APPENDICES

Glossary

Accronym	Definition
3G	Third Generation
ACK	Acknowledgement
AES	Advanced Encryption Standard
AES-CCM	Advanced Encryption Standard Counter with CBC-MAC Mode
ANSI	American National Standards Institute
AP	Access Point
AS	Authentication Server
BSSID	Basic Service Set Identifier
CAD	Computer Aided Design
CBC	Cipher Block Chaining
CCK	Complementary Code Keying
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CDMA	Code Division Multiple Access
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	Collision Sense Multiple Access/Collision Avoidance
CSMA/CD	Collision Sense Multiple Access/Collision Detection
CTS	Clear To Send
dB	Decibels
dBi	Decibels to isotropic antenna
dBm	Decibels to 1 milliwatt
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN

EDGE	Enhanced Data Rates for Global Evolution
EIRP	Effective Isotropic Radiated Power
EM	Electro-Magnetic
ESSID	Extended Service Set Identifier
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
GMK	Group Master Key
GPRS	General Packet Radio Service
GPS	Global Position System
GSM	Global System for Mobile Communications
GTK	Group Temporal Key
HIPERLAN	High performance radio LAN
HR/DSSS	High-Rate Direct-Sequence
HTTP	Hyper Text Transfer Protocol
IC	Integrity Check
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Industrial, Scientific, and Medical
ITU	International Telecommunication Union
IV	Initialisation Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
KML	Keyhole Markup Language
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Layer
MAC – OSI layer	Media Access Control
MAC – Security	Message Authentication Code

MAN	Metropolitan Area Network
MIC	Message Integrity Code
MIM	Man in the Middle
MIMO	Multiple Input Multiple Output
MSK	Master Session Key
MTU	Maximum Transmission Unit
NAV	Network Allocation Vector
nG	Next Generation
NLOS	Non Line of Sight
OFDM	Orthogonal Frequency Division Multiplexing
OMAC	One-key-MAC
OSI	Open Systems Interconnection
OUI	Organizationally Unique Identifiers
PAN	Personal Area Network
PEAP	Protected Extensible Authentication Protocol
PHY	Physical
PMK	Pairwise Master Key
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre Shared Key
PTK	Pairwise Transient Key/Pairwise Temporal Key
PTP	Point to Point
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RSA	Rivest, Shamir and Adleman
RSN	Robust Security Network
RSNA	Robust Security Network Associations
RSS	Received Signal Strength
RTS	Request To Send
SNR	Signal to Noise Ratio
SOHO	Small Office Home Office
SSH	Secure Shell
SSID	Service Set Identity

SSL	Secure Socket Layer
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TSN	Transient Security Network
TTLS	Tunneled Transport Layer Security
Tx	Transmitter
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIGLE	Wireless Geographic Logging Engine
WIGWAM	Wireless Gigabit with Advanced Multi-Media
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Networks
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Networks
WWD	World Wide Wardrive

Appendix A

This Appendix constitute a Sample of the information acquired during the practical site survey. The rest can be found on the CD in the Appendix directory.

