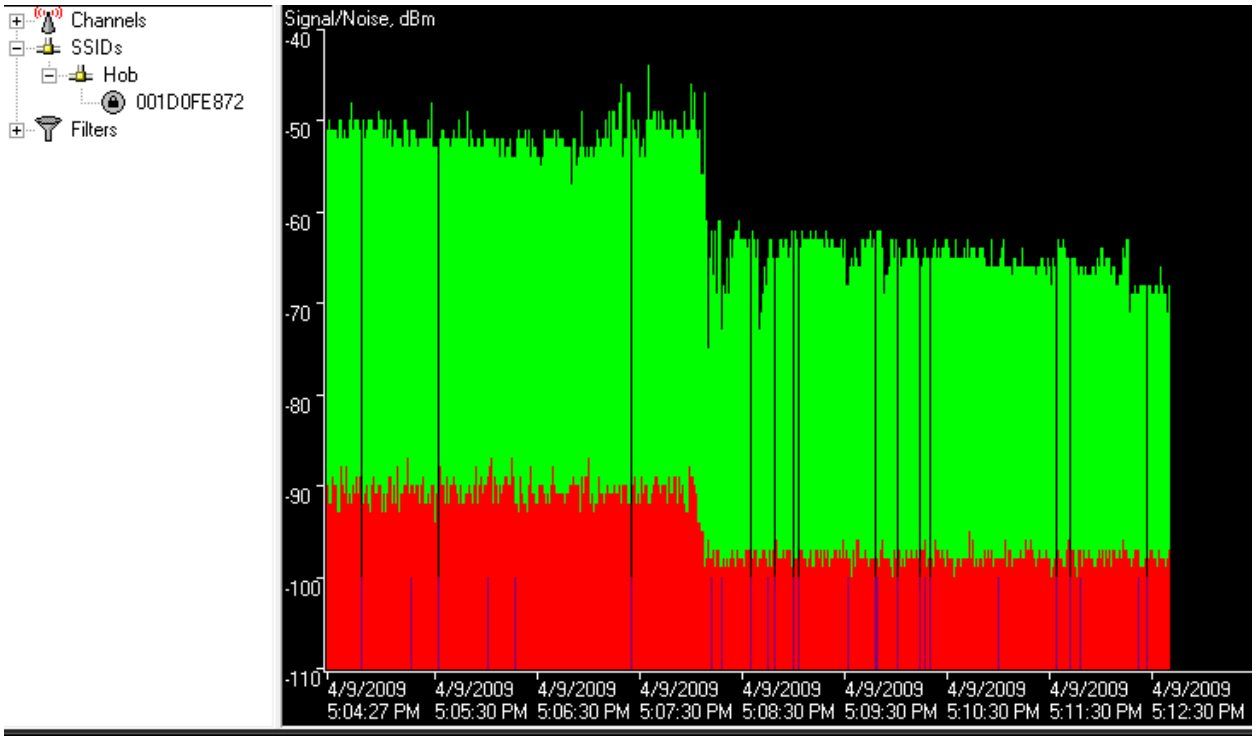

Figure 5: NetStumbler Graph showing Buffalo PCMCIA Signal Strength

The result from this test made me sceptical about using the Buffalo PCMCIA card, as I am used to seeing higher results, especially when in such close proximity to the AP. It should also be noted that only one network (my own) was detected while running this scan, even my MacBook default wireless network manager picks up between 2&3 APs in my area. So another test was subsequently tried using my Apple MacBook running the KisMAC application. KisMAC is an "open-source and free stumbler/scanner application for Mac OS X" (kismacng, 2009) and is a derivative of the Kismet application. The results of the scan can be seen in Figure 6 below. Notice in particular the average signal strength is 76dBm compared to the Buffalo PCMCIA card, with an average of 65dBm with the omni-directional antenna. The maximum rate of 94dBm can also be seen, this is a very high signal rating.

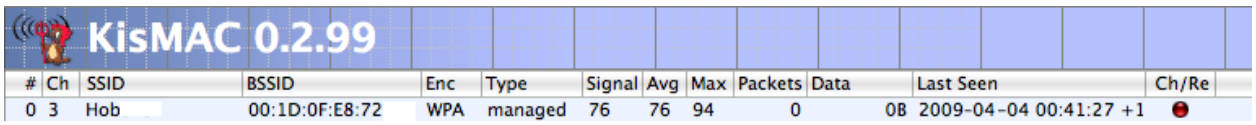

Figure 6: KisMAC Output

The wireless network adaptor in the Apple MacBook is an Apple AirPort Extreme and runs the Broadcom chipset. The AirPort also covers 802.11a/b/g standard compared to the Buffalo PCMCIA card which includes b/g only. This would result in more WLANs being detected in the field trials. There was also evidence that the MacBook was a better choice as it detected multiple networks that did not appear in the previous test.

