Wireless Security

Thoughts on Risks and Solutions (or just an Oxymoron?)

Kenneth Newman

Disclaimer: Designed to provoke discussion. May raise more questions than answers.

What is ‘Wireless’?

- ‘Wireless’ can include:
  - Bluetooth
  - Infrared (IrDA)
  - 2G
  - 3G
  - CDPD
  - CDMA
  - TDMA
  - GSM
  - GPRS
  - GPS
  - PCS
  - SMR
  - SMS
  - WAP
- ‘Wireless’ in this presentation is:
  - 802.11 (often called Wi-Fi: www.wi-fi.com)
  - Note: this spec only covers ‘b’ w/ 40-bit WEP
  - IEEE: standards.ieee.org/getieee802/802.11.html

Why Should it Be Secure?

- Retail
  - Point-of-sale, inventory
- Manufacturing
  - Distribution, telemetry, inventory
- Health care
  - Patient records, surgery, location tracking
- Legal
  - Depositions, discovery, trial prep, court room

Who Thinks it May Not Be Secure?

- The Pentagon
  - Instituted a ban on wireless networking
- The Secret Service
  - Performing wireless scans in DC and other areas
- Retailers
  - Best Buy, Home Depot, Barnes & Noble, etc.
- Academia
  - Found WEP/802.1x flaws (UC Berkeley, U MD, etc.)

Recent Quotes

To paraphrase one reviewer's comment on a wireless security book:

"Wireless security is like safe skydiving - if you want the safety and security, just *don't* do it."

To paraphrase a representative of a large network infrastructure provider :

"Wireless is like having an RJ45 *in your parking lot*."

Presentation Overview

- “This Means War!”
- Statistics
- Technical Risks
- Organizational Risks
- Solutions?

“This Means War…!”

- …Chalking (AltaVista found 2,139 results)
  - www.warchalking.org
- …Driving (815 results)
  - www.wardriving.com, wardriver.staticusers.net (advertising signs?)
- …Walking (22 results)
  - Increasing PDA availability: Toshiba e740, iPaq 5000, Tablet
  - Equipment easily concealed under clothing
  - http://www.defect.org/ipaq/

“This Means War…!” II

- …Flying/Storming (12 results)
  - http://arstechnica.com/wankerdesk/3q02/warflying-1.html (San Diego)
  - http://www.e3.com.au/stories.php?story=02/08/18/7667279 (Perth)
  - Strong signals at 1500’ w/ basic equipment
- …Spamming (1 result)
  - http://news.zdnet.co.uk/story/0,,t269-s2121857,00.html
  - Mass mailing against an open SMTP port
- …DDOS Zombies (No results, yet!)
- WorldWide WarDrive 26 Oct – 2 Nov 02
  - www.worldwidewardrive.org, www.godsmoke.com/wireless/wardrive

Statistics

- Standing: By my apartment window
  - 12 APs in 5 min., 6 defaults, 3 WEP
- Walking: Wall/Water/Broad Streets
  - 150+ APs in 20 min.
- Driving/Reading: ‘2600’ (19:2, Summer 02 issue)
  - 448 APs in 90 min., 75 defaults, 26% WEP
  - Web browsing, e-mail, IRC, and IM sessions
  - 33 B&N purchases 7Jun02 5:00-6:00 PM

More Statistics

- Driving/Sniffing: Def Con X, Las Vegas
  - 1st Annual Wardriving Contest
    - Winning team identified 1804 APs within 72 hrs
  - 2 hours traffic monitoring (www.airdefense.net/eNewsletter/defconx.shtm)
    - 807 attacks (10 new types) and 35 rogue APs
- Flying:
  - 437 APs , 60% default SSID*, 23% WEP
  - 100+ APs, scanning logs (no dump) on web site

Even More Statistics

- LanJacking and WarDriving, San Fran
  - www.dis.org/filez/#shipley
  - Most internally connected
  - 60% default configuration
  - 15% using WEP, 7% using WEP with a default key
- First WorldWide WarDrive 31 Aug – 7 Sep 02
  - 9374 APs, 30% WEP, 27% no WEP and default SSID
- Commuting: LIRR, 66 APs reported one morning
- On average approximately 50% default and 25% WEP

