

Wireless Security



By Nick von Dadelszen

Wireless Security History

- 802.11b Standard
 - Three security options
 - SSID
 - MAC filtering
 - WEP
- Easily Breakable
 - SSID Broadcasting
 - War-Driving
 - WEP cracking

Current Technologies

- 802.1X
 - RADIUS Authentication
 - Dynamic WEP encryption key distribution
 - Widely implemented by manufacturers late 2001 and 2002
- WPA
 - Wi-Fi Protected Access
 - security standard (required for certification)
 - Solves WEP issues by utilising TKIP
 - Includes 802.1X authentication
 - Allow Pre-shared Key mode (PSK) that doesn't require RADIUS (only considered slightly better than WEP)
 - Currently being implemented by manufacturers

The Future

- 802.11i
 - IEEE standard
 - Approved in July, starting to appear in the market
 - Includes WPA plus AES encryption
 - Still allows a shared-key mode
- WAPI
 - New standard produced by the Chinese government
 - Requires all Wi-Fi companies operating in China to comply with the standard
 - Requires international companies to partner with a local company to gain access to the standard (considered a national secret)

Wireless Security Issues

- Security is off by default
- Security is implemented poorly
 - Shared key modes, potentially less secure than WEP
- Reliance on security by obscurity
 - Disabling SSID broadcasting
 - MAC filtering

Wireless Technology Issues

- People want wireless NOW!
- If you don't implement it they will
- Wireless hotspots

Wellington WarDrive

- Kismet (802.11b)
 - 232 Networks
 - 142 unencrypted (includes hotspots)
- Netstumbler (802.11b/g)
 - 161 Networks
 - 91 unencrypted (includes 60 hotspots)
- 20% of networks still unencrypted (not including hotspots)

- Channels
- SSIDs
- Filters

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise
0020A64F3EFF	cafenet		11	54 Mbps		AP		31	-69	-100
020CF17F62D2	amoh		10	11 Mbps	(User-d...	Peer		26	-74	-100
0204235D9181	Deloitte-WP		11	11 Mbps	Intel	Peer			-69	-100
0020A64F4807	cafenet		6	54 Mbps		AP			-70	-100
000F6659D8AA			11	54 Mbps	Linksys	AP	WEP	23	-64	-100
00022DBA0C7E	cafenet		6	11 Mbps	Proxim (...)	AP			-65	-100
0020A651338F	cafenet		11	54 Mbps		AP			-60	-100
0020A6513629	cafenet		6	54 Mbps		AP			-73	-100
00E00304B3B7	MW-1122		8	11 Mbps	Nokia	AP	WEP		-76	-100
000F66E10485	PACRAD		6	54 Mbps	Linksys	AP	WEP		-56	-100
0020A651335F	cafenet		11	54 Mbps		AP			-59	-100
00022DB1A8C3	cafenet		11	11 Mbps	Proxim (...)	AP			-44	-100
0020A64F47D6	cafenet		6	54 Mbps		AP			-40	-100
00022DBA16CB	cafenet		1	11 Mbps	Proxim (...)	AP			-51	-100
00022D879279	cafenet		6	11 Mbps	Proxim (...)	AP			-65	-100
00022D879506	cafenet		6	11 Mbps	Proxim (...)	AP			-76	-100
000352F00BE0	Telecom Wireless Hotspot Service		1	54 Mbps		AP			-50	-100
00409654DD88			6	11 Mbps	Cisco	AP	WEP		-75	-100
000C41D660BA	linksys-g		6	54 Mbps	Linksys	AP			-78	-100
00409654044D	MSFTWLAN		6	11 Mbps	Cisco	AP	WEP		-78	-100
00022DB08995	cafenet		11	11 Mbps	Proxim (...)	AP			-47	-100
000785B3F76A			11	11 Mbps	Cisco	AP	WEP		-77	-100
00022D8796A0	cafenet		6	11 Mbps	Proxim (...)	AP			-63	-100
000CDB8158C1	wlan2		1	54 Mbps		AP	WEP		-78	-100
000785B3F42F			11	11 Mbps	Cisco	AP	WEP		-73	-100
000D889D8821	cafenet		11	22 Mbps	D-Link	AP			-76	-100
00022D8797D5	cafenet		6	11 Mbps	Proxim (...)	AP			-59	-100
00022DB1AC37	cafenet		1	11 Mbps	Proxim (...)	AP			-63	-100
000958FD6620	SYBASE-TRAVEL		11	54 Mbps	Netgear	AP	WEP		-53	-100
000352EFF9E0	Telecom Wireless Hotspot Service		1	54 Mbps		AP			-55	-100
000958AC5994	FUZZYNAVEL		3	54 Mbps	Netgear	AP	WEP		-61	-100
0020A64F4805	cafenet		11	54 Mbps		AP			-38	-100
000D88E60015	ZeroOne WiFi		6	54 Mbps	D-Link	AP			-72	-100
00095B53FED6	Becker		3	11 Mbps	Netgear	AP	WEP		-80	-100
00409641976D	L10_GA		6	11 Mbps	Cisco	AP	WEP		-77	-100
00026F0821D8	korokoro		6	11 Mbps	Senao Intl	AP			-77	-100