This left the issue of the ability to run the Kismet application on the Mac OS X platform. This was an exceptionally difficult process as Kismet is designed to be run only on Linux platforms and does not offer a ported version for OS X. However, it is possible to run a variety of different applications designed for Linux on OS X as it is based on a UNIX platform, which is similar to the Linux platform. After performing extensive research from a wide variety of sources from the Web, I managed to compile the Kismet application using XCode developer tools (XCode, 2009) for Mac and Darwin Ports (DarwinPorts, 2009). The combination of XCode and DarwinPorts provide extra functionality to the OS X system to allow the use of applications from other operating system platforms, especially Linux. The documentation available to achieve this is very limited and was finally achieved due to perseverance and a lot of troubleshooting.

Figure 7 shows the Kismet application running on Mac OS X under the same testing conditions in the HAN. It can be seen that multiple APs have been discovered which displays the signal power of the AirPort Extreme wireless network adaptor.

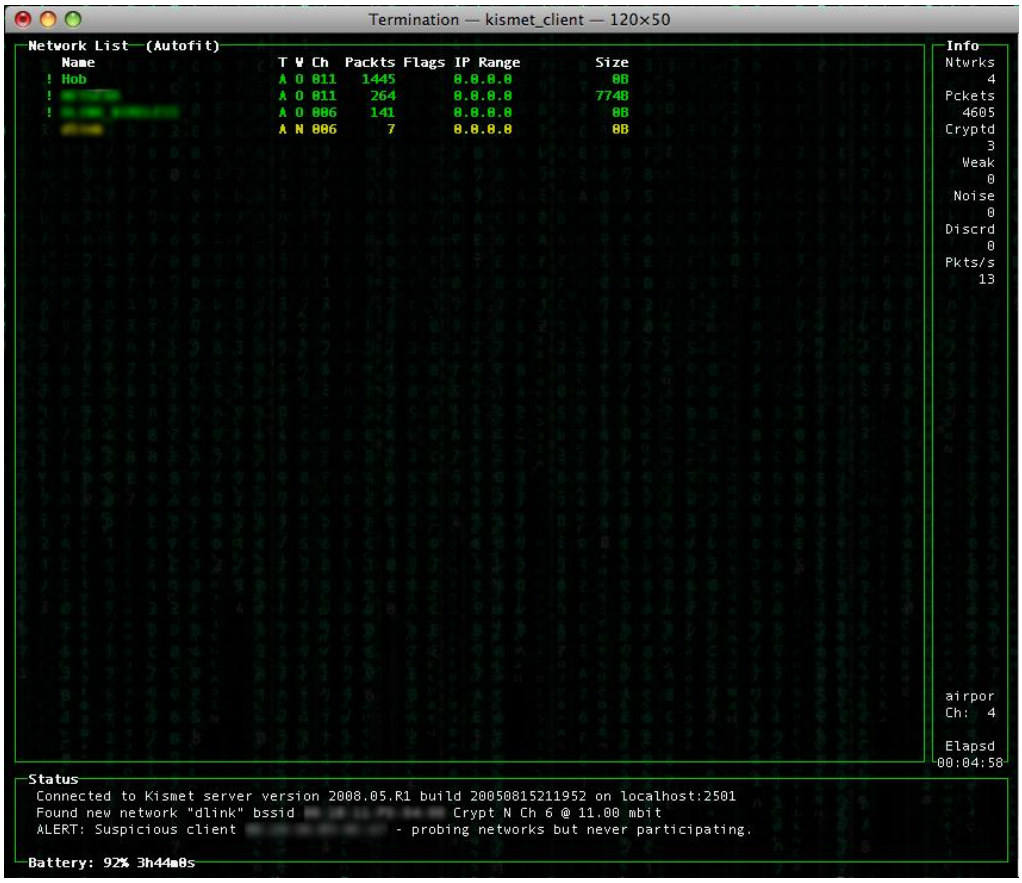

Figure 7: Kismet running on Mac OS X

The ability to run Kismet and the powerful wireless adaptor made the MacBook the new proposed testing method for the field trials. The final configuration and system was:

- Apple MacBook White (Model 5-2, released January 2009)
- Running Mac OSX Leopard (Version 10.5.6)
- Kismet version 2008.05.R1 (latest version at time of writing)
- Apple AirPort Extreme built-in network adaptor

This section of testing occupied the most time throughout the entire research project. Numerous attempts to use other network adaptors and operating systems were tried on both laptops, with no real headway. However, the HAN testing phase eventually showed that the optimal hardware and software solution was to use the Apple MacBook. The information and experience gained from first conducting these test trials resulted in a much simpler transition into the next testing phase in the field.