Network	NetType	ESSID	BSSID	Channel	Cloaked	Network	Encryption	Decrypted	MaxRate	Beacon	Data	Crypt	Weak	Network	FirstTime	GPSMaxSpd	GPSBestLat	GPSBestLon	GPSBestAlt	IPType	IP
1	infrastructure	DATABRIDGE-1	00:02:6F:34:83:74	1	No	1	WEP	No	11	51200	4	4	0	1	Fri Jul 7 18:44:08 2006	28.092848	-26.063864	27.968452	4647.185547	None	0.0.0.0
2	infrastructure	<no ssid>	00:02:6F:21:2B:AB	7	No	2	None	No	11	25600	0	0	0	2	Fri Jul 7 18:44:19 2006	18.319271	-26.064501	27.968567	4639.074219	None	0.0.0.0
3	infrastructure	QN1	00:02:6F:36:2E:70	11	No	3	WEP	No	11	25600	462	0	0	3	Fri Jul 7 18:44:30 2006	22.017879	-26.067667	27.969	4635.193359	TCP	192.193.194.34
4	infrastructure	QuickNet	00:02:6F:3E:13:CF	1	No	4	WEP	No	0	0	383	3	0	4	Fri Jul 7 18:44:31 2006	22.467834	-26.067667	27.969	4635.193359	TCP	192.193.194.59
5	infrastructure	QN-TBC	00:02:6F:3D:34:11	6	No	5	WEP	No	1	25600	67	0	0	5	Fri Jul 7 18:44:33 2006	28.621058	-26.067949	27.968966	4635.193359	TCP	192.193.194.23
6	infrastructure	GUI-B	00:02:6F:3F:75:DE	1	No	6	WEP,PPTP	No	0	0	2	0	0	6	Fri Jul 7 18:44:49 2006	30.090603	-26.068558	27.969072	4667.266113	None	0.0.0.0
7	infrastructure	marconi	00:02:6F:33:08:B3	6	No	7	WEP	No	11	25600	0	0	0	7	Fri Jul 7 18:44:58 2006	14.14309	-26.068724	27.96937	4687.973633	None	0.0.0.0
8	infrastructure	marconi	00:02:6F:3C:75:B6	6	No	8	WEP	No	11	25600	0	0	0	8	Fri Jul 7 18:45:23 2006	18.273241	-26.070068	27.972843	4724.161133	None	0.0.0.0
9	infrastructure	Work	00:0F:3D:3D:1F:2A	6	No	9	WEP	No	11	25600	0	0	0	9	Fri Jul 7 18:45:25 2006	17.746183	-26.070393	27.973108	4728.929688	None	0.0.0.0
10	infrastructure	Patio_Warehouse	00:02:6F:38:F3:04	11	No	10	WEP	No	0	0	0	0	0	10	Fri Jul 7 18:45:51 2006	28.228642	-26.070339	27.974855	4772.097168	None	0.0.0.0
11	infrastructure	Patio_Warehouse	00:02:6F:38:F2:CC	11	No	11	None	No	18	25600	0	0	0	11	Fri Jul 7 18:45:54 2006	27.707336	-26.069777	27.97533	4774.383789	None	0.0.0.0
12	infrastructure	Olivewood1	00:02:6F:3D:6B:5B	10	No	12	WEP	No	11	0	0	0	0	12	Fri Jul 7 18:46:33 2006	30.152746	-26.063059	27.981375	4744.650879	None	0.0.0.0
13	infrastructure	<no ssid>	00:16:B6:D9:55:A4	11	No	13	WEP	No	54	25600	0	0	0	13	Fri Jul 7 18:47:04 2006	30.300045	-26.058334	27.986952	4747.310547	None	0.0.0.0
14	infrastructure	<no ssid>	00:02:6F:39:F6:21	11	No	14	None	No	11	25600	13	0	0	14	Fri Jul 7 18:47:12 2006	30.091755	-26.05727	27.988222	4748.653809	None	0.0.0.0
15	infrastructure	wlan-ap	00:04:ED:55:1C:94	1	No	15	WEP	No	11	25600	0	0	0	15	Fri Jul 7 18:47:47 2006	30.357584	-26.051863	27.994627	4744.575195	None	0.0.0.0
16	infrastructure	<no ssid>	00:02:6F:35:96:41	1	No	16	WEP	No	11	25600	0	0	0	16	Fri Jul 7 18:47:50 2006	29.974375	-26.051401	27.995169	4744.521973	None	0.0.0.0
17	infrastructure	NLC Cell 2	00:11:95:7E:75:F6	6	No	17	WEP	No	22	25600	0	0	0	17	Fri Jul 7 18:48:11 2006	29.912233	-26.048018	27.999117	4745.056641	None	0.0.0.0
18	infrastructure	NLC Cell 1	00:11:95:7E:76:09	9	No	18	WEP	No	22	25600	0	0	0	18	Fri Jul 7 18:48:12 2006	29.912233	-26.047863	27.999294	4745.060059	None	0.0.0.0
19	ad-hoc	MLC	02:12:F9:6C:02:7C	11	No	19	WEP	No	11	25600	0	0	0	19	Fri Jul 7 18:48:16 2006	29.665966	-26.047253	28.000011	4744.960938	None	0.0.0.0
20	infrastructure	<no ssid>	00:12:0E:0A:29:EF	11	No	20	WEP,TKIP,WPA	No	22	51200	0	0	0	20	Fri Jul 7 18:48:24 2006	28.813238	-26.046244	28.001253	4744.964355	None	0.0.0.0
21	infrastructure	17Crawford	00:30:BD:9B:FC:D1	11	No	21	WEP	No	54	25600	0	0	0	21	Fri Jul 7 18:49:02 2006	18.429747	-26.041887	28.006226	4867.384277	None	0.0.0.0
22	infrastructure	linksys	00:14:BF:99:9F:5D	11	No	22	None	No	22	25600	0	0	0	22	Fri Jul 7 18:49:07 2006	30.349529	-26.041449	28.006962	4929.622559	None	0.0.0.0
23	infrastructure	Low Bull	00:30:BD:61:BB:F7	11	No	23	WEP	No	11	0	0	0	0	23	Fri Jul 7 18:49:30 2006	29.270098	-26.039318	28.010689	4810.419922	None	0.0.0.0
24	infrastructure	Cardinal	00:0F:CB:AD:1C:5A	11	No	24	WEP	No	36	25600	1	1	0	24	Fri Jul 7 18:49:47 2006	28.41967	-26.038033	28.014784	5020.134766	None	0.0.0.0
