1-1-2011

Wi-Fi security: wireless with confidence

Lucas Jacob
Deakin University

Damien Hutchinson
Deakin University

Jemal Abawajy
Deakin University

DOI: 10.4225/75/57a02b9aac5c8
4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

Wi-Fi SECURITY: WIRELESS WITH CONFIDENCE

Lucas Jacob, Damien Hutchinson, Jemal Abawajy
School of Information Technology, Deakin University
lajac@deakin.edu.au, drh@deakin.edu.au; jemal@deakin.edu.au

Abstract

Since the IEEE ratification of the 802.11 standard in 1999, continuous exploits have been discovered compromising the confidentiality, integrity and availability of 802.11 networks. This paper describes the justification for a project to assess the security status of wireless network usage in society. It reviews the status of both commercial and residential approaches to wireless network security in three major Victorian cities, Melbourne, Geelong and Mornington, in Australia. By War Driving these suburbs, actual data was gathered to indicate the security status of wireless networks and give a representation of modern attitudes towards wireless security for the sample population. Preliminary results are presented to demonstrate the extent to which commercial or residential suburbs address wireless security. At this stage in the research further work is required to completely analyse the results. It is anticipated that the results will be useful for providing input into a defence and attack methodology for improving the security of both residential and commercial use of wireless networks.

Keywords

War Driving; Wireless Security; 802.11 Security Protocols

INTRODUCTION

War Driving, the reconnaissance stage of any wireless network attack was invented by Peter Shipley in 1999 who first introduced his experiment "to the hacker community at DEFCON 9 in 2001" {Berghel, 2004 #35}. It involves "geographically locating and mapping wireless hot spots and their security types from a moving vehicle" {Cache, 2010 #32}. From here malicious users such as hackers and cyber criminals can target and break into vulnerable APs (Access Points).

Since 1999, the popularity of 802.11 networks has grown exponentially. Due to their flexibility, mobility, and scalability, wireless networks have been adapted in commercial, educational and household establishments, entrenching their use into everyday life. Yet introduction of wireless networks has opened several security flaws in many 802.11 security protocols. This poses a serious threat to both residential and commercial network owners as everyone that owns or manages a wireless network is vulnerable to both War Driving and wireless network attacks. However War Driving can also be used as a benevolent tool. By using War Driving to assess the security status of wireless networks within a specific geographical area, information can be gathered to determine the current security situation of that area.

The need for this research is apparent for three particular reasons. First there is limited evidence of this type of research having been performed and published in Australia. Second this area of research has not been progressively updated. The data previously collected by other researchers is out of date especially due to the continuous development of new attacks. Third this area of research needs to be updated to reflect the modern user approaches and trends in wireless network security.

This research concentrates on assessing and comparing wireless security through War Driving. In order to quantify the issue research was conducted in three main cities of Victoria, (Melbourne, Geelong and Mornington) taking into account both their commercial and residential demographics. The aim is to determine the degree to which users enforce wireless security. From this information implications for use will be discussed on a residential or commercial level, a geographic level or a socioeconomic level.

The next phase is to conduct a formal analysis on the data collected giving insight and justification as to why security is not enforced. A formal wireless network attack and defence methodology will also be included as a stage for further work.

The paper is organised as follows. The 'Background' presents an overview of War Driving and the major attacks against wireless networks are presented. The 'Evaluation Procedure,' describes the hardware, software and methods used to conduct the study in Melbourne, Geelong and Mornington. The 'Preliminary Results,'

section provides a preliminary review of the data collected. 'Future Work,' outlines what will be presented when further analysis is conducted.

BACKGROUND

In recent years several papers have been published including "Wireless Security in UAE: A Survey Paper" {Aloul, 2010 #1}, "Hack Boston: Monitoring Wireless Security Awareness in an Urban Setting" {Matthew, 2006 #6} and "The Art Of War Driving and Security Threats- A Malaysian Case Study" {Issac, 2005 #2}. In each case, the researchers attempt to determine the amount of vulnerable networks in specific geographic areas and to establish whether War Driving is a successful approach for network reconnaissance. Researchers have tried to quantify their research by reviewing different geographical areas, different community types and even conduct research over different periods of time.

