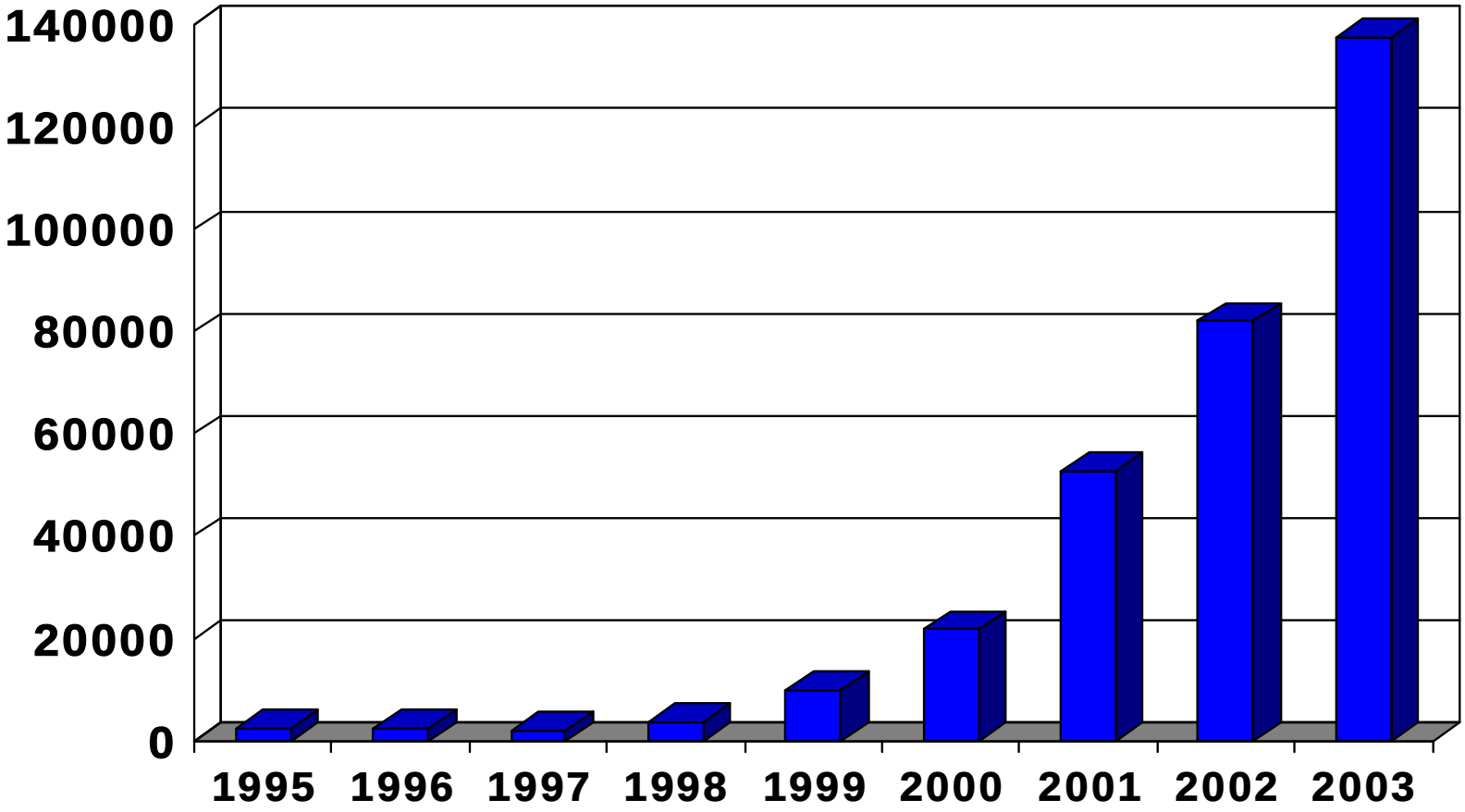
Why Worry about Security?