25	infrastructure	ADSL	00:0F:B5:56:87:D8	11	No	25	WEP	No	0	0	47	47	0	25	Fri Jul 7 18:49:48 2006	31.540586	-26.038033	28.014784	5020.134766	None	0.0.0.0
26	infrastructure	Inspec	00:12:A9:C1:32:F7	11	No	26	WEP	No	36	0	0	0	0	26	Fri Jul 7 18:49:52 2006	32.935333	-26.037697	28.015827	5017.570801	None	0.0.0.0
27	infrastructure	Allyns	00:02:6F:3C:65:26	6	No	27	WEP	No	11	25600	0	0	0	27	Fri Jul 7 18:49:57 2006	28.81669	-26.037312	28.016939	5017.20459	None	0.0.0.0
28	infrastructure	default	00:0E:2E:61:BB:C2	11	No	28	WEP	No	0	0	5	0	0	28	Fri Jul 7 18:49:58 2006	28.81669	-26.037312	28.016939	5017.20459	UDP	192.168.1.205
29	infrastructure	By Design	00:12:0E:13:87:FA	4	No	29	WEP	No	22	51200	0	0	0	29	Fri Jul 7 18:50:02 2006	28.81669	-26.037067	28.017921	5029.203125	None	0.0.0.0
30	infrastructure	DIG_DIM	00:11:95:3C:1C:B1	7	No	30	None	No	22	25600	0	0	0	30	Fri Jul 7 18:50:24 2006	32.525654	-26.03557	28.023546	4994.942871	None	0.0.0.0
31	infrastructure	VillaRoyale	00:02:6F:40:67:EA	6	No	31	None	No	1	25600	0	0	0	31	Fri Jul 7 18:50:26 2006	32.933029	-26.035437	28.024067	4990.867188	None	0.0.0.0
32	probe	<no ssid>	00:12:F0:21:EA:CB	0	No	32	None	No	18	0	0	0	0	32	Fri Jul 7 18:51:13 2006	30.46806	-26.033922	28.035786	4927.415039	None	0.0.0.0
33	infrastructure	sonicwall	00:06:B1:14:22:91	5	No	33	WEP	No	0	0	0	0	0	33	Fri Jul 7 18:51:15 2006	30.46806	-26.033991	28.036283	4927.526855	None	0.0.0.0
34	infrastructure	Drager	00:12:DA:A7:E3:60	3	No	34	None	No	18	25600	0	0	0	34	Fri Jul 7 18:51:16 2006	30.46806	-26.033991	28.036283	4927.526855	None	0.0.0.0
35	infrastructure	athreewds	00:11:95:FB:C4:90	1	No	35	WEP,TKIP,WPA,AES-CCM	No	36	25600	0	0	0	35	Fri Jul 7 18:51:17 2006	29.710846	-26.034115	28.037008	4928.055176	None	0.0.0.0
36	infrastructure	GIGABYTE	00:0D:61:79:FA:4E	6	No	36	None	No	36	25600	0	0	0	36	Fri Jul 7 18:51:39 2006	28.813238	-26.035416	28.041889	4894.012207	None	0.0.0.0
37	infrastructure	Renier & Claire	00:E0:98:4F:59:14	11	No	37	WEP	No	11	25600	0	0	0	37	Fri Jul 7 18:51:48 2006	28.769508	-26.035915	28.043722	4875.496094	None	0.0.0.0
38	infrastructure	hiside	00:04:E2:FF:BA:5A	8	No	38	WEP,TKIP,WPA,PSK,AES-CCM	No	36	25600	2	2	0	38	Fri Jul 7 18:51:53 2006	29.417397	-26.036276	28.045061	4863.648926	None	0.0.0.0
39	ad-hoc	AUSTAR	56:7E:F0:57:AA:E1	11	No	39	WEP	No	11	25600	0	0	0	39	Fri Jul 7 18:52:16 2006	27.505951	-26.037535	28.049887	4809.825684	None	0.0.0.0
40	infrastructure	wlan-ap	00:04:ED:55:26:EB	1	No	40	WEP,TKIP,WPA	No	11	25600	0	0	0	40	Fri Jul 7 18:52:16 2006	27.505951	-26.037535	28.049887	4809.825684	None	0.0.0.0
41	ad-hoc	KWHSENOA	0E:B3:6F:32:AD:64	13	No	41	WEP	No	11	25600	4	4	0	41	Fri Jul 7 18:52:17 2006	28.333363	-26.037582	28.050106	4805.249023	None	0.0.0.0
42	probe	<no ssid>	00:0B:CD:5B:0A:0B	0	No	42	None	No	36	0	0	0	0	42	Fri Jul 7 18:52:20 2006	27.700432	-26.037739	28.051008	4797.275879	None	0.0.0.0
43	infrastructure	WLAN2	00:14:6C:5F:0D:94	11	No	43	WEP	No	54	25600	3	3	0	43	Fri Jul 7 18:52:21 2006	29.563545	-26.037777	28.051233	4796.127441	None	0.0.0.0
44	infrastructure	DLINK_WIRELESS	00:11:95:9D:6B:E8	6	No	44	WEP	No	22	51200	0	0	0	44	Fri Jul 7 18:52:29 2006	29.772987	-26.037867	28.052824	4793.679199	None	0.0.0.0
45	infrastructure	Yoda	00:0F:3D:DF:C7:A5	6	No	45	WEP	No	36	25600	0	0	0	45	Fri Jul 7 18:52:29 2006	29.772987	-26.037867	28.052824	4793.679199	None	0.0.0.0
46	infrastructure	tweety	00:0F:3D:DF:C7:B9	6	No	46	None	No	36	25600	1	0	0	46	Fri Jul 7 18:52:29 2006	29.772987	-26.037867	28.052824	4793.679199	None	0.0.0.0
47	infrastructure	ITNWireless	00:15:E9:82:D4:E4	6	No	47	WEP	No	36	25600	0	0	0	47	Fri Jul 7 18:52:29 2006	29.015774	-26.037867	28.052824	4793.679199	None	0.0.0.0
48	infrastructure	IT Systems	00:0F:3D:DF:C5:D2	1	No	48	WEP	No	36	25600	4	4	0	48	Fri Jul 7 18:52:29 2006	30.020405	-26.037865	28.053049	4793.487793	None	0.0.0.0
49	infrastructure	Boardroom	00:0F:3D:DF:46:C6	1	No	49	WEP	No	36	25600	0	0	0	49	Fri Jul 7 18:52:29 2006	28.215982	-26.037865	28.053049	4793.487793	None	0.0.0.0

