Wireless (In)security: The true state of wireless security (updated!)

AMICUE

June 9th, 2005

Speech by Renderman

Render@Renderlab.net

Introduction

- Who Am I?
- Why Am I Here?
- Scope of this talk
- Why you should stay awake
- What you should be doing – Audience participation!

WLAN Glossary

- SSID: Service Set Identifier - Wifi network‘name’
- WEP: Wired Equivalency Protocol
- WPA(2): Wifi Protected Access
- Wi-Fi: Wireless Fidelity Group (a,b,g compliance certification)
- AP: Wireless Access Point
- Wardriver: Good guys
- Hackers: Good guys
- Bad guys: Bad Guys

Wireless Primer

- 802.11b
  - 2.4Ghz – License free
  - 11 channels, 2.412 –2.462 GHz
  - 11Mbps MAX
  - 40, 64, 128, 256 bit WEP & WPA Encryption
  - MAC filtering
  - SSID – logical network name
  - Cellular nature
  - Extremely popular
  - Ubiquitous

- 802.11a
  - 5 Ghz – License free
  - 54 Mbps MAX
  - Same Channels as 'B'
  - 64, 128, 152 bit WEP Encryption
  - MAC filtering
  - SSID – logical network name
  - Cellular nature
  - Short Range, Not backward compatible (‘A’ only units)

Wireless Primer

- 802.11g
  - 2.4Ghz – License free
  - 54 Mbps MAX
  - 64, 128, 152, 256 bit WEP & WPA Encryption
  - MAC filtering
  - SSID – logical network name
  - Cellular nature
  - Backwards compatible with ‘B’ gear

- ‘B/G’ combo units
- ‘A’ quickly becoming a ‘white elephant’
- All have similar security problems
- Interm patches to security suck
- Focus of this talk will be around ‘B’, but applicable to ‘A&G ‘ deployments

WLAN Basics

- Wi-Fi NIC is configured for the same SSID and frequency channel as AP
- If WEP/WPA is required, key is exchanged
- Session is established, TCP/IP, Net Bios, etc. Sessions continue as with wired net
- Seamless to user

WLAN Basics

- Various features among different models
- Usually have DHCP server, MAC filtering, WEP/WPA
- Wi-Fi is designed to ‘roam’ to strongest signal
- Many different manufacturers and many brands
  - Dlink
  - Linksys
  - Cisco
  - Apple
  - Netgear
  - Dog + World

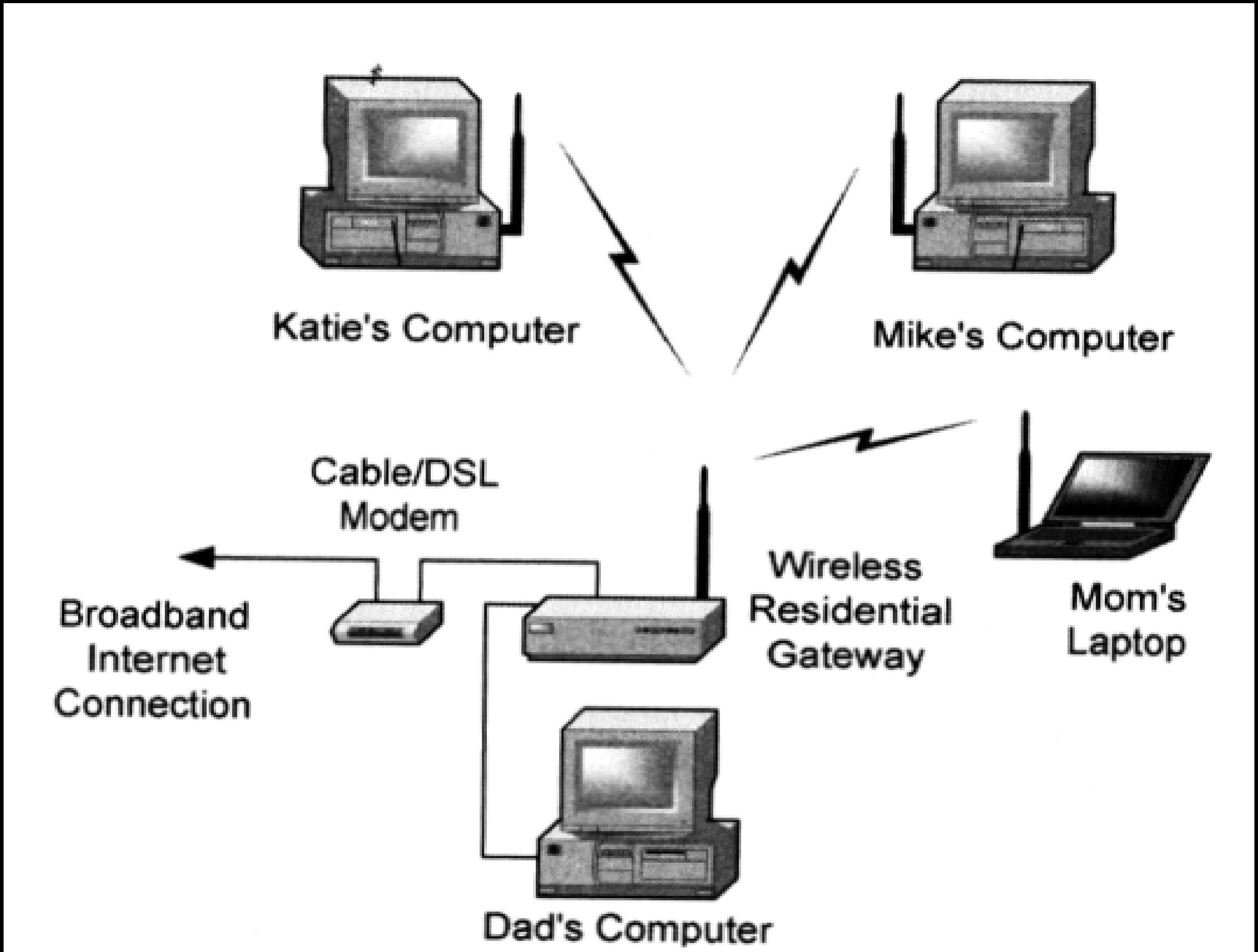
WEP

- Wired Equivalency Protocol
- Shared Key based Encryption to encapsulate all 802.11x traffic between Client and AP
- Based on RC4
- Standard on 802.11x gear

WPA

- 'Update' to WEP
- Uses TKIP key to improve security
- Also uses EAP for authentication
- WPA2 just released

Look Ma' No Wires!



