How to Set Up a Secure Home Wireless Network

What you don’t know about setting up a home wireless network can hurt you.

2008 APCUG Convention Session
Tom Jones, P.E., RCDD-NTS
AGENDA

• Some Terms Used In Wireless Networks
• The Alphabet Soup Of Wireless Networks
• Pros And Cons Of Each Type
• Different Types Of Security
• Major Concerns About An Unsecure Home Network
• The Process Of Properly Setting Up Security On A Wireless Home Network
Wireless Terms

- **Ad-Hoc Mode** - Two or More 802.11 Wireless Client Devices Communicating With Each Other Instead of Connecting to an AP
- **AP** - An 802.11 Access Point That Acts As a Communications Hub for Wireless LAN Networks
- **Channel** - A Specific Range of Frequencies
- **DSSS** - Direct Sequence Spread Spectrum
  - Uses a Chipping Sequence to Provide Reliable Higher Speed Data Communications Than FHSS
Wireless Terms

• Duplex - Full Duplex is the ability to send and receive at the same time; Half Duplex is one at a time
• FHSS - Frequency Hopping Spread Spectrum
  – Follows a pre-set pattern of frequency changes using spread spectrum technology
• Fresnel Zone - The area around the visual line-of-sight that radio waves spread out into after they leave the antenna
  – This area must be clear or else signal strength will weaken
Wireless Terms

• Infrastructure Mode - 802.11 Wireless Clients Communicating Through an AP
• ISM - Industrial, Scientific, & Medical Band
• MIMO - Multiple-input Multiple-output, the Process of Separating a Stream of Data and Sending It Simultaneously Over Two or More Antennas at Different Frequencies
• OFDM - Orthogonal Frequency Division Multiplexing, an FDM Modulation Technique for Transmitting Large Amounts of Data On a Radio Wave
Wireless Terms

• **OFDM** - Orthogonal Frequency Division Multiplexing, an FDM Modulation Technique for Transmitting Large Amounts of Digital Data Over a Radio Wave
• **Roaming** - Moving Seamlessly From One Area of Coverage to Another
• **SSID (Service Set Identifier)** - the network name that identifies a particular Wi-Fi access point
• **U-NII** - Unlicensed National Information Infrastructure Band
Radio Spectrum

- Shortwave radio
  - AM broadcast
  - Audio
- FM broadcast
  - Television
  - Cellular (840 MHz)
  - NPCS (1.9 GHz)

<table>
<thead>
<tr>
<th>Extremely low</th>
<th>Very low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Very high</th>
<th>Ultra-high</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super-high</td>
<td>Infrared</td>
<td>Visible light</td>
<td>Ultra-violet</td>
<td>X rays</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 902 MHz to 928 MHz
  - Cordless phone
  - IEEE 802.15.3a
  - Consumer electronics
- 2.4 GHz to 2.4835 GHz
  - IEEE 802.11b,g
  - IEEE 802.15.1
  - IEEE 802.15.3a
  - Cordless telephone
- 5.725 GHz to 5.875 GHz
  - IEEE 802.11a
  - HiperLAN 1, 2
  - Cordless telephone
Wireless Terminology Links

- http://wi-fiplanet.webopedia.com/
- http://www.wirelessdictionary.com/
- http://www.wirelessweek.com/content.aspx?id=136232&menuid=544#s
- http://www.jiwire.com/glossary.htm
- http://compnetworking.about.com/od/wirelessterms/
AGENDA

- Some Terms Used In Wireless Networks
- The Alphabet Soup Of Wireless Networks
- Pros And Cons Of Each Type
- Different Types Of Security
- Major Concerns About An Unsecure Home Network
The Alphabet Soup Of Wireless Networks

- 802.11a - 5 GHz, 54 Mbps (1999/2001)
- 802.11b - 2.4 GHz, 11 Mbps (1999)
- 802.11c - MAC Layer Bridging (Now in 802.1d)
- 802.11d - Extending 802.11 in Other Countries (2001)
- 802.11g - 2.4 GHz, 54 Mbps (2003)
- 802.11h - Adapting 802.11a for Europe Standards, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) (2004)
- 802.11i - Enhance 802.11 Security (*formerly part of 802.11e) (2004)
- 802.11j - 4.9-5.1 GHz Band for Japan (2004)
- 802.11k - WLAN Radio Resource Measurement
- 803.11l - not used by convention
- 802.11m - Maintenance to Correct Editorial and Technical Issues of 802.11
- 802.11n - Proposed (goal: fall 2008) 2.4 GHz and 5GHz, 100Mbps or better
- 803.11o - not used by convention
- 802.11p - Support for mobile (<200 kph) 5 GHz connections up to 1 kilometer
- 803.11q - not used by convention
- 802.11r - Fast roaming support for real-time applications such as VoIP
- 802.11s - Protocol for auto-configuring paths between APs for multicast, ESS Mesh Networking
- 802.11t - Performance metrics, measurement methodologies and test conditions
- 802.11u - Amend 802.11 MAC & PHY to support interworking with external networks
- 802.11v - Wireless Network Management enhancements
- 802.11w - Protected Management Frames
- 802.11x - (reserved and will not be used, can be confused with 802.1x Network Access Control)
- 802.11y - Contention Based Protocol and 3650-3700 MHz Operation in the U.S. (March 2008?)
- 802.11z - Extensions to Direct Link Setup (DLS) (Aug. 2007 - Dec. 2011)
The Letters That We Most Care About

