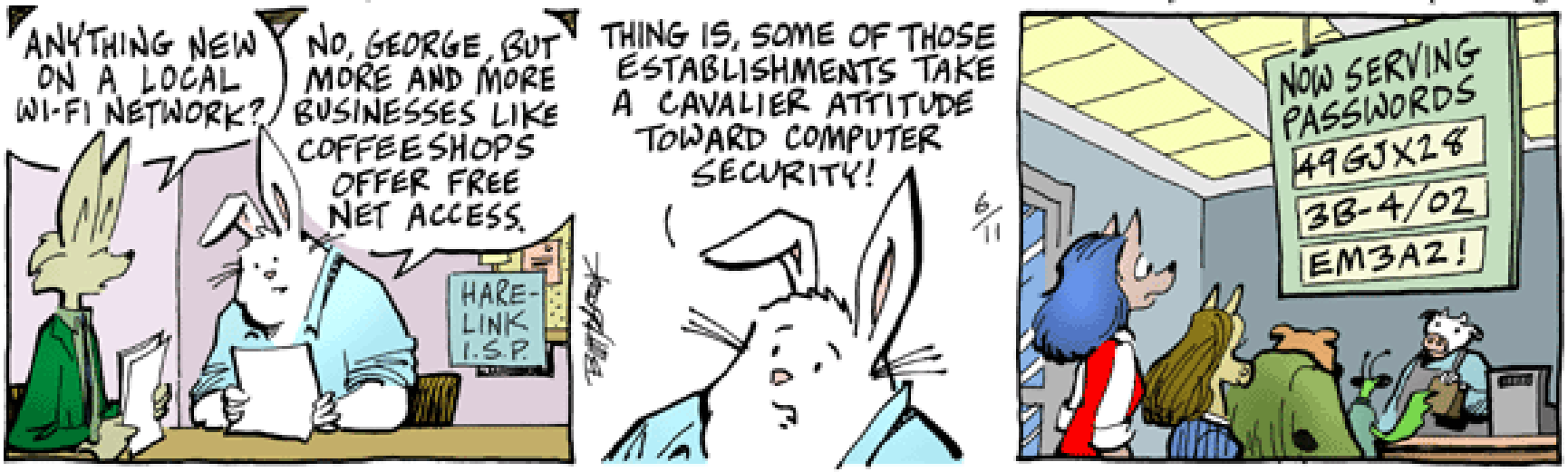
Kevin & Kell ©2005, Bill Holbrook Buy the books at www.plan9.org



Wireless Security

Michael H. Warfield

mhw@ISS.Net

INTERNET | SECURITY | SYSTEMS®

These slides will be available, after the conference, here:

http://www.wittsend.com/mhw/2005/Wireless-Security-LISA

Outline

- Introduction and Standards
- Common Uses and Abuses
- Security Incident Examples
- Access Control and Confidentiality
- Securing Wireless Networks
- Closing Summary and References

Introduction

- **Many forms of wireless**
- **Point-to-point**
  - Wi-Fi / 802.11
  - WiMax / 802.16
  - Bluetooth
  - 3rd Generation Cellular & Wireless Broadband
- **Wi-Fi is becoming ubiquitous**
- **Wireless is incredibly flexible**
  - Cost effective compared to hard wired networks
  - Works in harsh environments
  - Works in mobile environments

WiFi Standards (Alphabet Soup?)

802.11

- IEEE ratified in 1997
- General wireless standards family
- 2.4 GHz shared unlicensed band
- Covered by FCC Part 15 regulations
- Initially 1-2 Mbps
- Poor performance
- Poor acceptance

802.11a

- IEEE Ratified in 1999
- First ship in 2001
- 5 GHz unlicensed band
- 54 Mbps
- High Performance
- Costly
- Poor range
- Adoption was slow and poor

802.11b

- IEEE ratified in 1999
- 2.4Ghz shared unlicensed Band
- Up to 11Mbps
- Moderate Performance
- Relatively inexpensive
- Moderate range (twice that of 802.11a)
- Moderate interference from other services
- Quickly became very popular

802.11g

- IEEE ratified in June 2003
- Shipping in January 2003
- 2.4GHz shared unlicensed band
- 54 Mbps (Super G bounding to over 100 Mbps)
- Good Performance
- Inexpensive (dirt cheap)
- Powerful (many have third party upgrades)
- Compatible with 802.11b

802.11n

- 100+ Mbps
- Compatible with 802.11b and 802.11g
- Upcoming standard
- Multiple proposals submitted
- No consensus as of yet
- MIMO – 802.11n preview?