War Driving

Defined as "the act of moving around a specific area and mapping the population of wireless access points for statistical purposes" {Hurley, 2004 #52} , War Driving involves utilising special hardware and software to map the approximate location of discovered wireless APs within a specific geographic area.

While War Driving can be perceived as a method for exploit, it can also be perceived as a recreational activity. Several websites host competitions as to how many Wi-Fi hotspots can be successfully mapped and tallied {arkasha, 2001 #45}, and "statistics are used to raise awareness" {Hurley, 2004 #52}.

War Driving is not illegal; however it does reside within a legislative grey area. Legislation, specifically the *Cybercrime Act 2001 (cwlth)* and the *Criminal Code Act 1995 (cwlth)* mandate a computer offence as an act that "impairs the security, integrity and reliability of computer data and electronic communications" (Cybercrime, 2001; Criminal Code, 1995) This can apply as equipment used has the ability to impair and modify electronic communications, as hardware is continuously scanning for AP broadcast signals. However every time a legitimate client attempts to connect or find a wireless network, they are essentially committing the same crime. 802.11 also is broadcast on an open medium similar to that of television or radio, anyone with the right hardware simply needs to tune into a specific frequency.

From an industry perspective, War Driving is a method used in security practice during the reconnaissance stage of a penetration test. The reconnaissance stage is used to determine the business information assets of an organisation and gather as much data about these assets as possible. From here a penetration tester or even a malicious attacker would use the information discovered in the War Drive to break into the network.

As War Driving involves "covering terrain in search of wireless networks," {Matthew, 2006 #6} many methods of collecting data exist. Primarily wireless networks are found by driving a car, where a laptop is equipped with a wireless transmitter and a GPS for logging of geographic data (War Driving). However this also extended to other methods such as walking (War Walking), which is where an individual would use a mobile device such as a smart phone and physically walk or run, cycling (War Cycling) where an individual would use a mobile device but be riding a bicycle and even flying (War Flying) where an individual would use flying drone mounted with scanning equipment.

From a malicious attacker's perspective, a wireless attack can pose a major threat to corporate environments, especially where a compromise of network assets can affect the continuity of business operations. Once a malicious attacker has penetrated a wireless network, he generally has access to LAN (Local Area Network) resources including end devices, computers, servers and other network hardware. Specific threats that can arise from War Driving include "viruses spreading throughout the network, anonymous mass-mailing of unsolicited e-mail (spam) and illegal access to remote systems" {Matthew, 2006 #6}. A plethora of other threats could be exploited ranging from low lever ARP poisoning attacks, to high level remote exploits.

Even though War Driving has developed vastly since its introduction and the use of wireless networks usage is growing exponentially, there has been little research published and even less completed recently. Several researchers have presented different methods for analysis of specific geographical areas in various countries using different methods to gather War Driving data.

One case presents the issue of Wireless security in Malaysia through War Driving. Conducted in 2005 the authors aim to assess the physical "fuzzy boundaries," {Issac, 2005 #2} of wireless networks. Yet their research only covers an analysis of wireless networks on "some of the highways," {Issac, 2005 #2} in Malaysia. By shortening their War Driving scope to only main highways, the researchers reduce the ability to capture a holistic amount of data which reduces their ability to make specific conclusions about their research. While driving to

"different places, at different times," {Issac, 2005 #2} enabled the researchers to gather data from a variety of different environments, their research lacks structure to make any definitive conclusions about all of the wireless networks in a specific geographic area.

Another case presents the issue of wireless network growth and security awareness over two years, 2004 and 2005 and aims to "promote security awareness among wireless users" {Matthew, 2006 #6}. The researchers defined a geographical scope to collect information "regarding access points in a one mile radius of the Northeastern University campus," {Matthew, 2006 #6} in Boston Massachusetts, USA. The primary methods of information gathering used were "War Driving," and "War Walking" to access areas where cars were not able to reach; "to cover each area, cars were used with external antennas as well as walking down streets and through alleys" {Matthew, 2006 #6}.

By logging the data over a two year period the researchers were able to speculate on user attitudes towards security and highlight the growth of APs that were encrypted with WEP and those that were not. The outcomes indicated that "The number of APs versus the unprotected ones almost reversed over the two years. In 2004, 58% of the APs were not encrypted, while in 2005, 60% of them were" {Matthew, 2006 #6}.

