Wireless Auditing on a Budget

Open Source on Low Cost Hardware

James A. Edge Jr., CISSP, CISM, CISA, CPTE, MCSE
Sr. Security Analyst
Cincinnati Bell Technology Solutions

Agenda & Presentation Goals

- Background & Experience
- Wireless Handhelds
  - Past
  - Present
  - Future
- Wireless 802.11 Auditing
  - Access Point mapping
  - Rogue Access Point discovery
  - Wireless Security testing
  - Wireless client security
- Bluetooth Wireless Auditing
- Current Android Tools
- Questions

Agenda & Presentation Goals

- Provide detailed documentation on using the hardware and software discussed during this presentation.
- Continue to update the documentation and provide support for any audit team interested in using the hardware and tools discussed.

Background & Experience

- From 2004-2009 I was the an IT Auditor responsible for Penetration Testing for the audit shops in NY and GA.
- Specialized in Wireless Auditing using Open Source software.

Commercial Wireless Tools

- PROS:
  - Commercial Support
  - Simple, easy to use, interface
  - Enterprise Solution

- CONS:
  - Cost
  - Enterprise Solution
  - WiFi Only
  - Lack of audit features

Wireless Handheld History

Fluke Networks Waverunner
Wireless Network Analyzer
$7,000

Fluke Networks OptiView
Wireless Network Analyzer
$11,000

AirMagnet Handheld for Pocket PC
$5,000

Commercial Handhelds

Wireless Handheld History

Compaq Ipaq
Two slot PCMCIA backpack

SMC 802.11 b
External Antenna

Familiar Linux
Kismet

Compaq/HP Ipaq & Open Source Software

Wireless Handheld History

Holux GPS Compact Flash

Open Source Software and the Ipaq allowed for access point mapping with GPS

Wireless Handhelds Today

Fluke Networks AirCheck™
Wi-Fi Tester
$2,000

Fluke Networks EtherScope™
Series II Network Assistant
$7,000

Commercial Handhelds

Wireless Handhelds Today

$150

Nokia N810 Internet Tablet
Maemo Linux
802.11g, Bluetooth, & GPS

Nokia Internet Tablets

- 4.13 in diagonal screen
- Maemo Linux Operating System
  - Customized Debian Linux
- USB Host Mode (external 802.11 a/b/g/n and Ethernet adapters)
- Bluetooth GPS support
- Large hacker community supporting the devices and the operating system
  - Hardware hacking
  - Porting software

Nokia Internet Tablets

- Nokia N770
  - Released November 2005
  - Maemo Linux OS 2006
- Nokia N800
  - Released January 2007
  - Maemo Linux OS 2007 (Chinook)
  - Front Camera added
- Nokia N810
  - Released January 2007
  - Maemo Linux OS 2008 (Diablo)
  - Keyboard & GPS added
- Nokia N900
  - Released November 2009
  - Maemo Linux 5 (Fremantle)
  - Smartphone

Wireless Auditing with the N810

- Identify and mapping WiFi access points
- Tracking down potential rogue access points
- Testing WiFi Access Point security
- Testing WiFi client security
- Identify Bluetooth devices