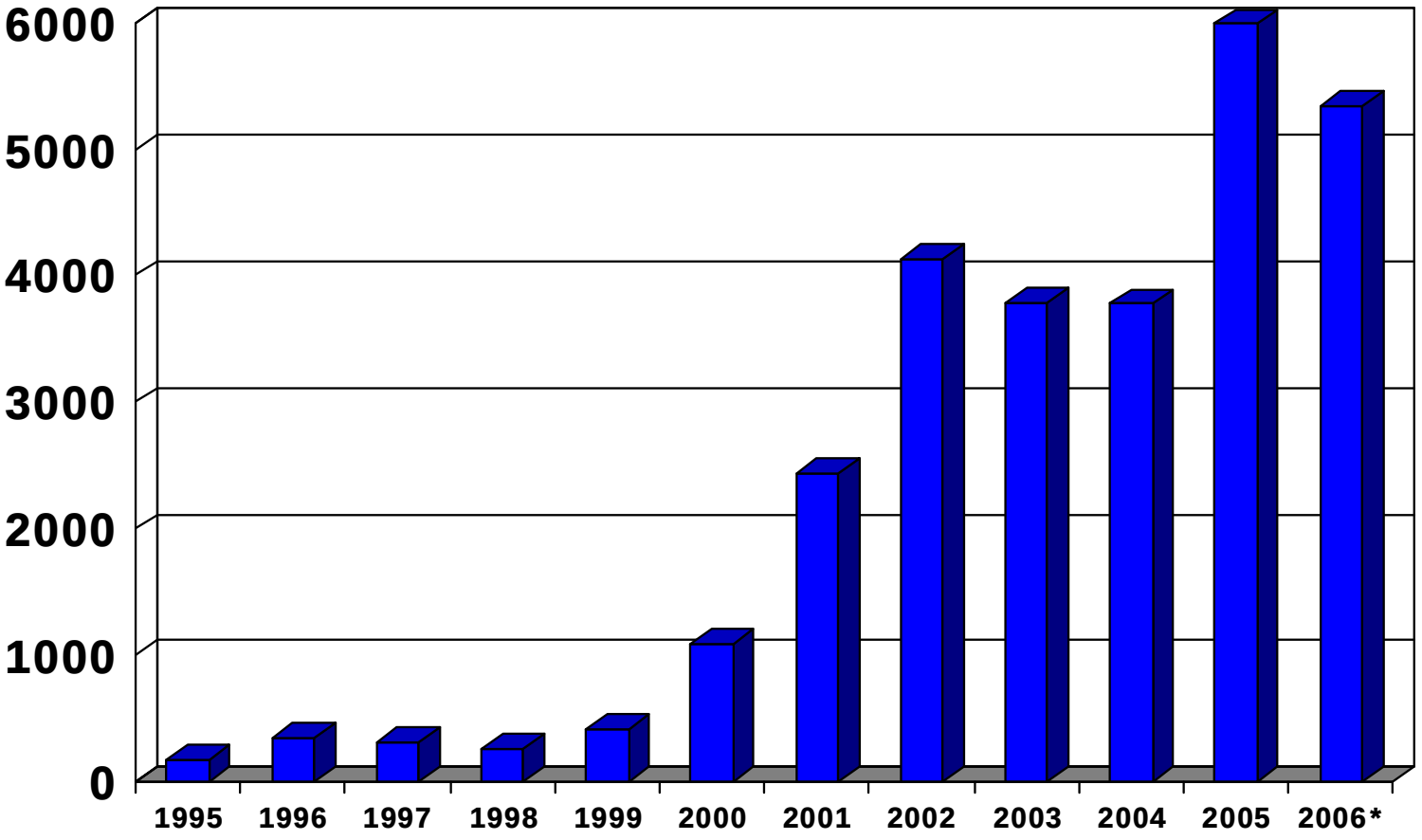
- Y2K Bug – 1/1/2000
- DDoS Attack of Yahoo, CNN – 2/2000
- Microsoft break-in – 10/2000
- SPAM and Phishing
- Viruses and Worms
  - Internet Worm – 11/1988
  - Melissa/ILoveYou Viruses – 1999 - 2000
  - CodeRed/Nimda/Slammer/Sobig – 2001-2003
  - MyDoom,Netsky/Bagel – 2004
  - SPAM/Virus Writer Connection
- Terrorist Attacks - 9/11/2001
- Numerous Web Defacements