However this research is limited to only WEP encrypted devices, WPA was released in 2003 {IEEE-SA, 2007 #37} and WPA2 was released in 2004 {IEEE-SA, 2007 #37}. Considering the experiment was conducted in 2004 and 2005 respectively, it would have been more significant for the researchers to incorporate WPA and WPA2 into the scope of their research.

A recent study conducted in 2010 presented a comparative analysis of two cities in the United Arab Emirates. The "Sheikh Zayad road and Internet City in Dubai and the Buhaira area in Sharjah" {Aloul, 2010 #1} were the two cities analysed and are commercial and residential cities respectively. By completing a comparative analysis of the two cities the researchers aimed to show whether residential or commercial suburbs implemented appropriate wireless security practices. This was achieved through War Driving and reviewing which of the cities enforced encryption and which of the cities enforced changing the default SSID of the router. The authors concluded that "security awareness among the public is higher in Dubai (a commercial suburb) than Sharjah (a residential suburb)" {Aloul, 2010 #1}. Kalbasie et al, justify their results as Dubai is a commercial suburb and that the "larger number of business offices and hotels are more concerned with wireless security" {Aloul, 2010 #1}.

However this paper only focuses on WEP as the security control and not on others such as WPA or WPA2. By restricting the scope of the research to only WEP encrypted networks, the research and what is considered as secure network practices is limited since WEP was found to be broken in 2001 and continued to be inadequate for providing secure communication of wireless networks, as evidenced by the attacks presented in the next section. Networks that enforce WEP as a security control are in fact not secure from malicious attacks and enabling WEP would only serve as a minor deterrent.

The extent to which wireless network analysis has been conducted in Australia is very limited. One study {Yek, 2006 #69}presents findings of a 2 year assessment of Western Australia's' capital city Perth (Yek, 2006). By canvassing "approximately 26 kms around Perth CBD (Central Business District) and several adjacent commercial areas," Yek aimed to identify as many wireless networks utilising 802.11 b and 802.11 g frequencies and conclude if the security status of Perth had improve over 24 months. Yek received both a positive increase in networks detected and those that had implemented secure practices. However Yeks' research only includes networks secured with WEP and that hide their BSSID. This research is also restrictive as no specific geographical boundaries are adhered to and several other suburbs are canvassed. While Yek did receive an increase in data collected this could be due to driving different streets on different occasions as no specific war map is detailed in his research.

Previous Wireless Network Attacks

Several cases of wireless attacks have been documented and demonstrated to show the insecurities in all three protocols. For WEP this has been evidenced by {Fluhrer, 2001 #14}, {Martin Beck, 2008 #16}, {KoreK, 2004 #17} and {Tews, 2007 #26}. For WPA by {Martin Beck, 2008 #16}, {Morii, 2009 #56}, and {Halvorsen, 2009 #39}. For WPA2 by {Ahmad, 2010 #49}. It should be noted a plethora of other attacks exist for wireless networks. These include DoS (Denial of Service) attacks, signal jamming and masquerading attacks such as rouge APs'. These attacks are considered out of scope for this paper as they affect all networks types regardless of encryption or authentication method.

PROCEDURE FOR EVALUATING WIRELESS SECURITY APS

In order to perform an accurate assessment between rural, suburban and urban environments, three main cities were used to compare both residential and commercial wireless security. These residential and commercial zones are attained from the council zoning rules and the geographic scope is restricted to that of the postcode. For this experiment the cities Melbourne, Geelong and Mornington were used. With respect to Melbourne the commercial zone is restricted to the CBD and the residential zone is restricted to suburb of Carlton. Geelong's commercial zone also consists of its CBD and its residential zone is restricted to the suburb of Whittington. Mornington does not have a CBD specifically but it does consist of several Business and Commercial zones, these zones characterise the commercial environment while the rest of the residential zones entail the residential environment. In order to ensure consistency all roads within the specific War Maps will be driven. Due to ethical restrictions specific GPS locations cannot be logged when War Driving. The following hardware will be used:

- Dell Inspiron 15r running Windows 7 (64bit)
- Alfa AWUSO36NHR 2000mW wireless adapter
- 9dBi Omni Directional Antenna
- Alfa 7dBi Directional Antenna

In order to conduct the War Drive specialised software must be used that will continuously scan and log all access points within range of the Wi-Fi receiver. For this experiment Vistumbler v10 will be used {Vistumbler, 2010 #57}. Vistumbler is a well known open source program for War Driving in Windows Vista and Windows 7 that records detailed information from APs scanned and enables various forms of data output. Combining these three factors determined Vistumbler as the most suitable program for undertaking the War Driving activity.

