WIRELESS SECURITY TOOLS

Johanna Janse van Rensburg, Barry Irwin

Rhodes University
G01j202j7@campus.ru.ac.za,
b.irwin@ru.ac.za
(083) 944 3924
Computer Science Department, Hamilton Building, Rhodes University 6139

ABSTRACT

The security concerns of 802.11 wireless networks have gained extensive attention over the past couple of years. With the introduction of the 802.11i standard the cryptographic side of the security was significantly improved. However it is not just the technology that ensures a secure wireless network. These networks are still vulnerable to attacks, for instance DOS attacks which affects the availability of the wireless network. As with a wired LAN, security is not a once off implementation but an ongoing procedure. Auditing must be done on a regular basis to asses the performance and security of these networks. From a security perspective auditing helps the administrator to detect unauthorized, negligent and unsolicited behaviour.

Even though the 802.11i standard has been available for almost two years; people still do not understand it and some institutions choose not to deploy it, because they might not need a high level of security. These institutions are subject to wireless security vulnerabilities that have been known for a while. Auditing is a necessity to these institutions. This paper discusses and evaluates proprietary and free software used to aid in mapping, analysing, securing and auditing a wireless network. The role each tool performs will be categorised into the functionality it achieves. For example, AirWave, mainly used to detect rogue access points, provides centralized monitoring by using the existing infrastructure to detect rogue unauthorized access points. Yet another unusual concept to protecting a wireless network from wardrivers is to hide a legitimate access point amongst thousands of fake access points. Fake AP, is a software tool which generates thousands of access points by sending out a multitude of beacon frames.

A second aim of this paper is to discuss the visualization of wireless audit data. For example, sniffing tools like Kismet and KismetEarth, a tool which plots GPS Kismet data visually on a GoogleEarth map. This map may be used to display all wireless networks in a town or city. Visualization tools can give the administrator a picture of the foot-print of the signal outside the organization. Another proprietary tool is AirMagnet which graphically depicts signal strength based on the floor plan of the building. These tools will be discussed in terms of their functionality with the aim to provide the network administrator with a holistic view of the status of the security and performance of a wireless network. This will aid the network administrator in maintaining a secure and reliable network.

KEY WORDS

WLAN Security, Tools, Audit

WIRELESS SECURITY TOOLS

1 INTRODUCTION

With the popular growth of WLANs a diverse set of tools has been developed specifically for 802.11 networks. WLANs differ from wired LANs in the physical and data link layer. Because of this, new challenges have been encountered in WLANs and innovative tools have been written to meet these challenges. They exist to carry out different functions and ultimately improve the manageability of a WLAN and provide control over the WLAN.

Wireless tools can perform any of the following functions:

- Wi-Fi Discovery Tool
- Raw Packet Capture Tool
- Traffic Analyzer
- Monitoring Tools
- Visualization tools
- Auditing
- Security

In the following sections a few tools that perform these functions are introduced.

2 SECURITY

In this section a look will be taken at some of the wireless hacking tools which exploit the vulnerabilities found in WEP and WPA.

2.1 Fake AP

Fake AP attempts to provide security through obscurity. It generates fake 802.11b access points, by sending out hundreds of beacon frames; confusing wardrivers and enabling the valid Access Point (AP) to hide between the fake access points [17]. However it is still possible to find the valid access point by looking at the *Packets* and *Size* field in Kismet as these will be low for the fake APs. An improvement has been written which inject 802.11 packets for the created ESSID's [14]. Fake AP can also be used maliciously, by confusing a rogue AP detection system. It could serve as another security layer.

2.2 AirCrack

AirCrack consist of a collection of tools to perform packet capture, WEP and WPA-PSK (Pre Shared Key) cracking and packet injection. It consists of the following programs [2]:

- airodump: 802.11 packet capture program
- aireplay: 802.11 packet injection program
- aircrack: static WEP and WPA-PSK key cracker
- airdecap: decrypts WEP/WPA capture files

In 2005 at an Information Systems Security Association (ISSA) conference given in Los Angeles [1], a team of FBI agents used AirCrack to crack a WEP encryption as a demonstration. It could require anything from 300 000 IV's for 40bit WEP to 1 million IV's for 104bit WEP [1]. It might take a whole day to capture the traffic, by using aireplay to inject packets into the network and generate traffic, this can be decreased to a few hours [1]. AirCrack can be run on both Windows and Linux [2].

