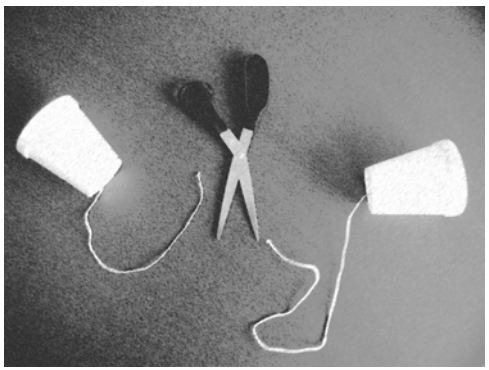
GSA FTS
Network Services Conference
April 15–18, 2002
Orlando, Florida

DISCOVER the POSSIBILITIES

Hello? Who's Listening In?



Wireless Security Basics.
Presented By: Chris O'Ferrell
C.T.O. NETSEC

INTRODUCTION

DISCOVER the POSSIBILITIES

- History of 802.11
- Wireless Basics
- 802.11b Security Issues
- Countermeasures
- Hacking Wireless
- Solutions

802.11 History

- The 802.11 working group was established in 1990 by the IEEE Executive Committee. Their goal was to create a wireless local area network (WLAN) standard. The standard specified an operating frequency in the 2.4GHz ISM (Industrial, Scientific, and Medical) band.
- Seven years later (1997), the group approved IEEE 802.11 as the world's first WLAN standard with data rates of 1 and 2 Mbps.
- In 1999 the working group approved two extensions to 802.11.
  - 802.11a - U-NII band - (Unlicensed National Information Infrastructure) 5GHz.
    - Operates at 54 Mbps (due to higher frequency)
    - Only allow access to clients within 40 – 50 feet due to power limits enforced by the FCC
  - 802.11b - 2.4GHz ISM band
    - Operates at 11 Mbps
    - Allows client access up to well over 1000 feet

802.11 History cont.

- The Whole Family
  - 802.11a - 54 megabits per second (SSDS - Spread-Spectrum Direct Sequence)
  - 802.11b -11 megabits per second (SSDS - Spread-Spectrum Direct Sequence)
  - 802.11c - Specification to cover bridge operation with IEEE 802.11 MAC's
  - 802.11d - Amendment to 802.11 specification regarding Telecommunication and information exchange between two systems and Extensions to operate in additional regulatory domains
  - 802.11e - Expand support for applications with Quality of Service requirements

802.11 History cont.

- 802.11f - Recommended Practice for Inter Access Point Protocol - (point to point roaming)
- 802.11g Standard for Higher Rate (20+ Mbps) Extensions in the 2.4GHz Band
- 802.11h - Spectrum Managed 802.11a - European-inspired additions to 802.11a. Requires devices to check whether given frequencies are in use before transmitting. (Dynamic Frequency Selection or DFS)
- 802.11i - Enhance the current 802.11 MAC to provide improvements in security. Working to find a replacement for WEP. Temporal Key Integrity Protocol (TKIP)
- 802.1X (not 802.11X) – Improving 802.11 security by - Extensible Authentication Protocol over LANs (EAPOL). Defines the way users authenticate themselves to a wireless LAN.

DISCOVER the POSSIBILITIES

Wireless Basics

Wireless Basics

- 802.11b - “WiFi” networks are typically implemented as either a standalone network solution, or to extend the capabilities of an existing wired network.
- The most common wireless configurations found today are:
    - Ad Hoc
    - Infrastructure modes

Wireless Basics cont.

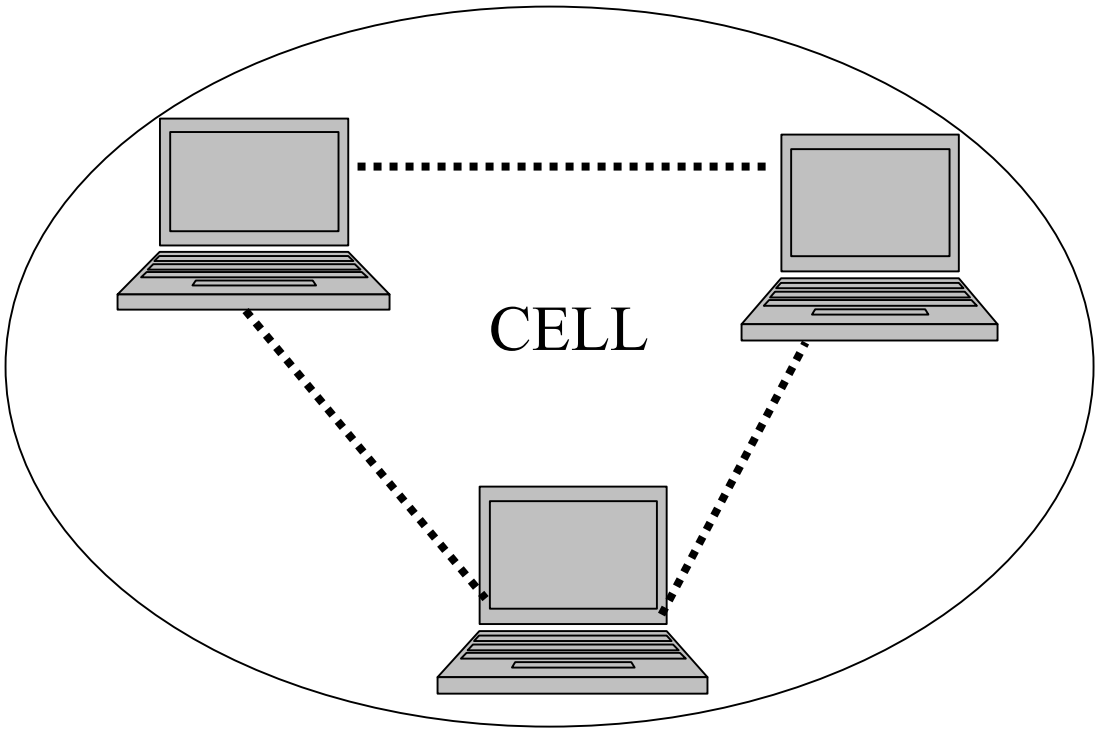
DISCOVER the POSSIBILITIES

Ad Hoc

- Also referred to as “Independent Basic Service Set” (IBSS)
- Provides peer-to-peer communication links between two or more wireless devices without the use of an AP
- This is the default setting on most wireless cards

Wireless Basics cont.

Ad Hoc - Peer-to-Peer Configuration



Wireless Laptop Computers

Wireless Basics cont.

