



 THE CONFERENCE ON  
**mobile & wireless**  
**SECURITY**  
**Session #8**

**Surveying Your Kingdom:  
Carrying Out a Successful Wireless  
Site Survey**



# Surveying Your Kingdom: Carrying Out a Successful Wireless Site Survey

**Session #8**

**Joe Grand and Lee Barken**

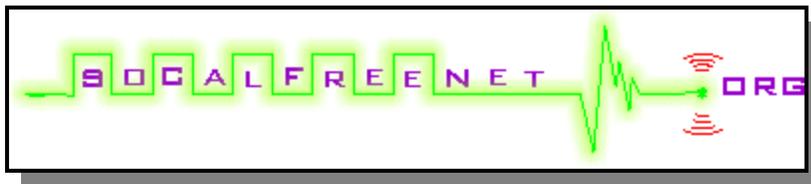
**Thursday, 10:45am - 12:00pm**



© 2005 Grand Idea Studio, Inc.

# Introduction

- Joe Grand, Grand Idea Studio, Inc.
  - [joe@grandideastudio.com](mailto:joe@grandideastudio.com)
- Lee Barken, CISSP, CCNA, MCP, CPA
  - [barken@mail.com](mailto:barken@mail.com)
  - [www.socalfreenet.org](http://www.socalfreenet.org)



# Agenda

- Policies
- Infrastructure
- Tools
- Mapping
- Controlling and Containing

# Getting Started

- Establishing your business goals and policies
- Creating a known-accurate network map
- Enforcing policy
- Staying on top of the latest attacks and trends
- Solutions will vary for each situation
  - **One size does not fit all**

# Policies

- Modification to existing security policies
  - **Add wireless-specific definitions**
- Allow only company-authorized wireless equipment
- All changes to network and configurations must be approved by IT

# Policies 2

- Strict enforcement and punishment
- Incident response policy for security events
- Continually revise policies to account for new & future threats
  - **Security is a process, not a product**

# Physical Infrastructure

- Signal strength
- Interference and noise
- Access points: How many and where?
- Outdoor deployments

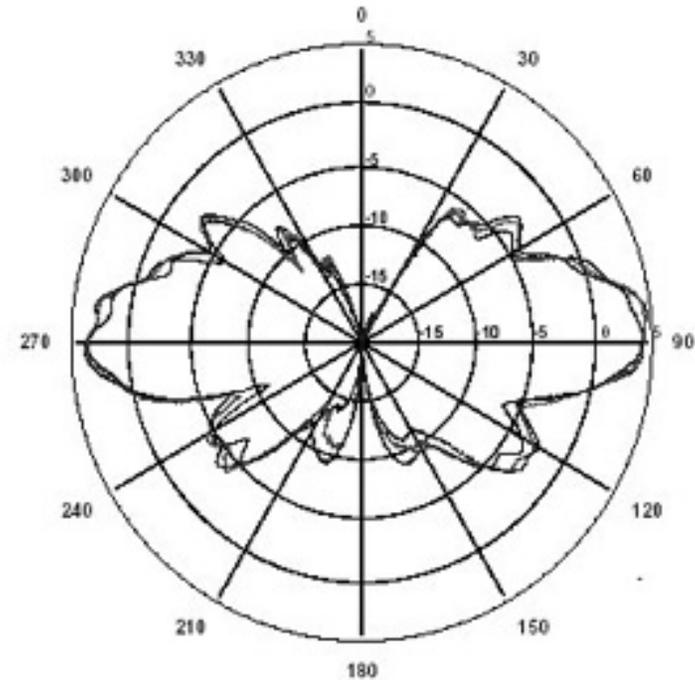
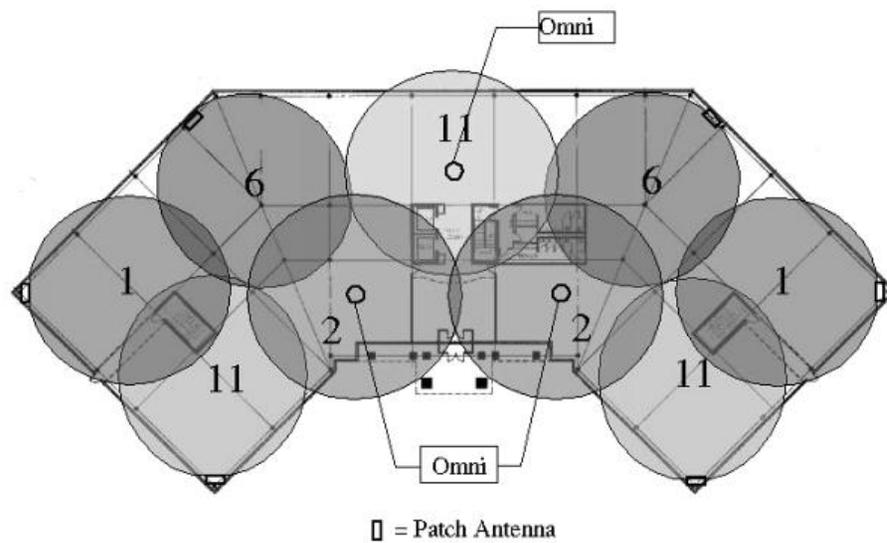
# Signal Strength