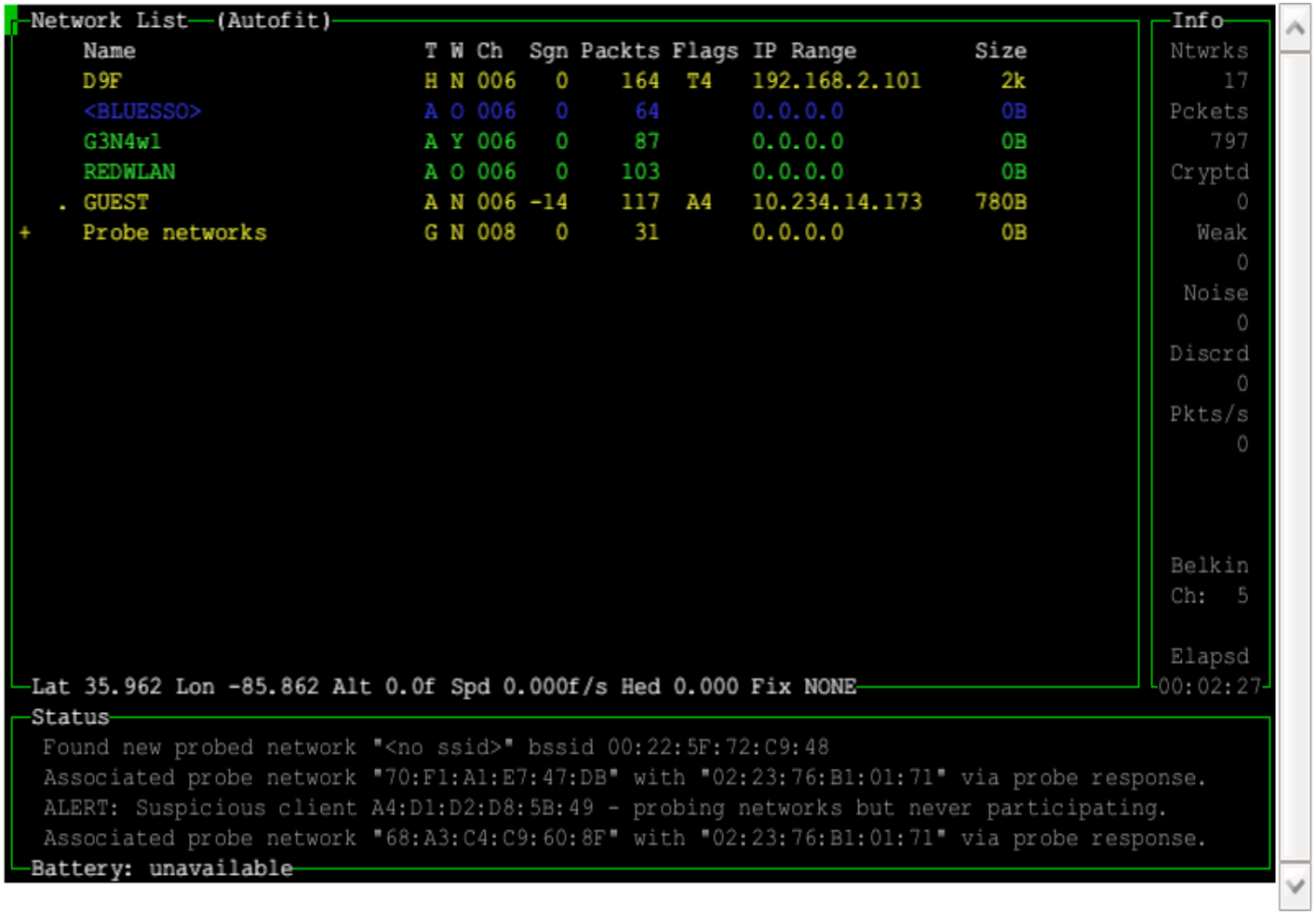
Wireless Auditing with the N810

- Kismet
  - 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.
- Aircrack-ng
  - 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.
  - Impersonate an access point to test wireless client security.
- Btscanner
  - Bluetooth scanner and brute-force tool

