Wireless Network Security

Neil Skea
Manoj Maharaj

Abstract

Wireless networking technology opens up a broad range of exciting possibilities for users. Application of technology can help to lower installation costs and time to deploy network infrastructure, can increase productivity and allows for a higher level of flexibility in how people make use of computers in their work and play. There is, however, an inherent information security risk in the use of wireless technology. Wireless signals do not adhere to the containment of walls, fences, wires and other physical constraints. Homes and businesses which host insecure wireless access points open themselves up to a wide range of security threats. To ensure the privacy of transmitted data, all current consumer grade hardware is embedded with various data encryption and protection schemes as a standard feature.

South Africa is currently experiencing tremendous growth in Internet usage and the penetration of broadband technologies in homes and businesses.

This study investigates and assesses the level of application of wireless network security in home and home-office environments – to determine the extent to which adequate security measures have been applied by end-users. Wireless network security can be passively and non-intrusively assessed by means of a wireless audit tool – a system designed to log wireless network signals and their associated security encryption schemes.

Keywords: Wireless Security, Wardriving, Networking

Problem Statement, Objectives and Research Questions

In an article entitled 'How to Secure your Wireless Network' by David Watson (ND), it is noted that although wireless hardware manufacturers provide security features with their products, many hardware vendors disable security features out of the box to ease configuration for end-users. It is conceivable that many end-users make the tacit assumption that the hardware vendors have designed the equipment they are buying with security in mind. Further more, in some circumstances, the possibility exists that security matters are not even considered by end-users when setting up wireless networks. In the same paper by Watson (ND), it is noted that a seven-month security audit conducted in 2002 by the International Chamber of Commerce's Cybercrime Service found that 94% of the 5000 networks audited in central London were completely insecure and could be accessed with little effort.

Homes and businesses which host insecure wireless access points open themselves up to a wide range of security threats. With clear, unobstructed space, a wireless signal may be accessible from more than 500m away from an access point using standard equipment (Williams 2006). Williams also notes that it is possible to detect and connect to wireless networks from further than 500m using readily available, sensitive high gain antennas. According to Posey (2005), in an informal article entitled 'Wireless Network Security for the Home', it is possible to remotely gain unauthorized access to data on computers connected to an insecure network – without the knowledge of the network owner. It is also possible for criminals to make use of unsecured wireless Internet connections to commit crimes and fraudulent activities. Criminal exploitations of wireless networks have been well documented (W1,W2,W3) . Computers can be incidental to a crime (used as storage devices), or can be used as a tool in the commission of a crime (Buys 2004). Traces of these activities by law enforcement agencies lead back to the owner of the Internet connection – and it is difficult to trace further. Owners of insecure wireless networks may find themselves under the spotlight of law enforcement agencies should their networks be compromised and used to commit crimes. It is possible to identify insecure networks through the practice of wardriving.

The practice of wardriving involves the search for wireless networks and the recording of their location and security related attributes (Berghel

2004). People who participate in wardrives often upload their results to Internet-based public databases, an example of which is WIGLE (W4). This is a major security risk for people who run unsecured wireless networks.

This leads to the problem statement for this research: Information regarding the level of application of embedded security features by end-users could prove invaluable to hardware vendors for future designs for wireless equipment. The increasing proliferation of wireless connectivity necessitates a heightened level of security awareness amongst end-users to ensure the confidentiality, integrity and availability of their data and transactions. To facilitate these objectives, there is a need to determine the extent to which adequate security measures have been applied by end-users to their wireless networks.

Hence the objective here is to assess the level of wireless network security to determine the extent to which adequate security measures have been implemented by end-users.

The research question is thus, 'To what extent have wireless application security measures been implemented by end-users to protect their home networks?'

Literature Survey

According to statistics issued by the International Telecommunication Union (ITU) (W6), as of 2008 there are approximately 3 566 000 Internet subscribers in South Africa – 12% (426 000) of these subscribers are connected to the Internet via broadband technologies. Although Internet penetration for the population of South Africa is extremely low at 7,51 subscriptions per 100 inhabitants as of 2008, South Africa is experiencing a mini growth explosion in the number of broadband connections in the country. According to the ITU, South Africa's broadband subscriptions have increased from approximately 60 000 subscribers in 2004 – to 426 000 in 2008 – a growth of 610% in 5 years. According to the Africa development indicators for 2007 as released by the World Bank, 2005 statistics reveal that South Africa as a country in Africa has the third highest penetration of Internet access per 1000 inhabitants – following the Seychelles and Morocco.

