Session #8

Surveying Your Kingdom: Carrying Out a Successful Wireless Site Survey

MIS TRAINING INSTITUTE

Surveying Your Kingdom: Carrying Out a Successful Wireless Site Survey

Session #8

Joe Grand and Lee Barken

Thursday, 10:45am - 12:00pm

THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Introduction

- Joe Grand, Grand Idea Studio, Inc.
  - **joe@grandideastudio.com**
- Lee Barken, CISSP, CCNA, MCP, CPA
  - **barken@mail.com**
  - **www.socalfreenet.org**

THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

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

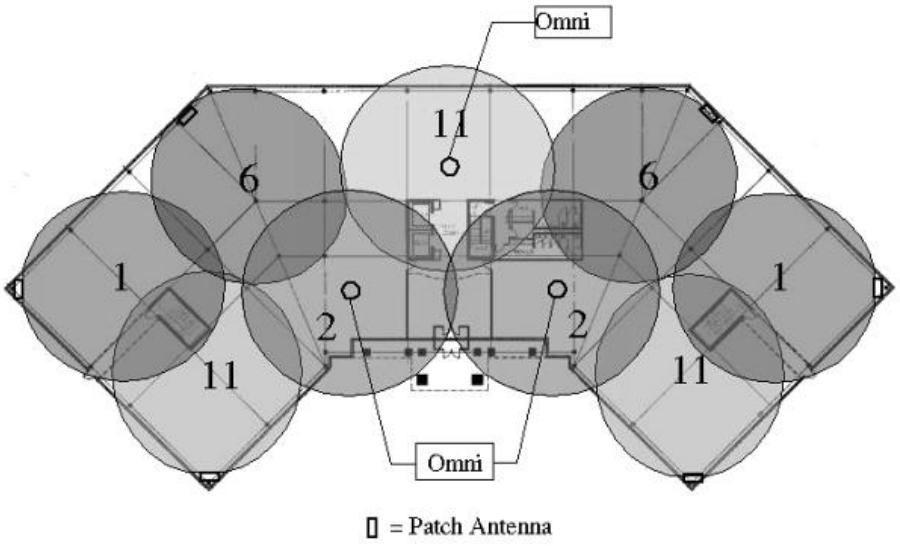
Signal Strength

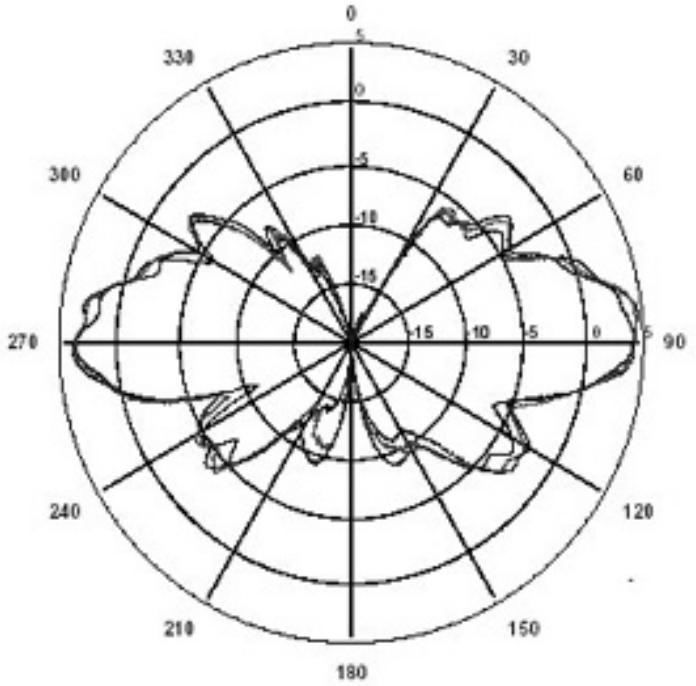
- Know your “network cloud”
- Goal is to limit the reach of the wireless network and to allow access only to authorized users
  - **Signal should be "just strong enough"**
- Signal leakage makes it easier for attackers to sniff or connect to your network
  - **Uncontrolled extension of wireless is like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

