Kismet & GPSdrive

Wireless network sniffing with Open Source Software

Antony Stone

Antony.Stone@Open.Source.IT
Wardriving

- The name “wardriving” is derived from “wardialling”, which means dialling arbitrary phone numbers to find out which ones are answered by modems (a historically popular method of accessing computers remotely).

- Wardriving means travelling around with radio equipment, listening out for wireless network signals, and recording information about the networks.
Background

- **Packet sniffing**
  - Long-established practice on cabled networks
  - Listen passively to packets from/to other machines passing on the wire
  - Requires NIC in “promiscuous mode”

- **Wireless packet sniffing**
  - Signals are broadcast by radio
  - Passive receiver can hear all communications
  - Wireless NIC still needs promiscuous mode
    - Actually, RFmon mode
Background

- Packet sniffing on cabled network - need physical connection
  - authorised user listening in on unauthorised traffic
- Packet sniffing on wireless network - can be (almost) anywhere
  - no requirement to be on the premises
  - may not be authorised user of network
  - passive sniffer impossible to detect
Why wireless packet sniffing?

- Access to interesting data
  - Targeted network eavesdropping
    - eg: content of emails
- Access to interesting information
  - Random network eavesdropping
    - eg: usernames / passwords
- Access to interesting networks
  - Bandwidth hijacking
    - eg: access to the Internet
802.11b networking

- 14 partially-overlapping channels ~2.45GHz

- Not all channels available in all countries
  - 11 in US, 13 in UK, 14 in Japan
802.11b networking

- Ad-hoc mode - between PCs (peer-to-peer)
- Infrastructure mode - Access Point is used like a hub on a cabled network
  - NB: a hub, not a switch - traffic is broadcast
- Each computer communicates with the AP
- Antenna on AP is very important
  - Signal power - strength of signals sent
  - Sensitivity - reception of weak signals
802.11b networking

- **SSID**
  - Service Set IDentifier
  - Name of the wireless network
- **BSSID**
  - Basic Service Set IDentifier
  - MAC address of Access Point
- **Beacon frame broadcasts**
  - “This is my BSSID!” every 0.1 seconds...
802.11b networking

- Passive network sniffing
  - 802.11 NIC in promiscuous mode with an antenna sensitive enough to pick up signals from:
    - Access Point
    - Communicating PCs
- Remote access to network (2-way)
  - Antenna needs to supply sufficient signal power to be picked up by Access Point (not PCs)
- Directional antennas are very helpful
Wireless network security

- WEP - Wired Equivalent Privacy
- Encrypt packet contents so that intercepting radio transmissions does not reveal data
- Data encryption based on RC4 algorithm
  - Same as used in SSL/TLS, Kerberos
  - Perfectly good stream cipher, if used correctly
- Cannot encrypt everything
- MAC addresses need to remain unencrypted
OSI & TCP/IP networking models

OSI 7-layer model

TCP/IP 4-layer model

Application
Presentation
Session
Transport
Network
Data Link
Physical

Application
Transport (TCP)
Internet (IP)
Network
Packets and headers

- HTTP request
  
  ```
  GET http://slashdot.org
  ```

- TCP header
  
  ```
  src/dst TCP ports
  ```

- IP header
  
  ```
  src/dst IP addresses
  ```

- Ethernet or 802.11b header
  
  ```
  src/dst MAC addresses
  ```
Kismet packet sniffer

- What information will Kismet record?
  - Channel number
  - Network name (SSID)
  - Access point MAC address (BSSID)
    - Access point Manufacturer
  - SSID set to default?
  - WEP on or off?
  - Number of client systems connected
  - IP address range in use (a bit of a guess)
  - Content of packets (datastream)
<table>
<thead>
<tr>
<th>Name</th>
<th>T</th>
<th>W</th>
<th>Ch</th>
<th>Sgn</th>
<th>Packts</th>
<th>Flags</th>
<th>IP</th>
<th>Range</th>
<th>Clnt</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steventon</td>
<td>AN</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>932</td>
<td>T3</td>
<td>192.168.</td>
<td>42.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>BTVOYAGER-22</td>
<td>AN</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>29</td>
<td>T3</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>MENDUS</td>
<td>AN</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>&lt;no ssid&gt;</td>
<td>AN</td>
<td>01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>swifts</td>
<td>AN</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>27</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>3Com</td>
<td>AN</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>MikeNet</td>
<td>AN</td>
<td>06</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>greenfields</td>
<td>AN</td>
<td>06</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>belkin54g</td>
<td>AN</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>QX136SZ</td>
<td>AN</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>TSLWR1</td>
<td>AN</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>TIG</td>
<td>AN</td>
<td>06</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>TIG</td>
<td>AN</td>
<td>06</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>linksys</td>
<td>AN</td>
<td>06</td>
<td>0</td>
<td>0</td>
<td>23</td>
<td>F</td>
<td>192.168.</td>
<td>1.1</td>
<td>0</td>
<td>0B</td>
</tr>
<tr>
<td>OSG</td>
<td>AN</td>
<td>01</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>U4</td>
<td>193.130.</td>
<td>242.1</td>
<td>1</td>
<td>2k</td>
</tr>
<tr>
<td>Rich Network</td>
<td>AN</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>59</td>
<td>0</td>
<td>0.0.0.0.</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0B</td>
</tr>
</tbody>
</table>

**Status**

Found new network "OSG" bssid 00:A0:F8:9C:20:9B WEP N Ch 1 @ 11.00 mbit
Found IP 193.130.242.1 for OSG::00:A0:E4:03:07:FE via UDP
Saving data files.

Found new network "Rich Network" bssid 00:0D:93:86:9C:41 WEP Y Ch 10 @ 11.00 mbit
Battery: 78% Oh0m0s
Kismet vs. Netstumbler

- Kismet places 802.11 card in RFmon mode, which allows full capture of data from all networks on all channels (sequentially)
- Netstumbler uses firmware on the 802.11 card to discover networks seen by the card
  - Active monitoring - Netstumbler is “noisy”
  - Netstumbler does not detect “cloaked” networks
  - Netstumbler does not capture data - only network names
Kismet - hardware

- Fundamental requirement is 802.11 card!
  - PCI
  - PCMCIA
  - USB
- Must support RFmon mode
  - eg: based on Prism2 chipset
- Some USB adapters
  - Netgear MA-111
Long range antennas

- Wardriving works best with omnidirectional antenna
  - PCMCIA built-in is not much good
    - Very short range
  - PCI built-in is better (but not great)
- External antennas
  - Discone
  - Pringles / soup tin cantenna
  - Parabolic reflector
Discone antenna

- Good “flat” omnidirectional reception
Pringles / soup tin cantenna

- Directional - increases signal:noise ratio

Projection = $\frac{1}{4}$ wavelength = 32mm

Alternative antenna positions
Parabolic reflector antenna

- Highly directional - very long range

Solid or mesh reflector

Focal point - USB adapter?
Choosing the right antenna

• Wardriving - omnidirectional receiver
  • Discone works well
  • Cantenna not ideal
  • Parabolic can be used to scan from a fixed point

• Network interception / hijacking - directional receive + transmit
  • Distance depends on location (car park / hilltop?)
  • Discone not good
  • Cantenna / parabolic depending on distance
Wireless network security

- 64-bit or 128-bit key
  - 40 or 104 'secret' bits, plus 24 'public' bits
  - 24 public bits are “Initialisation Vector”
- First bytes of IP header are predictable
  - “Known plaintext” attack
- Stream cipher
  - plaintext -XOR- key = cryptotext
  - plaintext -XOR- cryptotext = key
Wireless network (in)security

• Weak keys
  • $2^{24}$ Initialisation Vectors = 16 million
  • $\sim 9000$ indicate “weak keys”
    • Weak keys are easier to guess
• 802.11 does not say how IV should change
  • Some vendors start at zero and increment
  • Some choose (pseudo) random numbers
  • Random is worse because IVs will start to be reused after only 50% of the time!
Wireless network insecurity

- 24 bit IV
  - 16 million possible IVs
  - 1500 bytes per packet (max)
  - 11Mbits per second
  - IVs repeat after 5 hours!
- Less busy network - takes more time
- Smaller packets - takes less time
- WEP is guaranteed crackable, with purely passive sniffing, in a short time
GPSdrive

- GPSdrive is a completely independent package from Kismet, but includes Kismet support.
- GPSdrive displays position, velocity, track, waypoints, places on a moving-map display.
- GPSdrive is not a route-planning system:
  - Doesn't tell you where to go, shows you where you've been.
- Places can be stored in MySQL database:
  - Also in plain text files.
GPSdrive

- GPSdrive requires:
  - Computer (laptop is convenient)
  - GPS receiver (RS232 / USB connection)
- Maps can be pre-loaded, or added later
  - Not supplied with software
- Speech output supported via Festival
  - Commentary on distance from target, current speed, time
  - Calls out names of wireless networks as they are detected!
GPSdrive

- Additional features
  - Database supports multiple icon types
  - Includes speed cameras
  - Downloadable databases of speed camera locations
  - Speech synthesiser will call out distance to speed camera + current speed
    - Doesn't know area speed limits
Kismet & GPSdrive in combination

- Kismet records network details
- GPSdrive displays network SSIDs at their locations on moving map
- Calls out names of networks as they are detected
- Encrypted & unencrypted (WEP / open) networks are displayed with different symbols
- Map can be recalled later to identify location of “interesting” networks
Resources

- Kismet
  http://www.kismetwireless.net
- GPSdrive
  http://gpsdrive.kraftvoll.at
- Festival speech synthesis
  - linked from GPSdrive site, but also at
    http://www.cstr.ed.ac.uk/projects/festival
- Google for Discone, Cantenna, “DIY 802.11”