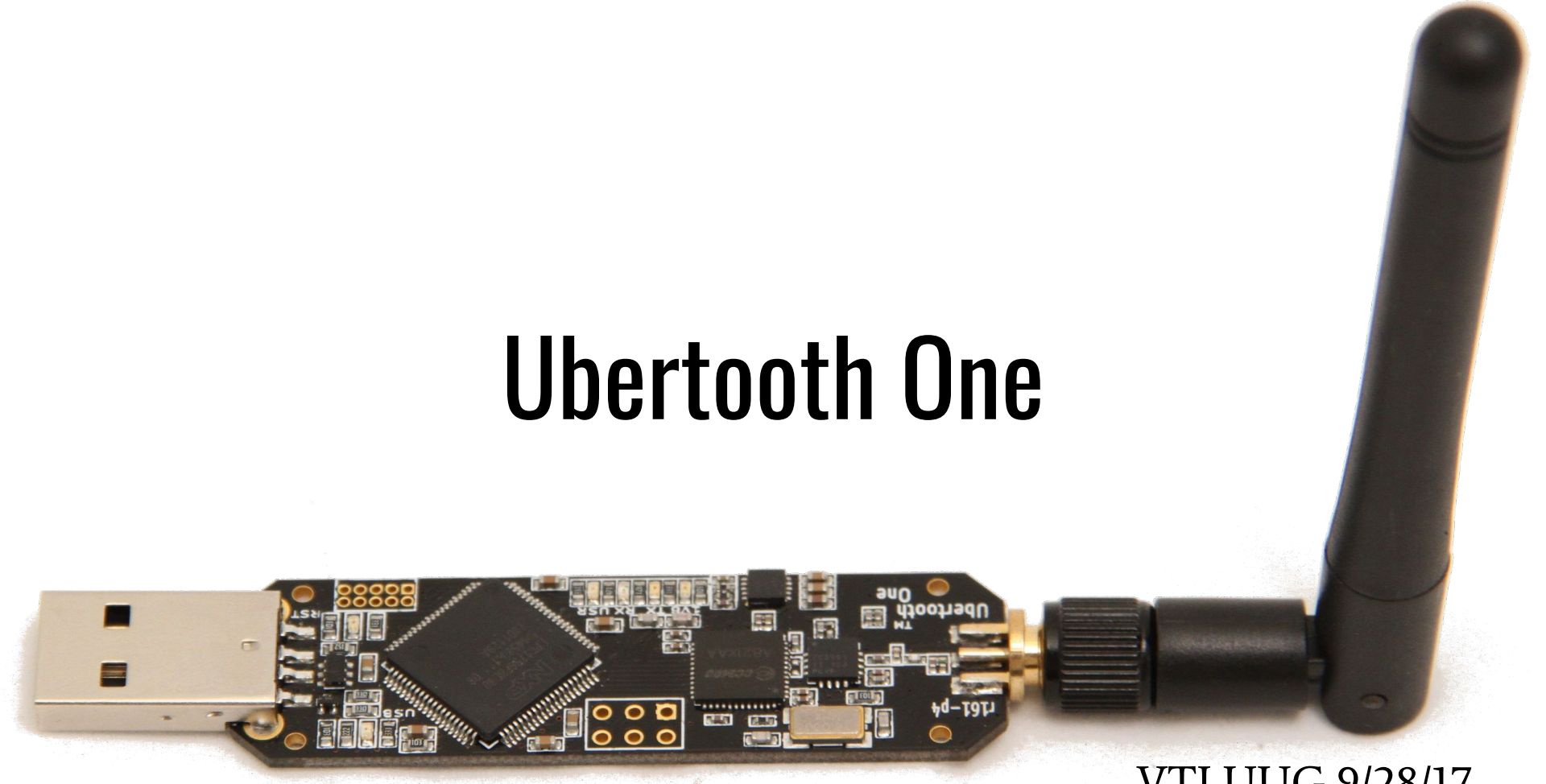
Ubertooth One

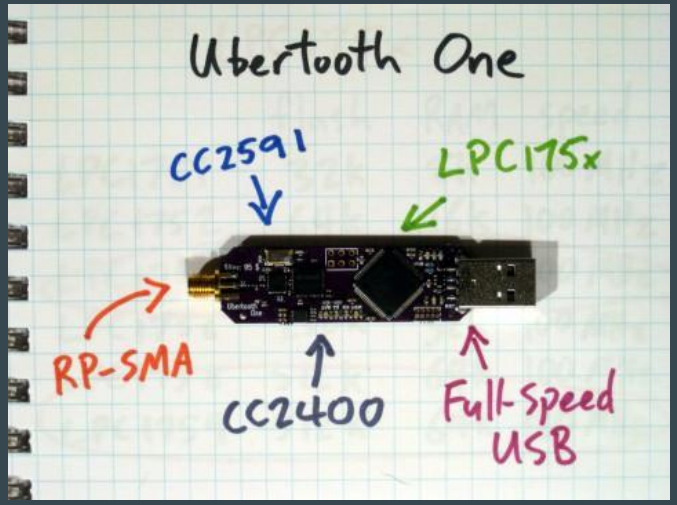