Reported Incidents



Source: CERT

Reported Vulnerabilities

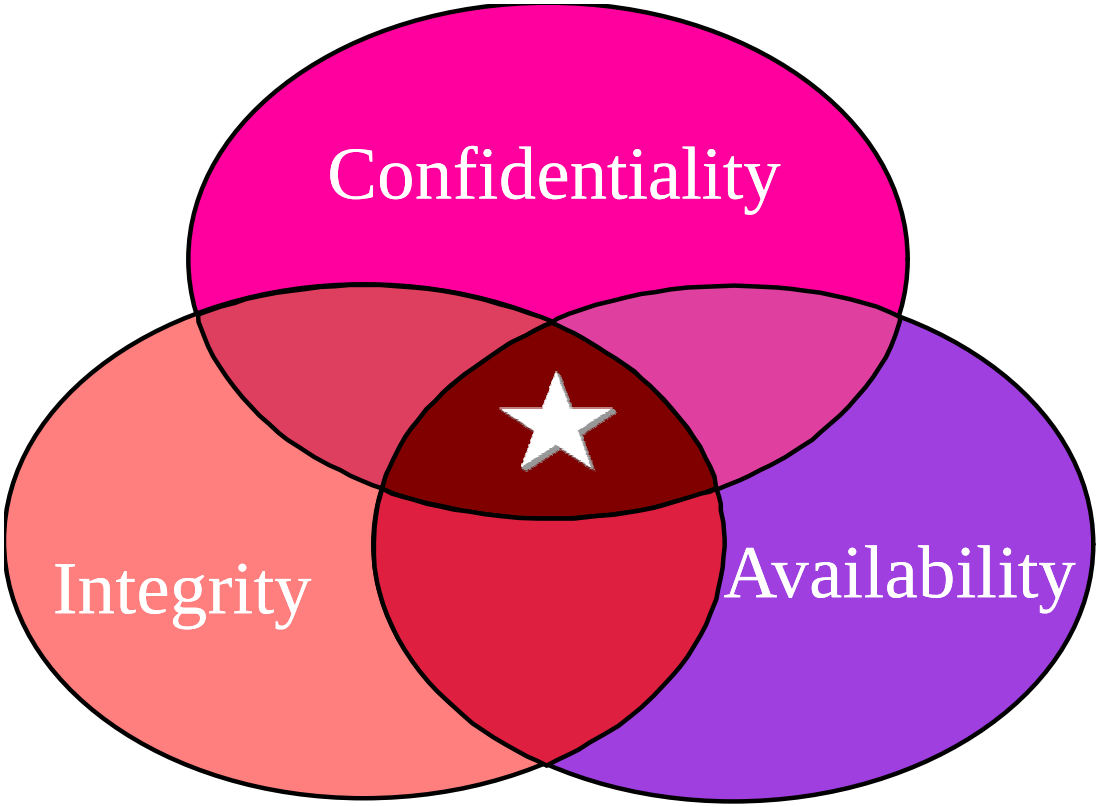


Source: CERT

How much security?

