

Wireless Security:

The tools and the tricks to securing your network



Brad "RenderMan" Haines
RenderLab.net & The Church of Wifi
render@renderlab.net

Introduction

- Who am I?
- Why am I here?
- Why are you here?
- Scope of the talk
- Why you should stay awake

About Brad/Render

- Security and Wireless consultant in Edmonton and area
- Hacker and Security enthusiast, I live for this stuff
- Co-Author of *RFID Security* (Syngress 2006)
- Security researcher and re-founder of the Church of Wifi security group
- Frequent speaker on wireless and security (HOPE, Defcon, Shmoocon, ICE)

“It is not the goal of this presentation to tell you not to use wireless networks, but make you aware of the risk so you can make informed decisions about your usage of wireless technology and do everything possible to protect your organizations network infrastructure, data, and integrity of its client computers.” - Paul Asadoorian

Why are you here?

- Why wireless security is increasingly important
- Wireless security misconceptions
- Wireless security attacks and tools
- Wireless security detection and prevention
- Defensive computing
- Ask questions if I lose you (Free stuff for good questions!)
- Stay awake, I throw things (Free stuff!)
- Thanks for seeing the hacker instead of the fed

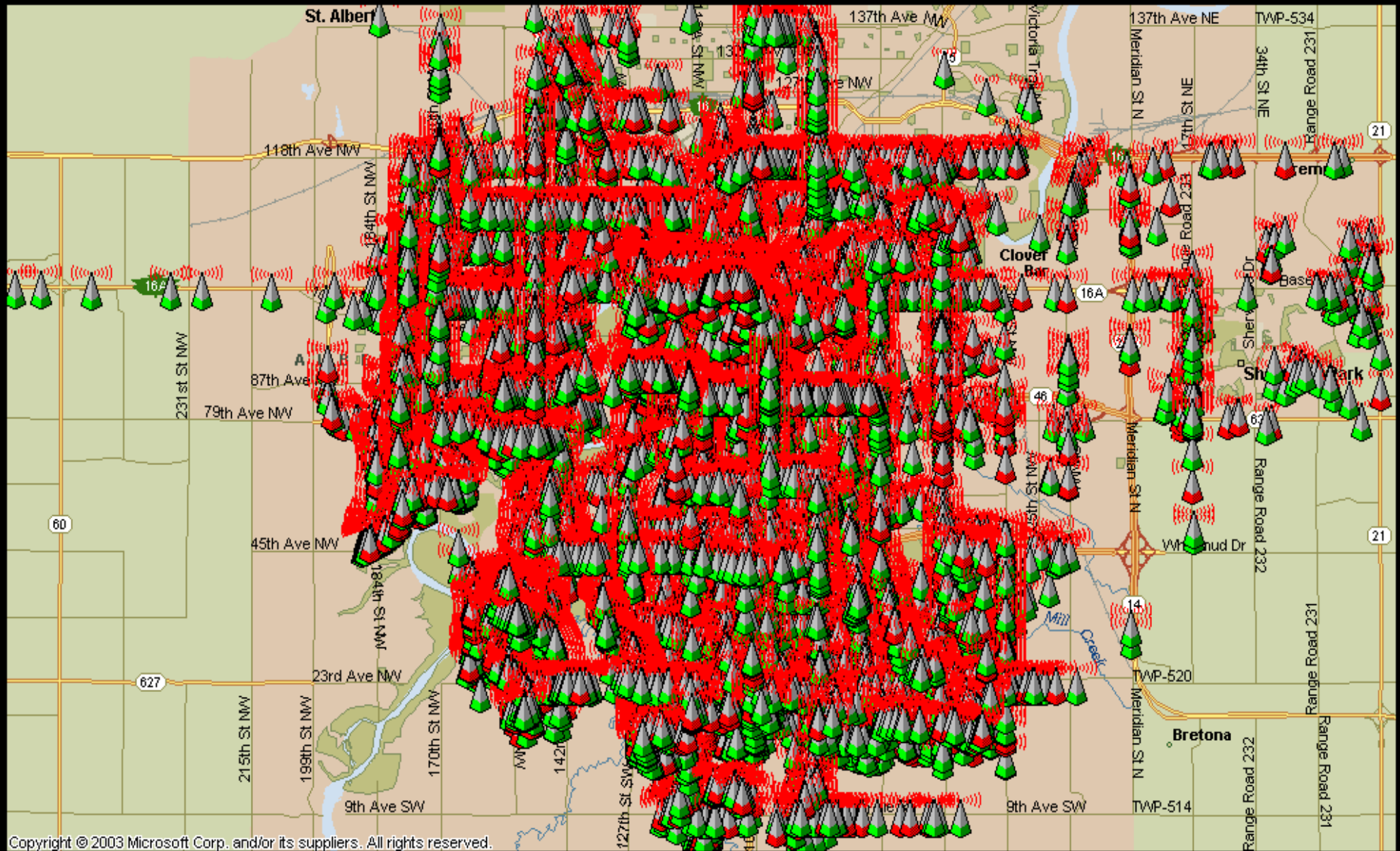
WiFi is everywhere

- \$30 for an AP at a computer shop
- Most laptops come with WiFi built in
- Surf from the bathtub!
- Personally discovered ~140,000 devices (~70,000 in Edmonton and area)
- Hotels, Airports, conferences, coffee shops, restaurants, etc...