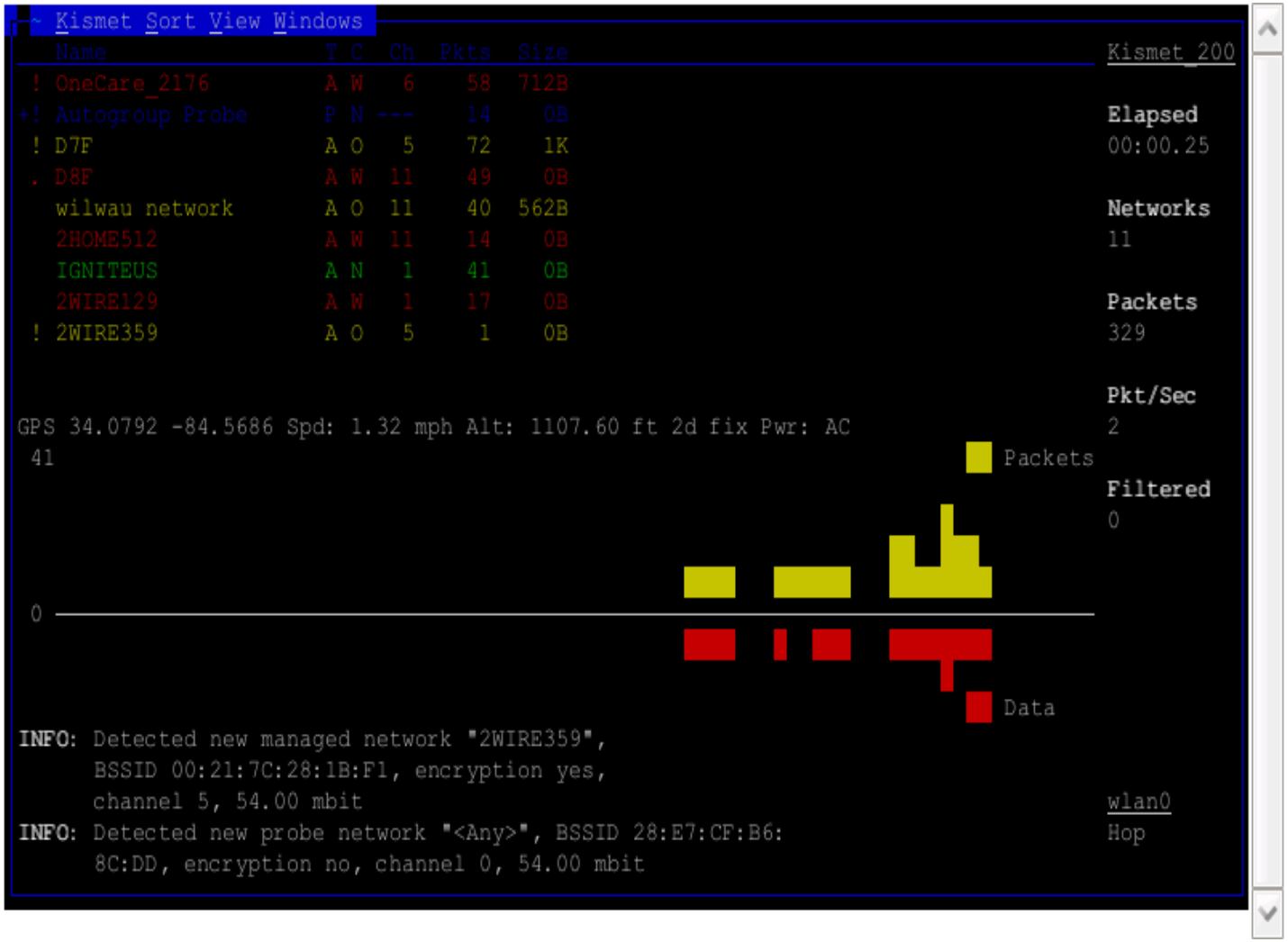
Nokia N810 802.11 Hardware

- Internal 802.11 wireless
  - No Opensource drivers for internal 802.11 wireless
  - Kismet does not support signal strength on internal wireless
  - Great for war driving/walking to map access points
- External 802.11 wireless USB adapter
  - Packet injection for AP/Client security testing
  - Signal strength readings for rogue access point tracking

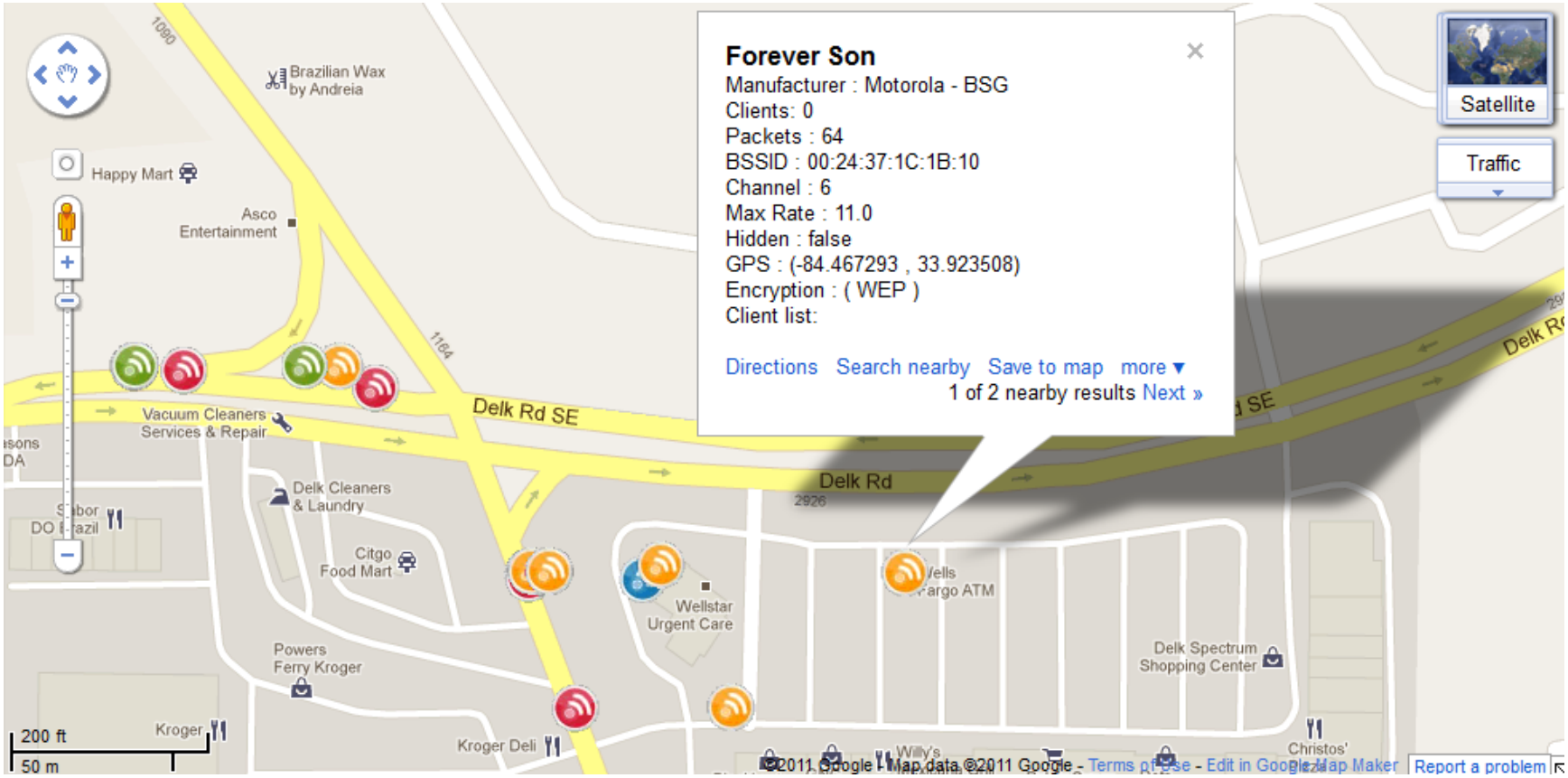
Kismet (Oldcore) on Nokia N810



Kismet (Newcore) on Nokia N810



Plotting Access Points



Kismet: Tracking Rogue APs

- Kismet signal strength readings can be useful in tracking where rogue access points are located.
  - Signal strength numbers vary by wireless chipset. You must always compare the numbers from the same card.
  - Test the wireless card on an AP you control to determine what signal readings
- MAC addresses obtained from Kismet can be researched to identify the manufacturer.