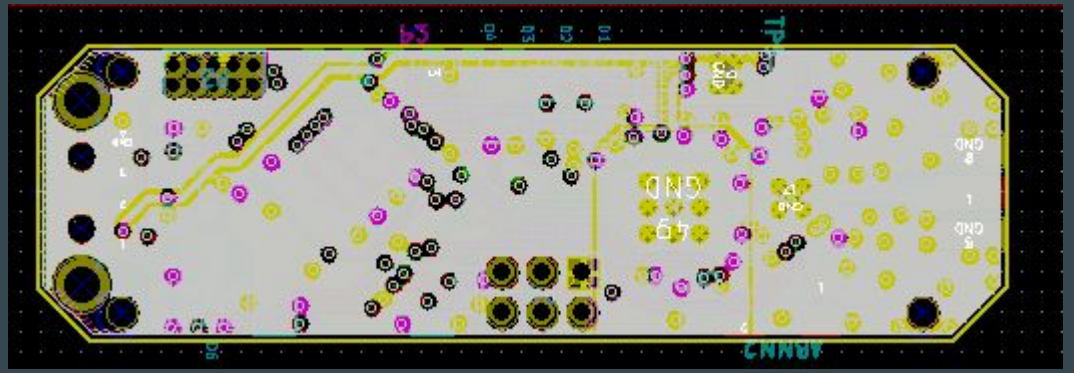
VTLUUG 9/28/17

pew

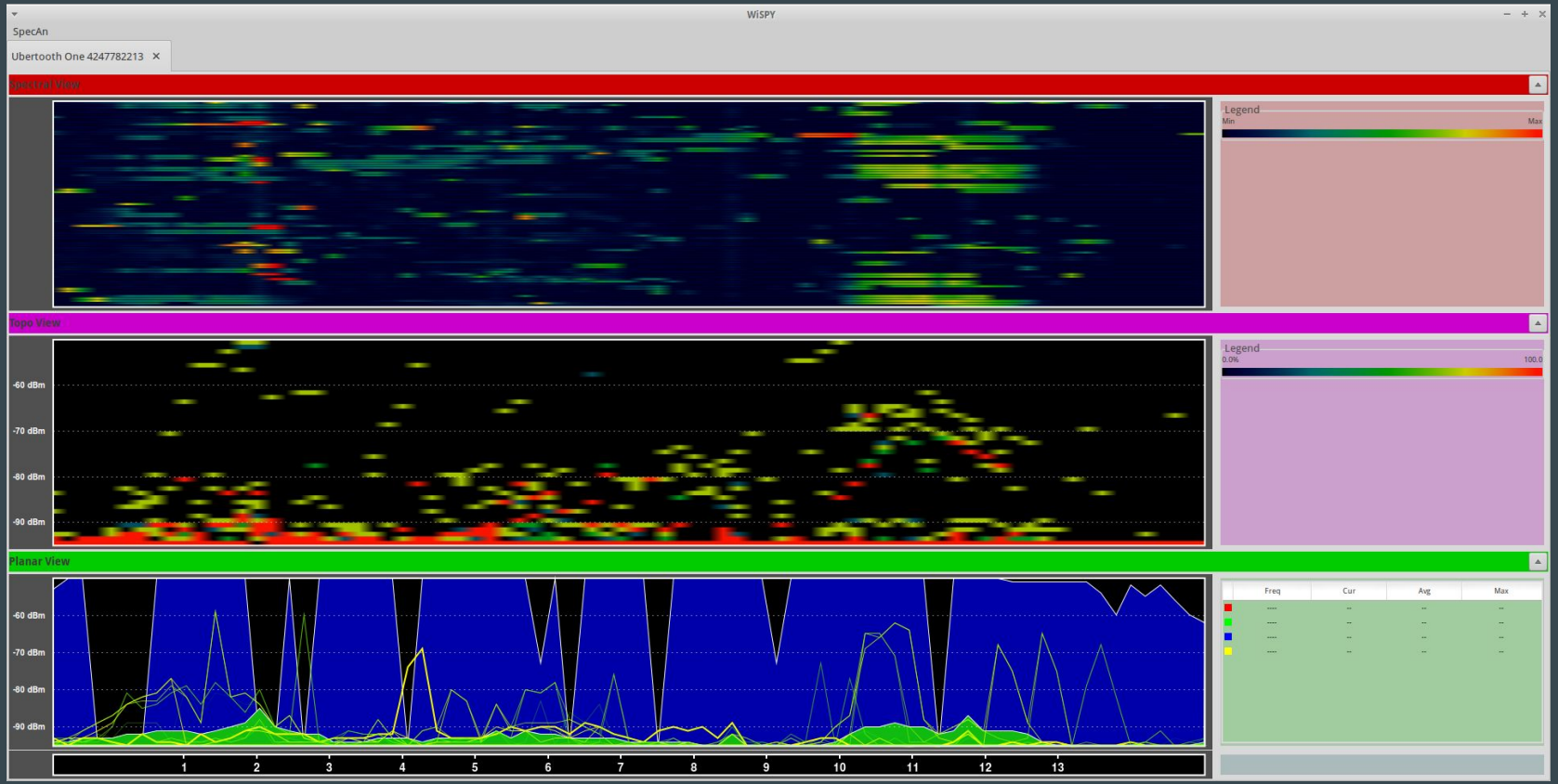
What is it?