More Devices

- Cell phones, PDA's, Refrigerators, Camera's, Game consoles, Washers & Dryers
- A 'Gee-Whiz' feature
- Drain on batteries
- Useful in a pinch
- Useful for impromptu wardriving

It's everywhere



Wireless Security

- Wireless security is not perfect
- Know your enemy and his tools
- Know your friends and their tools
- Know that they are sometimes the same
- It will affect you, stop running
- Don't forget Bluetooth!

Wardriving

- “The benign act of detecting wireless networks while in motion” - Blackwave
- Wireless networks are radios, Every card is a capable receiver
- Network information is broadcast with each packet - Network name, encryption status, associated clients all easily detected
- Add GPS for making fun maps
- Wigle.net – 7,851,320+ Nets with location (Nov 7th)

Kismet

- De facto free site survey tool
- Listens to all 802.11x traffic (Monitor Mode)
- Detects 'cloaked' networks
- Can include GPS for maps
- Remote drone sniffers for distributed monitoring
- Kismet-Newcore promises huge improvements
- Linux native, rough support in Windows (Kiswin, airpcap)
- Should be in every wireless toolkit

Kismet

- Very useful in monitoring your network
- Can detect several wireless attacks mentioned
- Good diagnostic tool
- Good for finding rogue AP's
- Have you spotted the rogue AP?

Kismet

root@wirelessdefence:~

File Edit View Terminal Tabs Help

Network List (Autofit)

Name	T	W	Ch	Pkts	Flags	IP Range
default	A	N	006	9	F	192.168.0.1
! iyonder.net	A	N	005	42	U4	10.254.178.254
! iyonder.net	A	N	001	22	A3	10.254.178.0
! eurospot	A	N	001	19	U4	204.26.5.166
! NETGEAR	A	0	006	5		0.0.0.0
. eurospot	A	N	011	14		0.0.0.0
! belkin54g	A	Y	011	17		0.0.0.0
! iyonder.net	A	N	011	16	A3	10.254.178.0
! tsunami	A	Y	007	17		0.0.0.0
! <no ssid>	A	0	003	11		0.0.0.0
Probe Networks	P	N	---	3		0.0.0.0
! iyonder.net	A	N	008	35		0.0.0.0
. <no ssid>	A	Y	011	5		0.0.0.0
NCDT_NET	A	Y	006	1		0.0.0.0
<no ssid>	A	Y	011	1		0.0.0.0

Info

Ntwrks
16
Pckets
228
Cryptd
4
Weak
0
Noise
0
Discrd
0
Pkts/s
8
Elapsd

00:00:20

Status

Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\036\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0 bssid 00:0A:8A:A2:C8:7F

Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP

Battery: AC 107%

Wireless security misconceptions

- *“Mac address filtering keeps most people out”*
- *“WEP is better than nothing”*
- *“I use WPA-PSK now, so I’m secure”*
- *“VPNs will protect me”*
- *“Nobody will find my wireless network”*

“Mac address filtering keeps most people out”

- MAC addresses can be observed without connecting
- Changing your own MAC address is easy
- A simple perl script makes it easy in linux:
 - <http://www.michiganwireless.org/tools/sirmacsalot/>
- Simple program to change it in Windows
 - <http://www.codeproject.com/tools/MacIdChanger.asp>
- Only useful in keeping authorized users from connecting unauthorized things

“WEP is better than nothing”

- WEP can be cracked in 10 minutes (any key length, start to finish)
- Goal is to collect enough IVs to be able to crack the key
 - IV = Initialization Vector, plain text appended to the key to avoid repetition
- Injecting packets to generate IV's
- Aircrack analyses the packets and gives you a key

[00:00:09] Tested 2 keys (got 1132959 IVs)

KB	depth	byte(vote)
0	0/ 1	86(266) 03(18) 32(9) 44(8) 81(5) EF(5) 05(4) 40(3) 7C(
1	0/ 1	65(398) B4(54) B9(17) F2(16) 93(15) C9(14) 79(13) 20(12) BA(
2	0/ 1	78(300) 50(78) 3E(8) 5F(8) B6(6) 8F(5) B1(3) 06(0) 0F(
3	0/ 1	38(225) 0F(33) 91(28) F1(21) CE(15) C0(12) CC(11) 93(9) 27(
4	0/ 1	8F(338) 48(15) D2(14) CB(12) 54(11) 49(10) B6(8) A2(7) 6C(
5	0/ 1	51(355) B1(25) 34(18) FC(16) 5C(15) 7E(13) 3A(11) D5(9) 23(
6	0/ 1	7B(288) 59(30) 65(26) DA(22) 46(20) DF(20) E0(16) 23(15) 54(
7	0/ 1	E0(998) D0(93) EE(75) 55(43) 44(39) 7D(33) 17(21) 12(20) 3C(
8	0/ 1	B4(226) 03(45) 7E(40) 26(36) E6(35) D8(28) 90(26) 91(20) 6E(
9	0/ 1	81(399) AC(44) 43(41) CE(33) 23(31) 95(27) D1(26) 19(23) 13(
10	0/ 1	8A(236) 9A(46) E8(46) 87(25) 85(23) 07(22) 30(22) 94(22) E4(
11	0/ 1	0D(279) 1A(28) 87(21) 6E(20) C3(20) F3(20) 03(19) 41(18) 73(
12	0/ 1	B1(355) 6F(37) 4C(31) 25(30) 6D(30) 8A(27) 22(26) 4B(26) EF(