Aircrack-ng: Encryption Testing

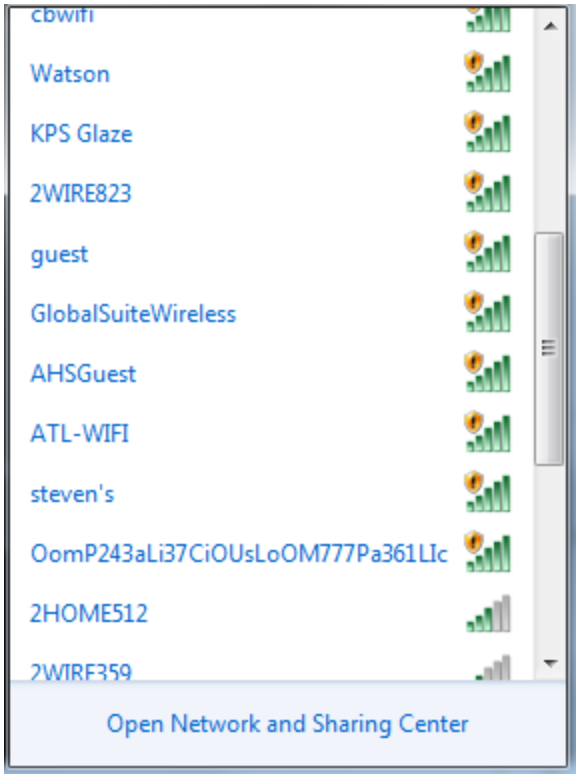
- Don’t even bother
  - WEP cracking is trivial and only should be done in a penetration testing environment where you need to access the network.
  - WPA/WPA2 have no weaknesses in the implementation of the protocol. Cracking an 8 character alphanumeric password will take 33 years using the best GPUs available.

Aircrack-ng: Client Security

- The airbase-ng command of the Aircrack-ng suite allows you to configure a decoy access point to test client side wireless security.
- Airbase-ng will mimic the name of any access point the client sends a probe request for.
  - If a client has previously connected to an access point at a coffee shop, airport, or hotel, it will save that information and send out a probe request in an attempt to connect to those access points when the wireless interface starts up.
  - Clients that connect to airbase-ng can be flagged for audit remediation steps.
- Advanced client side testing can leverage Metasploit for password sniffing and browser exploit attacks.

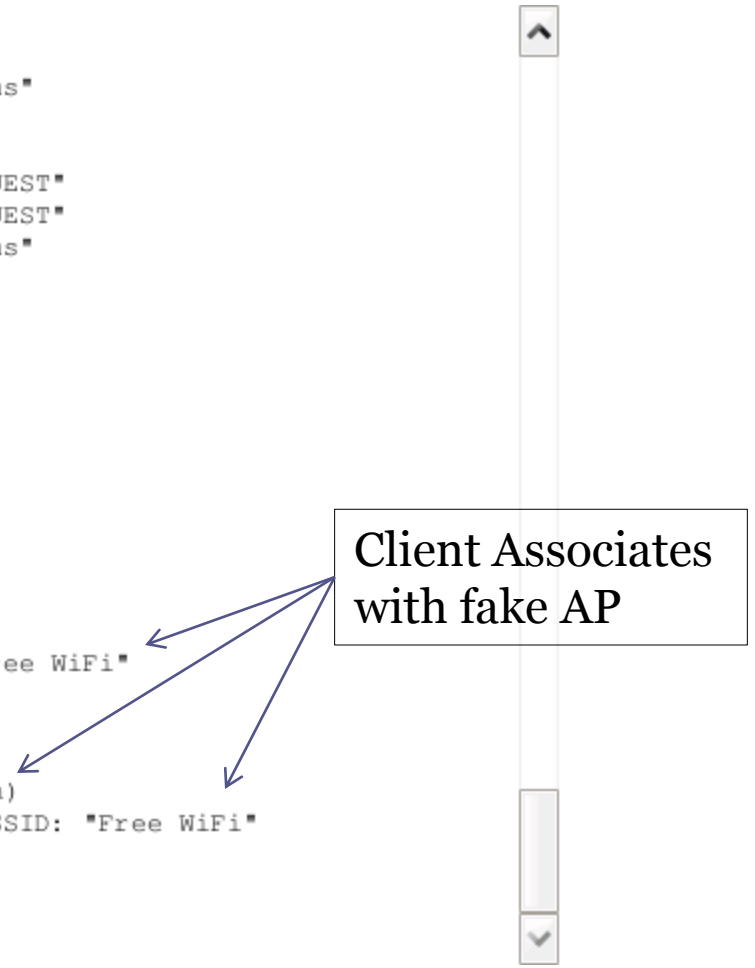
Aircrack-ng: Client Security

- Windows wireless client software will show all the “access points” available that airbase-ng is serving.
- These “access points” are names of all access points this client has connected to in the past.