Government aided initiatives such as the eThekwini Smart City Project (W8) and the Tshwane Smart City Project (W9) aim to bring greater

connectivity and accessibility to the Internet for South Africans. With the introduction of the Second National Operator, Neotel (W10), South Africa may benefit from increased competition in the telecommunications sector – which may help improve broadband penetration through competitive pricing against the incumbent provider.

With South Africa's winning of the bid to host the 2010 Soccer World Cup, there is increased investment in numerous sectors of the economy to ready the country for the event. Large projects to install undersea fibre optical cables to South Africa, including the SEACOM cable (W11), will dramatically improve the international bandwidth available in South Africa.

In a paper entitled Wireless Infidelity I: War Driving, Berghel (2004) suggests that wireless-networking technologies can be loosely grouped by topology into four categories. Personal Area Networks (PAN), Wireless Local Area Networks (WLAN), Wireless Metropolitan Area Network (WMAN) and Wireless Wide Area Networks (WWANs). Off-the-shelf, consumer grade wireless networking devices are categorised as Wireless Local Area Network (WLAN) equipment. This study concentrates on Wireless Local Area Networks utilised in domestic and small business environments.

Wireless networking technology opens up a broad range of possibilities for end-users, enabling end-users to enjoy the benefits of high-speed network connectivity together with increased mobility. According to Beech and Geelhoed of HP Laboratories (2002), end-user investment in wireless technology is driven by the perceptions of increased mobility, ease of installation and scalability of the technology. Although some users adopt wireless technology with these perceptions in mind, many end users have purchased wireless enabled routers primarily for their broadband functionality – and not specifically to set up a wireless network (Szewcyk 2006). According to Szewcyk, many broadband ADSL modems that are on the market today are supplied with embedded wireless functionality in an attempt to add value to the user experience. The predominant ADSL provider in South Africa, Telkom, provides wireless enabled ADSL modems as part of its package deal for broadband Internet access (W12). In an article entitled 'How to Secure your Wireless Network' by David Watson (ND), it is noted that many wireless network hardware vendors disable security features out of the box, to ease configuration for end users.

There are a wide range of security options available for securing WLAN networks from unauthorised access. These methods can be loosely grouped into authentication methods and encryption methods (Vibhuti 2005).

One of the most primitive of authentication methods is MAC (Media Access Control) authentication which uses a wireless network interfaces card's unique hardware ID to control access. There are numerous tools available that allow a hacker to penetrate this security measure (Vibhuti 2005).

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the two dominant encryption schemes used on wireless 802.11 networks to secure the data transmitted between nodes. There are variants of each of the two schemes: WEP is available with 64bit and 128bit key strength. WPA and WPA2 (a revision of the WPA encryption scheme designed for enterprise networks) can be operated in conjunction with various key rotation and authentication technologies. Wireless encryption schemes are mutually exclusive – you cannot operate more than one of the designated encryption schemes at the same time (Vibhuti 2005).

Technical flaws in both schemes have been amply illustrated by various authors including Mateti (2005), Moen (2004), Watson (2005) and Vibhuti (2005). It is well documented (W26) that it is possible to crack encryption schemes in a laboratory environment and retrieve the key using consumer grade wireless network equipment. Software that is freely available for download from the Internet (W13) can be used on a laptop computer to crack both WEP and WPA wireless encryption keys and gain unauthorised access to a wireless network.

It is possible to remotely gain unauthorized access to data on computers connected to an insecure network – without the knowledge of the network owner (Watson 2005). It is also possible for criminals to make use of unsecured wireless Internet connections to commit crimes and fraudulent activities. Computers can be incidental to a crime (used as storage devices), or can be used as a tool in the commission of a crime (Buys 2004). Traces of these activities by law enforcement agencies lead back to the owner of the Internet connection – and it is difficult to trace further.

Watson (2005) reports that there have been high profile security related incidents involving wireless technology in previous years. In his article entitled 'How to Secure your Wireless Network', Watson cites an

example where wireless cash registers of a US-based consumer electronic giant were found to be operating insecurely. In another example, Watson notes that the closed-circuit camera security system at the Headquarters for the US Defence Information Systems Agency (DISA) was operated and managed via an insecure wireless network – allowing accidental passersby easy access to security footage from the cameras on the network from across the road.