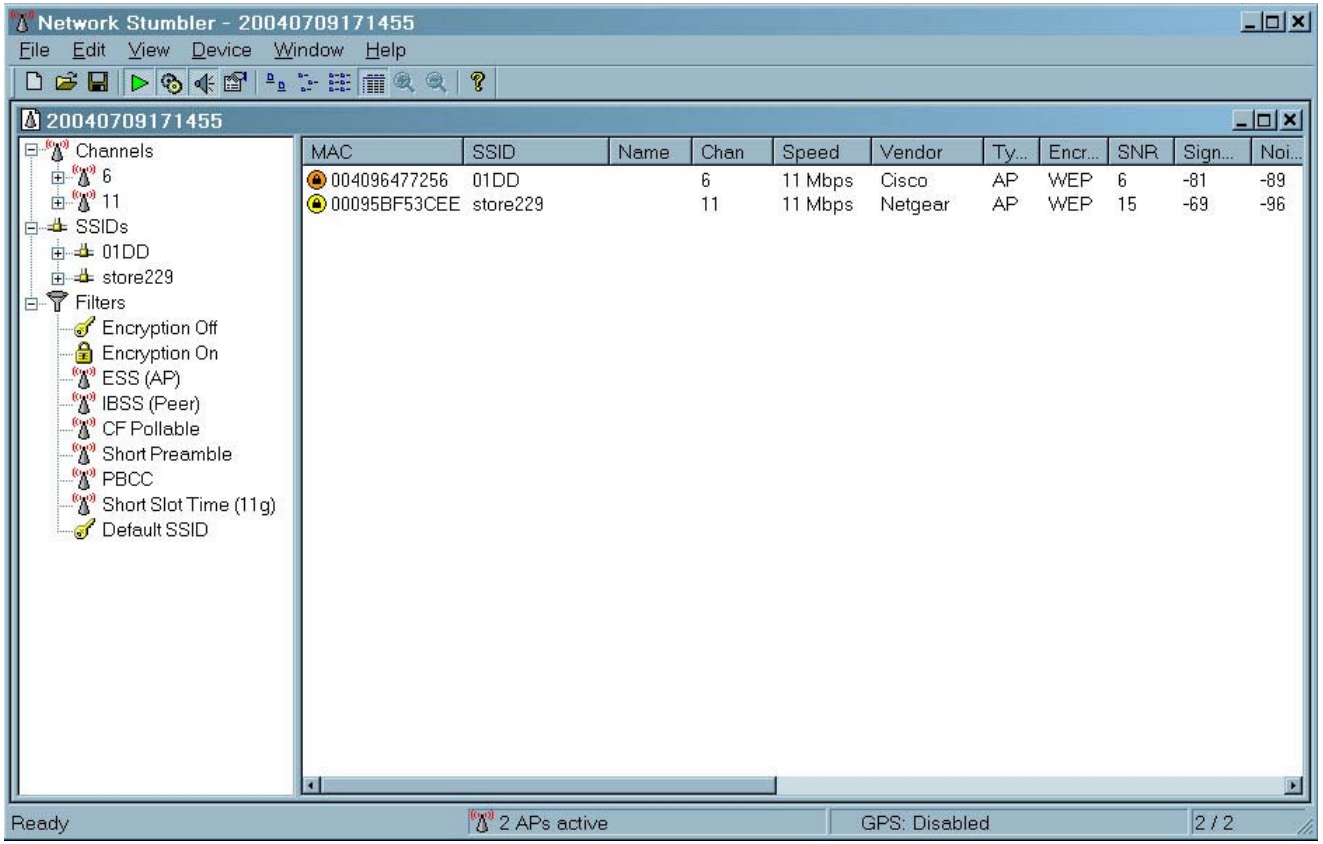
Toolbox: Freeware and Shareware

- 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**
- Pocket Warrior (Pocket PC)
  - **www.dataworm.net/pocketwarrior/index.html**
- NetChaser (Palm OS)
  - **www.bitsnbolts.com/netchaser.html**
- AirTraf (Linux)
  - **www.elixar.com**