To perform a WPA-PSK crack a 4 way-handshake need to be captured. This can be done by forcing clients to re-authenticate by sending de-authentication messages to the AP with aireplay. Once a 4 way-handshake has been found the master key can be found by performing a dictionary attack with aircrack [2].

802.11 management and control frames are not protected, which result in DOS vulnerabilities [22]. For example an adversary can flood the WLAN with associate messages, which will prevent any other host from sending data or connecting to the AP [2]. Alternatively if strong authentication is not provided an adversary can spoof itself as a valid access point, force a client to disconnect from a valid AP, and connect to the false AP.

2.3 Void11

Void11 generates association, de-authentication and authentication messages. De-authentication messages will force clients to drop their packets. A flood of authentication and association messages will cause clients to back-off which could result in a Denial of Service (DOS)[3].

2.4 coWPAtty

coWPAtty is a brute-force cracking tool [5]. The weakness of WPA is that it provides the option to use a Pre Shared Key (PSK) for Small Office Home Office (SOHO) users. Even though the password at no time get send across the network the process for generating the password can be duplicated. Furthermore all the required data fields to do this can easily be obtained. This tool exploits that specific weakness as it attempts to crack a password by comparing it to a dictionary. However it is not as simple as that, because the password is hidden beneath a few levels of algorithm. Therefore in order to compare the guessed password to the caught hash, all these algorithms need to be executed. This decrease the speed at which a password can be cracked, but easy passwords could be identified in a reasonable time. In order to perform the attack an EAP four-way handshake, password list and the SSID is required [5].

With the aid of this tool an audit can be done on a WLAN which implements WPA-PSK to find the weak passwords.

2.5 Audit

Wireless Audits are a recommended best practice by SANS [16]. Part of an audit involves discovering all access points in a specific area, then capturing some packets and analyzing them. Conducting an audit is similar to the procedures that an adversary would follow to find weaknesses in a WLAN. Therefore Kismet is used successfully by both wardrivers and auditors. Kismet is a multi-purpose tool which can serve as a Wi-Fi Discovery Tool, Raw Packet Capture Tool, Traffic Analyzer and Auditing tool. In this section Kismet will be discussed from the perspective of WLAN audit.

Kismet is a passive sniffer which scans the airwaves by hopping to all the channels to find the available 802.11b devices and some relevant data like the signal strength and signal-to-noise-ratio (SNR). Because it is a passive sniffer it can locate hidden SSIDs, sniff all management packets for a wireless network and discover the IP range used for the WLAN [15].

Once the data has been collected it must be analysed. From the data, network intrusions and interfering neighbouring access points can be identified [15]. Packets can be inspected to ensure that they are indeed using the selected security implementation, for example the particular EAP algorithm. Furthermore a list of the peripheral devices connected to the wireless network can be obtained. Keeping track of these is important as many peripheral devices support wireless. This feature might be switched on unintentionally, and this device can be accessed from outside the perimeters of the premises.

Rogue clients connected to the network can be seen from Kismet data [4]. Even with 802.11i rogue access points are a problem, one example is the case of a neighbouring company with an insecure access point. Employees might be able to surf the Internet using that AP and receive an IP address from the neighbouring DHCP server. This will create networking conflicts on the client machines and hamper their access to network resources to do their work [4].

WLAN security technologies like WEP, WPA, VPN and 802.11i are used to secure a WLAN. Most of the tools investigated in this section are not tools that provide security, but aid in the maintenance of the security of a WLAN.

3 VISUALIZATION

Several software packages exist to provide a visualization of a wireless network using radio propagation techniques. A few of the proprietary visualization packages are Ekahau, AWE-Communications and Airmagnet [6, 12, 18]. To date a non-proprietary package with similar quality does not exist. Although packages like Radio Mobile, a non-proprietary visualization package, work on similar principles [19]. These packages aid in the design and auditing phases of a wireless network. From a security perspective a visualization package can provide a visual footprint of a wireless network as depicted in Figure 1. With this, the signal spill of a network can be viewed. The Ekahau and AirMagnet packages have the ability to locate and display rogue access points on a map [6,12].