KEY FOUND! [86:65:78:38:8F:51:7B:E0:B4:81:8A:0D:B1]

“I use WPA-PSK now, so I’m secure”

- WPA-PSK protected networks are vulnerable to dictionary attacks
 - This now works with WPA-PSK & WPA2-PSK (802.11i)
- Product of the Church of Wifi
- 47s gig of lookup tables for the top 1000 most common SSID's (~1.1 million words each) for instant cracking
- 256 bit keys, but generated from a user selected passphrase
- Users continue to choose dumb passphrases

“I use WPA-PSK now, so I’m secure”

- Spoof the MAC of an AP and tell clients to disassociate
- Sniff the network for the handshake when they reconnect
- Use coWPAtty to run a dictionary against packets
- By pre-computing the hashes we are able to test **20,000 keys/sec** instead of just **20 keys/sec**

File Edit View Terminal Tabs Help

```
[root@wirelessdefence cowpatty-3.0]# ./cowpatty -r wpa-test-01.cap -f dict -s cuckoo  
cowpatty 3.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>
```

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack. Please be patient.

key no. 1000: apportion

key no. 2000: cantabile

key no. 3000: contract

key no. 4000: divisive

The PSK is "sausages".

4089 passphrases tested in 200.51 seconds: 20.39 passphrases/second

```
[root@wirelessdefence cowpatty-3.0]#
```

File Edit View Terminal Tabs Help

```
[root@wirelessdefence cowpatty-3.0]# ./cowpatty -r wpa-test-01.cap -d hashfile -s cuckoo  
cowpatty 3.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>
```

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack. Please be patient.

The PSK is "sausages".

4089 passphrases tested in 0.21 seconds: 19493.89 passphrases/second

```
[root@wirelessdefence cowpatty-3.0]#
```

“VPNs will protect me”

- IPSec-based VPNs offer good protection on the wireless network
- They use strong encryption and are generally not vulnerable to MitM attacks
- However, usually used over open WiFi connections (airports, cafes, etc)
- Clients may still be vulnerable to attack and can be proxies into the VPN

“VPNs will protect me”

- The follow are areas of potential doom:
 - Attacking a client that is already VPN connected over wireless
 - Attacking the VPN concentrator itself
 - Attacking the DNS or DHCP server
- Security is like Ogres; they have layers
- VPNs are a layer, but not the whole Ogre

“Nobody will find my wireless network”

- World record from Defcon 13, 2005 was 125 miles - They drove to another state to receive!
- Personally done 5Km shots easily
- Check Wigle.net, your probably already there
- Expect to be found, prepare an appropriate defense
- Don't make yourself a target, don't use an obvious SSID

Wireless Security Misconceptions

- MAC address spoofing continues to get easier with automated tools being developed
- WEP can be cracked in 10 minutes with easily obtainable and cheap hardware/software
- WPA-PSK is vulnerable to offline dictionary attacks that are increasing in speed dramatically
- VPNs and the associated infrastructure must be properly secured & maintained
- VPNs do not protect the end user from many attacks on open wireless networks
- Wifi can travel really, really, really far

Attack tools and Detection

- Ad-Hoc network “Features”
- KARMA
- Airpwn
- Deauth/Auth flooding
- RF Jamming

Client security

- Often overlooked
- Attack the client device directly, ignore the AP
- New and highly vulnerable field
- Driver vulnerabilities bypass firewalls

Hacking the Friendly Skies

- Presented by Simple Nomad at Shmoocon 2006
- Exploits Windows Ad-Hoc networking features to easily get on the same subnet with other clients
- Clients out of range of a network switch to ad-hoc mode with the same SSID
- This has not been fixed by Microsoft, not a vulnerability, but a behavior

Hacking the Friendly Skies

- People are vulnerable even when not near a network (even at 30,000 feet)
- When used in conjunction with other attacks, can be quite dangerous
- Properly securing your laptop helps
 - Firewall, patches, IDS, No shares open, etc
 - Turn off WiFi when not needed (saves battery too!)