It’s everywhere

- WiFi is a multi billion Dollar industry
  - $1.546 Billion in 2002
  - Set to rise (or fall, depending on the report?)
- Prices falling dramatically
- Most laptops/PDA’s Wi-Fi enabled from the factory
- Hotspots at Airports, Airplanes, Café’s, Hotels
- Very pervasive, very chic, ‘hot’ technology
- Intel’s ‘Unwired’ marketing push

Enough marketing and history

Time for the Wardriving and Fun Stuff

What is ‘Wardriving’

- ***WarDriving v. The <u>benign</u> act of locating and logging wireless access points while in motion. - Blackwave***
  - A.k.a, Network stumbling, lanjacking(?), whacking(?)
  - Using a Wi-Fi enabled device, to discover the presence of wireless networks for statistics and mapping purposes
  - Does not include idiots who connect, they are called criminals

What is ‘Wardriving’

- Factory software allows rudimentary ‘stumbling’
- First coined and automated by Pete Shipley of Dis.org in 2001
- Completely LEGAL!
- Now a competitive sport!
- Frighteningly effective

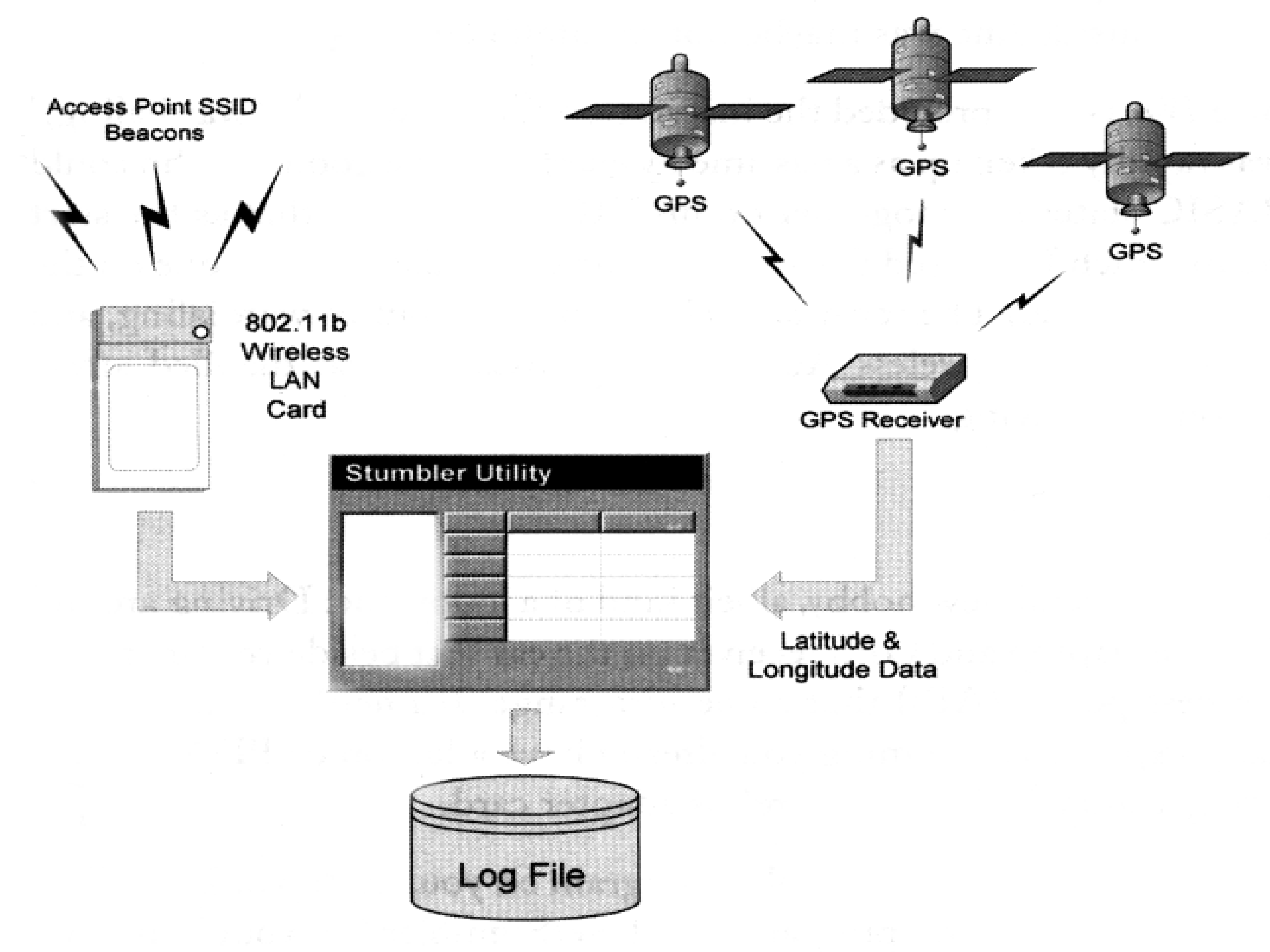
Wardriving 101

- Laptop or PDA
- 802.11b(or A or G) card
- Special software that supports the card (Netstumbler, Kismet, BSDairtools, Wellenreiter)
- Some form of conveyance (feet, bike, car, etc)
- Optional:
  - External antennas (Pringles can, omni, yagi, etc)
  - GPS for generating maps
  - Misc software (real-time tracking, routing)
  - Music
  - Co-pilot

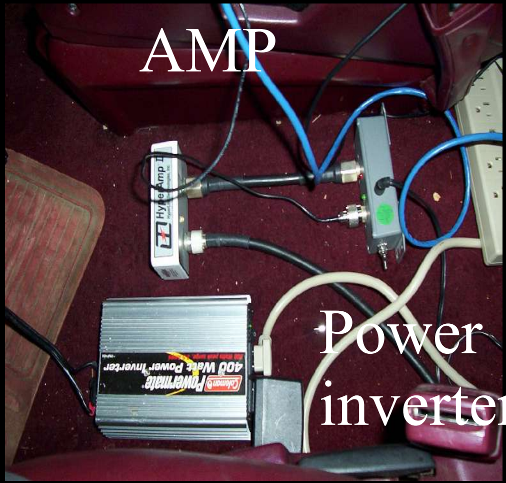
Passive Vs Active

- Netstumbler – Active, 'Pings' for and Listens for ‘Broadcast’ announcements ~100 per second)
- Kismet – Passive, Listens for any 802.11b traffic and determines network settings from packet capture. Able to detect ‘cloaked’ AP’s (SSID broadcast turned off)
- Both Free (as in beer)
- Both useful as site survey tools, used throughout the industry

Wardriving 101


Access Point SSID Beacons
GPS
GPS
GPS
802.11b Wireless LAN Card
GPS Receiver
Stumbler Utility
Latitude & Longitude Data
Log File