Technical Risks

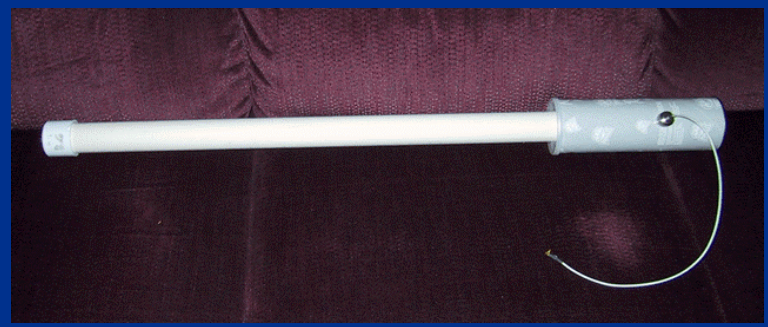
- Completely insecure vendor defaults
  - No WEP enabled, weak default SSIDs/passwords*, etc.
- Native security mechanisms alone limited
  - MAC filters, disable ‘beaconing’ (SSID broadcast), etc.
- Availability of scanning tools to identify APs
- Weak, device-only authentication
  - WEP/MAC/SSID subject to spoofing & MITM attacks

More Technical Risks

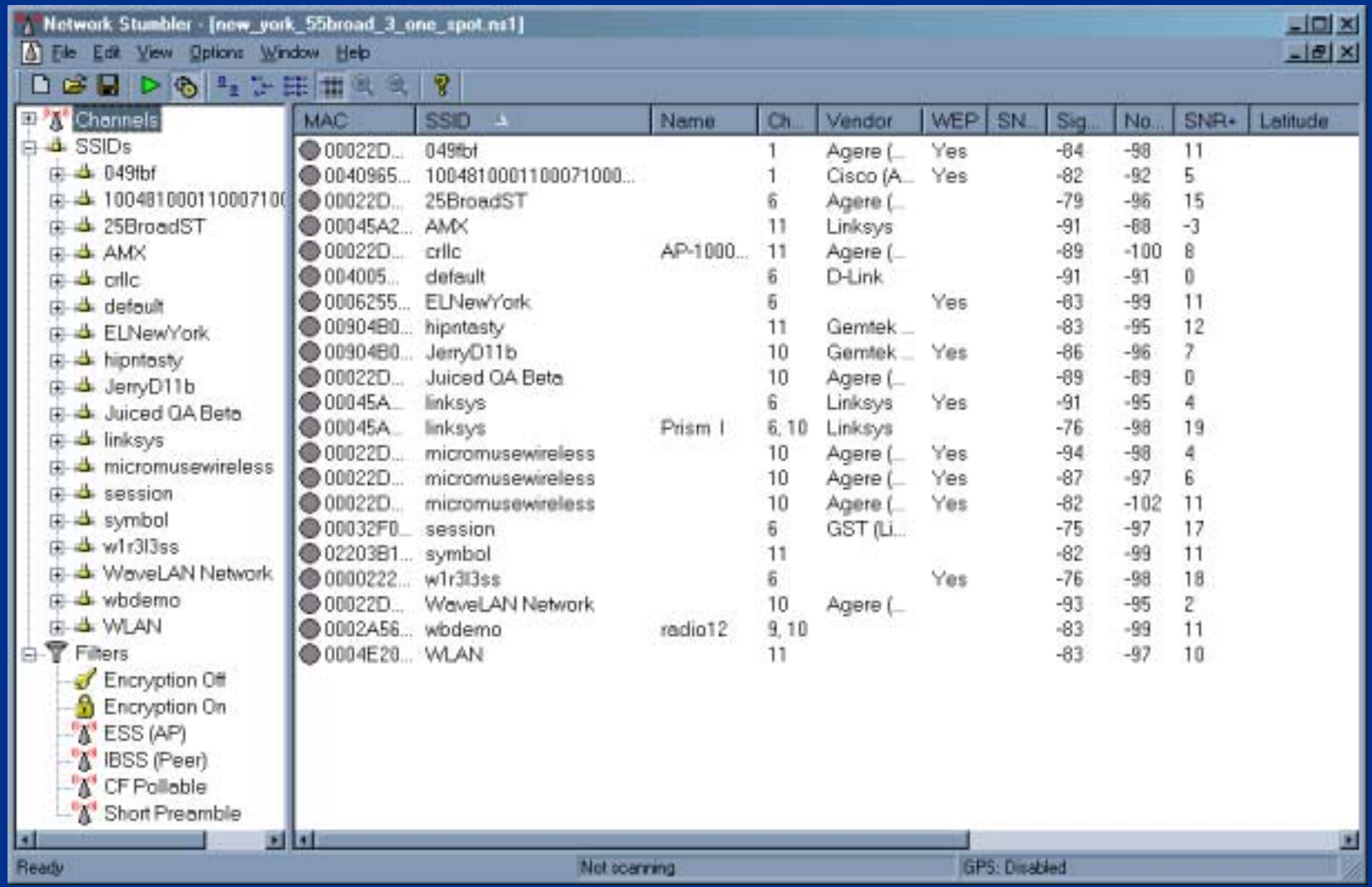
- "Less greasy chips"
  - or "From Pringles cans to PVC pipes"
  - http://www.oreillynet.com/cs/weblog/view/wlg/448/
- The Accidental Tourist "Is there a wireless network…"
  - Broadcast ("ANY") or null ESSID
  - http://www.techtv.com/screensavers/wirelessandmobiletips/story/0,24330,2185567,00.html
- 2.4 GHz cordless phone/microwave or 'Omerta' DOS
  - DOS trivial since disassociation is single, unauthenticated frame
- Passive sniffing (management/data frames) undetectable
  - Kismet, unlike Netstumbler, can be very quiet

