# Wireless:
# The good, the bad, & the ugly

Timothy G. O'Brien, NSA-IAM

Publicity & Social activities chairperson, Omaha Linux User's Group (OLUG)
Information Technology Manager, Thomas Power Library, Offutt AFB
Consultant

# Disclaimer

This presentation is intended for the attendees and may contain information that is privileged or unsuitable for overly sensitive persons with low self-esteem, no sense of humor, or irrational religious/political beliefs. Those of you with an overwhelming fear of the unknown will be gratified to learn that there is no intended hidden message revealed by reading this warning backwards, so just ignore that Alert Notice from Micro$oft. However, by pouring a complete circle of salt around yourself and your computer, you can ensure that no harm will befall you or your pets. Your mileage & satisfaction may vary, not all warranties apply during all time frames. Confirm these statements with your leadership before approval & implementation.

No individuals or equipment were harmed while producing this presentation, but it was created with recycled electrons. No animals were harmed in the transmission of this email, although if the raccoons keep getting into the trash I may have to do something about it. No individual, organization, or entity can be held liable or be quoted without written consent of the presenter.

I speak for no one, no one speaks for me

# Scope & Aims

- A 'volunteer' presentation on wireless and local implications for the attendees of the November 2003 CSF
- Raise the awareness of the good & bad around wireless
- Detail some suggestions & benchmarks for deployment that I found on the WWW & publications
- You will be able to determine the good, the bad, & the ugly

# Why wireless?

- Mobility
- Convenience
  - Ease, speed, & simplicity of setup
  - Does not equal secure
- Increased productivity
- Network access to areas that wires can not

# Why not wireless?

- Limited range
  - Usually to a floor of a house/building
- Limited number of concurrent users
- Limited/lack of security
- Limited product/availability for some types
- Something bigger/better coming down the road

# Types of Wireless

- Infrared
- 900 Mhz
- HomeRF
- 802.15 WPAN/Bluetooth
- WiFi – 802.11
- Not here yet, will not cover today
  - Digital Cell phone (2.5G/3G)
  - 802.16 Broadband Wireless

# Infrared - IR

- The first & most basic
  - 10 foot range, line of sight
  - 4 Mbps
- Used for
  - Remote controls
  - Synchronize data
  - Beam small amounts of data between PDA/Cell phone
  - Printer access for small devices
- Never really caught on

# 900 Mhz

Broadband Wireless
Cordless Telephones
low power video transmitter
X-cams?

# HomeRF

*The Home Radio Frequency Working Group developed a single specification (Shared Wireless Access Protocol-SWAP) for a broad range of inter operable consumer devices. SWAP is an open industry specification that allows PCs, peripherals, cordless telephones and other consumer devices to share and communicate voice and data in and around the home without the complication and expense of running new wires. The SWAP specification provides low cost voice and data communications in the 2.4GHz ISM band.*

http://www.palowireless.com/homerf/about.asp

*For wireless networks in homes - in contrast to 802.11, which was created for use in businesses.*

http://wi-fiplanet.webopedia.com/TERM/h/HomeRF.html

# 802.15 WPAN/Bluetooth

- Generally short range, pico networks or personal data clouds
- 802.15.1 = Bluetooth or WPAN
  - Short run cable replacement
    - 2.4GHz, 30 Ft range, with a theoretical 720 Kbps throughput
  - Wireless Personal Area Networks (WPAN)
    - IEEE trademark name
  - Bluetooth
    - Ericsson trademark name

# 802.15 WPAN/Bluetooth spamming

- Bluejacking
  - Phone owners leave Bluetooth switched on
    - Meaning that anyone within range can send a short message
    - Right now this is being done by pranksters
    - But one can't help wondering, how long before spammers

# 802.15 WPAN/Bluetooth

- 802.15.3a = Ultra Wide Band (UWB)
  - High speed using pulse radio all over the spectrum
  - Controversial, possible interference
  - Not clear on purpose or use from research