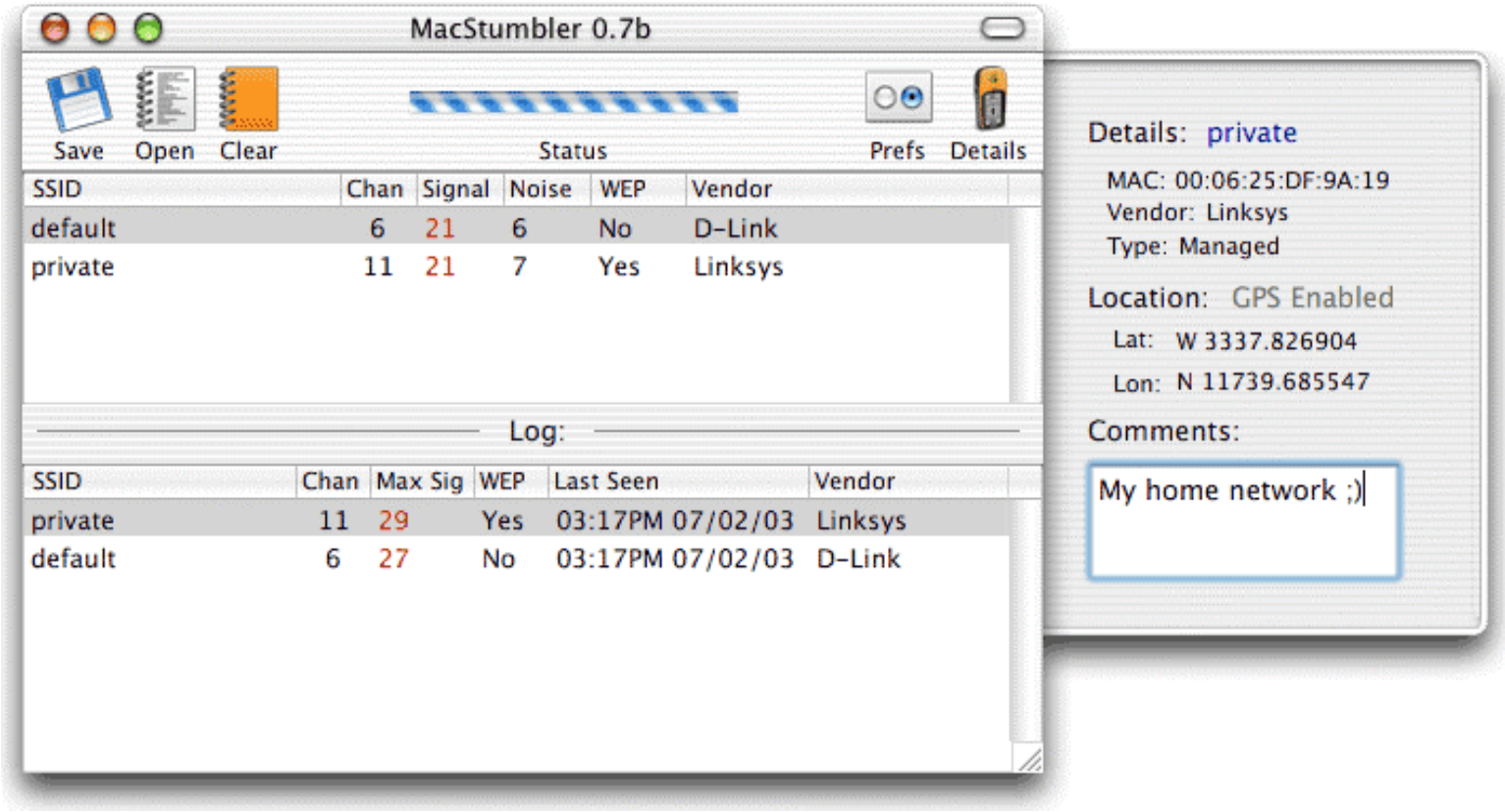
Toolbox: Network Stumbler



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

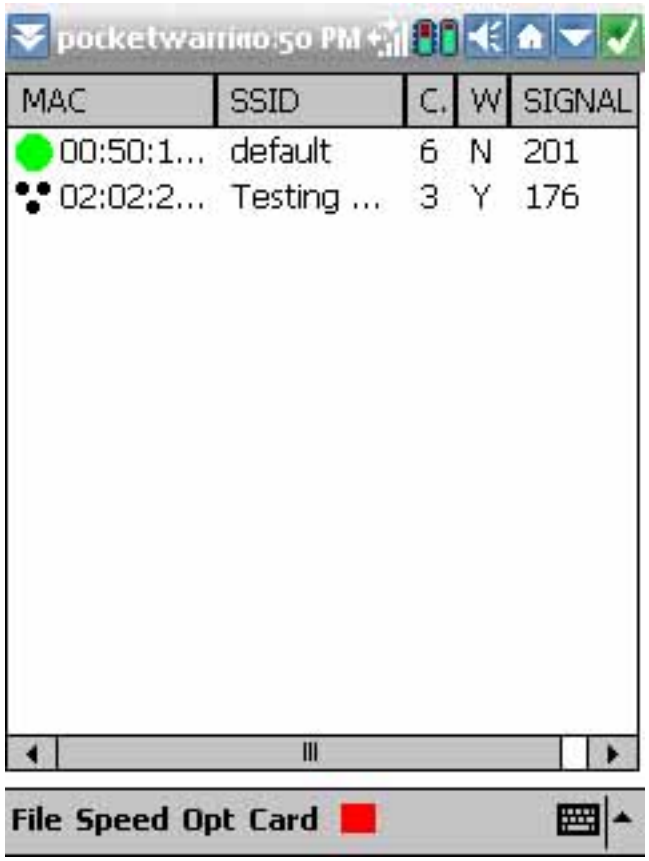
Toolbox: MacStumbler



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Toolbox: Pocket Warrior



