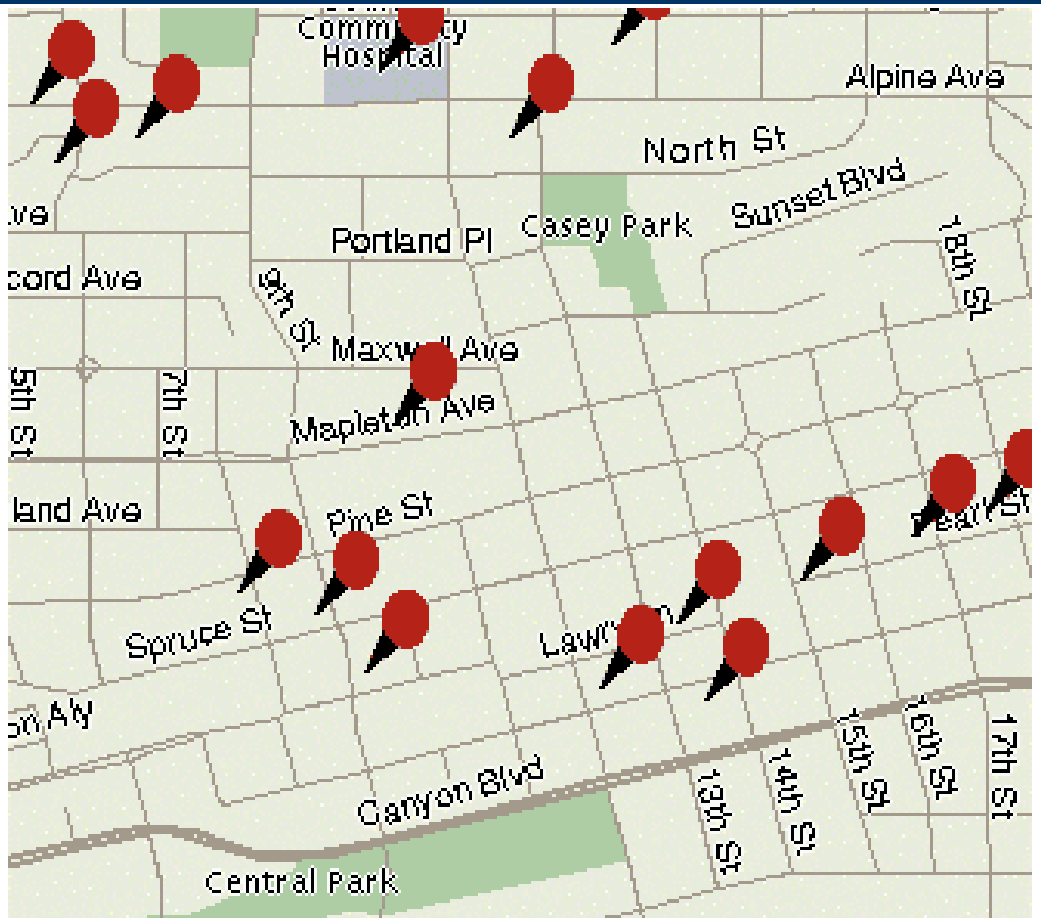
Boulder Labs

Wireless Nets Vulnerable



David Clements

Cyrus Hall

Robert Gray, Ph.D.

Boulder Labs

Outline

- Wireless Nets are pervasive
- Wireless Nets are vulnerable to threats
- Definition of WEP
- Attacks on WEP
- Drive-by results and Tools
- Securing Wireless Nets
- References

Boulder Labs

Wireless Nets are Everywhere

- Walk around the neighborhood - 4 nets in 5min
- Downtown, 50 nets in 4 hours
- 80% - 90% wide open
- $60 - $70 Cards selling like hotcakes
- Access Points - $100 - $150

