Wireless LANs, Best Practices Session One

David W. Borden, CISSP

Senior Systems Engineer

Lockheed Martin Corporation

david.borden@lackland.af.mil

dborden@gvtc.com

Who is David Borden?

- AA, BS, MS University of Maryland, University College, Graduate School of Management and Technology
- Performs daily on a DOD Contract where travel is performed to a DOD Site for the purpose of Computer System Vulnerability Assessment
- Emphasis: Build security into a system in the requirements and design phases vice after deployment (including Wireless)
- Has been a radio amateur for many years - good experience for wireless thinking

Agenda

I. Wireless LANs - An Introduction

- Session One - An Introduction and Basics
- Session Two -Best Practices with several case studies

II. Conclusions

III. References

IV. Questions

I. Wireless LANs - An Introduction

- You must become aware of wireless LANs in your purview
  - If you think you do not have any wireless, you better check
  - Your corporate data could be slipping over to your competition and you will never know
  - Basically innocent (but naive) employees could have installed wireless access

What is a Wireless LAN?

- A wireless LAN is a radio network connection
  - Usually consists of a Wireless Access Point (WAP) and a Wireless Client (often a PCMCIA card or USB device in a laptop, or CF card in PDA)
  - The WAP is usually connected to the corporate network; how it is connected is important.

How does a Wireless LAN differ from a Wired LAN?

- Wired LANs are physically protected from intrusion (equipment locked in closets)
- Wireless LANs are radio
  - Radio transceivers could be off the corporate campus (like Burger King)
  - If intruder remains passive (sniffing and saving corporate data), you may never know they are there (unless they use Net Stumbler)

A Short Wireless History

- FCC Michael Marcus opened three ISM Bands in 1985 (900 MHz, 2.4 GHz, 5.8 GHz)
- 1988 IEEE 802.11 Committee Started
- 1999 802.11b and 802.11a Standards Approved (400 pages)
- August 1999 six companies formed Wireless Ethernet Compatibility Alliance
- Name chosen was Wi-Fi (because it sounded like Hi-Fi) - later became "Wireless Fidelity"
- Wi-Fi did well because of home Broad Band (DSL and Cable)
- Fee based "Hot Spots" sprang up (some unintentional)
- May 2003 802.11g Approved (Fast 2.4 ghz)
- June 2003 802.11x Approved (EAP)
- Wi-Fi was improved to be "Wi-Fi Protected Alliance" (WPA)
- June 2004 802.11i Approved (Encryption improved with AES and IV fixed)
- Broadband is "real soon now"

What are the “Next Things”?

- WiMax
  - Wide-Area version of Wi-Fi
  - 70 mb throughput
  - Max range of 50km (30 miles)
- For home entertainment - WiMedia
  - 802.15.3
  - Short Range, High Capacity

IEEE Wireless Protocols

- 802.11a
- 802.11b
- 802.11g
- 802.11x
- 802.11i

802.11a

- Was promising, but range too short requiring more WAPs in each installation (at least double)
- 5 gHz band using ODFM
  - Multipath problems possible (more so on 5 gHz)
  - Interference is less than 802.11b
- 54 Mbs possible speed
- Decreased dry wall penetration from 802.1b (again - more WAPs needed)
- Twelve non overlapping channels allowed
  - Vendors currently supporting eight

802.11b

- 2.4 GHz ISM band using DSSS
  - Interference from microwave ovens, RF lights, cordless phones, burgler alarm systems
- Most popular currently because it is cheap
- 11 Mbps possible speed
- Dallas, TX Airport has a hot spot. Starbucks have hot spots - they are everywhere (the intended ones)
- Three non overlapping channels
  - Channel 1, Channel 6, Channel 11 in USA

802.11g

- Finally approved as a standard - May 2003
  - A/B/G hardware abundant to appear
- 54 Mbps max speed
- Older early adopters may get their hardware flashed to the new standard
- Dirty little secret is that if an 802.11g device sees any 802.11b traffic on the three channels, it lowers speed to 11 Mbs in order to be backward compatable
- Same frequencies as 802.11b
  - 2.4 GHz ISM band (thus interference likely)

