802.11 WIRELESS SECURITY

Adrian Crenshaw

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything - I'm just a geek with time on my hands

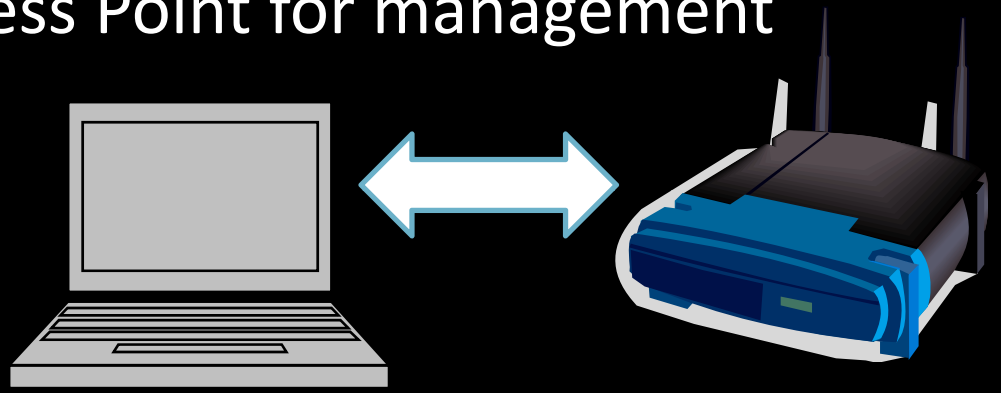
WiFi Basics

- 802.11 includes 802.11a/b/g/n
- 802.11a is in the 5 GHz band
- 802.11b/g is in the 2.4 GHz band
- 802.11n may be 2.4 GHz or 5 GHz

Infrastructure Vs. Adhoc

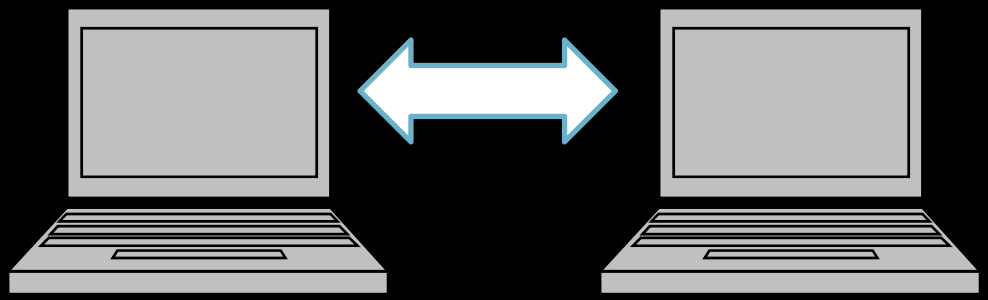
Infrastructure

- Uses and Access Point for management



Adhoc

- Is peer to peer



http://Irongeek.com

2.4 Channels

Channel Number	Lower Frequency MHz	Center Frequency MHz	Upper Frequency MHz
1	2 401	2 412	2 423
2	2 404	2 417	2 428
3	2 411	2 422	2 433
4	2 416	2 427	2 438
5	2 421	2 432	2 443
6	2 426	2 437	2 448
7	2 431	2 442	2 453
8	2 436	2 447	2 458
9	2 441	2 452	2 463
10	2 451	2 457	2 468
11	2 451	2 462	2 473
12	2 456	2 467	2 478
13	2 461	2 472	2 483
14	2 473	2 484	2 495

http://Irongeek.com

5 Ghz band?

2.4 GHz Spectrum	
Channel Number	Channel in GHz
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

2.4GHz - has 3 non-overlapping channels separated by 20MHz (1, 6 and 11). Using 40MHz channel bonding would require using two of the three available channels.

5 GHz Spectrum	
Channel Number	Channel in GHz
34	5.170
36	5.180
38	5.190
40	5.200
42	5.210
44	5.220
46	5.230
48	5.240
52	5.260
56	5.280
60	5.300
64	5.320
100	5.500
104	5.520
108	5.540
112	5.560
116	5.580
120	5.600
124	5.620
128	5.640
132	5.660
136	5.680
140	5.700
149	5.745
153	5.765
157	5.785
161	5.805
165	5.825

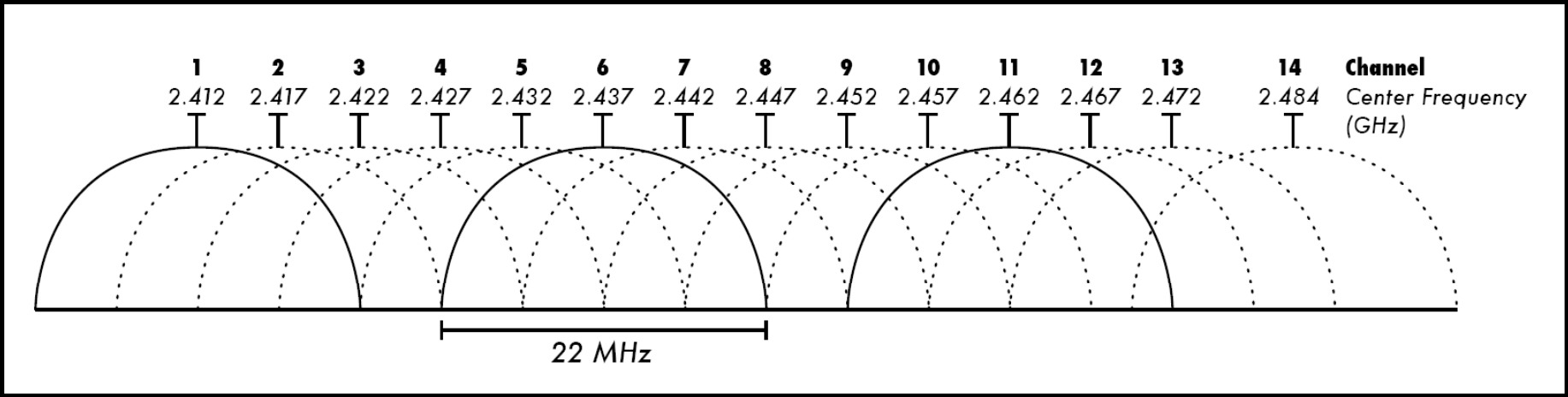
5GHz - has 24 non-overlapping channels separated by 20MHz. This allows up to 12 non-overlapping 40MHz channels.

Chart from http://www.intel.com/support/wireless/sb/CS-025343.htm

http://Irongeek.com

2.4 Overlap

Want no overlap? Go with 1, 6 or 11.