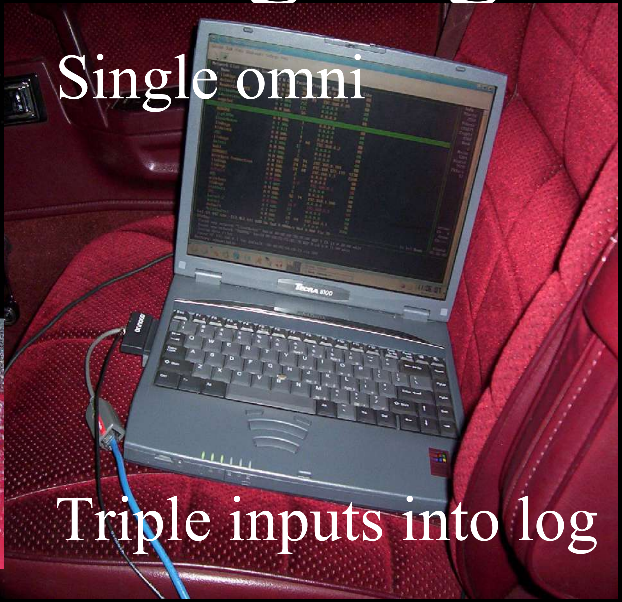
The RenderVan Wardriving Rig



AMP

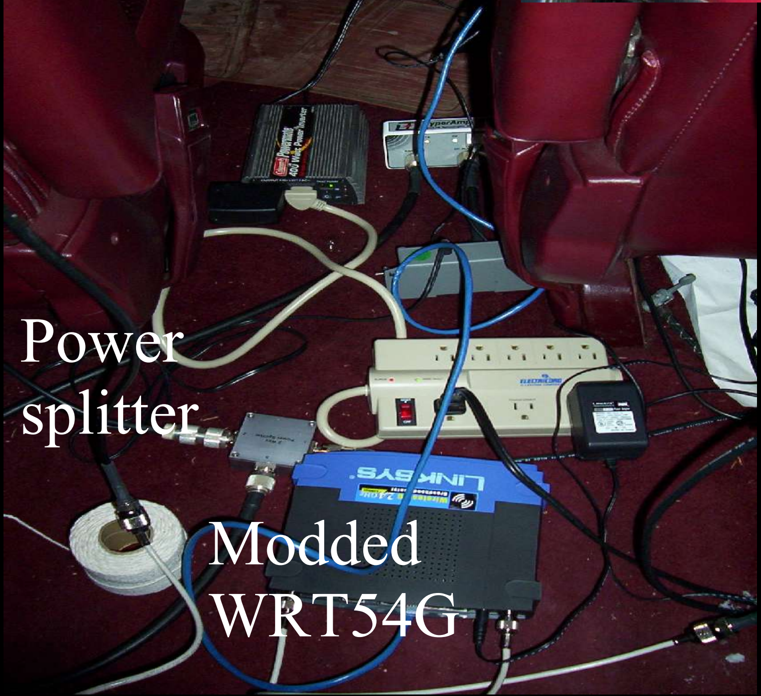
Power inverter

Dual Omni's



Single omni

Triple inputs into log

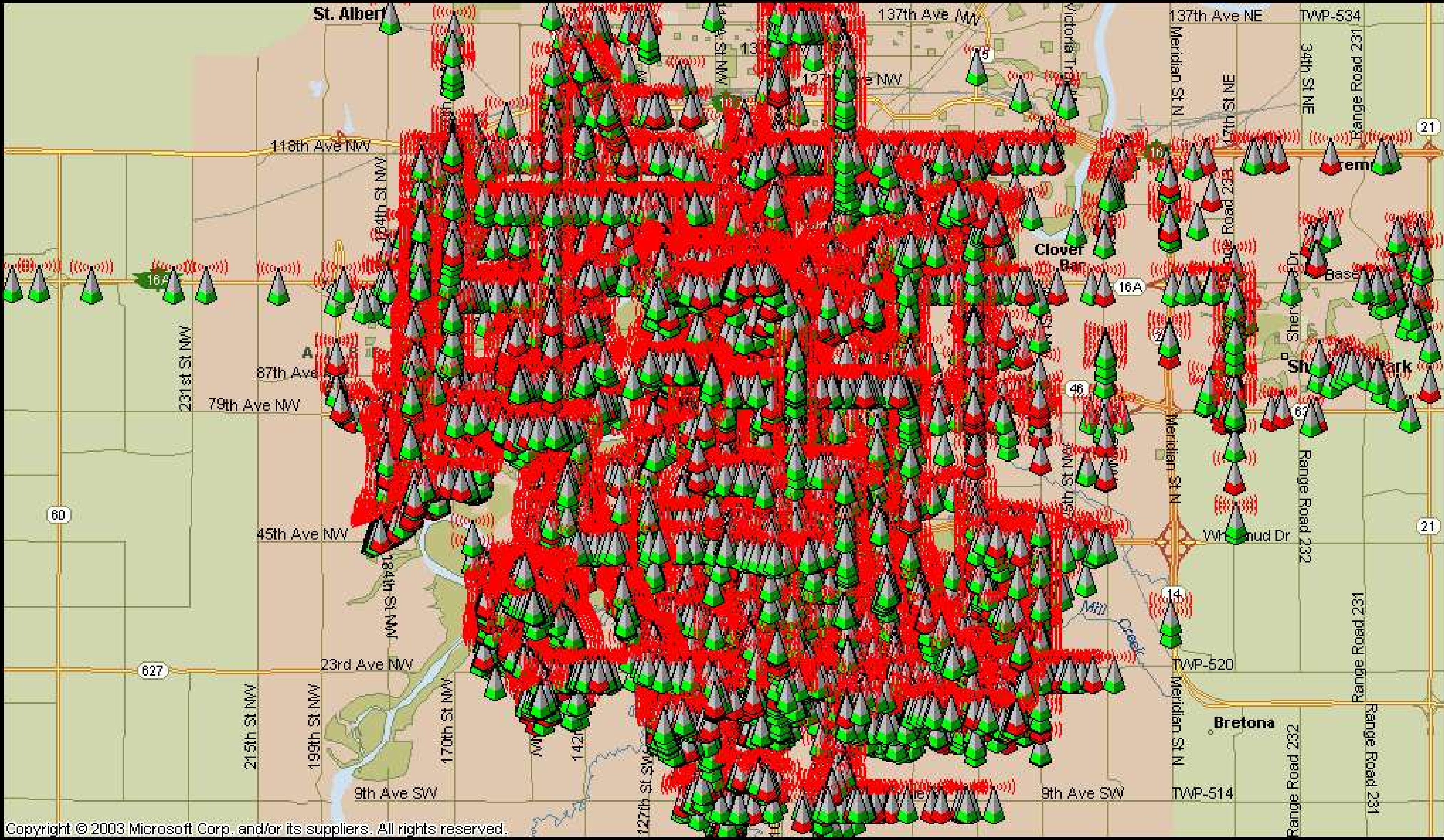


Power splitter

Modded WRT54G

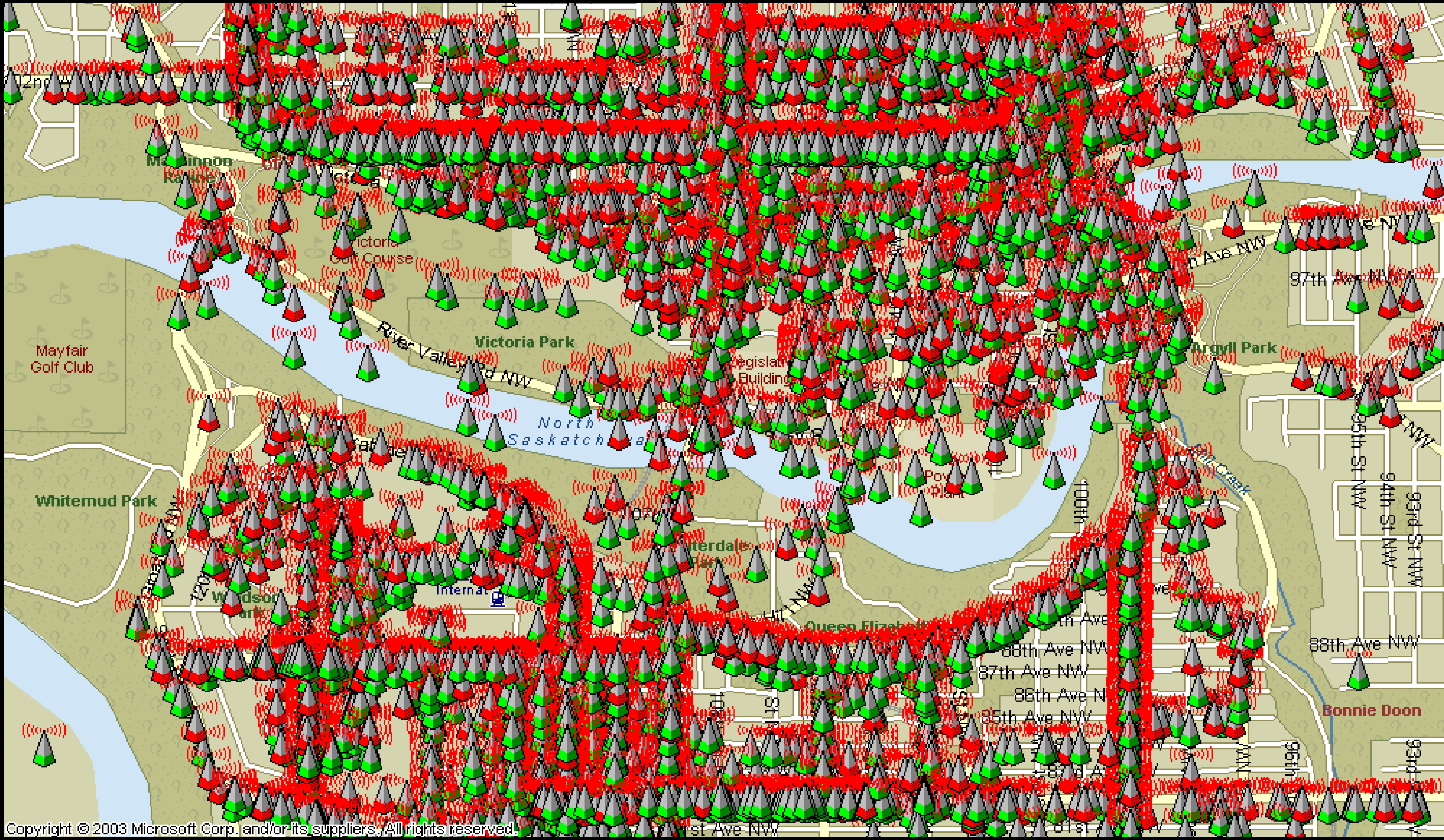
Dual yagis

Edmonton, Alberta as of May 29th 2005, 19,721 Access points



Copyright © 2003 Microsoft Corp. and/or its suppliers. All rights reserved.

Downtown and University Detail



Edmonton Statistics

Since March 2002

- – 19,721 separate Access points detected
- – 14,520 without WEP* (not necessarily insecure)
- – 5506 on default settings (very insecure)

- In the strangest of places
  - – Hospitals, health facilities, gov’t, hotels, trucking companies, breweries, homes, oil companies, schools, cafes, newspapers….

* Does not currently count WPA networks

Edmonton Survey Conclusions

- After many months and a lot of miles, It’s getting (slowly) better, BUT:
- Insecure population growing faster, but seems to be learning though (Setup is earier now)
- Wireless is popular even in the frozen north and getting bigger
- ‘It can’t happen here’ attitude
- Still a severe lack of understanding
- There is an interest in learning though (You’re here now aren’t you?)

Now that I have your attention…

What is the problem?

The problems with Wi-Fi

- No one RTFM’s or plans deployment
- AP’s left on defaults
- WEP - unsafe at any key length
- WPA - Just a matter of time....
- Inappropriate deployment
- ‘Rogue AP’s
- It’s a RADIO!

RTFM

- Buried security warnings and instructions
- No deployment warnings
- Manufacturers ignoring problem, bad for sales
- ‘We don’t need no stinkin’ Manual!’ IT attitude
- Is getting better, common manufacturer setup utils

Defaults

- 27.9% of AP’s in Edmonton on Default, ‘out of box’ settings