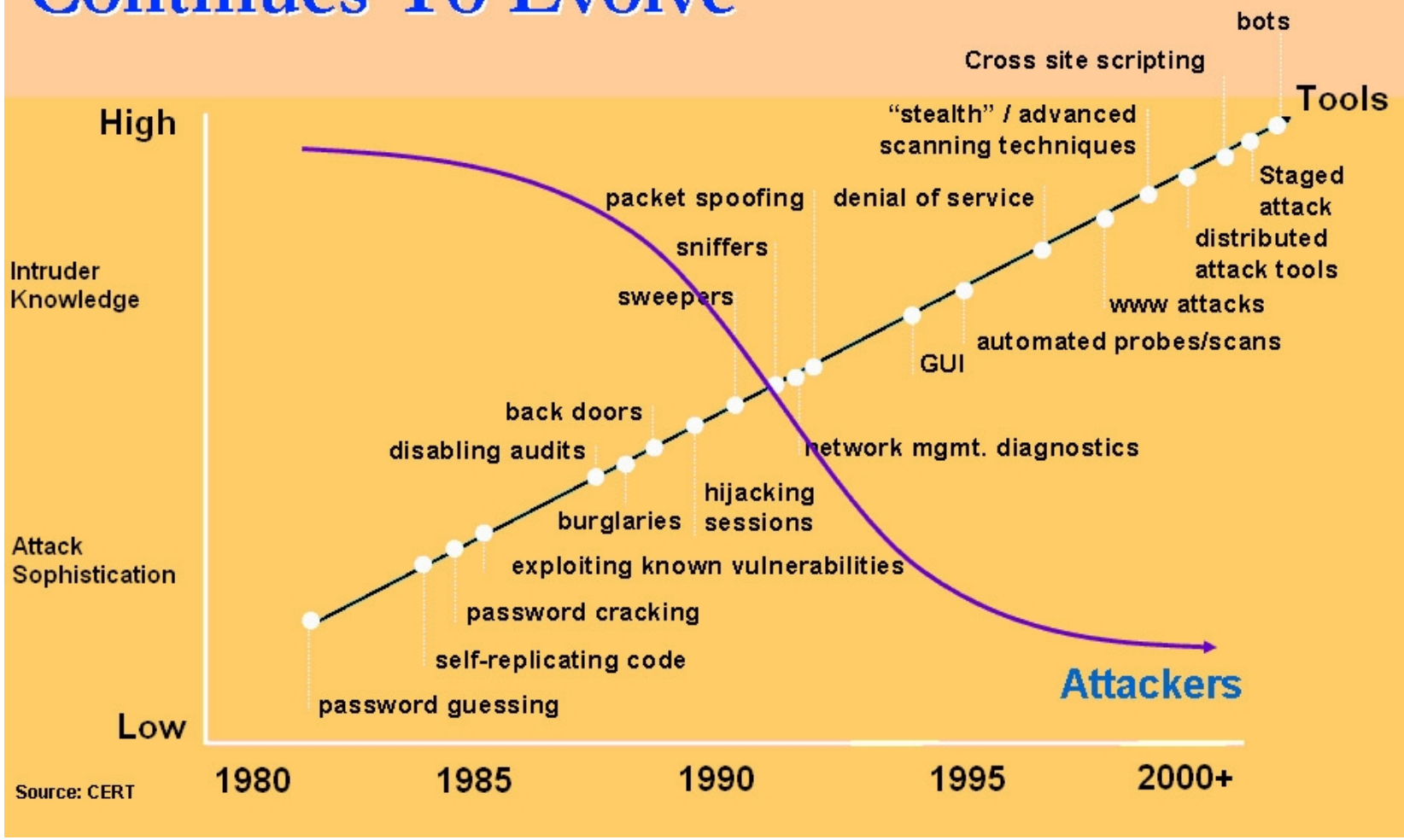
Beware of Security through Obscurity!!!