# WiFi - 802.11

- Can be the
  - Family of 802.11 technologies
  - Original 802.11 specification by the IEEE in 1997
    - (1 or 2 Mbps)
- WiFi = Wireless Fidelity
- Wireless LAN = Radio network connection
- WLAN = Wireless LAN

# WiFi terms

- Usually consists of a Wireless Access Point (WAP) & Wireless client (PCMCIA card & laptop/PDA)
  - WAP usually connected to the LAN
  - How the WAP is connected to LAN is important
- SSIDs
  - 'network name'
  - SSID on client & AP must match
  - SSIDs are broadcast by the AP
    - normally every 1000ms in beacons

# WiFi Encryption

- 64 bit WEP
- 128 bit WEP
- 156 bit WEP
  - Not in standard?

# WiFi Encryption – 64 bit

- Has a 24 bit initialization vector
  - Initialization vector sent in the clear
  - Leaves a 40 bit encryption
  - Easily broken by brute force
    - Tools available on Internet

# WiFi Encryption – 128 bit

- Has a 24 bit initialization vector
  - Initialization vector sent in the clear
  - Leaves a 104 bit encryption
  - Easily broken by brute force
    - Tools available on Internet

# 802.11

| Wireless standard | 802.11a | 802.11b | 802.11g |
|---|---|---|---|
| Max Mbps data rate | 54 Mbps | 11 Mbps | 54 Mpbs |
| Modulation Type | ODFM | CCK | CCK and ODFM |
| Supported Data Rates | 6, 9, 12, 18, 24, 36, 48, 54 Mbps | 1, 2, 5.5, 11 Mbps | OFDM: 6, 9, 12, 18, 24, 36, 48, 54 Mbps<br>CCK: 1, 2, 5.5, 11 M |
| Frequencies | 5.15–5.35 GHz<br>5.425–5.675 GHz<br>5.725–5.875 GHz | 2.4–2.497 GHz | 2.4–2.497 GHz |
| Encryption | 64, 128, 152 bit | 64 & 128 bit | 64 & 128 bit |
| Compatibility | Only 802.11a | Only 802.11b | 802.11a & 802.1 |
| Max Distance | 600 Meters | 300 Meters | 300 Meters |
| Hotspots | Few | Many | Few (so far) |

# 802.11a

- 5 gHz band using Orthogonal Frequency Division Multiplexing (ODFM)
  - Less interference than with 802.11b
  - Possible multi path problems
- 54 Mbs theoretical speed
- Decreased range from 802.11b
- 12 non-overlapping channels
  - One source list that vendors currently only support 8

# 802.11b

- 2.4 Ghz ISM band using direct-sequence spread spectrum (DSSS)
  - Interference from microwave ovens & lights using RF frequencies
- 11 Mbps possible speed
- Three non-overlapping channels
  - Channel 1, 6, & 11 (in USA)
- Most popular – it is all over the place

# 802.11b modes

- 802.11b has three different modes
  - Ad-Hoc
    - point to point
  - Infrastructure
    - point to multi point
  - Monitor
    - The lost mode

# 802.11b Ad-Hoc mode

- PC or PDA containing wireless hardware communicating directly
  - No controller or access point
- All must be within range
- Might not be a good idea for corporate or sensitive environments

# 802.11b Infrastructure mode

- PC or PDA containing wireless hardware communicating through a WAP
- Clients must first authenticate & associate with a WAP
- Deploy as many WAPs as needed for adequate coverage

# 802.11b Monitor mode

- WiFi PC card may be placed in monitor mode where no RF transmissions occurs
  - Allows for WLAN sniffing while remaining silent
  - Ethereal

# 802.11g

- Same frequencies as 802.11b
  - 2.4 Ghz ISM band
    - What about interference between B & G?
- 54 Mbps max speed
- Recently approved standard (May 2003)
- 802.11A/B/G hardware starting to appear
- Older early adapters may get flash upgrades to the approved standard

# 802.11e

- Quality of Service (QoS)
- Applications set delivery priority of specific data types
  - Some having precedence over others
- Packet bursting
  - Better performance in mixed client environment
    - 802.11b & 802.11g present in the same segment/cell
- Critical for WiFi & streaming media

