Rogue AP 101

Threat, Detection, & Defense

Beetle <beetle@shmoo.com>
Bruce Potter <gdead@shmoo.com>

Coming up...

- WiFi weakness
- Rogue AP 101
- Detection
- Defense?
- Resources
- Questions

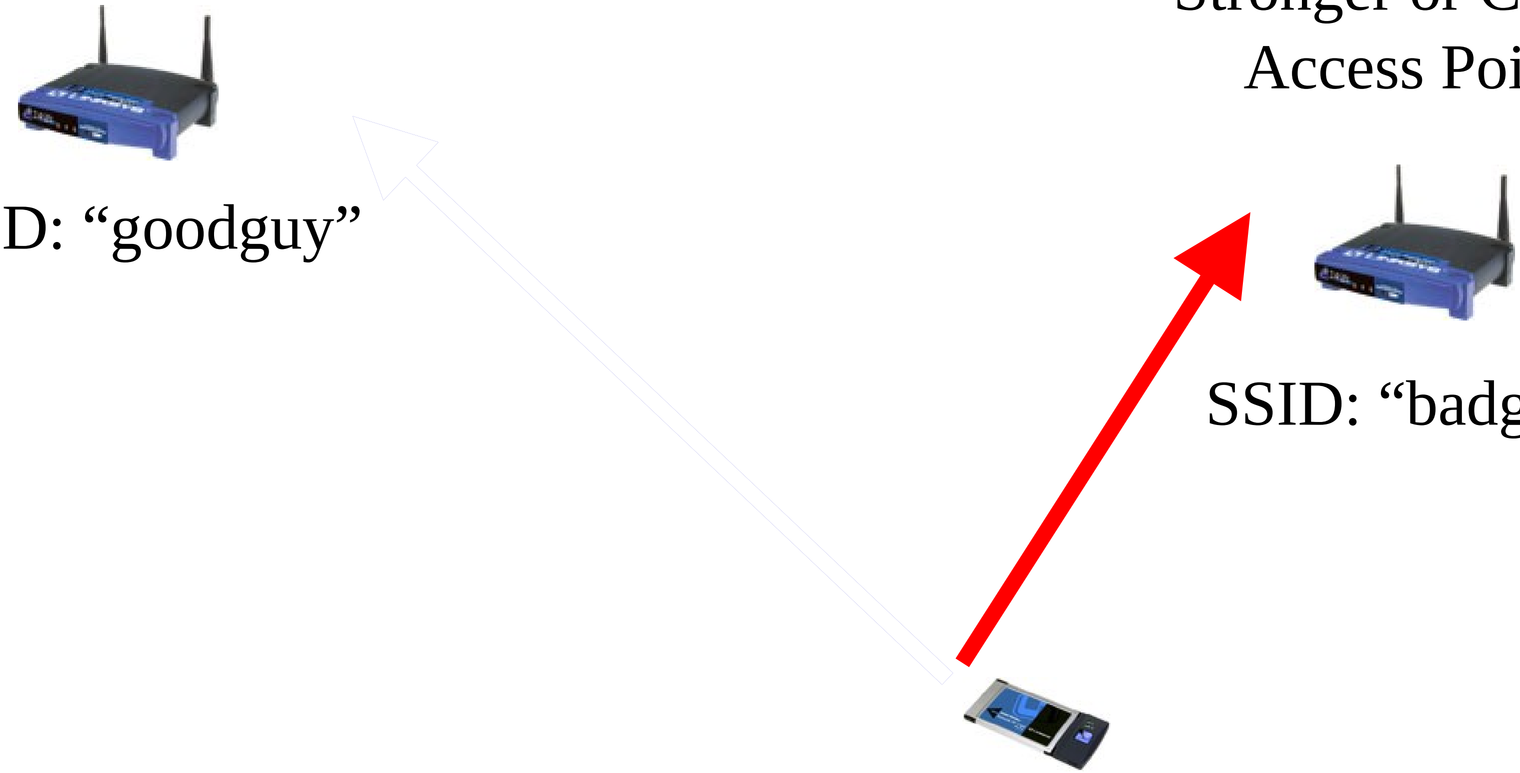
WiFi Security Soapbox…

- WEP can be cracked
- IPs can be spoofed
- MACs can be forged
- 2.4 GHz can be LEGALLY jammed
- “WiFi is the Wild West of Networking”
- But don’t worry… there’s always a “fix” on the horizon. Right?