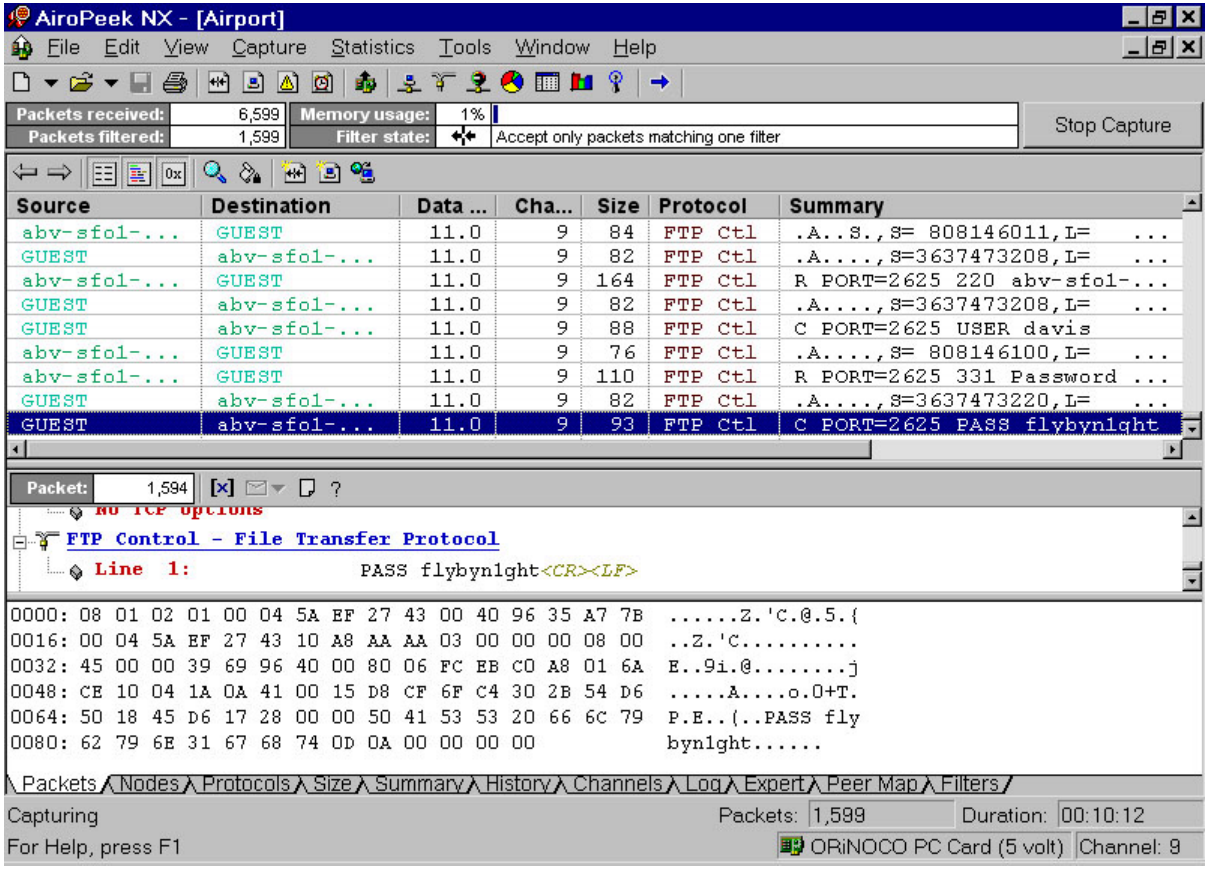
THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Toolbox: Commercial Software

- AirMagnet
  - **www.airmagnet.com**
- AiroPeek
  - **www.wildpackets.com**
- AirDefense
  - **www.airdefense.net**
- Latis BorderGuard Wireless
  - **www.latis.com**