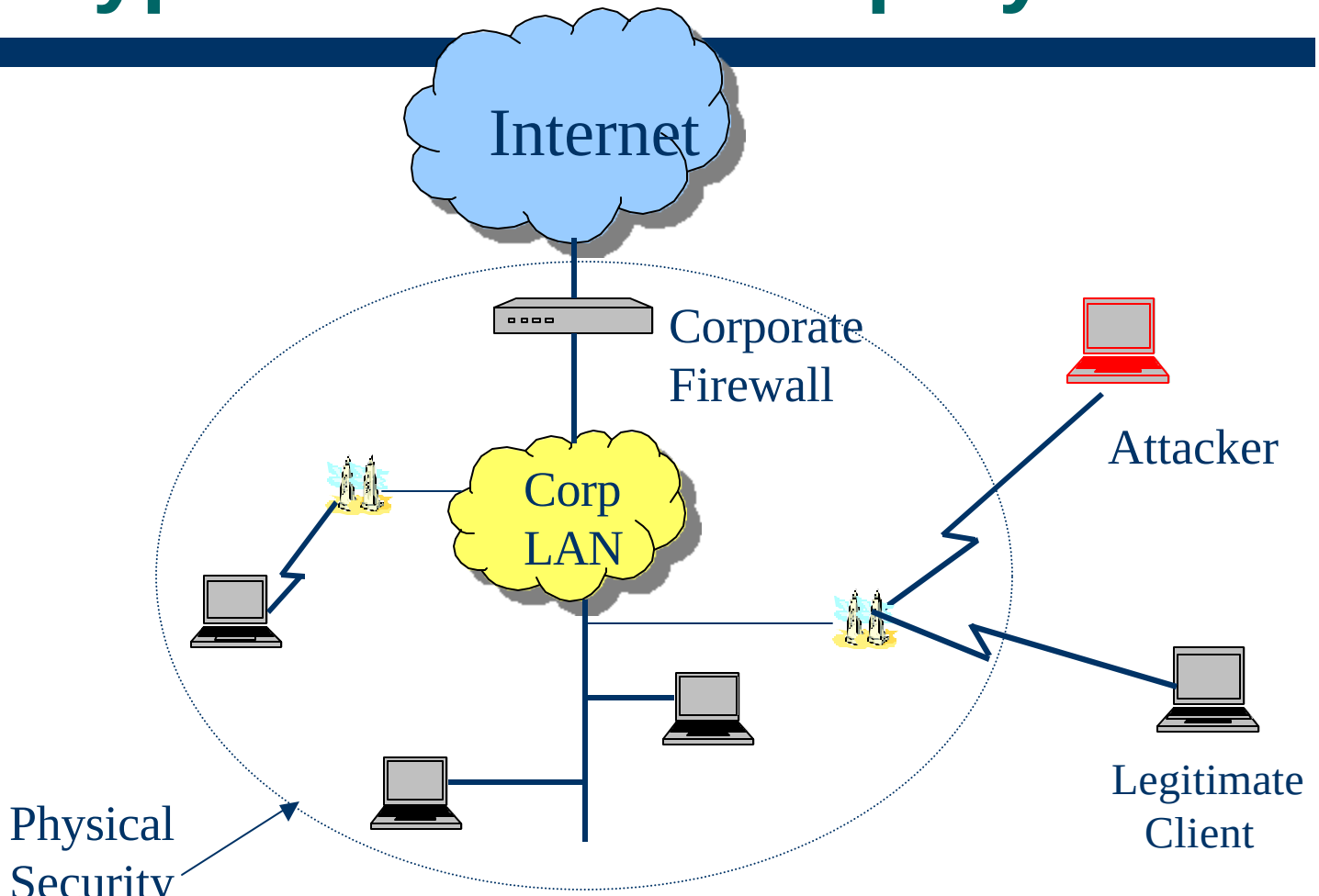
Boulder Labs

Threats

- **Loss of Confidentiality**
  - Competitors
  - Thieves
  - Disruptors
- **Identity Hijack**
  - Bad guys cause trouble on Internet as you
- **Disruption of Company Functionality**
  - Viruses
  - Trojan Horse
  - Data Integrity

Boulder Labs

Typical Wireless Deployment



Boulder Labs

Definitions

- 802.11b (aka. WiFi)
  - 11 Mbits/sec (actually 5 Mbits/sec data throughput)
  - Access Point – gateway to wired network
  - 11 channels
  - 2.4 GHz, 25 MHz per channel
- Active / Passive attacks

Boulder Labs

Wireless Range (802.11b)

- On card antennas: up to hundreds of feet
- Pair of yagi's – 10 miles for line-of-sight
- Type of walls biggest factor affecting range

Boulder Labs

Wired Equivalence Privacy (WEP)

- Yield privacy same as hard wire nets
- For 802.11b, two levels of encryptions:
  - 40-bit key (aka, silver, 64-bit)
  - 104-bit key (aka, gold, 128-bit)
- Encryption based on key and Initialization Vector
- IVs taken from 2^24 range
- IV is transmitted clear; key is not transmitted

Boulder Labs

WEP Security Goals

- Confidentiality – prevent eavesdropping
- Access control – who can use the net
- Data integrity – can packets be altered?