Bad Karma

- Rogue based attack, using “features” of the preferred network list
- Being the access point has it's advantages, you are the MitM
- Clients look for networks in their preferred list through probes
- Karma responds as the probed network
- Clients gladly connect to you

Bad Karma

- Karma has the ability to:
- **Respond to any probe request**
 - Provide a client with DHCP/DNS (poison DNS)
 - Become a web server for fake web sites (Phishing)
 - Proxies the client's traffic (password snarfing)
 - Take advantage of wireless driver vulnerabilities (r00t-fu)
- If you are the man in the middle, you can control what people send and receive....

File Edit View Terminal Tabs Help

```
[root@wirelessdefence karma-0.4]# bin/karma etc/karma.xml
```

```
Starting KARMA...
```

```
Loading config file etc/karma.xml
```

```
ACCESS-POINT is running
```

```
DNS-SERVER is running
```

```
DHCP-SERVER is running
```

```
POP3-SERVER is running
```

```
FTP-SERVER is running
```

```
[2006-01-20 22:43:58] INFO WEBrick 1.3.1
```

```
[2006-01-20 22:43:58] INFO ruby 1.8.4 (2005-12-24) [i386-linux]
```

```
[2006-01-20 22:43:58] INFO WEBrick::HTTPServer#start: pid=4962 port=80
```

```
HTTP-SERVER is running
```

```
CONTROLLER-SERVLET is running
```

```
EXAMPLE-WEB-EXPLOIT is running
```

```
Delivering judicious KARMA, hit Control-C to quit.
```

```
AccessPoint: 00:20:A6:54:3E:ED associated
```

```
DhcpServer: 00:20:a6:54:3e:ed (dell15150) <- 169.254.0.254
```

```
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
```

```
FTP: 169.254.0.254 myusername/mypassword
```

Good Karma

- Karma Detection: Use rglueap
- Catches clients who are automatically connecting to preferred SSIDs
- Answers to all probe requests just like Karma, holds them and reports on them
- IDS-like behavior, quarantine the mis-configured clients (dog pound)
- Still in beta, hard to setup...
- Could be detected by 'baiting' with lots of random probe requests

The Evil of Airpwn

- Uses two wireless cards, one to sniff, the other to inject (can use one card, but can be flaky)
- Injects responses to HTTP requests
- Responds quicker since we're on the same subnet and in the same room
- I now control your web content
- No demo, just goto <http://evilscheme.org/defcon/> - Warning, Goatse! NSFW!

The Evil of Airpwn

- Replace all image requests with goatse, tubgirl
- Browser based exploits (javascript)
- Image based exploits (WMF)
- Other apps (Eg. winamp playlists)
- Use your imagination
- Stumped the assembled masses at Defcon

Avoiding Airpwn'age

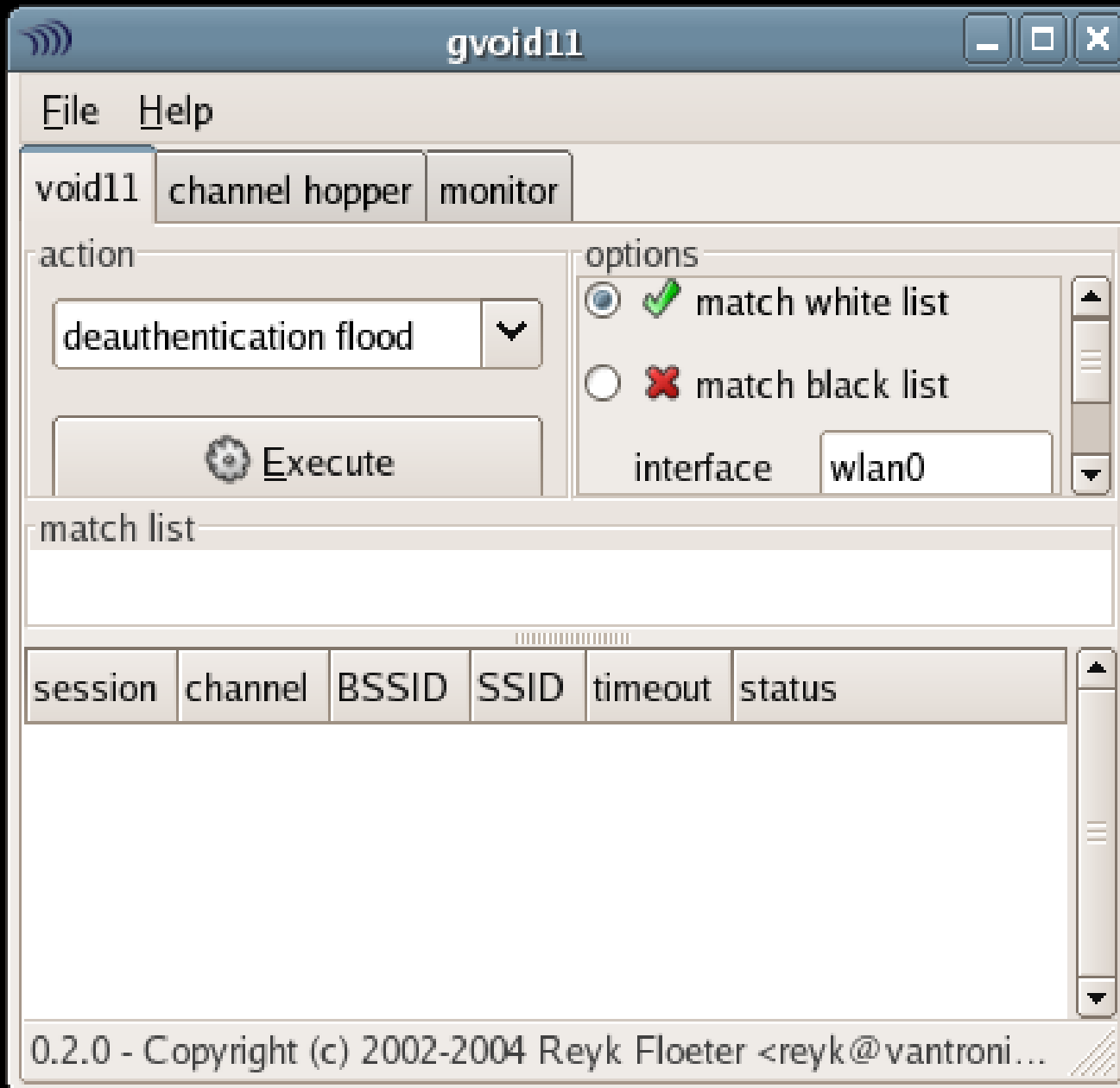
- Tunnel HTTP through something secure (SSH,SSL, IPSEC)
- Encrypt the link (WEP,WPA), keep attacker off
- Intelligent AP
 - Detect when a client spoofs the MAC of the AP
 - AP should see that a response came from the internal network and not the Internet
- Look around for people pointing and laughing at you, beat them senseless