In an informal report by the Durban Wireless Community (Jolley 2007), it was noted that numerous networks operated by professional Wireless Internet Service Providers (WISPs) in Durban operated insecurely – using none of the encryption schemes that are currently available for securing wireless networks. In a paper entitled 'Hacking Techniques in Wireless Networks' by Mateti (2005), techniques to 'sniff' unencrypted wireless network traffic are discussed in detail. Packet sniffing tools allow for the passive interception and logging of network traffic, for example, confidential emails, authentication details and private Internet related traffic. Customers who wish to transact confidentially across these networks should make use of Virtual Private Networks (VPNs), or SSH encryption to secure their data sessions over otherwise insecure networks as this will help to improve the level of security of these transactions. Unfortunately, the possibility exists that many users are not aware of the state of security employed on the WISP networks – and may transmit unprotected, confidential information over these networks not realising the dangers of doing so.

Wireless networks are often setup behind firewalls allowing a user to access the resources of an organization without passing through the organisation's border gateways thus exposing the organization to significant risk (Solms 2004).

Wireless auditing tools are designed for lawful, legitimate purposes (Berghel 2004). Wireless audit tools can be used to help with the control and regulation of output signal strength, monitor bandwidth consumption and plot the coverage patterns and availability of wireless networks. According to Potter (2005) in a paper entitled 'Wireless Vulnerability Assessment', wireless-auditing tools can be used by organisations to manage wireless vulnerabilities. Potter notes that wireless auditing tools could prove

invaluable to organisations that need to monitor for the presence of rogue access points to ensure a high level of network security.

Although wireless auditing tools are designed for lawful purposes, the possibility exists that the information collected by these tools could be used for unlawful purposes (Berghel 2004). From a technology perspective, the tools to perform wireless auditing are the same as the tools that could be used to gain information that could aid a hacker in gaining unauthorised access to a wireless network. One of the solutions to wireless security that presents itself is to raise the awareness of end-users regarding wireless security, the capabilities of wireless auditing tools and the uses to which they are put. End-users who are equipped with this knowledge would be better able to secure their networks from unauthorised access and misuse.

The ethics and legalities regarding the use of computer security assessment tools have been questioned over the past few years. The introduction of Paragraph 202 StGB by German lawmakers prohibits the development, hosting or distribution of computer security assessment tools within the country (W16). Computer security tools such as NMAP (W17) could be used for illegal purposes to gain unauthorised access to computer networks. The ban on security tools encompasses all related security tools – from popular penetration testing tools such as Backtrack (W18) to lesser-known tools including Kismac (W19).

Research Methodology

The practice of wardriving involves the search for wireless networks and the recording of their location and security related attributes. A war driver (person who conducts a wardrive) would utilise a wireless enabled portable computing device (usually a PDA / laptop computer), coupled to a GPS device. Purpose built software such as Netstumbler for Windows (W14) or Kismet for Linux (W15) is used to manage the scanning process and maintain a log file of discovered networks. Wardriving is a passive process – wireless auditing tools utilised in the wardriving process do not actively engage with surrounding wireless access points – and are set to detect (observe) and record network signals which are encountered during the scanning process. People who participate in wardrives may choose to upload their results to public databases that can be accessed via the Internet.

Databases such as WIGLE (W4) allow any registered user to learn the geographic location of any wireless network in the system. As of October 2008, the WIGLE database (W4) contained more than 17 million networks that have been detected and uploaded (site accessed 11 June 2009). This is a major security risk for people who run unsecured wireless networks – it is easy for attackers to learn the location of these networks by simply accessing an online database.

The research instrument used in this investigation was a wireless security-auditing tool - a software program installed on computer hardware to passively capture, log and analyse signals from wireless networks surrounding the user. A wireless security-auditing tool is used while wardriving to capture security related data for wireless networks.

Prior to conducting the wardrive, two routes of approximately 10km each were predetermined by means of a random sampling method. The routes selected are indicated on maps contained in the appendix.

Both of the predetermined routes were analysed on separate days - Monday the 22 of September 2008 and Tuesday the 30th of September 2008. The second drive was selected to fall within school holidays – with the assumption that users may switch off their wireless networks when not in use – during school holidays there is a greater chance that more networks will be available as learners would be at home and may be making use of the Internet.