Experimental Field Trial Testing Phase

Figure 8: Experimental Field Trial Route

After selecting a hardware and software solution from the trials conducted so far, I then needed to test and evaluate this solution in preliminary field trails.

Figure 5, to the left, shows the experimental field trial route chosen which started at the ferry berths in Downtown Auckland, went a short distance eastward along Quay St. then up Queen St. to the AUT WT Building.

This route is more or less central within the field trial area as well as being the route I walk after disembarking from the ferry to reach university. It thus allowed for the tests to be conducted multiple times to thoroughly evaluate the chosen hardware and software and to implement and/or correct specific issues that arose.

As walking had been the proposed method to travel, I prepared to conduct the experimental field trials with the MacBook laptop in my backpack while running the Kismet application. The ability to keep the laptop running with the lid closed was already projected as a potential issue in the proposal report. A solution was found from the website "iusethis.com" which I frequent for information and user reviews on software for all platforms. The light-weight application InsomniaX (Semaja, 2008) can be configured to enable OS X systems to continue operating while the lid is close, instead of the default 'sleep' function. The application description even details the use of the program to "go warwalking", which I found both informative and ironic.

I then conducted my first experimental field trial using the MacBook in my backpack with the Kismet application passively scanning WLANs on the proposed route. This first field trial ended

tragically with the MacBook overheating and power-off half-way through the trial route. The Kismet application did, however, manage to discover approximately 100 networks before the Mac OS X operating system automatically shutdown. This data was automatically saved into the Kismet output files before the shutdown occurred.

For the next trial run I added another application to the MacBook. This was smcFanControl (Eidac, 2009) which allows the user to adjust the speeds of the built-in fans on MacBooks running OS X. This application was recommended by a friend who also uses the software. The idea behind this was to increase the MacBooks internal fan rpm (revolutions per minute) to make the MacBook run cooler in the backpack. The application showed me that the default speed was set to 1800 rpm; I then used a built-in configuration setting of 'Higher RPM' which doubled the rpm to 3600. After conducting tests running only the Kismet application it was found that the MacBook ran at an average of 32°C @ 3600 rpm, compared to 43°C @ 1800 rpm.

The next experimental field trial was conducted using the same route with the MacBook fans operating at the Higher RPM setting. Unfortunately, this test ended with the MacBook overheating again. With the higher rpm it did not shutdown automatically, but was running at 76°C when I removed it from my backpack at AUT WT. This is an unsafe temperature for the MacBook to be running, so it was decided that to store it in a backpack would not be feasible.

The last experimental field trial conducted involved travelling the same route, but instead of storing the MacBook in the backpack, it was carried by hand without a case. As expected, this trial run provided no overheating issues and yielded a passive sniffing capture of the WLANs on the used route. This was, however, an impractical method to use for the final field trial due to the dangers of carrying the MacBook, as it was very new, very expensive and very dear to my heart.

From the information and experience gained from analysing the hardware, software and experimental field trials method it was finally concluded that the best method to collect the data would be using a vehicle. This was due to a number of reasons:

- Time factor to conduct the field trials. Driving would be exceptionally quicker than walking.
- MacBook issues of overheating. In a car the MacBook can be placed on the seat so it is able to operate without overheating or damaging it.
- The power of the MacBook AirPort wireless network adaptor would negate the adverse affects to signal strength in the car. For example, a car can act like a Ferriday cage to wireless signals which could have affected the results.

5.0 Field Trials & Findings

The final field trial was conducted on Wednesday the 27th of May 2009 from 13:05:58 to 13:51:30. During the 45 minute WarDrive of the Auckland CBD there were 3572 APs discovered. This was 15 times more data collected than in the previous study by Lin, in 2003, in which was 236 APs were gathered.

Figure 9 below shows a comparison of the two target survey areas. The map on the left shows the survey area tested by Lin for the WarDriving field runs. The map on the right shows the area I initially proposed to survey. At the time of writing my research proposal I was unaware of the specific area that Lin had included to survey in his study. Since that time I have now completely read his dissertation and learnt that the survey areas were very close, the only major difference being the exclusion/inclusion of the area between Customs St. West and Quay St. I therefore, determined to eliminate this from my final field trial area so as to bring the two survey areas into accord.

