Open WiFi issues

The Temptation of Open WiFi

Part I in the “Security as a Social Issue” Series
By dc0de

Wireless Networking Overview

- Wireless networks are “easy” to setup
  - “Plug and Play”
  - Authentication is often overlooked
- 802.11b equipment costs are continuing to drop
- Inexpensive WAP’s are highly available

Security Issues

- Wired Equivalence Privacy (WEP) is broken
- Cracking WEP is now considered “trivial”
  - AIRSNORT
  - WEPCrack
- WiFi Protected Access (WPA)
  - Encryption Scheme to “fix” WEP
  - Not widely used

Current Threats

- War-driving
- Drive-by-spamming
- Drive-by-surfing
- Drive-by-attacks
- Drive-by-hacking

War-driving

- Location of APs by the use of GPS and antenna's, very commonplace
- Large databases of information
  - www.wigle.net, over 1 million unique AP's in database today.
- War-Driving is NOT illegal, as long as a connection to the network is not obtained, i.e. obtaining an IP Address would break the law

Drive-by-spamming

- A spammer needs to send out 10,000 emails, making .05 cents for each, and doesn't want to use his internet service at home
- He simply drive to the next open AP, and sends out his 10,000 messages.
- The owner of the Open AP will lose his internet service, not the spammer.

Drive-by-surfing

- Someone wants to download some illegal software or other nefarious data
- Again, not wanting to use their internet connection, they simply drive to the next town, find an open WiFi point, and “get to work…”
- Again, any tracking / tracing, points at someone else

Drive-by-attacks

- Now, a hacker feels really invincible, and wishes to attack the US Government's web structure
- Where do they go to perform their attacks?
- When the government traces the attacks back, they are pointing at someone else...
- And, if they're really sneaky, they'll sniff the network first for a MAC address on the WiFi, and spoof that as their source MAC address... leaving only trails to the poor Open WiFi owner.

Drive-by-hacking

- Now, a hacker is bored, and want to collect some Personal Identifying Information, so they can “borrow” someone’s identity.
- They drive to an Open AP, search the local network and find the local hosts and search for any information that can be used to steal an identity.

Legislation

- Sarbanes-Oxley
  - Primarily Public Companies
- HIPPA
  - All Health Care Organizations, and affiliated organizations that deal with Patient Data