Boulder Labs

WEP's Crypto Mistakes

- WEP uses CRC for integrity
  - Need to use Message Digests for integrity
- WEP reuses cipher streams
  - Never reuse a cipher stream
- WEP uses partial key space
  - Use all available bits

Boulder Labs

General Encryption

Plaintext	Hello World	1011000100111
Keystream		1000000010001
Cypherstream		0011111111110

Boulder Labs

802.11b WEP Encryption

- Give everyone in a group the same key
- For every packet to be transmitted, choose IV
- IVs are integers from 0 to 2^24
- cypherstream ← RC4(IV • key)
- cyphertext ← plaintext ⊕ cypherstream
- Transmitted packet ← Hdr • IV • cyphertext

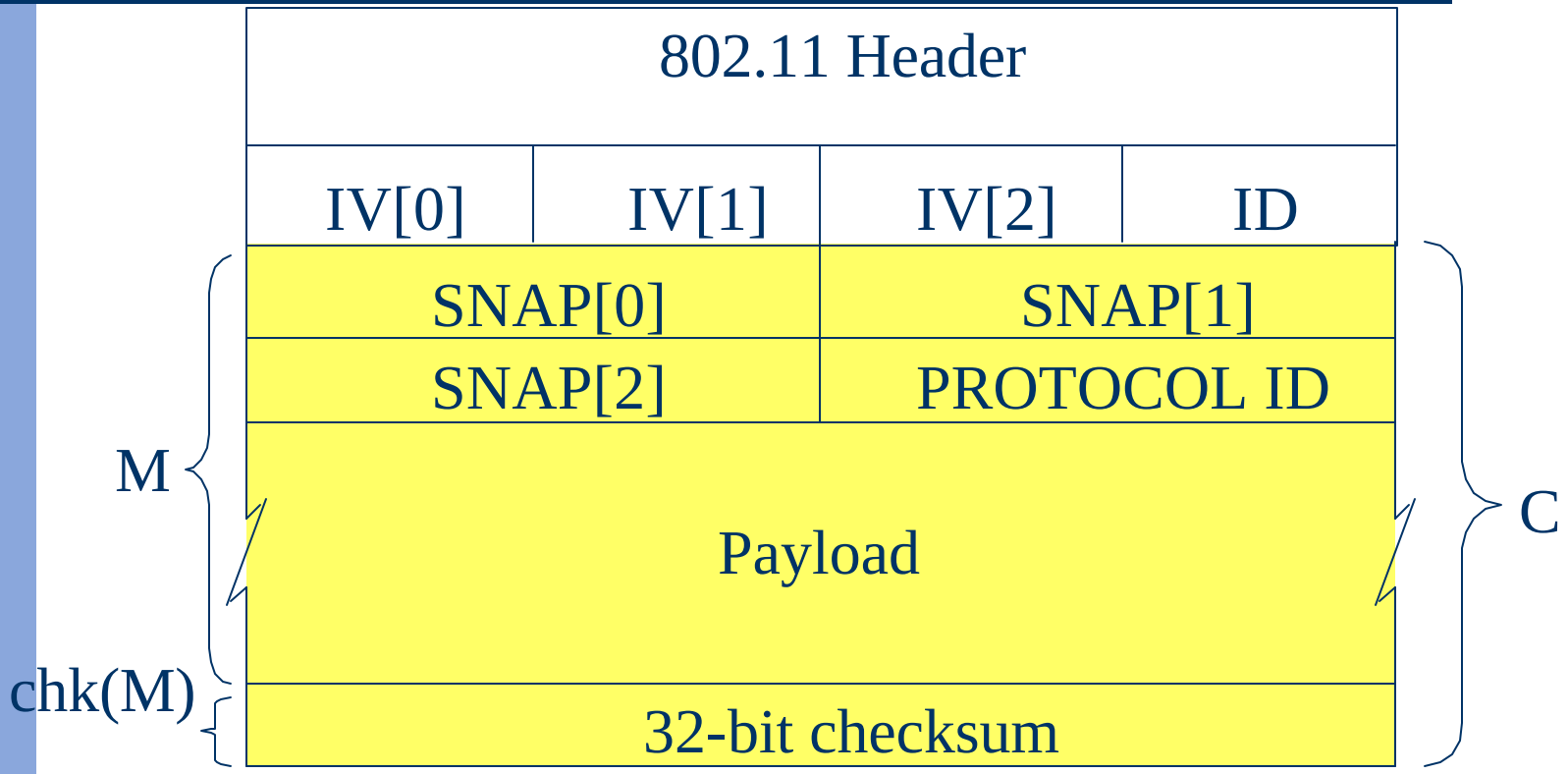
Boulder Labs

Key Generation

- 104 bits: 11001010001010000100101010111…
- Hex: 0x 1234567890123ABCDEF0123456
- Key generator
  - Passphrase: boobar129$$Z
  - Yields 104 bits, Ie. MD5, etc