Pic cribbed from Wikipedia

http://Irongeek.com

SSIDs

ESSID

- Stands for Extended Service Set identifier
- It's the network's name
- When people just say SSID, most times they mean the ESSID

BSSID

- Stands for Basic service set identifier
- It's the MAC Address of the Access Point, for example: DEADBEEFCAFE

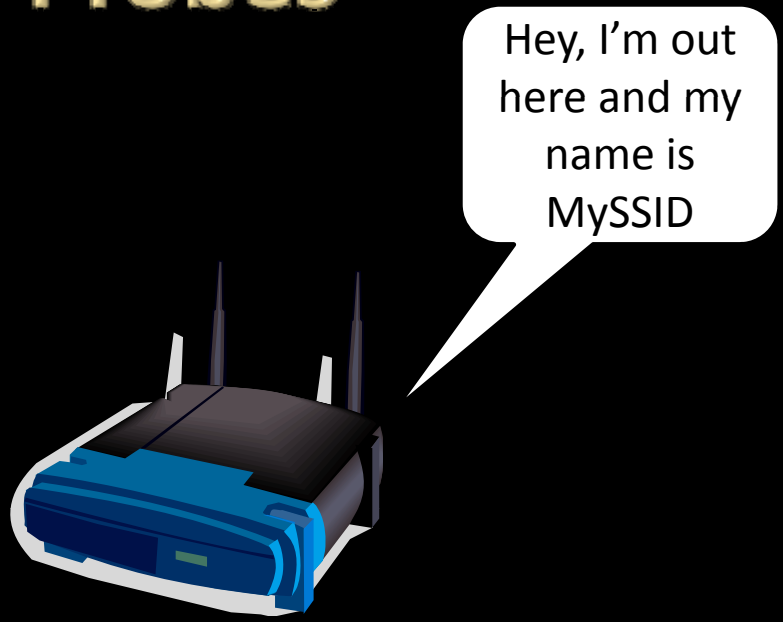
Valid SSIDs

- 32 characters
- Standard does not require ASCII characters
- I wonder if we can have fun with this?
- XSS or SQL injection via war driver?

Beacons and Probes

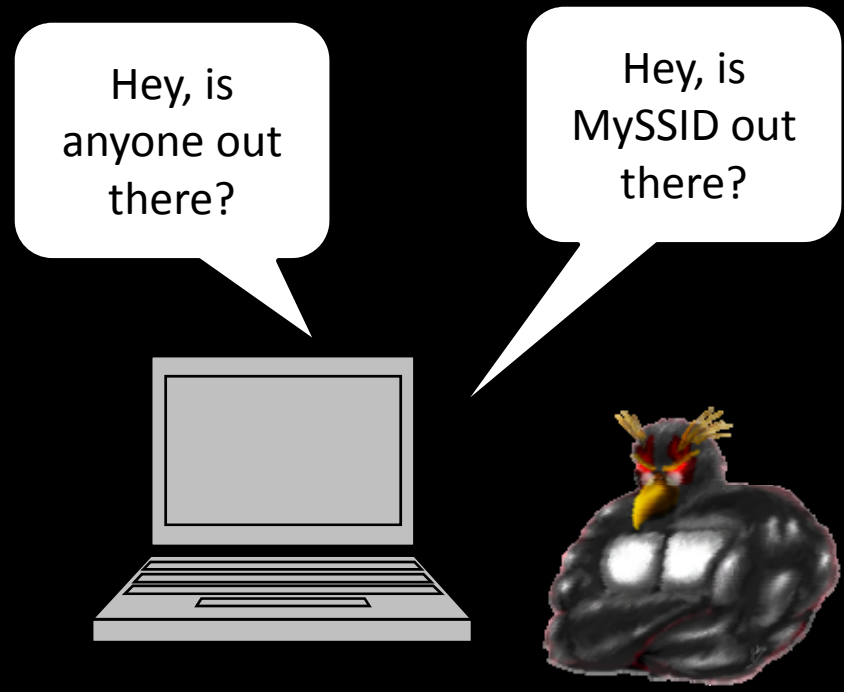
Beacons

- General come from APs saying “Hey, I’m out here!”



Probes

- General come from the clients asking “Hey, who is out there?” or “Is this specific SSID out there?”



Cloaking

- Some APs allow you to try to hide the SSID by not responding to probes and not sending their SSID in the beacons.