Aircrack-ng: Client Security

```
17:40:07  Got broadcast probe request from 00:27:10:68:31:A8
17:40:07  Got broadcast probe request from DC:2B:61:43:47:3A
17:40:07  Got directed probe request from 00:27:10:68:31:A8 - "Gus"
17:40:07  Got broadcast probe request from 60:FB:42:D8:CB:A4
17:40:11  Got broadcast probe request from 00:24:2B:9A:B3:A5
17:40:12  Got directed probe request from D8:30:62:76:D8:D3 - "GUEST"
17:40:12  Got directed probe request from D8:30:62:76:D8:D3 - "GUEST"
17:40:15  Got directed probe request from 00:27:10:68:31:A8 - "Gus"
17:40:15  Got broadcast probe request from 00:27:10:68:31:A8
17:40:16  Got broadcast probe request from 5C:AC:4C:6A:A5:3B
17:40:17  Got broadcast probe request from 00:24:2B:33:D0:A6
17:40:17  Got broadcast probe request from 00:24:2B:33:D0:A6
17:40:21  Got broadcast probe request from 00:27:10:68:31:A8
17:40:22  Got broadcast probe request from 90:4C:E5:2A:03:65
17:40:22  Got broadcast probe request from 90:4C:E5:2A:03:65
17:40:22  Got broadcast probe request from 90:4C:E5:2A:03:65
17:40:22  Got broadcast probe request from 90:21:55:C1:21:C9
17:40:22  Got broadcast probe request from C0:CB:38:81:67:F1
17:40:23  Got broadcast probe request from 00:22:FA:C8:21:30
17:40:23  Got broadcast probe request from 00:25:56:A0:DE:EA
17:40:24  Got directed probe request from 20:7C:8F:4F:BA:E0 - "Free WiFi"
17:40:24  Got broadcast probe request from 90:4C:E5:64:62:49
17:40:24  Got broadcast probe request from 00:24:2C:28:23:B4
17:40:24  Got broadcast probe request from 00:24:2C:28:23:B4
17:40:25  Got an auth request from 20:7C:8F:4F:BA:E0 (open system)
17:40:25  Client 20:7C:8F:4F:BA:E0 associated (unencrypted) to ESSID: "Free WiFi"
17:40:25  Got broadcast probe request from 7C:61:93:A3:06:C2
17:40:25  Got broadcast probe request from 7C:61:93:A3:06:C2
```