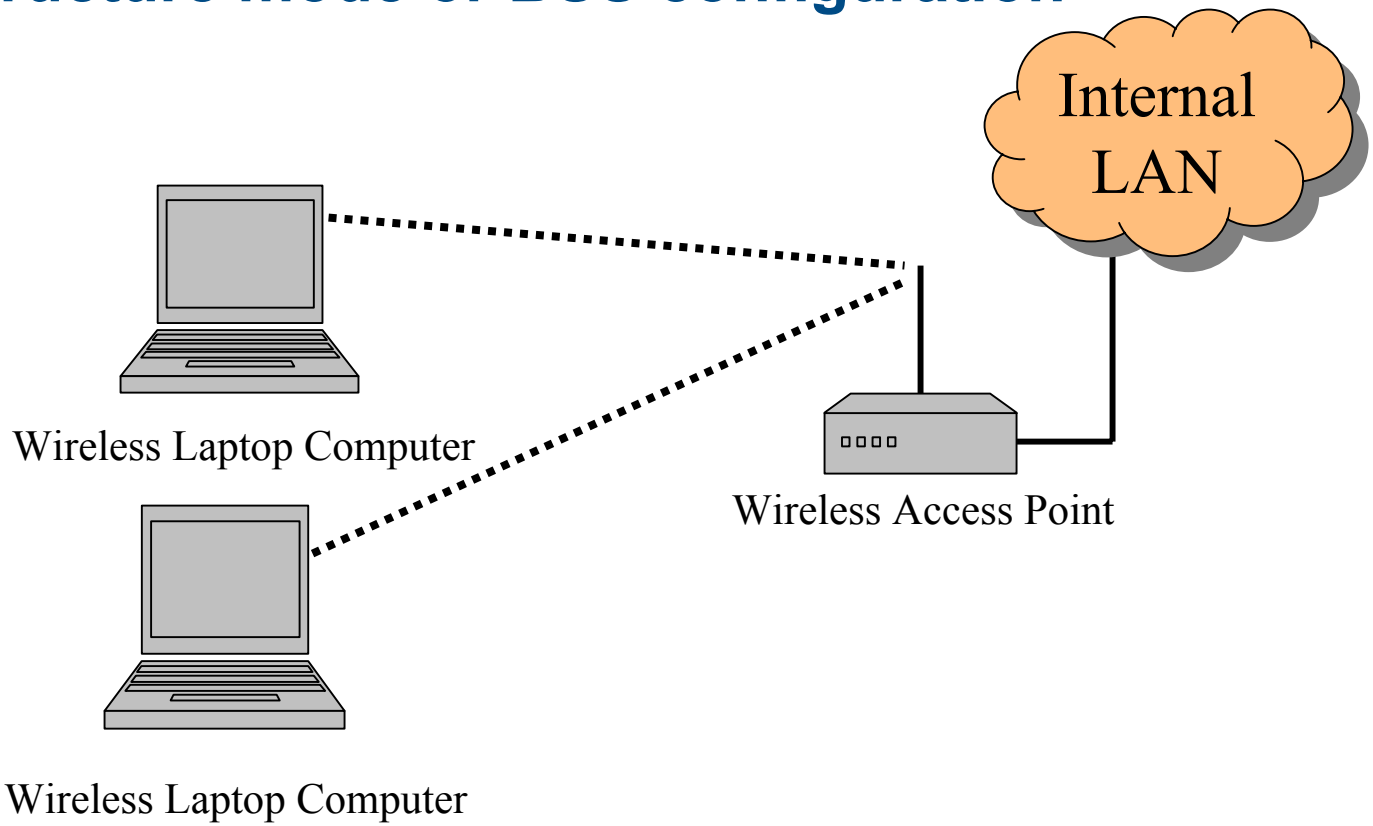
DISCOVER the POSSIBILITIES

Infrastructure

- Also known as “Basic Service Set” (BSS)
- Requires an Access Point and at least one wireless client
- Connections are initiated with the proper Service Set Identifier (SSID) - Shared secret manually entered on the AP and each client (Not scalable)
- Sometimes Wired Equivalent Privacy (WEP) encryption keys are also configured (Used about 30% of the time)

Wireless Basics cont.

Infrastructure mode or BSS configuration



Security Issues

802.11b Security Issues

DISCOVER the POSSIBILITIES

Antenna Signal

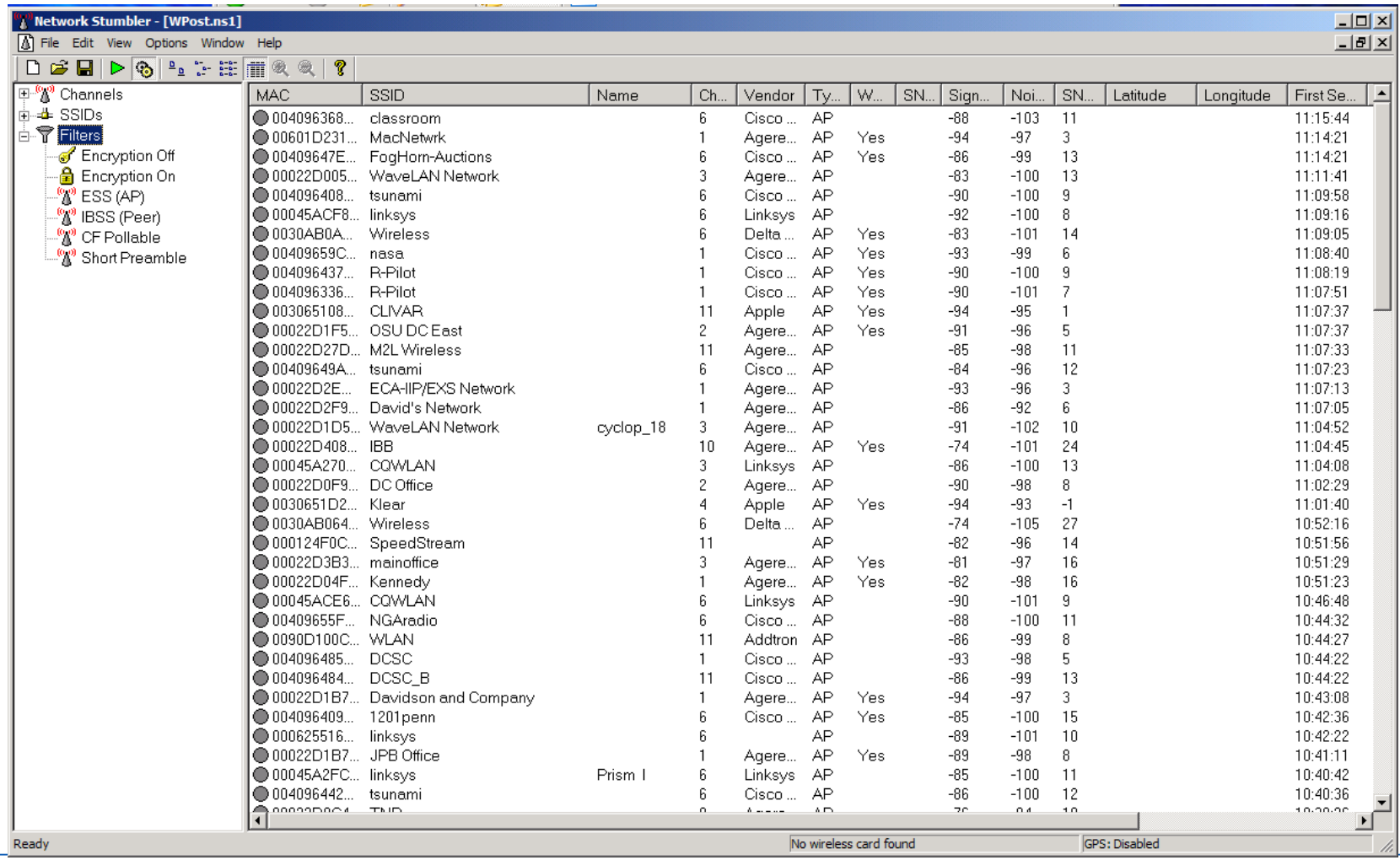
- Walls and doors do not provide sufficient containment of the wireless signal. An Access Point (AP) placed inside a typical office can transmit a signal anywhere up to 1000+ feet.
    - 300 feet in any direction will usually put you on a road, in a neighboring office or parking lot.
    - Vertical threats such as offices above and below should also be taken into consideration when selecting your AP's location.
    - Hackers will War-Drive at lunch looking for AP's used in conference rooms.