AppendixB

AlistofafewmanufacturerswiththeirdefaultAPpasswords

Manufacturer	Product	Protocol	UserID	Password	Access	LastModified
BlueCoatSystems	ProxySG	HTTP	admin	articon	Admin	2005/11/14
KTI	KS2600	Console	admin	123456	Admin	2005/11/14
KTI	KS2260	Console	admin	123	Admin	2005/11/14
Exabyte	Magnum20	FTP	anonymous	Exabyte	Admin	2005/11/15
Sorenson	SR-200	HTTP	(none)	admin	Admin	2005/11/16
D-Link	DI-524	HTTP	admin	(none)	Admin	2005/11/21
McAfee	SCM3100	Multi	scmadmin	scmchangeme	Admin	2005/11/23
Zebra	10/100PrintServer	Multi	admin	1234	Admin	2005/11/28
Xerox	DocumentCentre405	HTTP	admin	admin	Admin	2006/01/02
Netgear	GSM7224	HTTP	admin	(none)	Admin	2006/01/03
Gericom	Phoenix	Multi	Administrator	(none)	Admin	2006/01/04
Proxim	Orinoco600/2000	HTTP	(none)	(none)	Admin	2006/01/07
BauschDatacom	ProximaPRIADSLPSTNRouter4Wirefess	Multi	admin	epicrouter	Admin	2006/01/09
SunMicrosystems	ILOMofX4100	HTTP	root	changeme	Admin	2006/01/16
Conexant	Router	HTTP	n/a	admin	Admin	2006/01/21
dlink	adsl	HTTP	admin	admin	Admin	2006/01/21
Edimax	ES-5224RXM	Multi	admin	123	Admin	2006/01/23
IronPort	MessagingGatewayAppliance	Multi	admin	ironport	Admin	2006/01/25
3com	812	HTTP	Administrator	admin	Admin	2006/01/28
Asante	FM2008	Multi	admin	asante	Admin	2006/02/01
Broadlogic	XLTrouter	HTTP	webadmin	webadmin	Admin	2006/02/01
Broadlogic	XLTrouter	Telnet	admin	admin	Admin	2006/02/01
Broadlogic	XLTrouter	Telnet	installer	installer	Admin	2006/02/01
Cisco	Aironet	Multi	(none)	_Cisco	Admin	2006/02/01
Cisco	Aironet	Multi	Cisco	Cisco	Admin	2006/02/01
Cisco	HSE	Multi	root	blender	Admin	2006/02/01