Flooding

- Death Floods
 - Forge a deauth request from the AP to the client
 - Useful for IDSs, session containment
- Auth floods
 - Blast the AP with authentication requests
 - AP's freak out and shut down
- Broadcast floods
 - Generate thousands of fake access point beacons
 - Name them all the same as the target
 - No one knows what to connect to

Flooding












- Deauth most common
 - AP MAC and Client MAC are plaintext
 - Need smart gear to know not to disconnect
 - Void11
- Auth flood
 - Need intelligent AP
 - Need AP that can handle it
- FakeAP
 - Easy to spot, hard to mitigate
 - Fakeap, rfakeap



```
[root@wirelessdefence fakeap-0.3.2]# perl fakeap.pl --interface wlan0 --channel 11 --essid BANANA
fakeap 0.3.1 - Wardrivring countermeasures
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved
```

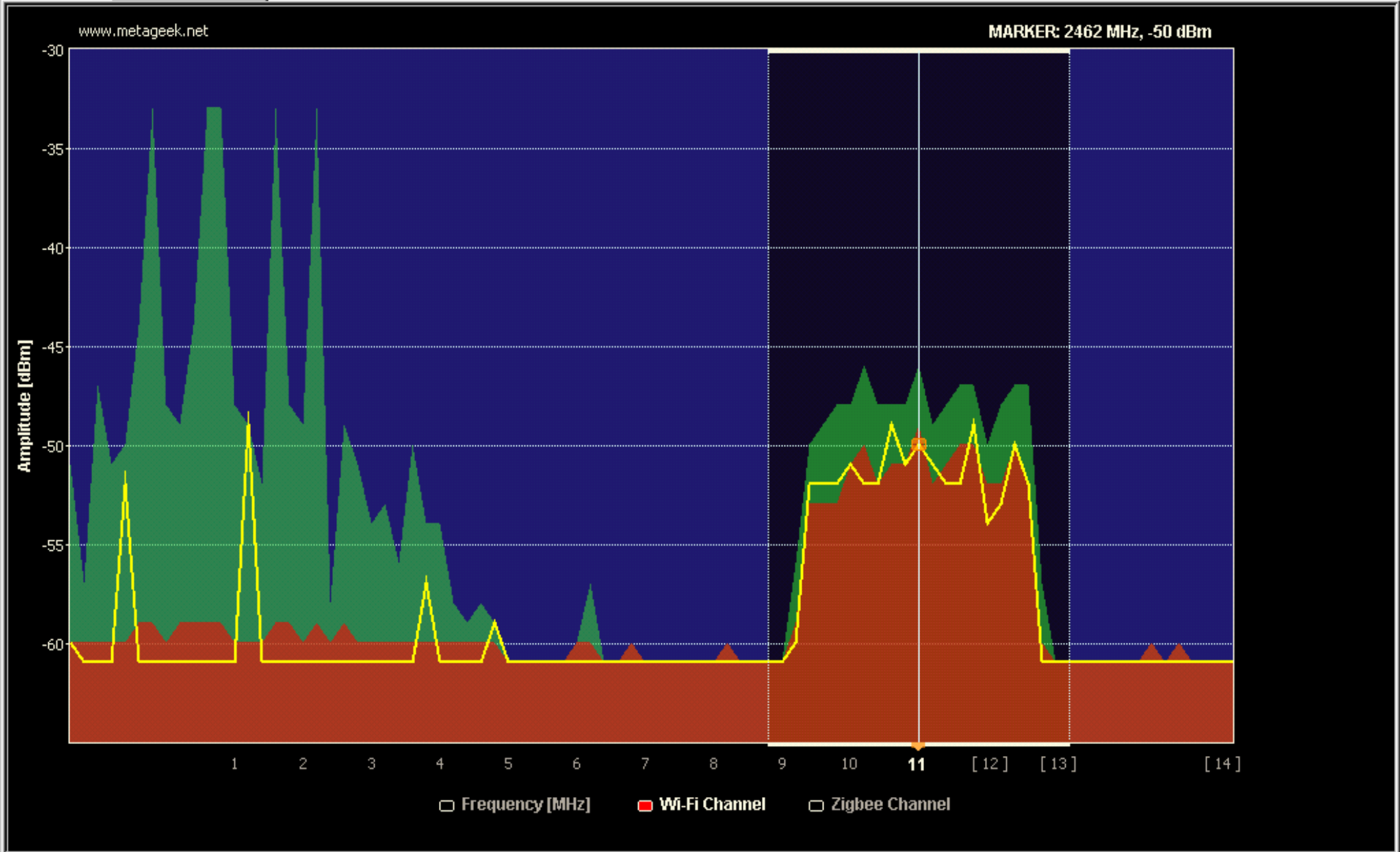
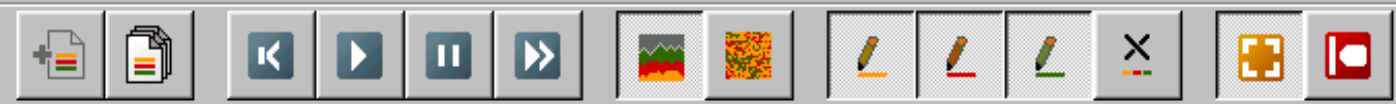
```
Using interface wlan0:
Static channel 11
Static ESSID BANANA
Using WEP with probability 1
Using supplied WEP key 866578388f517be0b4818a0db1
Using 4 words for ESSID generation
Using 2 vendors for MAC generation
```