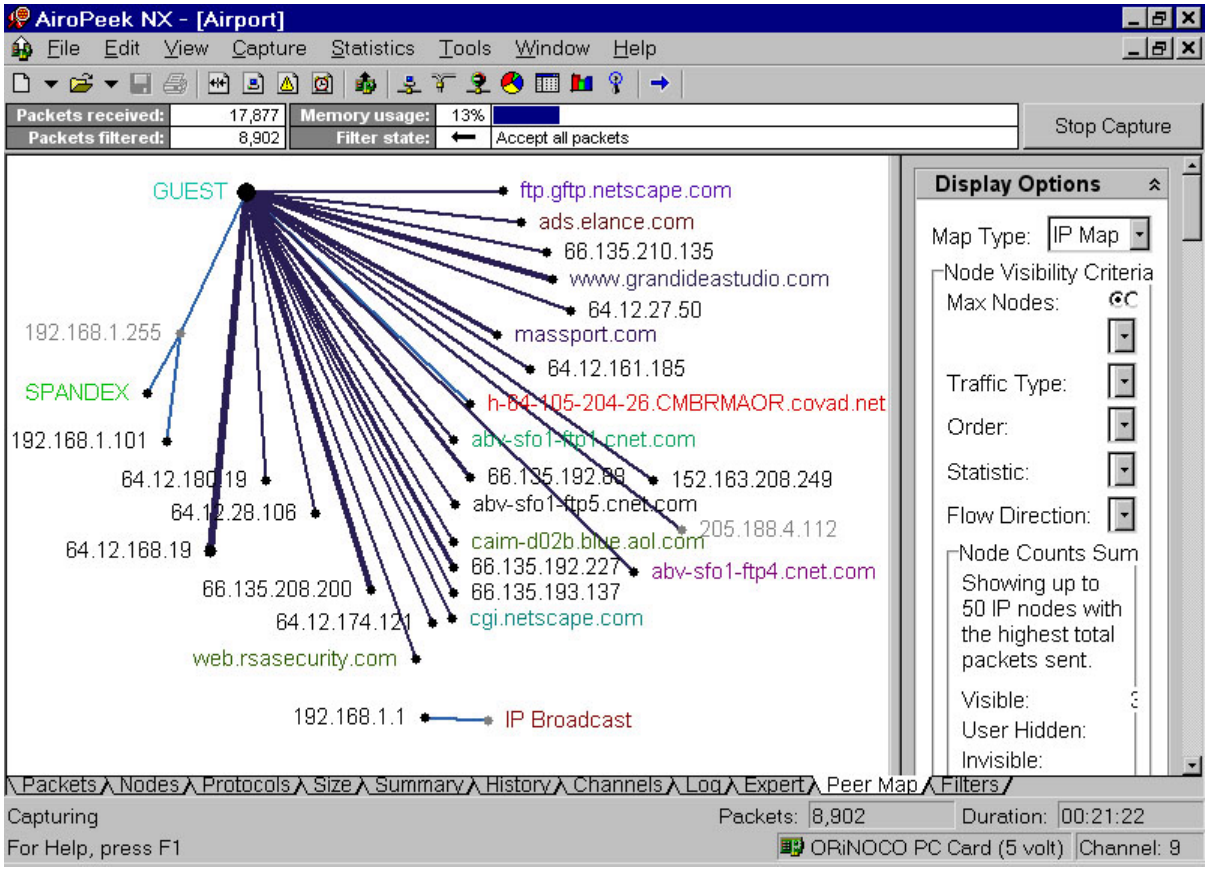
Toolbox: AiroPeek NX



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Toolbox: AiroPeek NX 2

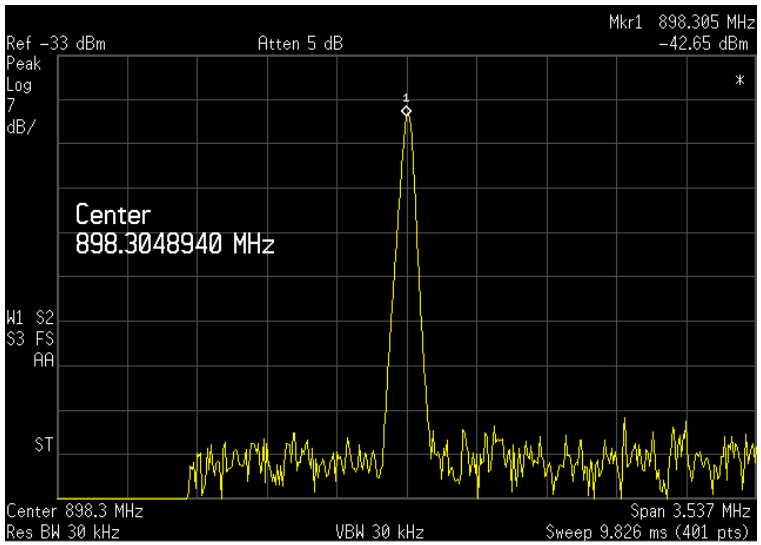


THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

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**



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Toolbox: Hardware 2

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

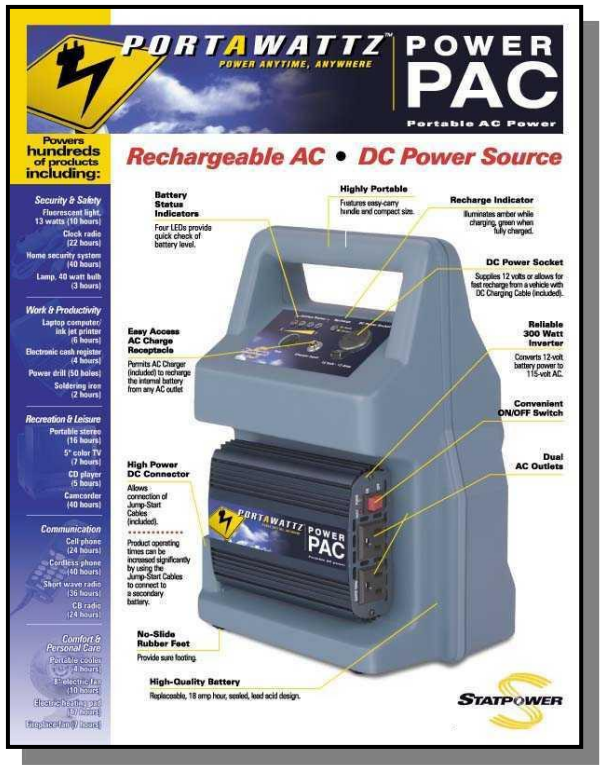
Toolbox: Hardware 3

THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Toolbox: Hardware 4

- Portable Power Packs
  - **www.xantrex.com/web/id/5/learn.asp**



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

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**
  - **www.networkintrusion.co.uk/wireless.htm**