802.11b Security Issues

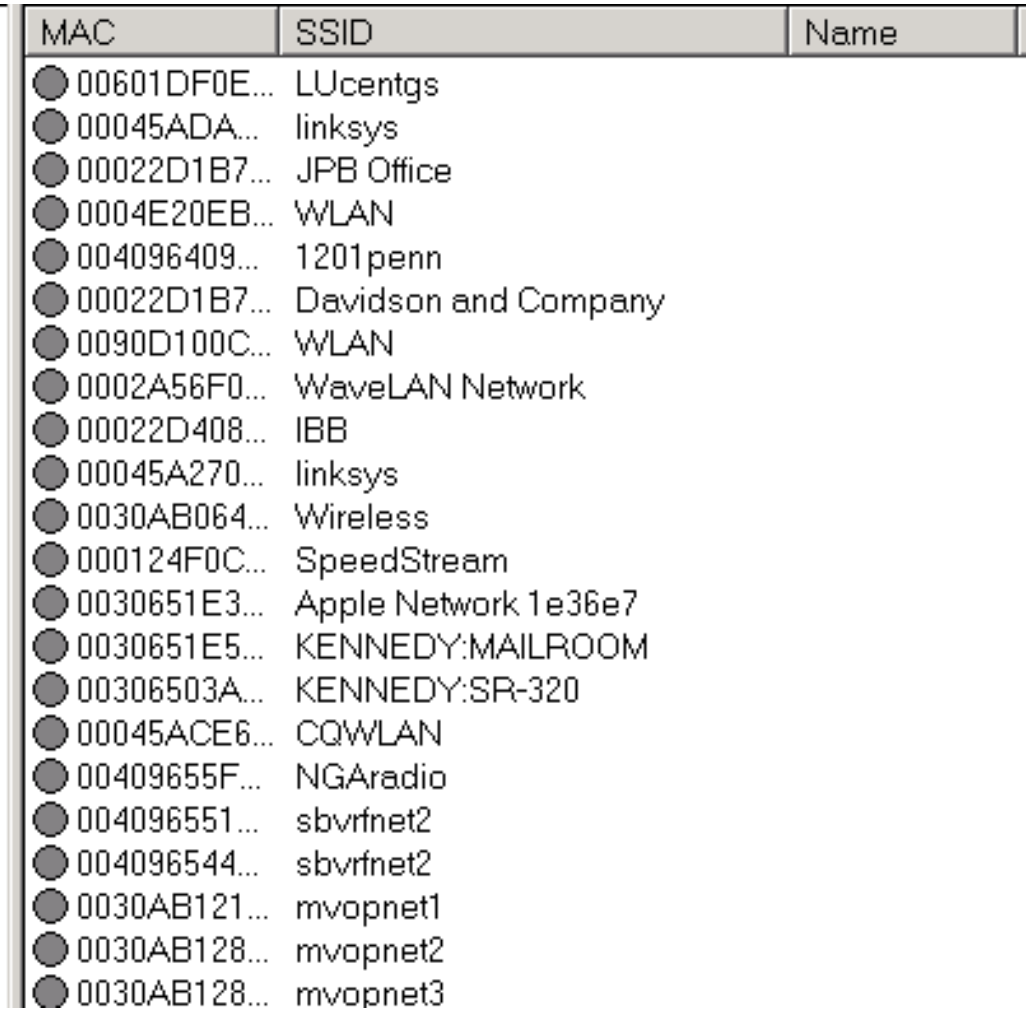
Service Set Identifier - SSID

- Some users believe that by using a complicated SSID an unauthorized user will have difficulty in gaining access to their AP.
  - SSID's are passed in the clear, even when WEP is enabled.
  - It is a trivial matter to download free software off the Internet "*http://www.netstumbler.com*" designed to intercept SSID's from a wireless communication session.