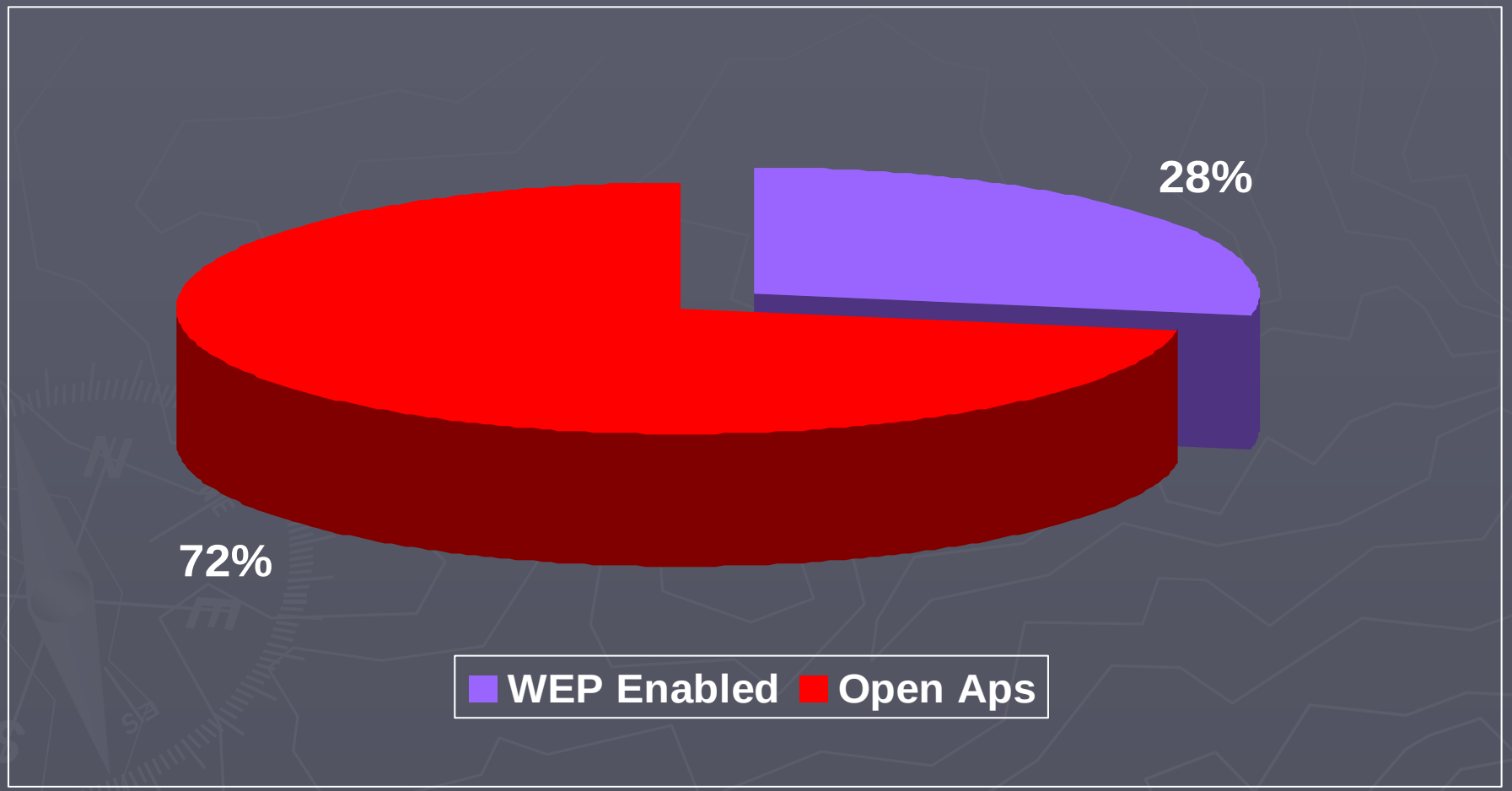
Legislation (cont...)

- GLBA
  - Anyone dealing with Personally Identifying Information (PII)
- California State Bill 1386
  - Effects any organization that could potentially release PII about a current or *future* California Resident.
- Future Legislation
  - CB 1386 turned Federal...
  - Others...