Goals of Security



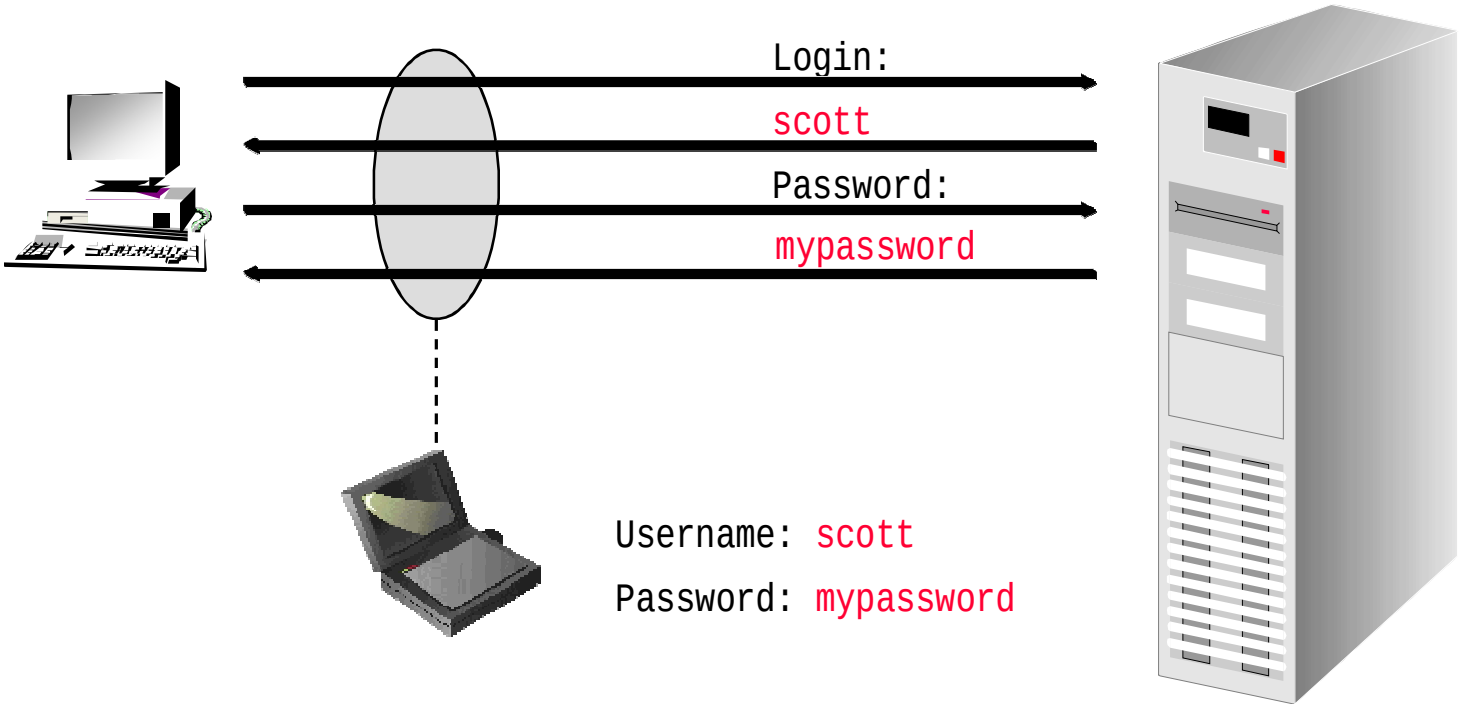
Accountability?