- Know your “network cloud”
- Goal is to limit the reach of the wireless network and to allow access only to authorized users
  - **Signal should be "just strong enough"**
- Signal leakage makes it easier for attackers to sniff or connect to your network
  - **Uncontrolled extension of wireless is like having a network jack on the outside of your building**

# Signal Strength 2

- Reduce Signal Leakage
  - Use directional, indoor antennas
  - Adjust TX wattage on APs and clients
  - Use multiple APs at lower power
- Attackers could still use high-gain, directional antennas to reach your network cloud

# Signal Strength 3



# Interference and Noise

- Concrete walls can attenuate wireless signals
- RF shielding glass or paint can be used to create a contained wireless environment
  - **Ex.:** [www.tempestusa.com/emiglass.html](http://www.tempestusa.com/emiglass.html)
- The structure of your building can affect where and how wireless signals propagate
- Noise from electronic equipment can interfere with wireless signals

# Access Points

- Rogue APs can be easily hidden in an office
  - **Often innocently connected by uninformed employees**
- Perform internal & perimeter searches to discover any rogue APs
- Keep network maps up-to-date
  - **Compare "current" to "known good" map**

# Access Points 2

- Verify that all MAC addresses on wireless network are approved
  - **Ex.: Latis IDS**
  - **Don't solely rely on this: SW and HW exists to change MAC address of NIC**
- Use wireless encryption
  - **Ex.: 128-bit WEP (even though it's broken, it's better than nothing), WPA, 802.11i**
- Use a VPN, if possible

# Outdoor Deployments

- Safety First!
  - Use lightning arrestors, proper grounding, Plenum/Riser rating, etc.
  - Don't fall off buildings
- Don't use 802.11b for building-to-building links
- Omni-directional antenna patterns change with Gain

# Outdoor Deployments 2

- For true “seamless roaming” (v. “nomadic roaming”), consider a commercial solution (Bluesocket, Vernier, ReefEdge)
- Test, test, test!
- No two wireless deployments are ever the same
  - **Variances in equipment, environment, specifications, etc.**

# Toolbox

- Building a toolbox for wireless site surveys
  - Software tools
  - Hardware tools
  - Policy enforcement tools