http://Irongeek.com

Antennas

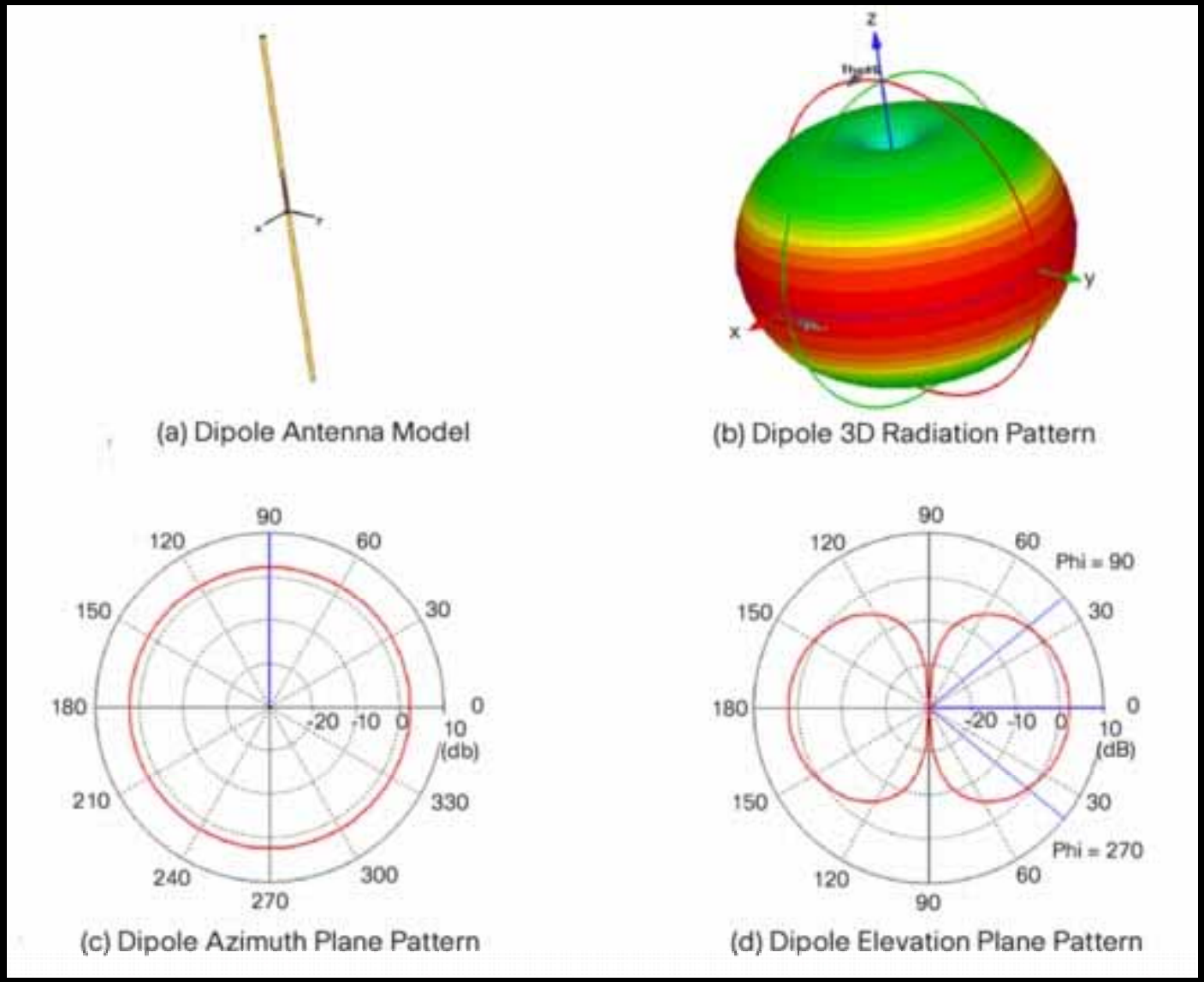
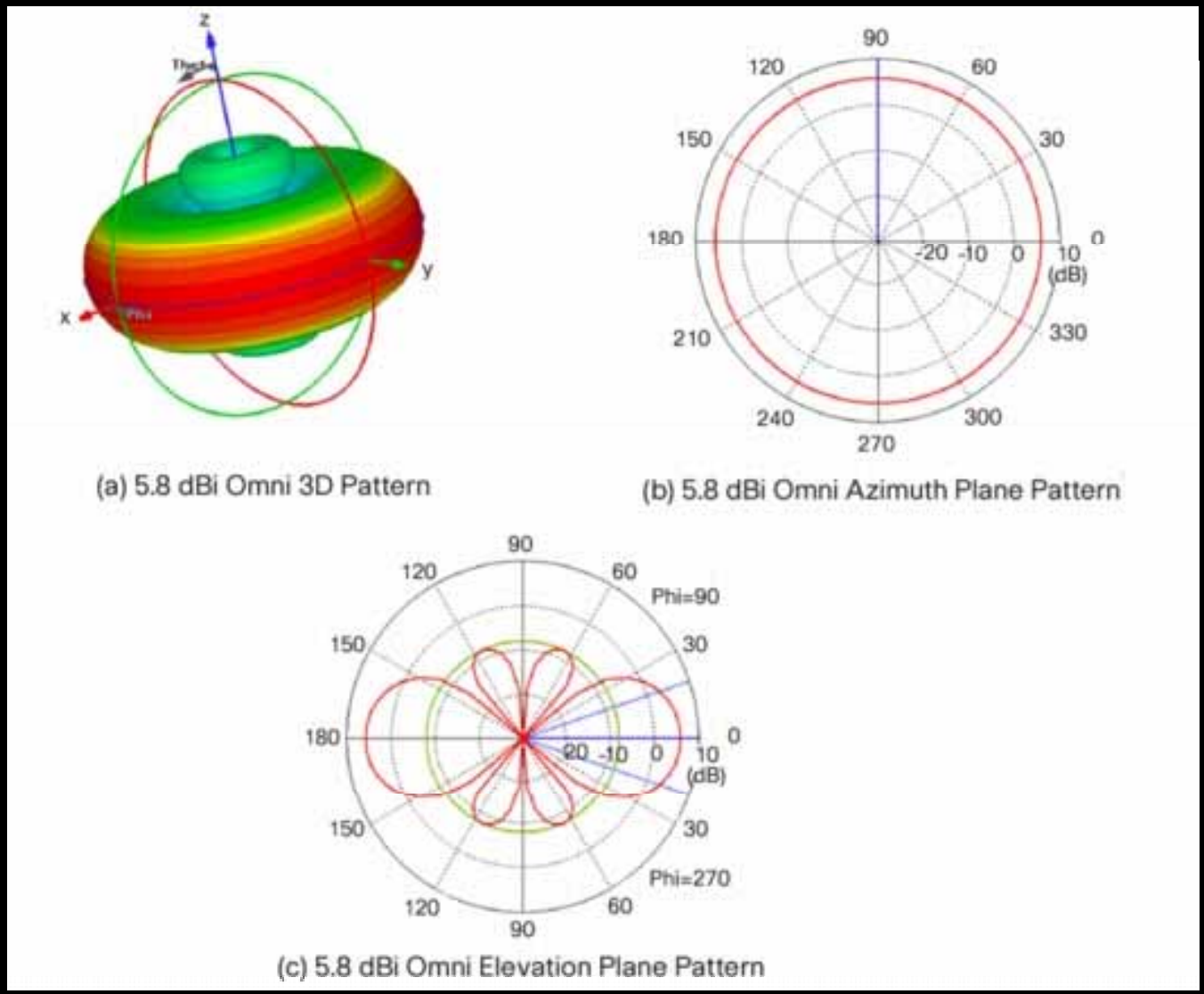


Image from:
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.html

http://Irongeek.com

Antennas



(a) 5.8 dBi Omni 3D Pattern

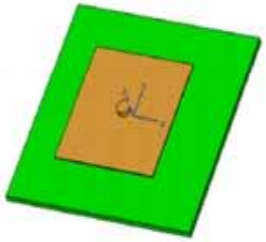
(b) 5.8 dBi Omni Azimuth Plane Pattern

(c) 5.8 dBi Omni Elevation Plane Pattern

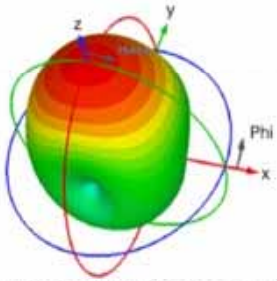
Image from:
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.html