802.1x

- Combines a port level access with authentication
- Client must first authenticate using Extensible Authentication Protocol (EAP)
- Types of EAP:
  - EAP SIM, EAP AKA, EAP SRP , EAP TLS, EAP TTLS, EAP GSS, LEAP, PEAP

802.1x (continued)

- EAP is defined in RFC 2284 (being revised after experience - RFC2284bis)
- So well suited to multi factor authentication
- Note: EAP provides no cryptographic protections (forged EAP-success?)
- 802.1x has no strong notion of a “session” and is weak

802.1x (continued)

- Authentication is normally done with a RADIUS server (RADIUS is Remote Authentication Dial In User Service) defined in RFC 2138
- Free RADIUS software is GPL or buy a RADIUS server
- RADIUS is vulnerable to the injection of forged requests in the right place
- Still a great protection, requires another user name and password before you can get on the WAP

802.11i

- Improved Security (RFC 2284BIS-08)
- Approved as a standard in June 2004
- Uses Temporal Key Integrity Protocol
  - TKIP (some call WPA)
- Advanced Encryption Standard (128 bit)
- Dictionary attack resistance but vulnerable to MITM
- Wiley hacker still sees level 2 maintenance frames
- IV vulnerability fixed (a big deal - great work)

802.11i (continued)

- Terms you need to read the reference:
  - Authentication Server (AS) - the RADIUS server
  - Access Point (AP) - we called this the WAP
  - Station (STA) - the client
  - Master Key (MK) - represents positive access decision
  - Pairwise Master Key (PMK) - authorization to access 802.11
  - Pairwise Transient Key (PTK) -Collection of operational keys
    - Key Confirmation (KCK) - binds PMK to AP, STA
    - Key Encryption (KEK) - used to distribute GTK
    - Temporal Key (PTK) - used to secure data traffic
  - Group Transient Key (GTK) - an operational key

802.11i (continued)

- Vendors planning September 2004 rollout (some a software in the AP replacement)
- IEEE documents still in the 100 dollar phase
- It will be some time before IEEE docs are free

BEST Documentation So Far

- Available on the Web, read the:
  - 802.11i Overview by Nancy Cam-Winget, Tim Moore, Dorothy Stanley, and Jesse Walker

The OSI Layered Model

- Wireless attacks come from Layer 1 and 2
- The OSI stack:
  - Layer 5: Application
  - Layer 6: Presentation
  - Layer 5: Session Layer
  - Layer 4: Transport Layer
  - Layer 3: Network Layer
  - Layer 2: Data Link Layer
  - Layer 1: Physical Layer

802.11b Modes

- Ad-Hoc (point to point)
- Infrastructure (point to multipoint) - also called Managed
- Repeater (range extension)
- Monitor (forgotten mode)

Device Modes

Managed - Wireless Client Card

Master - WAP Normal Mode

Repeater - WAP Repeats What It Hears

Ad-Hoc Mode

- Computers containing wireless hardware communicate with each other directly (no controller)
- All participants must be in RF range to communicate
- In a corporate community, you may not want this to be possible

Infrastructure (Managed) Mode

- All clients communicate with each other through a wireless access point (WAP)
- Clients must first authenticate and associate with a WAP before communication is possible
- You can deploy many supporting WAPs to increase coverage

Repeater

- Additional WAPs are deployed to extend range
- Additional WAPs communicate with each other to get the client's traffic to the eventual wire
- Each WAP can also have a wire - WAPs still communicate with each other

Monitor Mode

- Wireless PCMCIA cards may be placed in monitor mode where no transmission of RF energy occurs
- This mode allows sniffing of what is going on the wireless network while remaining silent
- Using free sniffing software (ethereal) all management frames may be seen
- Placing cards in monitor mode is best done using a UNIX computer
  - Two different monitor modes possible

Wireless Encryption

- 64 bit WEP (standard - lame)
- 128 bit WEP (not in specification - most popular)
- WPA is advanced encryption (uses Master Key and Session Key, Session Key is rotated frequently)
- 156 bit WEP (not in specification)

64 bit encryption

- Almost useless, step up to 128 bit encryption
- With 24 bit Initialization Vector (sent in the clear), there are actually only 40 bits of encryption
- May be easily broken by brute force
  - Tools available on the WWW