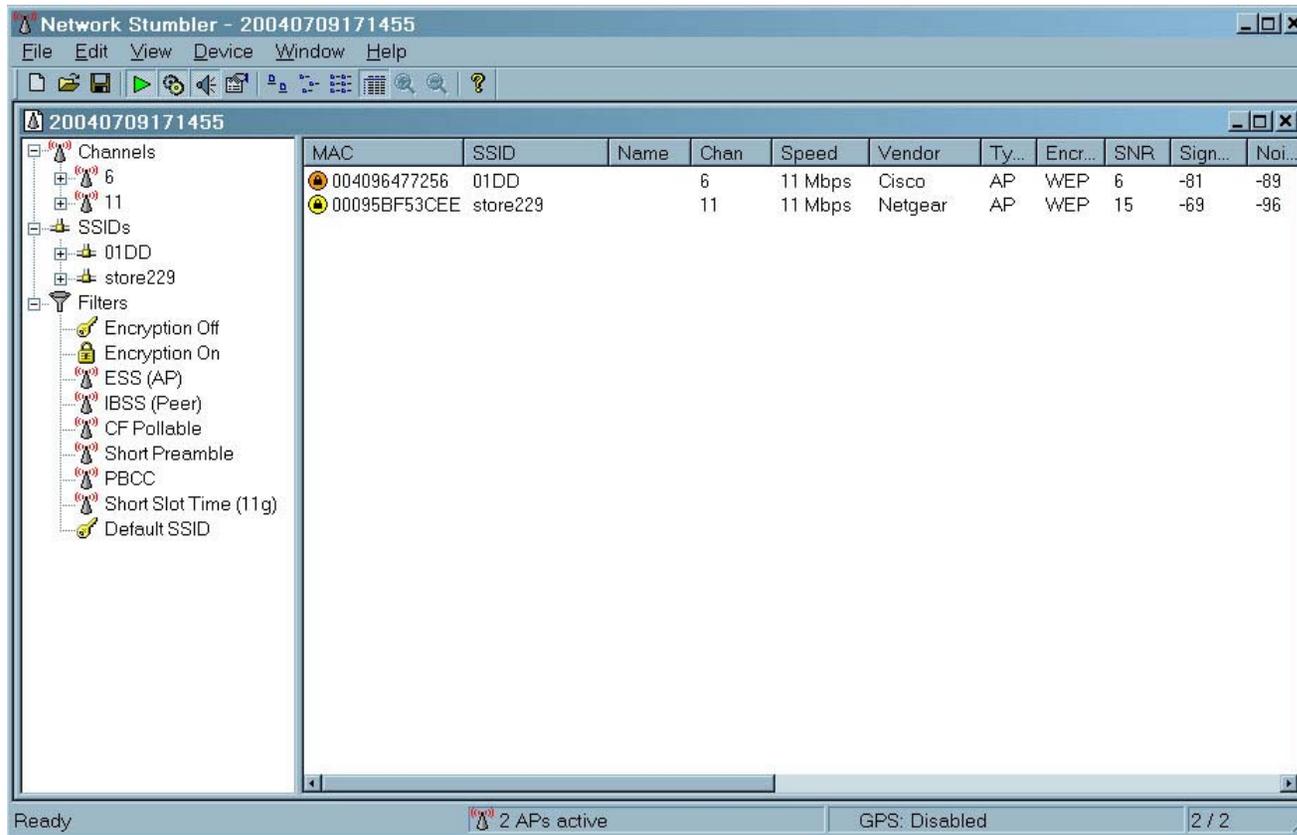
# Toolbox: Freeware and Shareware

- Kismet
  - `www.kismetwireless.net`
- KisMAC (OS X)
  - `www.binaervarianz.de/projekte/programmieren/kismac`
- Network Stumbler
  - `www.netstumbler.com`
- MacStumbler (OS X)
  - `www.macstumbler.com`

# Toolbox: Freeware and Shareware 2

- bsd-airtools (\*BSD)
  - [www.dachb0den.com/projects/bsd-airtools.html](http://www.dachb0den.com/projects/bsd-airtools.html)
- Pocket Warrior (Pocket PC)
  - [www.dataworm.net/pocketwarrior/index.html](http://www.dataworm.net/pocketwarrior/index.html)
- NetChaser (Palm OS)
  - [www.bitsnbolts.com/netchaser.html](http://www.bitsnbolts.com/netchaser.html)
- AirTraf (Linux)
  - [www.elixar.com](http://www.elixar.com)

# Toolbox: Network Stumbler



# Toolbox: MacStumbler

The screenshot shows the MacStumbler 0.7b application window. The main window contains a menu bar with 'Save', 'Open', and 'Clear' options. Below the menu bar is a 'Status' bar with a blue and white striped progress indicator. The main content area is divided into two sections: a table of detected networks and a 'Log' section. The 'private' network is selected, and its details are shown in a separate panel on the right.

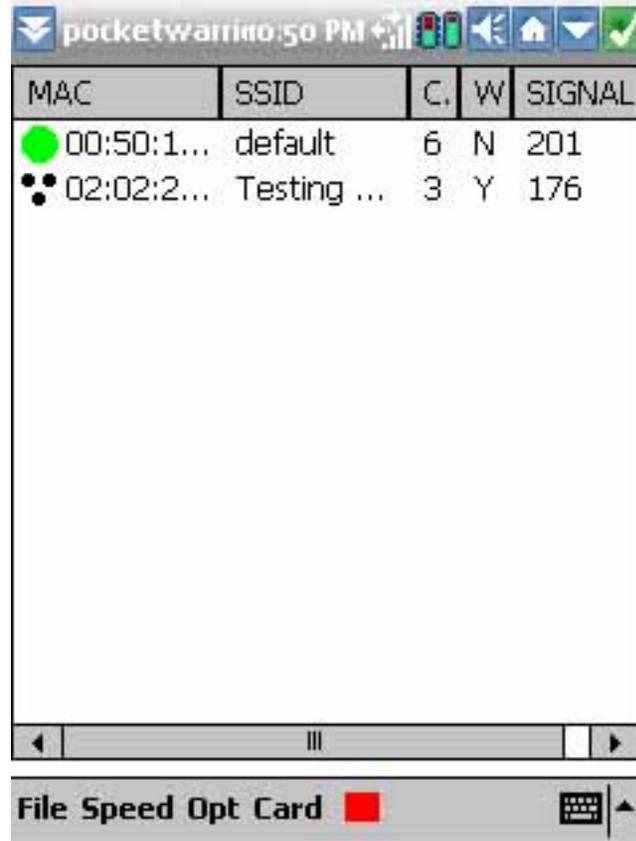
SSID	Chan	Signal	Noise	WEP	Vendor
default	6	21	6	No	D-Link
private	11	21	7	Yes	Linksys

SSID	Chan	Max Sig	WEP	Last Seen	Vendor
private	11	29	Yes	03:17PM 07/02/03	Linksys
default	6	27	No	03:17PM 07/02/03	D-Link

Details: private  
MAC: 00:06:25:DF:9A:19  
Vendor: Linksys  
Type: Managed  
Location: GPS Enabled  
Lat: W 3337.826904  
Lon: N 11739.685547  
Comments: My home network ;)|

# Toolbox: Pocket Warrior



The screenshot shows the Pocket Warrior application interface. At the top, the status bar displays the time as 10:50 PM and various system icons. Below the status bar is a table with the following columns: MAC, SSID, C., W, and SIGNAL. The table contains two rows of data:

MAC	SSID	C.	W	SIGNAL
● 00:50:1...	default	6	N	201
●● 02:02:2...	Testing ...	3	Y	176

Below the table is a navigation bar with a back arrow, a home button, and a forward arrow. At the bottom of the screen, there is a status bar with the text "File Speed Opt Card" and a red square icon.