http://Irongeek.com

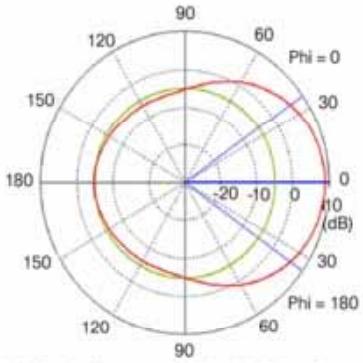
Antennas



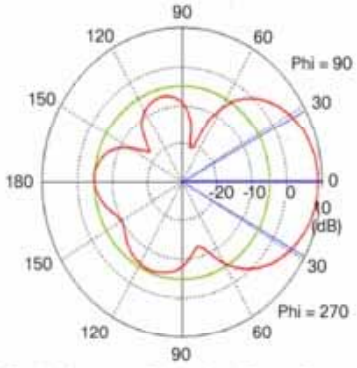
(a) Patch Antenna Model



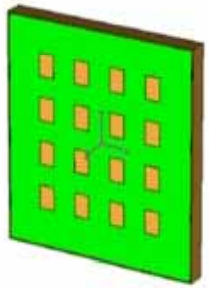
(b) Patch Antenna 3D Radiation Pattern



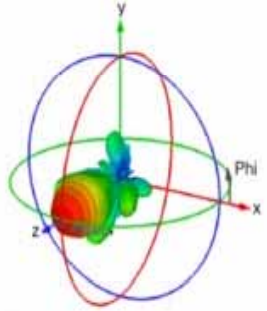
(c) Patch Antenna Azimuth Plane Pattern



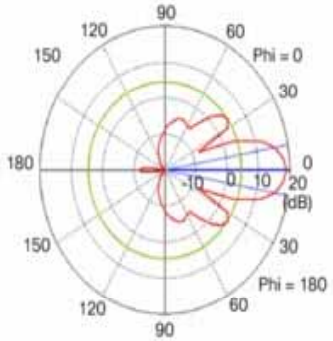
(d) Patch Antenna Elevation Plane Pattern



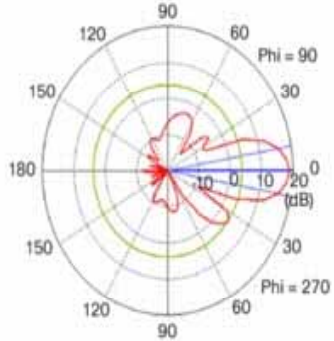
(a) 4x4 Patch Array Antenna



(b) 4x4 Patch Array 3D Radiation Pattern



(c) 4x4 Patch Array Azimuth Plane Pattern



(d) 4x4 Patch Array Elevation Plane Pattern

Image from:
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.html

http://Irongeek.com

Antennas

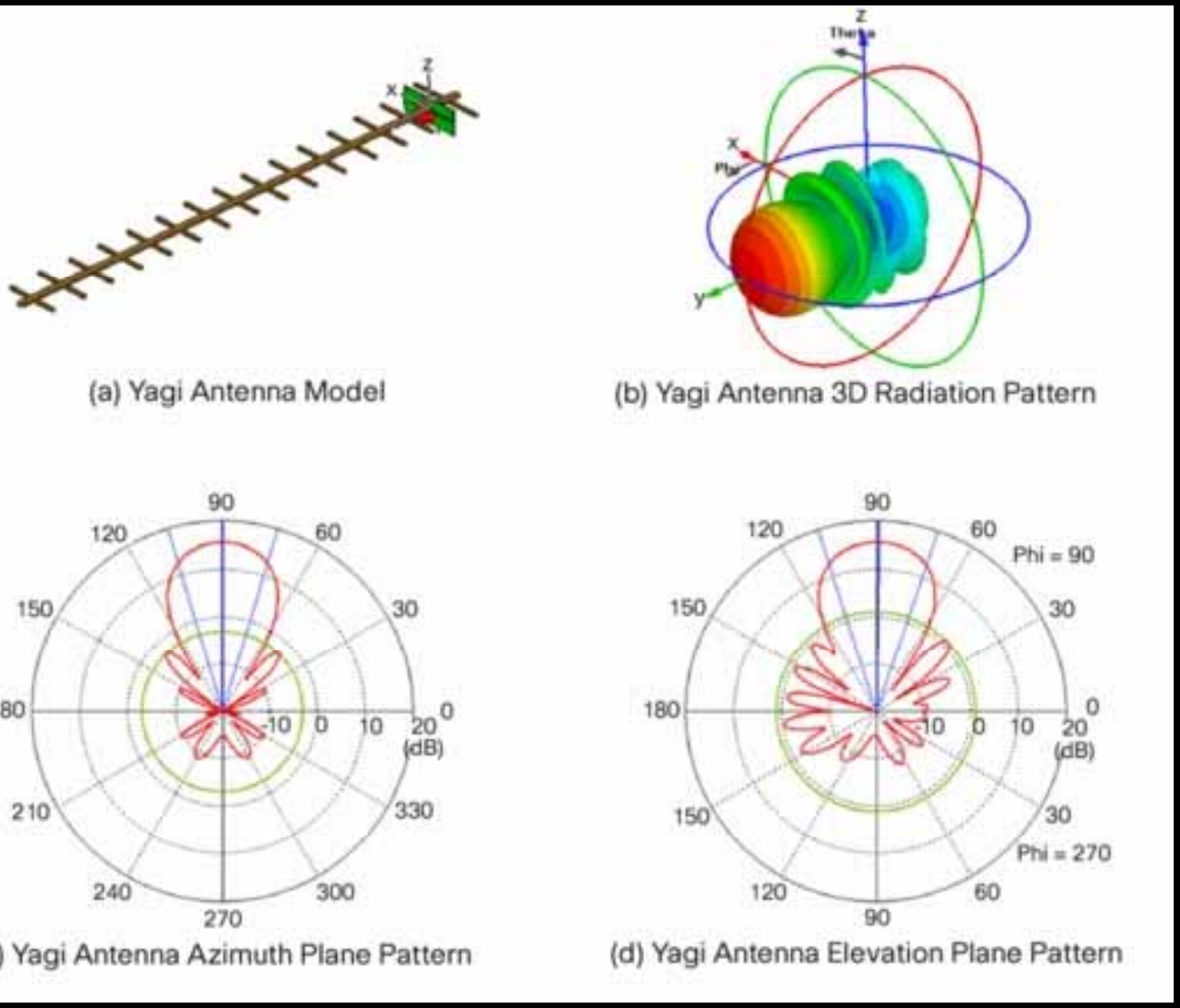


Image from:
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.html

http://Irongeek.com

What you want in a WiFi card

- USB is nice, since you can sometimes us it in VMWare
- Antenna connectors are nice
- Promiscuous mode
- Monitor mode
- Injection
- Master mode?