128 bit encryption

- With 24 bit Initialization Vector (IV sent in the clear), there are actually only 104 bits of encryption
- IV + WEP Key form the total key for one packets transmission
- IV selection is tricky (but mostly fixed now)
  - Must avoid 0x.. 0xFF 0x(<13)

Possible WEP Attacks

- Weak IVs (Fluher, Mantin, Shamir paper): Not any more -Older WAPs only
- Message Modification (change one bit,of cipher then redo the ICV)
- Arbaugh Inductive Attack (works on ICV - the checksum)
- Collision (key reuse) - Build decryption dictionaries keyed on IV
- Isolog (First bytes of encrypted frame are known - example: SNAP LLC Header)
  - Sometimes called the partial know plaintext attack or a crib (another example: Heil Hitler in Engima traffic)
- Known plaintext attack (feed in pings or UDP on wired side)
- Authentication Replay (gather challenge-response frames and replay)
- For those WAPs using passwords to generate key seed, use dictionary attack with John the Ripper rules
  - Probably can build dictionary of hex key seeds also (DA-DI-SA-BA-DB-05-54-AF-F0-0D) using standard substitutions (5=S 0=O 1=I 2=to 4=for) - Sometimes called the DE AD BEEF approach

War Driving, Walking, and Sitting

- Discovery is the first step to securing your network
- Remember war driving is legal, authentication/association and stealing service is not legal (unless it is encouraged - Seattle Wireless)
- While war driving is legal, driving in prohibited areas is not allowed and could get you shot) at some military bases
- In Windows, use Net Stumbler for hobby work (but you will miss WAPs properly configured and you will radiate)
- In Linux, use Kismet, host-ap drivers and PCMCIA combo card (802.11a, 802.11b, 802.11g) or USB device
  - Can get kismet CD that boots in your Windows laptop
- Use Kismet gpsmap" to generate WAP location map (Census Tiger Maps work well in United States)

War Driving History

- Ken Poulsen made popular the discovery of Wireless Access Points by driving around and RF sniffing (called“War Driving” in 2001). This term was coined after the “War Dialing” history of modem access to networks (from the movie War Games)
- War Dialing is still an essential part of any network assessment (discover rogue wire modems)
- War Driving is also an essential part of any network assessment (discover rogue access points)
- War Driving is now a hobby for some people
- Web sites exist with war driving maps posted

War Driving - Net Stumbler

- Popular Windows Operating System software is “Net Stumbler”
  - Uses Wireless Network cards with Lucent Chip Set
  - Lucent chip set cannot be placed in promiscuous mode, thus wireless management packets are not visible
  - Net Stumbler will miss any Wireless Access Point with a non existent (blank) SID or a SID consisting of only space characters “ “
  - Net Stumbler is not useful in network assessment