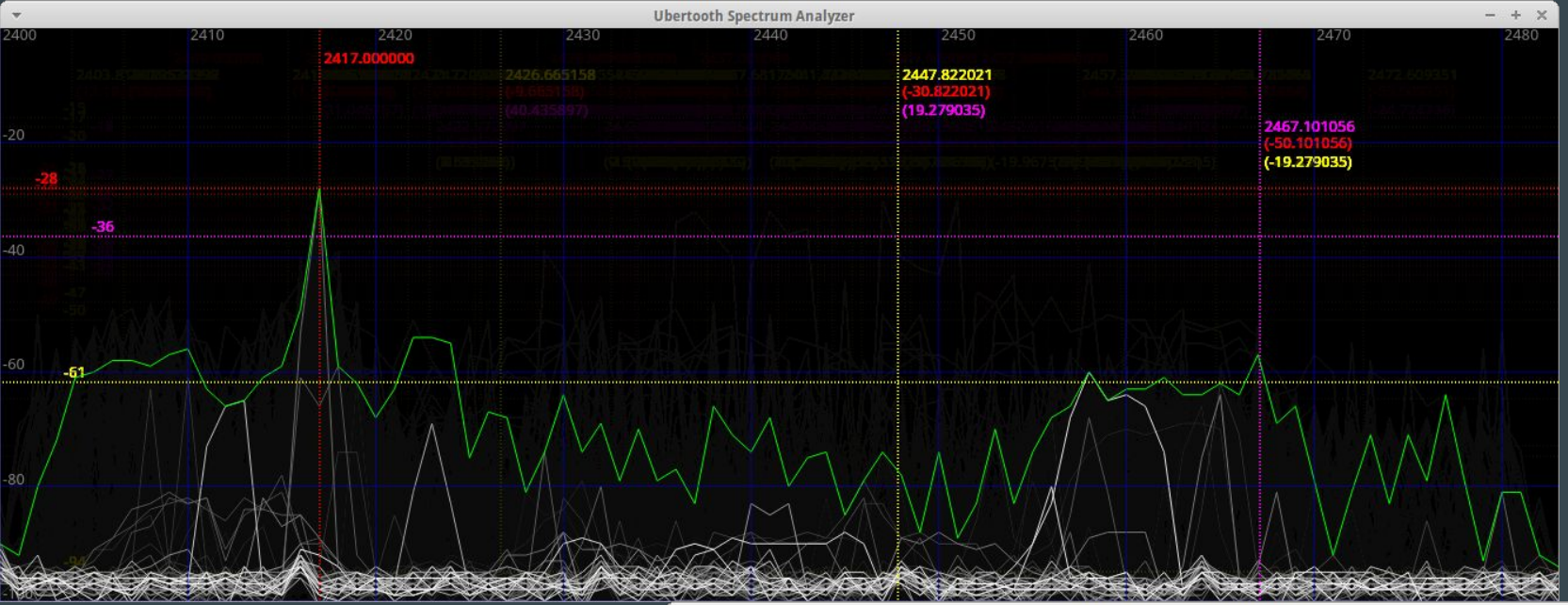
- 2.4GHz
- Wifi Analysis
- Bluetooth Classic
- Bluetooth LE
- $120
- https://github.com/greatscottgadgets/ubertooth
- Open source hardware