# Toolbox: Commercial Software

- AirMagnet
  - [www.airmagnet.com](http://www.airmagnet.com)
- AiroPeek
  - [www.wildpackets.com](http://www.wildpackets.com)
- AirDefense
  - [www.airdefense.net](http://www.airdefense.net)
- Latis BorderGuard Wireless
  - [www.latis.com](http://www.latis.com)

# Toolbox: AiroPeek NX

**AiroPeek NX - [Airport]**

File Edit View Capture Statistics Tools Window Help

Packets received: 6,599 Memory usage: 1%  
 Packets filtered: 1,599 Filter state: Accept only packets matching one filter

Source	Destination	Data ...	Cha...	Size	Protocol	Summary
abv-sfol-...	GUEST	11.0	9	84	FTP Ctl	.A..S.,S= 808146011,L= ...
GUEST	abv-sfol-...	11.0	9	82	FTP Ctl	.A....,S=3637473208,L= ...
abv-sfol-...	GUEST	11.0	9	164	FTP Ctl	R PORT=2625 220 abv-sfol-...
GUEST	abv-sfol-...	11.0	9	82	FTP Ctl	.A....,S=3637473208,L= ...
GUEST	abv-sfol-...	11.0	9	88	FTP Ctl	C PORT=2625 USER davis
abv-sfol-...	GUEST	11.0	9	76	FTP Ctl	.A....,S= 808146100,L= ...
abv-sfol-...	GUEST	11.0	9	110	FTP Ctl	R PORT=2625 331 Password ...
GUEST	abv-sfol-...	11.0	9	82	FTE Ctl	.A....,S=3637473220,L= ...
GUEST	abv-sfol-...	11.0	9	93	FTP Ctl	C PORT=2625 PASS flybynlight

Packet: 1,594

**FTP Control - File Transfer Protocol**

Line 1: PASS flybynlight<CR><LF>

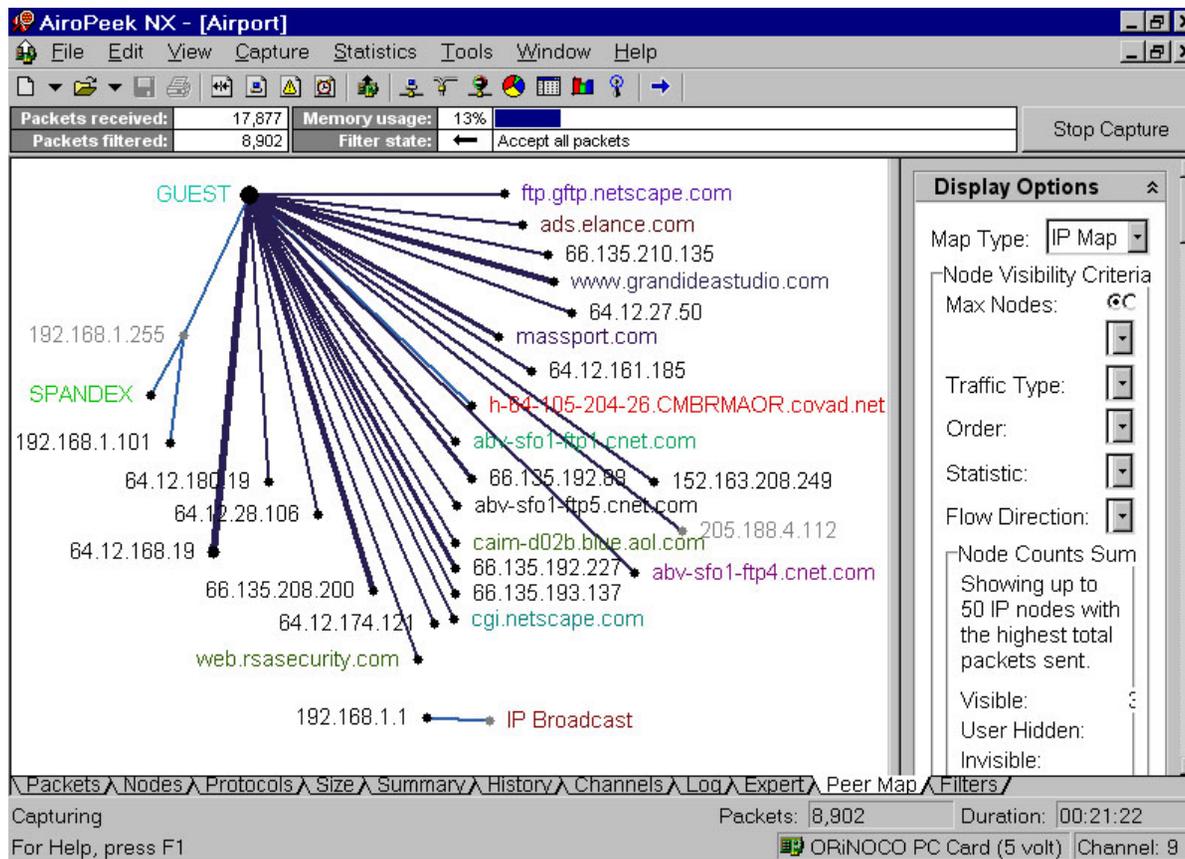
```

0000: 08 01 02 01 00 04 5A EF 27 43 00 40 96 35 A7 7B .....Z.'C.@.5.{
0016: 00 04 5A EF 27 43 10 A8 AA AA 03 00 00 08 00 ..Z.'C.....
0032: 45 00 00 39 69 96 40 00 80 06 FC EB C0 A8 01 6A E..9i.@.....j
0048: CE 10 04 1A 0A 41 00 15 D8 CF 6F C4 30 2B 54 D6 .....A.....o.+T.
0064: 50 18 45 D6 17 28 00 00 50 41 53 53 20 66 6C 79 P.E..{.PASS fly
0080: 62 79 6E 31 67 68 74 0D 0A 00 00 00 00 00 bynlight.....
  