Even More Technical Risks

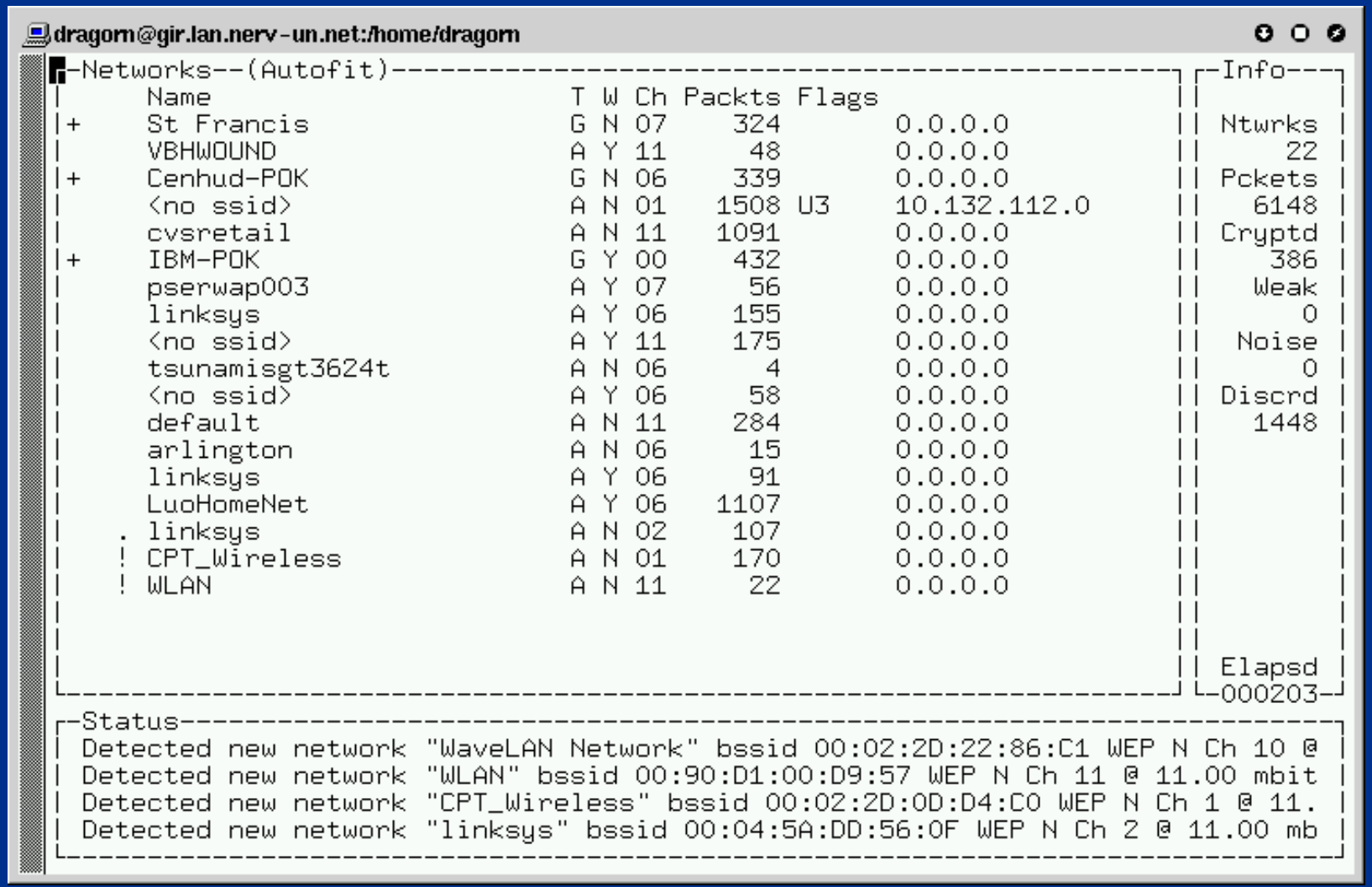
- Once associated, all traditional attacks apply
- Free HotSpots (opportunity for anonymous attacks)
  - http://www.nycwireless.net (Bowling Green, Rector Place)
  - Starbucks ($)
  - Hotels
  - Airports
  - Convention Centers
- AP power and signal 'bleed'
  - "I can see for miles and miles and miles and miles…"