What I have:

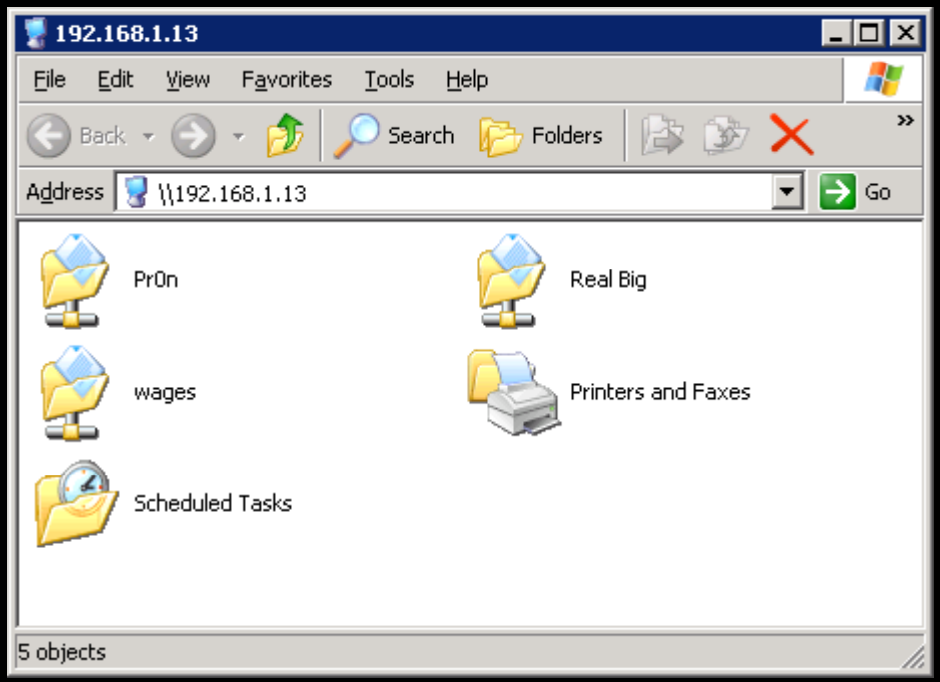
RT73 Based:
http://www.dealextreme.com/details.dx/sku.24688~r.48687660
ZyDAS1211 Based:
http://www.dealextreme.com/details.dx/sku.22682~r.48687660

A note on chipsets

- Some cards will support monitor but not promiscuous, or vice versa
- Atheros or RaLink are pretty good (ZyDAS seems ok too)
- Vendors change chipsets between different reversions of their adapters
- Some USB adapters can be used in VMWare
- Aircrack-NG chipset list
  http://www.aircrack-ng.org/doku.php?id=compatibility_drivers
- WinPCap list
  http://web.archive.org/web/20080102184219/http://www.micro-logix.com/WinPcap/Supported.asp

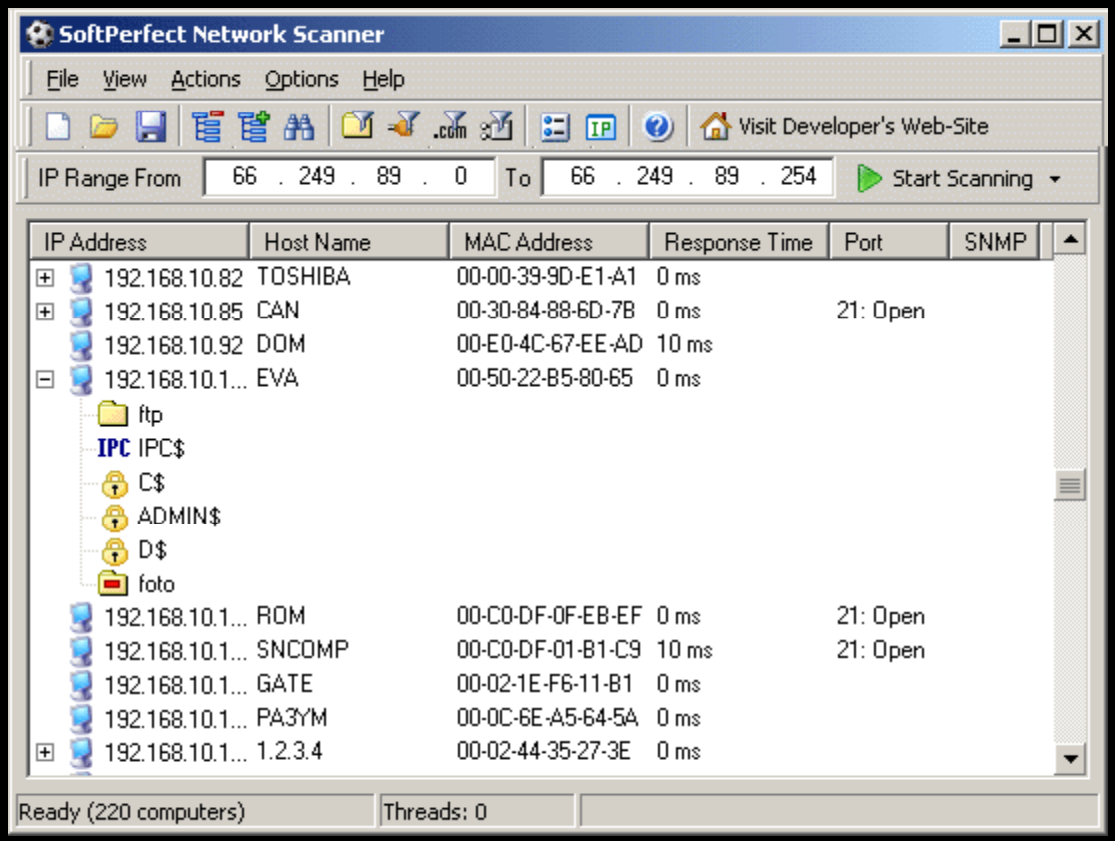
Open File Shares

- So, do you know what you're sharing?
- \\your-computer-name (or IP)