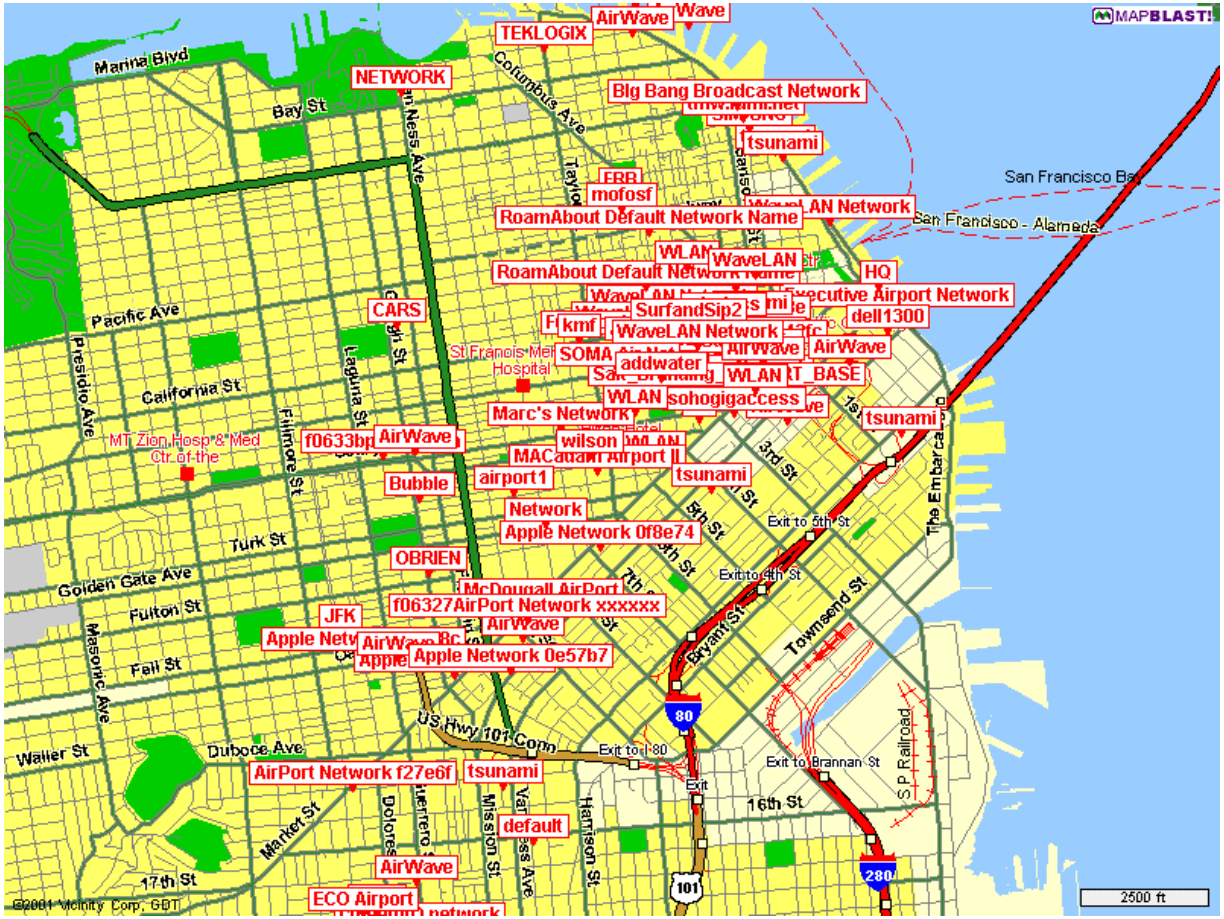
Mapping

- 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`**

Mapping 2

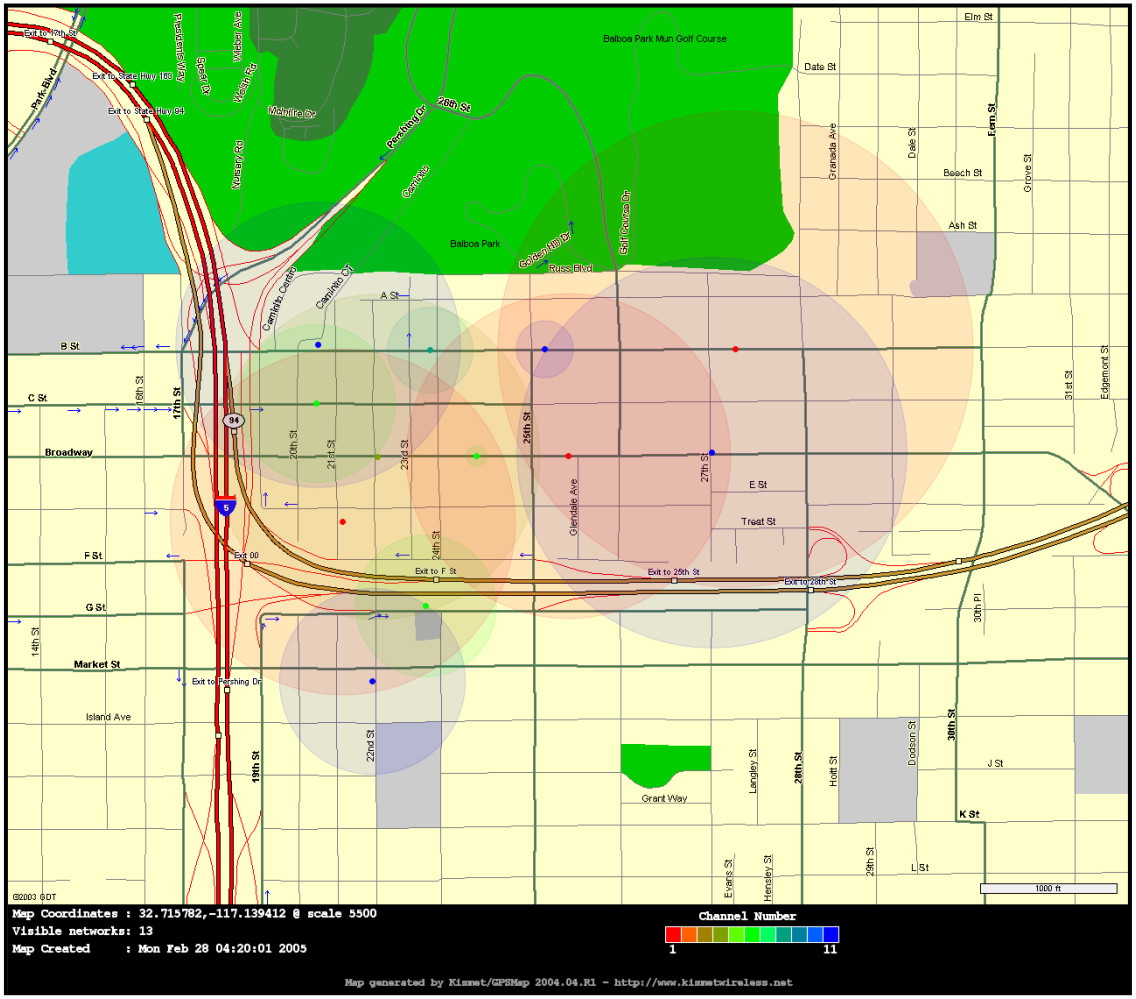
- Note specific locations of all APs and infrastructure
  - **Ex.: Network Chemistry, WildPackets products**
- Perform periodic audits to ensure the map is the same
- Excellent resource: **`www.wardriving.com`**

Mapping 3



(from www.dis.org/wl/maps)