Technical Risks: Tools: Netstumbler



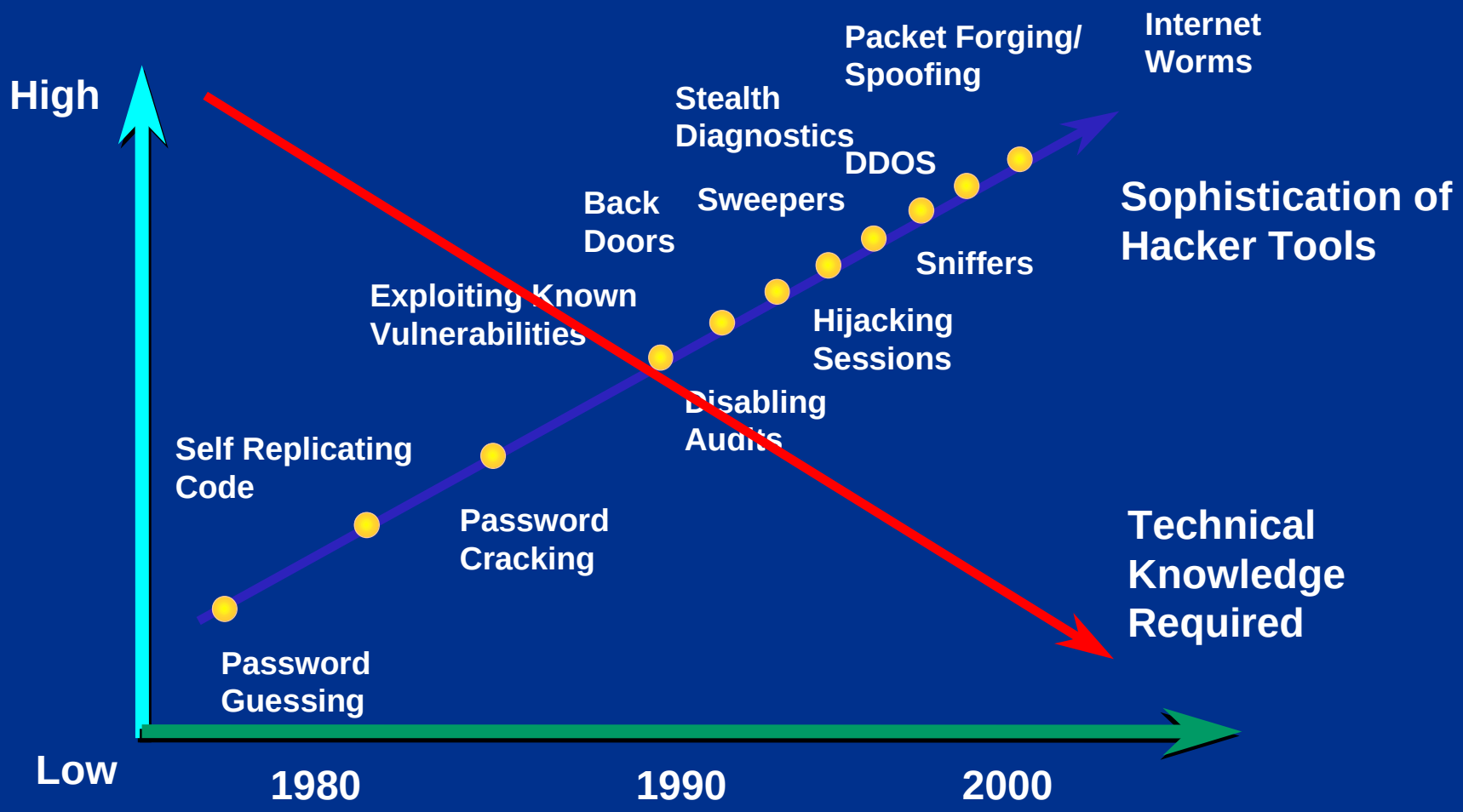
Technical Risks: Tools: Kismet



Technical Risks: WEP

- Short (24 bit) IVs cause key stream to repeat
- Weak (40 bit on older cards) crypto allowing brute forcing
- Shared keys w/out regular auto update
- Flawed RC4 model allowing key recovery
- Only data encrypted and not management traffic
- No mutual authentication to protect from rogue APs
- “But does it still serve a purpose?”

Technical Risks: General



Graph: Cisco, Inc.

Organizational Risks

- Staff have motive, means, and opportunity
  - Retail availability: JR Computers, CompUSA, etc.
  - Very low cost: under $50 for some cards (which can act as APs)
  - Ease of implementation: plug and play (again, insecure defaults)
  - Embedded in many new laptops (and PDAs/Tablets)
  - Difficult and time consuming to centrally detect
- Very broad (or 'Board') acceptance
  - Cool and exciting technology everyone wants
  - Mobility can lead to increased productivity/ROI ('Corridor Warriors')
  - Staff may already be using it on the road (hotel, airport, convention)
  - It may already be in your CEO/COO/CIO's office…

More Organizational Risks

- Inadvertent roaming to a stronger AP
  - Easy in densely populated urban areas
  - Your data could be crossing someone else's network (or visa versa)
    - Collaborators, clients, and competitors
- Information Leakage thru SSIDs and other fields
  - Company, group, or location names are a bad idea
- Scalability and consistency
  - Difficult to deploy securely across enterprise without effort ($$$)
- Lost/stolen devices expose WEP key(s)

Solutions?

- Establish wireless policies/AP configuration standards**
  - Along with all the other policies and standards you already have
- Harden PCs/laptops with wireless interfaces
  - Personal firewalls
  - Sector level encryption
  - Current Anti-Virus software and definitions
  - Apply updates/patches regularly
  - Prevent simultaneous wireless/wired connections
  - Host-based IDS?

More Solutions?

- Perform regular wireless scans/assessments
  - Leverage the same tools and devices as the attackers
    - What can you detect, associate to, access and how far away?
    - Confirm your polices and configuration standards are in place
  - Track databases: www.netstumbler.com/query.php, www.wigle.net
  - Detect ‘rogue’ APs violating your policies and standards
    - Monitor MAC address changes (particularly for know ranges)
    - Partner w/PhysSec for visual ‘sweeps’ and nightly ‘cart stumbling’
    - Vendor solutions: Isomair, AirDefense, and AirMagnet

Even More $olutions?