```

Packets / Nodes / Protocols / Size / Summary / History / Channels / Log / Expert / Peer Map / Filters /

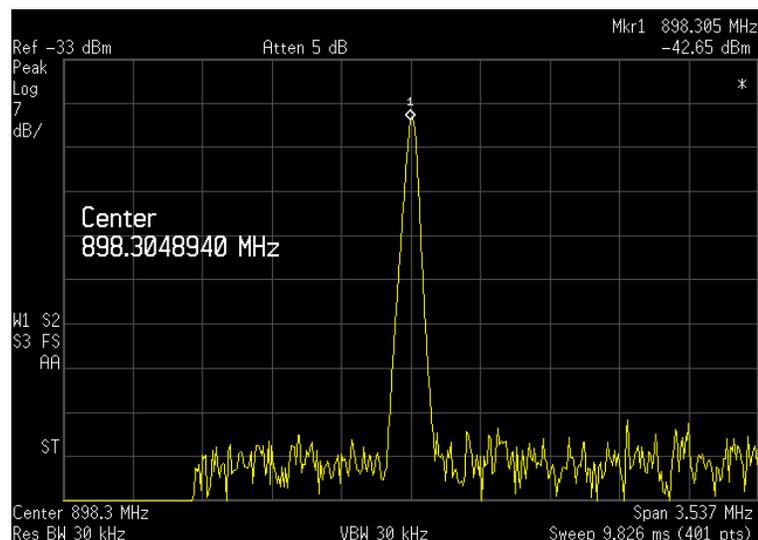
Capturing Packets: 1,599 Duration: 00:10:12  
 For Help, press F1 ORINOCO PC Card (5 volt) Channel: 9

# Toolbox: AiroPeek NX 2



# Toolbox: Hardware

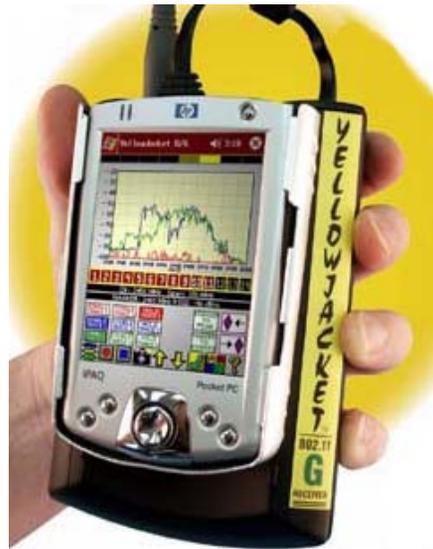
- PDA or laptop with mapping software
  - **Ex.: HP iPaq h4150 w/ built-in 802.11b**
- Standard “bug-finding” or amateur radio “fox hunting” techniques using
  - **Spectrum analyzer, frequency counter**