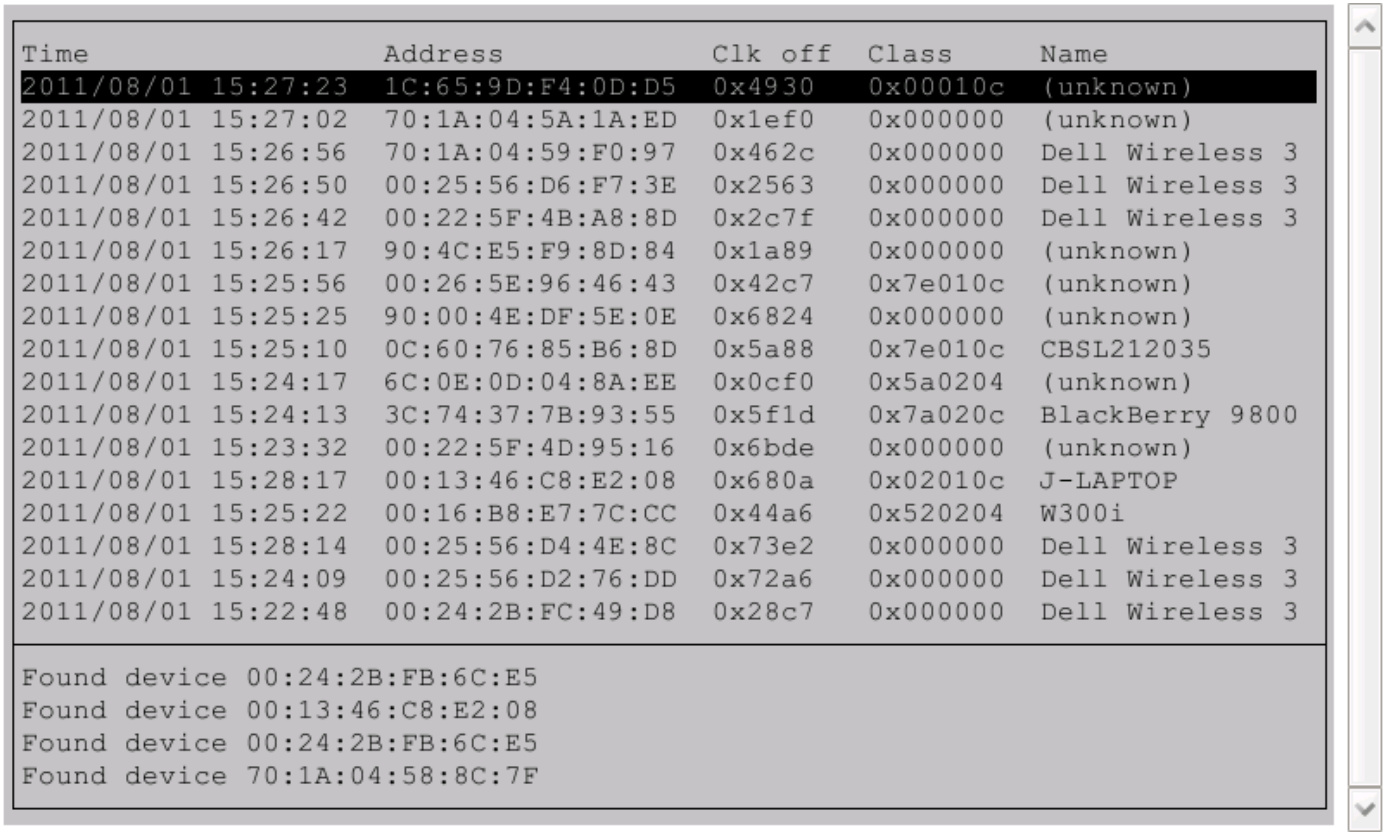


Bluetooth Security

- Btscanner
  - Text menu based Bluetooth sniffer that identifies all Bluetooth devices communicating in your environment.

Bluetooth Device Identification

Btscanner – Device scanning



Time	Address	Clk off	Class	Name
2011/08/01 15:27:23	1C:65:9D:F4:0D:D5	0x4930	0x00010c	(unknown)
2011/08/01 15:27:02	70:1A:04:5A:1A:ED	0x1ef0	0x000000	(unknown)
2011/08/01 15:26:56	70:1A:04:59:F0:97	0x462c	0x000000	Dell Wireless 3
2011/08/01 15:26:50	00:25:56:D6:F7:3E	0x2563	0x000000	Dell Wireless 3
2011/08/01 15:26:42	00:22:5F:4B:A8:8D	0x2c7f	0x000000	Dell Wireless 3
2011/08/01 15:26:17	90:4C:E5:F9:8D:84	0x1a89	0x000000	(unknown)
2011/08/01 15:25:56	00:26:5E:96:46:43	0x42c7	0x7e010c	(unknown)
2011/08/01 15:25:25	90:00:4E:DF:5E:0E	0x6824	0x000000	(unknown)
2011/08/01 15:25:10	0C:60:76:85:B6:8D	0x5a88	0x7e010c	CBSL212035
2011/08/01 15:24:17	6C:0E:0D:04:8A:EE	0x0cf0	0x5a0204	(unknown)
2011/08/01 15:24:13	3C:74:37:7B:93:55	0x5f1d	0x7a020c	BlackBerry 9800
2011/08/01 15:23:32	00:22:5F:4D:95:16	0x6bde	0x000000	(unknown)
2011/08/01 15:28:17	00:13:46:C8:E2:08	0x680a	0x02010c	J-LAPTOP
2011/08/01 15:25:22	00:16:B8:E7:7C:CC	0x44a6	0x520204	W300i
2011/08/01 15:28:14	00:25:56:D4:4E:8C	0x73e2	0x000000	Dell Wireless 3
2011/08/01 15:24:09	00:25:56:D2:76:DD	0x72a6	0x000000	Dell Wireless 3
2011/08/01 15:22:48	00:24:2B:FC:49:D8	0x28c7	0x000000	Dell Wireless 3

Found device 00:24:2B:FB:6C:E5
Found device 00:13:46:C8:E2:08
Found device 00:24:2B:FB:6C:E5
Found device 70:1A:04:58:8C:7F

Bluetooth Device Identification

Btscanner – Device details

```
RSSI:    +0   LQ:  000    TXPWR:  Cur   +0
Address:       3C:74:37:7B:93:55
Found by:      00:1D:6E:D9:4B:EB
OUI owner:
First seen:    2011/08/01 15:24:13
Last seen:     2011/08/01 15:24:13
Name:          BlackBerry 9800
Vulnerable to:
Clk off:       0x5f1d
Class:         0x7a020c
               Phone/Smart phone
Services:      Networking,Capturing,Object Transfer,Audio,Telephony

HCI Version
-----------
LMP Version: 2.1 (0x4) LMP Subversion: 0x1d1f
Manufacturer: Texas Instruments Inc. (13)
```

```
Found device 00:16:B8:E7:7C:CC
Found device 70:1A:04:58:8C:9E
Found device 00:25:56:D4:4E:8C
Found device 00:13:46:C8:E2:08
```

Bluetooth Vulnerabilities

- Microsoft Security Bulletin MS11-053 - Critical
  - Vulnerability in Bluetooth Stack Could Allow Remote Code Execution
  - http://www.microsoft.com/technet/security/Bulletin/MS11-053.mspx
  - Effects fully patched (as of 7/12/2011) Windows 7 and Vista.