802.11s

- IEEE Working group first met in July 2004
- 802.11 w/ Mesh topology
- Intel early proposal for 802.11s
- Builds on 802.11 a/b/g
- Should be applicable to 802.11n
- No current standards for 802.11 mesh
- Access points and nodes autonomously relay packets
- Self organizing and extensible

Common Uses

Hotspots

- **Hotspots are publicly accessible wireless zones**
- **Pay and free hotspots are proliferating**
- **Most airports now have hotspots**
  - Some are free, some for pay
- **Some hotels are opting for wireless for broadband**
  - Some are teaming up with wireless providers
- **Some coffee chains have wireless for customers**
- **Some people set up hotspots just for kicks**

Neighborhood Networks

- **Cul-De-Sac Area Networks (CDSAN)?**
- **High power APs cover a couple of small streets**
- **Antennas extend range even further**
- **YES! You really CAN be the ISP for your entire cul-de-sac!**
- **Example neighborhood net in Canada**
  - Broadband
  - VoIP
  - Video
  - Being commercialized for businesses

Municipal WiFi

- **Municipalities considering WiFi as a utility**
- **Antennas / Access Points on lights and utility poles**
- **Uniform coverage and management**
- **Narrows “the digital divide”**
- **Conflicts with commercial competition**
- **Mixed legislative actions**
- **Some active deployments**

Communities

- **Philadelphia**
  - Proposal for community WiFi resulted in state legislation to prevent it
  - Philadelphia has an exemption in resulting legislation
- **San Fransisco**
  - Google contracted to providing free service
- **New Orleans**
  - Free service in aftermath of Katrina using donated equipment
  - BellSouth reported to have withdrawn a donation as a result
- **New York**
  - A New York county has proposed mandating securing access points
  - Encryption is NOT mandatory
  - Security is mandatory even WITH encryption

Wireless VoIP

- **Wireless PBX**
- **Great for mobile employees**
  - Hospitals
  - Schools
  - Conference Centers
- **Cost effective**
- **Versatile**
- **Isolated Access Points and networks control security**
- **Potential evesdropping / sniffing threats**

Industry and Agriculture

- **Supports mobile equipment**
  - Farm equipment in the field
  - Mobile factory floor equipment and employees
- **Eases deployment and installation**
  - Wiring problems in old installations
- **Aids with hostile environments**
- **Not merely end networking services**
- **Part of the industrial process**

Personal Area Networks

- Wireless cards and access points are as cheap as network interfaces now
- Employees may install APs under desks for their laptops
- Convenient for home-to-office road warriors
- Home lan security problems may become corporate lan security problems
- Unauthorized or rogue access points can create gaping security holes
- Open workstations can open up your wired network

Common Abuses

Wardriving

- Popular sport
- Simple as a PDA
- A small mobile antenna is non-intrusive
- Pringles cans are cheap and effective antennas
- Good directional antennas can work for miles
- Automated tools build wardriving maps with gps
- Majority of access points have no encryption!
- Majority of access points use default settings!
- An FBI representative has stated that wardriving and warchalking are legal (but not bandwidth theft).

Inverse Wardriving

- **Wardriving with an Access Point**
- **Linux based access points have extra features**
  - Extra power
  - Remote command line
  - Can run Kismet on the Access Point
- **Trolling for open clients willing to connect**
- **Many workstations are enabled for “any” AP**
- **Can compromise associated wired networks**
- **Test runs at Democratic National Convention**

Open Workstations

- Common to “attach” to the “wrong” access point
- Many laptops come with built-in WiFi
- WiFi may be enabled without realization
- Difficult to lock down laptops to limited connections
- Open workstations may be contaminated outside of security perimeters
- Open workstations may bridge wireless to wired networks
- WiFi policy must include workstation setups!

Evil Twin

- Variation on the “inverse wardriving”
- Evil access point mimicks existing access point ESSID
- Looking for specific networks
- Not just for promiscuous workstations
- Increased power can override legitimate access points
- Evil twins can be more difficult to find than rogues
- Shield from within, shield from without

Hotspot Battles

- **Only 11 channels in North America**
- **Competition with and between fee services**
  - Providers have set up fee based wireless access
  - Cybercafes have set up wireless services
  - Competing individuals have used directional antennas to broadcast into competing locations
- **Organizations have set up free hot spots**
  - Companies seeking to set up services for a fee have come into conflict with community hotspots
  - Some hot-spots in airports have become free
- **WiFi spectrum is shared with Amateur Radio**
  - Amateurs use much more power
  - Accidental cross access and cross interference have occurred

Security Incidents (What were you thinking?)

INTERNET | SECURITY | SYSTEMS®

Information Leakage

- Information may leak from insecure wireless networks
- Networks may be routed over wireless links
- Information may leak in broadcast messages
- Attackers can use techniques such as “arp cache poisoning” to intercept and redirect traffic
- Schools have had student data accidentally exposed through wireless networks
- What's your legal liability?

