Wireless Network Security

DETAILS:

NAME: UMMADISETTY VAISHNAVI

REGNO OF SMART INTERNZ:SBAP0007267

EMAIL ID:21B05A0426@SVECW.EDU.IN

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
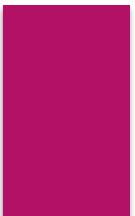feature.

OBJECTIVES

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.

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

- 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 .

Research Methodology

The practice of wardriving involves the search for wireless networks and therecording 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.

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.

DATA

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 .
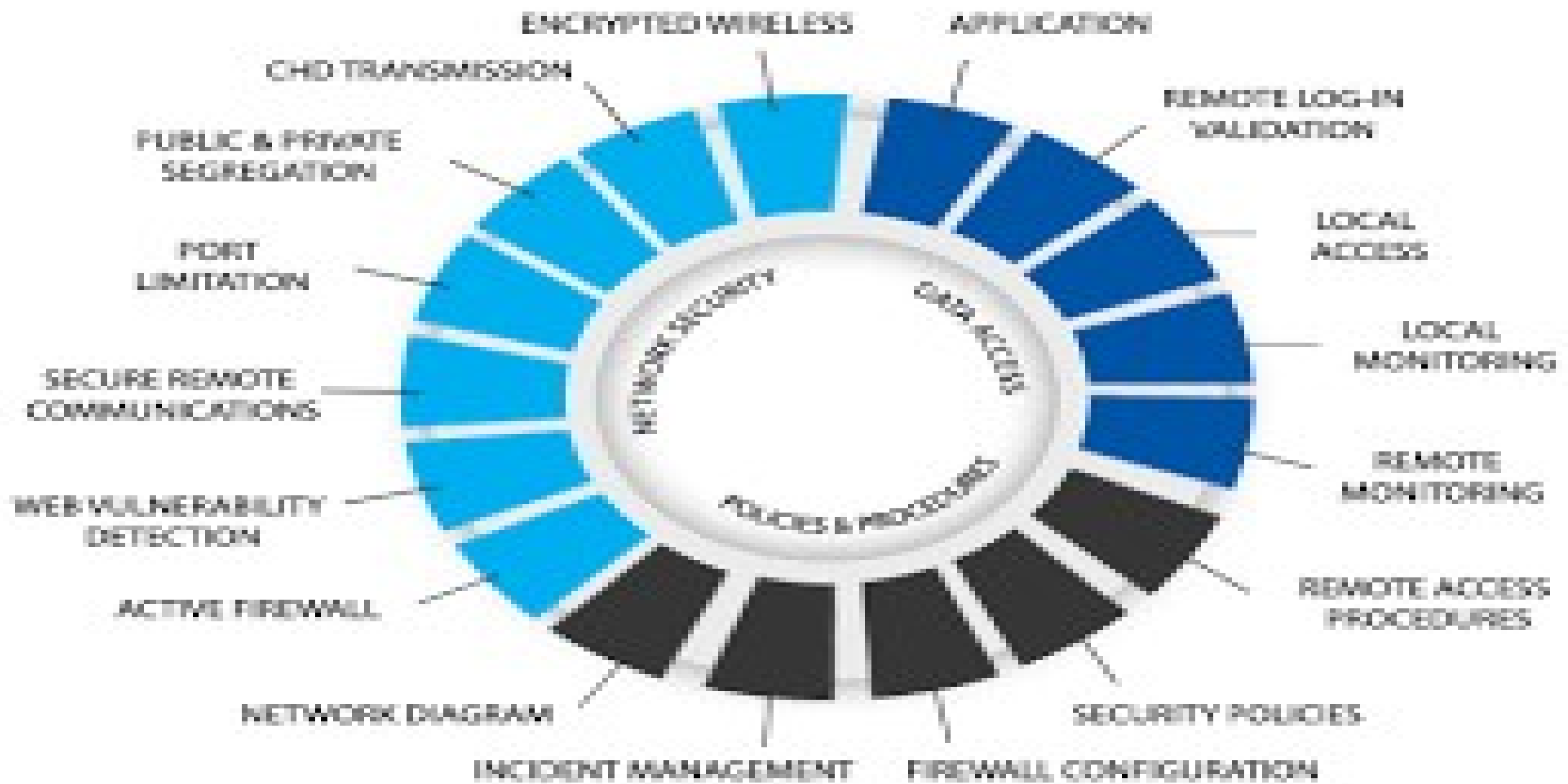
Executive Level Response Chart
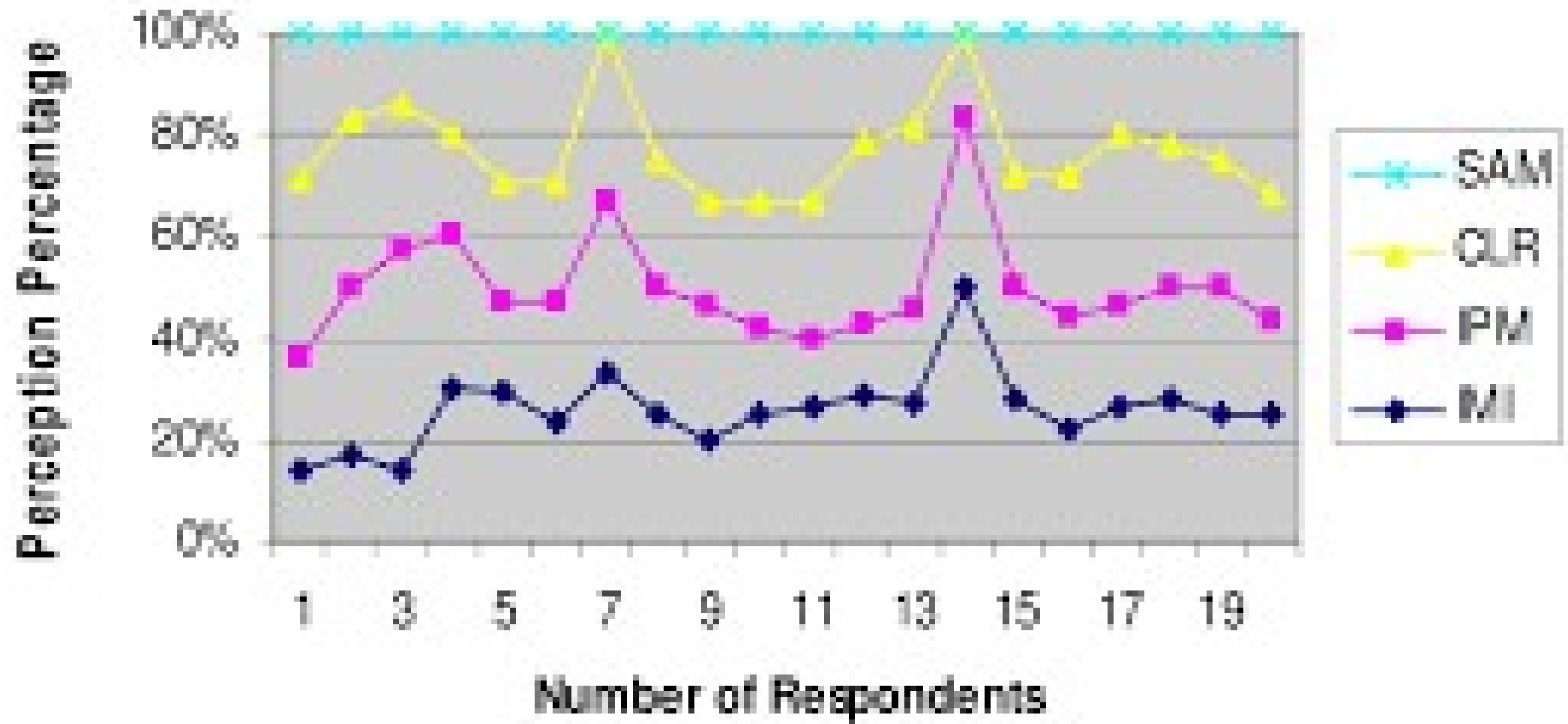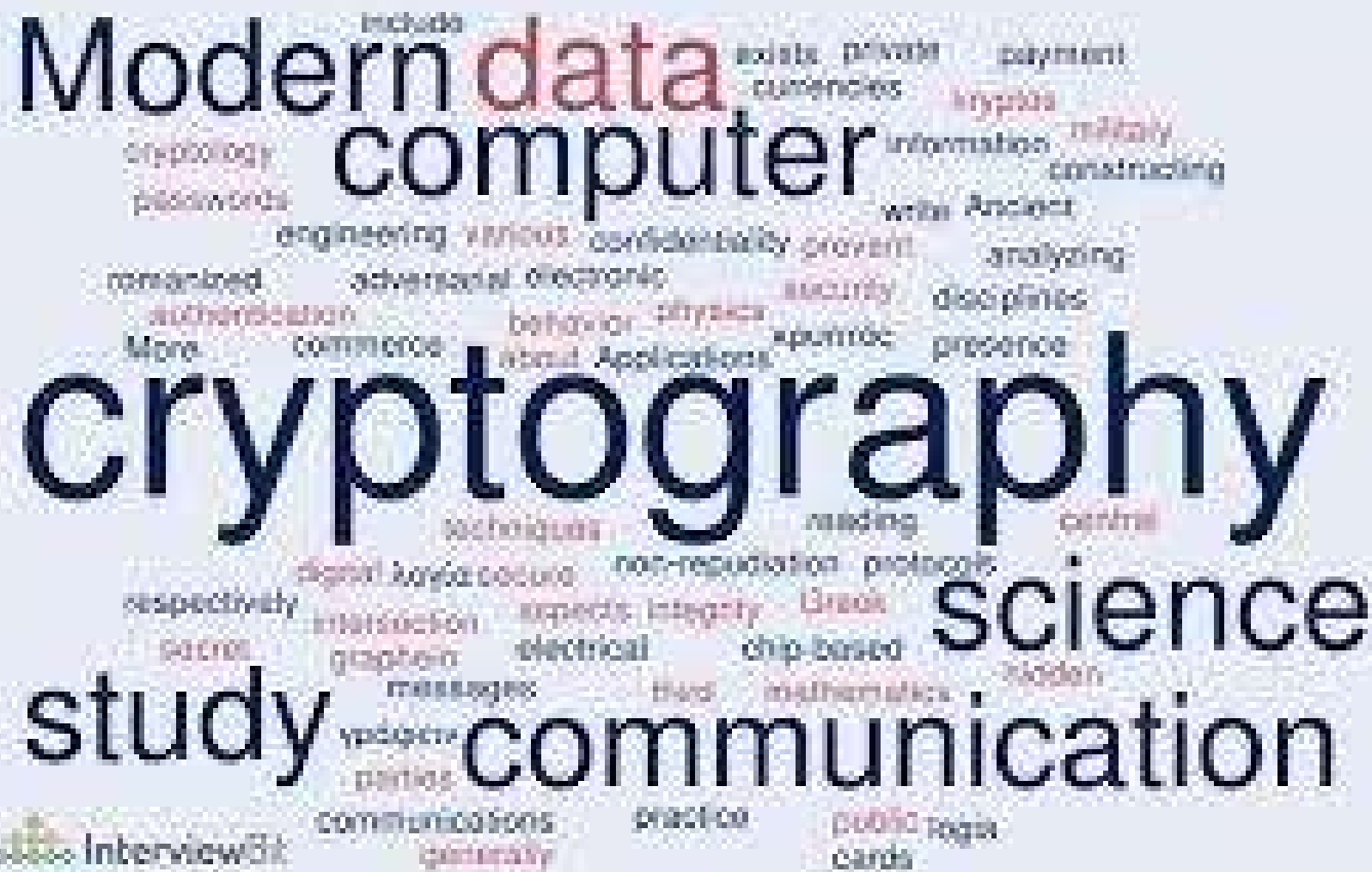
Advantages & Disadvantages