Example Setups

- Wide Open
- Portal w/ Password Authentication
- Portal w/ Token Authentication
- WEP, 802.1x to RADIUS, untrusted DMZ
- WEP, 802.1x, VPN gateways, PKI, DMZ
- Etc, etc, etc.
- There’s a bigger problem here, that none of these security solutions solve…

Why pick the lock, when you can ask for, and be given, the KEY?



Access Point

SSID: “goodguy”

Stronger or Closer Access Point

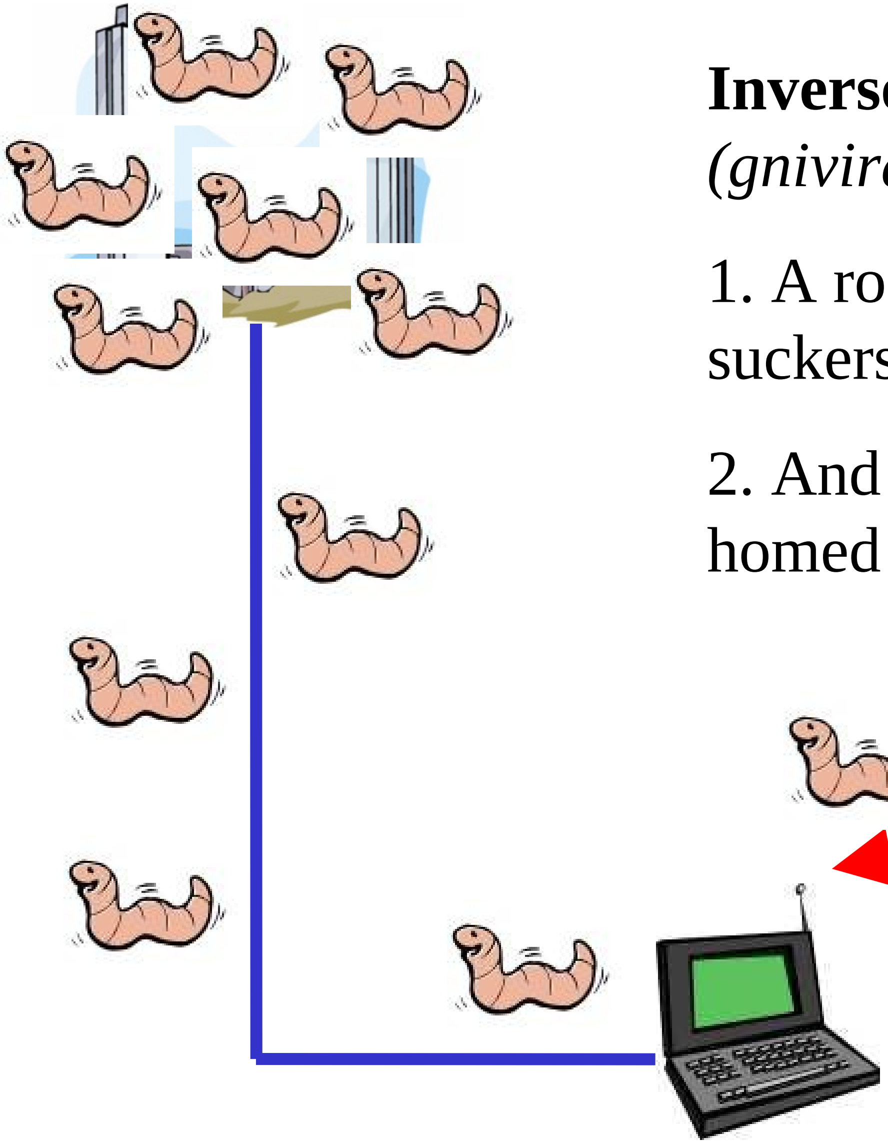
SSID: “badguy”

Wi-Fi Card

SSID: “badguy”

Rogue APs?