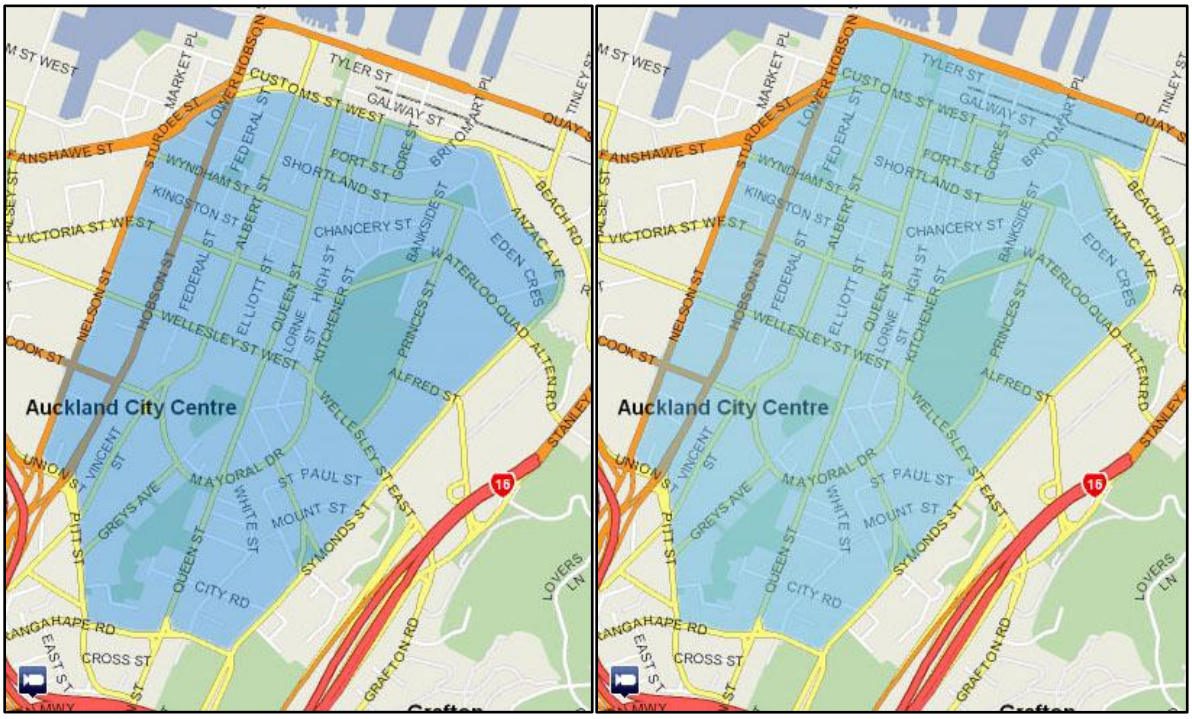

Figure 9: CBD Survey Area Comparison

Figure 10 below shows the actual route I travelled while conducting the field trial. I attempted to cover the whole area into a single Kismet output file and this was achieved by not stopping the application during the whole WarDrive. This was very important because, as I have previously outlined, the results of multiple Kismet files with such a large quantity of data are too hard to merge and compile.

Figure 10: CBD WarDrive Route

The data collected from the Kismet application during the final field trial was saved into a csv (comma-separated values) file. This file was then examined, filtered and aggregated into statistics using Microsoft Excel and a CSV file editor CSVed (CSVed, 2009). The original raw data from the field trial can be found in Appendix X, which is separated from this report.

The sections of data collected that was of importance to this study were:

- Encryption active
- Encryption type
- SSID Broadcast or Cloaked Networks
- SSID Naming Convention

Table 1 below shows the aggregated raw data collected during the field trials into categories based on the encryption implemented on the WLAN.

	Count	**Percentage**
No Encryption	1077	30.15%
WEP Encryption	697	19.51%
WPA Encryption	1798	50.34%
Total	3572	100%

Table 1: Aggregated Field Trial Results Based on Encryption Type

5.1 Comparison of Studies

Figures 11 and 12 below represent the field trial results (2009) and the field trial results of Lin (2003) respectively. The figures illustrate the comparison of encrypted and un-encrypted WLANs in Auckland CBD for the two separate studies.