Cisco	HSE	Multi	hsa	hsadb	Admin	2006/02/01
Cisco	WLSE	Multi	root	blender	Admin	2006/02/01
Cisco	WLSE	Multi	wlse	wlsedb	Admin	2006/02/01
Digicom	Michelangelo	Multi	admin	michelangelo	Admin	2006/02/01
Digicom	Michelangelo	Multi	user	password	User	2006/02/01
Enterasys	VerticalHorizon	Multi	tiger	tiger123	Admin	2006/02/01
Pentaoffice	SatRouter	Telnet	(none)	pento	Admin	2006/02/01
Pirelli	AGEADSLRouter	Multi	admin	microbusiness	Admin	2006/02/01
Pirelli	AGEADSLRouter	Multi	user	password	User	2006/02/01
System/32	VOS	Multi	install	secret	Admin	2006/02/01
Tandem	TACL	Multi	super.super	(none)	Admin	2006/02/01
Tandem	TACL	Multi	super.super	master	Admin	2006/02/01
VxWorks	misc	Multi	admin	admin	Admin	2006/02/01
VxWorks	misc	Multi	guest	guest	Guest	2006/02/01
Wang	Wang	Multi	CSG	SESAME	Admin	2006/02/01
Westell	Wang	Multi	CSG	SESAME	Admin	2006/02/01
Westell	Wirespeedwirelessrouter	Multi	admin	sysAdmin	Admin	2006/02/01
3COM	CoreBuilder	Telnet	n/a	admin	Admin	2006/02/02
CNET	CNET4PORTADSLMODEM	Multi	admin	epicrouter	Admin	2006/02/02
SMC	SMCWBR14-G	HTTP	(none)	smcadmin	Admin	2006/02/02
JAHT	adslrouter	HTTP	admin	epicrouter	Admin	2006/02/03
asmack	router	HTTP	admin	epicrouter	Admin	2006/02/03
D-Link	firewall	HTTP	admin	admin	Admin	2006/02/04
ovislink	WL-1120AP	Multi	root	(none)	Admin	2006/02/05
3COM	CoreBuilder	Telnet	n/a	(none)	Admin	2006/02/09
Linksys	WRT54G	HTTP	(none)	admin	Admin	2006/02/09
canyon	router	Multi	Administrator	admin	Admin	2006/02/09
Kalatel	CaliburDSR-2000e	Multi	n/a	3477	Admin	2006/02/13
3com	officeconnect	Multi	admin	(none)	Admin	2006/02/16
3com	officeconnect	Multi	admin	(none)	User	2006/02/16
IBM	T20	Multi	n/a	admin	Admin	2006/02/16
Asus	WL500gDeluxe	HTTP	admin	admin	Admin	2006/02/18

IBM	IBM	Multi	n/a	(none)	Admin	2006/02/20
Pentagram	CerberusADSLmodem+router	HTTP	admin	password	Admin	2006/02/21
Cisco	Aironet1200	HTTP	root	Cisco	Admin	2006/02/22
D-link	Di-707prouter	HTTP	admin	(none)	Admin	2006/02/25
Linksys	modelWRT54GCcompactwireless-Gbroadbandrouter	Multi	(none)	admin	Admin	2006/02/25
ihoi	oihoh	HTTP	Administrator	pilou	Admin	2006/03/05
AXUS	AXUSYOTTA	Multi	n/a	0	Admin	2006/03/07
D-link	DSL500G	Multi	admin	admin	Admin	2006/03/07
corecess	3113	Multi	admin	(none)	Admin	2006/03/07
Asus	P5P800	Multi	n/a	admin	User	2006/03/09
Dell	RemoteAccessCard	HTTP	root	calvin	Admin	2006/03/11
d-link	di-524	HTTP	admin	(none)	Admin	2006/03/13
ion	nelu	Multi	n/a	admin	Admin	2006/03/15
ion	nelu	Multi	Administrator	admin	Admin	2006/03/15
ASMAX	AR701u/ASMAXAR6024	HTTP	admin	epicrouter	Admin	2006/03/18
ASMAX	AR800C2	HTTP	admin	epicrouter	Admin	2006/03/18
ASMAX	AR800C2	HTTP	admin	epicrouter	Admin	2006/03/18
D-link	DSL-504T	HTTP	admin	admin	Admin	2006/03/18
D-link	DSL-G604T	Multi	admin	admin	Admin	2006/03/18
Draytek	Vigor2600	HTTP	admin	(none)	Admin	2006/03/18
LG	LAM200E/LAM200R	Multi	admin	epicrouter	Admin	2006/03/18
Linksys	AG241-ADSL2Gatewaywith4-PortSwitch	Multi	admin	admin	Admin	2006/03/18
Micronet	3351/3354	Multi	admin	epicrouter	Admin	2006/03/18
Planet	ADE-4110	HTTP	admin	epicrouter	Admin	2006/03/18
Planet	XRT-401D	HTTP	admin	1234	Admin	2006/03/18
Planet	ADE-4000	Multi	admin	epicrouter	Admin	2006/03/18
SAGEM	FAST1400	Multi	admin	epicrouter	Admin	2006/03/18
SMC	7204BRA	Multi	smc	smcadmin	Admin	2006/03/18
U.S.Robotics	SureConnect9003ADSLEthernet/USBRouter	Multi	root	12345	Admin	2006/03/18
U.S.Robotics	SureConnect9105ADSL4-PortRouter	HTTP	admin	admin	Admin	2006/03/18
3COM	OfficeConnectADSLWireless11gFirewallRouter	HTTP	(none)	admin	Admin	2006/03/25
ZyXEL	Prestige645	HTTP	admin	1234	Admin	2006/03/25

