Home Wireless Network Security Risk Analysis

By

Daniel Scott Livingston, BSc

A dissertation submitted to the
School of Computing
in partial fulfilment of the requirements for the degree of

Bachelor of Science with Honours

University of Tasmania

November, 2007

I, Daniel Scott Livingston, assert that this thesis, submitted in partial fulfilment of the requirements of the degree of Bachelor of Computing with Honours, contains no material which has been accepted for the award of any other degree or diploma in any tertiary institution, and that to my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the text of the thesis.

Daniel Scott Livingston

7/11/2007

Abstract

It is becoming more and more common place to find wireless networks present in residential homes. This thesis investigates whether these networks are set up securely, if home users use the security features that are available and whether or not home users lack the knowledge to make the choices to make their networks secure.

The thesis examines the risks associated with leaving a wireless network open and investigates whether or not such networks are frequented by casual "moochers" who simply wish to connect to the internet through these open wireless networks or alternatively whether there are attackers about with a more malicious intent

To answers these questions four methods were used: wardriving to detect the number of open networks in the Sandy Bay residential area; honeypots to attempt to see what attacker/intruders do on an open network; a device critique to examine the security features that are available on home devices; and a survey of home users to find out how and if the devices could be improved.

The results from this study show that there are a significant number of networks at risk, but that the honeypot system was not intruded upon. The user survey shows some possible directions for improvements in future wireless access points from a home user's point of view.

Acknowledgments

I wish to thank all those who have enabled me to complete this thesis and to my supervisors Mrs Jacky Hartnett and Dr Daniel Rolf for providing me with the opportunity to cover this topic.

Special thanks go to my fiancée for putting up with being ignored at times whilst I was working on this thesis.

Thank you to those who participated in my survey giving me some results to talk about.

Also, thanks goes to my fellow honours students whose discussion helped solidify my ideas and provided a starting point for others.

Again thank you to all those who have contributed or aided me in some way.

Contents

List of Figures

List of Tables

1 Introduction

"Mathematics is logical; people are erratic, capricious, and barely comprehensible." (Schneier 2000) These are the exact same sentiments that many home users would attribute to their experiences when attempting to decipher home networking equipment and their security features which largely are based upon mathematics and logic.

In the modern world it is common place to find computer networks present in many homes. It is also becoming increasingly common for these networks to include some form of wireless access. This wireless access if not secured can be accessed by others than those for which the service is intended. When this activity is constrained to simply gaining access to Internet services it has been termed wireless "mooching" or "piggybacking". Recently in the united kingdom ('Cautions for broadband 'theft" 2007) and Singapore ('Singapore leads in crackdown on Wi-Fi moochers' 2007) people have been charged with the theft of services because they conducted this activity.

The securing of these wireless networks could have prevented the unauthorised access to the wireless networks and the services they were connected to. Even the use of the wired equivalent privacy (WEP) scheme which has been shown to be insecure (Hytnen & Garcia 2006) but was part of the original IEEE 802.11 standard (1999, pp. 6,59-64), would stop the casual "moocher" from gaining access to the network. While use of the newer Wi-Fi protected access schemes (WPA or WPA2) when used correctly can (with current known vulnerability's) render the network secure from all but the most dedicated attacker (Hytnen & Garcia 2006).

The challenge that presents itself is that many wireless networks are left in an insecure state, which leaves them open to unauthorised access. What barriers exist that prevent users from using the security features provided on their wireless access points which would minimise the risk presented by their installation? Can users of limited technical knowledge be presented with technical information that is contained within the access point logs to enable them to identify if any unknown users have been present on their network?

2 Background Information

2.1 Home Networks

For many home network users the network is simply something that provides them with a service and is not something they think about often as it has become ubiquitous with their environment. In a paper presented to the 2007 conference on human factors in computing, Shehan and Edwards (2007) discuss the fact that a computer network is an infrastructure technology and for a pure end user (as home users generally are) of this infrastructure technology they are not aware or simply do not care how the network is operated and configured. They simply see the end functionality that lets them achieve their goals such as conducting email transactions or web browsing.

However as soon as this network infrastructure or an underlying component of it malfunctions, a new device is added or a configuration is changed it is suddenly thrust into the user's awareness and they often lack the skills to make the best choices when presented with options. Nevertheless there are conflicting goals concerning ease of use for the user and the best setup. Whereas the home user may simply want something to work "out of the box", this is often achieved through the sacrifice of more advanced configuration which would give security improvements.

2.1.1 Wireless Home Networks

Wireless networks facilitate the ubiquity of computer networks in the home. Users are not tethered by the location and length of wires. A wireless access point can be installed in most homes with little thought and reception can be achieved throughout the house and beyond.

As stated previously, home users will more often than not want something to work with minimal configuration "out of the box". The non-technical weaknesses of home wireless networking devices are illustrated by the fact that in the United States around a quarter of consumer wireless access points were returned according to Laszlo (2002). Of these returned devices a large portion of the reasons given for return were due to the failing of user expectation or an inability to successfully

configure the device. A study by Laszlo (2002) rank technical complexity of home networking devices as the largest single barrier to the success of home networking.

2.1.2 Wireless Home Networks – Software Aides

Wireless networks in conjunction with an automated configuration technology such as dynamic host configuration protocol (DHCP) enable in most cases a new device to be added and configured to full functionality in the network by simply turning it on and selecting the appropriate wireless network from the list of detected networks and providing the network key if one is required. It is this kind of simplicity that users of a home wireless network like which was identified during the research conducted for the design of Linksys's "EasyLink Advisor" software (Elmore, Hamilton & Ivaturi 2007). This preference for simplicity also extends to the administrators of these home networks, who in a large number of cases have very little networking knowledge. This will often lead to a number of the configuration settings not being configured to their optimal values for the given deployment scenario. The most concerning of these is when wireless security has been left disabled.

The challenge faced by Elmore, Hamilton and Ivaturi in designing their advisory software package (EasyLink Advisor) was to create a product that achieved the best possible device configuration for the user, whilst providing a configuration procedure with supporting information sufficient to guide the user to make the best choices regarding their given setup requirements. This was achieved through contextual help which was tailored to the degree of experience that the administrator believed they possessed. Experience levels of the users and their goals for a level of understanding were categorised into four different groups within "EasyLink advisor". These ranged from an expert, someone who considers themselves to already understands all the concepts employed on the configurable device down to those who simply "just want stuff to work" and have no desire to understand how their requirements are being achieved just simply that they are (Elmore, Hamilton & Ivaturi 2007, p. 1737).

2.2 Wireless Security

Wireless security can be defined as any measure that seeks to ensure the confidentiality of any data on the network, the integrity of the data on the network and the availability of the network resources to legitimate users of the network (Pfleeger & Pfleeger 2003, p. 11). For Australia "The Code of Practice for Information Security Management" (AS/NZS ISO/IEC 2006, pp. 77-81, 94) 17788 standard defines these three goals for general information systems and is inclusive of wireless networks. While this is intended for a commercial environment there is no reason a significant portion of the standard cannot apply to an ideal home wireless network

2.2.1 Security Goals

2.2.1.1 Confidentiality

Confidentiality means to limit the availability of information to those who are authorised to have access to it. This could also be interpreted as the desire for secrecy or privacy. Confidentiality in the context of networking is achieved through encryption (Pfleeger & Pfleeger 2003, p. 10). In regards to a wireless network this confidentiality protects the privacy of the information the user transmits on the network, this may include such things as banking details and passwords.

2.2.1.2 Integrity

The integrity of data in the context of wireless networking is that the information is as the authorised sender sent it. If an attacker is able to manipulate network communication the integrity of the communications channel is compromised (Stallings 2007, pp. 12-13).

This was originally addressed by the 802.11 design team by the inclusion of an integrity check value in the form of a cyclic redundancy checksum (CRC).

2.2.1.3 Availability

The goal of availability is to ensure network resources are available to legitimate users. A number of measure can be used to ensure no one single client on a wireless network receive service at the exclusion of others when the client is participating

normally. However in a wireless environment it is possible to flood the area with a high power jamming signal at the communications channel frequency that can disrupt communications

2.2.2 Protocols

A protocol is a set of predefined methods that enable all parties to communicate in a structured way. Wireless security protocols seek to provide some degree of assurance of the above common security goals by construction. Within the IEEE 802.11 group of standards there are a number of security protocols, the first and oldest being WEP (Wired Equivalence Privacy) and WPA (Wi-Fi Protected Access) which comes in 2 versions; WPA, which works on all access cards that conform to the original 802.11 standard but it does not work on first generation access points due to hardware limitations, and WPA2 which implementing the mandatory components of the 802.11i standard, which was designed to overcome the security short comings of the a,b and g standards. WPA2 works on more recent access cards and access points although a firmware upgrade will need to be run on compatible devices released prior to its wide spread adoption.