Boulder Labs

WEP Encrypted Packet



$$C = (M \bullet chk(M) \oplus RC4(IVi \bullet key)$$

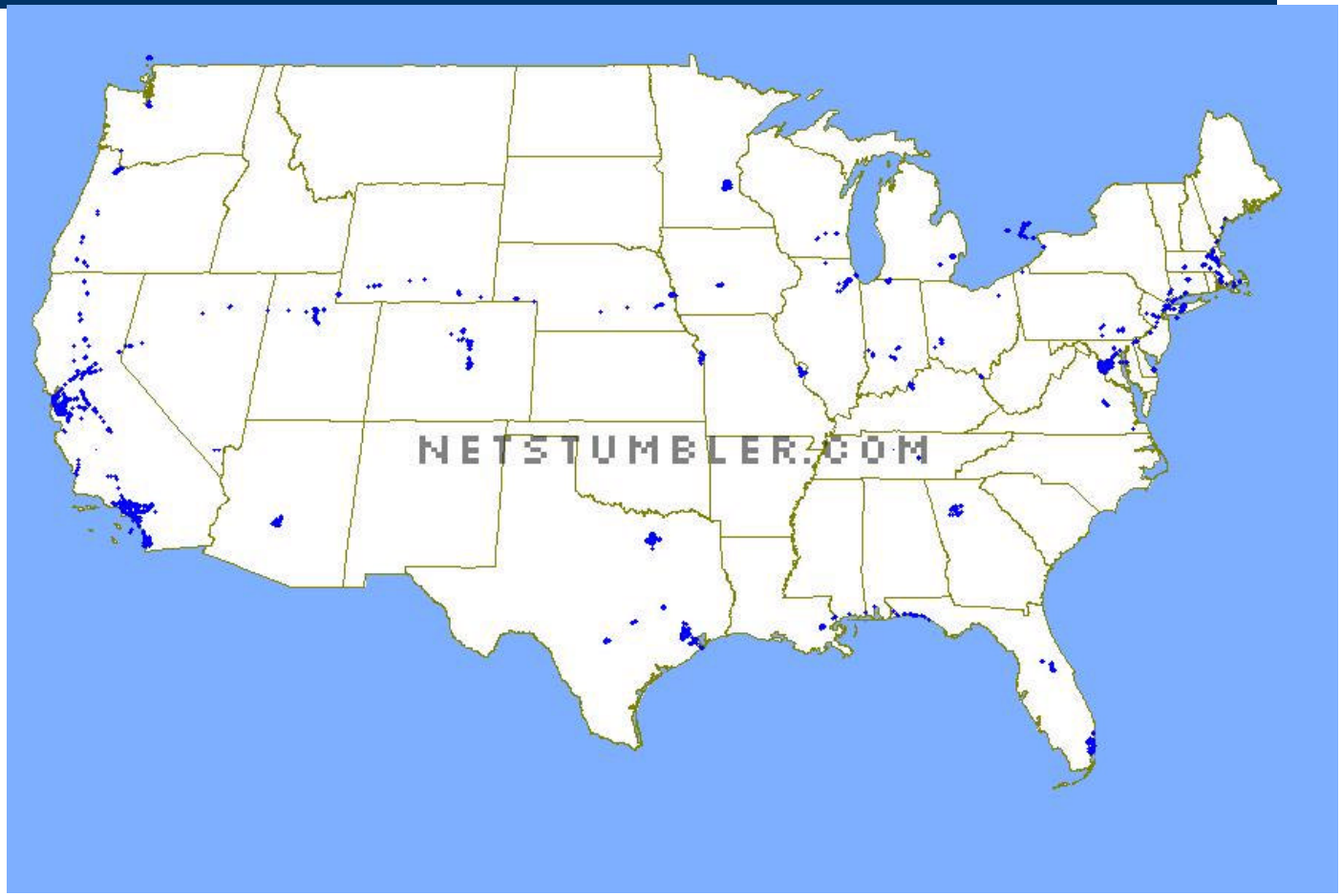
Boulder Labs

Attacks on WEP

- Exhaustive search of 2^21 (30 seconds)