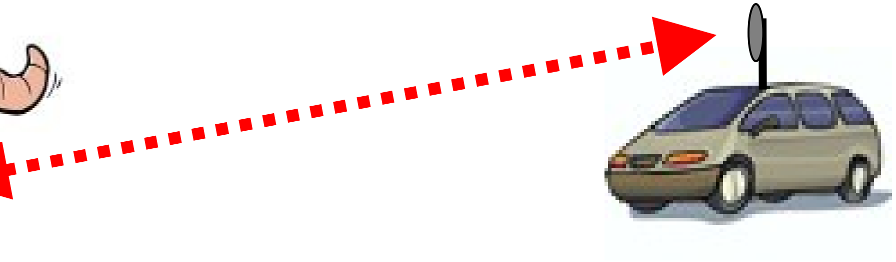
- Rogue AP = an unauthorized access point
- Traditional
  - corporate back-doors
  - corporate espionage
- Hotspots OR Corporate Environments
  - DoS
  - theft of user credentials
  - AP “cloning”



Inverse Wardriving *v.*
(gnivirdraw)

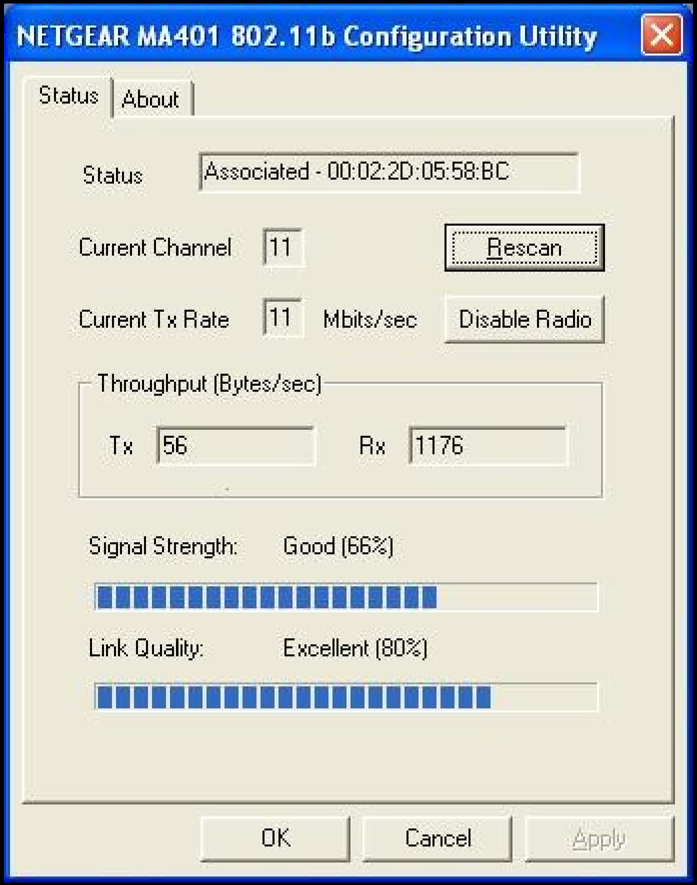
1. A rogue AP looking for “WiFi suckers”.

2. And you thought a user dual-homed with a **modem** was bad… ?



Rogue AP Mechanics

- “Create a competing wireless network.”
- AP can be actual AP or HostAP
- Create or modify captive portal behind AP
- Redirect users to “splash” page
- DoS or theft of user credentials, or WORSE
- Bold attacker will visit ground zero.
- Not-so-bold will drive-by with an amp.