- Connect APs to your network externally
  - firewall DMZ and application proxy controls
  - Limit types of applications/data (by useful life) made available
  - N-IDS, anomaly, malicious code, and virus protection
- Deploy more secure encryption options
  - Layer 2: 802.1x: EAP-TLS, EAP-TTLS, LEAP, PEAP (still emerging)
  - Layer 3: IPSEC VPN Tunnel (possible performance/roaming issues)
  - A combination of the two?
- Strong user-based authentication
  - SecureID and/or ACE/Radius

Are we there yet?

- Other ideas to consider
  - Lock client ‘location profiles’ (disable ‘Ad Hoc’ mode, etc.)
  - Deploy ‘fake’ APs: www.blackalchemy.to/Projects/fakeap/fake-ap.html
  - Run honeypots/honeynets to measure malicious activity
  - Set up a web page or SSID warning, “Authorized use only…”
  - Establish means to share scan results w/ collogues/neighbors
  - Remind users to consider that all wireless traffic can be ‘sniffed’

Appendix A*

- Default SSIDs (www.iss.net/wireless/WLAN_FAQ.php) :
  - Linksys – 'linksys'
    - Default management ID is <blank> and password is 'admin'
  - D-Link – 'default'
  - Netgear – 'Wireless'
    - Default WEP keys include 10 11 12 13 14 and 21 22 23 24 25
  - Cisco – 'tsunami'
  - 3Com – '101'
  - Lucent/Cabletron – 'RoamAbout Default Network Name'
  - Compaq – 'Compaq'
  - Intel – 'intel'

Appendix B**

- Configuration Standards:
  - Enable 128 bit WEP encryption (or strongest supported)
  - Change default WEP key to a ‘random’ value (rotate regularly)
  - Use ‘meaningless’ naming convention: SSID, status fields, etc.
  - Change default password(s) to ‘strong’ ones
  - Deny connections from null/’ANY’ ESSIDs
  - Disable SSID broadcast or increase beacon interval to maximum
  - Reduce signal strength and redirect antennas to minimize ‘bleed’
  - Increase minimum supported data rate

Appendix B**

- Configuration Standards (Cont):
  - Set SNMP traps on AP reset or configuration reload
  - Disable all unnecessary protocols on AP
  - Disable cleartext protocols for management on wireless interface
  - Deny management on wireless interface
  - Enable IP/MAC/protocol filtering for management on wired interface
  - Manage APs through terminal servers