Distance Is Relative



We DO have other dishes at hand here at the Massey Wellington campus, but they're not quite so portable ! Here's Tim showing our "Spider Skimmer" in it's "walkabout" mode - to spare yourself curious glances slip the antenna into a plastic shopping bag perhaps. For fixed use simply strap the bamboo handle to a tripod - or even -gasp!- cut it off. 6th May 2004

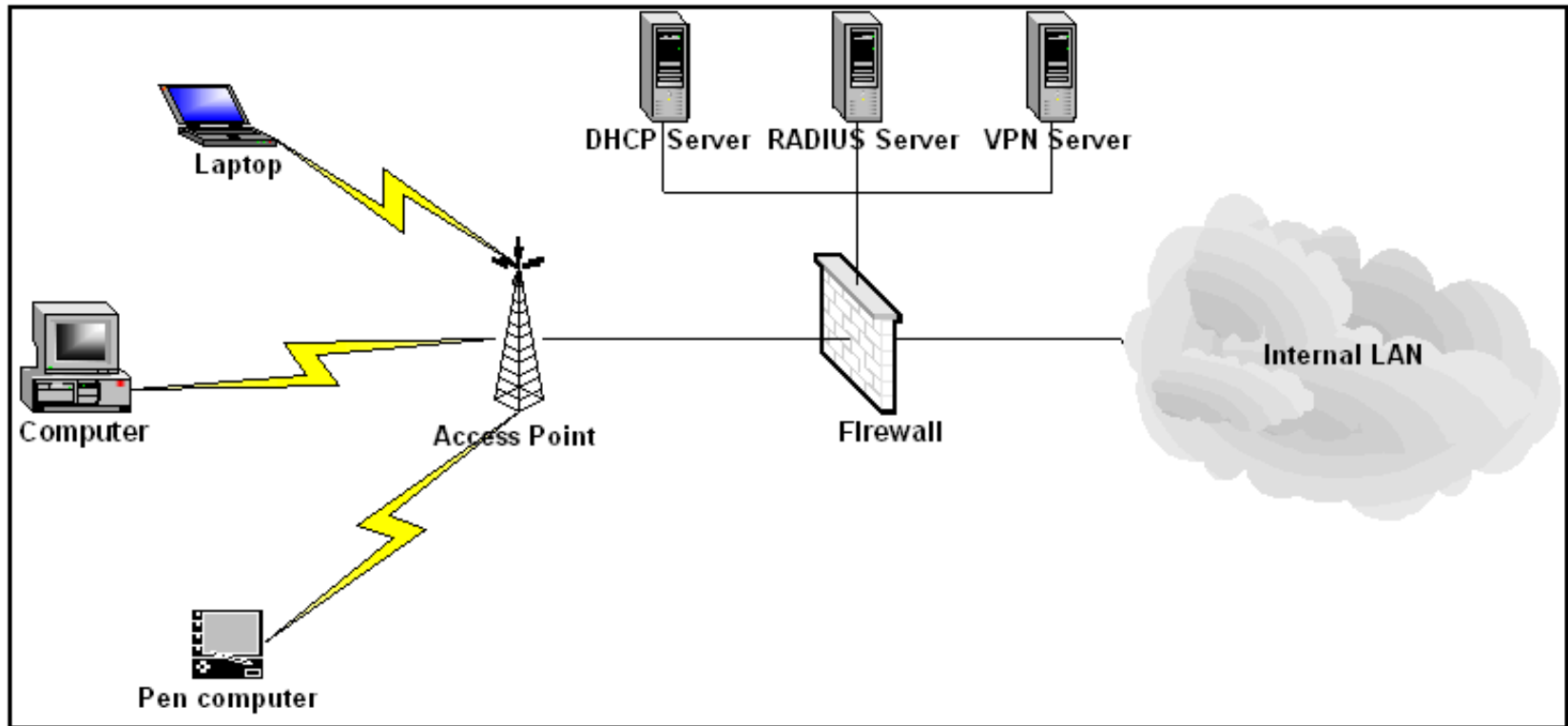
HotSpot Issues

- Public wireless access
 - CafeNet
 - Telecom Wireless Hotspot Service
- No authentication of Access Point
- Users enter account credentials to access Internet
- Prone to Rogue APs and credential theft
 - Airsnarf

Wireless Defenses

- Treat wireless networks as untrusted, like the Internet
- Rotate encryption keys
- Use strongest security available
- Can AP default admin user accounts
- Regularly search for rogue APs
- User hotspot education

Wireless Network Design



Other Technologies - Bluetooth

- Many phones now come with bluetooth
- More bluetooth devices than 802.11 devices
- All security is optional
- Most users don't bother to secure their phones
- Bluetooth Wardriving!!!

Base Address: 00:10:60:A5:0E:70