# Some security risks

- Packet capture & analysis
- Network mapping
- Target profiling & identification
- Information capture / theft (identity theft)
- Denial of service (DoS)
- Peer to peer
- Social Engineering
- Unauthorized access /control from remote locations
- Rogue WAPs

# WiFi security problems

- WiFi security was flawed from the design stage
  - Wired Equivalent Privacy (WEP)
    - (the link encryption mechanism) used by 802.11b was cracked in the lab within hours, then within 15 minutes
    - Can now use AirSnort or WEPCrack
    - Management of WEP keys can be challenging
- Numerous reports on Slashdot and even mainstream news sources on WiFi deployment security problems
  - Best Buy WiFi PoS (May 2002)

# Denial of Service

- WiFi is extremely vulnerable to DoS attacks
- 2.4 Ghz frequency range used by 802.11b is very susceptible to interference by cordless phones & microwaves
- White noise generators work great
  - DEFCON 11 (August 2003)

# Signal propagation

- Signals from the AP's & clients travel, and travel farther than we think
  - Through walls, ceilings, & furniture
- Propagation can be controlled by
  - Antennae selection & type
  - Antennae placement
  - Signal strength (of AP and by client WiFi card)

# Passive data collection

- With an intruder remaining passive & out of sight, sniffing & saving data; you may never know they are there

# WiFi war driving

- War driving is legal
  - Theft of services is not
  - Unauthorized access is not
  - authentication/association is grey area
    - Win2K & XP automatic association to open WAPs
- War driving to see first hand and possibly document the extent of WiFi & poor deployments
- Reasonable cost for basic setup
- Using laptop or PDA

# According to the FBI

*“It is not illegal to scan, but once a theft of service, denial of service, or theft of information occurs, then it becomes a Federal violation through 18USC1030. The FBI does not have a web site with this sort of information. You either need to pose the question to us or a cyber crime attorney (or our US Attorney's office).”*

From DEFCON 11 program

# Sioux City war drive

- Hosted by the Sioux City Linux Users Group
  - http://sclinux.org/
- Held on the afternoon of 8 November 2003
- Equipment used was
  - Standard Gateway laptop
  - Knoppix STD bootable CD-ROM
  - Using Kismet, saving logs to hard drive
  - Various antennae & cantennae, no GPS

# Sioux City war drive

- Three teams covered the Sioux City metro area
- In 1.5 hours
  - TEAM 1 APs Found : 227 Unique APs: 78
  - TEAM 2 APs Found : 339 Unique APs: 85
  - TEAM 3 APs Found : 437 Unique APs: 161
- Total of 1003 AP's found
- A total of unique APs: 324

# War driving in Omaha

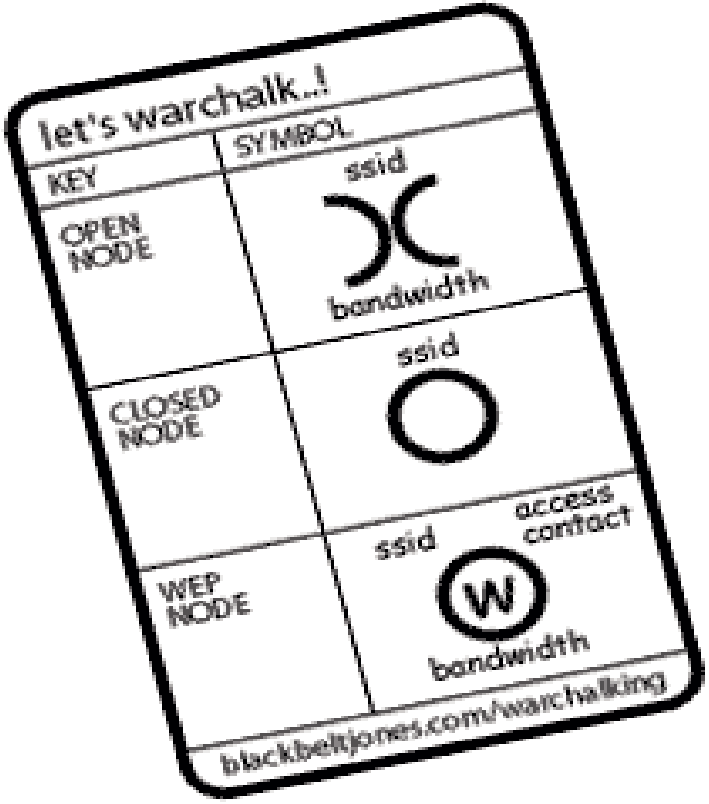
- Typically 'find' around 100 AP's an hour
  - Depending on the part of town
- Most are default settings
  - Tsunami, Linksys
- No problem finding open access points
- Interesting to find the same AP downtown during the day to show up in West Omaha at night