Cyber Attack Sophistication Continues To Evolve



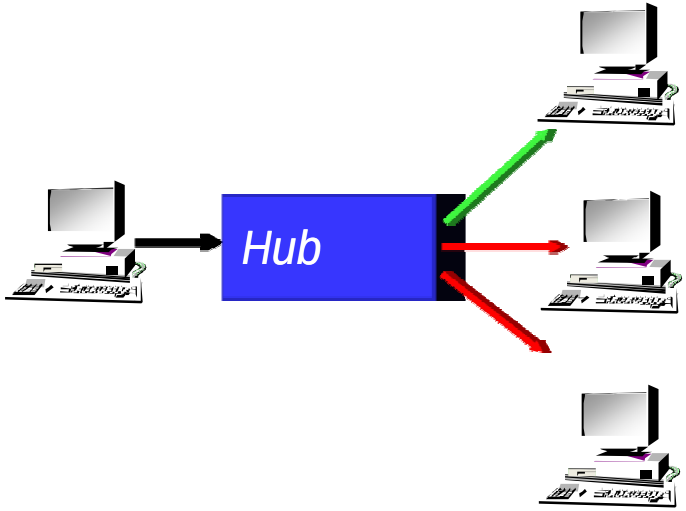
Source: CERT (Phishing Exposed)

Packet Sniffing

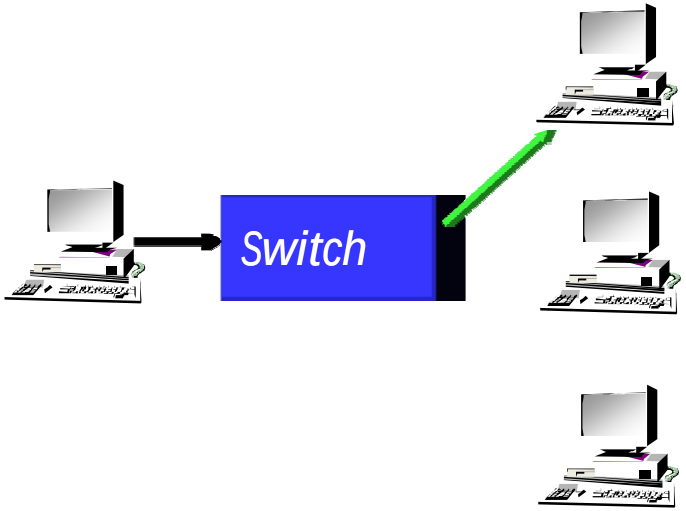


Wireless?!?!?!

Network Hubs vs. Switches



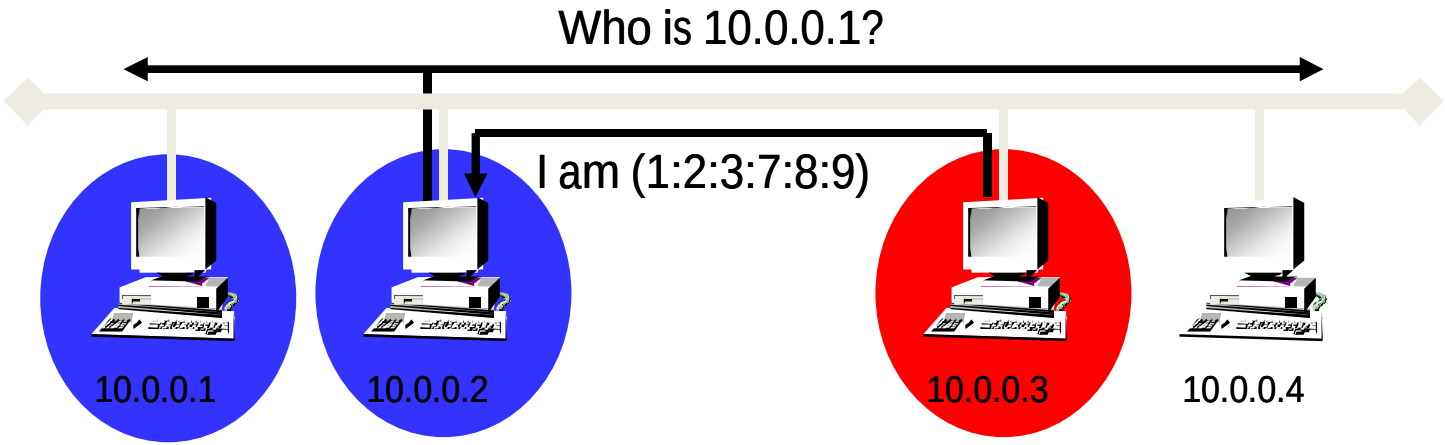
Everyone can see traffic



Virtual circuit between pair

Switch Attacks

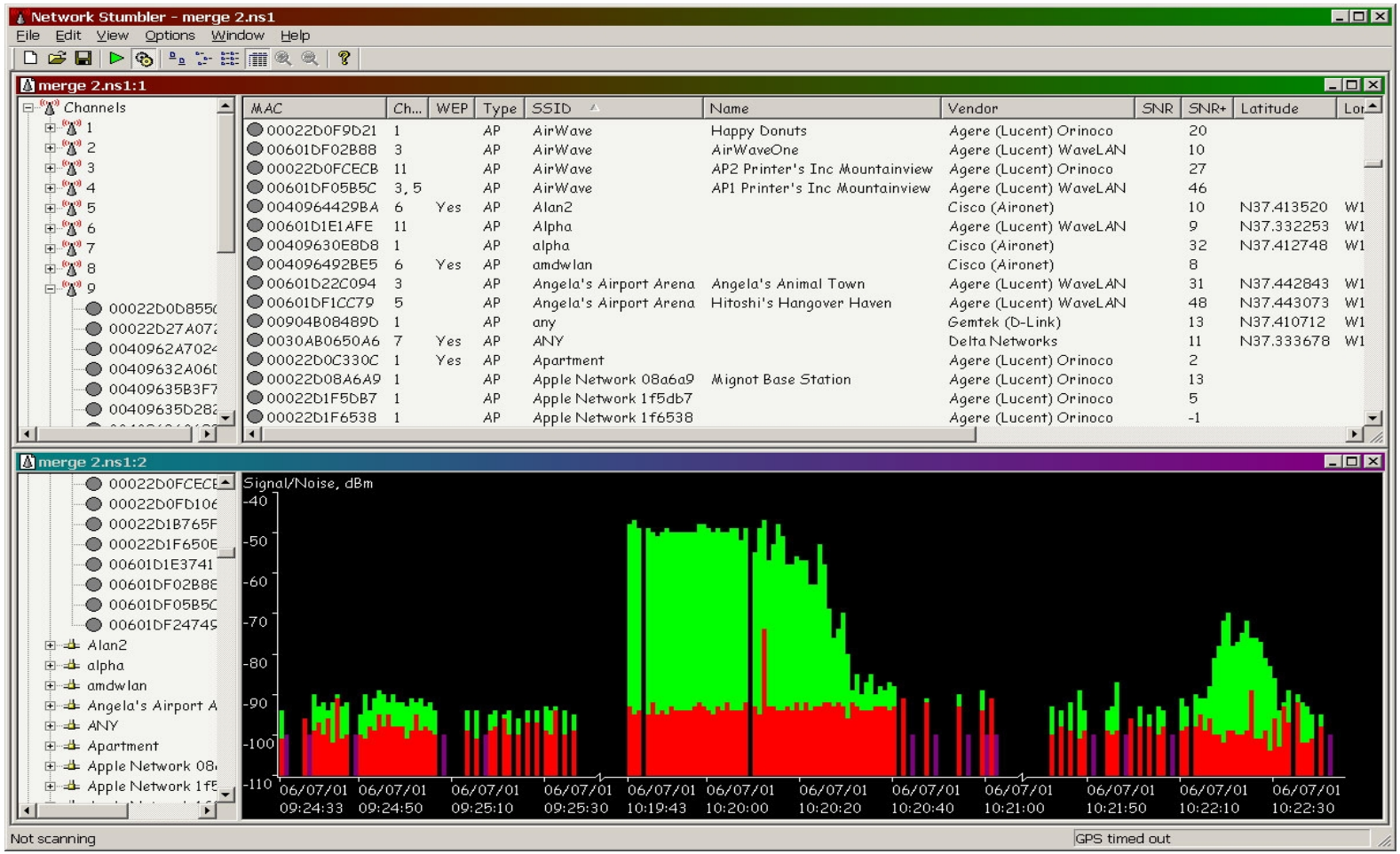
- MAC Flooding – switch will act like hub
- ARP Spoofing



