Real-time Bluetooth Device Detection with Blue Hydra

Granolocks
Zero_Chaos
Granolocks Narcissus

- Pwnie Express
- Focused on device detection
- Enjoys long walks in the woods
- Travel to exotic locations
- Draws pretty weird pictures
- Existential AF
- Hacking the planet
- Gives great back rubs
Zero_Chaos Narcissus

- Eagle Scout
- Open{Zaurus,Embedded,wrt} Maintainer
- Aircrack-ng Developer
  - Injection/Drivers, airmon-zc
- Pentoo Linux Developer
- Gentoo Linux Developer
- Random Hacker of ARMs
- Husband & Father
- Random Association of Wireless Researchers (RAWR)
  - Defcon/Shmoocon/etc Wireless CTF
- Far too easily entertained
- Not a lawyer
What is Bluetooth

- Cheap
- Cable replacement
- Frequency Hopping Spread Spectrum
- No monitor mode :-(
- Class
  - Class 1 100mW (high power devices, Sena dongle)
  - Class 2 10mW (phone / most laptops)
  - Class 3 1mW
Bluetooth Waterfall
Bluetooth Classic

- Discoverable
- Non-discoverable
- Pairing
Bluetooth Low Energy

- General Discoverability
- Limited Discoverability
- Non-discoverable
  - Yet somehow still advertises?
Bluetooth Proliferation

- Random IoT
- Wearables (sales in 2015)
  - Fitbit 21 million
  - Xiaomi 12 million
  - Apple 11.6 million
  - Garmin 3.3 million
  - Samsung 3.1 million
  - Others 27 million
  - Total 78.1 million
- *Source: IDC Worldwide Quarterly Quarterly Wearable Device Tracker, February 23, 2016*
Prior Art - Cracking

- Redfang
- Btcrack
- Crackle
  - Le pin cracker
- Bluesnarfer
  - Phonebook dumping from old phones
Prior Art - Discovery

- **Bluelog**
  - Discoverable classic mode only
  - No le support
  - Mostly a logger

- **Btscanner**
  - Discoverable classic mode only
  - No le support
  - Unmaintained
  - Neat gui
Useful Tools

- Bluez - Useful documentation and examples
- hciconfig
- hcitool
  - Only discoverable classic devices
  - Lescan works but hard to parse
  - outdated
- Test-scripts bluez-test discovery
  - Easy to modify
  - Shows classic and le
  - Hides some le devices
  - Teaches us how to talk to the bluetooth card
  - Only sees “discoverable” devices
Ubertooth

- Ubertooth-scan
- Ubertooth-rx
  - Ubertooth-rx -z
Blue Hydra - Goals

- Like airodump-ng and btscanner
- Support btle
- Find as many devices as possible
- Database backend
- Minimal direct hardware interfacing - for now :)
- *Not interested* in cracking/brute forcing
Blue Hydra design logic

- Languages used (by volume):
  - Ruby, Bash, Python

- Build on top of existing tools
  - Rapid development
  - Modify as needed
  - Minimize need to interact directly with hardware

- Run threads for each discrete task
- Unify into a processing thread
btmon

- Bluez btmon
- Monitor raw hci info passing between system and adapter
- Reasonably Parseable
- Receive info from many different tool commands in one place
- Monitor one or many bluetooth dongles
btmon Threads

- Execute and filter
- Batch messages by devices
- Parse message batches

```
> HCI Event: LE Meta Event (0x3e) plen 36 2016-01-16 09:01:25.623391
   LE Advertising Report (0x02)
   Num reports: 1
   Event type: Connectable undirected - ADV_IND (0x00)
   Address type: Public (0x00)
   Address: [redacted] (Logitech - Ultimate Ears)
   Data length: 24
   Flags: 0x06
       LE General Discoverable Mode
       BR/EDR Not Supported
   Name (short):
   128-bit Service UUIDs (complete): 1 entry
       72daa6c3-29c2-6283-0c4a-2818e4d37e75
   RSSI: -51 dBm (0xcd)
```
Bluetooth Discovery Thread

- Interaction Point with bluetooth device
- Fed commands from a queue
- Run classic discovery (bin/test-discovery)
- Listen for le advertisements (bin/test-discovery)
- Info from classic / le devices (hctiool)
- Test if devices are present (l2ping)
Ubertooth Thread

- Runs and parses ubertooth-rx -z -t
- Bluetooth Classic non-discoverable (transmitting)
- Currently sniffing for Bluetooth Basic Rate connections
- Optional, not a replacement for required BT device
Data processing thread

- Updates records
- Device Correlation
  - MAC
  - UAP/LAP (Ubertooth)
    significant: 00:00:BE:EF:CA:FE
  - LE Proximity ID / Major & Minor Number
    (ibeacon)
- Feedback Loop
CUI Thread

- Command-line User Interface
- Default Behavior
- Live View of devices
- Sortable by column
- Extensible columns to support smaller devices
DEMO

• Doing it live!
**Blue Hydra**: Devices Seen in last 300s

Queue status: result_queue: 0, info_scan_queue: 0, l2ping_queue: 0

Discovery status timers: 34, ubertooth status: not enabled

<table>
<thead>
<tr>
<th>SEEN</th>
<th>VERS</th>
<th>ADDRESS</th>
<th>RSSI</th>
<th>NAME</th>
<th>MANUF</th>
<th>RANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>+25s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:23:27:</strong>:<strong>:</strong></td>
<td>-30</td>
<td>XY-1D17-5E</td>
<td>iBeacon</td>
<td>0.11m</td>
</tr>
<tr>
<td>+163s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:23:29:</strong>:<strong>:</strong></td>
<td>-34</td>
<td>XY-4BF7-63</td>
<td>iBeacon</td>
<td>0.18m</td>
</tr>
<tr>
<td>+111s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:23:29:</strong>:<strong>:</strong></td>
<td>-36</td>
<td>XY-0D27-62</td>
<td>iBeacon</td>
<td>0.22m</td>
</tr>
<tr>
<td>+26s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:23:27:</strong>:<strong>:</strong></td>
<td>-38</td>
<td>XY-1D14-5E</td>
<td>iBeacon</td>
<td>0.09m</td>
</tr>
<tr>
<td>+117s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:23:2B:</strong>:<strong>:</strong></td>
<td>-38</td>
<td>XY-4BF4-63</td>
<td>iBeacon</td>
<td>0.09m</td>
</tr>
<tr>
<td>+18s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:23:29:</strong>:<strong>:</strong></td>
<td>-39</td>
<td>XY-0D24-62</td>
<td>iBeacon</td>
<td>0.09m</td>
</tr>
<tr>
<td>+10s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:5A:23:</strong>:<strong>:</strong></td>
<td>-65</td>
<td>One</td>
<td>Nordic Semiconductor ASA</td>
<td></td>
</tr>
<tr>
<td>+28s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>:BC:DA:</strong>:<strong>:</strong></td>
<td>-79</td>
<td></td>
<td>SamsungE</td>
<td></td>
</tr>
<tr>
<td>SEEN</td>
<td>VERS</td>
<td>ADDRESS</td>
<td>RSSI</td>
<td>NAME</td>
<td>MANUF</td>
<td>RANGE</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>---------------</td>
<td>------</td>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>+0s</td>
<td>BTLE</td>
<td>26:8A:***</td>
<td>-38</td>
<td>Logitech</td>
<td>Logitech</td>
<td></td>
</tr>
<tr>
<td>+2s</td>
<td>BTLE</td>
<td>26:0B:***</td>
<td>-44</td>
<td>Logitech</td>
<td>Logitech</td>
<td></td>
</tr>
<tr>
<td>+91s</td>
<td>BTLE</td>
<td>23:27:***</td>
<td>-51</td>
<td>XY-1D17-5E</td>
<td>iBeacon</td>
<td>1.12m</td>
</tr>
<tr>
<td>+13s</td>
<td>BTLE</td>
<td>23:29:***</td>
<td>-52</td>
<td>iBeacon</td>
<td>iBeacon</td>
<td>1.41m</td>
</tr>
<tr>
<td>+75s</td>
<td>BTLE</td>
<td>23:29:***</td>
<td>-54</td>
<td>XY-0D24-53</td>
<td>iBeacon</td>
<td>0.5m</td>
</tr>
<tr>
<td>+34s</td>
<td>BTLE</td>
<td>23:2C:***</td>
<td>-62</td>
<td>XY-4BF4-63</td>
<td>iBeacon</td>
<td>1.26m</td>
</tr>
<tr>
<td>+74s</td>
<td>BTLE</td>
<td>23:27:***</td>
<td>-62</td>
<td>XY-1D14-5E</td>
<td>iBeacon</td>
<td>1.26m</td>
</tr>
<tr>
<td>+50s</td>
<td>BTLE</td>
<td>E9:70:***</td>
<td>-79</td>
<td>Apple, Inc.</td>
<td>Apple, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

Blue Hydra: Devices Seen in last 300s
Queue status: result_queue: 0, info_scan_queue: 0, l2ping_queue: 0
Discovery status timers: 22, ubertooth status: not enabled
Blue Hydra: Devices Seen in last 300s
Queue status: result_queue: 0, info_scan_queue: 1, 12ping_queue: 0
Discovery status timers: 34, ubertooth status: not enabled

<table>
<thead>
<tr>
<th>SEEN</th>
<th>VERS</th>
<th>ADDRESS</th>
<th>RSSI ^</th>
<th>NAME</th>
<th>MANUF</th>
<th>RANGE</th>
<th>COMPANY</th>
<th>LE COMPANY DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>+7s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>26:8A:</strong>:**</td>
<td>-36</td>
<td>Logitech</td>
<td></td>
<td></td>
<td>not assigned</td>
<td>268a29ee</td>
</tr>
<tr>
<td>+8s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>26:88:</strong>:**</td>
<td>-39</td>
<td>Logitech</td>
<td></td>
<td></td>
<td>not assigned</td>
<td>268b1668</td>
</tr>
<tr>
<td>+26s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>23:27:</strong>:**</td>
<td>-51</td>
<td>XY-1D17-5E</td>
<td>iBeacon</td>
<td>1.12m</td>
<td>Apple, Inc.</td>
<td></td>
</tr>
<tr>
<td>+10s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>23:29:</strong>:**</td>
<td>-54</td>
<td>XY-0D24-53</td>
<td>iBeacon</td>
<td>0.5m</td>
<td>Apple, Inc.</td>
<td></td>
</tr>
<tr>
<td>+9s</td>
<td>BTLE</td>
<td><strong>:</strong>:<strong>23:27:</strong>:**</td>
<td>-62</td>
<td>XY-1D14-5E</td>
<td>iBeacon</td>
<td>1.26m</td>
<td>Apple, Inc.</td>
<td></td>
</tr>
</tbody>
</table>
Where to get it?

- https://github.com/pwnieexpress/blue_hydra
- Download, install deps, run from git checkout
- *or*
- Pentoo 2015.0 RC5 Live iso
Conclusions

- Bluetooth hasn’t been looked at much in years
- Simple idea, harder than expected
- Surprising to see just how many devices are out there
THANKS

- DEF CON for letting us present
- Pwnie Express for paying us to build blue hydra then turning around and letting us open source it
- Coconut Picard for helping us release this code as BSD
- Ubertooth team for being awesome
- Bluez team for our first solid beating
Q & A

Q&A will be in room <fill in the blank>

https://github.com/pwnieexpress/blue_hydra

@Zero_ChaosX
@granolocks