Hytnen & Garcia (2006) discuss the fact that the common security measures WEP, and WPA are susceptible to known attacks should an intruder wish to expend the effort to gain access to a network. WEP and the temporal key integrity protocol (TKIP) as used in some versions of WPA are vulnerable to known initialisation vector (IV) attacks, which enable a potential intruder to discover the key if they are able to capture enough network packets (a far greater amount for TKIP than WEP). Furthermore they suffer from a CRC attack because the use of CRC provides an invertible functional relationship to the data. WEP counter-mode which switches the encryption protocol from RC4 to AES removes the attack on the CRC field but is not common place in implementations.

Whilst WPA not using TKIP does not suffer from these attacks, it has weakness in it authentication model (Hytnen & Garcia 2006) which leaves it vulnerable to a dictionary based attack. This attack can be conducted offline through the use of captured packets (Hurley 2004, p. 348). Hytnen & Garcia (2006) state that it is estimated that to provide sufficient security based on the level of hardware available

at the time of their paper, a key (passphrase) of 20 characters or more must be used for WPA. A key of this length is far longer than most home users will choose to use, leaving them open to this attack. When choosing a WPA key users should be aware that it does not have to be something they have to commit to memory as it is reasonable to store a written version, which will allow them to choose a longer key. But they also need to be aware of how to choose a good passphrase to use as a key. Yan et al. (2004) has some discussion about this.

2.2.3 Wardriving

Evidence for the presence of insecure networks is shown by the data collected from wardring or related activities; "Wardriving" is a term given to the act of traversing an area whilst recording the detectable wireless networks and their physical and logical characteristics for subsequent statistical analysis. Characteristics may include information such as, the network service set identifier (SSID), any media access control addresses (MAC address; These are a unique hardware address for each network device consisting of a 48 bit number) of transmitting devices, physical radio frequency channel of transmission, security protocol in use and the network address space of transmitting devices if security is not being employed.

Peter Shipley popularised the term "Wardriving" when he conducted an 18-month survey of his local area in Berkeley, California in the United States of America. This was achieved through the use of an automated system (Hurley 2004, p. 3) of his own creation, which detect the presence of wireless networks and recorded details of their security status. Shipley then presented these results at the DefCon conference of July 2001 in an effort to raise awareness of the insecurities of the wireless networks in use at the time.

Data from this and other surveys (Hal 2004),(Hal & Jacob 2004), (Hytnen & Garcia 2006), suggest than many wireless networks at the time and location of the surveys were left in a completely open state. This would allow intruders to gain access with no effort at all.

This technique can be used by either researchers or attackers to locate open networks. For attackers this is something they can do very simply to establish the

location of network which they may attack. The attack may be for fun but the potential exists for them to have a much more malicious intent.

2.3 Intrusion Detection Systems (IDS)

Someone who gains unauthorised access to network resources is termed an intruder. Stallings (2007, p. 301) states that intruders may have benign or hostile intents and whilst benign intruders may be tolerated, they may consume network resources such as an external WAN link accessible via the wireless access point. Moreover it cannot be known in advance whether an intruder has benign or hostile intent. Hence this provides a motivation for using a method of detecting intruders and their activity on wireless networks.

The idea of an intrusion detection model evolved from James Anderson's paper "Computer Security Threat Monitoring and Surveillance" (Anderson 1980). The deceive work from which most modern systems and papers are based is Dr. Dorothy Denning's "An Intrusion Detection Model" (Denning 1987). The concept is to use a statistical comparison against a defined characteristic set which was created via training data in an attempt to profile network activity associated with a particular device as either normal or abnormal. Intrusion detection can be categorised into 2 classes based upon the detection methods they employ. Misuse and anomaly or supervised and unsupervised based intrusion detection (Boukerche 2006, p.948).

2.3.1 Misuse Detection

Misuse detection techniques use known profiles (patterns) or signatures of an attack to compare with the observed activity to detect an attack. These have the ability to accurately perceive a known attack but do not have the ability to detect an unknown attack and new attacks may have a profile that is significantly different to those of the known attacks and so will not be detected by this class of system (Zhang, Lee & Huang 2003).

2.3.2 Anomaly Detection

Anomaly detection methods are based on the assumption that a user's network behaviour is observable and does not change significantly over time. This can be used to create user network activity profiles for comparison to decide if the observed activity falls within the statistical range for normal user activity. This method has the capacity to detect known attacks and in contrast to misuse detection unknown attacks. Since anomaly's above a threshold value will be identified as intruder activity this method my cause a high number of false positives if a legitimate user performs irregular behaviour (Boukerche 2006, p. 948).

2.3.3 Supervised/Unsupervised Intrusion Detection Model

The supervised intrusion detection model is one which is based upon training data which corresponds to both normal usage and malicious activity undertaken on a network. This requires a supervisor (human) to spend time classifying the actions in the data. For a training set to be affective it generally needs to be large as there is a large range of activities that occur on a normal network. This can take a long time for a human to process which introduces the chance of classification errors on the part of the supervisor. Whilst unsupervised detection (anomaly detection over noisy data) uses machine learning techniques to identify intruder activity but is prone to a high number of false positives (Boukerche 2006, p. 948).

The problem associated with these methods in regards to intrusion for a home network is the difficulty in differentially profiling what is the activity profile of an intruder and what is normal use? Whilst the traditional profiles associated with intruders on traditional wired networks may apply, intruders of a non malicious nature may perform activities that are close to identical to those preformed by the legitimate users of these systems. (Zhang, Lee & Huang 2003)

2.3.4 IDS Data Analysis

The data analysis for intrusion detection systems (IDS) has traditionally been textual in nature and of a nature that would be unfathomable to most home users. The paper "A User-Centered Approach to Visualizing Network Traffic for Intrusion Detection"

by Goodall et al.(2005) presents a method for time-based network visualisation (TNV) which presents a colour based classification of network activity time in temporal and machine IP address based blocks. This graphical interpretation features the ability for users to probe more deeply into the data presented by using "tool tips" (popup text boxes that present more information about the object over which the cursor is positioned) to show information such as the TCP/UDP port number over which the traffic was conducted. The graphical interpretation of the data also allowed the users to perceive the link state between different devices in a temporal manner. While this study was not directed at giving an understanding of the traffic to a networking novice, it did show that a non expert was able to successfully interpret the data after familiarisation with the interface.

2.3.5 IDS - Wireless Evolution

Another direction of current intrusion detection systems research is specialising systems for wireless local area networks (WLAN's). This is illustrated by Hongu and Lixia (2004) as well as Kasarekar & Ramamurthy (2004) Chirumamilla and Ramamurthy (2003) and Zhang, Lee and Huang (2003). They discuss the use of a distributed intelligent agent based systems where each access point on the wireless network has its own intrusion detection agent. These agents can use whatever techniques for detection that are built into them. These techniques are machine learning based in 2 of the studies listed. These agents can either report to a central authority or interact in a peer to peer manner to share detection information and potential intrusion events. This combined network awareness is then used to make a collaborative decision about the legitimacy of detected activity on the network.

The features in the system proposed Chirumamilla and Ramamurthy (2003) provides the following functionality commonly found amongst most distributed wireless networks. It accepts registration and deregistration from AP's and client cards from a central administrator, scans the cells for rogue access points and sends and administrative alert if any are found. It also attempts to detect promiscuous wireless nodes by producing fake address resolution protocol (ARP) broadcast messages which contain a fake broadcast address. A promiscuous node will then replay to this fake broadcast effectively identifying itself if it is using the IP stack. This method is

described in the white paper "Detection of promiscuous Nodes Using ARP packets" by D. Sanai of securityfriday.com which was presented at the Black Hat USA 2001 Briefing (Sanai 2001). This method will only detect those nodes which are not operating in a passive mode.

2.3.6 Commercial Wireless IDS

Frank Bulk in his articles "Rogge hunters" (Bulk 2006) and "Time to tighten the wireless net" (Bulk 2005) written for the ACM's network computing journal, provides a review (current at 2005) of commercial wireless network security applications. However a number of detection mechanisms they employ (as illustrated in the previous section) are only applicable to the larger multi access point networks of the enterprise. Additionally the cost of such products (Bulk 2005, p. 70) is prohibitive for the home market and the interfaces are designed to be used by experienced networking staff.

2.3.7 Detection Errors – False Positives and Negatives

The degree of success of these and other intrusion detection systems can be measured by their ability successfully identify an intrusion to the network as well as the number of false positives they produce. (Zhang, Lee & Huang 2003) A specific system will have more specific performance metrics, designed to evaluate its ability to operate on its specific design goals as well (Chirumamilla & Ramamurthy 2003)

The effectiveness and hence value of an intrusion detection system can be gauged by its ability to minimise both the false negative and false positive alerts it generates (Gu et al. 2006). Intrusion detection systems may be fine-tuned through the adaptation of threshold variables to minimise these values. Gu et al (2006) discuss the lack of a single metric for the evaluation (and adjustment) of an intrusion detection system through the highlighting of a number of the current metrics used and then presenting their own approach to producing such a single metric.