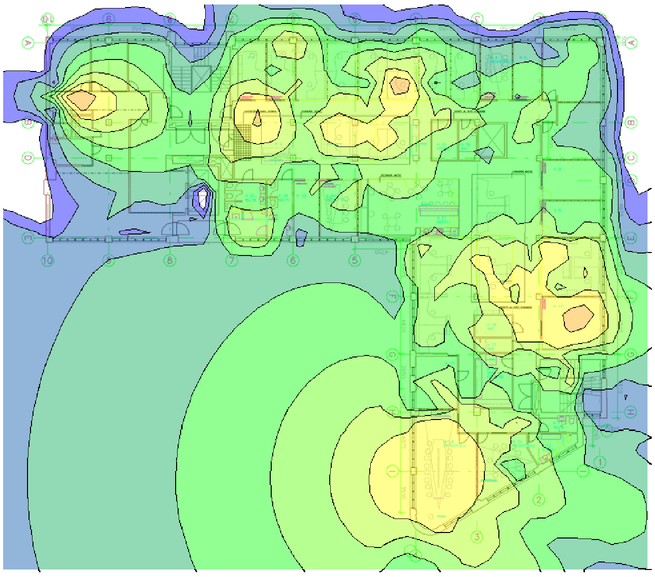


Figure 1 Signal Footprint, Yellow are strongest and different shades of green are less strong [6]

3.1 Kismet Earth

Kismet Earth is a php script which display WLAN information on a Google Earth map. It parses Kismet .xml and .gps files, to get the networks and coordinates to create a KML file which are used to map everything to Google Earth [13]. The following output gets generated [13]:

- Network icons at specific location with full description (SSID, BSSID, channel, encryption, clients, vendor info, etc.)
- The WarDrive path taken as depicted in Figure 2.
- A 3D visualization of a network's range, if enough GPS points have been captured

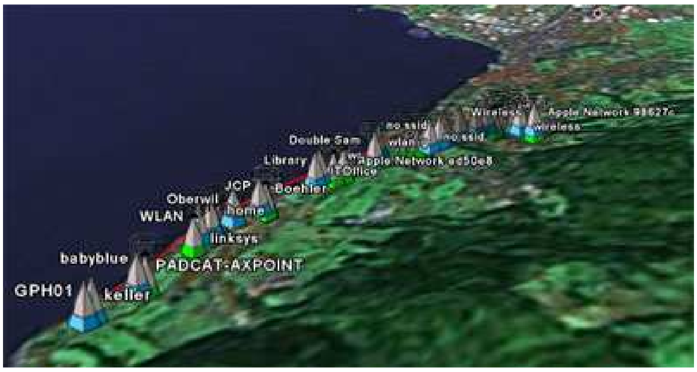


Figure 2 The Wardrive path taken with wireless networks found along the way [13]

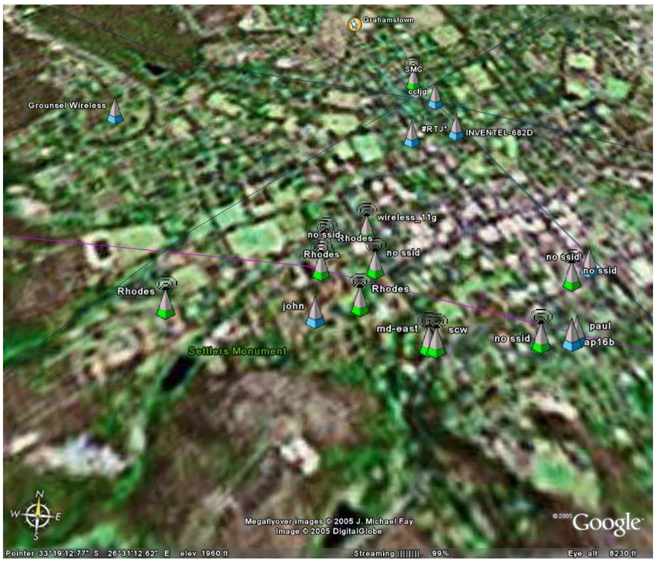


Figure 3 A Google Earth Map of some wireless networks found in Grahamstown, the blue ones have WEP enabled, the green indicates no encryption

Kismet Earth can be seen as both a wireless network discovery tool and a visualization tool. It provides a view of the exact position of wireless network activity in a city or a specific area as can be seen in Figure 3 [13]. The only drawback is that the quality of the picture depends on that provided by Google Earth.

3.2 Rogue Access Point Detection

Even though 802.11i protect clients from connecting to rogue APs many clients cannot implement 802.11i and are hence vulnerable to rogue APs. Therefore it is still necessary to perform rogue access point detection.