Scanning for shares

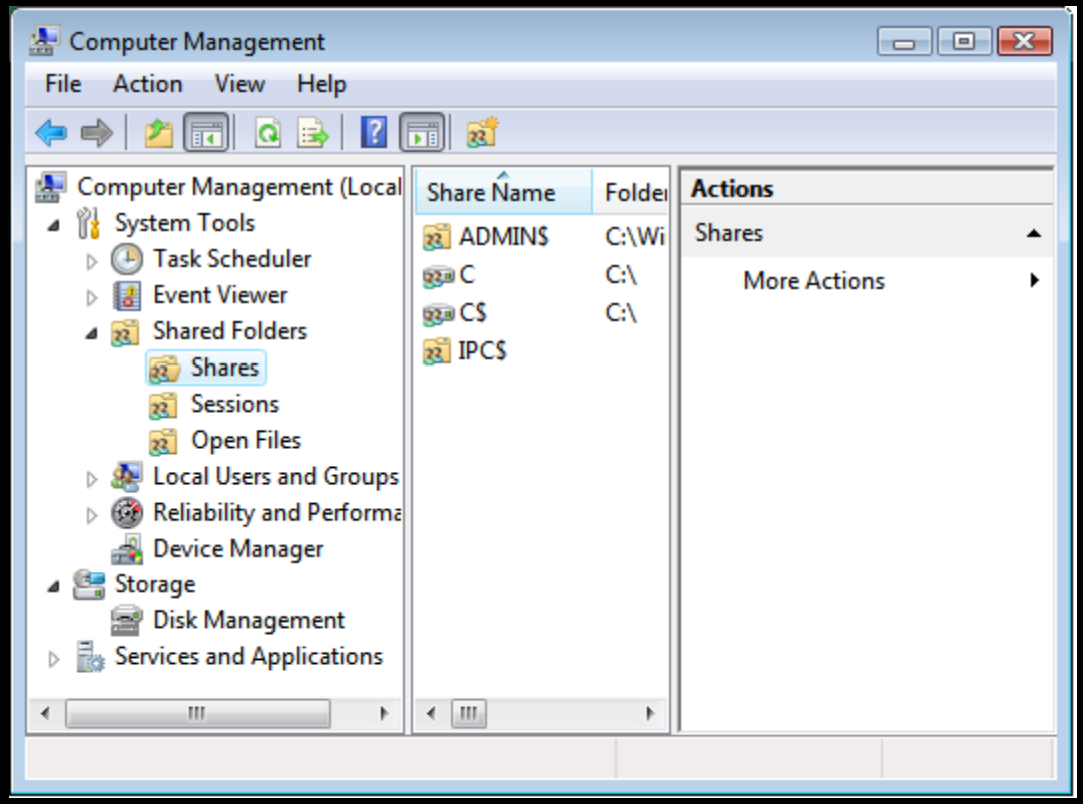
- Softperfect's NetScan



http://Irongeek.com

Change your sharing settings

- compmgmt.msc



- Firewall it off
- Click Start->Control Panel->Network Connections, then right click on your wireless connection, choose properties and uncheck "File and Printer Sharing for Microsoft Networks" to disable it.

http://Irongeek.com

Demo Time!!!

- NetScan

SNIFFERS

There will be more sniffers running at a hacker/security conference than at a bloodhound convention

http://Irongeek.com

Why worry about how you smell?

- Plaintext protocols can leak passwords:
  Telnet, HTTP, SMTP, SNMP, POP3, FTP, etc
- Files can be reassembled
- Private messages can be read

Promiscuous mode

- Not a network card of questionable sexual morals
- Have to be connected, won't see management frames
- Sometime it will be the only thing that gives you data, depending on the link layer
- With ARP poisoning, you may even be able to sniff data from the wired side of the LAN

Monitor mode

- Most of the time this will work:
  ifconfig wlan0 down
  iwconfig wlan0 mode monitor channel 9
  ifconfig wlan0 up

- If you have Aircrack-NG installed:
  airmon-ng <start|stop> <interface> [channel]

- Dump them packets for later perusal:
  tcpdump -i wlan0 -s 0 -w montest.pcap

- If you use Windows Vista (NDIS 6) try:
  Microsoft Network Monitor 3.2

Great sniffing tools

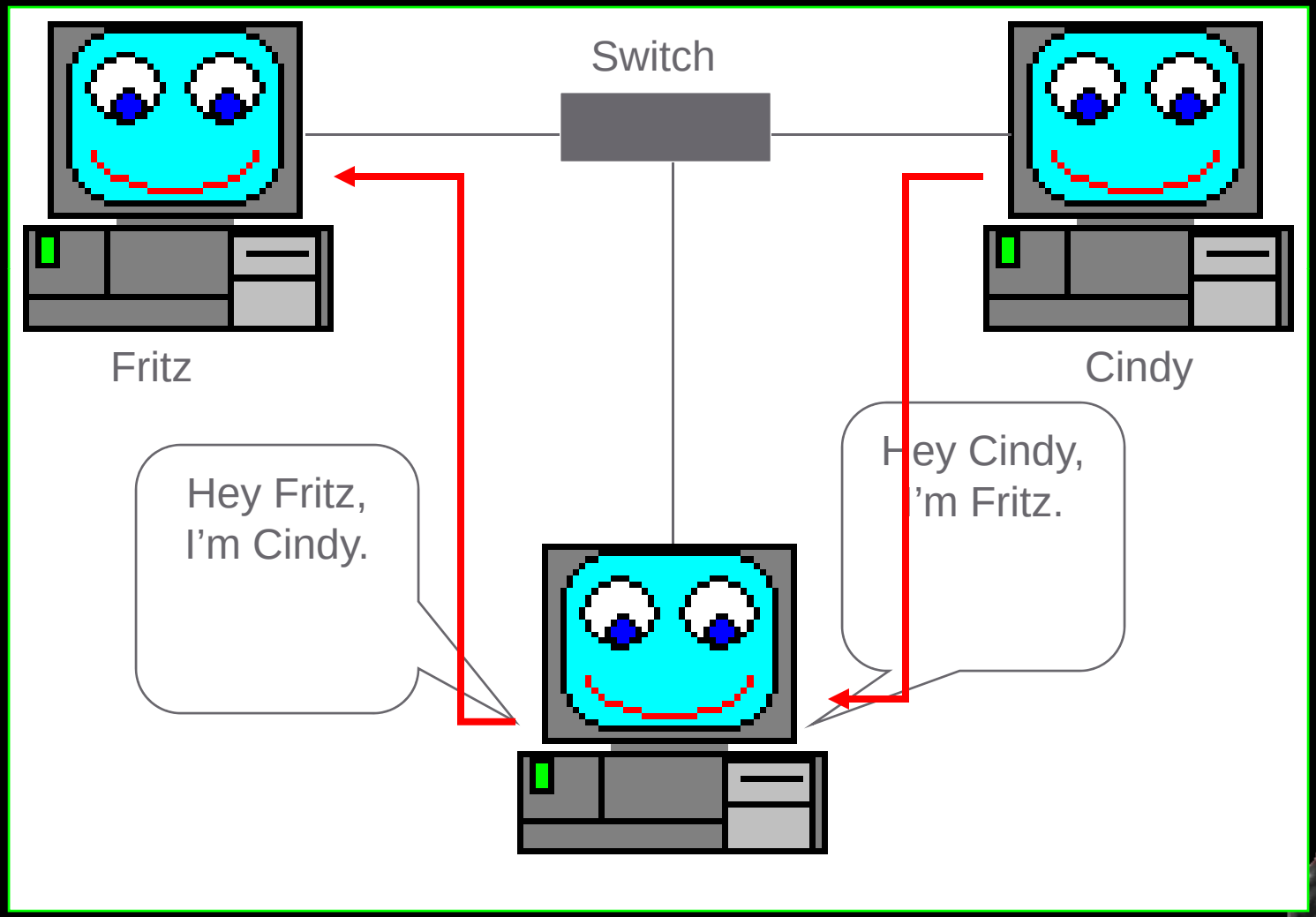
- Wireshark
  good for general purpose sniffing
- Ettercap
  good for password collection
- Cain
  good for password collection
- Dsniff (and related snarf tools)
  good for password collection and file snarfing
- NetworkMiner
  good for password collection and file snarfing
- Driftnet
  good for image snarfing