/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig76: ESSID=BANANA chan=11 Pwr=Def WEP=Y MAC=00:00:00:00:00:00

MAC	SSID	Chan	Speed	Type	Enc...
 0000CEB8D54F	BANANA	11	11 Mbps	AP	WEP
 0000C0B9F88	BANANA	11	11 Mbps	AP	WEP
 0000C72FFC8	BANANA	11	11 Mbps	AP	WEP
 0000C8AE489	BANANA	11	11 Mbps	AP	WEP
 0000C361C75	BANANA	11	11 Mbps	AP	WEP
 0000C1FA804	BANANA	11	11 Mbps	AP	WEP
 0000CE022FC4	BANANA	11	11 Mbps	AP	WEP
 0000CCB8DD6	BANANA	11	11 Mbps	AP	WEP
 0000CE579BE7	BANANA	11	11 Mbps	AP	WEP
 0000C5BC03C	BANANA	11	11 Mbps	AP	WEP
 0000C76DE04	BANANA	11	11 Mbps	AP	WEP

Jamming

- Flood the 2.4Ghz spectrum with noise
- Some WiFi cards, some special drivers and your off....
- Most people can't detect raw RF
- Can cause major headaches for managers and IT personnel



Unjamming

- Need a basic Wireless IDS
- Kismet detects some flood attacks
- Higher end wireless IDS's can contain rogue AP's and clients
- Not much legal recourse – Public frequencies

Unjamming

- Need to invest in at least a basic spectrum analyser
- Wi-Spy
 - \$99 (US)
 - Runs on all platforms
- Great for troubleshooting
- Fingerprinting sources of interference (microwaves, cordless phones)
- Useful in detecting covert channels (channel 14)



Summary

- **Windows default behavior on wireless networks could allow an attacker to be on the same subnet**
- **Karma allows attackers to be on the same subnet and/or hijack a wireless connection by answering to all SSIDs**
- **Karma is fairly easy to detect by sending random SSID requests and seeing who answers**
- **Airpwn can inject attack packets into the wireless network and answer for HTTP requests**
- **Detecting Airpwn is difficult, use tunneling**
- **Deauth/auth and broadcast floods are easy to detect, harder to do anything about**
- **RF jamming is easy, but can be detected with tools such as Wi-Spy**

Defensive computing

- Three areas of wireless security:
 - **Home** - Home users typically have connections to your organization's network
 - **Road** - This is when a machine will be attacked the most
 - **Enterprise** - Secure your own wireless environment as much as possible
- Each is as important as the others
- Must all be taken seriously

Wireless Security: HOME

- Keep out the “accidental” wireless users:
 - Adjust the power output of your access point (if possible)
 - Use MAC address filtering
 - Change the default SSID
 - Enable WPA/WPA2
 - Use a strong (20+ char) passphrase
 - Don't use dictionary words
 - Implement a captive portal
 - Change default passwords
 - Use HTTPS to configure it
 - Check settings once in a while