Three laptop computers were simultaneously utilised as research instruments to detect and log wireless networks while driving the predetermined routes:

- Apple Macintosh Macbook running OSX 10.5 – loaded with KisMac 0.21a to detect networks;
- Apple Macintosh Macbook Pro running OSX 10.5 – loaded with KisMac 0.21a to detect networks; and
- HP Compaq nx8220 laptop running Windows XP Professional – Loaded with Netstumbler 0.4.0 to detect wireless networks. The laptop was connected to a Garmin ETrex GPS to log the location of detected networks. The GPS provides accuracy of results to within 12 meters.

It is important to note the different hardware specifications of the laptop computers selected for the detection and logging of wireless networks for the wardrive. Variances in antenna gain, physical positioning of the internal antennas inside each laptop computer, the wireless chipset and other related factors may contribute to variances in the number of networks detected by each laptop computer and the effectiveness of each as a wireless audit tool. To ensure the maximum number of networks could be detected, multiple laptop computers with differing wireless specifications were utilised. The log files from each of the laptop computers were combined to create a master log file. Wireless access points can be uniquely identified by their MAC address as detected by the wireless auditing tool – allowing for any duplication of network detection to be eliminated.

A Garmin Nuvi 310 was used in addition to the Garmin ETrex in accordance with the predefined rule set to aid the researchers in the event of road closure or obstruction that would require a deviation from the route.

The wireless audit tool revealed the following attributes of each wireless network:

- SSID (Network Name);
- Network BSSID (MAC address of wireless access point);
- The level of encryption employed (None, WEP, WPA);
- The GPS location of the wardrive vehicle at the time the network was discovered;
- Signal strength, data rate configuration and various other technical attributes; and
- The possibility to detect the hardware vendor of the wireless access point by looking up the MAC address in a Hardware Vendor MAC address database – Netstumbler includes this functionality.

The log files from each of the three laptop computers were combined into a master log file that was analysed using Microsoft Excel, KisMac, Google Earth and SPSS.

Earth Stumbler v0.2 (W5) is a free utility that was used to convert the master log file from Netstumbler format to Google Earth KML format. This utility enabled the researcher to generate an additional data layer for Google Earth maps, which contains a distribution of the wireless networks detected.

Data Collection

Paragraph format, Times New Roman 11 pt, single space, justified, 1 cm indented, 6 pt spacing after.

Data Analysis

An understanding of the application of encryption schemes for wireless networks for the wardrive sample provides an insight into the level of security that end-users have implemented for their wireless networks. Figure 1 contains a summary of the application of wireless security schemes of the 234 uniquely identifiable wireless networks as detected during the co-ordinated wardrives of September 2008.

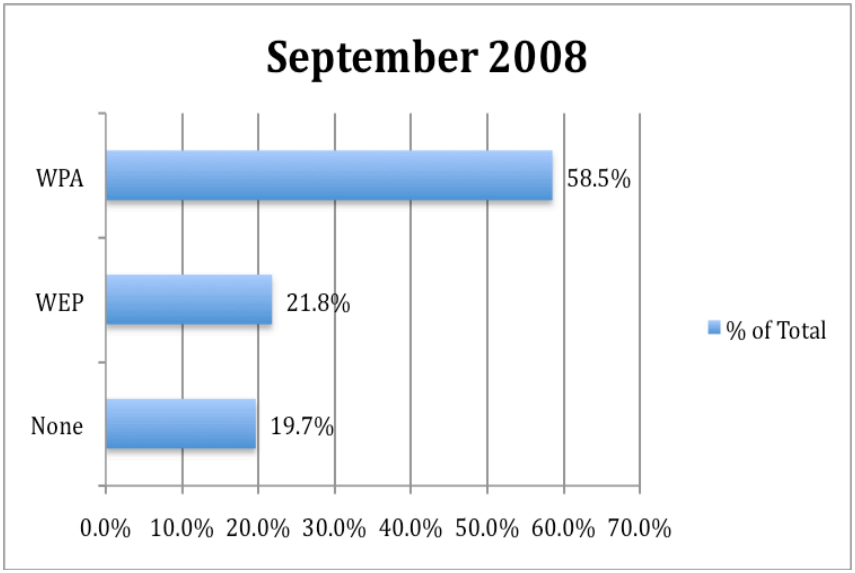

Figure 1: Detected Networks – September 2008

Figure 2 presents data for a wardrive conducted in June 2009 during which 325 unique networks were discovered.