# Toolbox: Hardware 2

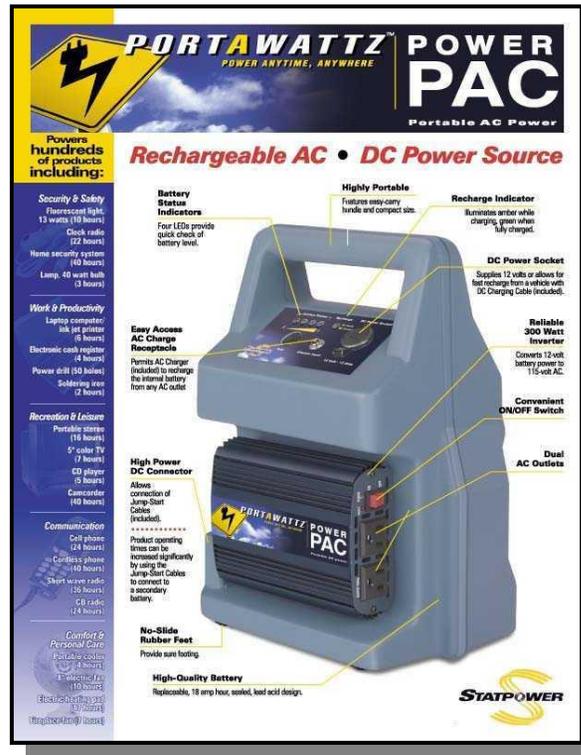
- Berkeley Varitronics Systems Yellowjacket
  - [www.bvsystems.com/Products/WLAN/YJ802.11a/yellowjacket802.11a.htm](http://www.bvsystems.com/Products/WLAN/YJ802.11a/yellowjacket802.11a.htm)
- Fluke Networks OptiView
  - [www.flukenetworks.com/us/LAN/Handheld+Testers/OptiView/Overview.htm](http://www.flukenetworks.com/us/LAN/Handheld+Testers/OptiView/Overview.htm)
- Kensington WiFi Finder
  - [www.kensington.com/html/3720.html](http://www.kensington.com/html/3720.html)

# Toolbox: Hardware 3



# Toolbox: Hardware 4

- Portable Power Packs
  - [www.xantrex.com/web/id/5/learn.asp](http://www.xantrex.com/web/id/5/learn.asp)



# Toolbox: Policy Enforcement

- Some commercial tools offer policy enforcement capabilities
  - **Ex.: AirDefense, Latis IDS**
- Continuous monitoring for new hosts, APs, MAC addresses, etc.

# Toolbox: Other Resources

- Article and listing of various additional tools
  - [www.networkmagazine.com/article/NMG20030305S0001](http://www.networkmagazine.com/article/NMG20030305S0001)
  - [www.networkintrusion.co.uk/wireless.htm](http://www.networkintrusion.co.uk/wireless.htm)

# Mapping

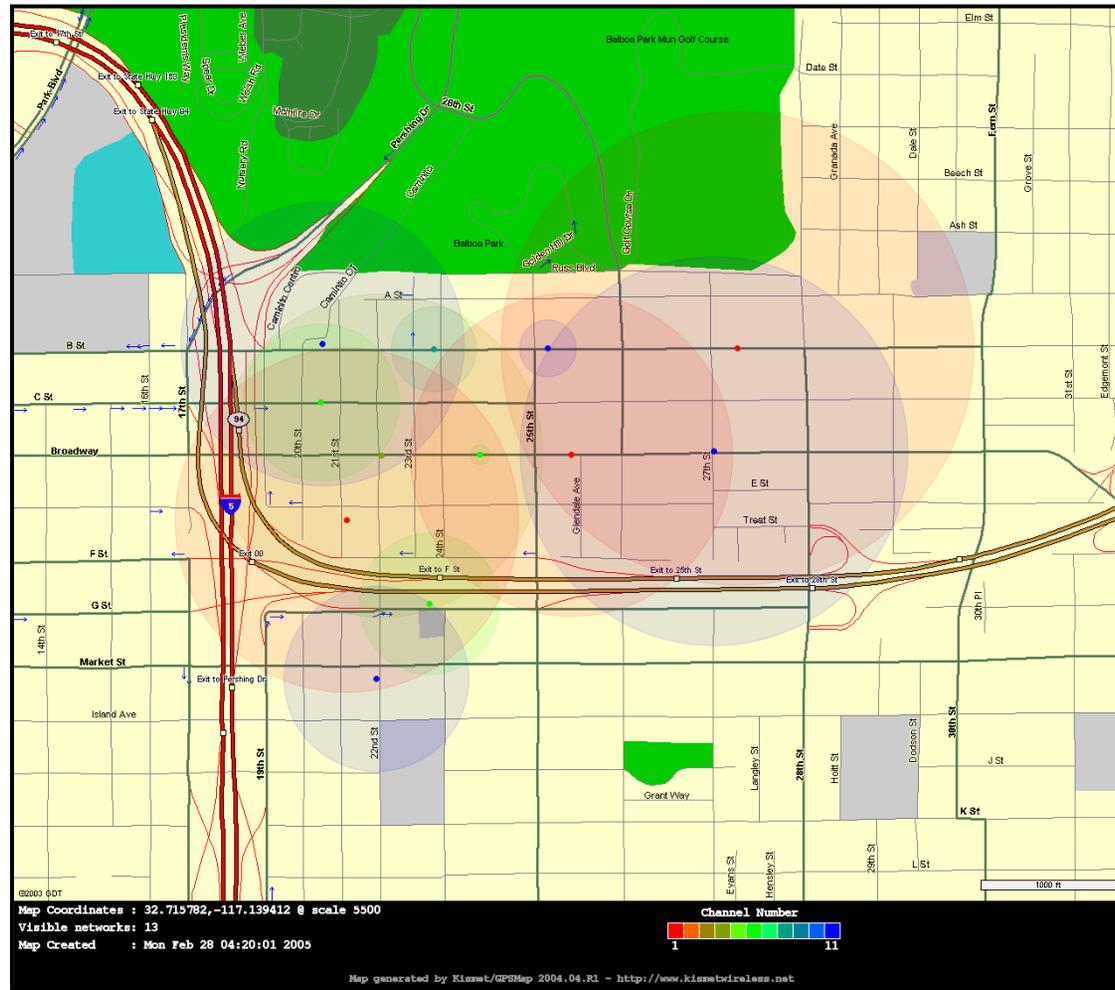
- Walk around your physical perimeter
  - A good excuse to get out of the office once in a while (Ex.: "War walking")
  - Have your security guards visually look for APs during their rounds
- Software with GPS (Global Positioning System) receiver to pinpoint locations
  - Many of the site surveying tools support GPS
  - Good site for information: [www.gpsinformation.net](http://www.gpsinformation.net)

