Wireless Hacking

Chun-Jen (James) Chung

Arizona State University
Wireless Equipment
Windows x. Linux

• Windows
  – Wireless NIC drivers are easy to get
  – Wireless hacking tools are few and weak
    • Unless you pay for AirPcap devices or OmniPeek

• Linux
  – Wireless NIC drivers are hard to get and install
  – Wireless hacking tools are much better
OmniPeek

- WildPackets now packages AiroPeek & EtherPeek together into OmniPeek
- A Windows-based sniffer for wireless and wired LANs
- Only supports a few wireless NICs
Chipsets of Wireless Cards

• For Linux, the best chipsets to use are Orinoco, Prism2.x/3, Atheros, and Cisco

• A good resource is at Madwifi
  – Go to http://madwifi-project.org/wiki/Compatibility
Antennas

- Omnidirectional antenna sends and receives in all directions
- Directional antennas focus the waves in one direction
  - The Cantenna shown is a directional antenna
Stacked Antennas

- Quad stacked antenna
  - Four omnidirectional antennas combined to focus the beam away from the vertical
  - Beamwidth: 360° Horizontal, 15° Vertical
  - Can go half a mile or more see right
WISPer

- Uses "multi-polarization" to send through trees and other obstructions
Global Positioning System (GPS)

- Locates you using signals from a set of satellites
- Works with war-driving software to create a map of access points
Pinpoint your Location with Wi-Fi

- Skyhook uses wardriving to make a database with the location of many Wi-Fi access points
- Can locate any portable Wi-Fi device
- An alternative to GPS
iPhone vs. Android

- The iPhone combines GPS, Wi-Fi, and cell tower location technology to locate you.

- You can wardrive with the Android phone and Wifiscan.
War-Driving Software
Terms

• Service Set Identifier (SSID)
  – An identifier to distinguish one access point from another

• Initialization Vector (IV)
  – Part of a Wired Equivalent Privacy (WEP) packet
  – Used in combination with the shared secret key to cipher the packet's data
NetStumbler

• Very popular Windows-based war-driving application
• Analyzes the 802.11 header and IV fields of the wireless packet to find:
  – SSID
  – MAC address
  – WEP usage and WEP key length (40 or 128 bit)
  – Signal range
  – Access point vendor
How NetStumbler Works

• NetStumbler broadcasts 802.11 Probe Requests
• All access points in the area send 802.11 Probe Responses containing network configuration information, such as their SSID and WEP status
• It can also use a GPS to mark the positions of networks it finds
### NetStumbler Screen

**Network Channels**

<table>
<thead>
<tr>
<th>MAC</th>
<th>SSID</th>
<th>Name</th>
<th>Chan</th>
<th>Speed</th>
<th>Vendor</th>
<th>Type</th>
<th>Enc...</th>
<th>SNR</th>
<th>Signal+</th>
<th>Noise-</th>
<th>SNR+</th>
<th>IP Addr</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0021D87E4480</td>
<td>asu</td>
<td></td>
<td>6</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>-92</td>
<td>-100</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00190706C940</td>
<td>asu</td>
<td></td>
<td>11</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>-88</td>
<td>-100</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CBD30</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>-90</td>
<td>-100</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CC110</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>-92</td>
<td>-100</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0018F8DAA2A4</td>
<td>Patrick Scrazy</td>
<td>6</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>-90</td>
<td>-100</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00065A80A300</td>
<td>2TEMPE411</td>
<td></td>
<td>11</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td>WEP</td>
<td>-82</td>
<td>-100</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CC210</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td>WEP</td>
<td>-80</td>
<td>-100</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00141BB75FA0</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>-80</td>
<td>-100</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00152C4E0B0</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>-84</td>
<td>-100</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CC240</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>16</td>
<td>-79</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00095BD9B10</td>
<td>CUBIC</td>
<td></td>
<td>2</td>
<td>54 Mbps</td>
<td>Netgear</td>
<td>AP</td>
<td></td>
<td>21</td>
<td>-67</td>
<td>33</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>001FCA4FC960</td>
<td>asu</td>
<td></td>
<td>11</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>16</td>
<td>-80</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346FD030</td>
<td>asu</td>
<td></td>
<td>6</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>12</td>
<td>-77</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>001120A44FB0</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>1</td>
<td>-71</td>
<td>29</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346FCE80</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>28</td>
<td>-65</td>
<td>35</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00190735E90</td>
<td>asu</td>
<td></td>
<td>1</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>35</td>
<td>-62</td>
<td>38</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CE20</td>
<td>asu</td>
<td></td>
<td>11</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>11</td>
<td>-79</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>001FCA82D850</td>
<td>asu</td>
<td></td>
<td>11</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>38</td>
<td>-51</td>
<td>49</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CFB80</td>
<td>asu</td>
<td></td>
<td>11</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>38</td>
<td>-54</td>
<td>46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F346CC080</td>
<td>asu</td>
<td></td>
<td>6</td>
<td>54 Mbps</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>37</td>
<td>-60</td>
<td>40</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>001F33B8FC94</td>
<td>brickyard</td>
<td></td>
<td>6</td>
<td>54 Mbps</td>
<td>(Fake)</td>
<td>AP</td>
<td></td>
<td>34</td>
<td>-62</td>
<td>38</td>
<td></td>
<td>192.168.1.1</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>
NetStumbler Countermeasures

• NetStumbler's relies on the Broadcast Probe Request

• Wireless equipment vendors will usually offer an option to disable this 802.11 feature, which effectively blinds NetStumbler
  – But it doesn't blind Kismet
Kismet

- Linux and BSD-based wireless sniffer
- Allows you to track wireless access points and their GPS locations like NetStumbler
- Allow spectrum analysis (with Wispy)
- Sniffs for 802.11 packets, such as Beacons and Association Requests
  - Gathers IP addresses and Cisco Discovery Protocol (CDP) names when it can
- Kismet Countermeasures
  - There's not much you can do to stop Kismet from finding your network
Kismet Features

- Windows version
  - Runs on cygwin, only supports two types of network cards

- Airsnort compatible weak-iv packet logging, however airsnort is too OLD, use aircrack-ng instead.

- Runtime decoding of WEP packets for known networks
Kismet

– You can use Backtrack

  • [http://www.remote-exploit.org/backtrack_download.html](http://www.remote-exploit.org/backtrack_download.html)

– However, here our demo is based on ubuntu, NIC Atheros AR5001X+, internal wireless card.

  • Madwifi [http://www.madwifi.com/](http://www.madwifi.com/)
### Network List (Channel)

<table>
<thead>
<tr>
<th>Name</th>
<th>T W Ch</th>
<th>Packets</th>
<th>Flags</th>
<th>IP Range</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;no ssid&gt;</td>
<td>AN-----</td>
<td>1</td>
<td>0</td>
<td>0.0.0.0</td>
<td>1285</td>
</tr>
<tr>
<td>DJWLAN</td>
<td>AY001</td>
<td>109</td>
<td>0</td>
<td>0.0.0.0</td>
<td>320B</td>
</tr>
<tr>
<td>CrossTownPS</td>
<td>AO001</td>
<td>85</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>alicia</td>
<td>AO001</td>
<td>69</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>&lt;no ssid&gt;</td>
<td>AO003</td>
<td>33</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>&lt;no ssid&gt;</td>
<td>AO006</td>
<td>17</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>&lt;mkchught&gt;</td>
<td>AY006</td>
<td>47</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>linksys</td>
<td>AY008</td>
<td>2</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>linksys</td>
<td>AO007</td>
<td>47</td>
<td>0</td>
<td>0.0.0.0</td>
<td>1k</td>
</tr>
<tr>
<td>Sudev</td>
<td>AO011</td>
<td>35</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>JNS Realty</td>
<td>AO011</td>
<td>18</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>jd32493</td>
<td>AO011</td>
<td>22</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
<tr>
<td>&lt;MilleniumFalcon&gt;</td>
<td>AO011</td>
<td>251</td>
<td>0</td>
<td>0.0.0.0</td>
<td>6k</td>
</tr>
<tr>
<td>Bruening Home</td>
<td>AO011</td>
<td>22</td>
<td>0</td>
<td>0.0.0.0</td>
<td>8B</td>
</tr>
</tbody>
</table>

### Status
- Found new probed network "MilleniumFalcon" bssid 00:23:31:5C:F9:E9
- Found SSID "MilleniumFalcon" for cloaked network BSSID 00:0F:B5:A9:CA:C6
- Associated probe network "00:19:02:4F:9D:E4" with "00:19:02:4F:9D:E4" via probe response.
- Battery: AC charging 92%
Wardriving

- Finding Wireless networks with a portable device
  - Image from overdrawn.net
Vistumbler (http://www.vistumbler.net/)

- Find Wireless access points
- GPS Support
- Compatible with Netstumbler
- Export access point GPS locations to a google earth kml file
- Live Google Earth Tracking - Auto KML automatically shows access points in google earth.
- Speaks Signal Strength using sound files, windows sound api, or MIDI
- Open Source
Cain (http://www.oxid.it/)

- It uses the Winpcap Packet Driver to control the wireless network card. Access points and ad-hoc networks are enumerated using 802.11 OIDs from Windows DDK at intervals of five seconds and WLANs parameters (MAC address, SSID, Vendor, WEP Encryption, Channels...) are displayed in the scanner list.

- With Abel, it can crack WEP’s password
• WiGLE
  (http://www.wigle.net/)
  – Collects wardriving data from users
  – Has over 16 million records
Wireless Scanning and Enumeration

• Goal of Scanning and Enumeration
  – To determine a method to gain system access

• For wireless networks, scanning and enumeration are combined, and happen simultaneously
Wireless Sniffers

• Not really any different from wired sniffers
• There are the usual issues with drivers, and getting a card into *monitor* mode
Wireshark WiFi

– Enable the wireless device in monitor mode
Identifying Wireless Network Defenses
SSID

• SSID can be found from any of these frames
  – **Beacons**
    • Sent continually by the access point (unless disabled)
  – **Probe Requests**
    • Sent by client systems wishing to connect
  – **Probe Responses**
    • Response to a Probe Request
  – **Association and Reassociation Requests**
    • Made by the client when joining or rejoining the network
• If SSID broadcasting is off, just send an authentication frame to force a reassociation
MAC Access Control

- Each MAC must be entered into the list of approved addresses
- High administrative effort, low security
- Attacker can just sniff MACs from clients and spoof them
Gaining Access
(Hacking 802.11)
Specifying the SSID

• In Windows, just select it from the available wireless networks
  – Click on set up a wireless network from a home or small office.
  – And then input the SSID
Changing your MAC

- In Windows Vista
  - Run `regedt32`
  - Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}`
  - Find REG_SZ name `NetworkAddress` and change it
- SMAC is easier
Device Manager

- Many Wi-Fi cards allow you to change the MAC in Windows' Device Manager
Attacks Against the WEP Algorithm

• Brute-force keyspace – takes weeks even for 40-bit keys (use Cain & Abel)

• Collect Initialization Vectors, which are sent in the clear, and correlate them with the first encrypted byte
  – This makes the brute-force process much faster
Tools that Exploit WEP Weaknesses

- Aircrack-ng or AirSnort (old)
- kismet
- Cain & Abel
- WLAN-Tools
- DWEPCrack
- WEPAttack
  - Cracks using the weak IV flaw
- Best countermeasure – use WPA/WPA2
WEP Crack Demo

- This demo is conducted in my home (please do not try it again 😊)
- Network configuration.
Run kismet to discover networks
Look at details about DJWLAN

<table>
<thead>
<tr>
<th>Network Details</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>DJWLAN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>localhost:2501</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BSSID</strong></td>
<td>00:8C:41:FF:54:2F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Carrier</strong></td>
<td>IEEE 802.11g</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manuf</strong></td>
<td>Linksys</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>Unknown</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Matched</strong></td>
<td>00:8C:41:00:00:00/FF:FF:FF:00:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Max Rate</strong></td>
<td>54.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BSS Time</strong></td>
<td>1949e31131c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Max Seen</strong></td>
<td>54800 kbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>First</strong></td>
<td>Sun Apr 26 20:57:48 2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Latest</strong></td>
<td>Sun Apr 26 21:04:46 2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Clients</strong></td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Access Point (infrastructure)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Channel</strong></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Encrypt</strong></td>
<td>WEP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decrypt</strong></td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Beacon</strong></td>
<td>25680 (26.214400 sec)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Packets</strong></td>
<td>450</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LLC</strong></td>
<td>446</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cprt</strong></td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weak</strong></td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dupe IV</strong></td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>3928</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Signal</strong></td>
<td>Power: 47 (best 79)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Noise</strong></td>
<td>94 (best -99)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IP Type</strong></td>
<td>None detected</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Min Loc</strong></td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Max Loc</strong></td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Battery: AC charging 94%
Look at who connect to DJWLAN

<table>
<thead>
<tr>
<th>MAC</th>
<th>Manuf</th>
<th>Data Crypt</th>
<th>Size</th>
<th>IP Range</th>
<th>Sgn</th>
<th>Nse</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:19:02:4F:90:E4</td>
<td>Unknown</td>
<td>2</td>
<td>2</td>
<td>182B 0.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:11:08:C7:B7:7E</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:0C:41:FF:54:2F</td>
<td>Linksys</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:23:31:6C:CF:0F</td>
<td>Unknown</td>
<td>2</td>
<td>2</td>
<td>156B 0.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:13:16:B7:4E:36</td>
<td>Linksys</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Run airodump to capture client traffic
Use aireplay-ng to replay the captured packet.
Use aireplay-ng to replay the captured packets.
Use aircrack-ng to crack my WEP.
HotSpotter

- Hotspotter--Like SSLstrip, it silently replaces a secure WiFi connection with an insecure one
- Works because Windows allows it, apparently happy to accept an insecure network as part of the same WLAN
Lightweight Extensible Authentication Protocol (LEAP)
What is LEAP?

- A proprietary protocol from Cisco Systems developed in 2000 to address the security weaknesses common in WEP
- LEAP is an 802.1X schema using a RADIUS server
- As of 2004, 46% of IT executives in the enterprise said that they used LEAP in their organizations
The Weakness of LEAP

• LEAP is fundamentally weak because it provides zero resistance to offline dictionary attacks
• It solely relies on MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) to protect the user credentials used for Wireless LAN authentication
MS-CHAPv2

• MS-CHAPv2 is notoriously weak because
  – It does not use a SALT in its NT hashes
  – Uses a weak 2 byte DES key
  – Sends usernames in clear text

• Because of this, offline dictionary and brute force attacks can be made much more efficient by a very large (4 gigabytes) database of likely passwords with pre-calculated hashes
Cisco's Defense

• LEAP is secure if the passwords are long and complex
  – 10 characters long with random upper case, lower case, numeric, and special characters

• The vast majority of passwords in most organizations do not meet these stringent requirements
  – Can be cracked in a few days or even a few minutes
LEAP Attacks
Anwrap

• Performs a dictionary attack on LEAP
• Written in Perl, easy to use
Asleap

• Grabs and decrypts weak LEAP passwords from Cisco wireless access points and corresponding wireless cards

• Integrated with Air-Jack to knock authenticated wireless users off targeted wireless networks
  – When the user reauthenticates, their password will be sniffed and cracked with Asleap
Countermeasures for LEAP

• Enforce strong passwords
• Continuously audit the services to make sure people don't use poor passwords
WPA/WPA2

• WPA/WPA2 is strong
• No major weaknesses
• However, if you use a weak Pre-Shared Key, it can be found with a dictionary attack
• Tool: Aircrack-ng
Denial of Service (DoS) Attacks

- Radio Interference
  - 802.11a, 11b, and 11g all use the 2.4-2.5GHz ISM band, which is extremely crowded at the moment

- Unauthenticated Management Frames
  - An attacker can spoof a deauthentication frame that looks like it came from the access point
    - wlan_jack in the Air-Jack suite does this