# Where WiFi is used / found

- Similar results in Omaha as other cites
  - Apartment buildings
  - 'Nicer' parts of town, individuals with expendable funds
    - College students
    - Information Technology workers (working at home?)
  - Coffee shops
  - City centers / business districts
  - Large warehouse type buildings

# War chalking

- The practice of marking a series of symbols (similar to hobo marks) on sidewalks and walls to indicate nearby wireless access.
- Have you seen it?
  - I did not think so.



# Simple measures to take

- Use directional/best antennae for situation
- Minimize WiFi broadcasts outside your needed area
  - Aim towards the inside of the building
  - Adjust transmitter power keeping signal inside
  - Adjust gain keeping reception inside
  - Test signals from inside & out to determine effectiveness
- Change the default settings

# Simple measures to take

- Use authentication mechanisms
- Segment WLAN from LAN
  - Using firewalls & VPN
- Only allow WiFi traffic to use specific protocols
- Disable DHCP, & use static IPs for clients
- Ensure equipment firmware is up to date
- Client MAC Address filtering

# Simple measures to take

- Do not forget the client!
  - Access points & clients are vulnerable
    - Attackers can & will go after the clients
  - Keep systems up to date with patches
  - Make sure the clients are hardened
    - Install on clients protection
      - Anti-Virus
      - Personal Firewall
      - IDS
    - Turn off file & print sharing

# WiFi Authentication mechanisms

- 802.1X (currently available)
  - Provides a conduit through which authentication credentials can pass
  - Extensible Authentication Protocol (EAP) over LAN/WLAN
    - But you decide on a specific type (TLD, TTLS, LEAP, PEAP)
  - Typically uses a Remote Authentication Dial-In User Service (RADIUS) server
    - RADIUS used to provide centralized authentication, authorization, and accounting for dial-up, VPN, & WLAN access.
    - Also handling key distribution
  - Protocol supposedly written by Microsoft & Enterasys

# WiFi Authentication mechanisms

- 802.11i
  - Standard is still being ratified (2004?)
    - IEEE's solution to security problems
    - Advanced Encryption Standard (AES)
    - Supposed improved security (RFC 2284BIS-08)
      - Dictionary attack resistance
      - But vulnerable to man in the middle attacks

# WiFi Authentication mechanisms

- 802.11i
  - Comprised of two primary components
    - Robust Security Network (RSN)
      - Provides authentication component
    - WiFi Protected Access (WPA)
      - Provides encryption component
      - WiFI Alliance's 'tactical security standard'

# WiFi Authentication mechanisms WiFi Protected Access (WPA)

- Supposedly designed to address the WEP security weaknesses
- Supposedly harder to crack by increased key size & life
- Generates & distributes encryption keys automatically
  - Temporal Key Integrity Protocol (TKIP)
    - Called the next generation WEP
    - Available via firmware upgrade to many products
- Integrity check on the header

# WiFi Authentication mechanisms WiFi Protected Access (WPA)

- Can be implemented in two ways
  - Enterprise mode
    - Using 802.1X & RADIUS server
  - Home mode
    - Uses Pre-shared keys (PSK)
- Already perceived problems and insecurity
  - The interface for choosing consumer passwords makes it simple to snarf a tiny bit of network traffic and perform an offline dictionary attack
    - Choose a longer key or invent 20 characters of gibberish.