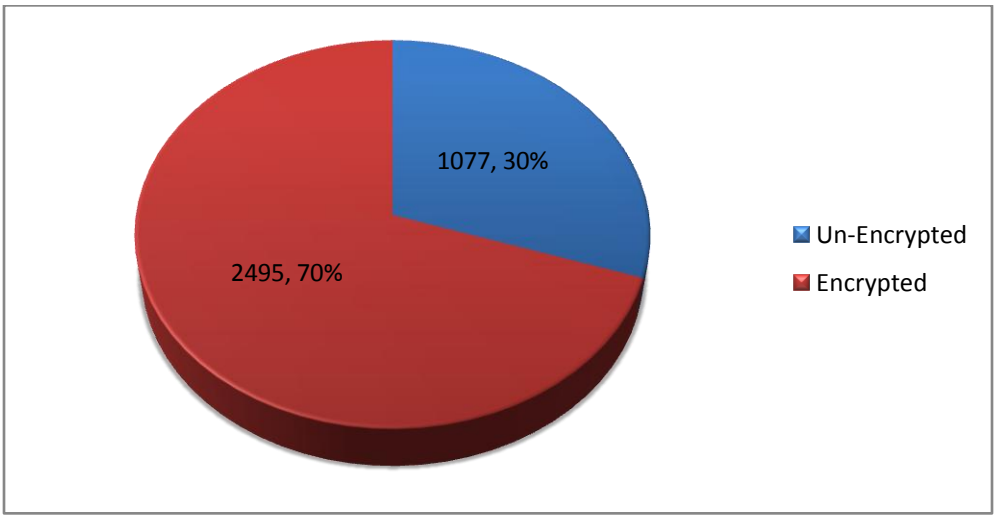

Figure 11: Field Trial Results (2009): Un-Encrypted vs. Encrypted

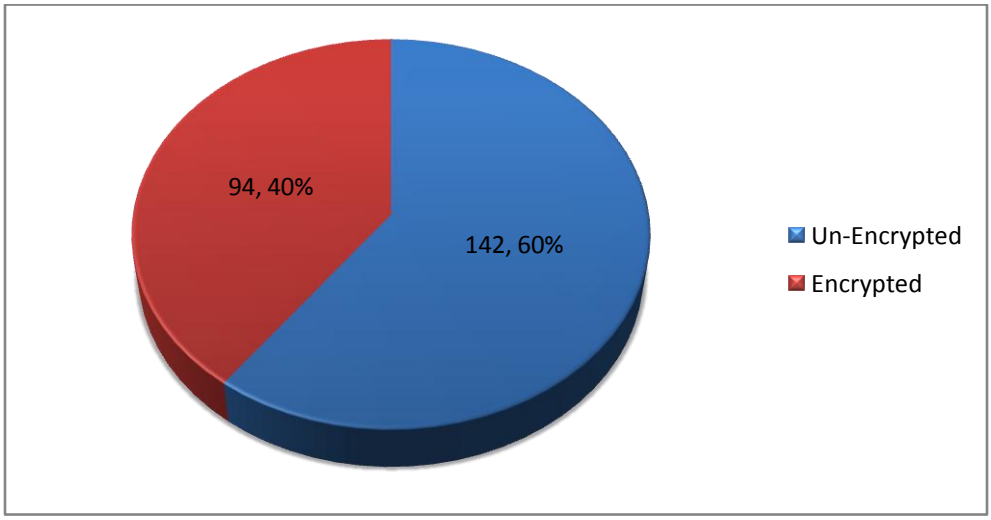

Figure 12: Lin (2003) Field Trial Results: Non-Encrypted vs. Encrypted

From my current field trial a total of 2,495 APs (say 70%) were found that have encryption implemented and 1077 APs (say 30%) that were not using any encryption at all. In comparison, the Lin (2003) results show a percentage of the encrypted APs at 39.8%, (say 40%) and un-encrypted APs at 60.2% (say 60%).

Therefore, in the 5 year time span since the Lin survey, the percentage of encrypted networks has increased from 39.8% to 69.85%. Even taking into account that Lin's data base of only 236 surveyed APs was used, the increase is significant.

Figure 13 further investigates the type of encryption used by APs in Auckland's CBD from my WarDrive field trial. The encrypted networks have been further separated into WEP or WPA categories.