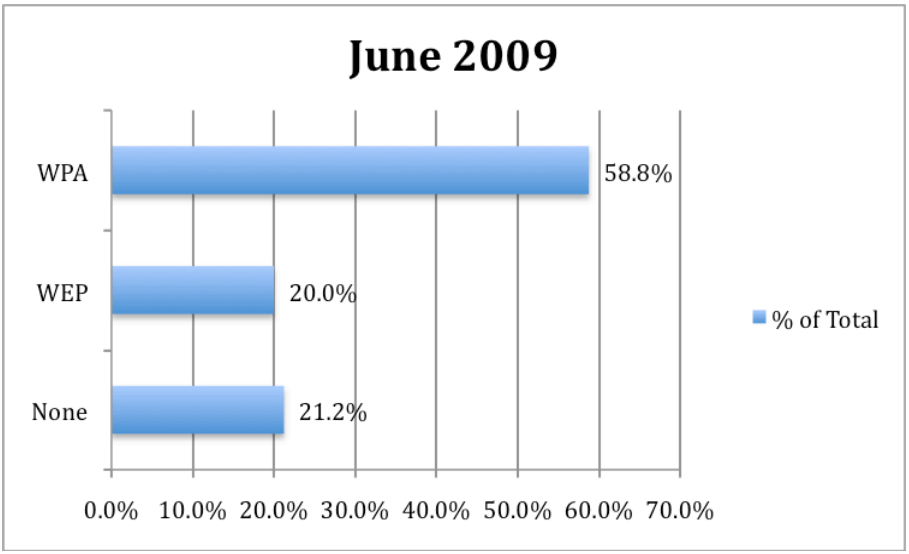

Figure 2: June 2009 Wardrive

The results of wardrives conducted during February 2007, September 2008 and June 2009 are collected in Table 1.

Security Level	June 2009		September 2008		February 2007 (Source: Jolley 2007)	
	Count	% of Total	Count	% of Total	Count	% of Total
None	69	21%	46	20%	293	39%
WEP	65	20%	51	22%	308	41%
WPA	191	59%	137	59%	156	21%
Total Networks	325		234		757	

Table 1: Summary of Detected Encryption Schemes

WEP encryption is considered a poor choice for securing a wireless networks due to the inherent technical flaws in the scheme which have been amply illustrated by various authors including (Mateti 2005), (Moen 2004) and (Vibhuti 2005). According to this definition, approximately 40% of the networks discovered during the 2008 and 2009 wardrives could be considered insecure.

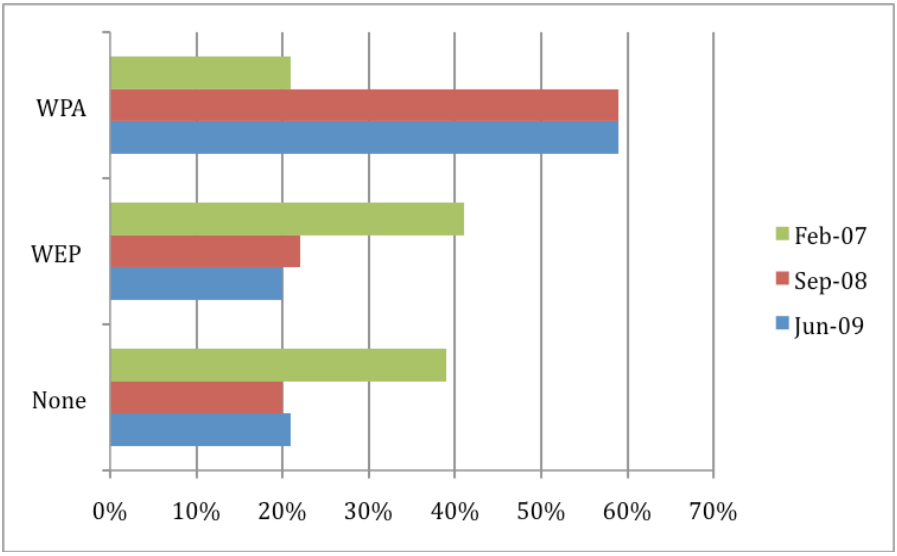

Figure 3: Encryption Schemes

WPA encryption is considered more secure than running an open network, or encrypting traffic using the WEP security scheme, Vibhuti (2005). Data from the September 2008 and June 2009 wardrives reveals a reduction in aggregate use of the WEP encryption scheme relative to the respective samples (41% reduced to 22% and then to 20%), as well as a reduction in the percentage of open networks detected from February 2007 to September 2008.