# Virtual Private Networks (VPN)

- Provides end to end encryption
- In many cases has enterprise level authentication
- VPNs typically use protocols such as IPSec, SSL, L2TP, & PPTP
- Idea: use WPA & VPN together, creating a strong security barrier on your WLAN
  - Added complexity & cost, troubleshooting issues

# Simple measures to take
# Policies, standards & procedures

- The first step to take
- Determine your customers needs
- Determine your management needs & political issues
- Define high level WLAN policies
  - Who can install APs
  - Who can use APs
  - Who can have access to the WLAN?
  - What applications & protocols can be used?

# Simple measures to take
# Policies, standards & procedures

- What standards will be used?
  - 802.11a, 802.11b, 802.11g; or a mixed environment?
  - Only WEP, or WPA?
  - Which mode of WPA (Enterprise or Home)?
  - VPN implementation as well?

# Simple measures to take Policies, standards & procedures

- Investigate & choose the optimal technology combinations to meet your requirements
- Develop a well planned out WLAN design
  - Include any and all solutions for
    - Technology components
    - Customer & management needs
    - Political issues
    - Security & management complexities
- Implement & Test
- Educate

# Policies, standards & procedures Educate

- End users
  - Security awareness, policies
  - Remove WiFi card if working off line
  - Use digital signatures & encryption with e-mail
  - How to use & proper use of WiFi
    - only connect to known APs
    - No 'ad-hoc' connections
    - Using hot spots securely

# Policies, standards & procedures Educate

- Help desk
  - Same as end users
  - Troubleshooting authentication issues

# Policies, standards & procedures Educate

- Network & System Admins
  - Same as end users
  - Admin policies & procedures
  - Not installing rogue APs
  - How to securely deploy APs and clients

# Policies, standards & procedures Educate

- Security & Information/Network Assurance folks
  - Testing for rogue Access points
  - Reviewing configurations and settings for policy compliance/enforcement

# Simple measure to take
# Monitor your network

- Monitor for AP's using commercial or Open Source solutions
  - Commercial products cost $3K to $7K
    - Solution overkill?
- Conduct periodic site surveys & assessments

# Simple measure to take
# Change the default settings

- SSID
- Broadcast Channel
- SNMP community name
- Disable SSID broadcast/beacons
- Default password
- Enable MAC address filtering
- Enable Encryption (WEP or WPA)
- Configure single (g) or mixed mode (b/g) for 802.11g
- Disable ad-hoc (P2P) mode

# Simple measure to take
# Change the default settings

- To make setup easy as possible, manufacturers ship products with all security turned off
  - Out of the box = unprotected

# Final thoughts

- There is a plethora of information out there on WiFi
  - The problem is getting through it all
  - Web sites, formal training/classes, books
  - http://omahawireless.unomaha.edu/
  - http://wifi.meetup.com/
- WiFi users = 'remote' users?
  - Treat them as the same

# Final thoughts

- Do not be some of the many 'low hanging fruit'
  - Yes, at least use WEP
- WiFi can have significant ROI if done correctly
- Do you know your WiFi environment at all times?
- Technology is quickly changing
  - 802.11n IEEE proposal 100 – 320 Mbps, 2005 - '06

# Final thoughts

- Mix & match products from any & all vendors?
- Need advanced features, functionality, & ultra high reliability?
  - then you are on the higher end of the market
- 802.11a products are supposedly in limited selection
- 802.11a, b, or g for home?? Go with 802.11g
  - Best balance of price, performance, & compatibility
    - Close to the performance of a, but the compatibility of b

# Shameless plug #1

A free showing of the independent film REVOLUTION OS by J.T.S. Moore on Wednesday November 19th, 2003 (tonight), hosted by the UNO ACM.

The film will start at 8:30pm in the Peter Kiewit Institute Room 279, which is just on the southwest corner of the 67th and Pacific Street intersection (south of Elmwood park)in Omaha, Nebraska.

# Shameless plug #2

Linux Install Fest

Saturday, January 17th, 2004
12 pm to 6 pm
AIM/Clarkson College - 44th and Douglas

www.olug.org