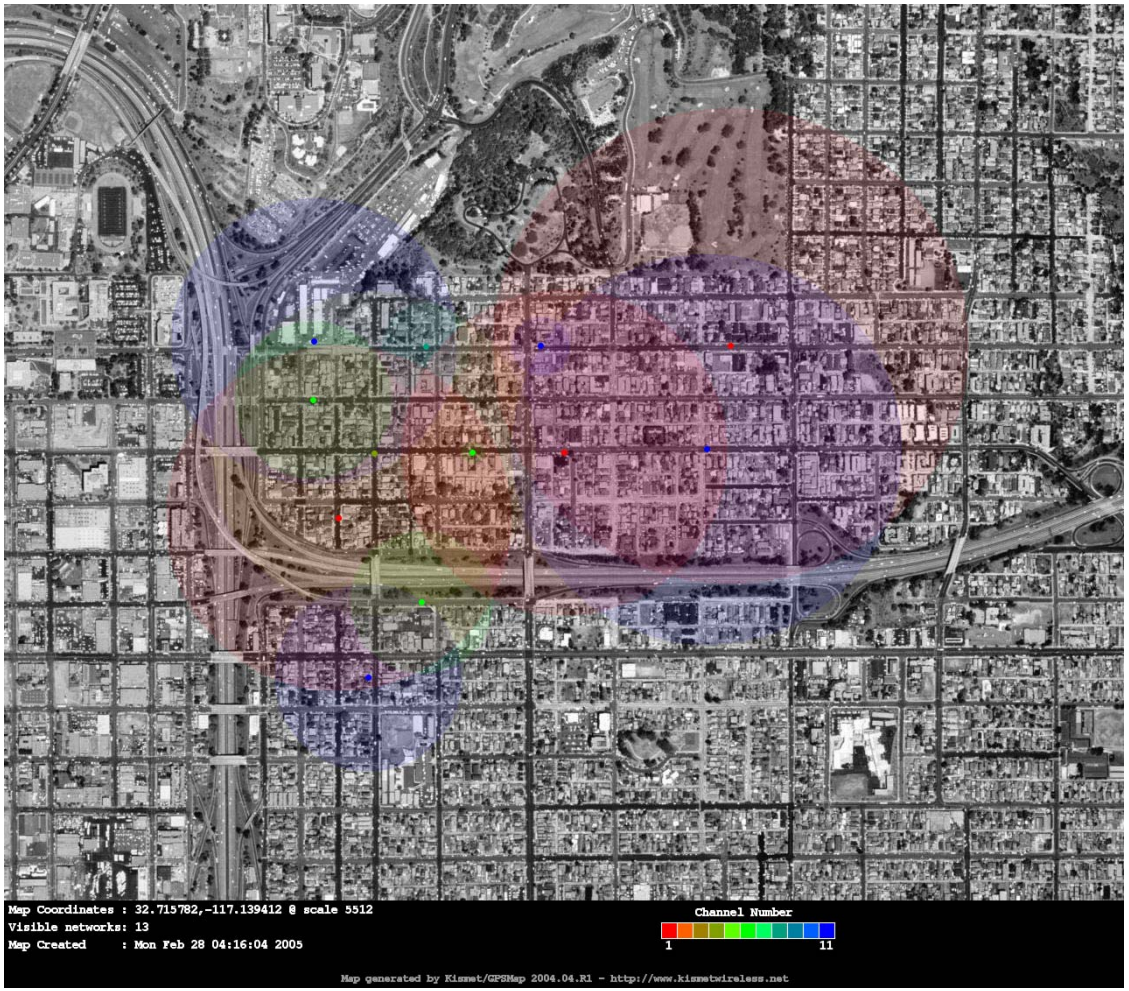
Mapping 4



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

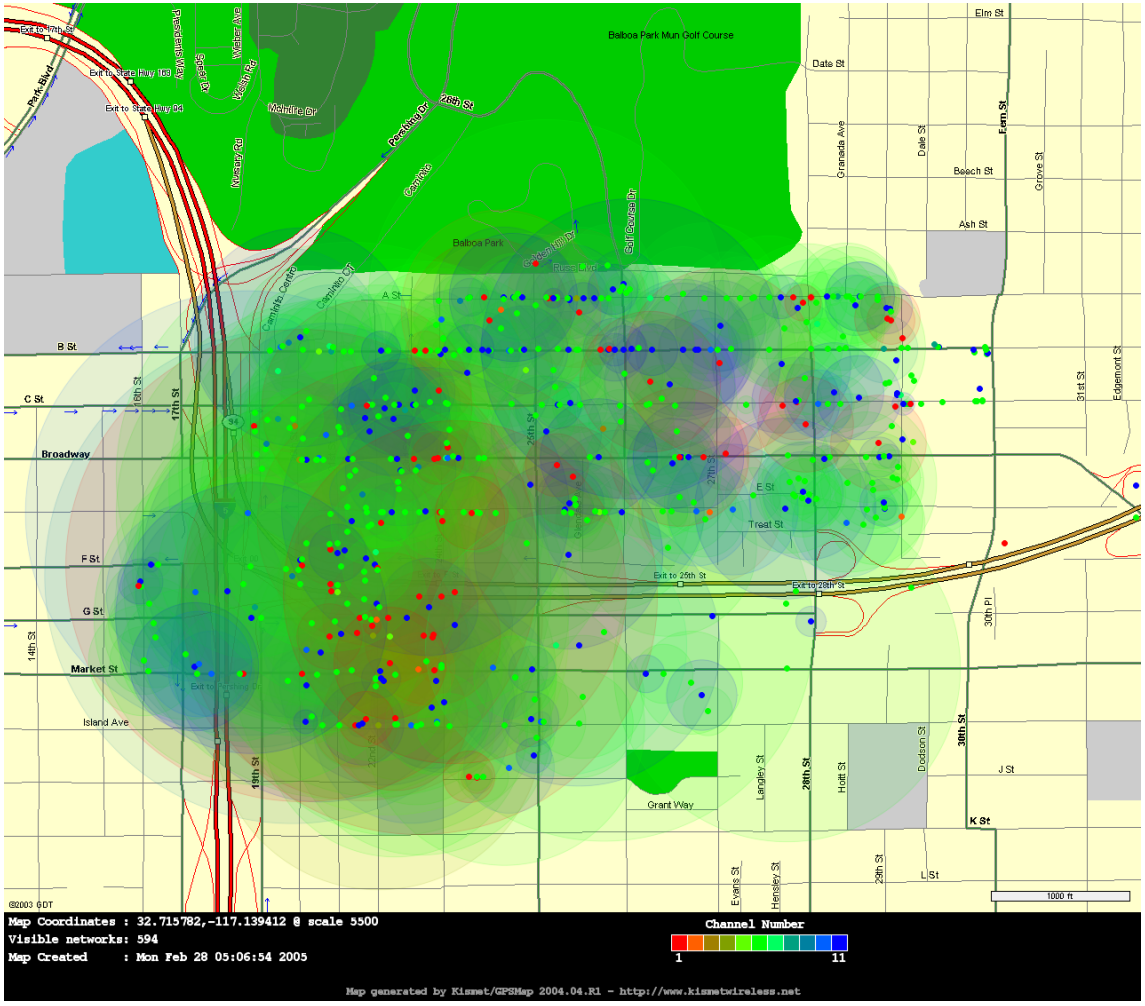
Mapping 5



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Mapping 6



THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

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

THE CONFERENCE ON mobile & wireless SECURITY

MIS TRAINING INSTITUTE

Thanks!

Joe Grand & Lee Barken

joe@grandideastudio.com

barken@mail.com