olitec(Trendchip)	sx202adsImodemrouter	HTTP	admin	admin	Admin	2006/03/25
CableAndWireless	ADSLModem/Router	Multi	admin	1234	Admin	2006/03/30
TelcoSystems	EdgeLink100	Console	telco	telco	telco	2006/04/02
DI624	D-LINK	HTTP	admin	password	Admin	2006/04/03
ZyXELZyWALLSeries	Prestige660R-61C	Multi	n/a	admin	Admin	2006/04/03
Ricoh	AficioAP3800C	HTTP	(none)	password	Admin	2006/04/05
Ricoh	Aficio2232C	Telnet	n/a	password	Admin	2006/04/05
edimax	wirelessadslrouter	Multi	admin	epicrouter	Admin	2006/04/10
Asmax	Ar-804u	HTTP	admin	epicrouter	Admin	2006/04/11
aztech	DSL-600E	HTTP	admin	admin	Admin	2006/04/12
comtrend	ct536+	Multi	admin	(none)	Admin	2006/04/14
QuintumTechnologies	TenorSeries	Multi	admin	admin	Admin	2006/04/19
Alcatel	OmniPCXOffice	FTP	ftp_inst	pbxk1064	Installer	2006/04/23
Alcatel	OmniPCXOffice	FTP	ftp_admi	kilo1987	Admin	2006/04/23
Alcatel	OmniPCXOffice	FTP	ftp_oper	help1954	Operator	2006/04/23
Alcatel	OmniPCXOffice	FTP	ftp_nmc	tuxalize	NMC	2006/04/23
Netgear	ADSLModemDG632	HTTP	admin	password	Admin	2006/04/23
AlliedTelesyn	AT-AR130(U)-10	HTTP	Manager	friend	Admin	2006/05/09
Mikrotik	RouterOS	HTTP	admin	(none)	Admin	2006/05/09
Netgear	WGT634U	HTTP	admin	password	Admin	2006/05/14
D-Link	DI-524	HTTP	user	(none)	User	2006/05/20
Ricoh	AP410N	HTTP	admin	(none)	Admin	2006/05/21
3ware	3DM	HTTP	Administrator	3ware	Admin	2006/05/26
ALCATEL	4400	Console	mtcl	(none)	User	2006/05/29
Netgear	GS724t	HTTP	n/a	password	Admin	2006/05/29
apple	airport5	Multi	root	admin	Admin	2006-00-03
Netgear	Router/Modem	Multi	admin	password	Admin	2006-00-04
SMC	Router/Modem	Multi	admin	barricade	Admin	2006-00-04
Nullsoft	Shoutcast	PLS	admin	changeme	Admin	2006-00-05
Conexant	Router	HTTP	n/a	epicrouter	Admin	2006-00-07
ZyXEL	Prestige900	HTTP	webadmin	1234	Admin	2006-00-10
Corecess	6808APC	Telnet	corecess	corecess	User	2006-00-18

NetworkEverywhere	NWR11B	HTTP	(none)	admin	Admin	2006-00-18
Netgear	MR314	Multi	admin	1234	Admin	2006-00-20
Aethra	StarbridgeEU	HTTP	admin	password	Admin	2006-00-23
Milan	mil-sm801p	Multi	root	root	Admin	2006-00-23
cisco	2600	Telnet	Administrator	admin	Admin	2006-00-25
giga	8ippro1000	Multi	Administrator	admin	Admin	2006-00-25
MinoltaQMS	Magicolor3100	HTTP	operator	(none)	Admin	2006-02-29
IBM	RemoteSupervisorAdapter(RSA)	HTTP	USERID	PASSW0RD	Admin	2006-02-30
IBM	BladeCenterMgmtConsole	HTTP	USERID	PASSW0RD	Admin	2006-02-30

Appendix C

In this Appendix a comparison between AirMagnet and Kismet are made.

Evaluation Criteria	AirMagnet
Policy Management	Provides an interface to customize detection and threshold parameters specifically to your site
Radio Frequency Management	Warn on channel Interference. Indicate noise by channel. A graph which indicates amount of interference on a channel.
Roaming	It can monitor the quality of Roaming for VoWLAN applications.
Measuring the Signal Coverage of an AP	Use the laptop to walk around to view the signal strength of APs
Reporting	Has an excellent reporting facility, can create a number of reports and very easy to use.
Support a GPS?	Yes
Packet Capture	Captures all packets and display the content, You can replay the data in the way it looked when it was captured.
Security	Display encryption scheme used by an AP, and MIC TKIP. Look at all the devices not just Aps for security vulnerabilities
DOS attacks	Warns on Association and Authentication DOS attacks.
Exploit vulnerability?	No
Locate Devices	Provides a tracking tool to do this for eg locating a rogue device
Output	Can export data to a CSV format, i.e. db or excel format Proprietary **.amc** - data can be played back exactly the way it started Ethereal format **.epc** Sniffer format **.cap**
Documentation	Excellent, a comprehensive help system For each policy implementation an explanation is provided for erg a type of DOS attack gets comprehensively explained. Empowereing the user to fully understand it, so an informed decision can be made.
Installation	Trivial – Only on Windows
Configuration	Non required for initial use, however to set up the policy for a specific WLAN requires work, and even then guided steps are provided.
Ease of use	Trivial
Network Performance	Has a tool to test the network performance
Charts/Summaries and Reports	All very good.
Alarms/Alerts	Once a certain threshold has been reached or a property has been breached an alarm gets thrown. For e.g. report on weak IV's, Slow key rotations, Open System Authentication Provides for both security and performance insurance
Radio Propagation Visualization	The Visualization of the data is not available in this tool. The closest they get to radio propagation visualization is an approximation of where clients are relative to their APs.
Card Support	Many are supported, they are listed on their website
Auditing Tool	Yes