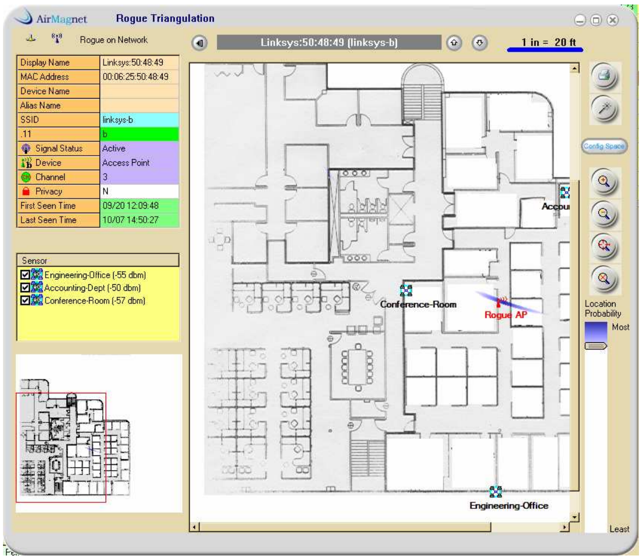
The main problem with using Kismet to detect rogue access points is that it is too intermittent to continuously protect a network from rogues. Active rogue access point detection is necessary to detect them before they can do any real damage [8]. AirWave and WiFi Manager are two proprietary packages which performs rogue access point detection [7, 20].

A number of ways exist to detect and remove rogue access points. Probes may be installed in various locations on the site which continuously monitors all 802.11 traffic. However this might prove to be an expensive option [8].

Another option is to use the existing access points to detect neighbouring access points. Not all access points possess this ability. The access points are limited to its coverage area to detect the rogues and access points operating outside it will be overlooked [7]. Proxim access points have this ability [8].

Alternatively wireless network management software can use protocols like, SNMP or Telnet to discover access points on the LAN. The discovered access points will need to be compared to a list of valid access points. These can be identified by their MAC, SSID, Vendor and Channel. If an invalid AP is discovered, its MAC address can be blocked on the port it uses in the switch [7].

As mentioned earlier the Ekahau and AirMagnet packages have the ability to locate and display rogue access points on a map of a floor-plan. In Figure 4 the exact location of the rogue access points are shown.



Display Name	Linksys:50:48:49
MAC Address	00:06:25:50:48:49
Device Name	
Alias Name	
SSID	linksys-b
.11	b
Signal Status	Active
Device	Access Point
Channel	3
Privacy	N
First Seen Time	09/20 12:09:48
Last Seen Time	10/07 14:50:27

Sensor
☑ Engineering-Office (-55 dbm)
☑ Accounting-Dept (-50 dbm)
☑ Conference-Room (-57 dbm)

Figure 4 –AirMagnet uses triangulation to locate Rogue Access Points [12]

4 REPORTING

None of the non-proprietary tools provide reporting functionality, however some of the proprietary software mentioned earlier do. Useful information provided by these tools includes [12]

- Security Alarms Detected – These alarms could include clients using open communication, disabled WEP, DOS RF Jamming attack.
- Rogue Access Points – A list of these and their locations.
- Utilization of Access Points – An analysis of the usage percentage on access points.
- Utilization of Channels - An analysis of the usage percentage on channels.
- Access Point Configurations – A report which list the access point configuration of each AP.
- Performance Alarms

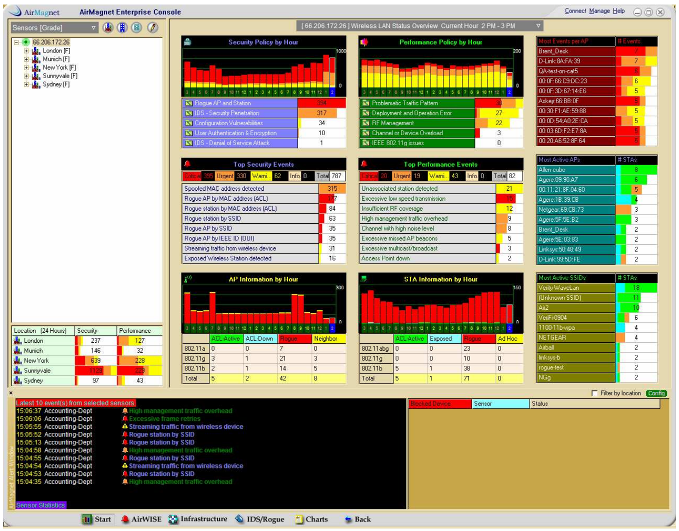
These reports provide the administrator with a holistic view of the activity of a WLAN. These can aid the administrator to make critical decisions on the configuration of Access Points.