All roads within the War Map are scanned using the 9dBi Omni directional antenna to pick up as many access points as possible in a 360 degree radius of the car. When War Driving the perimeter of the War Map, a 7dBi Directional antenna was used to ensure only access points within the Map were canvassed.

Based on the literature and the exploits outlined previously, the various security protocols (and associated controls) displayed in table 1 were defined as the benchmark for measuring the degree of secure wireless network practices implemented for each wireless AP. A wireless network was considered secure if it is using WPA2 with 802.1x for authentication and CCMP-AES for encryption.

Table 1. 802.11 Security Protocols required for a secure wireless network

802.11 Security Protocol	**Security Level**
WEP	Not secure
WPA (PSK)	
TKIP	Not Secure
CCMP-AES	Not Secure
WPA (802.1x)	
TKIP	Not Secure
CCMP-AES	Not Secure
WPA2 (PSK)	
TKIP	Not Secure
CCMP-AES	Not Secure
WPA2 (802.1x)	
TKIP	Secure (not preferable)

CCMP-AES	Secure (preferable)

PERLIMINARY RESULTS

Figure 1 through to figure 6 represent preliminary results based on data gathered from all of the locations (Melbourne, Geelong and Mornington) and show a brief comparison of the existing secure wireless networks.

Commercial:

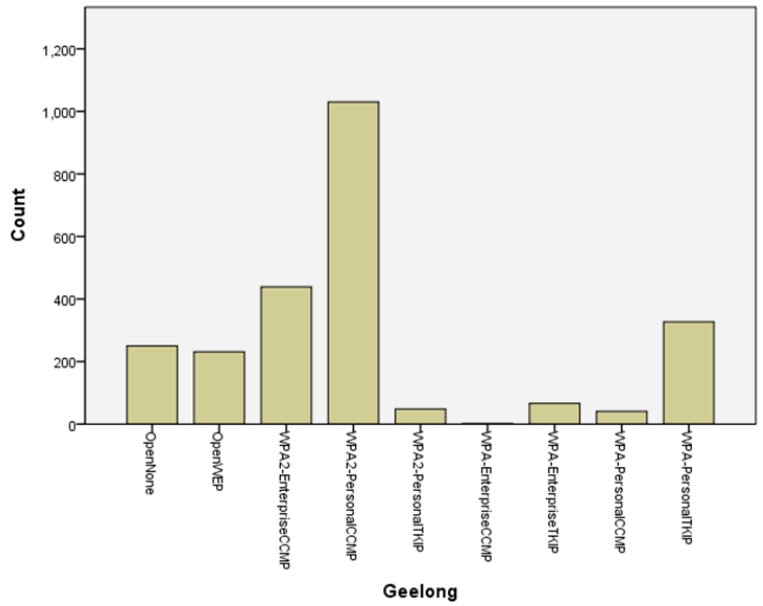

Figure 1. Data gathered from war driving every street in Geelong (CBD)