Planning Tool	No
How it scans	Passive
Attached clients to Aps	Yes
IDS?	Yes
Overall rating	Excellent

Evaluation Criteria	Kismet
Policy Management	No enforced policy management
Radio Frequency Management	Display Noise levels on a channel Log APs by channel number, from this interference can be derived of overlapping channels. Provide summary of percentage of total amount of APs found on each channel
Roaming	Do Not test for the reliability of roaming across APs
Measuring the Signal Coverage of an AP	Use the laptop to walk around to view the signal strength of APs
Reporting	No reporting facility
Support a GPS?	Yes
Packet Capture	Yes
Security	Display encryption scheme used by an AP, and MIC TKIP. Look at all the devices not just APs for security vulnerabilities.
DOS attacks	Through reporting on management frames (DeAuth/Disassociation) floods
Exploit vulnerability?	Yes, runtime decoding of WEP packets
Locate Devices	Can do by simply walking around until the strongest signal is found Has a “follow network center option” which needs a GPS to find the estimated network center.
Output	.csv .gps .xml Ethereal format **.epc**
Documentation	Average
Installation	Easy – only on Linux.
Configuration	One has to manually go through the configuration file to edit various features.
Ease of use	Easy
Network Performance	No such facility
Charts/Summaries and Reports	Almost None, display the % of APs on each channel.
Alarms/Alerts	Yes, it gives an alert for: Netstumbler, Deauth/Diassoc flood, Broadcast Disassoc/Deauth and a few others; however these are not reported in a user friendly format.
Radio Propagation Visualization	Uses gpsmap to provide visualization, however this tool assumes that all Aps are Omniderection
Card Support	A few cards not supported, more than 20 supported
Auditing Tool	Yes
Planning Tool	Not really
How it scans	Passive, can decloak hidden SSIDs
Attached clients to Aps	Can view all clients attached to an AP. Allows for multiple Kismet clients and a server, hence nodes can be set up at different areas and the data can be assembled in one point.
IDS?	Can throw a few alerts, And connect to a Snort IDS.
Overall rating	Good

Appendix D

A sample list of OUIs, with their manufacturer and manufacturer list. More can be found on the CD.

OUI	Organization
ID	ADRESS
00-00-00 (hex)	XEROX CORPORATION
0	XEROX CORPORATION M/S 105-50C 800 PHILLIPS ROAD WEBSTER NY 14580 UNITED STATES
00-00-01	XEROX CORPORATION
1	XEROX CORPORATION ZEROX SYSTEMS INSTITUTE M/S 105-50C 800 PHILLIPS ROAD WEBER NY 14580 UNITED STATES
00-00-02	XEROX CORPORATION
2	XEROX CORPORATION XEROX SYSTEMS INSTITUTE M/S 105-50C 800 PHILLIPS ROAD WEBSTER NY 14580 UNITED STATES
00-00-03	XEROX CORPORATION
3	ZEROX SYSTEMS INSTITUTE ZEROX SYSTEMS INSTITUTE M/S 105-50CEW AVENUE 800 PHILLIPS ROAD WEBSTER NY 14580 UNITED STATES
00-00-04	XEROX CORPORATION
4	XEROX CORPORATION OFFICE SYSTEMS DIVISION M/S 105-50C 800 PHILLIPS ROAD4 WEBSTER NY 14580 UNITED STATES
00-00-05	XEROX CORPORATION
5	XEROX CORPORATION OFFICE SYSTEMS DIVISION M/S 105-50C 800 PHILLIPS ROAD WEBSTER NY 14580

UNITED STATES

00-00-06 XEROX CORPORATION
6 XEROX CORPORATION
OFFICE SYSTEMS DIVISION
M/S 105-50C 800 PHILLIPS ROAD4
WEBSTER NY 14580
UNITED STATES

00-00-07 XEROX CORPORATION
7 XEROX CORPORATION
OFFICE SYSTEMS DIVISION
M/S 105-50C 800 PHILLIPS ROAD
WEBSTER NY 14580
UNITED STATES