802.11b Security Issues



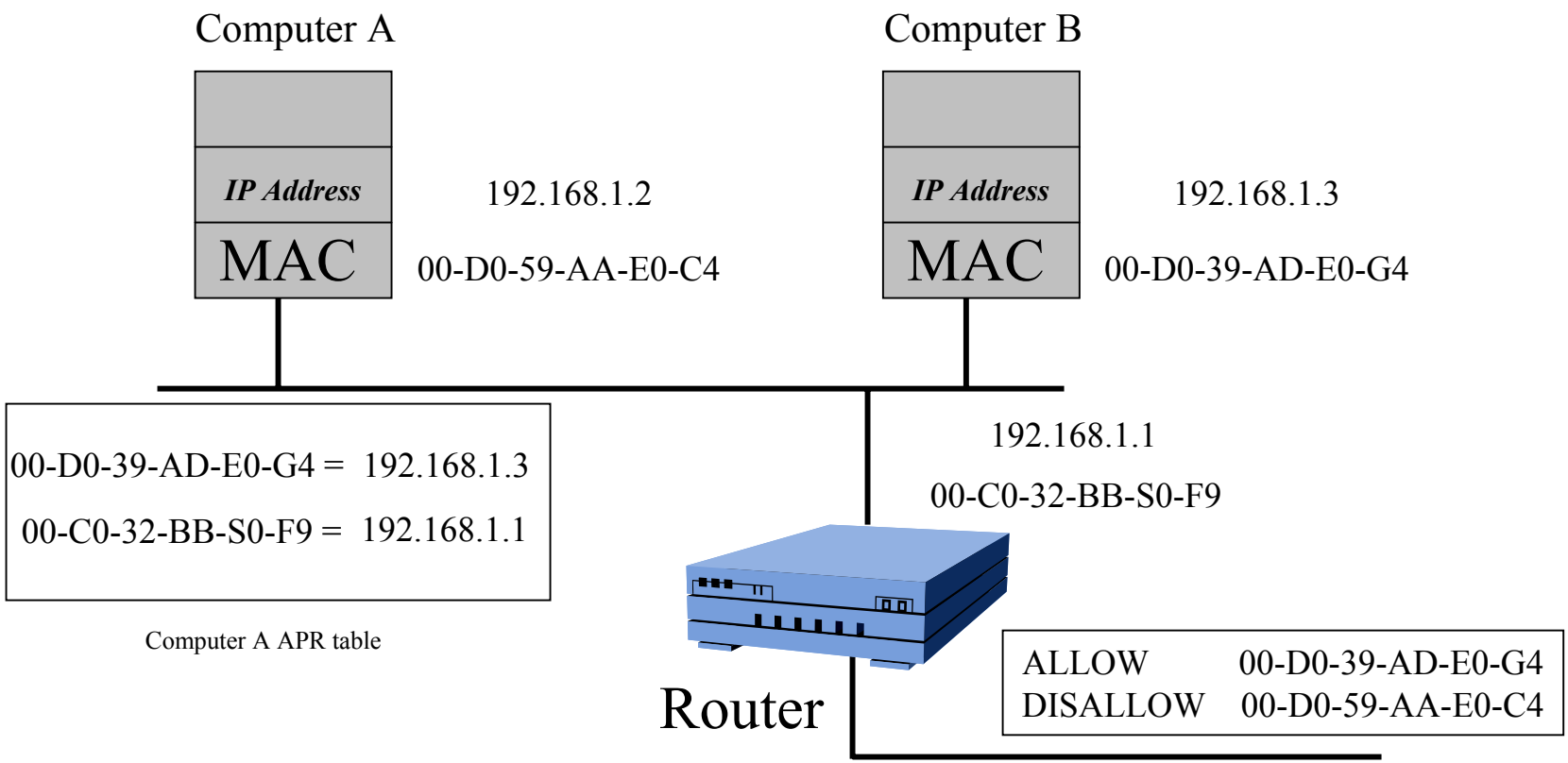
802.11b Security Issues



MAC	SSID	Name
00601DF0E...	LUcentgs	
00045ADA...	linksys	
00022D1B7...	JPB Office	
0004E20EB...	WLAN	
004096409...	1201penn	
00022D1B7...	Davidson and Company	
0090D100C...	WLAN	
0002A56F0...	WaveLAN Network	
00022D408...	IBB	
00045A270...	linksys	
0030AB064...	Wireless	
000124F0C...	SpeedStream	
0030651E3...	Apple Network 1e36e7	
0030651E5...	KENNEDY:MAILROOM	
00306503A...	KENNEDY:SR-320	
00045ACE6...	CQWLAN	
00409655F...	NGAradio	
004096551...	sbvrfnet2	
004096544...	sbvrfnet2	
0030AB121...	mvopnet1	
0030AB128...	mvopnet2	
0030AB128...	mvopnet3	

802.11b Security Issues

Access Control at the MAC (Media Access Control)



802.11b Security Issues

- Access Control at the MAC (Media Access Control)
- Most administrators feel that MAC layer filtering provides adequate security by allowing clients with non-restricted MAC addresses to connect to the wireless network.
  - MAC addresses are passed in the clear
  - MAC addresses can easily be changed:
    - Linux with an “Ifconfig” command
    - Windows via a Registry edit or changing setting within the “Network Connections” utility for the specific interface
    - Configuration utility that comes with some wireless cards
    - Free software found on the Internet

802.11b Security Issues

DISCOVER the POSSIBILITIES

Wired Equivalent Privacy (WEP)

- WEP gives administrators a false sense of security.
- Even when WEP is properly configured and deployed on a wireless network, it is still a trivial matter to break the encryption and gain access to the AP.
  - WEP keys are static and configured manually (Not a scaleable solution)
  - WEP requires the same secret key be shared by all wireless users within the cell
  - Free software on the Internet is available that is used to crack the encryption.
    - *http://sourceforge.net/projects/airsnort/*

      or
    - http://airsnort.shmoo.com/
    - *http://www.dachb0den.com/projects/bsd-airtools.html*

802.11b Security Issues

DISCOVER the POSSIBILITIES

User Network Access Controls

- One area that is commonly overlooked is the ability to regulate internal network access.
  - Most users have varying levels of access to internal resources.
  - All wireless users could potentially be entering the network by the same wireless AP.

802.11b Security Issues

Access Point (AP)

- Placing an AP on the inside of your network will extend its access past any physical barriers or controls.
  - AP are small and only take a few minutes to connect to your internal network
  - The level of sophistication needed to install an AP is low

802.11b Security Issues

DISCOVER the POSSIBILITIES

Denial of Service

- A user with malicious intent could configure a client to bombard the AP with thousands of connection requests eventually leading to the complete shutdown of the targeted AP.
- RF noise generation – Arc Welder – homemade jamming device
- Eventual saturation of RF devices – Bluetooth, 802.11b and g devices, etc.

Countermeasures

Countermeasures

Antenna Signal – Countermeasures

- Proper selection of Antenna – Parabolic, etc.
- Attenuate the signal by reducing transmitter power if possible
- Ground interior walls (If metal construction)
- Thermally Insulate exterior glass using metallic window treatments
- Smart positioning of AP's
- Lining closets housing the AP with aluminum foil
- Use of metallic paints – Extreme

Countermeasures

SSID - Countermeasures

- Turn off SSID broadcasting at the AP if possible (Not all AP vendors allow this)
- Understand that SSID's provide "Zero" security
- Avoid using a SSID that gives away information about your network. ("TaxNet1" or "Kennedy:Mailroom")

Countermeasures

MAC ACL – Countermeasures

- Do not depend on MAC layer filtering as your only security solution for providing secure AP access
- Use Intrusion Detection Servers IDS to alert you when an excessive number of unsolicited ARP replies are detected on the network
- Use the tool, “arpwatch” HTTP://www-nrg.ee.lbl.gov- This tool will provide E-mail notification when IP to MAC bindings change.

Countermeasures

WEP - Countermeasures

- Proprietary solutions offered by certain vendors are all incorporating dynamic key management into their products. (Cisco, Enterasys, AVAYA, etc.) Be careful not to commit yourself to a single vendor specific solution.
- Use IPSec VPN software
- EAP/802.1X Extensible Authentication Protocol (EAP) to provide centralized authentication – (RADIUS, etc.) and dynamic key distribution

Countermeasures

User Access Control - Countermeasure

- Use multiple AP's to access different segments of the network each with a unique SSID's.
- Use a third party VPN solution to connect the users to the appropriate network segment.
  - This solution can be used through a single AP for all users. Each user would be routed internally to the appropriate VPN endpoint within the corporate network.

Countermeasures

Access Point (AP)

- Update your corporate policy to prohibit the installation an AP without the approval of internal security or the IT department
- Always place AP's outside a firewall, inside a DMZ, or within a sandbox network.
- Disable unused ports on the internal switches until needed. (Especially in conference rooms.)
- Monitor any new MAC address's on the internal network that are discovered – "ArpWatch"