- ‘It works, don’t screw with it’ attitude
- Quick start guides ignore security
- Technical glitches and frustration
- Failure to realize that ANYONE can connect and use your connection

Wired equivalency protocol

- Uses RC4
- Export restrictions kept key at 40bit, very weak 64bit added later on
- Proprietary extensions for 128bit and up, incompatible between manufacturers, making for headaches and users ignoring it
- Static Key, hard to change in large deployments
- Found weak in July 2001
- Fluhrer, Mantin, and Shamir ('S' in RSA) Broke RC4 in August 2001 which lead to…
- Airsnort : 5-10M Packets + Luck = WEP Key
- Further breaks/weaknesses over the years leaves...
- Aircrack : 300K Packets + 30 seconds = WEP Key

Deployment problems

- Often behind firewalls and other security devices on the ‘Trusted’ side of the network
- Should be treated as a wall jack; Would you run cat5 to the parking lot?
- Current implementation makes security hard to maintain (rotating keys, updating MAC filters)
- Attitudes: ‘No one would want to break in here’, ‘No one will find me’, ‘Security costs too much’
- Technical bugs in trying to setup a secure system

Rogue AP’s

- Employee’s being ‘helpful’, or ‘creative’
- IT staff unaware, not caring
- No company policies, or no enforcement
- No IT auditing – ‘rogue hunting’
- Often on defaults (ID10T errors)
- Gee whiz factor for the boss
- Temporary becomes permanent
- Teddy-Net

Remember: It’s a Radio!

- Broadcasts far beyond walls and property
- If WEP/WPA not enabled, data is sent in the clear
- Email, database queries, FTP, messenger…
- Data sent in all directions
- Long distance connection <55 miles
- All Wi-Fi gear is a Tx & Rx
- Wi-Fi is ‘cellular’ in nature, designed to associate with the strongest signal (even if it’s not yours)
- Poorly designed spec allows for all sorts of fun

There Is Hope!

