IoT Red Team

Adithya Rao Alkankara

Ashton Sopher

Daniel Chong

Joseph Shenouda

Justin Wang

Rishika Sakhuja

Samuel Minkin

Objective

To successfully attack the Blue Team's Internet of Things system.

There are three primary types of attacks we will be trying to conduct.

- Sniffing: reading data that is being sent.
- Jamming: preventing data from being sent (ex. interfering with signals).
- Spoofing: sending fake or edited data without Blue Team noticing.

Methods and Technologies

Software:

- openHAB IoT framework
- GNU Radio

Sensors:

- TI Sensortag CC2650
- TI Sensortag CC2541
- Pip Sensor

Other hardware:

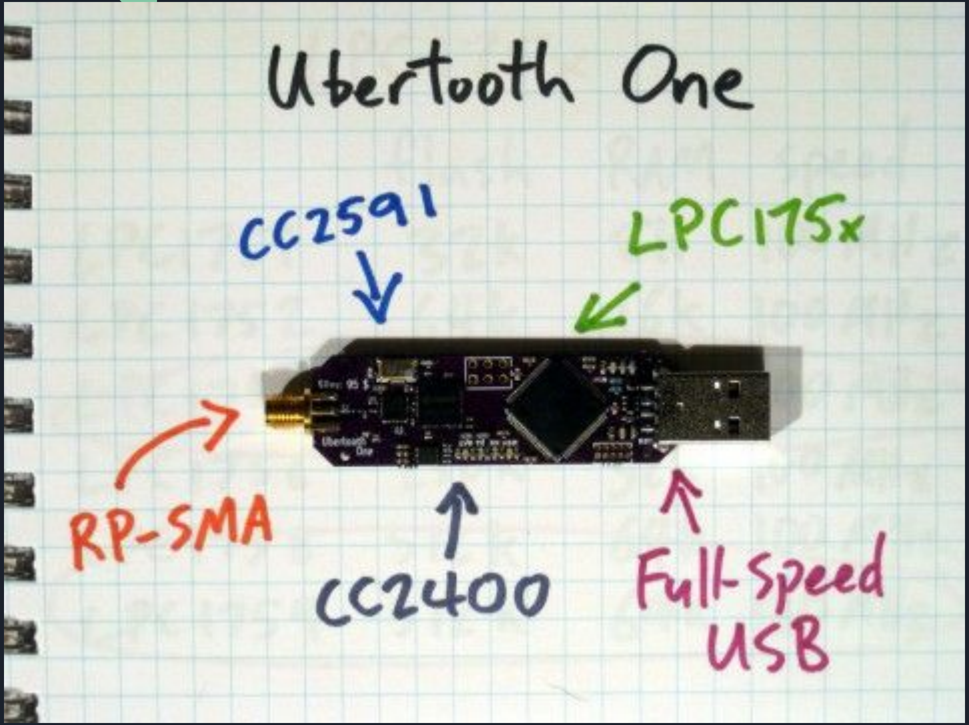
- Ubertooth One
- WINLAB ORBIT
- USRP X310

This Past Week

- Researched specific Bluetooth attack strategies
- Researched various IoT frameworks
- Acquired an Ubertooth one and set it up on our computers to detect nearby bluetooth traffic
- Got started with Wireshark and its various capabilities and functions

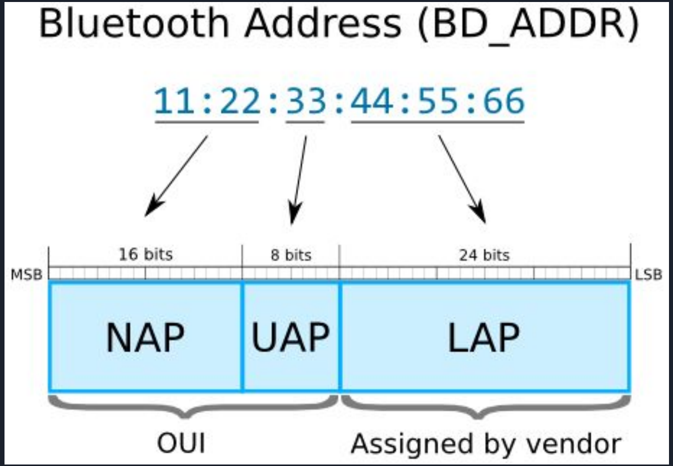
Ubertooth One
The world's first affordable Bluetooth monitoring and development platform.