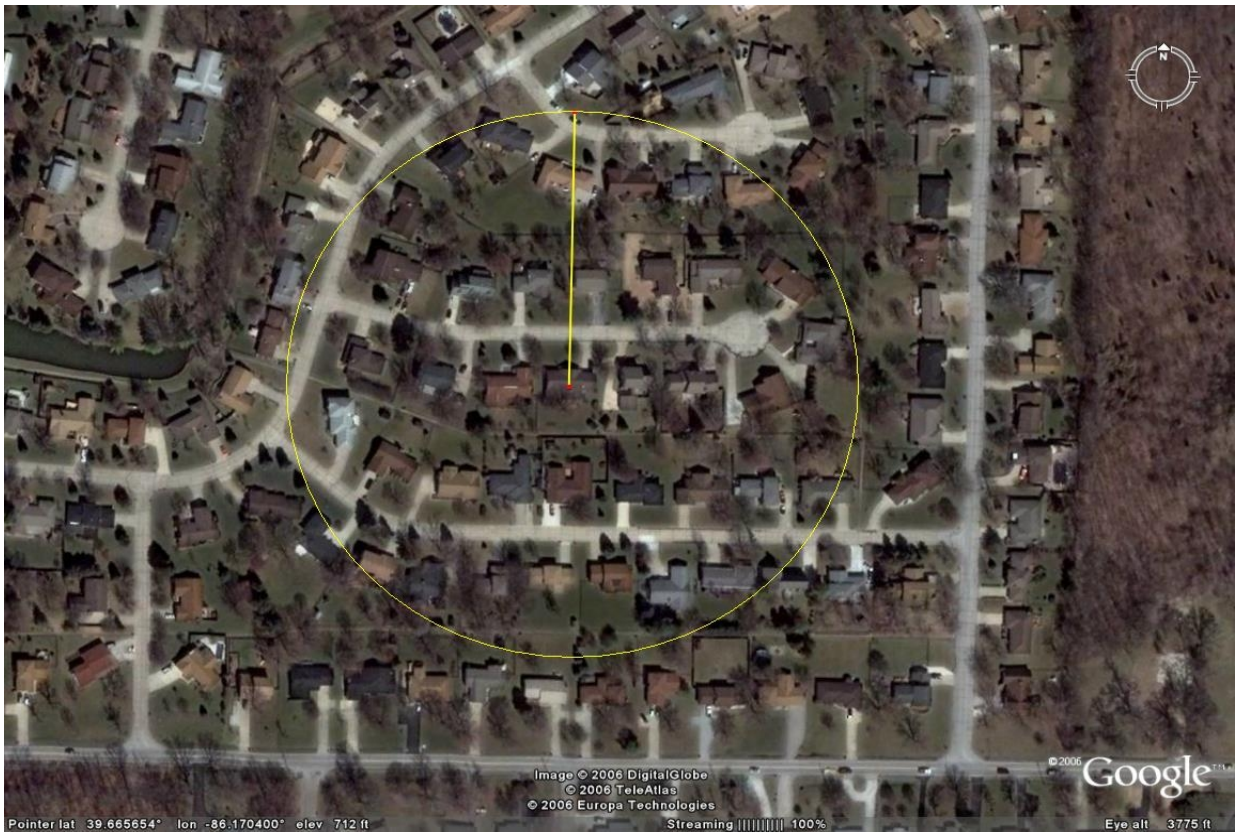
Wireless Networks

- Extend Network Boundaries
- Security Components
  - Service Set Identifier (SSID)
    - Shared secret key
    - SSID Broadcast issues
  - MAC-Based ACL
  - Encryption
    - Wired Equivalent Protocol (WEP) – Weak!!!
    - Wi-Fi Protected Access (WPA)

Wardriving


Network Stumbler - merge 2.ns1
File Edit View Options Window Help
merge 2.ns1:1
Channels
1
2
3
4
5
6
7
8
9
MAC Ch... WEP Type SSID Name Vendor SNR SNR+ Latitude
00022D0F9D21 1 AP AirWave Happy Donuts Agere (Lucent) Orinoco 20
00601DF02B88 3 AP AirWave AirWaveOne Agere (Lucent) WaveLAN 10
00022D0FCECB 11 AP AirWave AP2 Printer's Inc Mountainview Agere (Lucent) Orinoco 27
00601DF05B5C 3, 5 AP AirWave AP1 Printer's Inc Mountainview Agere (Lucent) WaveLAN 46
0040964429BA 6 Yes AP Alan2 Cisco (Aironet) 10 N37.413520 W1
00601D1E1AFE 11 AP Alpha Agere (Lucent) WaveLAN 9 N37.332253 W1
00409630E8D8 1 AP alpha Cisco (Aironet) 32 N37.412748 W1
004096492BE5 6 Yes AP amdwlan Cisco (Aironet) 8
00601D22C094 3 AP Angela's Airport Arena Angela's Animal Town Agere (Lucent) WaveLAN 31 N37.442843 W1
00601DF1CC79 5 AP Angela's Airport Arena Hitoshi's Hangover Haven Agere (Lucent) WaveLAN 48 N37.443073 W1
00904B08489D 1 AP any Gemtek (D-Link) 13 N37.410712 W1
0030AB0650A6 7 Yes AP ANY Delta Networks 11 N37.333678 W1
00022D0C330C 1 Yes AP Apartment Agere (Lucent) Orinoco 2
00022D08A6A9 1 AP Apple Network 08a6a9 Mignot Base Station Agere (Lucent) Orinoco 13
00022D1F5DB7 1 AP Apple Network 1f5db7 Agere (Lucent) Orinoco 5
00022D1F6538 1 AP Apple Network 1f6538 Agere (Lucent) Orinoco -1
merge 2.ns1:2
Alan2
alpha
amdwlan
Angela's Airport A
ANY
Apartment
Signal/Noise, dBm
-40
-50
-60
-70
-80
-90
-100
-110
06/07/01 09:24:33
06/07/01 09:24:50
06/07/01 09:25:10
06/07/01 09:25:30
06/07/01 10:19:43
06/07/01 10:20:00
06/07/01 10:20:20
06/07/01 10:20:40
06/07/01 10:21:00
06/07/01 10:21:50
06/07/01 10:22:10
06/07/01 10:22:30
Not scanning
GPS timed out

High Power Mode



450ft = 40 houses, 4 streets

Low Power Mode

150ft = 6 Houses, 1 street

IP Address Spoofing

- Replace actual source address in IP packets
- Prevent packets from being traced back
- Exploit IP address-based trust relationships

DNS Spoofing

- DNS/ARP Cache Poisoning
- Break in and change trusted machine entry to point to the attackers host address
- Trust-based access to other machines
  - Berkeley *R* Commands
  - Remote File systems (NFS)