Wireless Security: ROAD

- Make sure you're not an access point!
 - ICS Turns your card into an access point
 - People use your computer to access the network
- Don't automatically connect to networks
 - The network you connect to may not be safe
 - Be aware that by default you will always probe for open networks in your list
 - On both Windows and OS X
- Other wireless clients are better, like Intel
- Vista will fix some of this

Wireless Security: ROAD

- Do not connect to non-preferred networks
- Only connect to infrastructure networks
- Connect to networks “On-Demand”, not automatically
- Turn Off WiFi when not in use
- Be highly suspicious of where you are connecting
- Use VPN's

Wireless Security: ENTERPRISE

- Choose a managed system
 - Aruba, Cisco, Meru networks, etc..
- They can detect rogues and some attacks
- Choose an EAP type to distribute to clients
 - Three major ones:
 - EAP-PEAP - Built-in to Windows XP
 - EAP-TLS - Requires PKI
 - EAP-TTLS - Requires 3rd party supplicant under Windows

Wireless Security: ENTERPRISE

- Manage the client:
 - Personal Firewall
 - Central patch management
 - Enforce client security before connecting to network
 - Intrusion Prevention
- If the client is a risk, don't let them on!

Bluetooth: The forgotten wireless

- Bluetooth isn't safe either
- Most common on Cellphones
- Class 1 radio can travel 100 Meters
- 'Bluesniper' antenna detects at over half a mile
- Cheap (~\$40-50 for an adapter) and not normally checked for
- Lots of devices are default discoverable
- 21 devices discoverable out of 400 ICE attendees! (~19% of attendees)

- Apply Filter**
- Last Seen**
- Yesterday (20)
 - Now (4)
 - Last Hour (2)
- Location**
- ICE Conference (26)
- Type**
- Smart Phone (13)
 - Cellular Phone (11)
 - Handheld Computer (2)
- Services**
- SDP Server (2)
 - Fax (1)
 - Dial-up Networking (8)
 - Bluetooth Serial Port (1)
 - OBEX Object Push (9)
 - OBEX File Transfer (6)
 - Handsfree Audio Gateway (1)
 - Service Discovery (2)
 - Voice Gateway (8)
 - AVRCP Target (1)
 - Imaging (1)
 - SyncMLClient (1)
 - Nokia OBEX PC Suite Services (1)
 - Nokia SyncML Server (1)
 - SIM Access (1)
 - Hands-Free Audio Gateway (1)
 - Headset Audio Gateway (1)
 - WBTEXT (2)
 - HSP Gateway (2)
 - HFP Gateway (2)
 - Dialup Networking (2)
 - Object Exchange (2)
 - File Transfer (2)
- Hide Inactive Devices

Name	First Seen/LastSeen	Type/Flags	Location
Greg (00:0F:86:05:72:44)	11/06/06 at 11:33:25 (21) 11/06/06 at 11:49:43	Smart Phone	ICE Conference
BlackBerry 8700 (00:0F:86:43:19:25)	11/06/06 at 11:33:28 (90) 11/06/06 at 13:20:18	Smart Phone	ICE Conference
Nokia 6600 (00:0E:6D:44:FC:79)	11/06/06 at 11:34:31 (126) 11/06/06 at 13:21:17	Cellular Phone SDP	ICE Conference
Audiovox SMT5600 (00:09:2D:17:93:A4)	11/06/06 at 11:35:18 (89) 11/06/06 at 12:30:02	Smart Phone SDP	ICE Conference
NOKIA N80 (00:12:D1:08:74:5C)	11/06/06 at 11:50:15 (117) 11/06/06 at 15:06:54	Smart Phone SDP	ICE Conference
ZHAI (00:16:DB:55:4C:88)	11/06/06 at 11:50:34 (38) 11/06/06 at 13:18:27	Cellular Phone SDP	ICE Conference
Unknown (00:07:3F:06:3F:3F)	11/06/06 at 11:52:00 (1) 11/06/06 at 11:52:00	Smart Phone	ICE Conference
Unknown (00:09:2D:5B:81:21)	11/06/06 at 11:54:04 (2) 11/06/06 at 11:54:28	Handheld Computer	ICE Conference
Audiovox SMT 5600 (00:09:2D:05:D9:EB)	11/06/06 at 11:54:44 (28) 11/06/06 at 12:29:31	Smart Phone SDP	ICE Conference
Nokia 6265i (00:12:D2:6D:55:A2)	11/06/06 at 11:55:17 (37) 11/06/06 at 12:29:31	Cellular Phone SDP	ICE Conference
tkX BlackBerry 8100 (00:0F:86:5A:74:3B)	11/06/06 at 12:24:26 (101) 11/06/06 at 14:42:04	Smart Phone	ICE Conference
Michael Smithq (00:07:E0:63:B3:D2)	11/06/06 at 13:13:16 (44) 11/06/06 at 15:06:24	Smart Phone SDP	ICE Conference
T610 (00:0A:D9:F0:29:1B)	11/06/06 at 13:13:22 (112) 11/06/06 at 15:09:16	Cellular Phone SDP	ICE Conference
BlackBerry 7250 (00:0F:86:4F:1A:FE)	11/06/06 at 13:15:26 (29) 11/06/06 at 13:26:44	Smart Phone	ICE Conference
BlackBerry 7250 (00:0F:86:1C:D6:0A)	11/06/06 at 13:20:37 (144) 11/06/06 at 15:09:16	Smart Phone	ICE Conference
Unknown (00:16:B8:2E:29:E4)	11/06/06 at 13:24:38 (2) 11/06/06 at 13:25:00	Cellular Phone	ICE Conference
motoq (00:17:E2:2D:9A:3E)	11/06/06 at 14:33:02 (66) 11/06/06 at 15:09:08	Smart Phone SDP	ICE Conference
T610 (00:0F:DE:03:5C:A6)	11/06/06 at 14:50:39 (7) 11/06/06 at 15:07:21	Cellular Phone SDP	ICE Conference
Nokia 6265i (00:12:D2:BC:DF:B0)	11/06/06 at 14:55:23 (23) 11/07/06 at 15:10:02	Cellular Phone SDP	ICE Conference
Unknown (00:16:B8:28:FF:C0)	11/06/06 at 15:04:49 (1) 11/06/06 at 15:04:49	Cellular Phone	ICE Conference
Unknown	11/06/06 at 15:09:16 (1)	Cellular Phone	ICE Conference