- Exhaustive search of 2^40 (45 days)
- Dictionary attack - 1M words per minute
- Weak IVs (2hrs for 40bit; 8 hours for 104 bit)
- IV tables
- Packet Altering

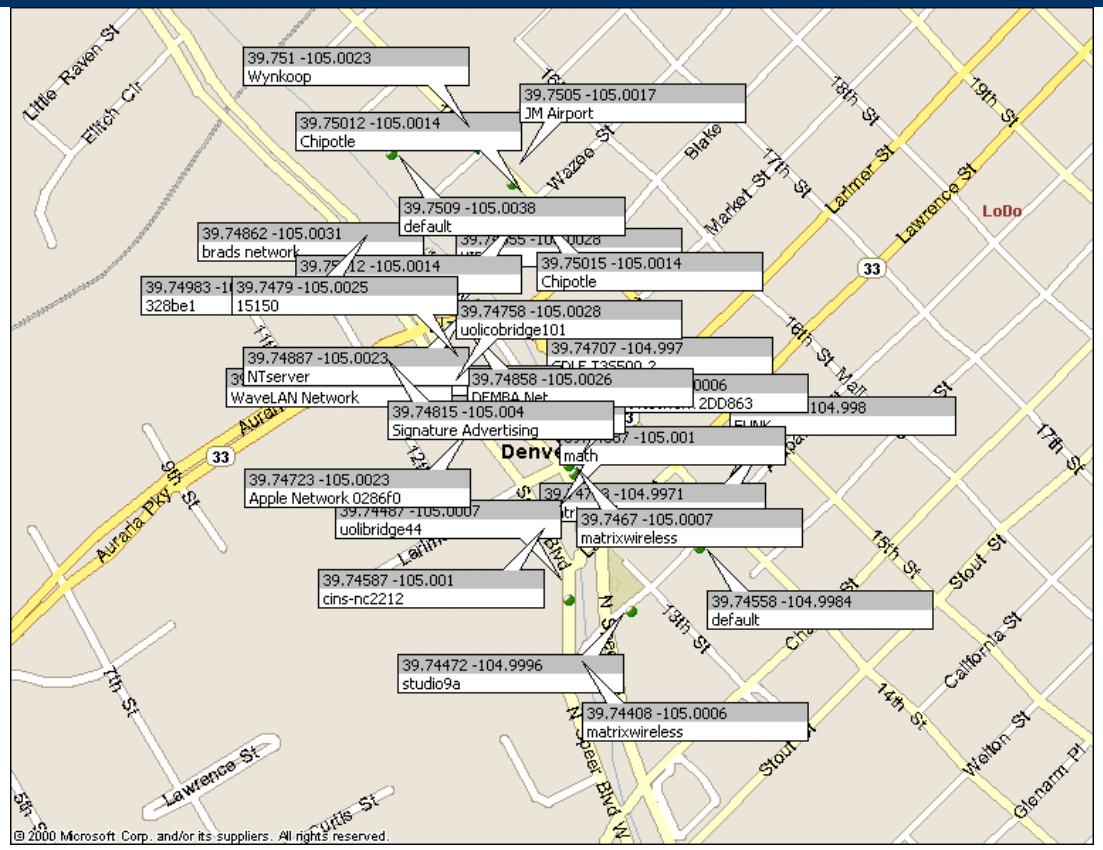
Boulder Labs

Wardriving (USA)