2.3.8 Wireless IDS for the Home

The current development areas of wireless intrusion detection systems are more targeted to the large multi access point networks not typical of the home user. In general the home setup will simply consist of a single wireless access point and a number of clients. This does provide a choke point (a point where all data must pass through) not present in the distributed environments illustrated in Chirumamilla and Ramamurthy (2003). Additionaly in the general home environment there will be no dedicated hardware apart from the access point itself to run intrusion detection on. Home access points in general do run on hardware which is capable of providing a software environment able to support a degree of intrusion detection on the device. The Linksys WRT54G is an example of a device available to the home market that provides the environment necessary to create an on device intrusion detection system, as it runs a variant of the Linux Kernel (http://www.linksys.com) and has the computation and memory capacity to perform the required functions.

Another project for the same hardware intended for home use is the "tiny PEAP" project (Lee et al. 2005) which aims to provide full enterprise wireless security capabilitys to this piece of home hardware. "tiny PEAP" runs a remote authentication dial in user service (RADIUS) server and user database directly on the access point itself, eliminating the need for an external server as required in the normal enterprise solution.

The capability of this device has been demonstrated by such projects as "Blue box"(linksysco 2007), which while not being an intrusion detection system in itself it serves to illustrate the customisability of this device. The custom blue box ROM image turns the device into more of an intrusion or wardriving tool than an intrusion detection system with the inclusion of kismet an example of a tool that operates in RF monitoring mode (Kershaw 2007), to capture any network activity of the channel being monitored (Hurley 2004, p. 139). A blue box installed router would enable even a complete novice to become an intruder on an insecure wireless home network, through one of its features which is to detect any open networks and provide access to that network and its services through the WRT54G's built in Ethernet ports.

3 Methodology

3.1 Honeypot

For intrusion detection systems to be effective it is fundamental to know what activities an intruder is likely to perform. To gather the information which is required to formulate an effective profile of a typical attacker, observations of real attacks need to be made. An interesting question to ask is whether there is a difference between attackers in a residential environment as opposed to a commercial one? It is speculated that attackers in a residential environment may more accurately be described as "moochers" as they simply seek to utilise the Internet connection that many of these access points provide.

Network intruder behaviour can be observed by leaving an open network which logs all activity that occurs. Such systems are termed honeypots. Lance Spitzner, a honeypot expert and the moderator of the honeypots mailing list, concisely defines a honeypot as '*an information system resource whose value lies in unauthorised or illicit use of that resource*' (Spitzner 2003b).

One of the earlier descriptions of the honeypot concept first appeared in literature in Clifford Stoll's book '*The Cuckoo's Egg: tracking a spy through the maze of computer espionage*'(1989). Through the non-fiction thriller Stoll documents the events and thought processes he went through over a series of events where an attacker infiltrated a number of computer system and had his activities logged by Stoll.

Cheswick (1990) describes a system that was designed to be compromised by an attacker so as to observe their actions. Cheswick led an attacker on a trail for a number of months in order to trace his location and observe his techniques. Cheswick did not want to give the attacker an account on the system; instead he constructed a software 'jail' and logged the attacker's techniques. Cheswick concluded that although the jail was appealing, it was complicated to set up and insecure. He then decided that a better solution would be to set up a disposable

system with real security vulnerabilities in the future. This paper documented the first case of a true honeypot.

Pudney & Slay (2005) describes wireless access points honeypots and a methodology for their establishment and data collection. Results from their study are one of the few studies of its kind specifically relating to honeypots used in a wireless environment identified in published literature of an academic nature.

Their study conducted in the CBD of Adelaide Australia, utilised 3 honeypots as described to record the activities and frequency of people connecting to these honeypots. To simulate the presence of other computers and provide the opportunity for malicious intent to occur they used "honeyd" which is an open source honeypot daemon developed by Niels Provos from the University of Michigan designed to provide the appearance of a number of computers with un-patched security flaws in operation on the network.

Pudney & Slay used "honeyd" to create virtual systems in addition to the routing of all traffic designated to the internet through the logging host as was done in this work. This eliminates one major problem identified by Spitzner (2003c, pp. 53-55) relating to the narrow field of view of honeypot systems when used on a wired network.

In their discussion, Pudney & Slay state they found that detailed conclusions from their data could not be drawn regarding the exact intent of the intruders who did not perform attacks or probes against the fake hosts on the network. They note the limitation of their study as the lack of an internet connection which would have provided the opportunity for a larger range of potentially undesirable activities to occur.

Furthermore for a honeypot to be effective any participants must not realise that they are participating in a honeypot network else they may change their behaviours whilst under observation. The honeypot system used in this study employs some of the deception in depth concepts outlined in Suen Yeks paper '*Measuring the effectiveness of deception in a wireless honeypot*' (2003)

3.1.1 The Equipment and Setup

The equipment used within this study was selected to represent common hardware as would be found in a number of homes. The locations used should be considered to represent an average home in which a wireless access point may be left open and provides access to a standard home Internet connection. However it is noted that the range of locations is limited and that no testing was done in a high density population areas such as a unit complex.

The setup used to conduct the data collection for this thesis consisted of 3 major components:

- A wireless access point
- A PC running
    - Network Activity logging software
    - Virtual hosts on the network to attack
- Internet connection bridged invisibly through logging host

A generic home access point, the Netgear WGT624 v2 was configured with no wireless security enabled which would allow anyone to connect. The base station was configured to operate on the least congested channel in the location area so as to cause minimal disruption to other networks in the area. Channel selection is unlikely to affect the number of potential attackers as when searching for networks it is normal to perform a sweep across all channels. The operated in mode was set to b+g to allow the largest possible diversity of devices to connect. The access point is not compatible with type a (5GHz) networks however this is not seen as a significant limitation as most potential intruders will have hardware compatible with the 2.4 GHz class b or g networks.

All traffic occurring on the device was routed to a log computer. The log computer consisted of a generic PC system running a Linux distribution and was connected to an external WAN (Internet) link as well as the wireless access point. Wireshark (formerly known as Ethereal) provided a vital capture tool which was used to log all network traffic occurring on the wireless access point enroute via the log computer to the internet (Orebaugh, Ramirez & Burke 2007, pp. 29,31,34,81). Honeyd was used to simulate a generic windows XP system and a generic Linux system, so that anyone

connected through the wireless the network would see a network which would appear to consist of the 2 PC systems and a gateway to the internet.

3.1.2 Location 1

Operation of the honeypot system commenced on 1st of Augusts 2007 and collected data till the 24th of September 2007. This provided 54 full days of data collection at this location. Location 1 is described as a residential house in parliament St Sandy Bay situated opposite a park and near an intersection. No unit complexes or similar high population density structures are within wireless communication range.

The following wireless networks were also in operation in the immediate area as detectable via the war driving setup (See section 3.2) from the location of the base station.

SSID	Channel	Security
Jock	3	WPA
Belkin54g	11	WPA
NEATGEAR	11	WPA
DLINK	6	WPA

Table 1 Honeypot Location 1 Neighbouring WLAN's in order of decreasing signal strength

Using the generic internal wireless card of the wardriving laptop two way communications could be established from a maximum of 35m away on the road side and only about 15m on the back side of the house (due to the large number of walls in-between). The network was detectable from greater than 50m away up and down the road and further across into the park.

Furthermore location 1 is frequently passed by a moderate volume of pedestrian traffic.

3.1.3 Location 2

The same system was relocated to location 2 and operated continuously for a further 35 days (25th of September till the 30th of October, 2007). Location 2 is described as a residential house neighbouring some small unit complexes on Regent St Sandy Bay.

The following Networks were detectable from the location of the base station:

SSID	Channel	Security
CeCe	1	WPA
WLAN-AP-624W	11	WPA
DLINK	11	NONE
Linksys	11	WPA
BigPond3900	11	WPA
BlackMax	11	NONE
BFHN	11	NONE
lighthouse	6	NONE
PoweredByDodo	10	WEP
GreenLAN	2	WPA
Home	6	NONE
<NO SSID>	6	NONE

Table 2 Honeypot Location 2 Neighbouring WLAN's in order of decreasing signal strength

Again using the generic internal wireless card of the wardriving laptop 2 way communications could be established from a maximum of 35m away in all directions. The network was detectable from greater than 50m away up and 100m down the road.

Figure 1 Honeypot site locations

3.1.4 Legal and Ethical Issues

The use of honey pots to collect data provides a number of legal and ethical issues. Spitzner (2003a, p. 16) provides a discussion on the legal issues associated with a honeypot, with a united states focus but the issues he addresses still apply in Australia. The main points are

- Entrapment
- Harm to others
- Right to monitor

Entrapment is where someone (in this case the researchers) encouraged someone to commit a crime whist collecting evidence to prosecute them. This is avoided in this study by the decision to not prosecute anyone using this honeypot system.

A malicious intruder may use the honeypot system and its resources to achieve a number of nefarious goals. In this case all that can be done is monitor the honeypot regularly and halt any such activities when they are detected.

From the network activities that were logged any personally identifiable information was purged. The goal of this research was to assess what type of activities would an intruder under take (attack computer or use the internet connection provided). This was sufficient to receive approval for the experiment from the universities ethics board.

The logs that were recorded were stored in an encrypted database, so if an attacker had compromised the deception and attacked the log computer itself they would be unable to view the logs and extract any information before they would have been detected and their communication shut off.