LS	Address	Clk Off	Class	Name
25	00:0E:ED:25:F8:00	0x69b3	0x50020c	CSC 7610
27	00:0A:D9:B0:17:05	0x451e	0x520204	n/a
20	00:60:57:92:BA:0F	0x23d8	0x500204	n/a
20	00:0E:07:55:E4:17	0x185e	0x520204	T610
68	00:07:E0:2E:5E:20	0x0a50	0x100114	n/a
28	00:10:60:A2:6F:2F	0x1790	0x320104	n/a
18	00:02:C7:07:38:32	0x0869	0x12010c	n/a
19	00:02:C7:2E:DB:36	0x2780	0x400204	n/a
72	00:0E:07:6B:E0:39	0x0a7a	0x520204	K700i
20	00:0E:07:52:B9:41	0x4441	0x520204	n/a
25	00:0E:07:55:E2:44	0x5daf	0x520204	n/a
27	00:60:57:62:D7:47	0x2bbc	0x502204	n/a
20	00:02:EE:19:B6:56	0x1e1a	0x502204	Nokia 6310
24	08:00:1F:BE:09:64	0x0e12	0x500204	Dee
11	00:10:60:A6:F9:72	0x5a9b	0x120104	n/a
21	00:0E:07:20:D4:76	0x6f30	0x520204	SacksT610
18	00:02:EE:51:77:86	0x4636	0x502204	n/a
11	00:10:C6:26:24:9B	0x3196	0x00010c	n/a
27	00:0E:6D:2C:2B:9E	0x6eff	0x500204	n/a
13	00:0A:D9:DD:58:A0	0x48d8	0x520204	T610
20	00:0A:3A:50:89:A2	0x08fd	0x00010c	n/a

Devices found: 21

Non-discoverable Phones

- Most bluetooth devices allow you to make them non-discoverable
- Do not broadcast
- Still able brute-force MAC address to connect
- Redfang tool does this for you

Bluetooth Attacks

- Bluesnarfing
- Backdooring
- Bluebugging
- Bluejacking