NETGEAR MA401 802.11b Configuration Utility

Status: Associated - 00:02:2D:05:58:BC

Current Channel: 11

Current Tx Rate: 11 Mbits/sec

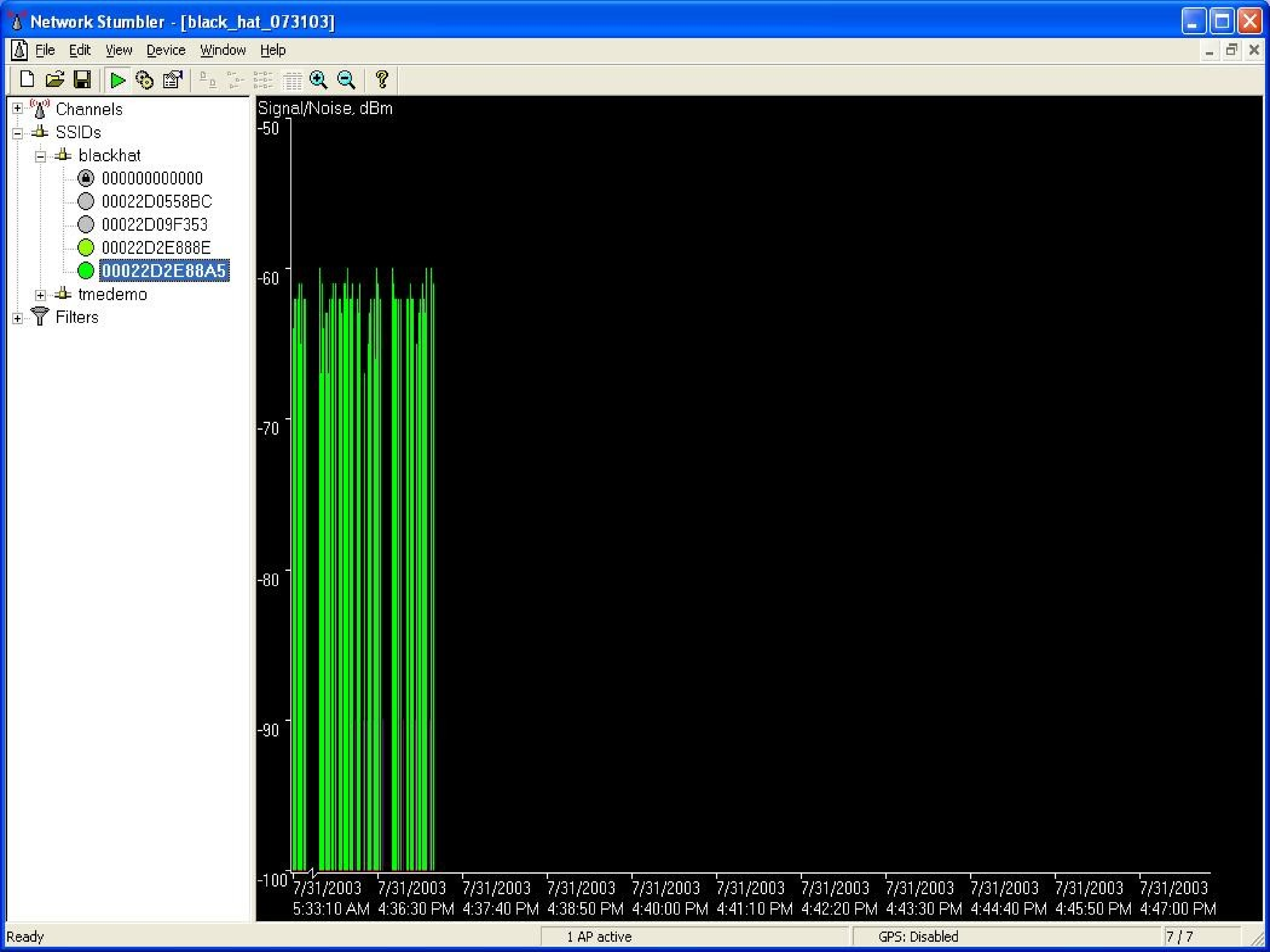
Throughput (Bytes/sec)

Tx: 56

Rx: 1176

Signal Strength: Good (66%)

Link Quality: Excellent (80%)