- 802.11a - 5 GHz, 54 Mbps (1999/2001)
- 802.11b - 2.4 GHz, 11 Mbps (1999)
- 802.11g - 2.4 GHz, 54 Mbps (2003)
- 802.11n - Proposed (goal: fall 2008) 2.4 GHz and 5GHz, 100Mbps or better
- 802.11i - Enhance 802.11 Security (*formerly part of 802.11e) (2004)
Other Wireless Standards

- **802.15** - Wireless Personal Area Networks (WPAN)
  - Includes Bluetooth
- **802.16** - Wireless Metropolitan Area Networks (WMAN)
  - Includes WiMax
- **802.20** - Mobile Wireless Metropolitan Area Networks (WMAN)
  - Includes MobileFi
AGENDA

• Some Terms Used In Wireless Networks
• The Alphabet Soup Of Wireless Networks
• Pros And Cons Of Each Type
• Different Types Of Security
• Major Concerns About An Unsecure Home Network
• The Process Of Properly Setting Up Security On A Wireless Home Network
Pros And Cons Of Each 802.11 Type

• Factors That Vary By Type
  – Bandwidth / Throughput
  – Range
  – Compatibility
  – Interference / Reliability

• Common Factors
  – Security
  – Wi-Fi Certification (http://www.wi-fi.org/)
# Maximum Throughput

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>Approximate Throughput (Mbps)</th>
<th>Throughput as Percentage of 802.11b Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>802.11g (802.11b clients in cell)</td>
<td>54</td>
<td>8</td>
</tr>
<tr>
<td>802.11g (no 802.11b clients in cell)</td>
<td>54</td>
<td>22</td>
</tr>
<tr>
<td>802.11a</td>
<td>54</td>
<td>25</td>
</tr>
<tr>
<td>Data Rate (Mbps)</td>
<td>802.11a (40 mW with 6dBi gain diversity patch antenna) Range</td>
<td>802.11g (100 mW with 2.2 dBi gain diversity dipole antenna)</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>54</td>
<td>45 ft (13 m)</td>
<td>90 ft (27 m)</td>
</tr>
<tr>
<td>48</td>
<td>50 ft (15 m)</td>
<td>95 ft (29 m)</td>
</tr>
<tr>
<td>36</td>
<td>65 ft (19 m)</td>
<td>100 ft (30 m)</td>
</tr>
<tr>
<td>24</td>
<td>85 ft (26 m)</td>
<td>140 ft (42 m)</td>
</tr>
<tr>
<td>18</td>
<td>110 ft (33 m)</td>
<td>180 ft (54 m)</td>
</tr>
<tr>
<td>12</td>
<td>130 ft (39 m)</td>
<td>210 ft (64 m)</td>
</tr>
<tr>
<td>11</td>
<td>-</td>
<td>160 ft (48 m)</td>
</tr>
<tr>
<td>9</td>
<td>150 ft (45 m)</td>
<td>250 ft (76 m)</td>
</tr>
<tr>
<td>6</td>
<td>165 ft (50 m)</td>
<td>300 ft (91 m)</td>
</tr>
<tr>
<td>5.5</td>
<td>-</td>
<td>220 ft (67 m)</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>270 ft (82m)</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>410 ft (124 m)</td>
</tr>
</tbody>
</table>
Compatibility

• 802.11g Can Support 802.11b
  – Both Use Same Frequencies
• 802.11a Not Compatible with b or g
  – Different Frequencies
  – Separate Radio Transmitter & Receiver
  – Separate Antennae
• Proposed 802.11n Uses Both Frequencies
Interference

• Many Other Devices Use The Same Unlicensed Frequencies
  – Microwave Ovens
  – Wireless Home Phones
  – Bluetooth Devices
  – Wireless Keyboards, Mice, Headphones
AGENDA