# Mapping 2

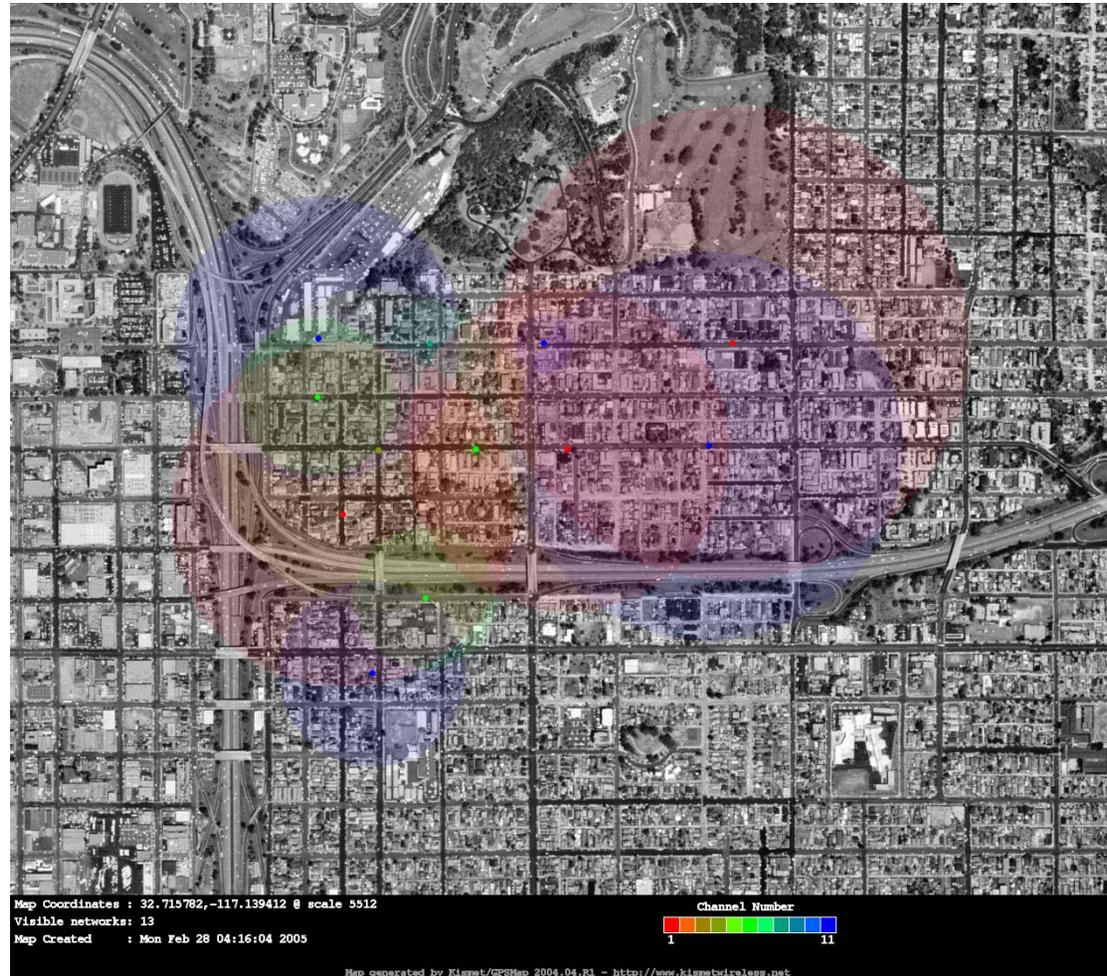
- Note specific locations of all APs and infrastructure
  - **Ex.: Network Chemistry, WildPackets products**
- Perform periodic audits to ensure the map is the same
- Excellent resource: [www.wardriving.com](http://www.wardriving.com)