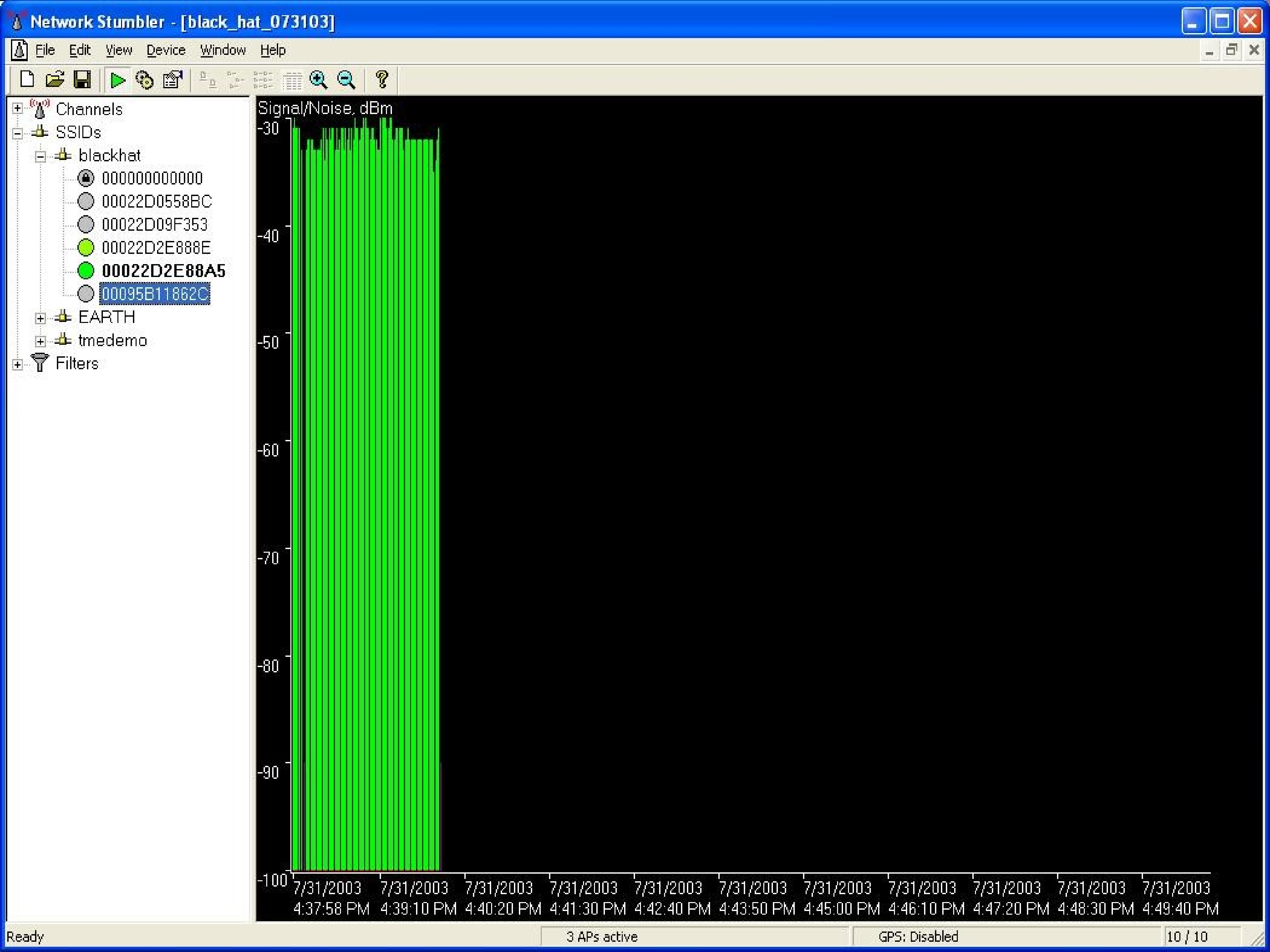


Ready

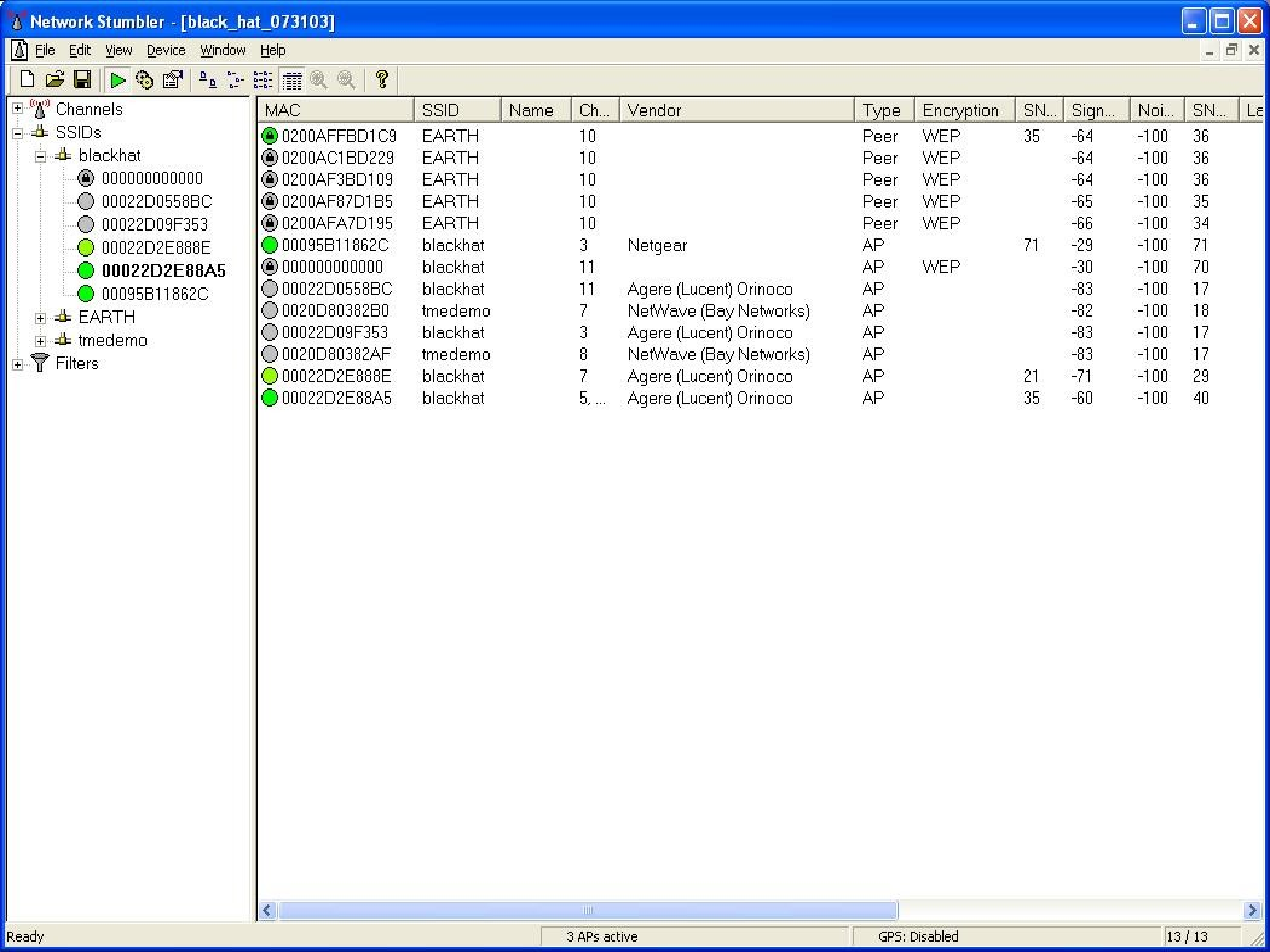
1 AP active

GPS: Disabled

7 / 7



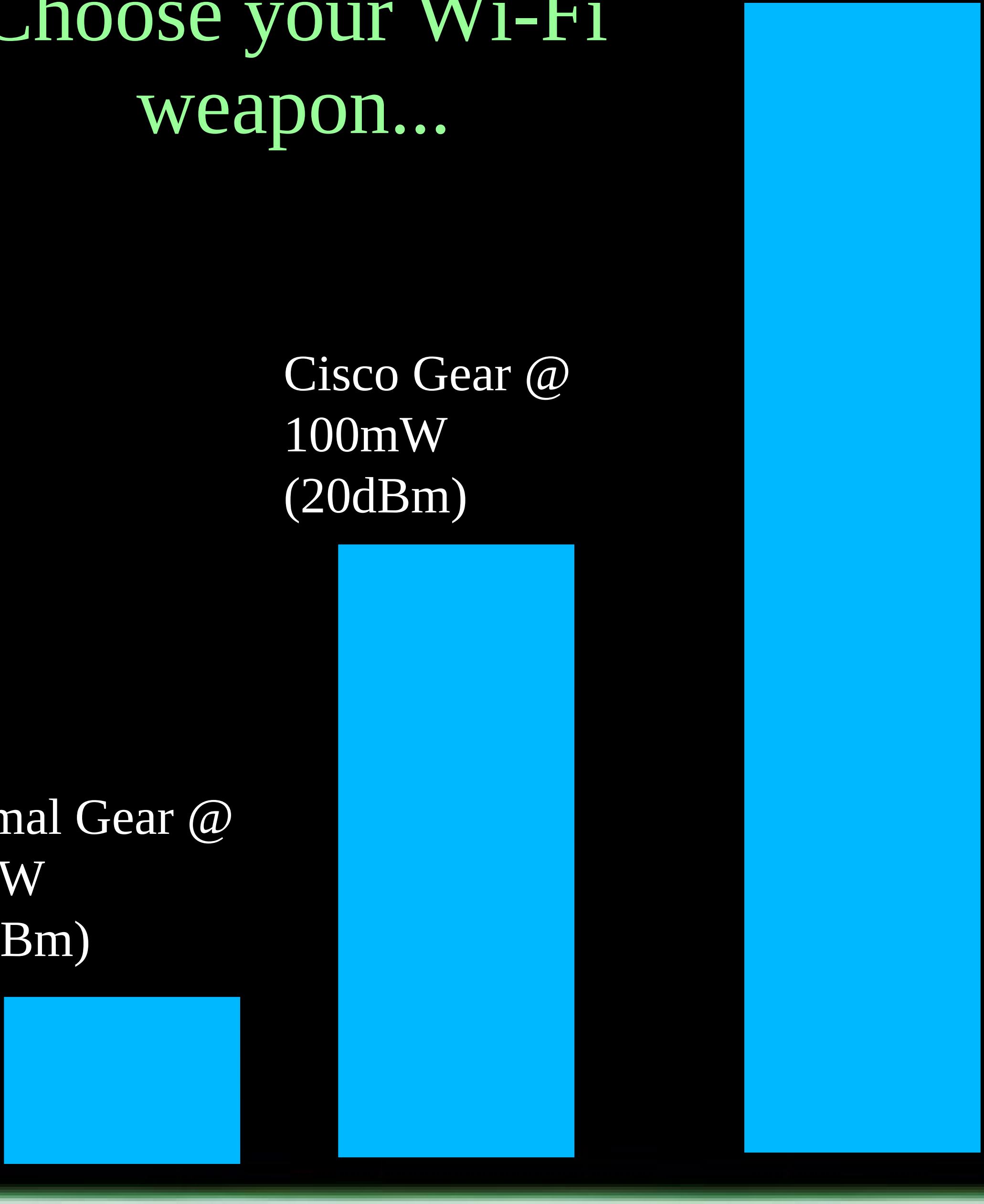
Network Stumbler - [black_hat_073103]
File
Edit
View
Device
Window
Help
Channels
SSIDs
blackhat
000000000000
00022D0558BC
00022D09F353
00022D2E888E
00022D2E88A5
00095B11862C
EARTH
tmedemo
Filters
Signal/Noise, dBm
-30
-40
-50
-60
-70
-80
-90
-100
7/31/2003 4:37:58 PM
7/31/2003 4:39:10 PM
7/31/2003 4:40:20 PM
7/31/2003 4:41:30 PM
7/31/2003 4:42:40 PM
7/31/2003 4:43:50 PM
7/31/2003 4:45:00 PM
7/31/2003 4:46:10 PM
7/31/2003 4:47:20 PM
7/31/2003 4:48:30 PM
7/31/2003 4:49:40 PM
Ready
3 APs active
GPS: Disabled
10 / 10