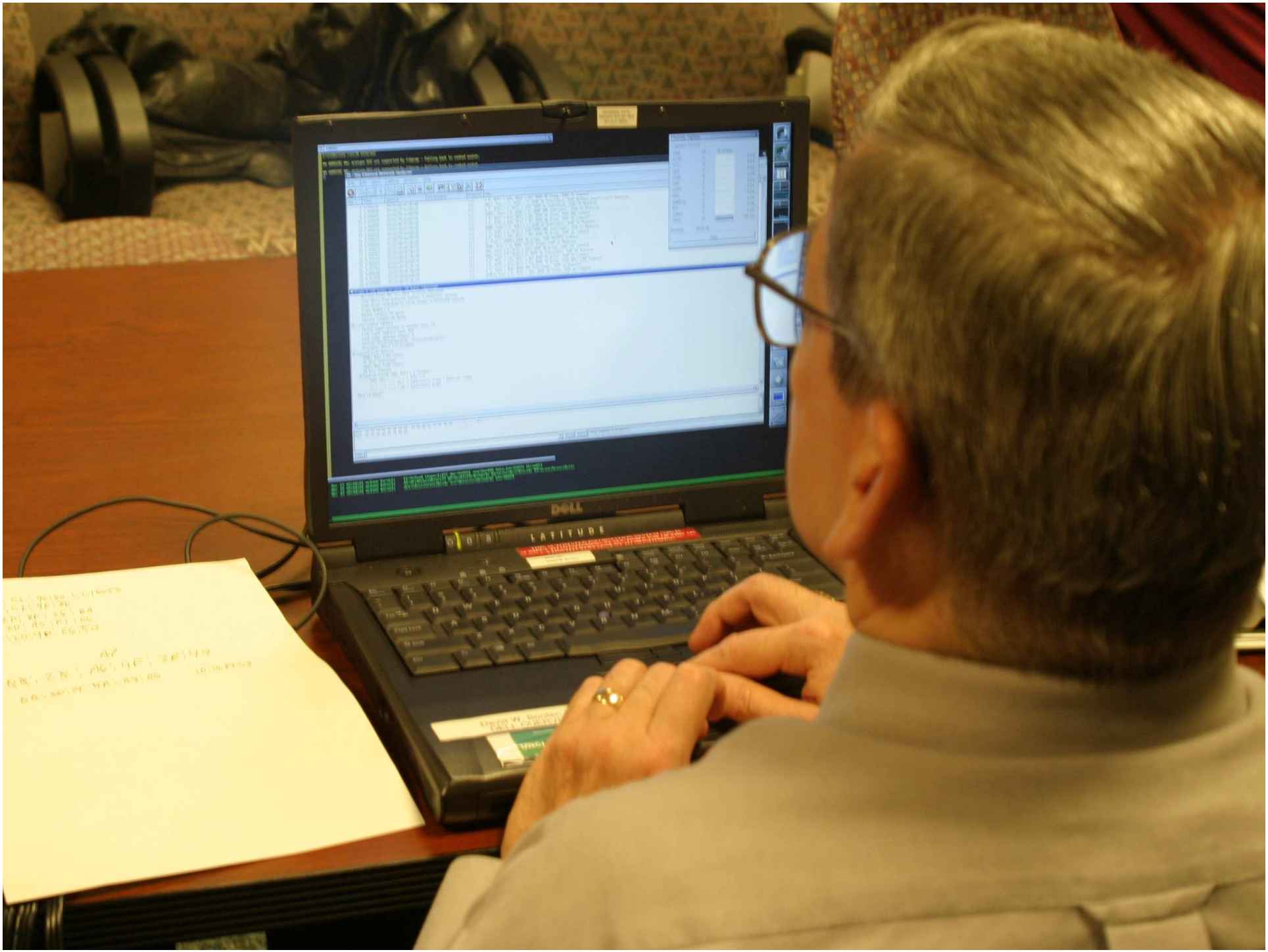
War Driving - GPSDRIVE

War Driving Antennas

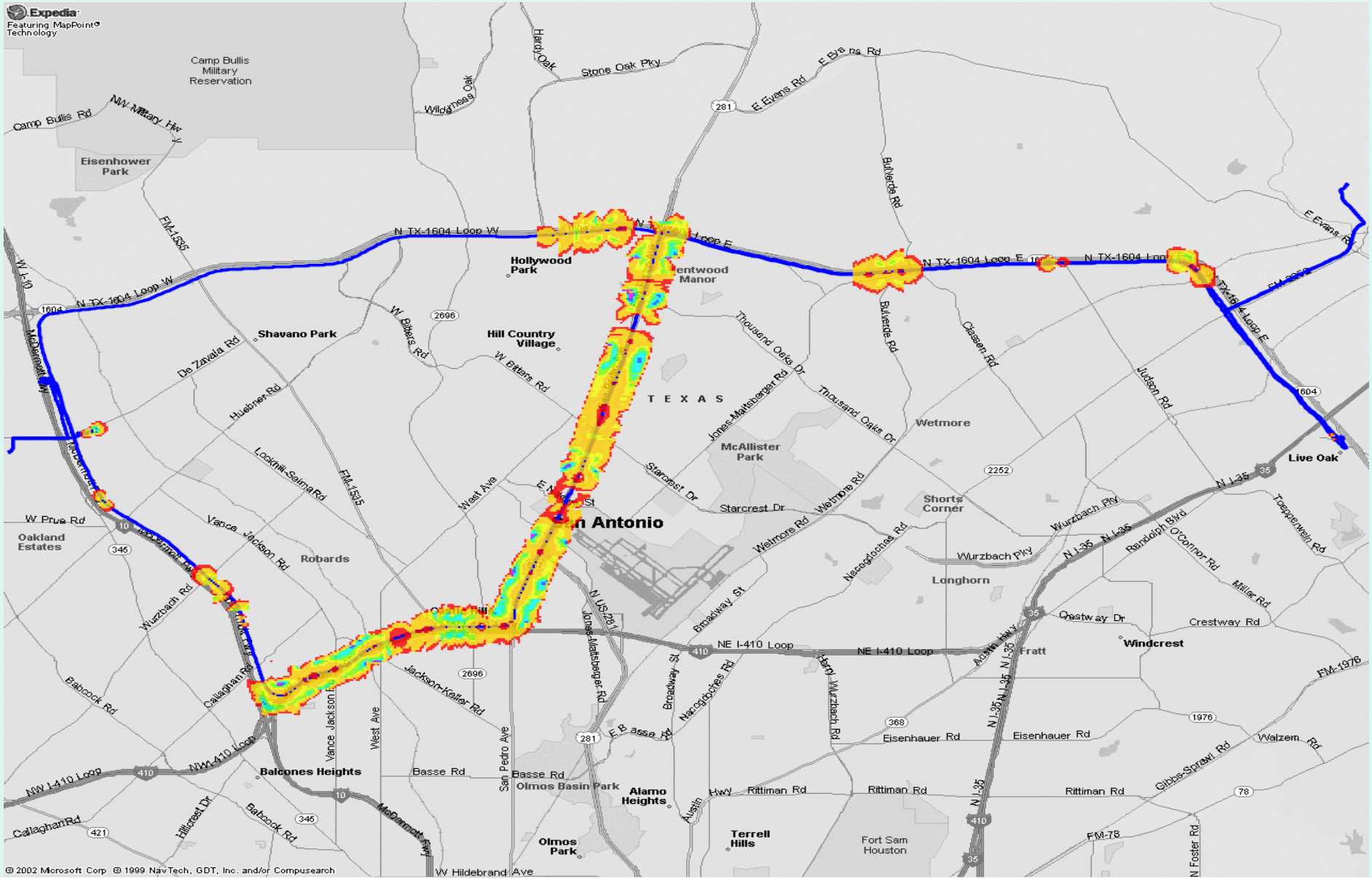
War Driving Devices

War Driving - Geolocation

My Invention - War Sitting


DELL
LATITUDE

Typical War Driving Map



Mapping

- Best for analysis is a center dot for each WAP and label with BSSID (MAC address of the WAP)
- Can use radius plot
  - Looks like a bunch of circles, but each circle is an attempt to show how far away WAP can be accessed
- Can use distributed power plot
  - This attempts to show falloff of WAP power (strong near emitter, weaker the further away you go)

WLAN Vulnerabilities

- There are many ways
- Rogue Client used by intruder to steal network access
- Rogue Access Point used by trusted employee (unknown to IT department)
  - Rogue Access Point established by hacker (requires MAC spoof and host-ap)
  - Man in the middle attack (disassociation by same channel rogue access point, grab real client to another rogue access point (at least 3 channels away, then setup rogue client to real access point)

WLAN Vulnerabilities (cont)

- More Ways:
  - OSI Level 2 attack using ARP
  - WEP Cracking (previously mentioned) followed by Authentication & Association or just listening
  - Denial of Service (broadcast disassociation of all clients or high power RF attack or authentication response spoof flooding)
  - Traffic injection (useful for bad stuff detector spoofing)

WLAN Intrusion Detection Devices

- From the wireless side
  - Detect rogue access points (using DF)
  - Detect rogue clients, access points, stumblers (using DF)
  - Best is to deny rogue hookup by linking detector to the access point and use geolocation mechanism (more later)
- From the wired side
  - Know allowed MAC addresses, alarm on others
  - Should alarm on ARP storm or ARP cache poison (look in cache for several entries for the same MAC)
  - Possible to use free program “arpwatch”

Risk

- Perform risk assessment before any wireless installation, home, or enterprise
- If the data being passed is private, proprietary, or sensitive - employ additional encryption
- If an enterprise, employ an intrusion detection system (this means you have to read the logs or employ a software agent to read them)
- Much more of this next session when we examine best practices and case studies

Session One, Questions

?