00-00-08 XEROX CORPORATION
8 XEROX CORPORATION
OFFICE SYSTEMS DIVISION
M/S 105-50C 800 PHILLIPS ROAD
WEBSTER NY 14580
UNITED STATES

00-00-09 XEROX CORPORATION
9 XEROX CORPORATION
1350 JEFFERSON ROAD
ROCHE STER NY 14623
UNITED STATES

00-00-0A (hex) OMRON TATEISI ELECTRONICS CO.
00000A (base 16) OMRON TATEISI ELECTRONICS CO.
SECTION NFF, SYSTEM R&D LABS.
RESEARCH & TECH. ASSESSMNT DIV SHIMOKAII
KYOTO KYOTO 617 JAPAN
JAPAN

00-00-0B (hex) MATRIX CORPORATION
00000B (base 16) MATRIX CORPORATION
1203 NEW HOPE ROAD
RALEIGH NORTH CAROLINA 276
UNITED STATES

00-00-0C (hex) CISCO SYSTEMS, INC.
00000C (base 16) CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-1706
UNITED STATES

00-00-0D (hex) FIBRONICS LTD.
00000D (base 16) FIBRONICS LTD.

MATAM TECHNOLOGY CENTER
HAIFA
ISRAEL
ISRAEL

00-00-0E (hex) FUJITSU LIMITED
00000E (base 16) FUJITSU LIMITED
COMPUTER SYS. ARCHITECTURE DEP
MAINFRAME DIV. 1015 KAMIKODANAKA, NAKAH
KAWASAKI 211
JAPAN

00-00-0F (hex) NEXT, INC.
00000F (base 16) NEXT, INC.
3475 DEER CREEK ROAD
PALOALTO CA 94304
UNITED STATES

00-00-10 (hex) SYTEK INC.
10 (base 16) SYTEK INC.
1125 CHARLESTON ROAD
MOUNTAIN VIEW CA 94043
UNITED STATES

00-00-11 (hex) NORMEREL SYSTEMES
11 (base 16) NORMEREL SYSTEMES
58 RU 58 RUE POTTIER
78150 78150 LE CHESNAY
FRANCE
FRANCE

00-00-12 (hex) INFORMATION TECHNOLOGY LIMITED
12 (base 16) INFORMATION TECHNOLOGY LIMITED
MAYLANDS AVE. HEMEL HEMPSTEAD
HERTS ENGLAND
UNITED KINGDOM

00-00-13 (hex) CAMEX
13 (base 16) CAMEX
75 KNEELAND STREET
BOSTON MA 02111
UNITED STATES

00-00-14 (hex) NETRONIX
14 (base 16) NETRONIX
1372 MCDOWELL BLVD.
PETULAMA CA 94952
UNITED STATES

00-00-15 (hex) DATAPOINT CORPORATION

15 (base 16) DATAPOINT CORPORATION
9725 DATAPOINT DRIVE
SAN ANTONIO TX 78284
UNITED STATES

00-00-16 (hex) DU PONT PIXEL SYSTEMS .
16 (base 16) DU PONT PIXEL SYSTEMS .
MEADLAKE PLACE
THORPE LEA ROAD EGHAM, SURREY TW20 8HE
ENGLAND
UNITED KINGDOM

00-00-17 (hex) TEKELEC
17 (base 16) TEKELEC
26540 AGOURA ROAD
CALABASAS CA 91302
UNITED STATES

00-00-18 (hex) WEBSTER COMPUTER CORPORATION
18 (base 16) WEBSTER COMPUTER CORPORATION
16040 REDWOOD LODGE ROAD
LOS GATOS CA 95033-9260
UNITED STATES

00-00-19 (hex) APPLIED DYNAMICS INTERNATIONAL
19 (base 16) APPLIED DYNAMICS INTERNATIONAL
3800 STONE SCHOOL ROAD
ANN ARBOR MI 48104-2499
UNITED STATES

00-00-1A (hex) ADVANCED MICRO DEVICES
00001A (base 16) ADVANCED MICRO DEVICES
P.O. P.O. BOX 3453
SUNNYVALE CA 94088
UNITED STATES

00-00-1B (hex) NOVELL INC.
00001B (base 16) NOVELL INC.
122 E 122 EAST 1700 SOUTH
M/S: E-12-1
PROVOUT 84606
UNITED STATES

00-00-1C (hex) BELL TECHNOLOGIES
00001C (base 16) BELL TECHNOLOGIES
330 WARREN AVENUE
FREMONT CA 94539
UNITED STATES

00-00-1D	(hex) CABLETRON SYSTEMS, INC.
00001D	(base 16) CABLETRON SYSTEMS, INC.
35 IN	35 INDUSTRIAL WAY P.O. BOX 5005 ROCHESTER NH 03867 UNITED STATES