5 USING THE TOOLS

Once a WLAN has been deployed the above tools can aid to maintain the security of the WLAN and to adhere to the security policy. Several proprietary and non-proprietary tools were introduced in this paper which can aid to achieve this; however proprietary tools provide a more mature solution for the complete management of the WLAN.

The cracking tools like coWPAty and AirCrack can be used to identify weak passwords on a WLAN [5].

By using a scanning tool like Kismet a snapshot of the wireless activity in the WLAN area can be obtained. It provides the administrator with a view of the information a wardriver will see. The data collected by Kismet can be plugged into Kismet Earth, which will provide a geographical plot of the wireless networks detected [13]. The problem with using Kismet is that the auditing is done intermittent [8]. An approach is needed which provides continuous monitoring of the status of the WLAN. This is necessary to provide the administrator of unusual activity when it occurs. For example a threshold might be set for the AP; once this threshold is reached the WLAN administrator will be informed. Analysing the Kismet data is manually done by the WLAN administrator, which is a time-consuming task. Reporting analyses and categorises the data in an easy to understand format. For example some useful info would be to list the top security events by the hour. Figure 5 is a picture taken from AirMagnet that lists some useful information. Note that all this information can be obtained at one glance of the screen.



Location (24 Hours)	Security	Performance
London	237	127
Munich	146	32
New York	639	228
Sunnyvale	1129	229
Sydney	97	43

Security Policy by Hour	
Rogue AP and Station	394
IDS - Security Penetration	317
Configuration Vulnerabilities	34
User Authentication & Encryption	10
IDS - Denial of Service Attack	1

Performance Policy by Hour	
Problematic Traffic Pattern	30
Deployment and Operation Error	27
RF Management	22
Channel or Device Overload	3
IEEE 802.11g issues	0

Most Events per AP	# Events
Brent_Desk	7
D-Link:8A:FA:39	7
QA-test-on-cat5	6
00:0F:66:C9:DC:23	6
00:0F:3D:67:14:E6	5
Askey:66:BB:0F	5
00:30:F1:AE:59:88	5
00:0D:54:A0:2E:CA	5
00:03:6D:F2:E7:8A	5
00:20:A6:52:8F:64	5

Top Security Events

Critical 395 Urgent 330 Warni... 62 Info. 0 Total 787

Spoofed MAC address detected	315
Rogue AP by MAC address (ACL)	177
Rogue station by MAC address (ACL)	84
Rogue station by SSID	63
Rogue AP by SSID	35
Rogue AP by IEEE ID (OUI)	35
Streaming traffic from wireless device	31
Exposed Wireless Station detected	16

Top Performance Events

Critical 20 Urgent 19 Warni... 43 Info. 0 Total 82

Unassociated station detected	21
Excessive low speed transmission	15
Insufficient RF coverage	12
High management traffic overhead	9
Channel with high noise level	8
Excessive missed AP beacons	5
Excessive multicast/broadcast	3
Access Point down	2

Most Active APs	# STAs
Allen-cube	8
Agere:09:90:A7	6
00:11:21:8F:04:60	5
Agere:1B:39:CB	4
Netgear:69:CB:73	3
Agere:5F:5E:B2	3
Brent_Desk	2
Agere:5E:03:83	2
Linksys:50:48:49	2
D-Link:99:5D:FE	2

	ACL-Active	ACL-Down	Rogue	Neighbor
802.11a	0	0	7	0
802.11g	3	1	21	3
802.11b	2	1	14	5
Total	5	2	42	8

	ACL-Active	Exposed	Rogue	Ad Hoc
802.11abg	0	0	23	0
802.11g	0	0	10	0
802.11b	5	1	38	0
Total	5	1	71	0