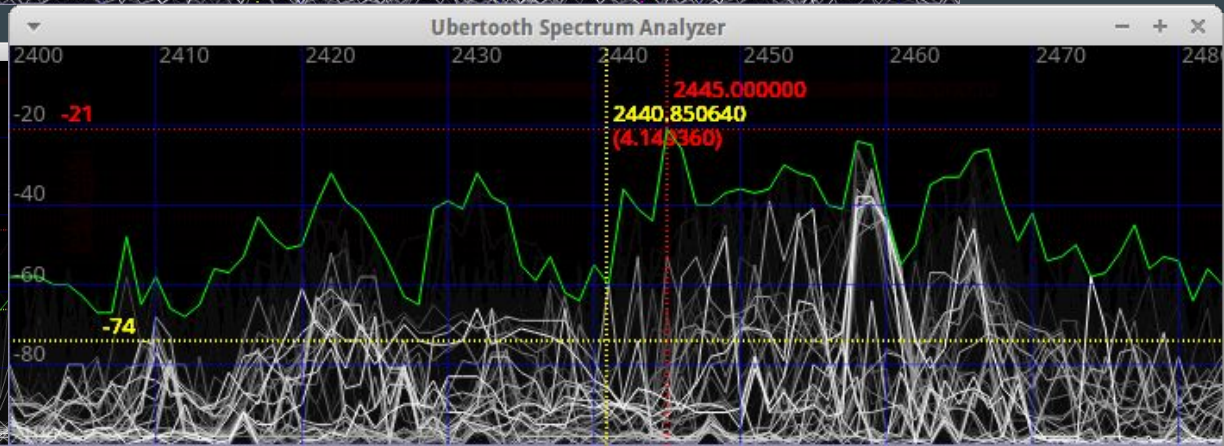


Spectrum Analysis




Ubertooth Spectrum Analyzer
2400
2410
2420
2430
2440
2450
2460
2470
2480
2417.000000
2426.665158
2447.822021
(-30.822021)
(19.279035)
2467.101056
(-50.101056)
(-19.279035)
-20
-28
-36
-40
-60
-61
-80

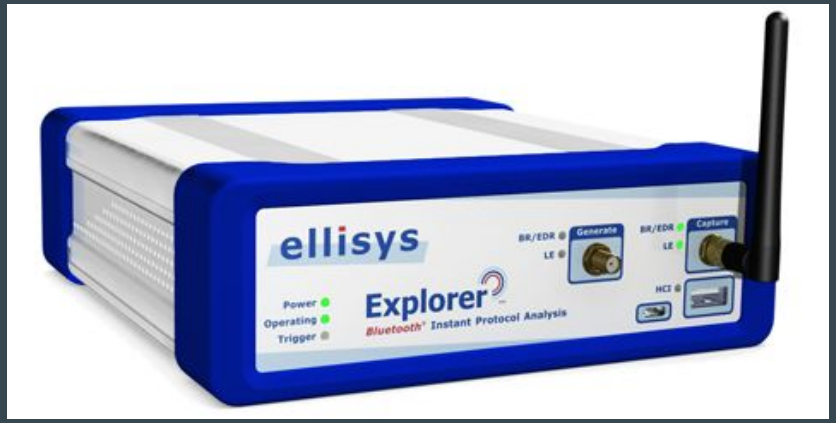
Ubertooth Spectrum Analyzer
2400
2410
2420
2430
2440
2450
2416.000000
2448.197587
(-32.197587)
-20
-40
-44
-60
-64
-80


Ubertooth Spectrum Analyzer
2400
2410
2420
2430
2440
2450
2460
2470
2445.000000
2440.850640
(4.149360)
-20
-21
-40
-60
-74
-80

Why Ubertooth?