The results from the coordinated wardrives during September 2008 and June 2009 suggest a significant improvement in the aggregate security configuration of the networks detected when compared with data collected by the Durban Wireless Community in February 2007.

Answers to Research Questions

Results from the wardrives of June 2009 and September 2008, combined with results from the Durban Wireless Community wardrive of February reveal a trend in the application of security schemes by end-users for their wireless networks.

As discussed, WPA is considered a more secure encryption scheme than WEP and is generally accepted as the current benchmark scheme for wireless security (Vibhuti 2005). A comparison of the aggregate results from each of the aforementioned studies reveals an increase in the application of the WPA encryption scheme for end-user wireless networks.

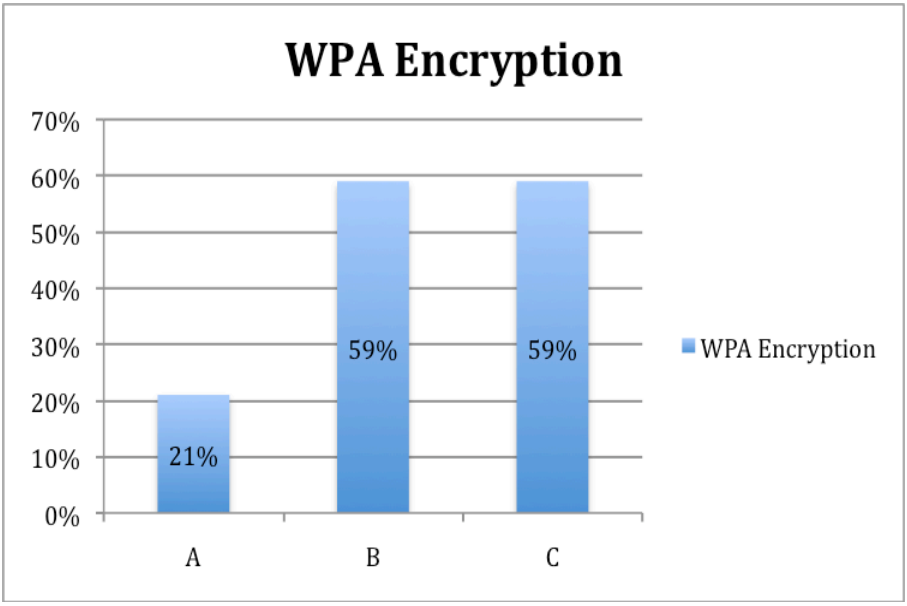

Figure 4: WPA Encryption - June 2009 (C), Sept 2008 (B) and Feb 2007 (A)

A comparison of the aggregated results from each of the aforementioned studies reveals an increase in the application of the WPA encryption scheme for end-user wireless networks. Data from the wardrives conducted by the researcher in September 2008 shows a significant increase

in the percentage of secure networks of the sample compared with historical data. This upward trend would suggest an improvement in the security posture of end-users, as a greater proportion of the sample is using the more secure encryption scheme. Data from the wardrive of June 2009 shows a negligible increase in the percentage of WPA secured networks when compared with September 2008.

As indicated earlier, WEP is considered a weak encryption scheme compared to WPA (Vibhuti 2005). Certain authors including Watson (ND) and Szewczyk (2006) have suggested that WEP encrypted networks should be categorised as insecure networks from a security perspective due to the relative ease with which these networks can be compromised. Converse to the noted increase in the percentage of networks which are secured with WPA, there is a downward trend for the application of the WEP encryption scheme for wireless networks. A comparison of results from the three datasets reveals a downward trend in the application of WEP encryption for wireless networks. There is a decrease from 41% in February 2007 to 22% and 20% detected for September 2008 and June 2009 respectively.

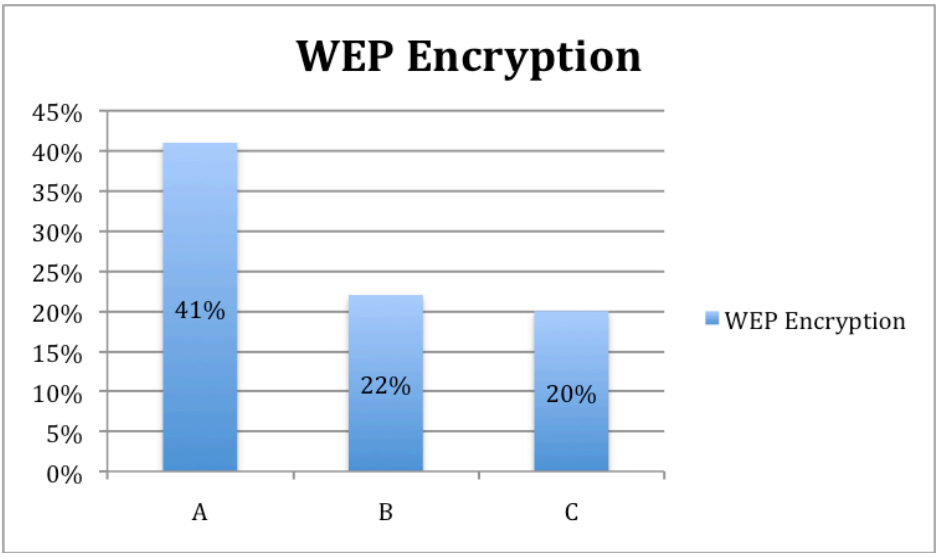

Figure 5: WEP Encryption - June 2009 (C), Sept 2008 (B) and Feb 2007 (A)

The percentage of networks detected which lack WEP or WPA encryption has decreased from 38% in February 2007, to 20% in September 2008. There is a marginal increase (1%) in the number of unsecured networks in June 2009. It is conceivable that a portion of the unsecured (no wireless encryption scheme applied) networks detected may have been intentionally setup in this manner. Wireless hotspots in hotels, restaurants and other areas (especially bed and breakfast establishments) are often configured to operate without WEP or WPA encryption to simplify access for patrons (Vibhuti 2005). This paradigm may explain the 1% increase in unsecured networks as detected in June 2009.

Conclusion

As discussed in the Data Analysis section of this paper, there is a general improvement in the security posture of wireless networks from February 2007 to June 2009. Penetration of the WPA encryption scheme has increased from 21% to 59% in just over two years. The percentage of unsecured networks has dropped from 39% to 21% in the same timeframe. WEP secured wireless networks have decreased from 41% to 20% from 2007 to 2009. It is conceivable that the remaining WEP secured networks detected during 2009 are comprised from older network hardware – the majority of modern wireless access points are either unsecure by default, or force the end-user to apply WPA encryption before enabling the service (Vibhuti 2005), or alternatively, as indicated earlier, are left open intentionally. It is expected that as this hardware is upgraded in the coming years, the utilization of the WEP encryption scheme will tend to zero, as WEP is generally more difficult to configure from the usability point of view and is less secure than WPA.

Wireless networking technology serves as a powerful enabler for mobility. However, there are inherent information security risks associated with the use of this technology. It is of utmost importance that wherever possible, wirelessly transmitted data is secured by means of an encryption scheme to ensure the confidentiality and integrity of a transmission, as well as to prevent network resources from being accessed by unauthorized users.

It is important to note some of the SSIDs (text based, user defined identifiers for wireless networks) detected during the wardrive were set to

values that could reveal sensitive information about the network owner or the network itself, thus compromising security. Individuals who use their home addresses, first names, surnames or any other personally identifiable information for naming their wireless networks are essentially providing data that could be used in an exploit by a social engineer. Social engineering is the art of manipulating people into performing actions or divulging confidential information (Powers 2006). It is therefore recommended that end-users choose SSIDs that do not reveal personal information about the network owner of the network itself.

The 2010 Soccer World Cup in South Africa has resulted in an associated influx of people and an increase in online commercial transactions. It is of utmost importance that security is considered while planning the expansion of computer networks – in homes, businesses and government. The explosive growth of broadband technologies in South Africa, combined with the low levels of computer education and technical skill could result in South Africans becoming targets for computer based crimes. End-users need to be security conscious to protect their data and transactions – especially when making use of wireless technology.