- WPA as an interim fix
- 802.1x
- Cisco LEAP now slowly being shared among manufacturers
- Manufacturers starting ‘Secure by Default’ and common setup utilities
- Manuals starting to discuss security bluntly
- XP SP2 makes setup a lot easier
- Lots of press

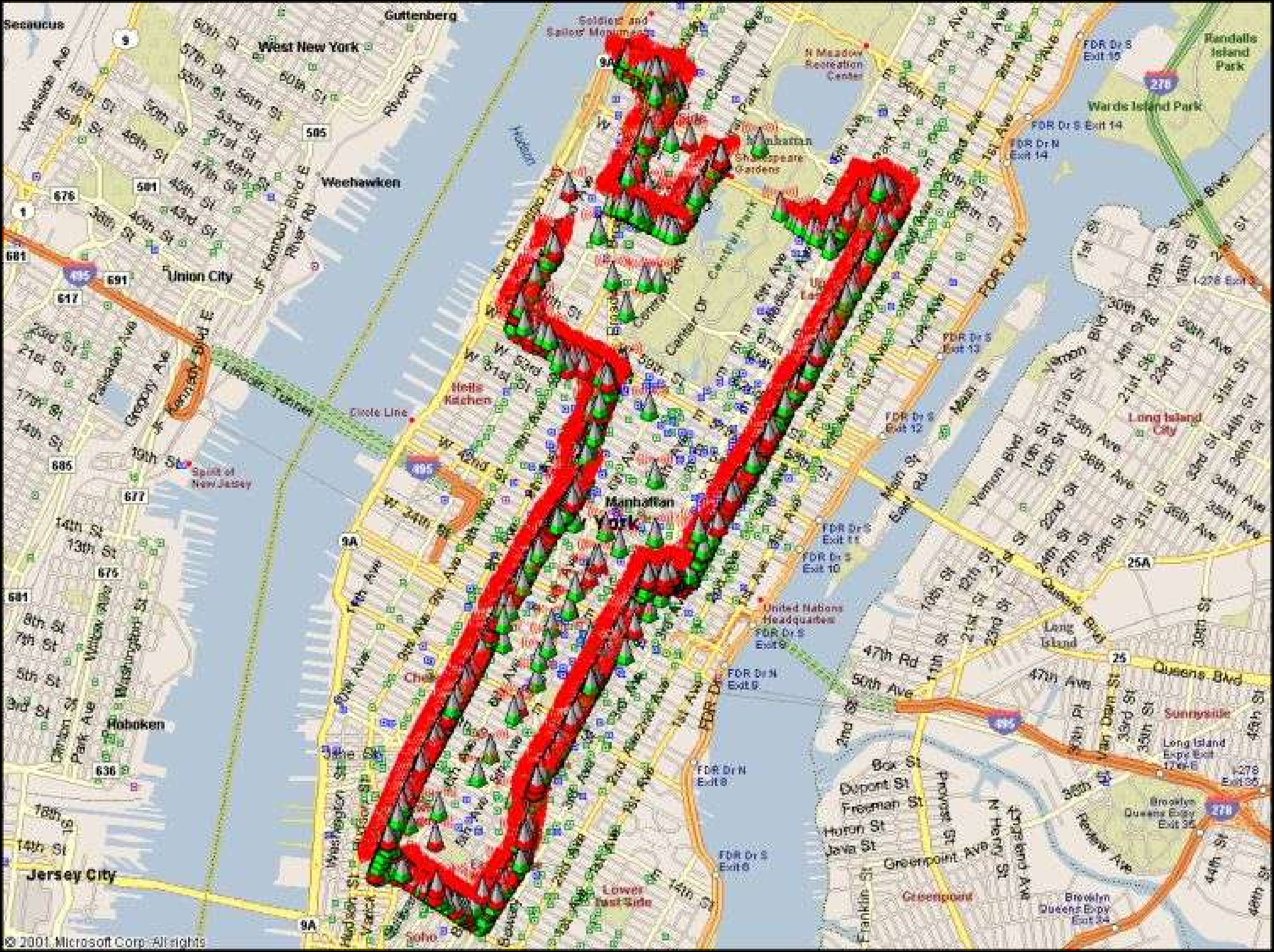
Suggestions for right now

- Set a company policy and enforce it. Big Bat!
- Use WEP/WPA at a minimum – Keep out sign
- EAP (Extensible Authentication Protocol), Cisco
- RADIUS, 802.1x, VPNs, captive portals
- Audit network from wired side
- Audit network from wireless side
- Locate AP's in front of firewall, captive portal or other authentication (RADIUS, etc)
- Hire professionals for installation and advice (Many Wardrivers are professionals)