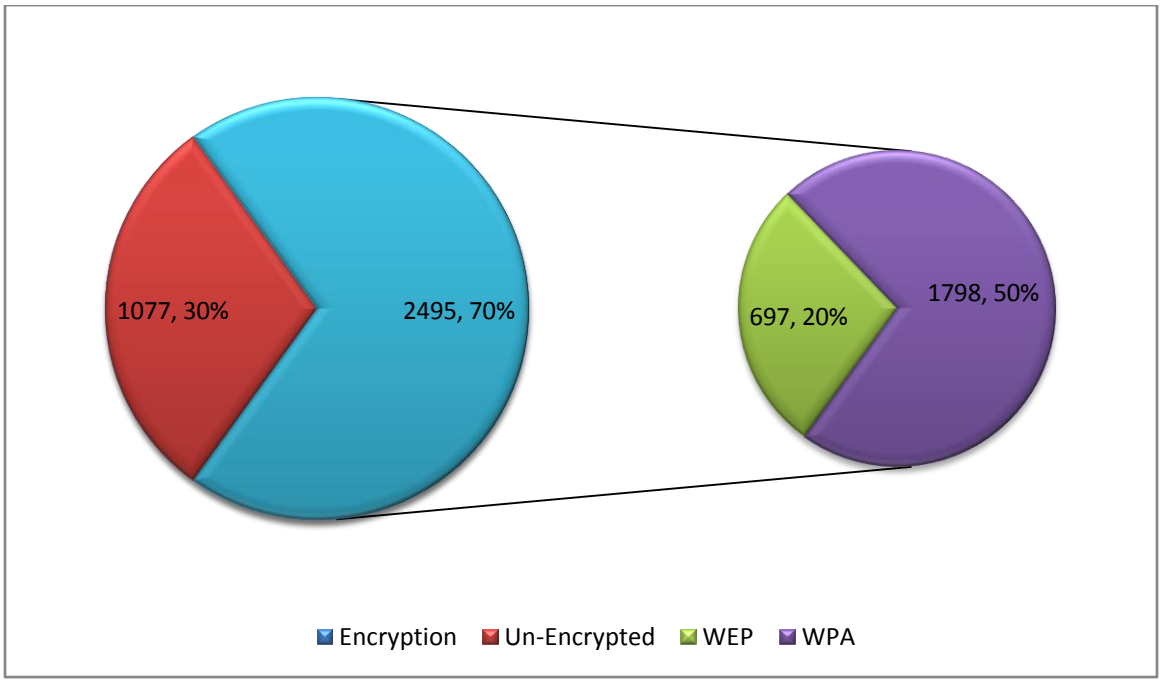

Figure 13: Field Trial Results: Encryption Types

The pie graph on the left shows the total number of networks divided into encrypted or not encrypted. The encrypted networks section is shown divided into which encryption has been implemented, which is seen in the pie graph on the right. This shows that 50% of all the networks surveyed have the stronger WPA encryption solution implemented, and 20% have the older and weaker WEP standard.

One of the most interesting results from the field trial results was the number of WLANs that had disabled the broadcast function of the SSID was extremely low. Table 2 below shows the count of cloaked SSIDs from the field trial was 26, which is 0.73%. Unfortunately there was no data available from the Lin (2003) Field Trial for comparison.

Network Type	**Count**	**Percentage**
Cloaked SSID	26	0.73%
Normal SSID Broadcast	3546	99.27%
Total	3572	100%

Table 2: SSID Properties: Cloaked vs. Normal

6.0 Analysis and Discussion

The most important factor regarding answering my research question was the data for comparison from the previous WarDriving study of Auckland CBD by Lin (2003). As stated there was a huge climb in the number of WLANs discovered between this field trial and the Lin (2003) field trial. This field trial collected 3572 APs and Lin (2003) study collected 236 APs.

There are a number of reasons for this dramatic change in numbers of target data collected:

- The popularity of wireless networking has dramatically increased for both home and business users. The cost has also decreased for wireless networking equipment. Both of these have hugely increased the presence of WLANs.
- The power of signal strength has increased dramatically, from new standards allowing higher and longer signal range and the increase in the power and strength of wireless adaptors in personal computers. This means wireless networks have greater range then before, thus they can be more easily discovered from outside of the location.

However, this could also be a result of a poor methodology chosen by Lin (2003) when conducting his field trials. For example, because of the following limitations restricted on his study:

- Only IEEE 802.11b-based WLANs were scanned.
- Using an external high-gain omni-directional antenna mounted on the roof of the vehicle instead of a built-in one to extend the scanning range.

The wireless network adaptor used by Lin (2003) was an Orinoco Gold PCMCIA card. This card has the ability to scan both 802.11b/g networks, so I am unsure why he outlines that only 802.11b networks were scanned. I thought that the ability to only scan 802.11b networks would have decreased results as 802.11g is the most popular standard used by most APs.

The limitation of not using an omni-directional antenna would have definitely decreased the numbers of WLANs discovered by Lin (2003). Figure 5, of Section 4.3, has already displayed the huge benefit of using an omni-directional antenna to gain extra signal strength. With more signal strength, more networks would have been discovered.