Threats to Reputation

- Wireless is easy to use for inappropriate activity
- Retail chains have used wireless for temporary cash registers
- Researchers have found insecure wireless nets broadcasting sensitive customer information
- Publication of wireless leaks have lead to major public relations incidents for several companies
- What if the researchers had been “bad guys”?
- (Some have been)

Computer Break-ins

- Major hardware chain had an insecure wireless network in Michigan
- Intruders used it to break into the home office computers in North Carolina
- Law enforcement contacted but access not shut down during investigation
- Intruders were caught sitting in the parking lot during a subsequent break-in
- What about using a high gain directional antennas?

Spammers

- **Drive-by-spamming is taking place**
  - Spammers can send millions of E-Mails in minutes
  - Your servers get blamed
  - Your abuse people get harassed
  - Your company gets blacklisted
- **California man plead guilty to spamming people through unprotected hotspots**
  - Convicted under Can-Spam Act
  - What about wireless theft?
- **Also being used to launch phishing scams**

Extortionists

- **Extortionists have exploited open access points**
- **Maryland man used unsecured wireless networks to make “untraceable” threats and extortion demands**
- **Threats traced to homes and a dentist's office**
- **Caught by his demand for money**
  - (Make the check payable to...)

Simple Bandwidth Theft

- Individual in Florida observes someone sitting in his neighborhood playing with a laptop
- Individual hides laptop whenever people approach
- Individual still present several hours later
- Suspicious behavior reported to police
- Police find the suspicious individual using WiFi
- Charged with theft of bandwidth
- Other charges pending?
- Neighborhood watch?

Other Illegal Activities

- Canadian police caught an individual driving the wrong way down a one-way residential street
- Individual had wardriving equipment in the car
- Individual had been exploiting open residential access points to download child pornography
- Additional charge: Theft of telecommunications
- What if it was your access point?
- How would you explain the network activity to law enforcement?

Denial of Service

- Various Denial of Service attacks possible
- “Omerta” disassociate attacks disconnect workstations
- RF attacks overwhelm channels and spectrum
- Overpowered access points generate interference
- General congestion and channel crowding
- RF “Ping of Death”
- Unlicensed services are not protected from RF interference

Access and Confidentiality

INTERNET | SECURITY | SYSTEMS®

Gateway Control

- Access control through an application gateway
- Use web site authentication to open a firewall
- Little or no link level security
- Wireless traffic may be sniffed
- Very common in hotels
- Very common in paid-for “hot spots”
- Somewhat common at universities
- Prone to “information leakage”
- Prone to MAC hijacking

MAC level access control

- Access granted based on MAC address
- No protection from sniffing
- MAC addresses may be spoofed or hijacked
- Business often have batches of MAC addresses
- Administrative headache to maintain MAC tables
- Does not scale well

SSID Access Control

- SSID broadcast (Wi-Fi network name)
- Cloak a network by disabling SSID broadcast
- Network can still be probed and uncloaked
- Network traffic can still be sniffed
- SSID can be determined from other traffic
- Automated tools are designed to collect information about cloaked networks
- Useful for network selection control
- Little use as access control
- Can help with network selection control
- Does indicate that this is NOT a public network

To SSID or Not To SSID

- **Advantages to broadcasting SSID / ESSID**
  - Autodetection of Networks by workstations
- **Disadvantages to broadcasting SSID / ESSID**
  - Closed network names appearing on foreign workstations
  - Potential for accidental connections (if not encrypted)
- **Advantages to NOT broadcasting SSID / ESSID**
  - Notice: “This network is not public”
  - Accidental connections highly unlikely
- **Disadvantages to NOT broadcasting SSID / ESSID**
  - Manual configuration of networks and workstations
  - “False sense of security”

WEP

- **Wire Equivalent Privacy**
- **IEEE standard adopted in 2000**
- **Simple shared key encryption**
  - 40/56 bit DES (export grade - worthless)
  - 128 bit RC4
- **Weakness unveiled in 2001 led to many attacks**
  - Design is vulnerable to plaintext codebook attacks
  - Some implementations are extremely insecure
- **Recent attacks effective against all variations**

WPA

- Wireless Protected Access
- Based on subset of IEEE 802.11i draft
- WiFi Alliance interim specification
- Can use preshared keys (PSK – WPA Personal)
- Can use Radius / EAP / LEAP authentication
- Uses stronger encryption and initialization vectors
- TKIP avoids IV codebook attacks
- Problems with PSK and weak passwords
- Support is mandatory for Wi-Fi logo

802.11i / WPA2

- Security standard applicable to 802.11 family
- Application of 802.1X to 802.11 protocols
- Ratified by IEEE in mid 2004
- WiFi alliance brands 802.11i as WPA2
- Requires AES layer 2 encryption
- Fully encrypted WLAN
- Not all legacy cards can be supported
- Support for Windows XP/SP2 and Linux available