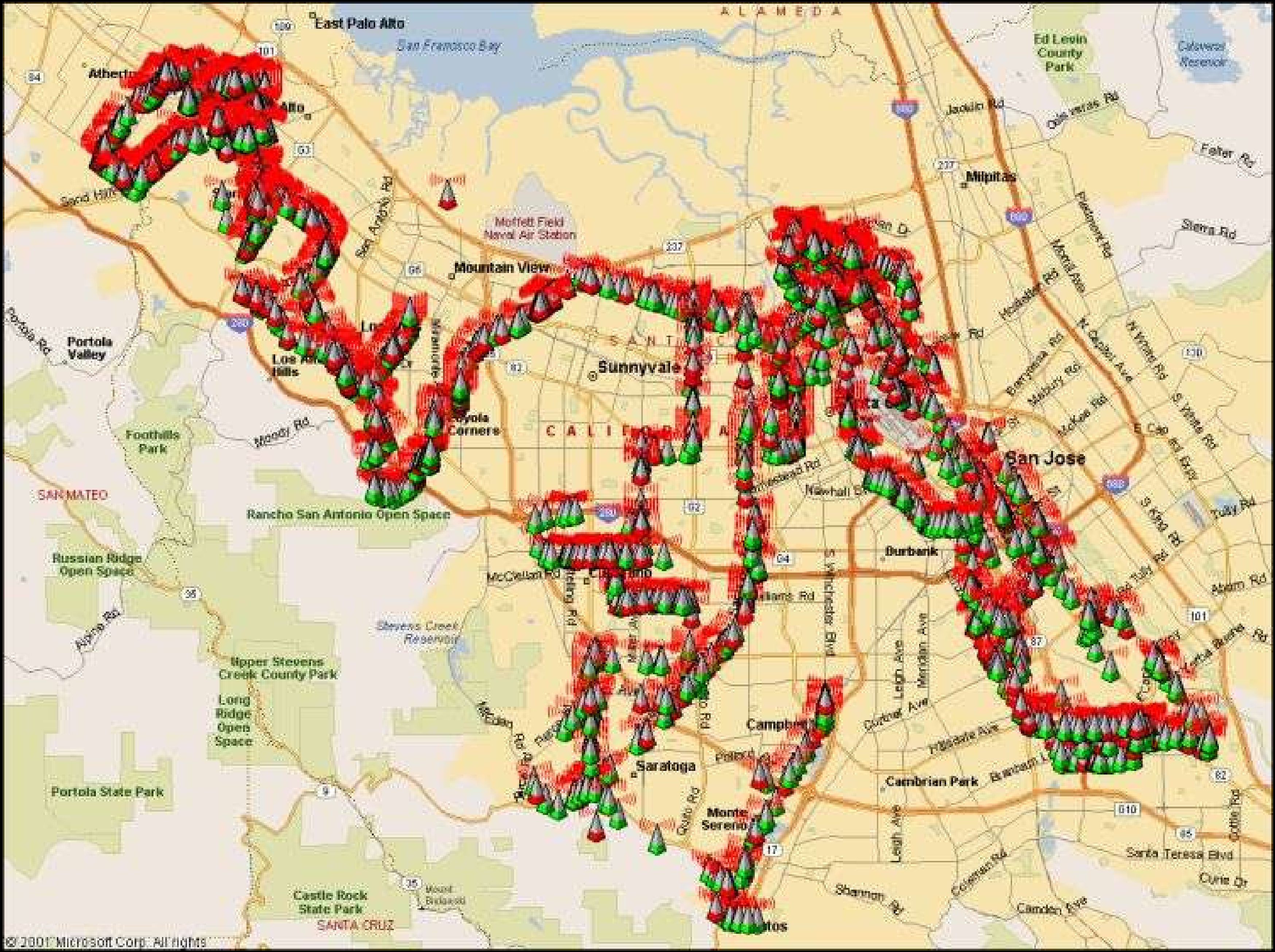
It’s not Just an Edmonton problem

In 2002, the Worldwide Wardrive was founded to provide a worldwide ‘snapshot’ of wireless usage and security for statistical analysis and awareness

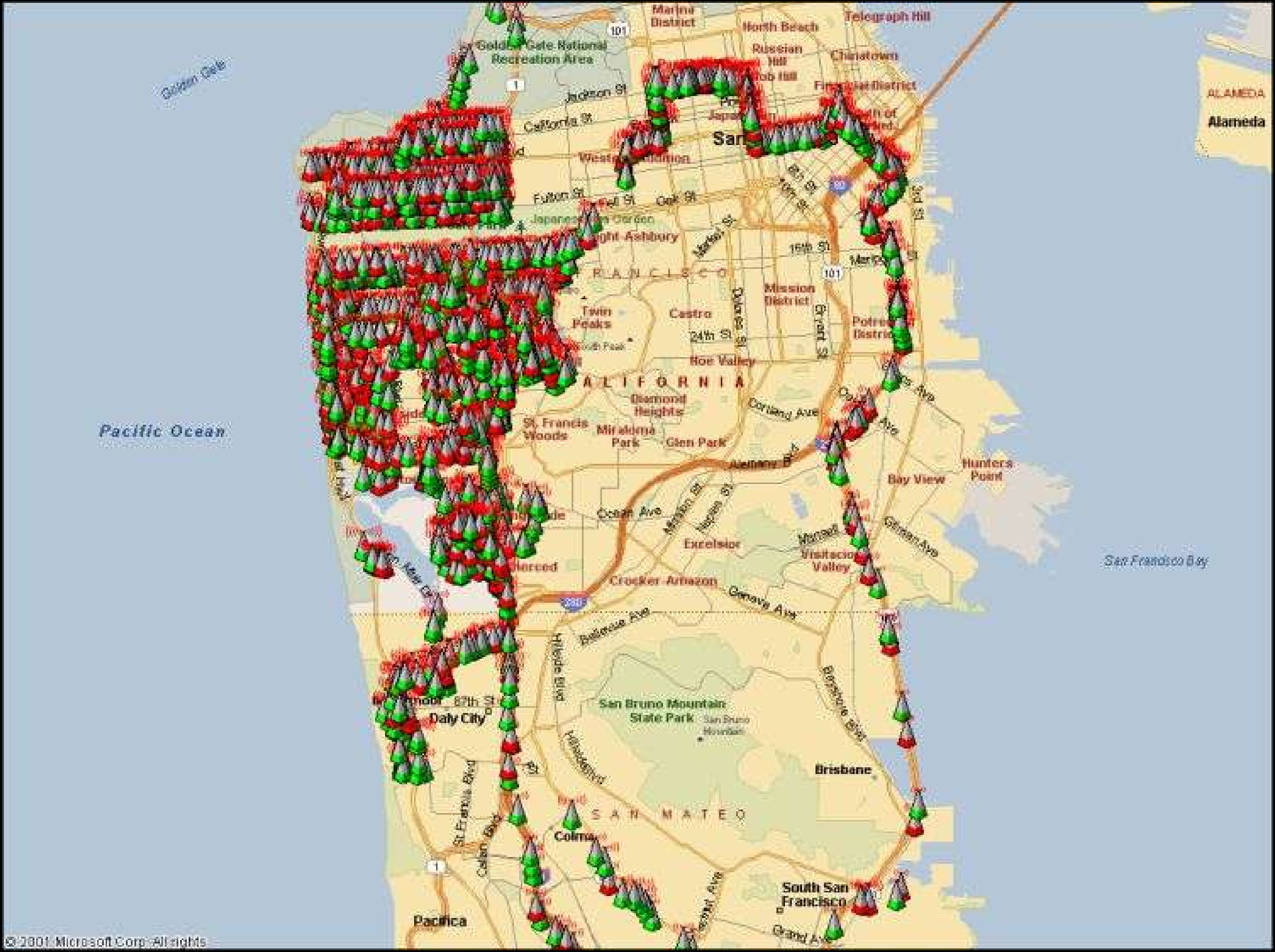
NYC –WWWD3


Secaucus
Guttenberg
West New York
Weehawken
Union City
Hoboken
Jersey City
Soldiers' and Sailors' Monument
N Meadow Recreation Center
Shakespeare Gardens
Central Park
Hells Kitchen
Manhattan
York
Chelsea
Soho
Lower East Side
United Nations Headquarters
Randalls Island Park
Wards Island Park
Long Island City
Sunnyside
Greenpoint
Lincoln Tunnel
Circle Line
Spirit of New Jersey
Queens Blvd
FDR Dr
Broadway
W 42nd St
W 34th St
W 52nd St
W 51st St
Joe Dimaggio Hwy
River Rd
Kennedy Blvd E
Palisade Ave
Willow Ave
Washington St
Park Ave
Lexington Ave
Madison Ave
1st Ave
2nd Ave
3rd Ave
York Ave
Vernon Blvd
Jackson Ave
Greenpoint Ave
Brooklyn Queens Expy
Long Island Expy
9A
495
278
25
25A
© 2001 Microsoft Corp. All rights