Countermeasures

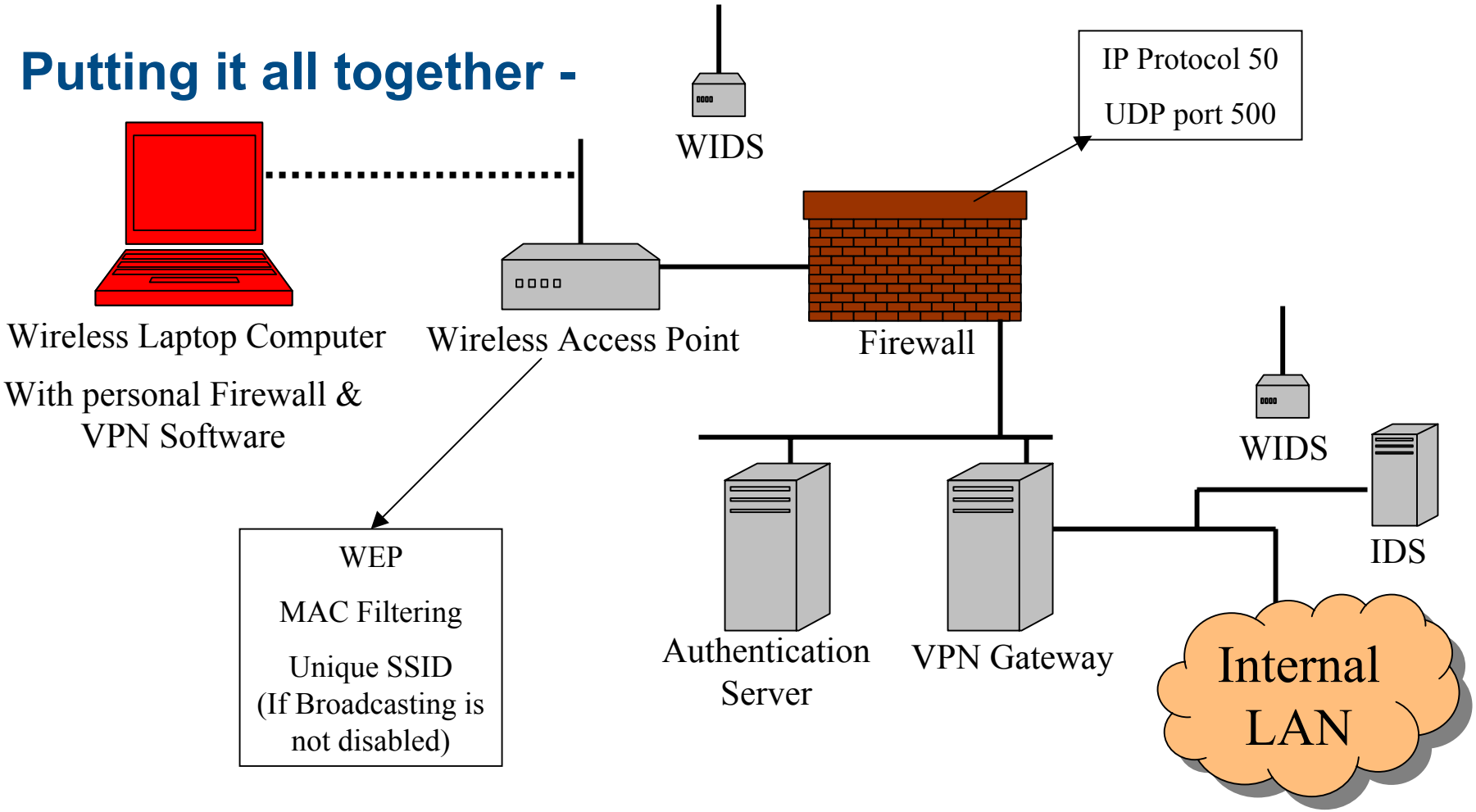
DOS

Shield the perimeter of your building

- **This will help in two ways:**
  - **Help contain your wireless signal within a defined perimeter**
  - **Reduce the risk of outside RF interference**