It should also be noted that encryption method and non-broadcasting SSID are not the only security methods that can be implemented on 802.11 WLANs. Some WLANs found during the study to have no encryption active may still have other security methods implemented to stop unauthorised users connecting to the network. For example, these networks could have Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) implemented. These solutions provide a centralised authorisation and authentication management for clients who connect to the network. In such a system, users would connect to the WLAN and be prompted to enter user credentials (username and password) to gain access to the network.

These security methods are unable to be evaluated in this study, because it would require connection and examination of the network which has been already deemed as an illegal procedure. However, based on the naming convention of SSIDs used in some WLANs it is possible to isolate some of the networks that are using these procedures of centralised administration based on personal knowledge. For example, it is known that AUT and UOA (University of Auckland) both have a centralised authentication system for their networks that are un-encrypted. These WLANs are provided as 'campus hotspots' for university students to use and require credentials to log onto the network.

Further analysis of the WLANs that were un-encrypted revealed that there were 23 APs from AUT (SSID name AUT-Unisurf-City) and 167 APs from UOA (SSID names 'UOA' and 'UOA-Guest') were found. Out of the total 1077 un-encrypted networks found the above university networks compile to 17.6%. This shows that even though a WLAN is un-encrypted, there is still security precautions implemented.

As previously stated the number of cloaked networks was extremely low, with a total percentage of 0.73%. Cloaked networks remove the SSID ability to broadcast itself, which contains the name of the AP that provides the radio signal to connect to the network. SSID's are basically used by humans to identify a network during the connection phase. Disabling the SSID broadcast means that a network cannot be connected to, as it does not appear in the list of available networks in a wireless client. Therefore the user needs to know the exact name of the SSID in order to connect to it. The removal of this feature can cause issues with availability and functionality of the WLAN.

I consider this one of the best and least implemented security feature of the 802.11 standard. This is because very few wireless network scanners are able to discover cloaked networks, Kismet is one of the very few. Cloaked networks would not be visible to users connecting from a personal computer using their wireless client manager (usually a built-in feature).

From the results obtained and analysed it can be concluded that security is a layered approach rather than a piece of software or a single configuration.

7.0 Limitations of Study, Future Work and Insights

7.1 Limitations

There were several limitations to this study. The predominant limitation was that of time. The report entailed that 60 hours were to be spent for the complete assignment, including writing it up. It is estimated that I used rather more than the allocated time, up to approximately 80 hours.

Without the limitation of time the data gathered would have been more complete with the whole survey area tested. The final field trial did not cover the whole area that was at first proposed.

Additionally, more time was needed to investigate, analyse and record the collected data. The grouping of SSIDs into groups based on their identifiability could not be achieved as the 3572 networks found would need to be sorted singularly. This is extremely time consuming as several statistics for each network need to be examined.

Another limitation to this study was the availability and cost of hardware. During my attempts to compile a testing machine I bought various wireless adaptors and accessories. Both the availability for these hardware pieces (due to the age, not available at retail shops) and the costs involved (compared to my very small student allowance) restricted the choices of how to conduct the field tests.

Item	Cost	Use?
Buffalo PCMCIA Card	$35	Was not used as switched to MacBook with internal AirPort, because it only supported 802.11b
iPaq 3975	$50	Not used as encountered too many issues
iPaq PCMCIA Expansion Pack	$40	Bought off TradeMe, received broken, main reason I ceased iPaq attempt
Orinoco Gold PCMCIA	$25	Still waiting for TradeMe member to post it !!!!
Laptop Battery for Toshiba 1800	$80	Did not end up using for Field Trial

The chart above shows a list of the items purchased and their respective cost.

Although the final laptop configuration provided an excellent testing machine; there are definitely other advantageous additions that could have been made. For example, a USB wireless network adaptor would have been the best network adaptor for the field trials. This is because the adaptor can be plugged into an extension cord and fastened to the outside of the car used in the survey. However, with the time factor and my financial limitations exceeded this was not feasible.

7.2 Possible future work

There were a number of thoughts and ideas regarding this study that I discovered through the process of writing a proposal and conducting the field trials.

A comparative study of how Auckland businesses in the CBD secure their WLANs, gathering data from the respective businesses in the form of questionnaires could possibly make a good thesis topic. This study would certainly need ethics approval, but some interesting insight could be gained. For example, security precautions taken that are not revealed by this study such as un-encrypted networks that use another form of post-connection authentication. However, it may be difficult to gather this sort of data as it is usually protected information that businesses do not like to expose.

This study could also benefit from a further investigation at another 5 year interval. I believe that the large quantity of data I have gathered could provide a solid base for comparison in a future study.