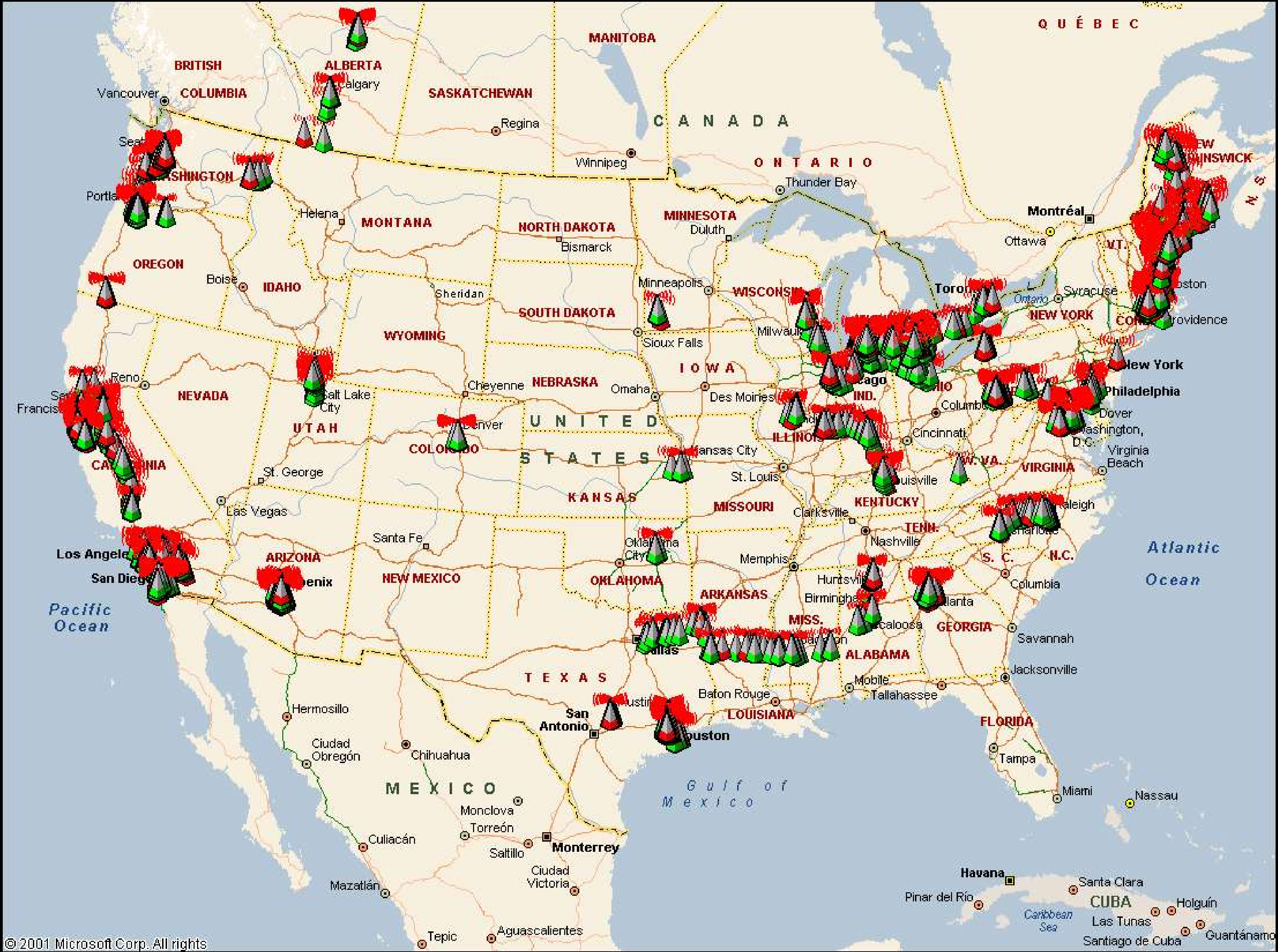
Silicon Valley –WWWD3



San Francisco –WWWD3



North America –WWWD3



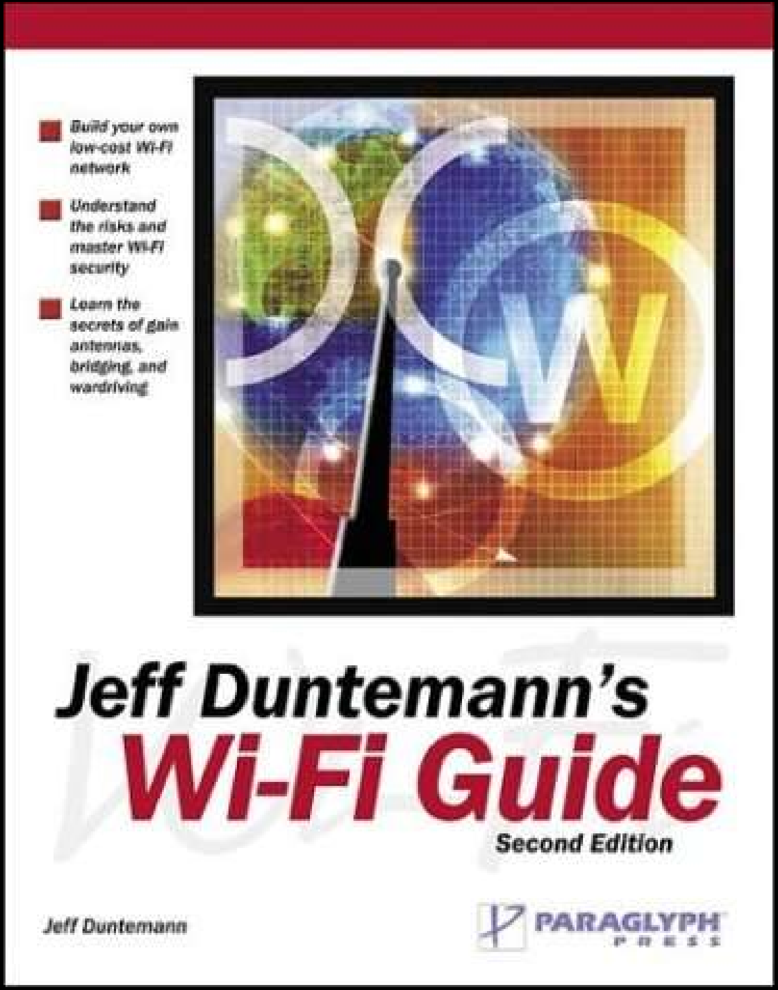
WWWD

- WWWD4 – June 28th to July 5th 2004

Category	Total	Percent	Change
Total AP’s	228,537	100	
WEP Enabled	87,647	38.3	+6.04
No WEP Enabled	140,890	61.6	-6.04
Default SSID	71,805	31.4	+3.57
Default SSID and No WEP	62,859	27.5	+2.47