Countermeasures

Putting it all together -



Hacking Wireless

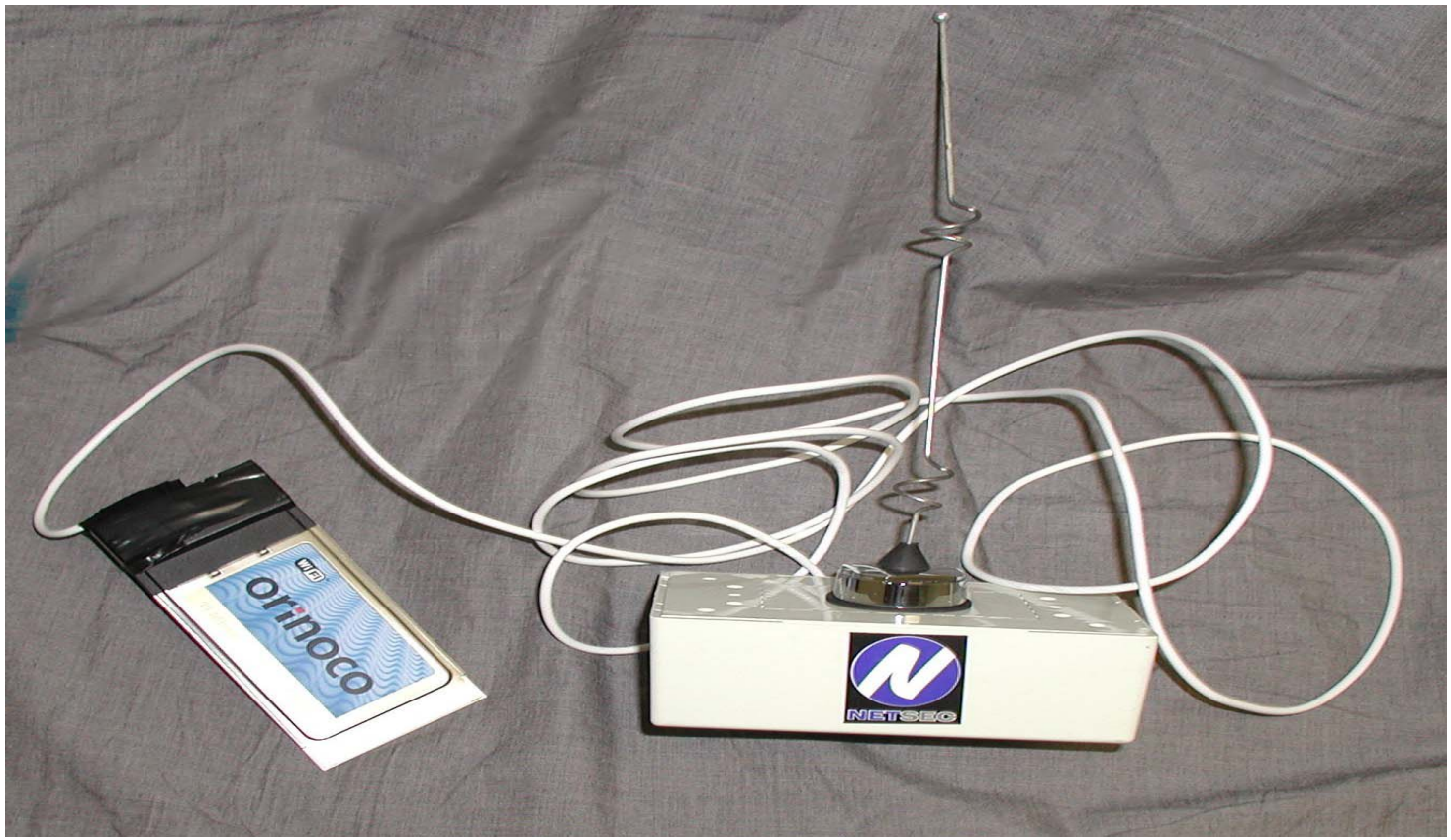
DISCOVER the POSSIBILITIES

Tools of the Trade

Hacking Wireless - Tools

DISCOVER the POSSIBILITIES

Wireless Card and Antenna



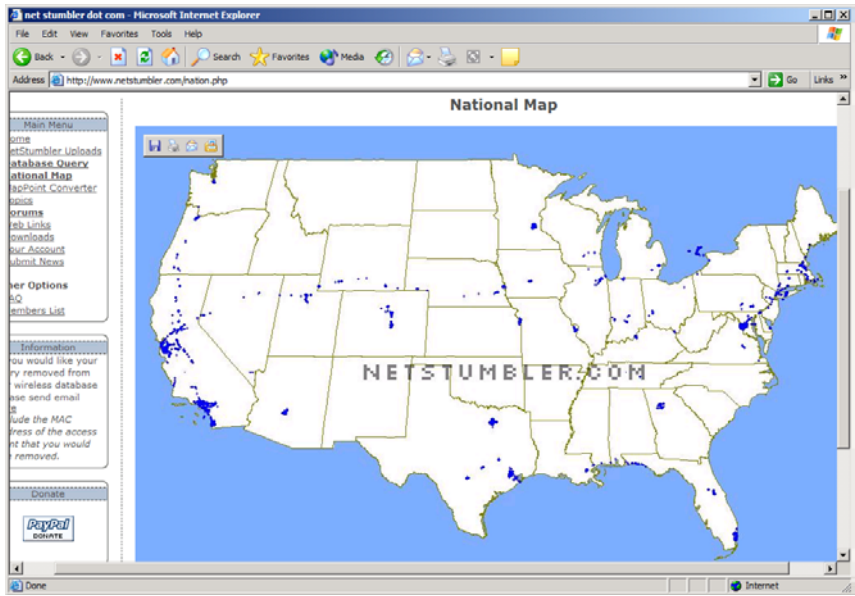
Hacking Wireless - Tools

DISCOVER the POSSIBILITIES

War-Driving Rig – Laptop, wireless card and Antenna

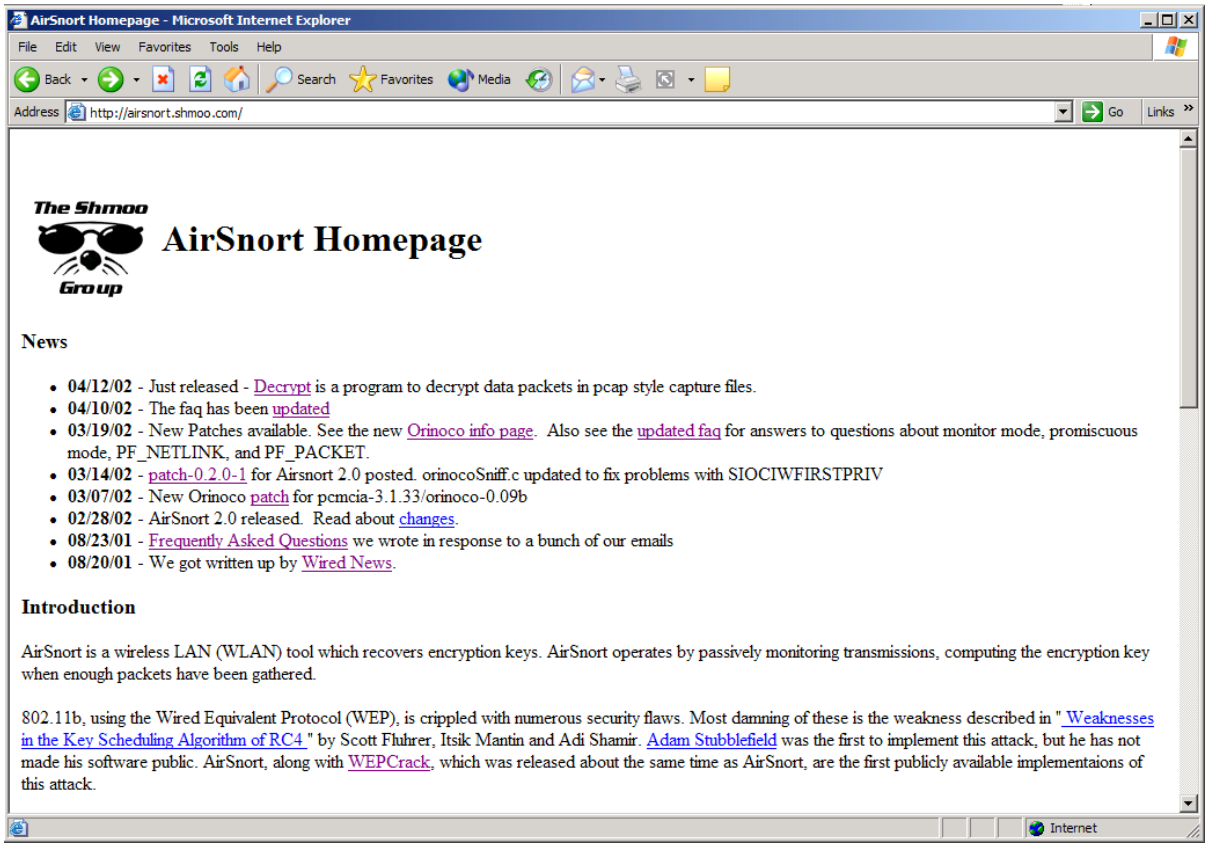
Hacking Wireless - Tools

War-Driving Software – Netstumbler – (Identifies: SSID, signal strength, AP manufacture, GPS coordinates, etc.)



Hacking Wireless - Tools

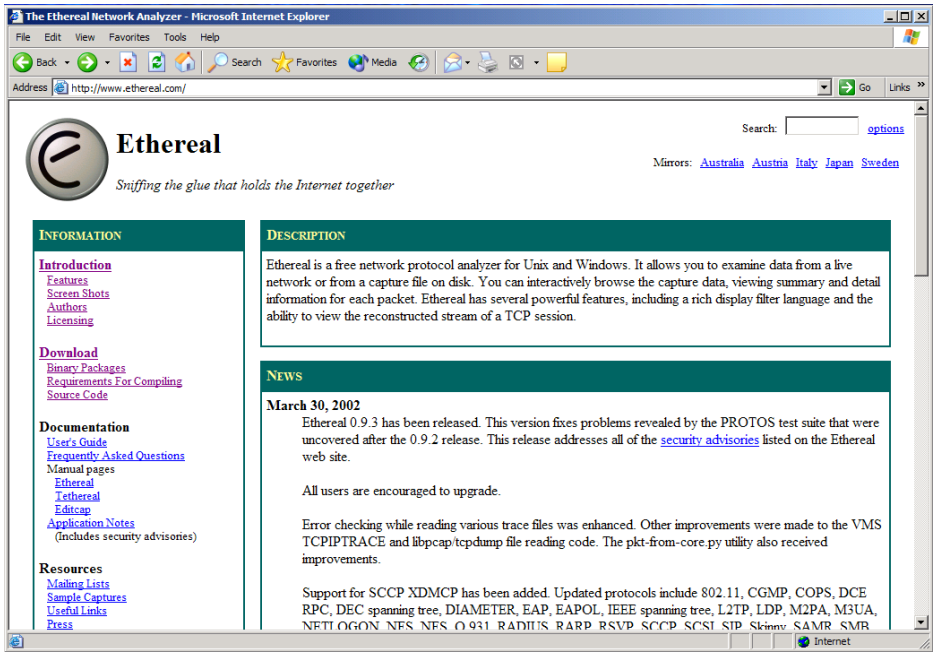
War-Driving Software – AirSnort – (Use to crack WEP encryption)

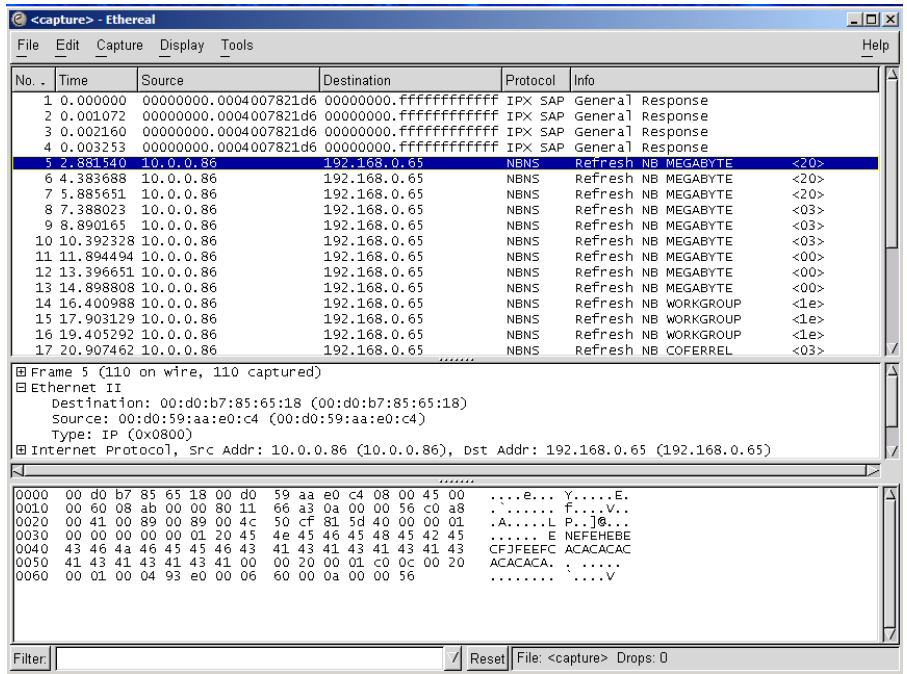


Hacking Wireless – Additional Tools

DISCOVER the POSSIBILITIES

Sniffing Software – Ethereal – "*Sniffing the glue that holds the Internet together.*"