Boulder Labs

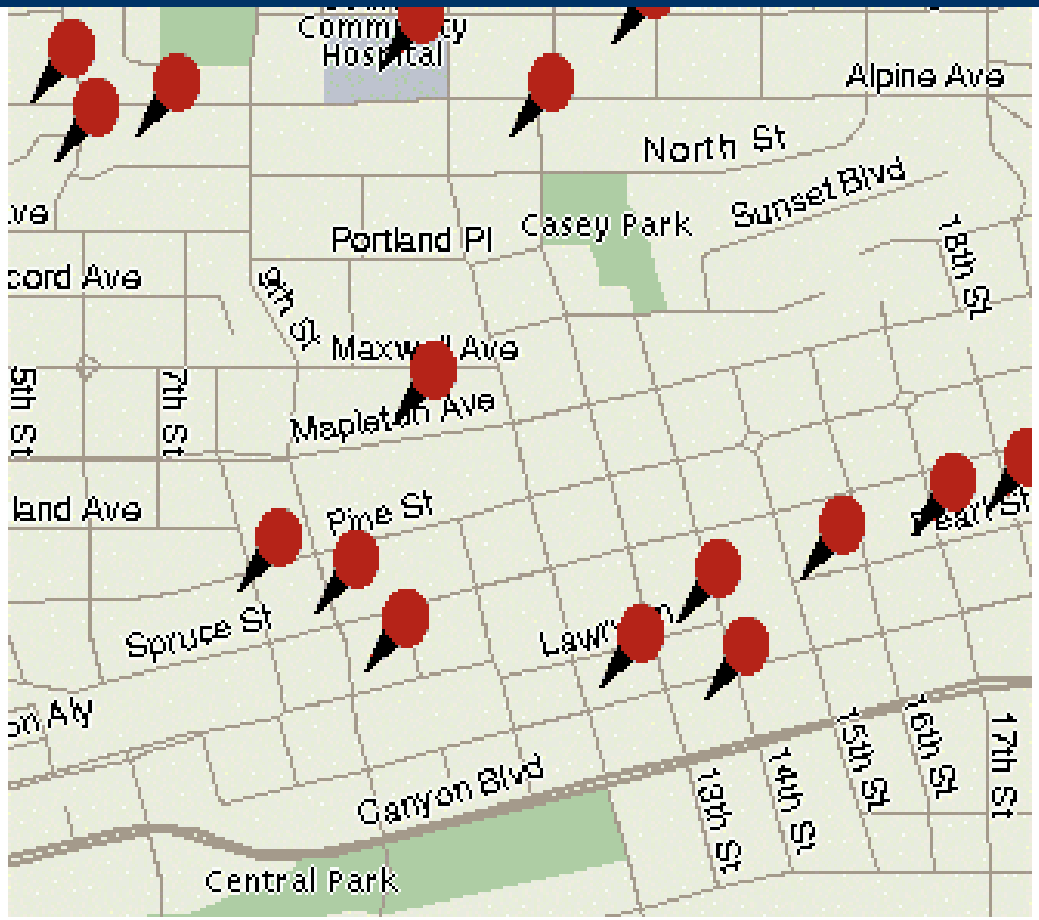
Wardriving (Denver)



http://www.athomeprd.com/~jimb/wardriving/index.html

Boulder Labs

Wardriving (Boulder)



Boulder Labs

Wardriving Tools

- Stumblers
  - Netstumbler (Windows) www.netstumbler.com
  - dstumbler (BSD) www.dachb0den.com
- Capture and Crack utilities
  - airsnort (linux) www.airsnort.shmoo.com
  - bsd-airtools (BSD) www.dachb0den.com
    - prism2ctl , dstumbler , dwepdump , dwepcrack