3.2 Wardrive

3.2.1 Goals

There is plenty of evidence that in the past a large portion of wireless networks have been left open (Hal 2004) and this section of the study seeks to establish if this is still true and to what degree open networks occur in a residential environment.

The statistical data required about local wireless networks in a residential area (Sandy Bay) can be collected to gauge the number of and hence the significance of the proportion of home users leaving their networks unnecessarily vulnerable. The networks detected by the wardriving survey were characterised by presence (or lack of) and type of encryption employed upon them. A global positioning system (GPS) unit was employed to give a spatial relation to the area surveyed however this was not tied to the networks detected to give their distribution due to ethical considerations about identifying an individual's networks at risk.

3.2.2 The Equipment and Setup

The wardriving equipment consisted of a generic laptop with the following wireless Hardware:

- Intel PRO/Wireless LAN 2100 3B Mini PCI (internal)
- Netgear WG511 PCMCIA adapter

For network detection and log creation "Kismet" which is an 802.11 layer 2 wireless network detector was used, with the wireless card in a passive promiscuous mode.

The following information was logged:

- Network Type
- SSID
- Network Channel
- BSSID (MAC Address)
- Cryptography Used
- Beacon Time
- Detected IP Range

3.2.3 Detection Procedure

Traversal routes were selected from the residential zones within the Sandy Bay region such that they should form a representative sample of the entire Sandy bay area and potentially represent a generic residential area. Each area was traversed 3 separate times to establish the number of and security state of the base stations which were consistently present and in a consistent security state. This should allow an assessment of the level of security employed by users of home wireless networks.

The routes were traversed on foot with the laptop placed in a backpack. Given an average walking speed and the presence of dual wireless cards a large amount of detection time was spent on any given channel giving a high likely hood of detection in the space illustrated below.

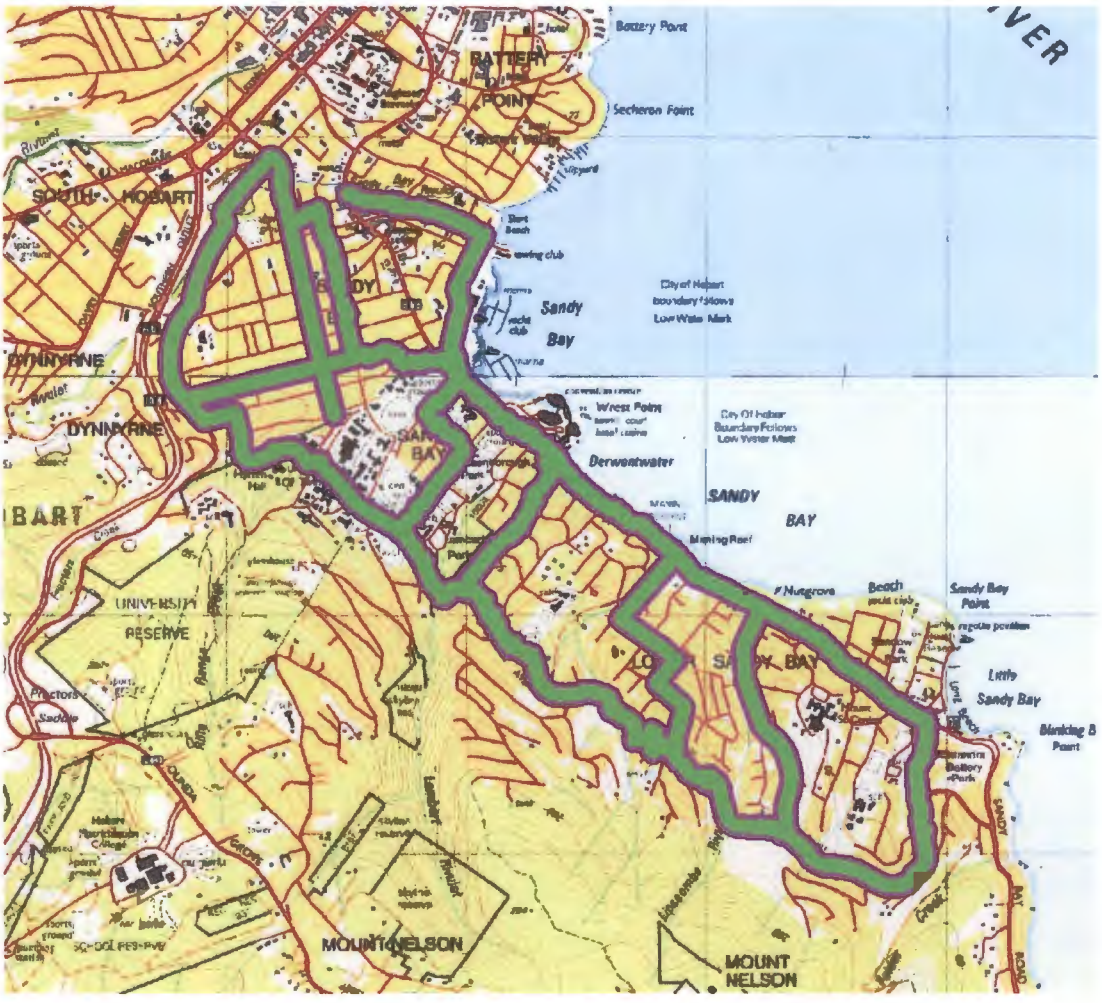

Figure 2 Area Assessed

The green area shows a 30 meter buffer around the area traversed; this represents an approximate area for which any base stations present would have been detected. The purple area shows a 50m buffer and it is fairly likely any base stations present in this area would have been detected. The exact area of detection cannot be determined as there are too many unknown variables however these areas represent conservative estimates given the speed of traversal. It is worth noting that the setup (with no special antenna) is capable of detecting the University of Tasmania's UANA and UANA-Setup networks from the opposite end of Regent St which is a distance of just over 1 Km in a clear line of sight.

3.2.4 Legal and Ethical Issues

Contained within the paper by Hira Sathu titled '*WarDriving: Technical and Legal Context*'(2006) is a discussion about the legality of wardriving which states that there

is currently no legal president established in most countries regarding the legality or otherwise of wardriving. Notably a section on Australia and New Zealand law is included which states that Australia has no definitive case law for theft of network service by unauthorised means.

The Australia Federal Cybercrime Act 2001 section 476 provides the closest description to covering the activities involved in wardriving. The potentially relevant clauses are listed below:

- *Unauthorized access, modification or impairment with intent to commit a serious offence*

- *Unauthorized modification of data where the offender is reckless as to whether the modification will impair data, covering situations such as where a hacker unintentionally impairs data in the course of unauthorized access to a computer system*

- *Unauthorized impairment of electronic communications, including 'denial of service' attacks'*

However these clauses do not explicitly cover the activities which are conducted during a wardrive. Hence unless other criminal activity that specifically violates the act occurs through the networks found through wardriving. Nevertheless this still does not apply the act to the wardriving itself, as it would be those other criminal activities rather than the wardriving itself that violate the act.

Hence if no active probing or utilisation of networks resources occurs and no analysis of captured packets to extract private or personal information happens there should be no legal issues with collecting information in a manner such as this. Consequently this is the approach undertaken for the wardriving data collection involved in this study.

The procedure that was undertaken to conduct this study was also sanctioned by the relevant university ethics board. This was done to ensure that there was minimal ethical impact from this study as determined by an authoritative body.

3.3 Device Critique

3.3.1 Goals

To gain an understanding of the security defaults/recommendations that are present on common home wireless access points a sample of common devices was undertaken. It is hoped that this could highlight possible improvements to the devices deployed in many homes.

This would be done through the collect of data pertaining to the information provided on/with the device about the security relevance of settings such as wireless encryption. In addition the devices default configuration in regards to security aspects were assessed.

3.3.2 Method

To collect the relevant information about the devices the device manuals were consulted and were possible the actual devices themselves to confirm what was suggested by the manual. This information was entered into a database table constructed for this task.

Devices to be included in this critique were selected based upon the popularity ratings of devices in the whirlpool broadband hardware database (whirlpool broadband multimedia 2007) these popularity ratings are based on the availability of the hardware from internet service providers and the hardware they subsidise (to decrease their support line costs due to staff familiarity were the clients hardware) as these should reflect common choices by the target group of home users. The hardware includes both stand alone wireless access points and ADSL modems with built in wireless access points.

3.4 User Survey

3.4.1 Goals

It is not adequately understood whether home users would like an intrusion detection system present in their wireless access point or even if they are concerned about the

risks of having a wireless network. A Survey of home users gives the opportunity to evaluate if the current methods of conveying information in regards to the technical setup options are adequate. In addition to what kind of alert methods users would see as acceptable form an intrusion detection system.

These are the questions we hope to answer by conducting the user survey.

3.4.2 Design

The design goals for the survey were that it should be compliable in a short amount of time to hopefully increase the number of participants and increase the thought given to each question.

The survey questions used were either a simple yes, no or unsure response choice or psychometric response scale questions. For the response scale questions a Likert scale was used as is standard for these types of surveys (Goodall et al. 2005; Schaik & Ling 2007).