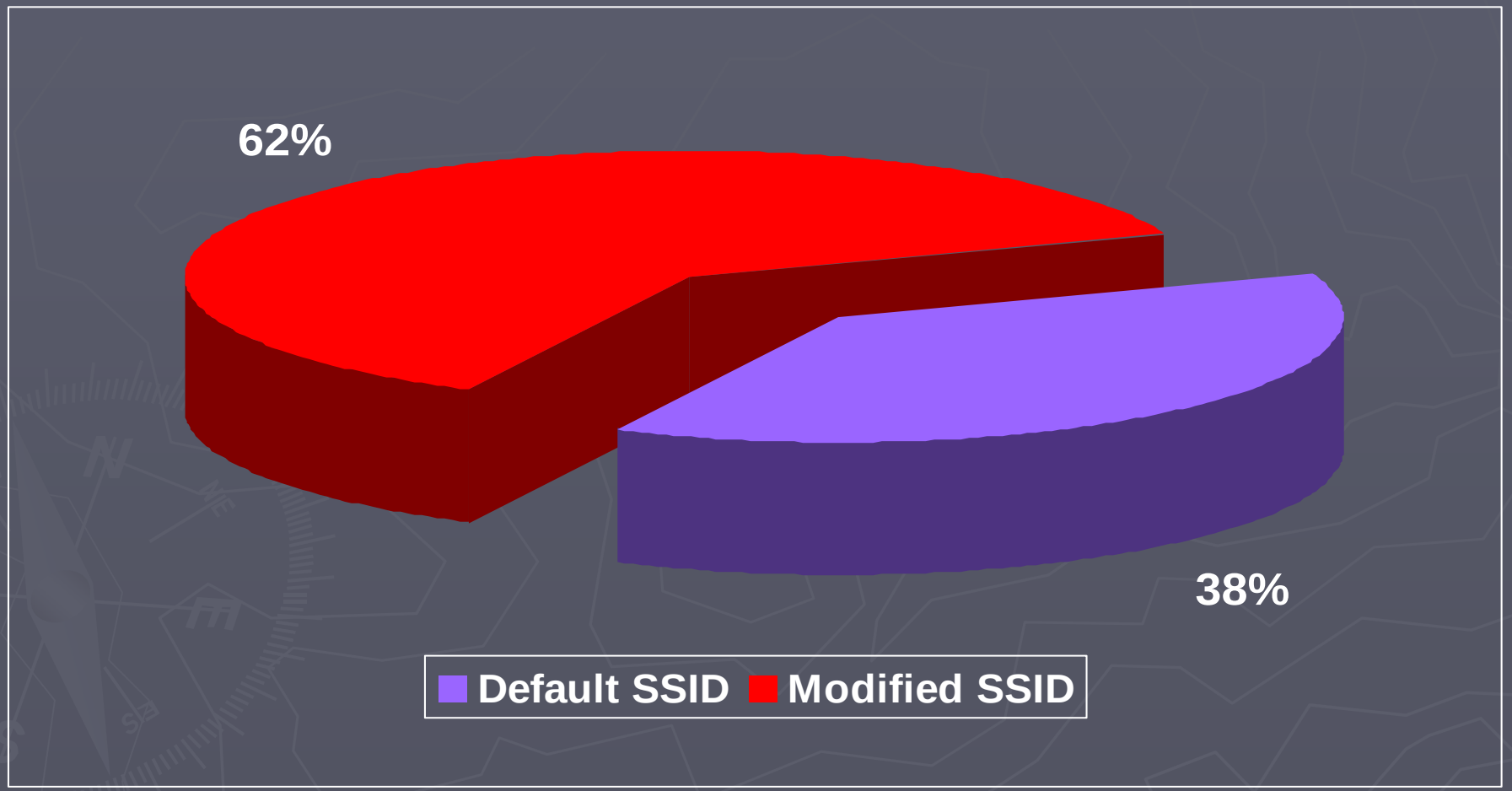
Sample Data - Wardrive

- Trip on Tuesday, June 8th 2004
- Total distance traveled: 150.6 miles
- Time Started: 16:23
- Time Stopped: 18:36
- Total time: 2:13 minutes
- Total AP's: 191