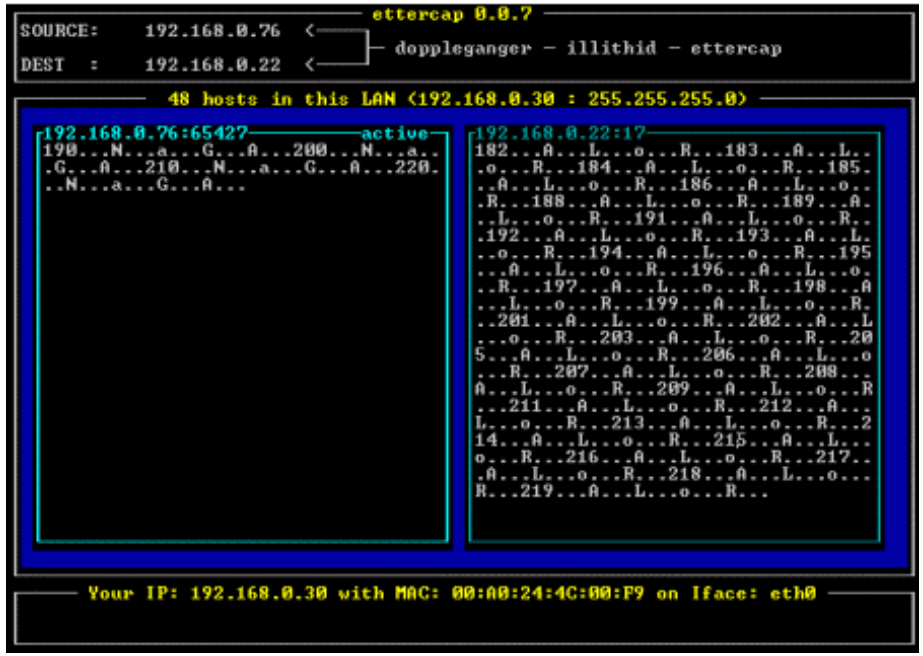




Hacking Wireless – Additional Tools

DISCOVER the POSSIBILITIES

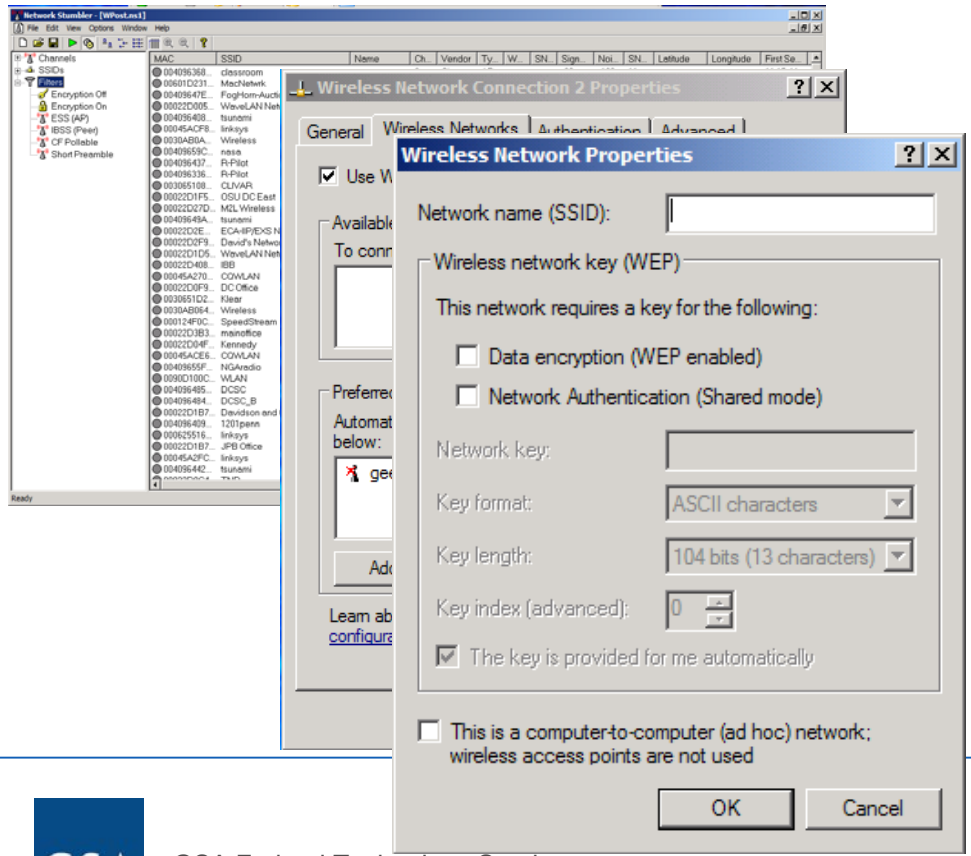
Ettercap – *HTTP://ettercap.sourceforge.net* – Used in ARP Cache Poisoning, Man-in-the-Middle attacks

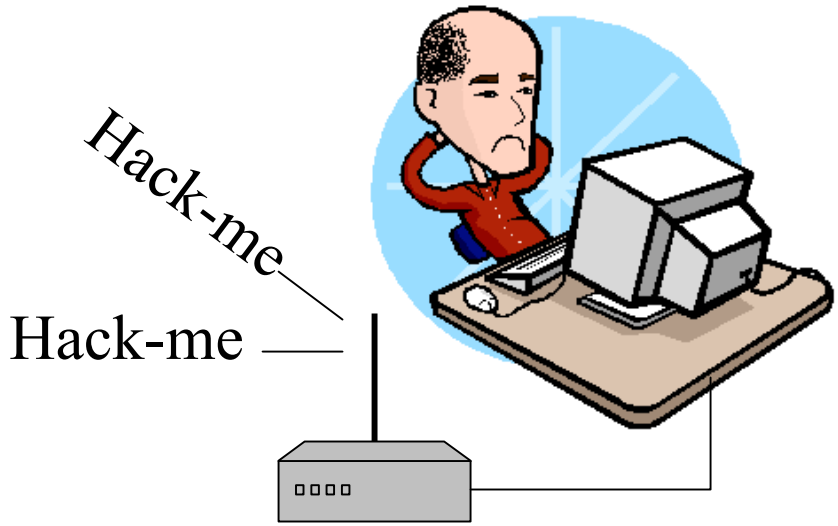


The Attacks

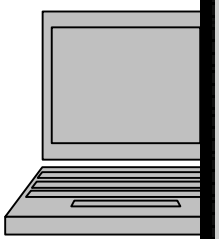
Hacking Wireless – The Attacks

DISCOVER the POSSIBILITIES





Hacking Wireless – The Attacks



Wireless Ha

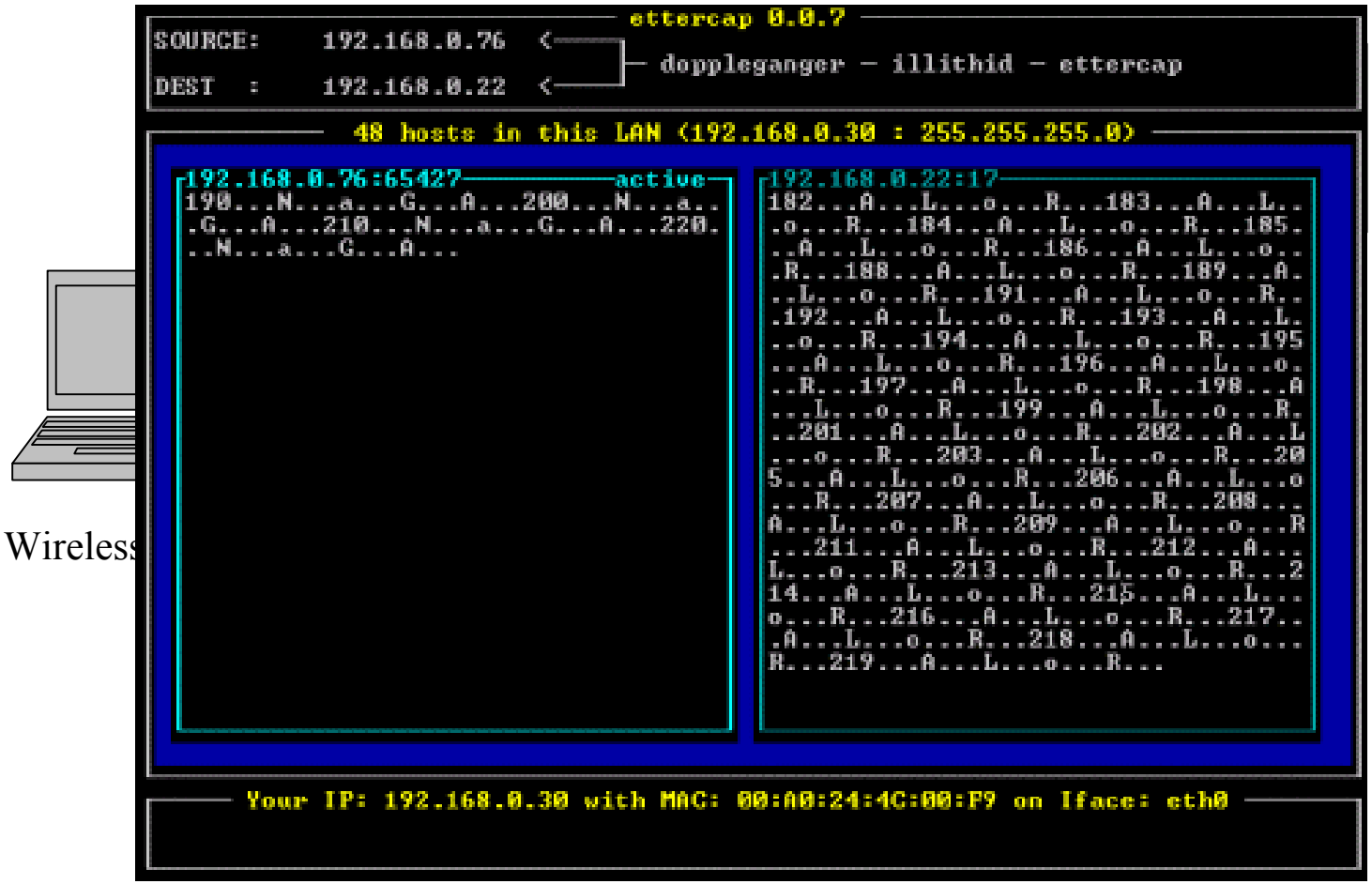
```
ettercap 0.0.7

48 hosts in this LAN (192.168.0.30 : 255.255.255.0)

  1)     192.168.0.76          1)     192.168.0.76
  2)     192.168.0.22          2)     192.168.0.22
  3)   192.168.0.205          3)   192.168.0.205
  4)   192.168.0.123          4)   192.168.0.123
  5)    192.168.0.89          5)    192.168.0.89
  6)   192.168.0.235          6)   192.168.0.235
  7)   192.168.0.194          7)   192.168.0.194
  8)    192.168.0.90          8)    192.168.0.90
  9)   192.168.0.199          9)   192.168.0.199
 10)   192.168.0.183         10)   192.168.0.183
 11)    192.168.0.98         11)    192.168.0.98
 12)   192.168.0.191         12)   192.168.0.191
 13)   192.168.0.135         13)   192.168.0.135
 14)   192.168.0.214         14)   192.168.0.214
 15)   192.168.0.191         15)   192.168.0.191
 16)   192.168.0.232         16)   192.168.0.232
 17)    192.168.0.46         17)    192.168.0.46
 18)    192.168.0.18         18)    192.168.0.18
 19)   192.168.0.128         19)   192.168.0.128
 20)   192.168.0.190         20)   192.168.0.190
 21)   192.168.0.103         21)   192.168.0.103
 22)    192.168.0.68         22)    192.168.0.68
 23)    192.168.0.19         23)    192.168.0.19
 24)   192.168.0.222         24)   192.168.0.222
 25)   192.168.0.210         25)   192.168.0.210
 26)    192.168.0.63         26)    192.168.0.63
 27)    192.168.0.21         27)    192.168.0.21

Your IP: 192.168.0.30 with MAC: 00:A0:24:4C:00:F9 on Iface: eth0
Host: Unknown host (192.168.0.76) : 19:00:00:00:4C:26
```

Hacking Wireless – The Attacks



Wireless

Hacking Wireless – The Attacks

ARP Cache Attacks can also be launched against:

- **Wireless Clients connected to the AP**
- **Wireless Clients and Wired Clients**
- **Wireless Home Users (Couch Networks)**
- **And may other combinations**

DISCOVER the POSSIBILITIES

Solutions

Solutions

Holistic Approach

- Prevention
- Identification
- Response

Solutions

DISCOVER the POSSIBILITIES

Prevention

- Create a completely separate wireless security policy
- Do a complete Site Survey before placement of AP's
- Wireless networks should always be treated as un-trusted and never placed behind corporate firewalls
- Use MAC layer filtering
- Be sure to change the SSID from the default value and disable broadcasting if possible
- Use encryption, even WEP - (Low hanging fruit theory)
- Static IP's vs DHCP
- Use third party software for additional security – Authentication, VPN encryption
- Use personal Firewall software on your wireless clients systems
- Install the latest security patches and firmware updates on you wireless equipment

Solutions

DISCOVER the POSSIBILITIES

Identification

- Deploy Wireless IDS sensors
- Identify your signal range – clients with antennas can pick up you signal further away than without one
- Periodically scan your facility for rouge access points using the same software covered today
- Check your internal logs for strange anomalies concerning MAC addresses

Solutions

Response

- Have an adequate response plan in place to deal with malicious activity
- Have the ability to log activity of a malicious user to aid in prosecution
- The ability to control and reconfigure your AP on the fly

DISCOVER the POSSIBILITIES

Questions?