Only BR/BLE sniffer

Only $25k

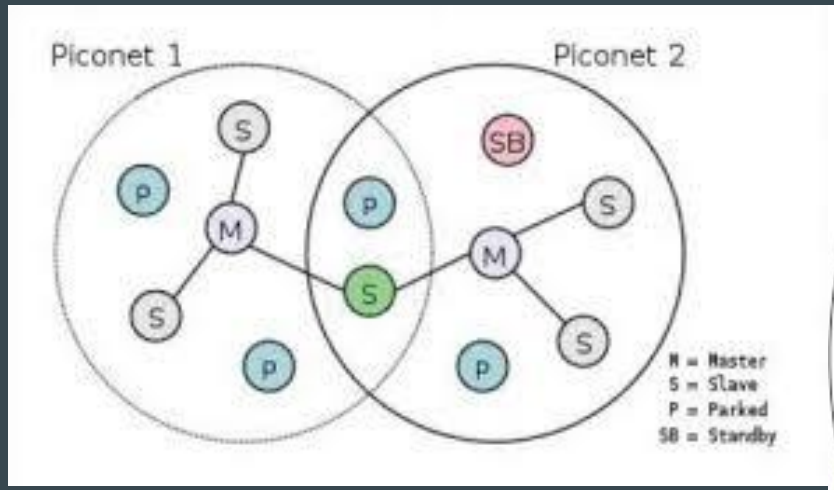


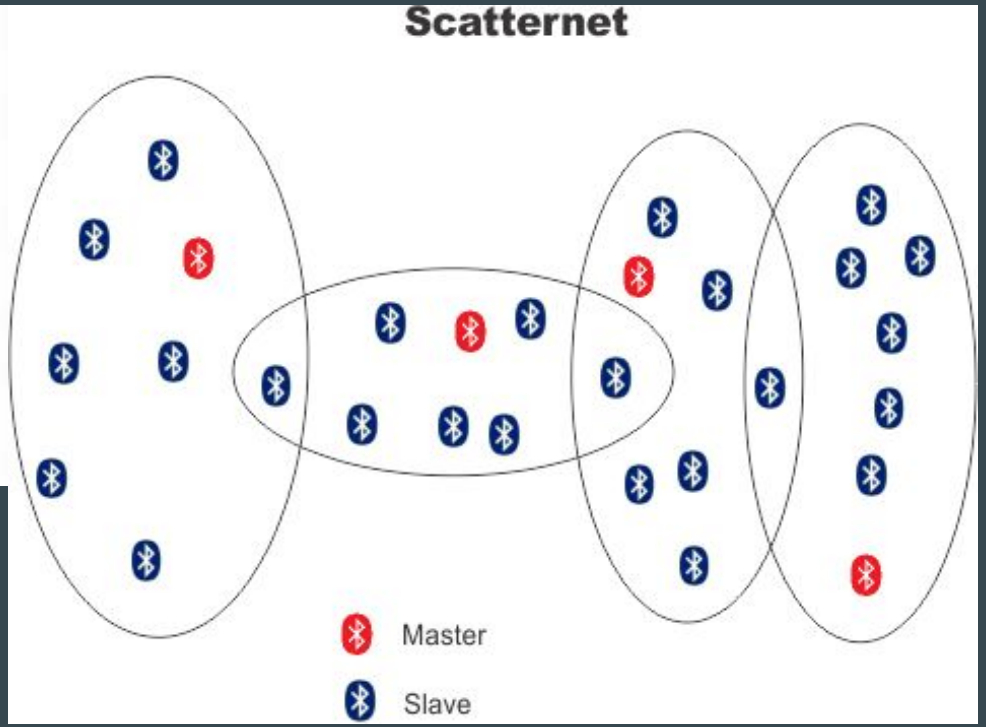
IoT

How do I do stuff with it?