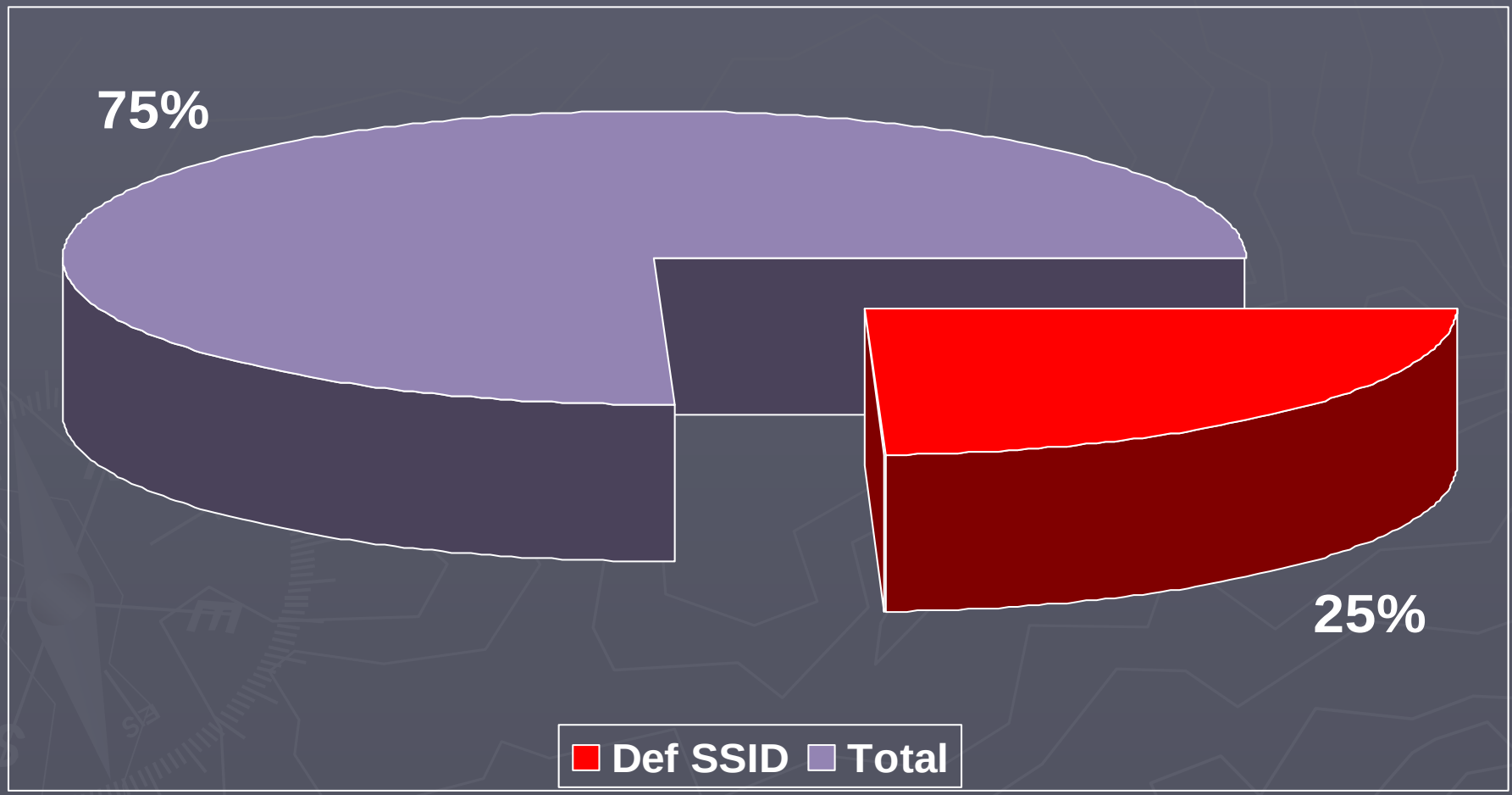
Non-Encrypted AP's



Default SSID



Default SSID w/No Encryption



Interesting SSIDs

- American_Financial
- AT&T Wireless
- Best Inn
- Flying J (Truck Stop)
- Georgia Education Articulation Committee (KSU)
- Hampton Inn
- Motorola
- Orange (Home Depot)
- Resurgens (Drs Office)
- SummitMG – Summit Marketing
- Truckstop.Net (Truck Stop)
- TurboChef - Atlanta – Headquarters
- ITOffice
- Leatherworld
- Arescom – Hotel Wifi Provider
- Board Room
- Upstairs
- Downstairs
- dscwireless – Wireless Alarm System
- fwatlanta
- GCCInternet – a Cartersville ISP
- GlobalSuiteWireless
- GUC – Gwinnett University Center
- GSBA - Georgia School Boards Association Inc
- mysis – Mysis Healthcare Systems

Results could be catastrophic

- ~ 46 APs available for nefarious use
- If only 10% of those are open, then the problem still exists
- Similar to a Submarine, leaving any hatch open, is a problem.

Incidents

- Lowes Wifi Hack
  - http://www.securityfocus.com/news/8835
  - A 20 and 21 yr old collected credit card #'s from the Parking lot... on an open WIFI network installed in the Southfield, Michigan Lowes.
- MAC Address Filtering at a Dr's. Office
  - http://www.rfklabs.com/community/viewtopic.php?t=5&sid=515486a668476ea6a8f02917e5d59256

Tools

- WEPCrack
  - http://sourceforge.net/projects/wepcrack/
- Wi-Foo – a comprehensive list of attack tools
  - http://www.wi-foo.com/index-3.html
- AirSnort
  - http://airsnort.shmoo.com/

Summary

- Open WiFi allows anonymous injection of threats into the internet with little recourse
- Open WiFi inside a corporation could be catastrophic to the company

Next Steps

- Education is key
  - Consumers need the education as well as corporate security
- White Papers and Solutions
- Secure by Default
  - Product Manufacturers need to enable security solutions in hardware