This method presents the subject with a statement and they asked to rank their level of agreement. For instance on a 5 point Likert as used for the relevant questions in this survey, the participant selects a score 1-5 where

- **1** Strongly disagree
- **2** Disagree
- **3** Neutral (neither disagree nor agree)
- **4** Agree
- **5** Strongly agree

Inherently the response data can then be only treated as ordinal as it cannot be assumed that that the test subject perceived the distance between adjacent response levels as equidistant and moreover that every individual perceived the distance as the same. An ordinal ranking allows the data to be analysed for correlations between response groups with a non-parametric test (where the model structure is not predetermined, it is determined by the response data).

3.4.3 The survey

See appendix A for a copy of the survey and the accompanying information sheets as provided to the participants.

The survey consisted of 5 sections the following is a summary of what they were and what was the goal of the contained questions.

- **Section 1** – Current home setup
    - Assess what type of user is doing the survey
- **Section 2** – Wireless risks
    - Assess awareness of security risks
- **Section 3** – Intrusion detection
    - Assess users views about intrusion detection help
- **Section 4** – Alert methods
    - Asks what alert methods would be preferable for an IDS
- **Section 5** – Additional comments

In total the survey consisted of 25 questions designed to first profile the sample group. It then seeks to finds out there opinion on possible ways in which a wireless intrusion detection system could be implemented in future devices.

Participants in the survey were all volunteers. Initial recruitment was from community members who were attending a talk about wireless network security conducted at the university. An additional number of other home users (of a non-technical background) were also found and allowed to participate in the study.

4 Results

The following section details the results and provides a discussion of the findings from the research that set out to answer these questions:

- What are the risks with leaving a wireless network open in a residential area
- How great are those risks
- How many network are left are left open by home users
- What are the default settings for home access points
- Would users like an intrusion detection system for their access point
- If so how could it be designed to best suit a home users

4.1 Honeypot

The Honeypot system was set up to investigate the kind of attacks that might occur on an unprotected network located within the area of Sandy Bay. The main question of interest was to determine if attackers were simply interested in "mooching" network services, specifically free Internet access, or was they also interested in attacking the access point and other hosts present on the network.

4.1.1 Data

It was found that over the course of the 89 days of operation for which the honeypot system logged access no unknown MAC addresses either accessed the network or used its resources. The only recorded usage was by the researcher's own devices which were used to test the operational status of the honeypot.

4.1.2 Discussion

The lack of any attempted use of the honeypot system over the operational period is surprising as this is contradictory to the limited evidence available from other studies. The evidence collected by this experiment suggests that there may not be a high risk associated with leaving a wireless system open in the Sandy Bay residential

area. However it should be noted that a number of factors could have influenced the outcomes of this experiment.

- Limited operation Time
- Non-optimum locations
- Limited number of honeypots

The locations used for this study were the researcher's residences at the time of the experiment. These locations were used as to overcome the limitation of previous studies where the honeypot did not allow an intruder to connect to the Internet.

The honeypot was allowed to run for as long as possible, within the constraints of available hardware and time. However the amount of time for which the experiment ran and number and type of locations chosen is in no way represents an intensive study. However if an unsolicited usage had occurred over this limited time period it would have suggested that a significant risk would be associated with leaving an network open in this area.

Furthermore it is possible that the honeypot was indeed found by passive wardriving techniques, such as those used in another section of this study. Such techniques would leave no trace in the honeypot logs as it is possible just to detect the honeypots access point's synchronisation beacons and not to interact with the access point itself. However if the honeypot was detected it was not found suitably interesting for those who discovered it to warrant investigate further investigation.

4.2 Wardrive

The aim of the wardriving exercise was to determine the extent to which home, and perhaps commercial, wireless networks had been left either completely unprotected or with the minimal protection afforded by WEP. The area to be investigated was lower Sandy Bay in Hobart.

4.2.1 Data Summary

The wardriving data was collected on the following dates and approximate times in the year 2007. The area assessed can be seen in section 3.2.3 and the spatial location data can be found in appendix C. Known special case networks such as the Universities UANA and UANA setup networks have been removed from the data as these would bias the results. However a large number of these base stations were detected. Data is presented for war drives that took place on the following three dates:

- Thursday the 23rd of August 8pm – 12pm
- Monday the 24th of September 1pm – 5pm
- Saturday the 13 of October 9am – 1pm

The following table represents the number of networks detected during the experiment broken down according to the type of networks that they correspond to.

Network Type	Number	%
Infrastructure	1148	81
AD-Hoc	33	2
Probe	232	16
Total	1413	

Table 3 Detected Networks Summary

The following image shows the number of networks that were detected within 50m of a grid of aggregated points. This was done so as to preserve some anonymity of the networks whilst still showing the approximate distribution. It was found that there were a larger number of networks found in proximity to buildings such as unit complexes which would have a higher population density. This may suggest a correlation between population density and density of wireless networks.

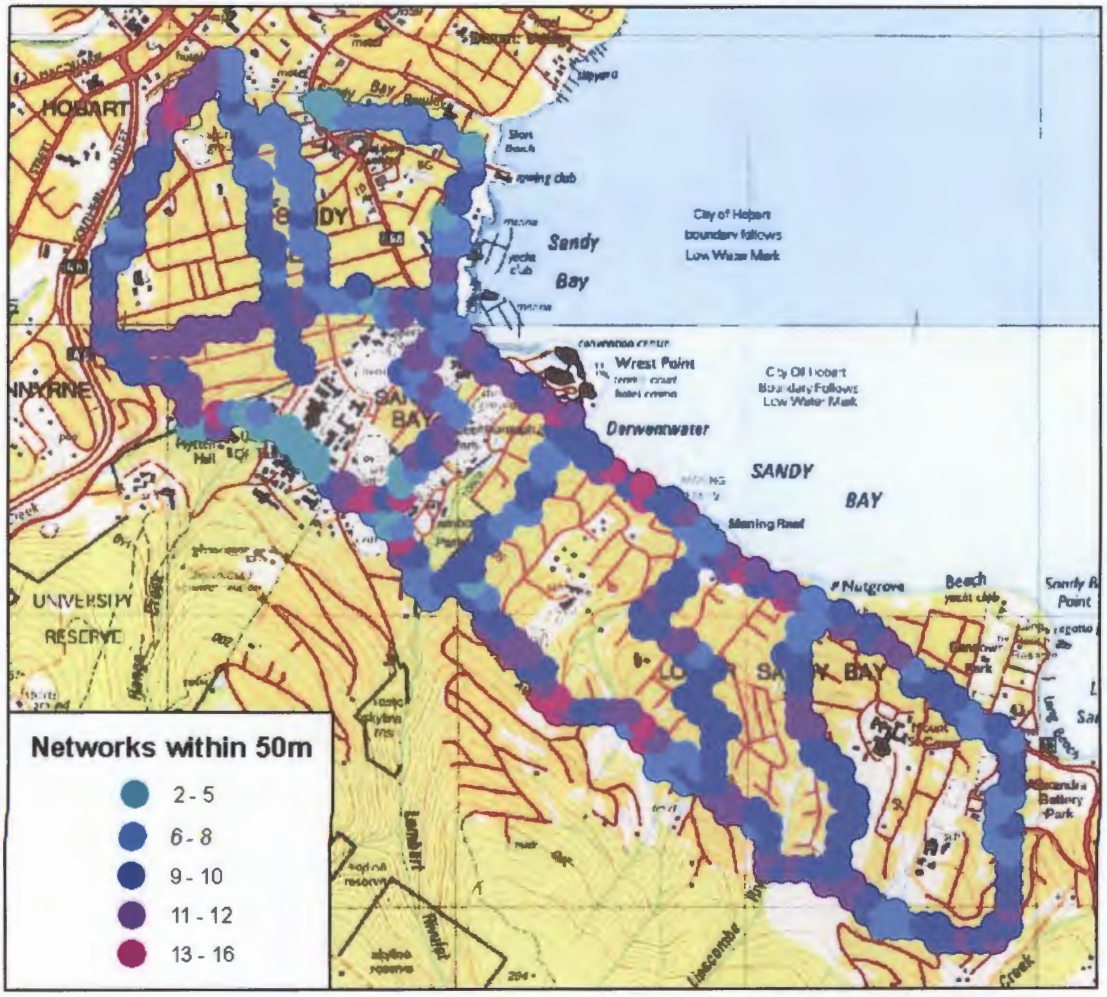

Figure 3 Aggregated data showing Networks detected within 50 m

Henceforth only the infrastructure networks are considered in the numbers and discussion that follows. This is because the infrastructure networks represent the permanent networks which this study is focused on. The AD-Hoc networks represent a temporary network setup between 2 client devices and the probes represent devices attempting to access an infrastructure network.

A summary of the wireless security protocol used by the networks is given below. The category WPA encompasses all variants of WPA. This is because when compared to WEP and none (No Security) each variant offers a similarly high level of security within the currently known vulnerabilities of the WPA class of protocols.