Bluecasing/Bluesnarfing

- Bluetooth relies on a pin to 'pair'
 - Typically the default is “0000”
 - I think that was the combination to my luggage (I changed it from 1234)
- There are numerous tools and attacks that allow you to:
 - Download address book
 - Change address book
 - Delete address book
 - Make calls
 - Listen to calls

Bluetooth hacking

- Really easy to get started. All you need is:
 - A Bluetooth adapter (now coming built in)
 - Laptop
 - Software (free)
 - Time
- 'Bluebag' shows size of problem
 - 23 hours of scanning, 1400 discoverable devices
 - Many ripe with vulnerabilities
 - Wardrivers starting to include Bluetooth

Bluetooth Hacking

- Bluesnarf
 - Snarfs info from BT phones (address lists, history, SMS's, etc)
- Btscanner
 - Scanner for detecting discoverable devices
 - Discover vulnerable models for Bluesnarf attack
- Bluetooth convergant devices
 - PDA's, laptops with WiFi and Bluetooth might secure the WiFi, but allow Bluetooth users to route through to the WiFi....

Bluetooth Hacking

- Bluetooth access points
 - Bridges wired net to Bluetooth, much like WiFi
 - Rogue access point undetectable through normal WiFi scanning
 - Can be hidden anywhere
- Car Whisperer
 - Many cars have built in 'hands free' with default '0000' pins. Works with some headsets too
 - Record audio from the car mic or Inject audio into the speakers
 - Imagine the possibilities in traffic!

Bluetooth Root Canal

- Turn off discoverable on your phone (or save your battery and turn off Bluetooth entirely)
- Use non-default PIN's (not possible on headsets, mice and other small devices)
- Scan for Bluetooth!
 - Scan for discoverable
 - Scan with spectrum analyser for non-discoverable devices
 - Bluetooth may be what's causing your WiFi interference?

Resources

- Read – Wardriving & Wireless penetrations testing – Syngress 2006
- Forums – netstumbler.org Ask intelligent questions or suffer!
- Try the tools yourself – Backtrack Live CD, wirelessdefense.org
- Hire professionals for second opinions
- Keep up to date – pauldotcom.com podcast

Resources

- Antennas and cards
 - www.wardrivingworld.com
 - www.fab-corp.com
- Tools and How-To's
 - www.wirelessdefense.org
 - www.remote-exploit.org
 - www.personalwireless.org/tools
- Bluetooth hacking
 - www.trifinite.org
 - www.digitalammunition.com

Resources

- Random links of interesting things:
 - <http://beastbox.net/wepcracking.swf>
 - http://www.churchofwifi.org/Project_Display.asp?PID=87
 - <http://shmoocon.org/2006/videos/ChurchOfWiFi.mp4>
 - <http://beastbox.net/WPA.swf>
 - <http://www.wifi-shootout.com/>
 - <http://pauldotcom.com/WirelessNetSec.pdf>
 - <http://www.securityfocus.com/infocus/1814>
 - <http://www.theta44.org/karma/>
 - <http://airpwn.sourceforge.net/>
 - <http://www.metageek.net/>
 - <http://www.renderlab.net>

Thanks!

- Special thanks to:
 - Paul, Larry and Nick from pauldotcom.com
 - Wirelessdefense.org
 - Thorn, Josh Wright, Dragorn, Audit, Chris
 - The Church of Wifi
 - Netstumbler Forums
 - Syngress (free books!)
 - ICE - CIPS

Questions?

render@renderlab.net

780-619-0924

www.renderlab.net