Most Active SSIDs	# STAs
Verity-WaveLan	18
(Unknown SSID)	11
Air2	10
VeriFi-0904	6
1100-11b-wpa	4
NETGEAR	4
Airball	2
linksys-b	2
rogue-test	2
NGg	2

```
Latest 10 event(s) from selected sensors
15:06:37 Accounting-Dept    High management traffic overhead
15:06:06 Accounting-Dept    Excessive frame retries
15:05:55 Accounting-Dept    Streaming traffic from wireless device
15:05:52 Accounting-Dept    Rogue station by SSID
15:05:13 Accounting-Dept    Rogue station by SSID
15:04:58 Accounting-Dept    High management traffic overhead
15:04:55 Accounting-Dept    Rogue station by SSID
15:04:54 Accounting-Dept    Streaming traffic from wireless device
15:04:53 Accounting-Dept    Rogue station by SSID
15:04:35 Accounting-Dept    High management traffic overhead
```

Blocked Device	Sensor	Status

Figure 5: Report of activities on the WLAN [12]

From a security perspective this is what a WLAN administrator needs to maintain the security and availability of a WLAN.

6 CONCLUSION

Wireless networks have gained extensive attention over the past couple of years and will continue to do so as new standards are introduced, making them more powerful and resulting in new implementations. As a result of this research many wireless software tools have been developed. A few of these tools was introduced in this paper with the focus on the functionality they achieve. However many more similar packages which provide similar functionality exist. The aim is to provide the reader with an introduction of the type of tools available; all of which can aid in the management of a WLAN and can be used to enforce the wireless policies of an organisation.

7 REFERENCE:

[1] H. Cheung. FBI Teaches Lesson In How To Break Into Wi-Fi Networks http://www.compliancepipeline.com/160502612. April 2005

[2] C Devine. Aircrack Documentation http://www.wirelessdefence.org/Contents/AircrackORIGINAL.html April 2006

[3] Void11. http://www.wirelessdefence.org/Contents/Void11Main.htm April 2006

[4] B. M. Posey. Make a robust wireless audit of your network with Kismet http://techupdate.zdnet.com/techupdate/stories/main/robust_wireless_audit_Kismet.html?tag=tu.tk.7901.f4 November 18, 2003

[5] S. Fogie. Cracking Wi-Fi Protected Access (WPA) http://www.informit.com/articles/article.asp?p=369221 March 2005

[6] Ekahau Site Survey Report. http://www.ekahau.com/ss/report/ April 2006

[7] ManagEngine WiFi Manager 4.3, Rogue Access Point Detection, http://manageengine.adventnet.com/products/wifi-manager/rogue-access-point-detection.html. April 2006

[8] Proxim – rogues

[9] M. Bialoglowy. "Bluetooth Security Review, Part1." SecurityFocus. <http://www.securityfocus.com/infocus/1836>. 2005.

[10] J. Wrolstad. Mabir Smartphone Virus Targets Symbian-Based Mobile Phones http://www.contact-center-today.com/ccttechbrief/story.xhtml?story_id=32327 April 2005

[11] McAfee, SymbOS/Mabir.a!sis. http://vil.nai.com/vil/content/v_132804.htm May 2005

[12] Airmagnet. http://www.airmagnet.com/products/reporter_samplereports.htm April 2006

[13] Kismet Earth home page. http://www.niquille.com/2005/09/24/kismet-earth-v01/ April 2006

[14] N Suri , A Thompson, J Torok and B Waite. Fake AP Tested Compiled and Improvised http://www.secguru.com/nsuri/fakeap_tested_compiled_and_improvised April 2006

[15] A Weiss. Introduction to Kismet http://www.wi-fiplanet.com/tutorials/article.php/3595531 March 2006

[16] SANS organisation, http://www.sans.org/ April 2006

[17] Black Alchemy Enterprises, Fake AP. http://www.blackalchemy.to/project/fakeap/ April 2006

[18] AWE Communications Wave Propagation and Radio Network Planning http://www.awe-communications.com/ April 2006

[19] Radio Mobile home page. http://www.cplus.org/rmw/english1.html April 2006

[20] AirWave Home Page. http://www.airwave.com April 2006

[21] Bloover. http://trifinite.org/trifinite_stuff_blooover.html. April 2006

[22] C. He and J.C. Mitchell, Security Analysis and Improvements for IEEE 802.11i, *Network and Distributed System Security Symposium (NDSS ‘05)*, February, 2005.

8 ACKNOWLEDGEMENT

This work was undertaken in the Distributed Multimedia Centre of Excellence at Rhodes University, with financial support from Telkom SA, Business Connexion, Comverse, Verso Technologies, Tellabs and StorTech THRIP, and the National Research Foundation.