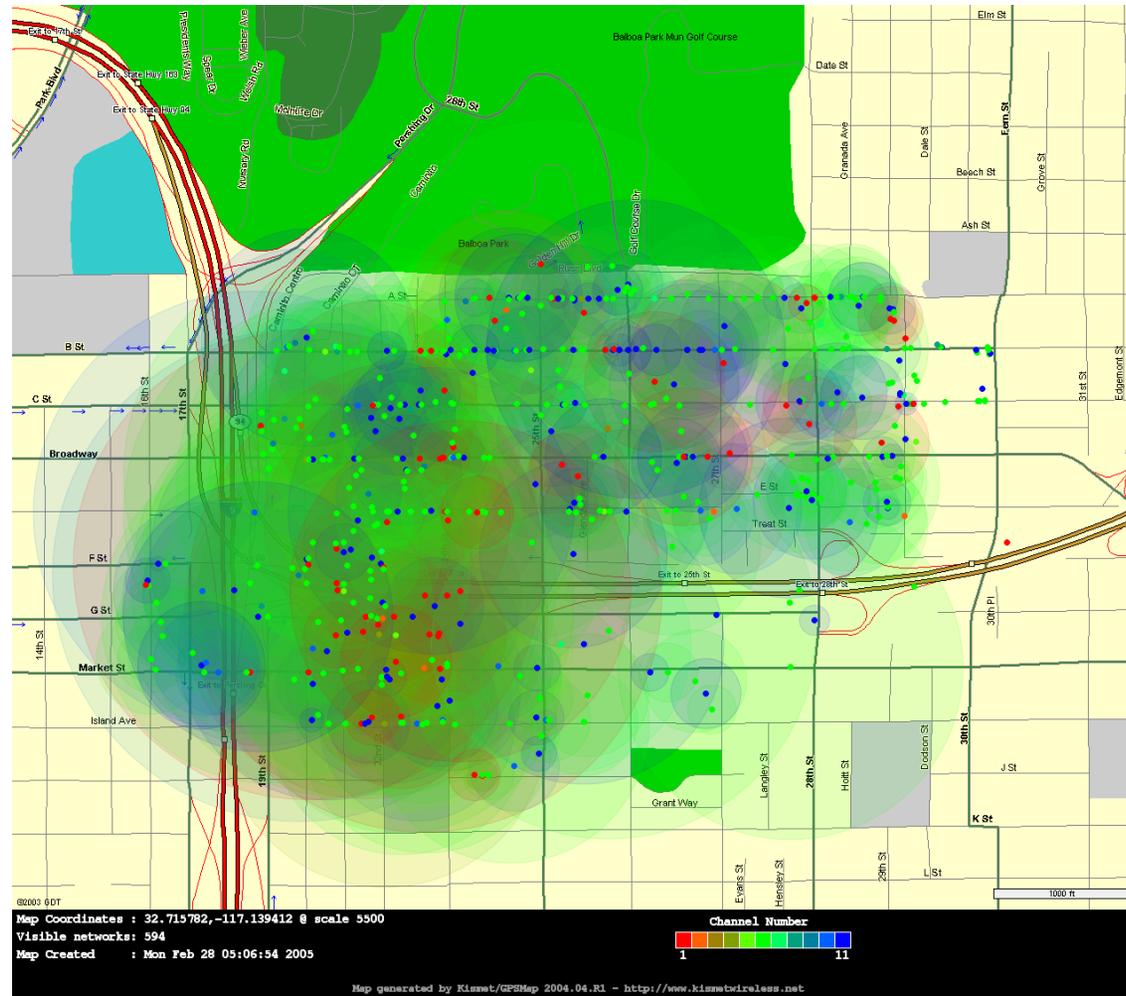
# Mapping 4



# Mapping 5



# Mapping 6



# Controlling and Containing

- Recurring review of policies, infrastructure, and business requirements
- Strict enforcement
  - **Wireless IDS and monitoring systems**
  - **Don't rely too much on technology or vendors - remember the human factor**
- Strict punishment
  - **Each action must have a consequence**
  - **If your bark is louder than your bite, people won't listen**

# Conclusions

- Know your network
- Your network will never be 100% secure
  - **Do your best to come close**
  - **Security is a process, not a product**
- Keep up-to-date with attack trends
- Continuous enforcement and monitoring is a must

# Thanks!

## Joe Grand & Lee Barken

joe@grandideastudio.com

barken@mail.com



© 2005 Grand Idea Studio, Inc.