Bluetooth Vulnerabilities

Joshua Talbot, security intelligence manager for **Symantec Security Response**, said the vulnerability could be exploited without any alerts being sent to the victim PC.

"An attacker would exploit this by sending specific malicious data to the targeted computer while establishing a Bluetooth connection," Talbot said. "Because of a memory corruption issue at the heart of this vulnerability, the attacker would then gain access to the computer. All this would happen before any notification alerts the targeted user that another computer has requested a Bluetooth connection."

Although it is unlikely, such a vulnerability could be used to power a computer worm that spreads from one Bluetooth-enabled Windows laptop to another, Talbot said.

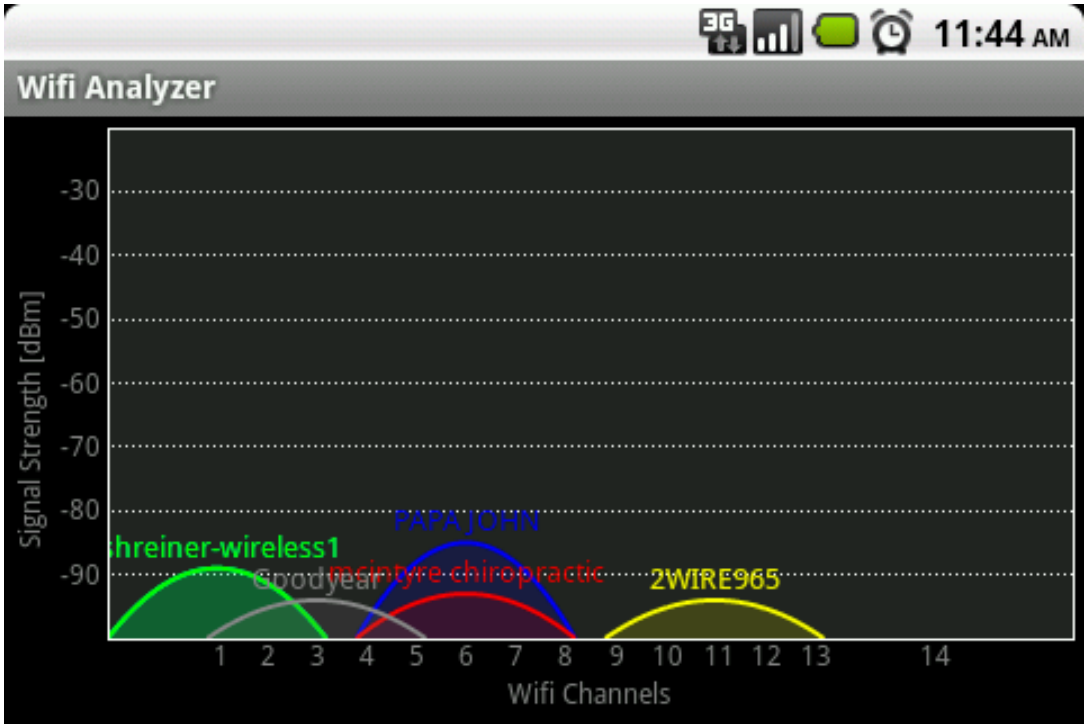
http://krebsonsecurity.com/2011/07/microsoft-fixes-scary-bluetooth-flaw-21-others/

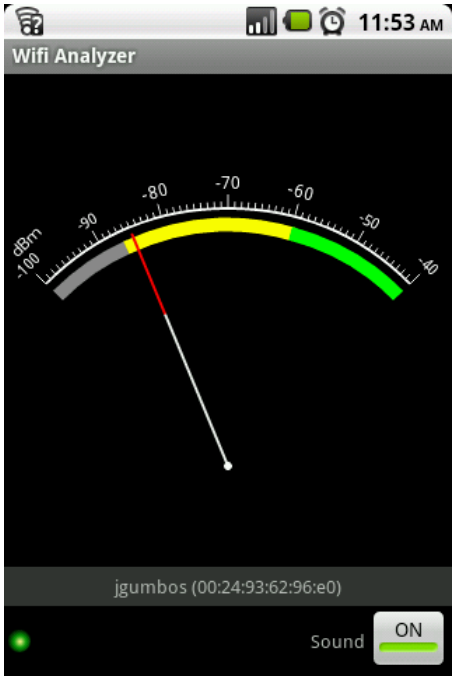
Wireless Handheld Future…

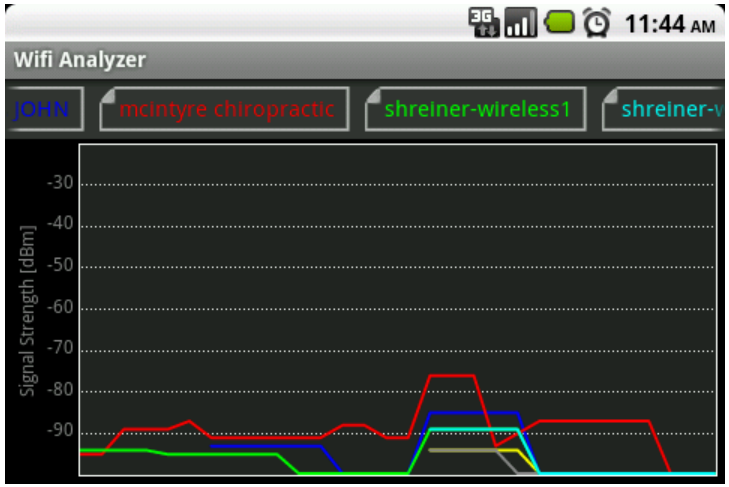
Wireless Handheld
A Peak into the Future