• Some Terms Used In Wireless Networks
• The Alphabet Soup Of Wireless Networks
• Pros And Cons Of Each Type
• Different Types Of Security
• Major Concerns About An Unsecure Home Network
• The Process Of Properly Setting Up Security On A Wireless Home Network
Types of Wireless Network Security

- None (Open Network)
  - Default Mode
- Independent of Other Security Types
  - Change Admin ID and Password If Possible
  - Turn Off SSID Broadcast
  - MAC Address Filtering
- WEP
  - Wired Equivalent Privacy
- WPA
  - Wi-Fi Protected Access
- WPA2
  - Wi-Fi Protected Access version 2
Open Network

• Default Mode for Wireless Hardware
• Default Administrative Account ID and Password Can Be Found On the Internet
• No Restrictions on Who Connects
• SSID Often Manufacturer’s Name
• SSID Is Openly Broadcast
• No Encryption of Data
Change Admin ID and Password

- Each AP Provides Some Configuration Ability
- Provides Access to Make Changes Through Administrative Account
- Default Account ID and Passwords Available on Internet
  - http://www.cirt.net/cgi-bin/passwd.pl
  - Etc.
SSID Broadcast

- Most APs Provide Choice of SSID Broadcast ON or OFF
- Clients Cannot Connect Unless Client SSID Is Set to Match AP SSID
- Unfortunately, Many Tools Available to Detect SSID, Even Without Broadcast On
MAC Address Filtering

- Sets Access Point to Allow Connections Only From Specific Computers
  - Based On Physical or Media Access Control Address
  - Each Address Must Be Entered Manually On the Access Point
WEP

- Initial Security Standard for 802.11b
- Intended to Be As Secure As Wired Networks
- Minimal Security and Privacy
- Found to Be Too Easily Broken
  - Uses Either 64 Bit Or 128 Bit Keys
  - Actual User Keys (Codes) Are 40 Bits And 104 Bits, With The Extra 24 Bits Used By Something Called The Initialization Vector (IV)
WPA

• Adapted While Waiting for 802.11i
• Interim Solution to Weaknesses of WEP
  – IV Length Increased To 48 Bits
  – Uses TSC (TKIP Sequence Counter) to Help Prevent The Re-use of IV Keys
  – Master Keys Are Never Directly Used
  – Provides Better Key Management
WPA2

- Incorporated Into 802.11i Standard
- Uses AES (Advanced Encryption Standard) for More Secure Encryption
- Provides for Both Home and Enterprise
  - Home Version Uses Pre-Defined Keys
  - Enterprise Version Requires EAP (Extensible Authentication Protocol) Server
  - Creates New Session for Each Association
AGENDA

- Some Terms Used In Wireless Networks
- The Alphabet Soup Of Wireless Networks
- Pros And Cons Of Each Type
- Different Types Of Security
- Major Concerns About An Unsecure Home Network
Wireless Hacking

- Unauthorized Access
- MITM (Man In The Middle) Attacks
- Disconnection Attacks
- Eavesdropping
- Rogue Connections
- Spoofing
- DoS Attacks
- Jamming
War Driving

- Wi-Fi Freeloader Or Hacker Trying To Get Personal Information
- Cruise Neighborhoods Or Areas Around Schools Or Libraries
- Find Wireless Networks With Little Or No Security Applied
- Use Network
- Capture Data
War Driving Tools

- Need Only Laptop And Good Directional Antenna
- Cantenna Or Other Homemade Often Best
- Many Designs Available On Internet
War Chalking

- War Chalking is the process of identifying sites for other freeloaders or hackers
War Chalking

- Other War Chalking Symbols

- Open
- Invisible node (No SSID broadcast)
- Closed (multiple controls)
- WEP enabled
- MAC Address Access control
- Pay Network (Starbucks, WayPort, etc.)
- HUNY
- Warning HoneyPot trap
AGENDA

- Some Terms Used In Wireless Networks
- The Alphabet Soup Of Wireless Networks
- Pros And Cons Of Each Type
- Different Types Of Security
- Major Concerns About An Unsecure Home Network

Setting Up a Secure Home Network

- If Wireless Not Being Used, Turn It Off
  - Turn AP Off When Gone On Vacations
- Change Access Account ID & Password
  - Disable Remote Access If Available
- Change SSID and Turn Off Broadcast
- If Limited PCs to Attach, Set MAC Address Filtering
Setting Up a Secure Home Network

- Use Strongest Security Type Available
  - WPA2, WPA, WEP
- Record Current SSID, Passwords, etc.
- Change Them Monthly
- Enable Firewall Protection If Possible
- Choose Best Location for AP
- Choose Best Orientation of Antennas
Questions and Comments

• Any Questions?
• Please Fill Out the Evaluation Forms
• Thank You For Attending!