Security	Number detected	%
None	305	26.57
WEP	522	45.47
WPA	315	27.96

Table 4 Infrastructure Network Security Protocols Detected Summary

Approximately half of the networks detected that had no security enabled also had default SSID's. Three networks were detected that had hidden SSID's 2 of which had no encryption and one used WEP.

The first 12 bits of the MAC addresses of the base stations detected can be used identify the manufacturer of the hardware. This is because these bits are uniquely assigned by the IEEE to a manufacturer. A full list can be found at the IEEE's website (IEEE 2007) . This list was used to identify the manufacturer of the wireless chipsets detected in the study.

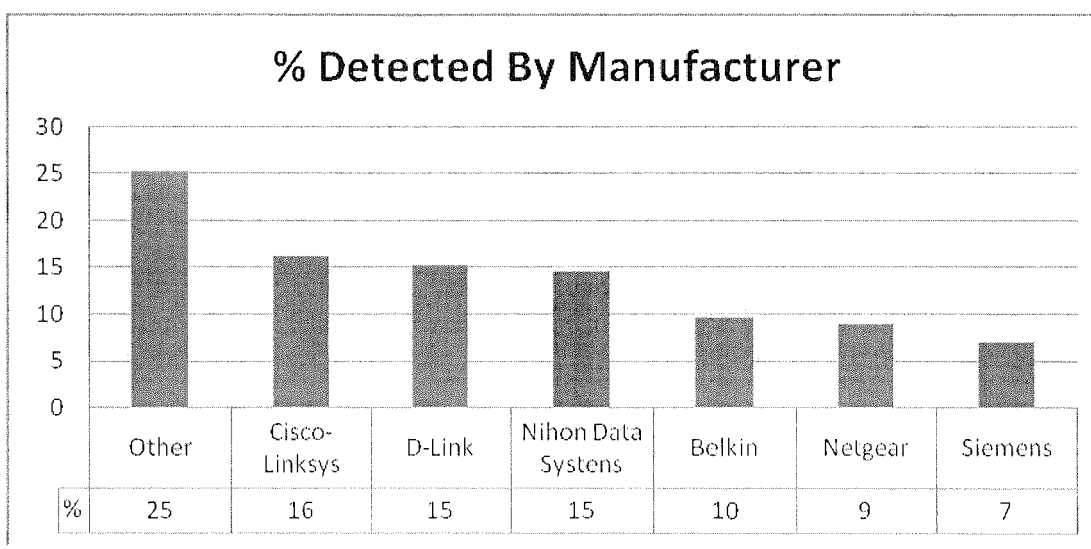

Figure 4 % of Networks Detected By Manufacturer

It should be noted that while Nihon Data Systems is not a recognised brand it however occupies the third largest percentage by a single chipset brand. This is

probably due to the fact that Nihon Data Systems is the manufacturer of the wireless chip set present in most of the ADSL plus wireless modems provided by Telstra.

4.2.2 Discussion

The data shows around 26.6% of the networks detected within the assessed region failed to use any wireless security. This is a statistically significant (with 95% confidence interval) number of wireless networks that are in a vulnerable state. As such a significant percentage of wireless networks are left open to exploitation.

The passive nature of the network detection meant that no attempt was made to use any resources of the open network. Hence there can be no certainty that other forms of security were not implemented on these networks; for example an access control list based on client MAC addresses. However it seems unlikely that any significant number of these open networks would employ such measures, as the technical knowledge required to implement these alternate security measures, requires a higher level of technical proficiency than the implementation of WPA or WEP security in the wireless network in the first place. Furthermore when such measures are used they are normally employed as an extra layer underneath the wireless security protocol to give a greater depth of defence for the network.

No assumptions can be made about the strength of the keys that were selected and used with the WPA encrypted networks. Nevertheless this is something that could be easily tested through an offline dictionary based attack as discussed in Hytnen & Garcia (2006). This would allow a more detailed view of the security of home wireless networks. However ethical considerations meant that this could not be pursued during this study as there are ethical considerations to be made.

The presence of default SSID's on networks with no security suggest that these access point may have been left in an essentially default state by the users. This is indicated by the lack of change in other observed configurable details. As a result it is also likely that a significant proportion of these access points would have a default administrator password. This could leave them open to a number of complex attacks designed to steal private information such as online banking details.

These attacks could happen if a malicious attacker were to configure the access point to redirect traffic through a device under the attackers control perhaps through the DNS configuration or routing tables. This would allow the attacker to execute a man in the middle attack such as those discussed in Xia & Brustoloni (2005). Alternatively the attacker could open ports on the devices firewall and disable the security that is normally present on the WAN link on these devices, and thus allow the attacker to use the device as they wish from the comfort of their own home.

A further dissection of the data shows that of the networks for which no encryption was detected, the ratios of device chipsets present do not matched the overall distribution.

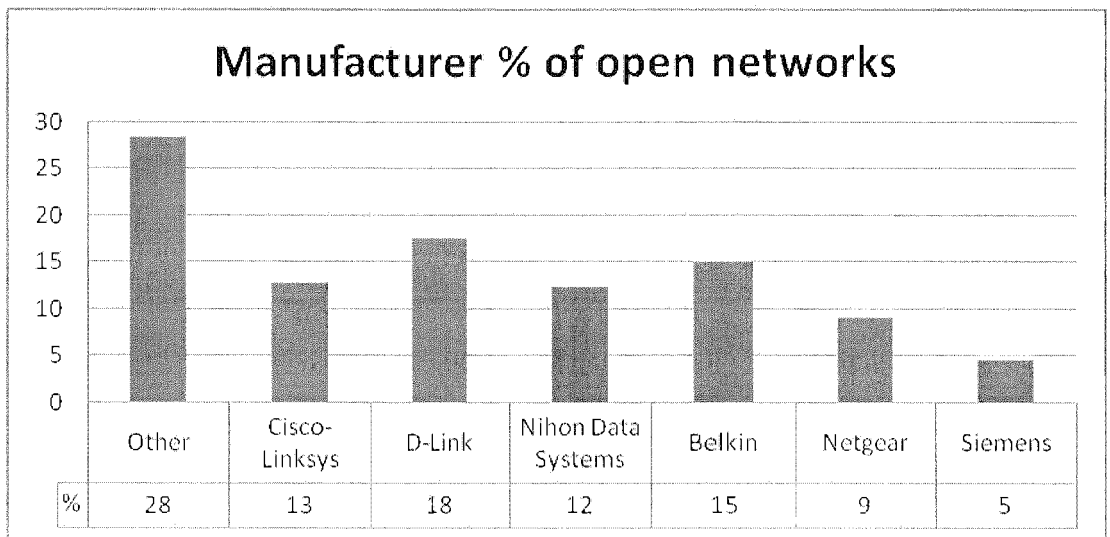

Figure 5 Manufacturer % of open networks

Manufacturer	% Difference
Other	3
Cisco-Linksys	-3
D-Link	2
Nihon Data	-2
Belkin	5
Netgear	0
Siemens	-2

Figure 6 Difference between open and overall manufacturer representation

These differences may suggest that devices that use certain chip sets may be more likely to be configured with security enabled. However the differences are within the range of statistical sampling error, so a large sample would be needed to determine whether this is a factor. However this would not determine what aspect of these devices is conducive to better security setup if such a brand relationship does exist so a study directly testing what makes a device more likely to be setup securely would be more beneficial.

4.3 Device Critique

This section of the work examined commonly available home wireless access points in order to determine whether or not there was anything in the nature of the device itself or its software that would lead to home wireless networks being left unprotected.

4.3.1 Data summary

In total 17 of the more popular devices were assessed and included in the critique. Devices from each manufacture were included to approximately match the ratios of the access points found through the wardriving experiment (See Figure 3). Where multiple versions of a device existed, the most current version with most current firmware was used. This is because the information was not always accessible for some of the earlier versions. However in a number of devices it was noted that it was common for WPA2 to only be supported in a more recent firmware version. It is believed that most home users would not update the firmware in their wireless access points.

In the following table WPA represents the maximum version that the device is capable of or '0' represents that it does not support any version. A full version of the data collected is available in appendix B. User names and passwords encased in < > represent the lack of a password or user name, both of which should be required in order to administer the device.

Brand	Model	Default User Name	Default Password	Default IP	Default SSID	WPA
Belkin	F1PI241EGau	<no username>	admin	10.1.1.1	WLAN	2
Belkin	F5D8231au4	Administrator	<None>	10.1.1.1	Belkin_Pre_N	2
Billion	5100W	admin	admin	192.168.1.254	wlan-ap	0
Billion	7300G	admin	admin	192.168.1.254	wlan-ap	2
Billion	7402VGP	admin	admin	192.168.1.254	wlan-ap	1
Dlink	G604T	Admin	Admin	10.1.1.1	DLINK	1
Dlink	DWL-2100AP	Admin	<none>	192.168.0.50	default	2
Dynalink	RTA1025W	admin	admin	192.168.1.1	RTA1025W-8D1CF9	2
Linksys	WRT54GL	admin	admin	192.168.1.1	linksys	2
Linksys	WAG54Gv2	admin	admin	192.168.1.1	linksys	1
Netcomm	NB9W	admin	admin	192.168.1.1	wireless	2
Netcomm	NB5PLUS4W	admin	admin	192.168.1.1	wireless	1
Netgear	DG834G	admin	password	192.168.0.1	NETGEAR	2
Netgear	WGT624	admin	password	192.168.1.1	NETGEAR	2
Siemens	SpeedStream 6520	admin	admin	10.0.0.138	SpeedStream	1
Thomson	SpeedTouch 585	<None>	<None>	192.168.1.254	SpeedTouch	2
TP-Link	TL-WR642G	admin	admin	192.168.1.1	TP-Link	2

Figure 7 Device Critique

The following is a summary of the major findings that arise from the data.

- Default username and passwords are predictable
- None of the assessed devices had wireless security on by default

4.3.2 Discussion

Across the range of devices included in the critique none provided a wireless intrusion detection system. All of the assessed devices provide a firewall for their

WAN link, but the wireless network was considered an internal part of the network and that inherently the devices within that could trust each other.

An important aspect of a device for this study would be whether or not it provides an adequate level of help to the user about the selection of wireless security settings. However this could not accurately be assessed by the researcher, as it is not possible to pretend to a level of understanding of an average home user when one infact has a much greater level of understanding. Should further investigation into this area of device comparison be needed a survey could be conducted with a large number of novice users of approximately the same skill level asked to rank the devices.

4.4 User Survey

The role of the user survey was to understand more about the current level of knowledge about wireless security in home users and also to understand the kind of features they might like to find on their wireless access points in order to improve the security of their home wireless networks.

4.4.1 Survey Section 1

The user survey received 30 valid responses from 31 participants. One survey was rejected due to the ambiguity in determining which answer the participant intended to select. The full tabulated raw responses data can be seen at appendix C accompanied by summaries of variance and the response ranges. The statistical significance of the responses cannot be meaningfully calculated due to the limited size of the sample group. As such the responses can only be treated as a guide to what the opinions of a larger group would have been.

An important variable of the survey was the selection of the group of participants such that it could be representative of a typical home user. This was done through the recruitment process. Another important variable was the skill level and knowledge that the users possessed. Section 1 of the survey hoped to establish such a profile and is summarised:

- The average participants network knowledge was low with a mean & median of 2 out of 5
- 2/3 use setup wizards for their access points
- 2/3 were unsure if they used wireless security or not
- 1/6 of the participants said they did not use wireless security

The results from section one of the survey does suggest the participants fall within the intended target group. This supports the way in which they were recruited.

4.4.2 Survey Section 2

Section 2 of the survey focused on assessing the level of knowledge posses by the focus group about the risks of wireless networks and their opinion of wireless moochers.

- 5/6 did believe there was a risk through having a wireless network
- 2/3 were moderately concerned about the risk
- Majority felt strongly against moochers (with no malicious intent)
- Most felt they would be unaware if they did have an intruder

It is noted that a potential bias may exist in the responses to the question asking about matters to do with wireless security as the participants were primed to be concerned by the very fact of answering a survey about wireless security. This should be taken into consideration when drawing any conclusion from the data.

4.4.3 Survey Section 3

Section 3 of the survey dealt with intrusion detection and how willing home users were to accept help in setting one up and have extra features added specifically to help them understand any information presented to them.

Question 2 of this section '*would you like the detection-*' (in regards to an IDS) *'-to be fully automatic*?' produced a dichotomy between the participants in the results:

- 2/3 agreed or strongly agreed with this
- 1/3 felt strongly against the idea

It was also found that there was also a correlation between these two groups and their responses to question 4 '*Would you be prepared to authorise each new device that is connected to your network?*' of the same section.

The idea of a visual representation of log data such as that discussed in Goodall et al (2005) was not found to be appealing to most participants. There was no correlation found between those who did find such an idea appealing and any other trends in questions answered.

4.4.4 Survey Section 4

Section 4 of the survey asked the users what kind of alerts they would like or dislike on an intrusion detection system present on their home wireless access point.

- 23/30 liked the idea of an alert email
- The majority disliked the idea of an SMS being sent to them
- There was a general dislike of the idea of an audible alarm

There was a correlation between the group that said they would like an intrusion detection system to be fully automatic and those who only wanted to be alerted when there was a high probability of an intruder and correspondingly the other respondents tended to be more willing to be presented with false alarms.

4.4.5 Survey Section 5

Section 5 of the survey was provided so that participants could provide any additional comments they wished to make. However no comments were recorded which were of any relevance to the study.

4.4.6 Discussion

The 30 responses received do not represent a large enough sample to give an acceptable degree of confidence from any conclusions drawn from the data. The data can only be used as an indicator of the distribution of a larger sample and hence what such a population would might like. The discussion that follows acknowledges the limitations of the sample size of the data and makes claims based only upon that which is indicated by the sample.

The sample group self rated themselves with a low technical understanding as was anticipated for this target group. As 2/3 of the respondents said that they used the setup wizards on their devices this is a clear area where an improvement could be made in the help provided or the recommendations made in regards to security. This is supported by the fact that all the users who reported that they were unsure if they used wireless security or not had used the setup wizards. Correlating the result from the wardriving experiment where 26.6% of the wireless networks in the area were left open it is likely that around a quarter of those who used the setup wizards did not enable wireless security.

The survey respondents generally did not like the idea of an intruder using their network and more specifically the Internet access this provides, even if the intent of the intruder was non malicious. However most said that they would be unaware if such a user did "mooch" their internet connection.

While the question of whether participants would like an intrusion detection system present in a future access point, was responded to with a general consensus of yes, the question then needs to be asked is what kind of associated cost they would be prepared to pay for this facility? However this was not asked in this survey and should be something to be considered in any future surveys of a similar nature.

Furthermore of those asked about an intrusion detection system the 2/3 who liked the idea of the system being fully automatic were mostly those also willing to authorise any new device when it was first used. This would allow the creation of a simple system to create an access control list based on the MAC addresses of the approved devices, once authorised by the owner in this way. However such a system would not be complete as the MAC addresses of authorised devices could be faked by a skilled

intruder allowing them access. However such a system would add an extra layer of security at little cost.

It is interesting that the respondents in general only wished to be alerted to an intruder if there was a high likelihood of an intruder. This low tolerance level for false positives, reflects a general low level of understanding about the dangers from intrusions onto their network. Of the alert methods ranked (email, SMS, audible alarm) the most non intrusive of the options, the email alert was the most preferred amongst the sample group. There was actually a recorded dislike by a number of people of the SMS and audible alarm methods. This could be interpreted as a desire to be alerted about intruders in a manner that does not demand their immediate attention.

5 Conclusions and Future work

This study set out to investigate the level of wireless security awareness among home users in the Sandy Bay are of Hobart and to examine the risks associated with this. The war driving experiment and user surveys confirmed the low level of wireless security awareness shown in previous studies. An analysis of the various access devices found in the study did not show that device type used influenced the vulnerability of the wireless system that they supported. However, the honeypot system failed to attract any attackers.

The activity recorded on the honeypot over the operational period of 89 days would suggest a lower than anticipated risk associated with leaving a wireless network in a vulnerable state in a residential environment as no attacks/intrusions at all were detected. However with consideration of the conflicting results from the similar studies conducted and the acknowledged limitations associated with this one no conclusion can be drawn as to the real risked faced by residential users. Further investigation is required to more accurately assess the risks that the users of home wireless networks face.

Future research involving honeypot systems could consist of a more detailed study consisting of a larger number of honeypots deployed over a longer time could be carried out to consolidate the actual risk faced by users of home wireless networks. A more detailed study of the factor that location plays should also be considered to test the following variables:

- Number of neighbouring networks and their security state
- Population within communication range (Unit complex v stand alone house)

In addition to allowing a more accurate level of risk assessment the data collected by such future honeypots in a residential environment could allow a profile of attackers' in these environments to be created for potential use in an intrusion detection system. This is assuming that intrusions/attacks would occur.

Another aspect that could be investigated is how the level of appeal of a honey pot is affected by changes to some of its defining characteristic. This would also extend the

work of Yek (2003) in measuring the effectiveness of the deception of a honeypot. This could lead to an improvement to the design of honeypots systems potentially increasing the amount and quality of data collected.

It was found through the course of this study that there are a significant number (26.6%) of open wireless networks in the Sandy Bay region. Given the ease in which these networks can be found and intruded upon, this is suggestive that users are not aware neither of neither the risks nor the simple measures that they can take to reduce the risks that they face. Hence this would suggest that users of home networks may benefit from an increased education about the risks and counter measures associated with wireless networks.

The wardriving results do not suggest that any one manufacturer's devices have a statistically significant tendency to be not configured with wireless security more than any others. This then suggests that more could be done by all manufacturers to increase the adoption of wireless security by their users.

It is unknown what strength keys the users of WPA for their home networks are choosing. Using Current hardware and cracking techniques passwords should be of around a length of 20 characters or greater (Hytnen & Garcia 2006) and should not be made up of simple words. It has been shown (Yan et al. 2004) that users presented with better education and help will chose better passwords.

Furthermore it is possible to test the predicted weakness of these passwords by attempting on off line dictionary based attack on captured passwords as stated in Hytnen & Garcia (2006). However this raises ethical issues. Another alternative would be to have users anonymously submit their old passwords after running an education session about selecting good passwords

Noting the limitations presented by the small sample size, the results from the user survey suggest that home users would be willing to have a wireless network intrusion detection system and in general provide it with some operational assistance. The results moreover suggest that any such intrusion detection system should have a non-intrusive alert method.

The results from the user survey also suggest that more research could be directed into creating a better and more helpful and educational user interface for wireless

access points. A study could assess what presentation methods were most effective at conveying the need security message and educating the users about their choices.

In conclusion home users do not appear to be aware of the risk of having an open network given the percentage of open networks found. It would seem they need more help to ensure they make the best possible choices regarding security of their wireless networks in the future.

Physical Layer (PHY) Specifications, 1999 edn, ANSI/IEEE, 16/05/2006, Standards Document, <http://standards.ieee.org/getieee802/802.11.html>.

---- 2007, *IEEE OUI and Company id Assignments*, 25/10/2007, <http://standards.ieee.org/regauth/oui/oui.txt>.

Kasarekar, V & Ramamurthy, B 2004, 'Distributed hybrid agent based intrusion detection and real time response system', paper presented to Proceedings - First International Conference on Broadband Networks, BroadNets 2004, San Jose, CA.

Kershaw, M 2007, *kismetwireless*, 06/11/2007, <http://www.kismetwireless.net/>.

Laszlo, J 2002, 'Home Networking: seizing Near-term opertunities to extend conectivity to every room', *Jupiter Research*, 09/07/2002.

Lee, B, Gruen, J, Takahashi, T, Lee, W & Lipton, R 2005, *tinyPEAP on the WRT54G/GS*, 06/11/2007, <http://www.tinypeap.org/index.html>.

linksysco 2007, *Blue Box*, 06/11/2007, <http://linksysco.com/box.php>.

Orebaugh, A, Ramirez, G & Burke, J 2007, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*, Syngress Publishing, Inc, Rockland.

Pfleeger, C & Pfleeger, S 2003, *Security in computing*, 3rd edn, Prentice-Hall, Upper Saddle River, NJ.

Pudney, P & Slay, J 2005, 'An investigation of unauthorised use of wireless networks in Adelaide, South Australia', *Information Security and Privacy. 10th Australasian Conference, ACISP 2005. Proceedings (Lecture Notes in Computer Science Vol. 3574)*, pp. 29-39.

Sanai, D 2001, *Detection of promiscuous Nodes Using ARP packets*, 14/05/2007, White paper presented at the Black Hat USA 2001 Briefing, <http://www.blackhat.com/presentations/bh-usa-01/DaijiSanai/bh-usa-01-Sanai.ppt>.

Sathu, H 2006, 'WarDriving: Technical and Legal Context', paper presented to 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, 27-29/05/2006.

Schaik, PV & Ling, J 2007, 'Design parameters of rating scales for web sites', *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 14, no. 1.

Schneier, B 2000, *Secrets and Lies*, Wiley, New York.

Shehan, E & Edwards, WK 2007, 'Home networking and HCI: what hath god wrought?' paper presented to Conference on Human Factors in Computing Systems, San Jose, CA, USA.

'Singapore leads in crackdown on Wi-Fi moochers', 2007, *Australian, The*, p. 32.

Spitzner, L 2003a, 'The Honeynet Project: trapping the hackers', *Security & Privacy Magazine, IEEE*, vol. 1, no. 2, pp. 15-23.

---- 2003b, *Honeypots: are they illegal?, updated 12/06/2003*, viewed 27/10/2007.

---- 2003c, *Honeypots: tracking hackers*, Addison-Wesley, Boston.

Stallings, W 2007, *Network Security Essentials: Applications and Standards*, third edn, Pearson Prentice Hall, Upper Saddle River.

Stoll, C 1989, *The Cuckoo's Egg: tracking a spy through the maze of computer espionage*, Pan Books, London.

whirlpool broadband multimedia 2007, *Broadband Hardware Database*, 10/09/2007, <http://whirlpool.net.au/index.cfm?a=h_models>.

Xia, H & Brustoloni, JC 2005, 'Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks', paper presented to 14th international conference on World Wide Web, Chiba, Japan.

Yan, J, Blackwell, A, Anderson, R & Grant, A 2004, 'Password memorability and security: empirical results', *Security & Privacy Magazine, IEEE*, vol. 2, no. 5, pp. 25-31.

Yek, S 2003, 'Measuring the effectiveness of deception in a wireless honeypot', paper presented to 1st Australian Computer, Networks & Information forensics conference, Perth, WA, Australia.

Zhang, Y, Lee, W & Huang, Y-A 2003, 'Intrusion detection techniques for mobile wireless networks', *Wireless Networks*, vol. 9, no. 5, pp. 545-556.

7 Appendices

7.1 Appendix A – User Survey

See companion CD for survey sheets and digital version of response data

	section 1									section 2						section 3					section 4				
	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5
1	2	1	2	3	2		2	2	3	3	4	5	2	2	4	1	4	4	5	4	5	4	5	1	3
2	2	2								4	4	5	1	1	2	1	1	1	2	1	1	2			1
3	3	1	1	3	1	1	1	2	1	2	2	1	2	1	2	1	1	1	1	1	1	2	2	2	1
4	2	1	1	3	2	3	2	3	1	4	5	5	2	1	3	1	5	5	4	4	4	3	4	2	4
5	2	1	1	2	3		2	1	1	5	4	5	2	1	2	1	5	4	4	4	5	4	4	3	3
6	1	1	1	3	3		2	3	1	4	3	3	1	1	1	1	5	3	3	3	3	3	5	1	1
7	4	1	2	3	1	2	2	2	1	4	2	4	2	1	1	1	5	5	4	5	4	4	5	1	4
8	1	1	3		1	2	2	2	1	4	2	5	3	1	1	1	5	2	3	4	4	3	3	4	4
9	5	1	2	2	1	2	1	2	1	4	1	5	5	1	5	1	1	5	5	3	4	3	4	1	1
10	2	1	2	3	2	3	2	2	3	3	4	5	2	2	4	1	4	4	5	4	5	4	5	1	3
11	3	1	1	3	1	1	1	2	1	4	4	5	1	1	2	1	1	1	2	1	3	3	5	1	1
12	1	1	1	3	1	1	1	2	1	2	2	1	2	1	2	1	1	1	1	1	3	3	2	2	1
13	2	1	1	3	2	3	2	3	1	4	5	5	2	1	3	1	5	5	4	2	4	3	4	2	1
14	2	1	1	2	3		2	1	1	5	4	5	2	1	2	1	5	4	2	1	5	4	4	3	2
15	1	1	1	3	3	3	2	3	1	4	3	3	1	1	4	1	5	3	3	3	3	3	5	1	1
16	4	1	2	3	1	2	2	3	1	4	2	4	2	1	1	1	5	5	4	3	4	4	5	1	2
17	1	1	3	1	1	2	2	1	1	4	2	5	3	1	1	1	5	2	3	3	4	3	3	4	1
18	2	1	2	3	2	3	2	2	3	3	4	5	2	2	4	1	4	4	5	2	5	4	5	1	2
19	1	1	1	3	1	1	1	1	1	4	4	5	1	1	2	1	1	1	2	1	1	2	5	1	1
20	2	1	2	2	2	3	2	3	3	3	4	5	2	2	4	1	4	4	5	2	5	4	5	1	3
21	2	1	1	1	2	3	2	2	3	4	4	5	1	1	2	1	1	1	2	1	1	2	5	1	1
22	2	1	1	3	2	3	2	1	3	3	4	5	2	2	4	1	4	3	5	2	5	4	5	1	2
23	2	1	2	3	2	3	2	2	3	3	4	5	2	2	4	1	4	3	3	1	5	4	5	1	1
24	2	2								4	4	5	1	1	2	1	1	2	2	1	1	2	5	1	1
25	3	1	2	3	1	2	2	3		2	2	1	2	1	2	1	1	2	1	1	1	2	2	2	1
26	2	1	1	3	2	3	2	3	1	4	5	5	2	1	2	1	5	5	4	1	4	3	4	2	1
27	2	1	1	2	3	3	2	1	1	5	4	5	2	1	2	1	5	1	1	1	5	4	4	3	2
28	1	1	1	3	3	3	2	3	1	4	3	3	1	1	1	1	5	3	3	1	3	3	5	1	2
29	4	1	2	3	1	2	2	2	1	4	2	4	2	1	1	1	5	5	4	1	4	4	5	1	1
30	1	1	1	3	1	2	2	2	1	4	2	5	3	1	1	1	5	2	3	3	4	3	3	4	1

Files: Information sheet.doc

Wireless network user security survey.doc

Survey_Data.xls

Survey_Data.pdf

7.2 Appendix B – Device Critique

See companion CD

Files: Device.xml

7.3 Appendix C – Wardriving

See companion CD

Files: wardrive_data.xls

Track.shp

TrackB30.shp

TrackB50.shp

50mNets.shp