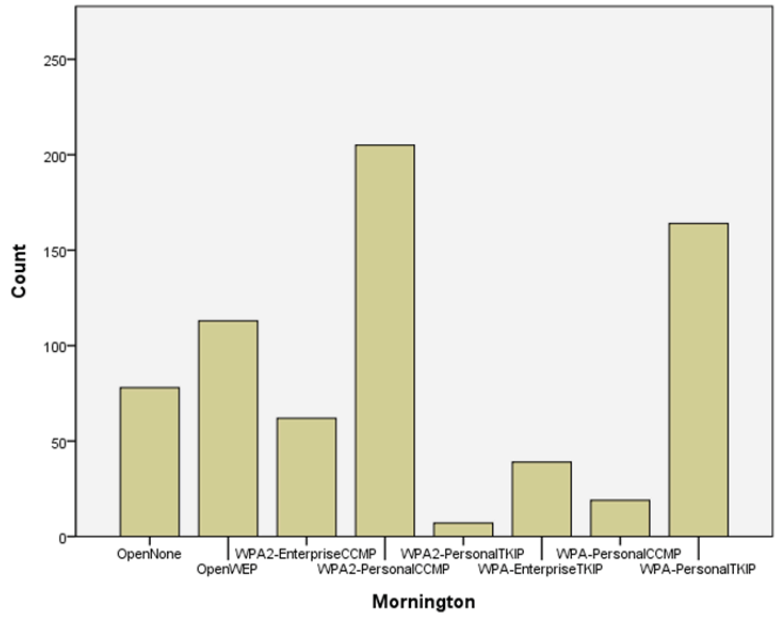

Figure 2. Data gathered from war driving every street in Mornington (Industrial Zone)

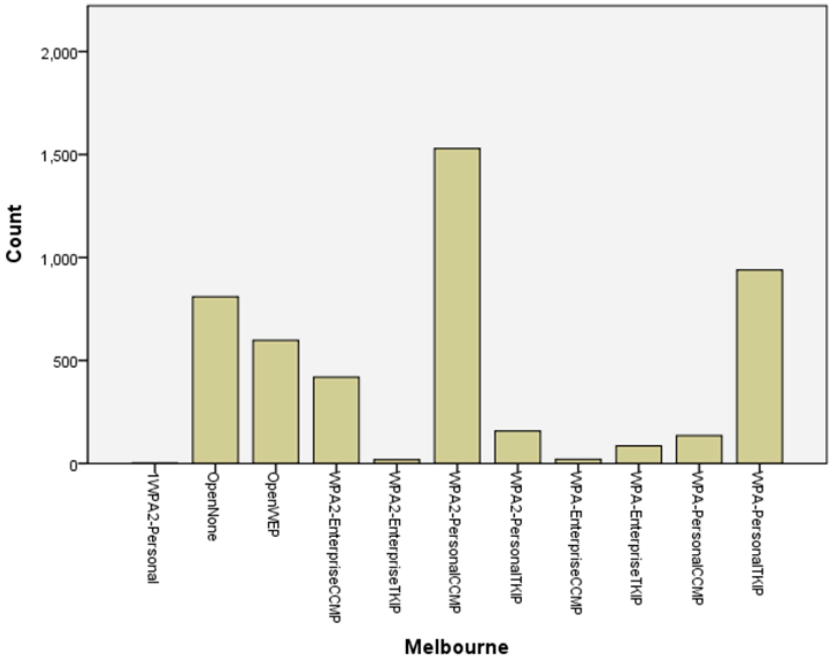

Figure 3. Data gathered from war driving every street in Melbourne (CBD)

Residential:

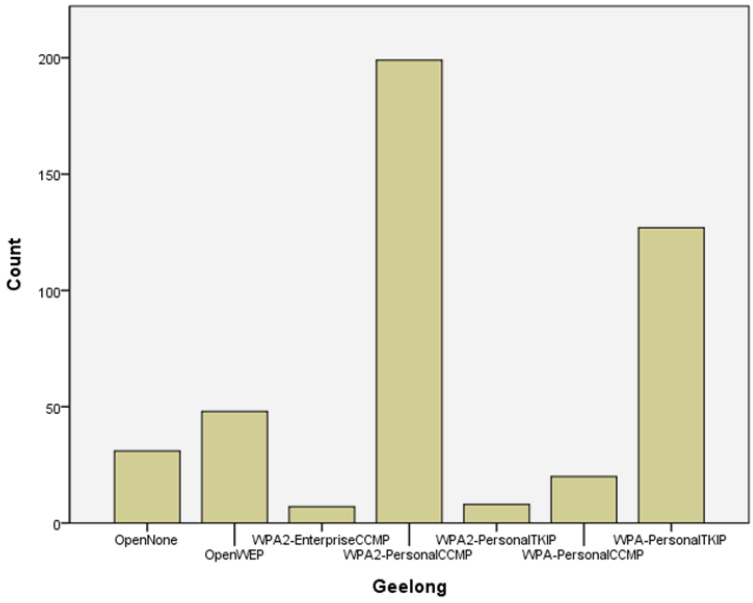

Figure 4. Data gathered from war driving every street in Whittington

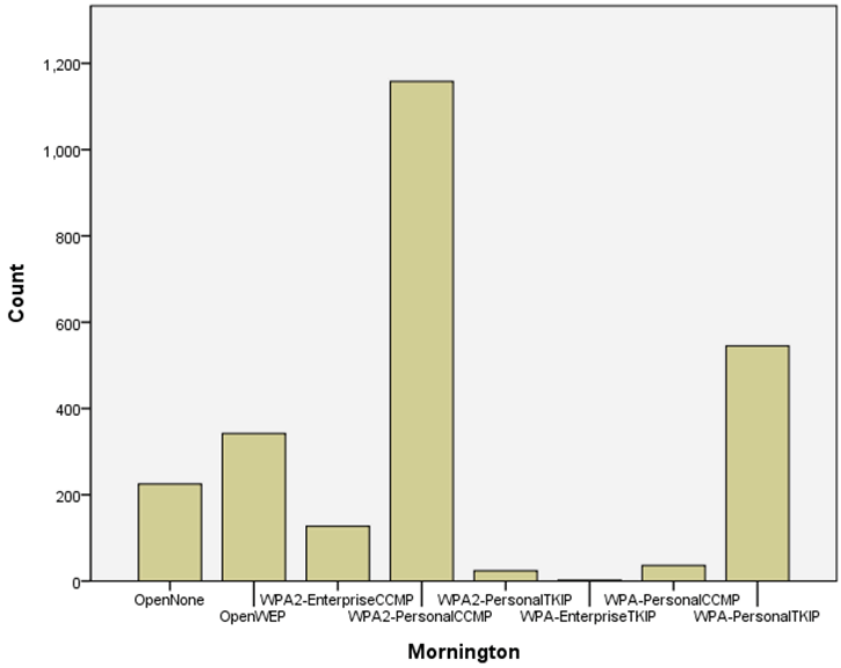

Figure 5. Data gathered from war driving every street in Mornington (Residential Zones)

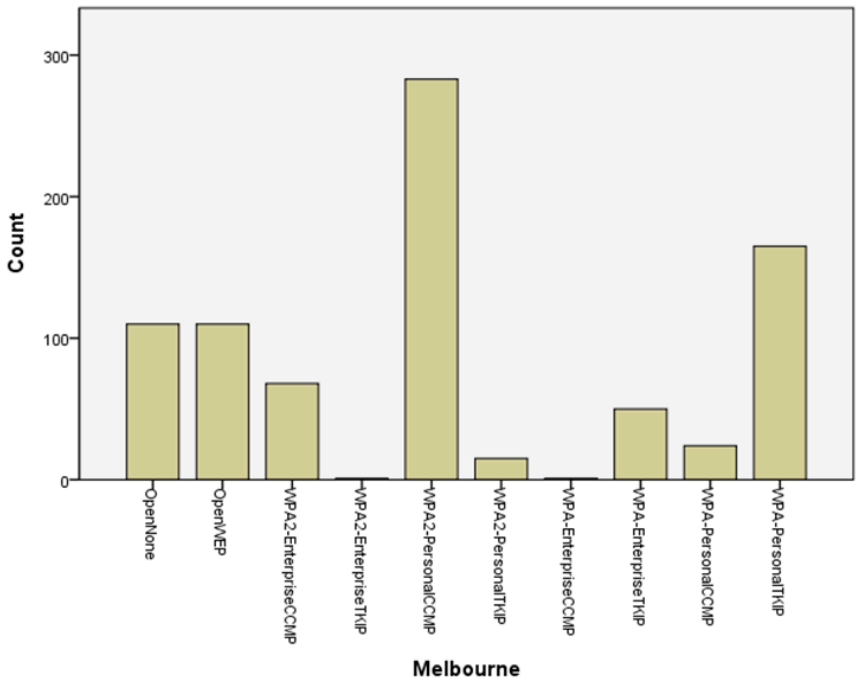

Figure 6. Data gathered from war driving every street in Carlton

Based on the data gathered it was shown that wireless security is enforced more in commercial environments rather residential environments. At the same time Melbourne also had the highest amount of open networks without encryption enabled. However many businesses such as Mc Donald's, Starbucks and various other organisations provide free internet access for customers on a restricted and controlled network. Therefore not all networks would be classified as completely insecure.