MAC	SSID	Name	Ch...	Vendor	Type	Encryption	SN...	Sign...	Noi...	SN...	Le
0200AFFBD1C9	EARTH		10		Peer	WEP	35	-64	-100	36	
0200AC1BD229	EARTH		10		Peer	WEP		-64	-100	36	
0200AF3BD109	EARTH		10		Peer	WEP		-64	-100	36	
0200AF87D1B5	EARTH		10		Peer	WEP		-65	-100	35	
0200AFA7D195	EARTH		10		Peer	WEP		-66	-100	34	
00095B11862C	blackhat		3	Netgear	AP		71	-29	-100	71	
000000000000	blackhat		11		AP	WEP		-30	-100	70	
00022D0558BC	blackhat		11	Agere (Lucent) Orinoco	AP			-83	-100	17	
0020D80382B0	tmedemo		7	NetWave (Bay Networks)	AP			-82	-100	18	
00022D09F353	blackhat		3	Agere (Lucent) Orinoco	AP			-83	-100	17	
0020D80382AF	tmedemo		8	NetWave (Bay Networks)	AP			-83	-100	17	
00022D2E888E	blackhat		7	Agere (Lucent) Orinoco	AP		21	-71	-100	29	
00022D2E88A5	blackhat		5, ...	Agere (Lucent) Orinoco	AP		35	-60	-100	40	

Ready | 3 APs active | GPS: Disabled | 13 / 13

Choose your Wi-Fi weapon...



Normal Gear @
25mW
(14dBm)

Cisco Gear @
100mW
(20dBm)

Senao Gear @
200mW
(23dBm)

Use a 15dBd antenna with a Senao for 38dBd total...

6 WATTS!

Vs 25mW?

No contest!

Airsnarf

- Nothing special
- Simplifies HostAP, httpd, dhcpd, Net::DNS, and iptables setup
- Simple example rogue AP
- Demonstration

What’s the big deal?

- Regardless of WiFi security infrastructure, you ARE “vulnerable” to this
- Users WILL give up credentials, WEP keys, you name it
- If you’ve got SSO, doh!
- Physically finding the rogue AP / client can be a challenge
- This is more of a traditional social engineering problem than a technical vulnerability—what’s the “patch”?

Detection

- ANY wireless activity (if policy is no WiFi)
- Duplicate SSIDs
- Different / mismatching MACs
- Interference / SNR spikes
- Association requests
- More…

Client Defense Strategies

- Local AP awareness
- User education
- One-time authentication mechanisms
- Application authentication
- No WiFi? No WiFi connected to Intranet?
- A defence kit for wireless users…? Sort of a ZoneAlarm for WiFi
- *gasp* OS-level awareness of the problem?

HotSpot Defense Kit

- A first pass at making something *usable*
- Checks for changes in
  - ESSID (for clients using ANY)
  - MAC addr of AP (if you roam this may be legit)
  - Default route or router MAC
  - Signal strength
- Currently OS X only

HotSpotDK NG

- Obviously, other OS's…
- Add configuration options for larger networks
  - White-listed MAC's for roaming
  - A sensitivity slider
  - Link status change monitoring (deassoc)

- Why hasn't this been done by now?

A Real Fix - 802.1x

- Link layer authentication
  - Port Based with extensible auth
- Two discrete parts
  - 1x - port-based auth for Ethernet networks
  - EAP - extensible authentication for PPP
- A real layer 2 solution
  - Everything at a higher level fails somehow

802.1x

- Need an EAP method that supports bi-directional authentication
  - Eg: EAP-TTLS, PEAP, etc…
  - EAP-MD5 will not really cut it
- To be included in 802.11i
  - Does NOT provide for encryption
- Will it work as a auth model for public networks?

Links that make you go “hmmm”

- Airsnarf - http://airsnarf.shmoo.com
- ISS Wireless LAN Security FAQ - http://www.iss.net/wireless/WLAN_FAQ.php
- SANS Wireless Reading Room - http://www.sans.org/rr/catindex.php?cat_id=68
- SAFE: Wireless LAN Security in Depth - http://www.cisco.com/go/safe
- Google - “wireless security”
- Airjack – http://802.11ninja.net/airjack/

FYI

- CTF data is available now... http://cctf.shmoo.com
- New Bluetooth tool, “FTC”, http://bluetooth.shmoo.com

Questions?