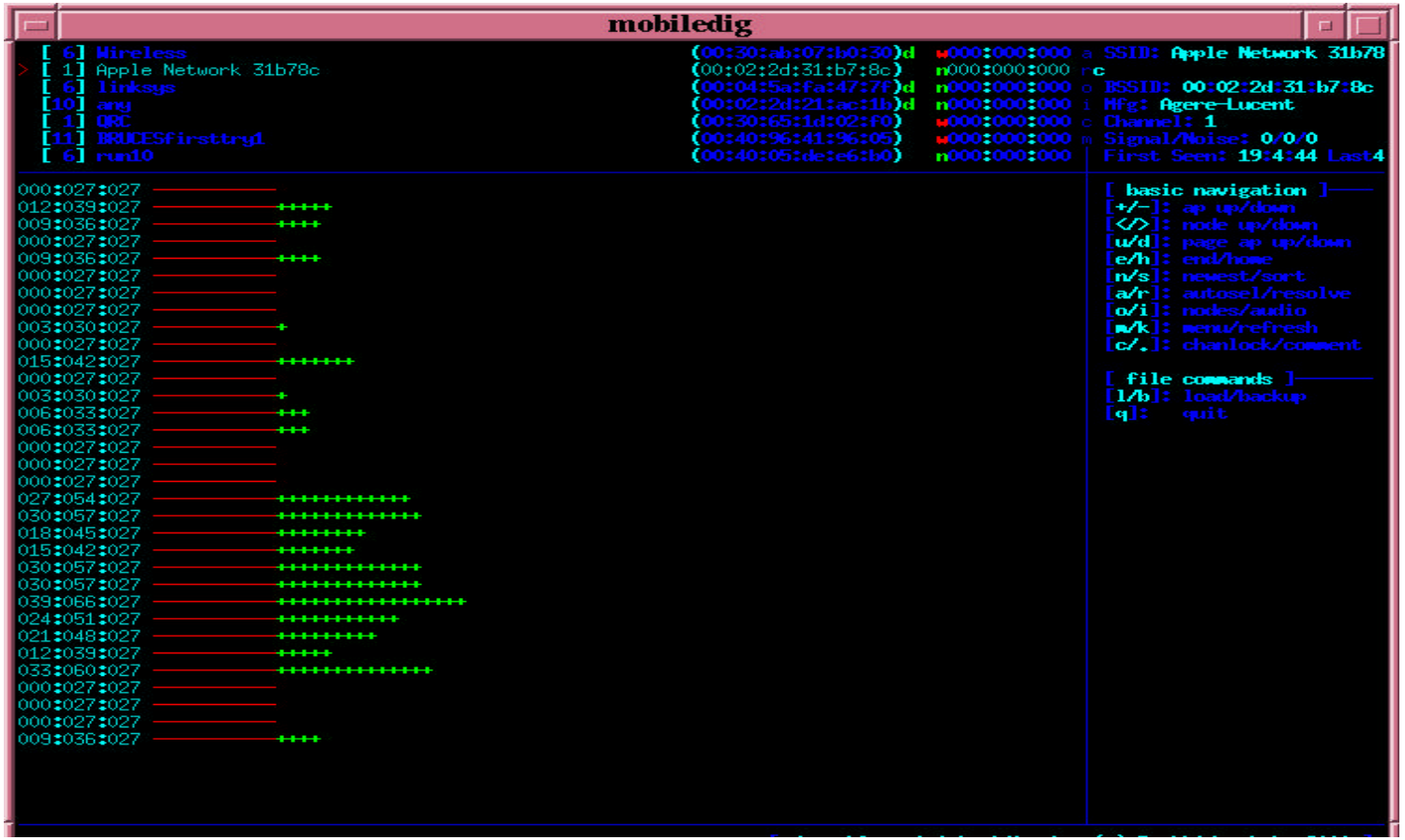
Boulder Labs

dstumbler

- Used to find Wireless Networks
- Works with Prism2 and Hermes Cards
- Detects WEP on/off
- Detects default settings

Boulder Labs

dstumbler Screenshot



Boulder Labs

dwepdump

- Used to gather packets
- Works with Prism2 cards
- Passive Sniffing
- Use it in 104 bit or 40 bit mode
- Used for weak KSA attack (60 packets)

Boulder Labs

dwepcrack

- Used to retrieve encryption keys
- 21-bit attack
- Dictionary attack
- Weak KSA attack

Boulder Labs

How to secure Wireless

- Treat 802.11b as external (outside firewall)
- 802.11x
- Vendors (non-standard, Cisco, Agere)
- Secure services: SSL, SSH, IMAP/S
- IPsec
- Use 104-bit keys and change frequently

Boulder Labs

References

- Borisov, Goldberg, Wagner
  - Intercepting Mobile Security of the WEP Algorithm. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Fluhrer, Mantin, Shamir
  - Weaknesses in the Key Scheduling Algorithm of RC4 http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf
- Stubblefield, Ioannidis, Rubin
  - Using the Fluhrer, Mantin, Shamir Attack to Break WEP http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf