WiFi capture and injection on various Oses revisited

Thomas d’Otreppe
whoami

• Security researcher
• Author of Aircrack-ng
• Created Offensive Security Wireless Attacks aka WiFu
• Software developer @ MainNerve
Agenda

• What’s monitor mode?
• Linux
• Windows
• BSD
• OSX
• Android
• Demos
What’s that?

- Monitor (aka RF Mon) mode is awesome
- Packet injection is awesomer
Linux

• Most popular platform
  • WiFi adapters are cheap
  • Has had support for a very long time
    • Lots of tools support it

• WiFi stack got better over time
  • Custom
  • ieee80211
  • mac80211
Adapter support

• Most of them (if not too new)
• https://wikidevi.com
• Vendor drivers:
  • No monitor mode support
  • Never, ever
Tools

- Aircrack-ng
- Wireshark
- Kismet
- Tcpdump
- Dumpcap
- A lot more…
Enable monitor mode

1. airmon-ng check kill
2. airmon-ng start wlan0

Start capturing
• airodump-ng wlan0mon
Wireshark

• Capture → Options
tcpdump and others

- As root, use `-i` to put interface in monitor mode
  - `tcpdump -I -i wlan0`
  - `dumpcap -I wlan0`
  - `tshark -I -i wlan0`
Wireshark, tcpdump and others

• Sometimes monitor mode/changing link layer (to 802.11) fails.
  → Exit and try again, it will work
Windows

• Getting better
• Some tools in common with Linux
## Windows - Hardware

<table>
<thead>
<tr>
<th></th>
<th>Savvius aka Wildpackets</th>
<th>Riverbed Airpcap</th>
<th>Npcap</th>
<th>Acrylic WiFi Professional</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>API</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Commercial</td>
<td>Commercial</td>
<td>Open source</td>
<td>Commercial</td>
</tr>
<tr>
<td><strong>Adapter</strong></td>
<td>Custom</td>
<td>Custom</td>
<td>Any*</td>
<td>Airpcap/Others**</td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td>Wildpackets only</td>
<td>Wireshark, commercial and open source</td>
<td>Wireshark</td>
<td>Airodump-ng</td>
</tr>
<tr>
<td><strong>802.11</strong></td>
<td>ac</td>
<td>n</td>
<td>depends</td>
<td>Depends</td>
</tr>
<tr>
<td><strong>Packet injection</strong></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Monitor mode</strong></td>
<td>GUI</td>
<td>GUI</td>
<td>Command line</td>
<td>Automatic (GUI)</td>
</tr>
</tbody>
</table>

* All drivers have monitor mode but hit and miss

Windows – Open source

- Wireshark
- Aircrack-ng (0.9.X)
- Kismet
- Cain and Abel
Windows – Closed source

- Riverbed Steelcentral
- Microsoft Network Monitor
- Elcomsoft Wireless Network Auditor
- Commview For WiFi
Enable monitor mode - Airpcap

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>508574.246939</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>242 Beacon frame, SN=3657, FN=0, Flags=........C, BI=100, SSID...</td>
<td></td>
</tr>
<tr>
<td>508674.249560</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3658, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>508774.269081</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3659, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>508874.289356</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3660, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>508974.308826</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3661, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>509074.328473</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3662, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>509174.347613</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>242 Beacon frame, SN=3663, FN=0, Flags=........C, BI=100, SSID...</td>
<td></td>
</tr>
<tr>
<td>509274.356251</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3664, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>509374.366973</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3665, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>509474.389256</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3666, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
<tr>
<td>509574.408674</td>
<td>Azurewave_7d:b8:e1</td>
<td>Broadcast</td>
<td>802.11</td>
<td></td>
<td>54 Null function (No data), SN=3667, FN=0, Flags=.......F.C</td>
<td></td>
</tr>
</tbody>
</table>

Frame 3515: 54 bytes on wire (432 bits), 54 bytes captured
Radiotap Header v0, Length 26
802.11 radio information
IEEE 802.11 Null function (No data), Flags: ........F.C
Enable monitor mode - NPcap

Command Prompt

Usage: WlanHelper [Commands]
   or: WlanHelper {Interface Name or GUID} [Options]

OPTIONS:
  mode
      mode <managed|monitor|master..> : Set interface operation mode
  mode
      mode : Get interface operation mode
  mode
      mode <managed|monitor|master..> : Get all operation modes supported by the interface, comma-separated
  channel
      channel <1-14> : Set interface channel
      channel : Get interface channel
  freq
      freq : Get interface frequency
      freq <VALUE> : Set interface frequency (only works in monitor mode)

COMMANDS:
  -h : Print this help summary page
  -l : Enter the interactive mode

OPERATION MODES:
  managed : The Extensible Station (ExtSTA) operation mode
  monitor : The Network Monitor (NetMon) operation mode
  master : The Extensible Access Point (ExtAP) operation mode (supported from Windows 7 and later)
  wfd_device : The Wi-Fi Direct Device operation mode (supported from Windows 8 and later)
  wfd_owner : The Wi-Fi Direct Group Owner operation mode (supported from Windows 8 and later)
  wfd_client : The Wi-Fi Direct Client operation mode (supported from Windows 8 and later)

EXAMPLES:
  WlanHelper Wi-Fi mode
  WlanHelper 42df4d7a-2764-43ac-b58e-3df569c447da channel 11
  WlanHelper 42df4d7a-2764-43ac-b58e-3df569c447da freq 2
  WlanHelper "Wireless Network Connection" mode monitor

SEE THE MAN PAGE (https://github.com/nmap/npcap) FOR MORE OPTIONS AND EXAMPLES

C:\Users\Thomas>
Enable monitor mode - NPcap

• Run Command Prompt as Administrator

```bash
C:\Windows\system32> wlanhelper -i
WlanHelper [Interactive Mode]:
*****************************
0. daeac469-611e-4978-80af-bdea07663be2
   Name: Wi-Fi
   Description: Intel(R) Dual Band Wireless-AC 3165
   State: "disconnected"
   Operation Mode: "Extensible Station (ExtSTA)"
Enter the choice (0, 1,..) of the wireless card you want to operate on:
0
Enter the operation mode (0, 1 or 2) you want to switch to for the chosen wireless card:
0: Extensible Station (ExtSTA)
1: Network Monitor (NetMon)
2: Extensible Access Point (ExtAP)
```
**NPcap - Notes**

- Command line must be run as Administrator
- WiFi card must be enabled
- There can be only one
  - Airpcap or Npcap, you have to choose
- Still in beta, and releases often
BSD

- Similar support as in Linux in the mid-2000
- Limited driver and adapter support
  - Mostly old 802.11bg
- Not very well documented
- Different support depending on BSD flavor
FreeBSD/DragonflyBSD

- Use `ifconfig` to put interface in monitor mode
  - `ifconfig wlan create wlandev ${IFACE} wlanmode monitor`
- Monitor interface name has to be `wlanX`
• Use your favorite tool (Wireshark, Tcpdump, Aircrack-ng, Kismet)
• Airmon-ng has support for *ath* and *urtwn* drivers
  • Atheros
  • Realtek USB
FreeBSD - Notes

• Load drivers in `/boot/loader.conf`
  • Realtek: `if_urtwn_load="YES"`
  • Atheros: `if_ath_load="YES"`

• Accept Realtek license (`/boot/loader.conf`):
  • `legal.realtek.license_ack=1`

• Might not complain if firmware is not loaded
  • But will not give any packet

• For other drivers, look in man pages for info
FreeBSD/DragonflyBSD - Problems

- Injection is supposed to work in FreeBSD
- DragonflyBSD unstable
- Lots of other adapters supported but lots discontinued (or too old to be useful)
Other BSD flavor

• **NetBSD**
  - No need to put interface in monitor mode or accept license and load driver
  - Kinda laggy in Airodump-ng

• **OpenBSD**
  - Seems unstable
  - `ifconfig ${IFACE} chan 6`
  - `ifconfig ${IFACE} mediaopt monitor`
  - `ifconfig ${IFACE} up`
• Started in Tiger (10.4.0) and improved over time
OS X – GUI

• Hold ‘Option’ key and click on the wireless icon
• Select ‘Open Wireless Diagnostics…’
OS X – GUI

• Select ‘Sniffer’ in the ‘Window’ menu
Use your Mac as a dedicated sniffer to capture Wi-Fi traffic. Choose a channel and channel width, then click 'Start' to begin. Click 'Stop' when you are finished and a wireless capture file will be placed on your desktop.

Channel: 6
Width: 20 MHz
OS X - GUI

• .wcap file on your desktop
• Just a regular PCAP file
• Use Wireshark/Aircrack-ng/Airodump-ng/…
OS X – Command line

• Command:

  sudo
  /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport <INTERFACE> sniff <CHANNEL>

• Parameters:
  • Interface: usually en1
  • Channel

• Output: PCAP file in /tmp
### Wireshark - Capture Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Traffic</th>
<th>Link-layer Header</th>
<th>Promiscuous</th>
<th>Snapslen (B)</th>
<th>Buffer (MB)</th>
<th>Monitor Mode</th>
<th>Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet: en0</td>
<td>Ethernet</td>
<td>enabled</td>
<td>default</td>
<td>2</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi: en1</td>
<td>Per-Packet Information</td>
<td>enabled</td>
<td>default</td>
<td>2</td>
<td>enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>p2p0</td>
<td>Raw IP</td>
<td>enabled</td>
<td>default</td>
<td>2</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loopback: lo0</td>
<td>BSD loopback</td>
<td>enabled</td>
<td>default</td>
<td>2</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **OS X - Wireshark**

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
OS X - Notes

• Wireshark Wireless toolbar doesn’t allow changing settings → command line
• No live display or channel change while capturing with built-in GUI tools

• Change channel: `airport -c CHANNEL`
  • No channel validation/list in command line
  • No space between `c` and channel number
Android

- Wi-Fi PCAP Capture
- Other useful tools:
  - CloudShark upload
  - PCAP reader
Android - Set-up

- Connect AWUS036H to a micro USB to USB female adapter to the device
- It will ask if you want to start the app when connecting adapter. Answer Yes.
- First time might fail. Exit, unplug adapter then plug it back
Android - Capture

• Select channel(s) then click on capture at the bottom.
• Use the same button to stop capture
• When done capturing, use Cloudshark, PCAP reader or download capture to computer
Demo

- Windows
  - Airpcap
  - Npcap
- Linux
- BSD
- Android
Which OS has best support?

• One thing to remember:
  • Even if a card says 802.11n or ac, it might not support capturing packets in this mode

• Ranked
  1. Linux – Widest range of adapters/tools supported
  2. Windows – Best adapter
  3. OSX
  4. FreeBSD (> DragonflyBSD > OpenBSD/NetBSD)
     Android
What’s the best adapter?

- **Windows**: Airpcap
- **Linux**:  
  - TP-Link WN722N  
  - Alfa AWUS051NH v2  
- **FreeBSD**:  
  - PCI/MiniPCI: Atheros 5xxx  
  - USB: TEW-648UBM  
- **Android**: Alfa AWUS036H
Resource

• Wireshark documentation: https://wiki.wireshark.org/CaptureSetup/WLAN
That's all Folks!