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

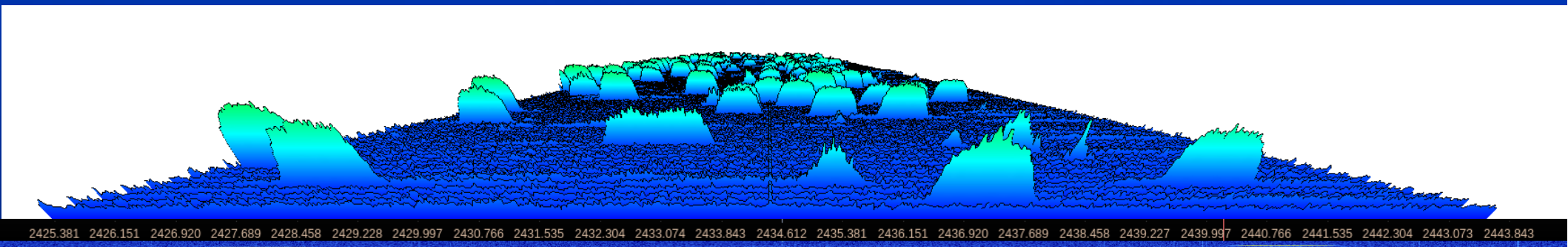


What is Bluetooth

- 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



PWNIE EXPRESS

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 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  - outdated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



PWNIE EXPRESS

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:    :26:51:    (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)
    physical: DE:AD:BE:EF:CA:FE
    ubertooth: ??:??:BE:EF:CA:FE
    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!

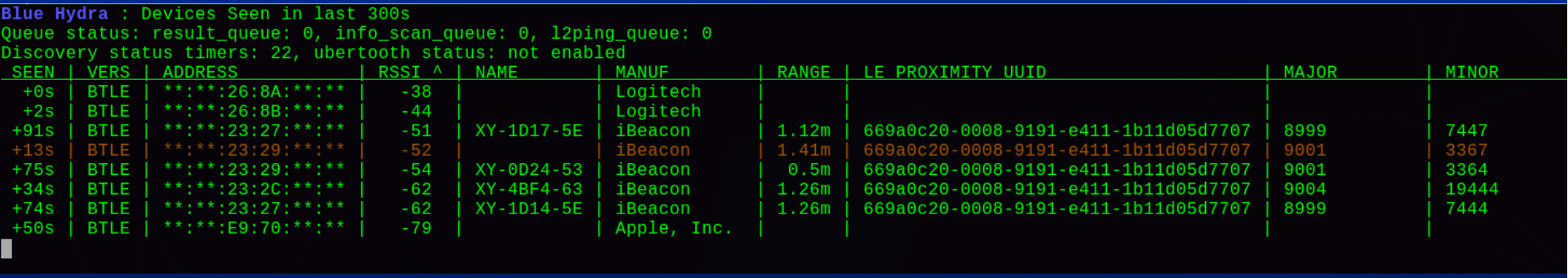


DEMO backup

```
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
 SEEN   | VERS | ADDRESS           | RSSI ^ | NAME        | MANUF                      | RANGE
  +25s  | BTLE | **:**:23:27:**:** |   -30  | XY-1D17-5E  | iBeacon                    | 0.11m
 +163s  | BTLE | **:**:23:2C:**:** |   -34  | XY-4BF7-63  | iBeacon                    | 0.18m
 +111s  | BTLE | **:**:23:29:**:** |   -36  | XY-0D27-62  | iBeacon                    | 0.22m
  +26s  | BTLE | **:**:23:27:**:** |   -38  | XY-1D14-5E  | iBeacon                    | 0.09m
 +117s  | BTLE | **:**:23:2C:**:** |   -38  | XY-4BF4-63  | iBeacon                    | 0.09m
  +18s  | BTLE | **:**:23:29:**:** |   -39  | XY-0D24-62  | iBeacon                    | 0.09m
  +10s  | BTLE | **:**:5A:23:**:** |   -65  | One         | Nordic Semiconductor ASA   |
  +28s  | BTLE | **:**:BC:DA:**:** |   -79  |             | SamsungE                   |
```



DEMO backup


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
SEEN | VERS | ADDRESS | RSSI ^ | NAME | MANUF | RANGE | LE PROXIMITY UUID | MAJOR | MINOR
+0s | BTLE | **:**:26:8A:**:** | -38 | | Logitech | | | |
+2s | BTLE | **:**:26:8B:**:** | -44 | | Logitech | | | |
+91s | BTLE | **:**:23:27:**:** | -51 | XY-1D17-5E | iBeacon | 1.12m | 669a0c20-0008-9191-e411-1b11d05d7707 | 8999 | 7447
+13s | BTLE | **:**:23:29:**:** | -52 | | iBeacon | 1.41m | 669a0c20-0008-9191-e411-1b11d05d7707 | 9001 | 3367
+75s | BTLE | **:**:23:29:**:** | -54 | XY-0D24-53 | iBeacon | 0.5m | 669a0c20-0008-9191-e411-1b11d05d7707 | 9001 | 3364
+34s | BTLE | **:**:23:2C:**:** | -62 | XY-4BF4-63 | iBeacon | 1.26m | 669a0c20-0008-9191-e411-1b11d05d7707 | 9004 | 19444
+74s | BTLE | **:**:23:27:**:** | -62 | XY-1D14-5E | iBeacon | 1.26m | 669a0c20-0008-9191-e411-1b11d05d7707 | 8999 | 7444
+50s | BTLE | **:**:E9:70:**:** | -79 | | Apple, Inc. | | | |


PWNIE
EXPRESS

DEMO backup

```
Blue Hydra : Devices Seen in last 300s
Queue status: result_queue: 0, info_scan_queue: 1, l2ping_queue: 0
Discovery status timers: 34, ubertooth status: not enabled
 SEEN | VERS | ADDRESS           | RSSI ^ | NAME        | MANUF    | RANGE | COMPANY         | LE COMPANY DATA
  +7s | BTLE | **:**:26:8A:**:** |   -36  |             | Logitech |       | not assigned    | 268a29ee
  +8s | BTLE | **:**:26:8B:**:** |   -39  |             | Logitech |       | not assigned    | 268b1668
 +26s | BTLE | **:**:23:27:**:** |   -51  | XY-1D17-5E  | iBeacon  | 1.12m | Apple, Inc.     |
 +10s | BTLE | **:**:23:29:**:** |   -54  | XY-0D24-53  | iBeacon  |  0.5m | Apple, Inc.     |
  +9s | BTLE | **:**:23:27:**:** |   -62  | XY-1D14-5E  | iBeacon  | 1.26m | Apple, Inc.     |
```



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