MAN IN THE MIDDLE

AKA: Monkey in the Middle

http://Irongeek.com

Looks a little like this



ARP Poisoning

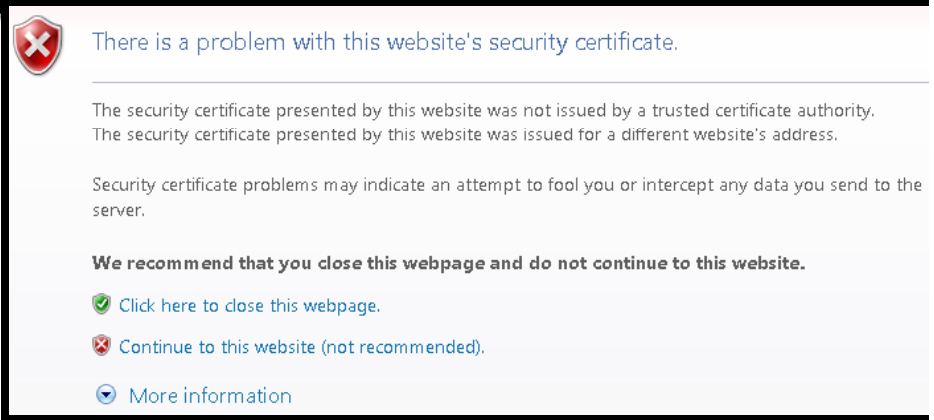
- On the local subnet, IPs are translated to MAC addresses using ARP (Address Resolution Protocol)
- ARP queries are sent and listened for, and a table of IPs to MACs is built (arp -a)
- Pulling off a MITM (Man In The Middle) attack
- If you MITM a connection, you can proxy it and sometime get around encryption
  - SSL
  - RDP
  - WPA

Tools for MITM

- Cain
- Ettercap
- The-Middler
- SSLStrip

Signs of MITM

- SSL/TLS Warnings



- Slow connections
- IP conflicts
- DecaffeinatID: A Very Simple IDS / Log Watching App / ARPWatch For Windows
  http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows

Demo Time!!!

- Wireshark Promiscuous mode
- Cain and ARP poisoning
- Wireshark in RFMon mode
- TCPDump and wlan2eth
- NetworkMiner
- Ettercap

  etterfilter ig.filter -o ig.ef
  ettercap -T -q -F ig.ef -M ARP /192.168.1.1/ //
  (From http://www.irongeek.com/i.php?page=security/ettercapfilter)
- NetworkMonitor 3.2 and mention nm2lp

WARDRIVING:FINDING ACCESS POINTS

Rogue or Otherwise

http://Irongeek.com

What you need to wardrive

- A WiFi Device (Laptop, PDA, Phone, Internet Tablet)

- Software to find APs

What really helps

- GPS

- Car Inverter
- Mapping software
- Different antennas

Types of Wardriving Apps

- Active (Sends probes, listens to beacons)
  Examples: NetStumbler, Vistumbler, InSSIDer, WiFiFoFum

- Passive (Listens in Monitor Mode for beacons, associations)
  Examples: Kismet, Kismac

Passive for the Win!!!

Probes:

- Don't have to actively probe, giving away that someone was looking
- Can find "cloaked" SSIDs if there is any association traffic
- Can pick up probes from clients

Cons:

- Pretty much, you have to use a *nix based OS

Demo Time!!!

- Netstumbler
- Vistumbler
- InSSIDer
- Kismet (new and old core)
  - And show why MAC filtering is useless
- Kismac

Changing your MAC Address

Linux:

ifconfig eth0 down hw ether 00:00:00:00:00:01

ifconfig eth0 up

Or edit

/etc/network/interfaces

Or if you want to add a package

macchanger eth1

Windows:

For some drivers, it's in the device config GUI

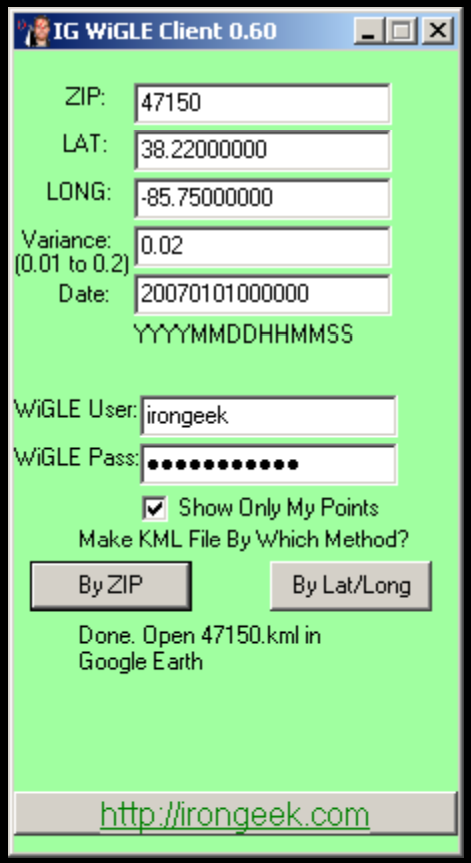
Or

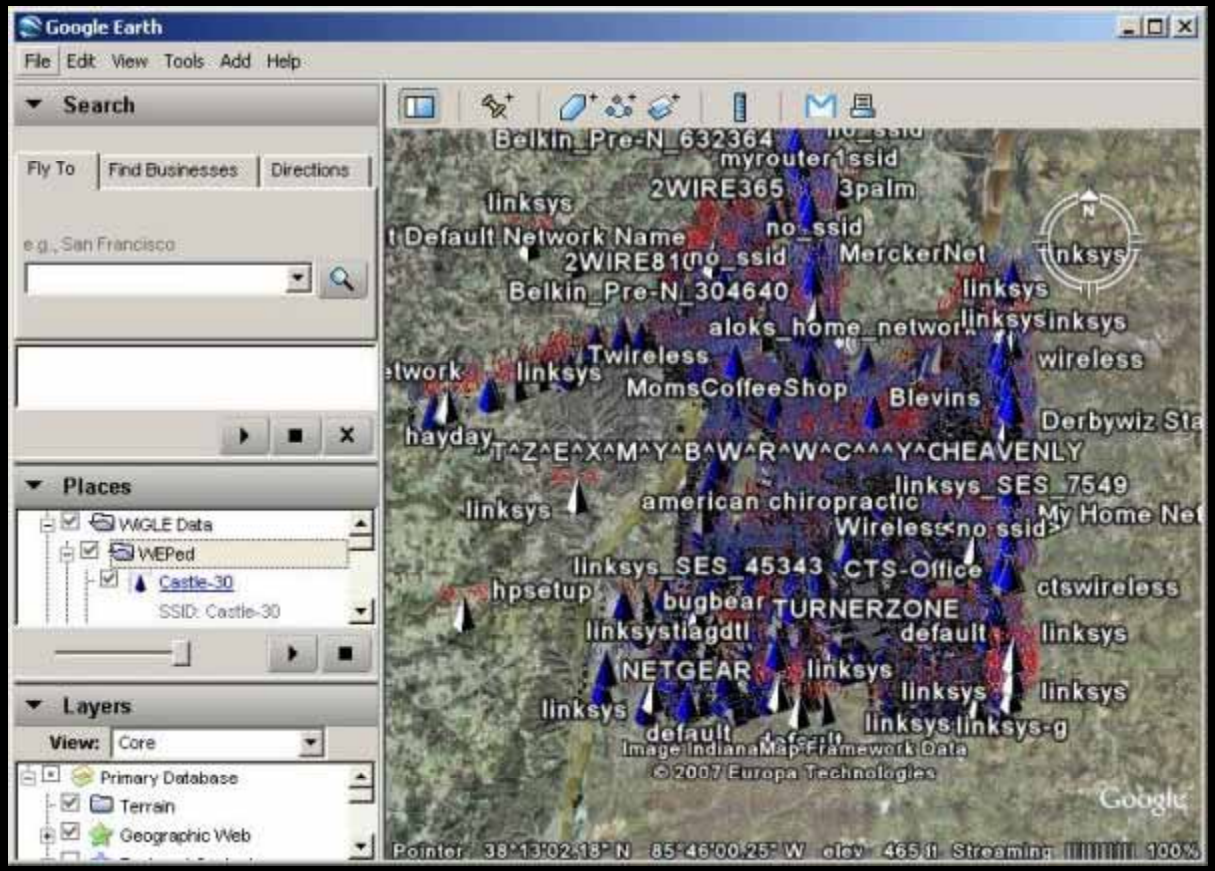
Regedit it's entry in
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\