7.3 Personal Insights

The amount I have learnt from conducting this research was astronomical, from the process of planning the research in the report proposal to attempting to gather data and formulate a result and finally write a report.

One of the major learning curves that I confronted was that when designing a proposed method to gather data one needs to expect issues and problems that will undoubtedly arise from the proposal stage. I ran into issues at almost every stage of the research implementation including hardware problems, software platform and configuration issues and ethical issues on whether to even conduct the research method. This emphasises the reasons to start planning and testing early to allow for the myriad of problems that may be encountered.

The ability to document clearly at all steps has also, once again, proven to be an essential element to research and gather data effectively. Although I have become better at documenting throughout my studies I have once again learnt that it is exceptionally important. I was very keen to be able to gather the data needed to provide a clear and logical answer to the research question I proposed to answer. However, there were parts of my research design and evaluation that I neglected to document and save which hindered the final report. For example, I did not save any kismet output files from the HAN testing and Experimental Field Trials sections.

At the outset of the research proposal I thought that my personal knowledge and experience with wireless networks was quite high, considering it as one of my speciality topics within my information systems skill set. But, I have since learnt a great deal about evaluating wireless networks, their security features and the 802.11 standard in general.

I have also been motivated to start developing tools such as Kismet and NetStumbler. They completely rely on public contribution and many of these programmes are beginning to fade away, and are subsequently not updated. For example, the latest release of NetStumbler version 0.4.0 was April, 2004. Revolutions in the 802.11 standard, introducing 802.11n will further change the operation of wireless networking and could impact the functionality of these programmes.

Another motivation gained from this study was to provide documentation back to the community. I am currently working on a Kismet multi-platform tutorial and FAQ of combined information from the developer, other community information available and the information I have gained from conducting this study.

8.0 Conclusion

This report has proposed and conducted WarDriving field trials of Auckland's CBD in order to evaluate the security of WLANs. The data has been collected and analysed producing aggregated statistics which were then compared to a previous study conducted by Lin, 2003.

So, has the security of wireless networks improved in Auckland's CBD in the past 5 years?

It can be concluded that the security of wireless networks has, indeed, improved over the last 5 years. The two studies have illustrated that the percentage of encrypted networks has almost doubled during that time. However, the results also indicate that up to 30% of networks could still currently suffer from security issues.

Information security remains a primary concern in the Information Technology sector. This study further highlights the need to continually analyse and evaluate the systems that we have in place to assure security issues are addressed and mitigated.

9.0 References

AUT KB. (2009) AUT Ethics Knowledge Base. Retrieved May 23, 2009 from, http://www.intouch.aut.ac.nz/intouch/Ethics/knowledge_base/kb_sub.php?articleid=139&sectionid=84

AUTEC. (2008) Getting Ethics Approval. Retrieved May 23, 2009 from, http://www.intouch.aut.ac.nz/intouch/Ethics/knowledge_base/docs/Powerpoint/Getting%20Ethics%20Approval%202017122008.pps

CSVed. (2009) CSV file editor, Unicode compatible on Windows XP NT 2000. Retrieved May 29, 2009 from, http://www.csved.sjfrankle.nl/

DarwinPorts. (2009) The Original DarwinPorts: Open Source on Mac OS X. Retrieved May 27, 2009 from, http://www.darwinports.com/

Eidac. (2009) sncFanControl. Retrieved May 30, 2009 from, http://www.eidac.de/

Hoar, S. B. (2006): 802.11 – Wi-Fi Technology, Trends and Legal Issues. Retrieved April 17, 2009 from http://www.law.uoregon.edu

Kismet. (2009). *Kismet.* Retrieved May 26, 2009, from http://www.kismetwireless.net/

kismacng. (2009). *KisMAC-ng.* Retrieved June 2, 2009, from http://www.trac.kismac-ng.net/

Lin, C.-T., Sathu, H., & Joyce, D. (2004). Wireless network security, *Proceedings of the Seventeenth Annual Conference of the National Advisory Committee on Computing Qualifications*. Pgs 337-340.

Lin, C-T. (2003) "IEEE 802.11b-based Wireless Network Security", *Master of Computing Dissertation*, Unitec New Zealand.

Milner, M., (2004). *NetStumbler ReadMe.* Retrieved April 27, 2009, from http://www.stumbler.net/readme/readme_0_4_0.html

Semaja. (2009). *Semaja2: InsomniaX.* Retrieved May 24, 2009, from http://www.semaja2.net/insomniaxinfo

XCode. (2009) Tools - XCode. Retrieved May 29, 2009 from, http://www.developer.apple.com/TOOLS/xcode/