HTC Droid
Android Linux
802.11g, Bluetooth, & GPS

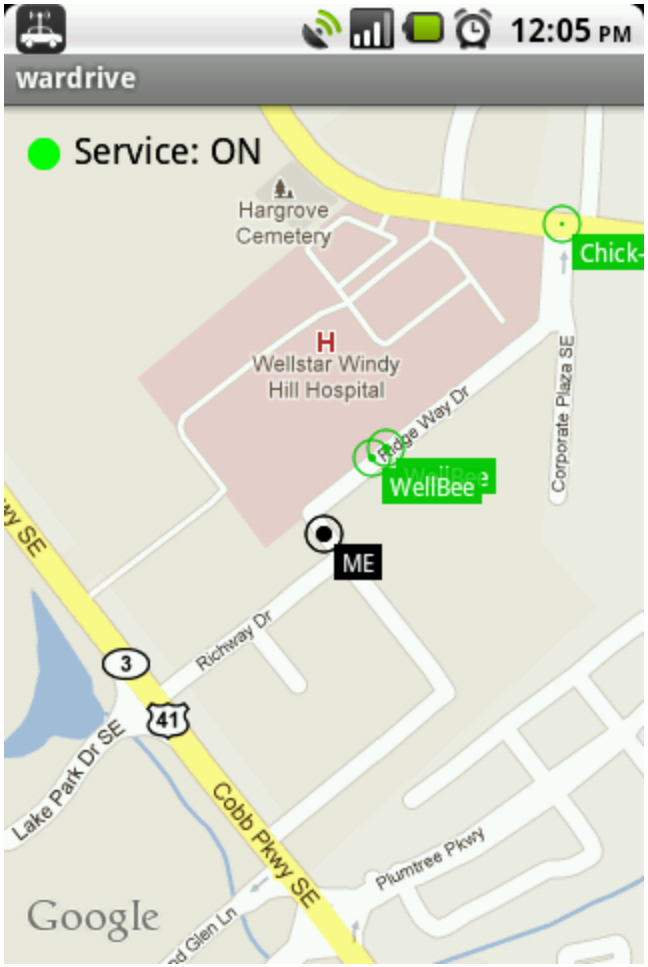
WiFi Analyzer





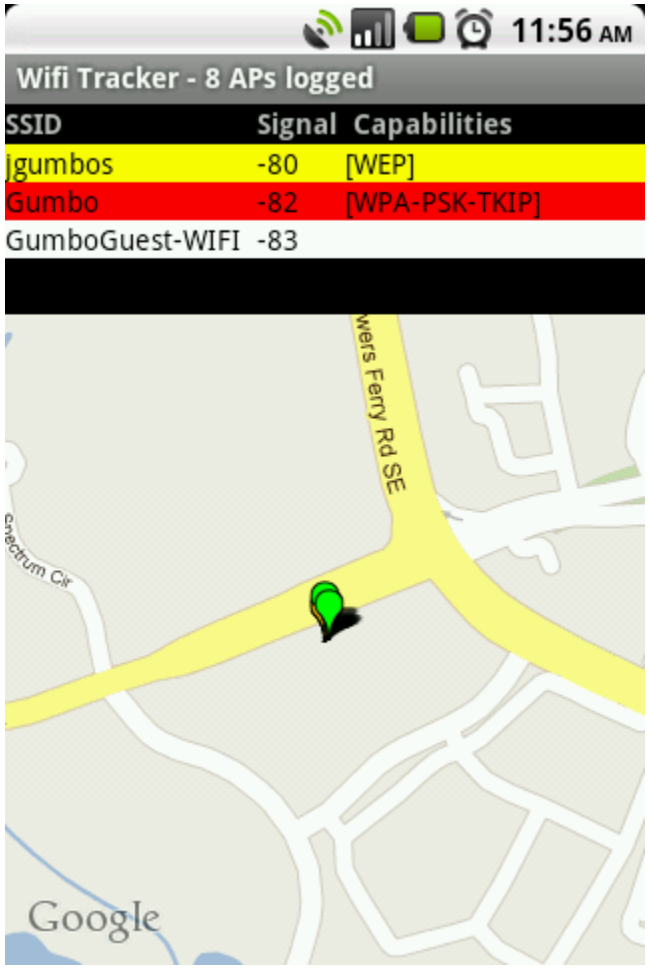


Wardrive



Map access points using the phones internal wireless, GPS, and Google Maps.

WiFi Tracker



Questions

Contact Information

James A. Edge Jr.
james.edge@cbts.cinbell.com
james.edge@jedge.com
http://www.jedge.com