Or use MadMACs

http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer

Mapping with IGiGLE





http://www.irongeek.com/i.php?page=security/igigle-wigle-wifi-to-google-earth-client-for-wardrive-mapping

Demo Time!!!

- IGiGLE

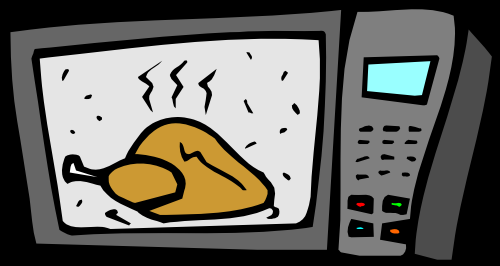
Finding Rouge Access Points From The Wired Side

- By MAC Address
  OUI list at http://standards.ieee.org/regauth/oui/oui.txt
- Port numbers and banner grabbing
- Check out:
  http://pauldotcom.com/2008/11/discovering-rogue-access-point.html

Denial of Service

- Not much you can do about it
- Lot's of stuff in the 2.4GHz band





- 802.11 was not designed to be robust against deliberate DoS
- Deauthentication attack time!!!

Packet Injection

- The ability to stick packets in the air, without associating
- Useful for generating extra traffic when you want to collect weak Ivs to crack WEP
- Also useful for DoS attacks, or to make a client re-associate so you can sniff the SSID

Demo Time!!!

- Aireplay test and deauth with rt73:

  iwconfig

  airmon-ng start wlan0 1

<May have to unplug, replug>

  airmon-ng start wlan0 1

  aireplay-ng wlan0 -9 -i mon0

  aireplay-ng wlan0 -0 0 -e SomeSSID

U3 to grab keys

- Using the autorun functionality of a U3 thumbdrive to quickly dump data off of a target box (some times a U3 Switchblade)
- In this case, I use NirSoft's WirelessKeyView to dump the WEP and WPA keys

Demo Time!!!

- U3 Switchblade/WirelessKeyView

Evil Twin Attack

- Do you know for sure who you are attaching to?
- Can use tools like Hotspotter or Karma
- Who do you auto connect to when in range?
- Mention the “AdHock worm”

Demo Jasager

- Jasager/Karma from:
  http://www.digininja.org/jasager/
- Using the following Firmware:
  http://piranha.klashed.net
- Hak5 forums for more details:
  http://hak5.org/forums/index.php?showforum=49

Tunneling

Look into the following:

- VPN/Hamachi
- SSH port forwarding
- DD-WRT has built in VPN support
- Tor is not a VPN substitute , but can help with staying anonymous
- Watch out for folks “following you home” to your own network

Links to tools

BackTrack
http://www.remote-exploit.org/backtrack.html

SoftPerfect Network Scanner
http://www.softperfect.com/products/networkscanner/

Aircrack-ng
http://www.aircrack-ng.org

TCPDump/Libpcap
http://www.tcpdump.org/

Microsoft Network Monitor
http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=f4db40af-1e08-4a21-a26b-ec2f4dc4190d&displaylang=en

DecaffeinatID
http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows

Cain
http://www.oxid.it/cain.html

Ettercap
http://ettercap.sourceforge.net/

Wireshark
http://www.wireshark.org/

Wlan2eth
http://www.willhackforsushi.com/?page_id=79

Nm2lp
http://www.inguardians.com/tools/

NetworkMiner
http://sourceforge.net/projects/networkminer/

NetStumbler
http://www.netstumbler.com/

Vistumbler
http://www.vistumbler.net/

InSSIDer
http://www.metageek.net/products/inssider

Kismet
http://www.kismetwireless.net/

IGiGLE
http://www.irongeek.com/i.php?page=security/igigle-wigle-wifi-to-google-earth-client-for-wardrive-mapping

Google Earth
http://earth.google.com/

WirelessKeyView
http://www.nirsoft.net/utils/wireless_key.html

Hotspotter
http://www.remote-exploit.org/codes_hotspotter.html

Karma
http://wirelessdefence.org/Contents/KARMAMain.htm

http://Irongeek.com

Events

- Free ISSA classes
- ISSA Meeting
  http://issa-kentuckiana.org/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Phreaknic/Notacon/Outerz0ne
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

Thanks

- Brian and Jeff
  http://www.pocodoy.com/blog/
- Joshua Wright
  http://www.willhackforsushi.com/
  http://www.inguardians.com/pubs/Vista_Wireless_Power_Tools-Wright.pdf
- Muts and crew for BT4
- Robin Wood
- Hak5 Crew
- Russell Butturin
- ColdSteal for the Fon
  http://www.i-trash.org
- Kelly for getting us the room and organizing things
- Folks at Binrev and Pauldotcom
- Louisville ISSA
- Larry “metadata” Pesce
  http://pauldotcom.com
- John for the extra camera

http://Irongeek.com

Helping with the free classes

- Got old hardware you would like to donate?
- Is there a subject you would like to teach?
- Let others know about upcoming classes, and the videos of previous classes.

QUESTIONS?

42

http://Irongeek.com