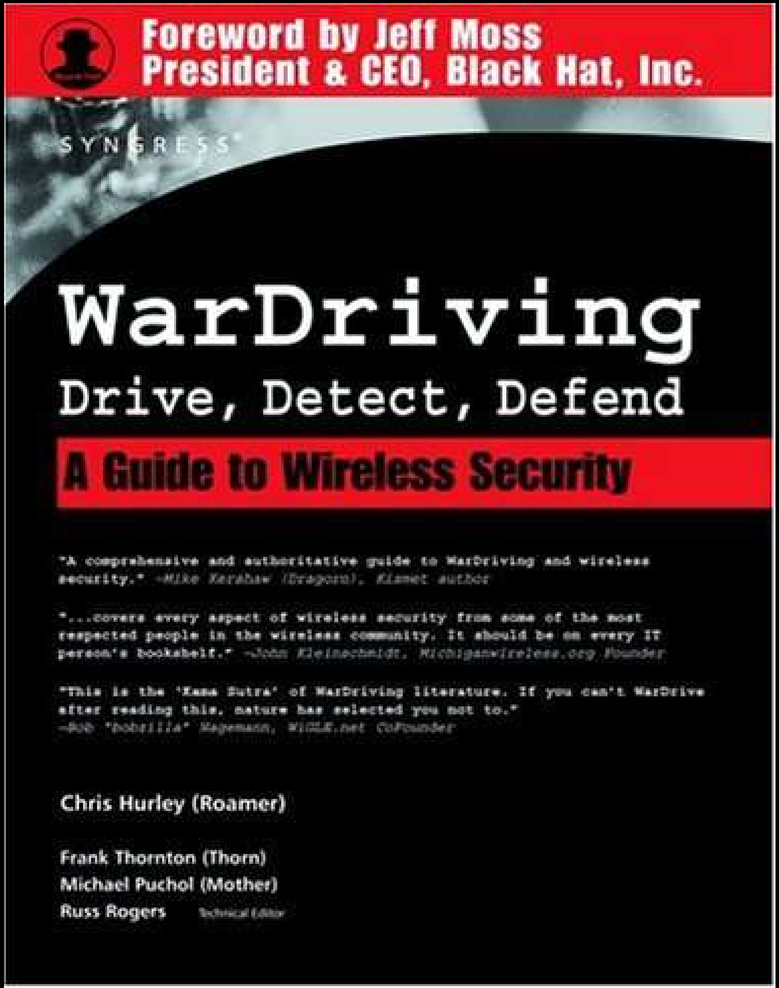
Resources

- Wardriver Approved
- 2 Chapters about wardriving
- Real world information, not theory based. Very practical
- Best book on real world security and implementation
- Written by one of the coolest people I know


Build your own low-cost Wi-Fi network
Understand the risks and master Wi-Fi security
Learn the secrets of gain antennas, bridging, and wardriving
Jeff Duntemann's
Wi-Fi Guide
Second Edition
Jeff Duntemann
PARAGLYPH PRESS

Resources

- Wardriver Written
- Complete How-to Guide
- Real world information, not theory based. Very practical
- Covers History and Ethics (as written by me!)
- “The 'Kama Sutra' of wardriving literature”
- Please buy through amazon.com link on www.blackthornsystems.com



Foreword by Jeff Moss
President & CEO, Black Hat, Inc.

SYNGRESS

WarDriving

Drive, Detect, Defend

A Guide to Wireless Security

"A comprehensive and authoritative guide to WarDriving and wireless security." –Mike Kershaw (Dragorn), Kismet author

"...covers every aspect of wireless security from some of the most respected people in the wireless community. It should be on every IT person's bookshelf." –John Kleinschmidt, Michiganwireless.org Founder

"This is the 'Kama Sutra' of WarDriving literature. If you can't WarDrive after reading this, nature has selected you not to."
–Bob "bobzilla" Hagemann, WiGLE.net CoFounder

Chris Hurley (Roamer)

Frank Thornton (Thorn)
Michael Puchol (Mother)
Russ Rogers Technical Editor

Wigle.net

- Online Mapping Engine for AP’s
- Great way to check if you’ve been stumbled
- 3,000,000 AP’s mapped since Sept 2001
- Great resource in large cities for quick-and-dirty site surveys
- Proof that there’s wireless everywhere
- Great 'I-told-you-so' site to show the boss!

Websites

- Worldwidewardrive.org – Home of the WWWD
- Netstumbler.com – Wardriving software - Win32
- Kismetwireless.net – Wardriving Software - Unix
- Wardriving.com – Wardriving news and software
- Renderlab.net – Local Wardriving info and guides
- Fab-corp.com – Making a living off my addiction
- Wigle.net – Wirless maps
- Wifimaps.com – More Wireless maps
- personalwireless.com/tools – Tools archive

Demo’s & Questions

Questions, Comments, Accusations, Demontrations

Wireless Ways To Make Your Day Suck

- Wifi is a Radio
- Management frames control a lot of the connection
- Very poorly designed (What authentication?)
- No client controls for authenticating AP's
- What helps can also hinder
- Cleartext data can be folded, spindled and mutilated

Why you should worry

- Unless you know the attacks, how can you guage risk?
- Understanding why your network goes to hell at 3:17pm each day
- Most attacks don't leave blatent fingerprints
- Many attacks can lead to further penetration
- Sometimes it's just weird stuff that makes you pull your hair out

Void11 – Deauth Attack

- Client end session and sends a 'Deauthentication' frame for it's MAC to the AP to signal end of the session
- We can see the AP's MAC, the clients MAC.... What happens if we broadcast a spoofed deauth frame mid session?
- How to grind your network to a halt, FAST!
- Also useful as an anti-rogue tool!

Aircrack

- WEP cracker that uses statistical analysis of encrypted frames to 'guesstimate' key
- First 24bits of key are known!
- 64bit=40bit, 128bit=104bit
- 40bit=150,000 frames, 104bit=500,000 to 1M frames required
- Aireplay allows for quick generation of encrypted traffic
- 1-2hrs to collect on a busy network

Airpwn

- Debuted at Defcon 12 to much amusement
- Man-In-The-Middle replacement of data
- Listen for 'GET' request of images/HTML and replace with our own
- Requires 2 cards, 1 recieve, 1 send
- Fun party trick, but could also be used to inject malicious payloads into websurfing at, oh say, a public hotspot....

Airsnarf

- 'Fake' access point tool ('Evil Twin' AP)
- Turns your laptop into an access point for MITM attacks
- Simply replace login screen with public hotspot login page, overpower legit AP, all users now send their data through you, and logins and passwords are sent to root@localhost
- You control DNS as well...

Hotspotter

- Listens for clients preferred network
- Compares to internal list of known hotspots
- Configures itself to be that hotspot
- Can be made to run any sort of script/command after succesful association (Port scan? Malicious payload upload?)
- Could be extended to respond to ANY network probes....

FakeAP

- 'Spew' random becon frames of fake networks to hide your AP among the noise
- What happens if someone does it to you?
- XP likes to cling to the strongest signal
- 400000 identical SSID networks anyone?
- How about at a legit hotspot? Conference?
- Neat party trick, not overly useful in production

Help! What do I do!

- Wi-Fi needs planning
- Hire a professional!
- Site survey
- Invest in higher end gear
- Failover plan, what happens if it goes down?
- Layer 2 monitoring? Wireless IDS? Tracking gear? Disipline device?
- Don't do it because of the 'gee whiz' factor

Conclusions

- Wifi is not for everyone or every situation
- There are risks with any network
- Know thy enemy, Know your risks
- Slowly getting better
- Keep up on the news

Thank you.

Questions?