References

Beech, S L & E Geelhoed 2002. User Attitudes towards Wireless Technology. Accessed on 12 October 2008 at: http://www.mobilebristol.com/PDF/Intro/2002-04.html.

Berghel, H 2004. Wireless Infidelity I: Wardriving. 1 Accessed on 2 October 2008 at http://portal.acm.org/citation.cfm?id=1015879.

Buys, R 2004. *Cyberlaw - The Law of the Internet in South Africa.* Second Edition. Pretoria: Van Schaik Publishers.

Jolley, D 2007. Durban Wireless Community Wardrive Results. 10 October 2008, http://www.dwc.za.net.

Mateti, P 2005. Hacking Techniques in Wireless Networks. Accessed on 8 October 2008 at: http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.doc.

Moen, V & H Raddum 2004. Weaknesses in the Temporal Key Hash of WPA. Accessed on 1 October 2008 at: http://portal.acm.org/citation.cfm?id=997132.

Posey, B 2005. Wireless Network Security for the Home. Accessed on 3 October 2008 at: http://www.windowsecurity.com/articles/Wireless-Network-Security-Home.html?printversion.

Potter, B 2005. Wireless Vulnerability Assessment. Accessed on 3 October 2008 at: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJG4GHB78C_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=f7ee561c1e401163766611aea217a008.

Solms, B 2004. From Secure Wired Networks to Secure Wireless Networks - What are the Extra Risks? Accessed on 29 September 2008 at: http://adam.rau.ac.za/~basie/PDF/sdarticle8.pdf.

Szewczyk, P 2006. *Individuals' Perceptions of Wireless Security in the Home Environment.* Perth: SCISSEC & Edith Cowan University.

Vibhuti, S 2005. IEEE 802.11 WEP Wired Equivalent Privacy Concepts and Vulnerability. Accessed on 29 September 2008 at: http://www.cs.sjsu.edu/faculty/ stamp/CS265/projects/Spr05/papers/WEP.pdf.

Watson, D n.d. How to Secure your Wireless Network. Accessed on 30 September 2008 at: http://www.sciencedirect.com/science?_ob=ArticleURL udi=B6VJG46F4CH79&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=9b5348133d8d11cc5bcc41017a53a8c2.

Williams, P 2006. Cappuccino, Muffin, WiFi - But What about Security? Accessed on 30 September 2008 at: http://www.sciencedirect.com/science?_ob= articleURL&_udi=B6VJG4M59H08&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=741bb0b08fbbc64c7f2893a03994ccbb.

No	Reference	Date Accessed
W1	http://news.cnet.com/Wi-Fi-arrest-highlights-security-dangers/2100-1039_3-5112000.htm	27 October 2008
W2	http://www.securityfocus.com/print/news/7438,	28 October 2008
W3	http://www.theregister.co.uk/2005/08/19/finnish_wifi_bank_hack/print.html	28 October 2008
W4	http://www.wigle.net	28 October 2008
W5	http://mboffin.com/earthstumbler/	21 October 2008
W6	http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#,	22 October 2008
W7	http://www.worldwideworx.com/	22 October 2008
W8	http://smartcitydurban.wordpress.com/2008/09/08/imagine-durban-smart-city-accessible-city/	27 October 2008
W9	http://www.iweek.co.za/ViewStory.asp?StoryID=176345	27 October 2008
W10	http://www.neotel.com	27 October 2008
W11	http://www.southafrica.info/business/economy/infrastructure/seacom-150808.htm,	27 October 2008
W12	http://www.telkom.co.za/products_services/dsl/index.html,	28 October 2008
W13	http://www.darknet.org.uk/2008/01/backtrack-live-hacking-cd-beta-3-released	02 October 2008
W14	http://www.netstumbler.com	29 October 2008
W15	http://www.kismetwireless.net	29 October 2008
W16	http://www.heise-online.co.uk/security/Germany-passes-Anti-Hacking-laws--/news/90255,	20 October 2008
W17	http://www.nmap.org	20 October 2008
W18	http://www.darknet.org.uk/2006/02/backtrack-a-merger-between-whax-and-auditor/	20 October 2008
W19	http://www.kismac.de	20 October 2008

Neal M. Skea
University of KwaZulu-Natal
neilskea@gmail.com

Manoj S. Maharaj
University of KwaZulu-Natal
maharajms@ukzn.ac.za