- ▶ **Freedom from wires:** Can be configured with the use of any physical connection.

- ▶ **Easy to setup:** Wireless network is easy to expand and setup

- ▶ **Better or global coverage:** It provides global reach by providing networking in places such as rural areas, battlefields, etc... where wiring is not feasible.

- ▶ **Flexibility:** Wireless network is more flexible and adaptable compared to a wired network.

- ▶ **Cost-effectiveness:** Since it is easy to install and doesn't require cables, the wireless network is relatively cheaper.

- ▶ **Mobile and portable:** Wireless network is easy to carry and re-install in another place.

- ▶ As communication is done through open space, it is less secure.

- ▶ Unreliability

- ▶ More open to interference.

- ▶ Increased chance of jamming.

- ▶ Transmission speed is comparably less.

- ▶ it has a limited amount of bandwidth for communication and breaches of network security.

- ▶ Wireless networks require a careful radio frequency when they are installed.

Wireless Network Applications

▶ Basic Configurations. In most cases, the wireless network is merely an extension of an existing wired network. ...

▶ Internet Access. ...

▶ Voice over Wireless. ...

▶ Inventory Control. ...

▶ Health Care. ...

▶ Education. ...

▶ Real Estate. ...

▶ Utilities.

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.

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.

Future scope

In developed countries, new wireless network tech will make transferring data faster, more reliable and more secure. It will also enable new data-hungry technologies like IoT, VR and even holograms. IoT has already started to take hold but has a much larger potential than is being expressed today.