FUTURE WORK

Future work will include an in depth analysis of the results collected. From these results the research should highlight where good Wireless Security standards are enforced in Victoria and where they are not. Furthermore the results should underline if security is upheld more in commercial or residential zoned areas and overall if Melbourne, Geelong or Mornington impose wireless security the most.

A defence and attack methodology will also be developed to demonstrate processes to secure Wireless Networks. This methodology will outline current attacks and how to secure a wireless network to deter them. An attack methodology will also be included to highlight how these attacks manifest and how to execute them on a vulnerable wireless network. This will serve as an exercise in awareness for users to appropriately test and secure their wireless networks.

CONCLUSION

While Wireless networks have enabled a greater amount of accessibility to end users, they have also opened many security flaws for potential hackers and cyber criminals. If addressed properly networking wirelessly can be secure, however this study confirms the need for security to be addressed. While security trends have risen over the years, so have the amount of threats available for exploitation. This study has extended on previous work where limitations were found in the approach to discover wireless networks using disparate demographics and outdated insecure protocols. Initial findings indicate that wireless security is still a serious issue in society today irrespective of residential or commercial networks. Our contribution has been to explore whether security is enforced more in residential or commercial suburbs. Further analysis and evaluation of the results from this experiment is required to deliberate on the outcome of this premise.

REFERENCES

Ahmad, M. S. (2010). WPA Too!

Aloul, F. A. (2010, 8-11 Nov. 2010). *Information security awareness in UAE: A survey paper.* Paper presented at the Internet Technology and Secured Transactions (ICITST), 2010 International Conference for.

arkasha, & bobzilla. (2001). wigle.net Retrieved 5/08, 2011, from http://wigle.net/

Berghel, H. (2004). Wireless Infidelity I: War Driving. *Communications of the ACM on Digital Village*, 21-27.

Cache, J., Wright, J., & Liu, V. (2010). *Hacking Exposed Wireless: Wireless Security Secrets & Solutions, Second Edition* (2nd ed.): McGraw-Hill.

Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. In S. Vaudenay & A. Youssef (Eds.), *Selected Areas in Cryptography* (Vol. 2259, pp. 1-24): Springer Berlin / Heidelberg.

Halvorsen, F. M., & Haugen, O. (2009). *Cryptanalysis of IEEE 802.11i TKIP.* Master of Science in Communication Technology, Norwegian University of Science and Technology. Retrieved from http://wiki-files.aircrack-ng.org/doc/tkip_master.pdf

Hurley, C. (2004). *WarDriving : Drive, Detect, Defend: a Guide to Wireless Security*. Rockland, MA, USA Syngress Publishing

IEEE-SA. (2007). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *Communications Magazine*

Issac, B., Jacob, S. M., & Mohammed, L. A. (2005, 16-18 Nov. 2005). *The art of war driving and security threats - a Malaysian case study.* Paper presented at the Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on.

KoreK. (2004). Experimental WEP attacks Retrieved 22/06, 2011, from http://www.netstumbler.org/unix-linux/chopchop-experimental-wep-attacks-t12489.html

Martin Beck, E. T. (2008). Practical Attacks against WEP and WPA. *http://dl.aircrack-ng.org/breakingwepandwpa.pdf.*

Matthew, B. K., Keith, D. B., & Stefano, B. (2006, May 2006). *Hack Boston: Monitoring Wireless Security Awareness in an Urban Setting.* Paper presented at the Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on.

Morii, T. O. a. M. (2009). A practical message falsification attack on WPA. *Cryptography and Information Security Conf. System Joint Workshop on Information Security*.

Tews, E., Weinmann, R.-P., & Pyshkin, A. (2007). Breaking 104 Bit WEP in Less Than 60 Seconds. In S. Kim, M. Yung & H.-W. Lee (Eds.), *Information Security Applications* (Vol. 4867, pp. 188-202): Springer Berlin / Heidelberg.

Vistumbler. (2010). Vistumbler Retrieved 2/05, 2011, from http://www.vistumbler.net/

Yek, S. (2006). Wily Attackers Seek Wireless Networks in Perth, Western Australia for Easy Targets *EC2ND 2005*, 125-136.