Appendix C

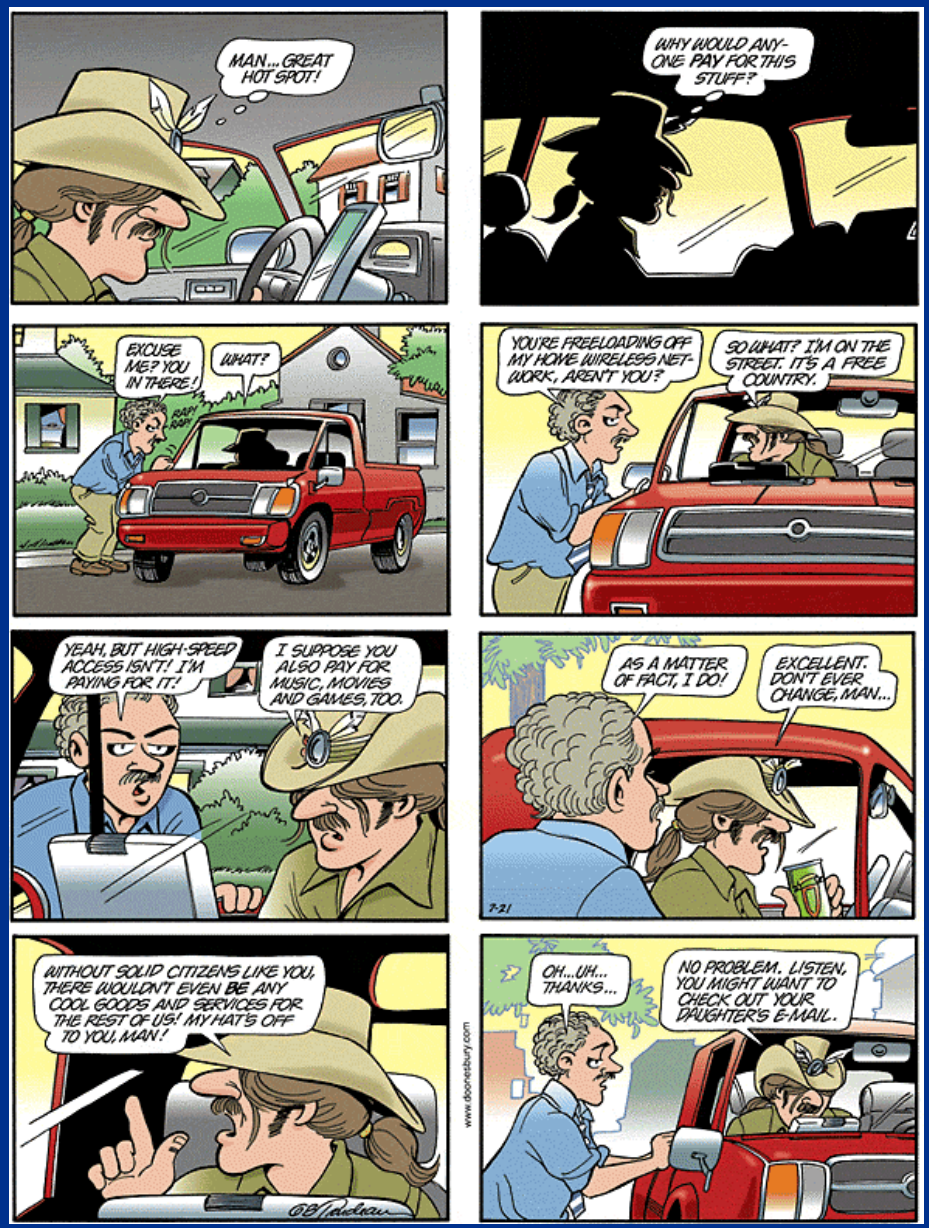
- More URLs:
  - Air Magnet (assessment tool w/ hardware): www.airmagnet.com
  - Wellenreiter (assessment tool): www.remote-exploit.org
  - Kismet (assessment tool): www.kismetwireless.com
  - Warlinux (bootable distro): sourceforge.net/projects/warlinux/
  - Airopeek (sniffer): www.wildpackets.com
  - Ethereal (sniffer): www.ethereal.com
  - Ettercap (switched LAN sniffer): ettercap.sourceforge.net
  - NAI Sniffer: www.sniffer.com/products/wireless.asp
  - Airsnort (cryptanalysis): airsnort.shmoo.com
  - Wepcrack (cryptanalysis): wepcrack.sourceforge.net

Appendix C

- More URLs (Cont):
  - Airtools (cryptanalysis): www.dachb0den.com/projects/bsd-airtools.html
  - Isomair (monitoring): www.isomair.com
  - AirDefense (monitoring): www.airdefense.net
  - Security Recommendations: www.cisco.com/go/safe/
  - Portal: www.wardriving.info
  - Legal Opinion: www.wardrivingisnotacrime.org
  - Hotspots: www.cisco.com/go/hotspots/
  - Hotspots: www.80211hotspots.com
  - Hotspots: www.wifinder.com
  - Hotspots: www.freenetworks.org

Appendix D

- World Wide War Drive II Weekend Update
  - Louisville
    - 237 APs, 187 w/o WEP, 116 default SSIDs
  - Denver
    - 750 APs, 479 w/o WEP, 147 default SSIDs
  - Massachusetts
    - 2856 APs, 2055 w/o WEP, 1064 default SSIDs
  - Seoul
    - 53 APs



Questions,

Comments, or

Complaints?

Kenneth Newman

khn15@columbia.edu