Virtual Private Networks

- **Virtual Private Networks (VPNs) can provide secure connections on insecure networks**
  - IPSec
  - PPTP
  - L2TP
- **VPNs should be used in open environments for secure access to private resources**
- **VPNs do not protect from threats or viruses on the open network**
- **VPNs should be used with personal firewalls**

Securing Wireless Networks

INTERNET | SECURITY | SYSTEMS®

Securing your network

- Define your wireless policy in writing and enforce
- Don't use default settings!
- Change the SSID
- Disable SSID broadcast, if so desired
- Use WPA if possible (802.11i when available)
- Use WEP where WPA is not available
- Watch for rogue access points and eliminate
- Treat wireless networks as untrusted networks
- Keep access points and systems up to date!

Physical Access

- **Plan for physical (RF) access controls**
- **Reduce power to reduce leakage**
- **Use more access points for better defined coverage**
- **Plan antenna locations**
  - Avoid outer walls
- **Provide for shielding of sensitive areas**
- **Provide spot coverage for weak areas**
- **Test for RF leakage and coverage**

Encryption and authentication

- **What level(s) are necessary and/or sufficient?**
- **What is being protected?**
  - Confidentiality?
  - Access?
- **Link level**
  - WEP/WPA/WPA2
- **VPN**
- **Application**
- **Multiple layers may be necessary**

Security on Open Networks

- **Use a secure VPN to access private resources**
- **Use SSL encrypted versions of access protocols**
  - https instead of http
  - pop3s instead of pop3
  - imaps instead of imap
- **Use a personal firewall or similar protection**
- **Use an intrusion protection system (IPS)**
- **Scan for viruses**
- **Keep systems religiously up to date**

Securing WEP

- Use WEP only if nothing else better is available
- Use 128 bit encryption
- Test all access points for weak packets (Kismet)
- Consider changing shared access keys periodically or when security situation changes
- Use with MAC controls on small networks
- Keep access points behind a firewall in a DMZ
- Assume the network is untrusted and provide for additional security

Securing WPA/WPA2

- **Use WPA2 or WPA when ever available**
- **Use hardened authentication where possible**
  - Radius
  - EAP / LEAP
- **Use strong passwords for WPA Pre-Shared Keys**
  - Minimum of 17 characters
  - Include complex characters (numbers, caps, punc)
  - It's easier to break weak passwords on WPA PSK than it is to do codebook attacks on WEP!

Who Forgot to Invite the Cryptographers?

- **Hardened crypto may not be hardened security**
  - Flaws in algorithms
  - Flaws in design
  - Flaws in implementation
- **WEP used RC4 – 128 bit cryptography**
  - Lots of design and implementation errors
- **WPA was suppose to address flaws in WEP**
  - Still some problems in WPA-PSK
- **SSL servers on APs may be using shared certificates**
  - Static shared certificates are worse than shared keys
  - People can download firmware with certificates to your AP
  - Dynamic, self-signed, certificates are better than shared certs

Deception Tools

- Fake access points can befuddle war drivers
- Deception tools can detect intruders looking for access
- Access attempts to honeypot access points can trigger alerts that intruders may be in the area
- Fake access points do no good if they are not monitored and maintained!
- Generally not a worth-while investment unless you are protecting a high profile target

Closing

INTERNET | SECURITY | SYSTEMS®

Summary

- Wireless networking is inherently insecure
- Default configurations are insecure
- Wireless takes effort and direction to secure
- Wireless networks can be made secure
- Insecure networks can be used securely
- Simply throwing cryptography at it may not be the answer!
- Be paranoid – They are out there and they are out to get you!

Tools

- Kismet <www.kismetwireless.net>
- Airsnort <airsnort.shmoo.com>
- BSD-Airtools <www.dachb0den.com>
- THC-Wardrive <www.thc.org>
- Netstumbler <stumbler.net>
- AiroPeek <www.ig.com.au/AiroPeekMain.htm>
- Airmagnet <www.airmagnet.com>
- FakeAP <www.blackalchemy.to/project/fakeap>
- Wardriving CD <http://www.wardrive.net/wardriving/tools>

Resources and References

- http://www.wittsend.com/mhw/2005/Wireless-Security-LISA
- http://www.informationheadquarters.com/Internet/WIFI.shtml
- http://www.networkintrusion.co.uk/wireless.htm
- http://www.usbwifi.orcon.net.nz/
- http://www.wi-fi.org/
- http://www.wifinetnews.com/
- http://www.wi-fiplanet.com/
- http://grouper.ieee.org/groups/802/11/
- http://www.drizzle.com/~aboba/IEEE/

Wireless Security

Michael H. Warfield

mhw@ISS.Net

mhw@WittsEnd.com

INTERNET | SECURITY | SYSTEMS®