- https://hakshop.myshopify.com/products/ubertooth-one
- Follow this guide and watch lots of videos talks:
  - https://github.com/greatscottgadgets/ubertooth/wiki
- https://google.com

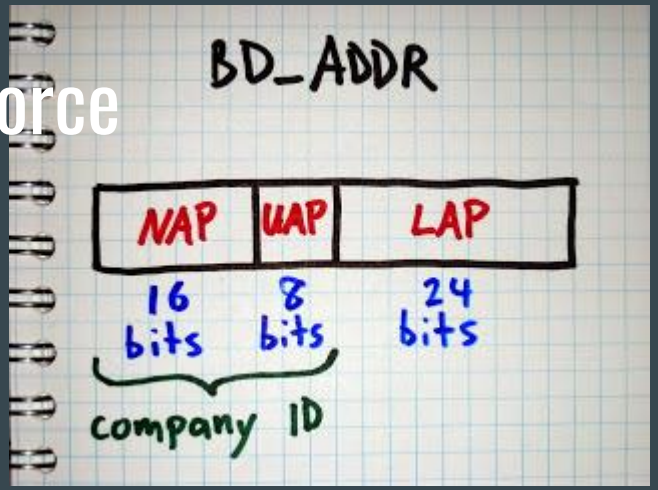
Bluetooth piconet





Need to know master

Discovering Devices (Classic) - Brute Force

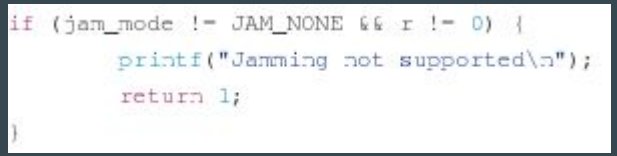


- NAP = Non-significant address part
- UAP = Upper address part
- LAP = Lower address part
- Need UAP + LAP of master device
- LAP is transmitted, UAP not so much
- Since UAP is only 8 bits, brute force works (most of the time)
- Limited # of bluetooth manufactures, so UAP can be easy to find
    - Monitorable, devices aren't always connected

Discovering Devices (BLE)

- Much more straightforward
- Ubertooth sees address of devices when they transmit and gets Adaptive Frequency Hopping (AFH) Map
- Ubertooth is sent data then XOR's with Linear Feedback Shift Register
  - More on that here:
  - http://ubertooth.blogspot.com/2013/05/speeding-up-crc-calculations-for.html
- Packets are then output to PCAP format :)

Viewing data from BLE PCAP output

- Crackle is used to decrypt BLE data
  - https://github.com/mikeryan/crackle/
- Requires pairing process to be captured
- Some devices advertise using BLE, then switch to classic bluetooth for pairing and data transfer
- Ubertooth doesn't support incomplete AFH maps yet, Google Wear might use this. (Not enough tests to be sure)
- Jamming isn't supported, even though some people say it is
  - 

```
if (jam_mode != JAM_NONE && r != 0) {
        printf("Jamming not supported\n");
        return 1;
}
```

If you happen to have BLE device on you, turn it on

The more connections, the better chance for interception

Demo

- Follow along: https://github.com/greatscottgadgets/ubertooth/wiki
  - Or google “ubertooth github”
- BLE PCAP capture
- ubertooth-btle -f -c /tmp/pipe
- btle.data_header.length > 0 || btle.advertising_header.pdu_type == 0x05
  - Filter out important information
- Hopefully I’ll have a working example in the next 2-3 weeks

Cracking BLE

- https://github.com/mikeryan/crackle
-

Questions?

Documentation

- Lots of talks, but not very good documentation.
  - Github wiki is the best way to get started

http://lacklustre.net/bluetooth/#talks

Bluetooth Packet Sniffing Using Project Ubertooth - Dominic Spill

https://www.youtube.com/watch?v=HU5qi7wimAM

http://ubertooth.blogspot.com/

Bad opsec

Never post passwords in open channels...

or open email lists

2014

Hey all

The undergrad and graduate teams for CSAW are posted below. practice before Friday.

Undergrad Team Name: **CARDiac Arrest**
Password: eV#5G*z30lYp&WT

Graduate/Other Team Name: **Team ' or 1=1 --**
Password: eV#5G*z30lYp&WT

Thanks,

2015

9:45 AM

ok

Welcome to CSAW

guiez

look

Team name is CARDiac Arrest

for undergrads

Team ' or 1=1 for everyone else

password for both is eV#5G*z30lYp&WT

2016

Hey all

CSAW capture the flag competition starts Friday (9/16) and goes thr
can qualify to fly out to New York if they score high enough. The und

Here is the deets:

Website: https://ctf.csaw.io/
Helpful resources to get started: https://captf.com/practice-ctf/

Undergrad Team
Team name (username): CARDiac Arrest
Password: Security1

Everyone Else
Team name: ' or 1=1
Password: Security1

Thanks,