Ubertooth One



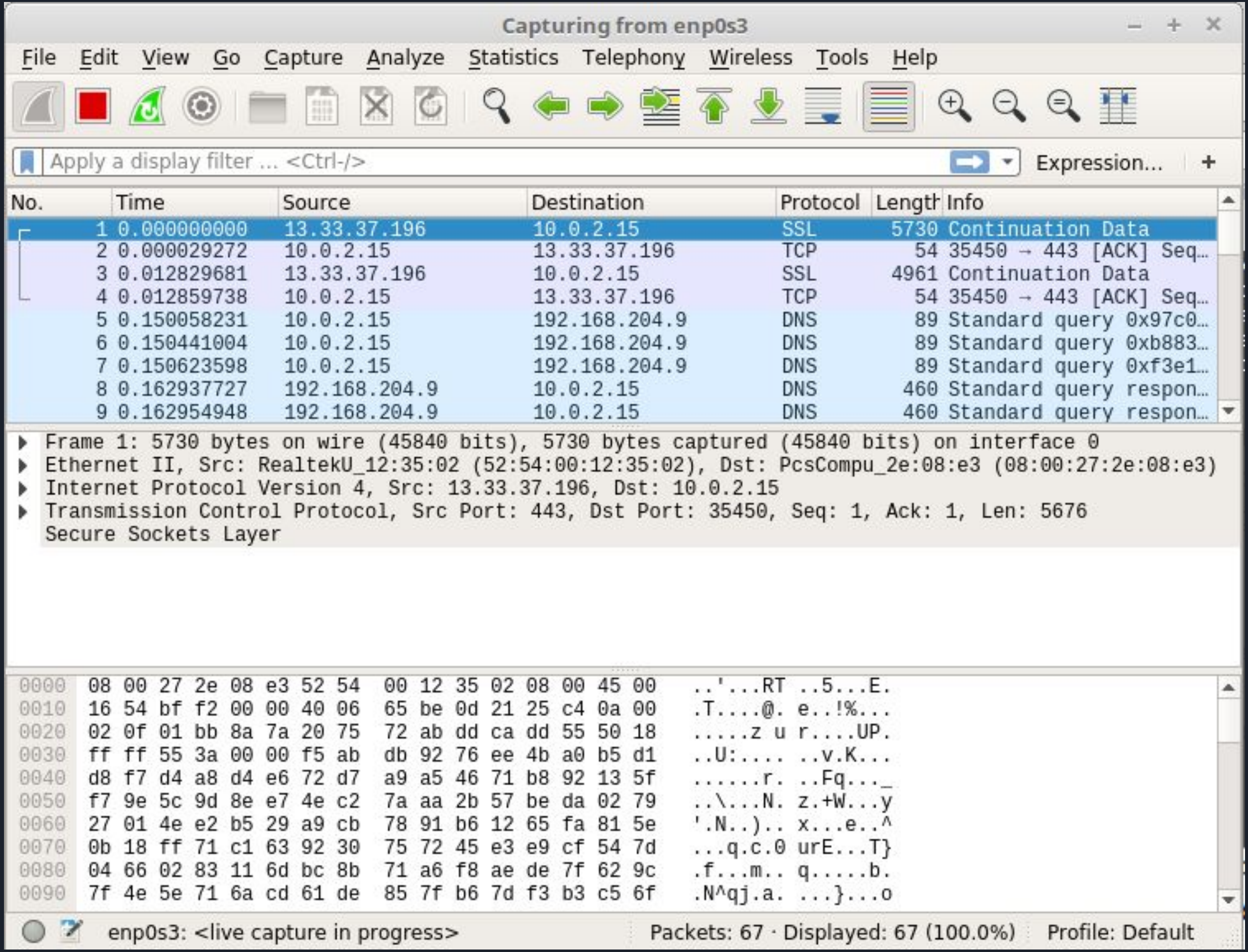
Features:

- Open source 2.4GHz device used for bluetooth experimentation
- Not only sends and receives 2.4GHz signals but can also work in monitor mode capturing bluetooth traffic in real time
- Ubertooth one software allows us to track all the bluetooth



WIRESHARK

- Open-source application to sniff data back and forth off of ethernet, WiFi, BLE or a Raw USB traffic.
- Designed to understand structures (encapsulation) of different protocols.
- Equipped with bunch of filters to read specific data
- Mainly used to troubleshoot network issues and also to develop and test software.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	13.33.37.196	10.0.2.15	SSL	5730	Continuation Data
2	0.000029272	10.0.2.15	13.33.37.196	TCP	54	35450 → 443 [ACK] Seq…
3	0.012829681	13.33.37.196	10.0.2.15	SSL	4961	Continuation Data
4	0.012859738	10.0.2.15	13.33.37.196	TCP	54	35450 → 443 [ACK] Seq…
5	0.150058231	10.0.2.15	192.168.204.9	DNS	89	Standard query 0x97c0…
6	0.150441004	10.0.2.15	192.168.204.9	DNS	89	Standard query 0xb883…
7	0.150623598	10.0.2.15	192.168.204.9	DNS	89	Standard query 0xf3e1…
8	0.162937727	192.168.204.9	10.0.2.15	DNS	460	Standard query respon…
9	0.162954948	192.168.204.9	10.0.2.15	DNS	460	Standard query respon…

```
▸ Frame 1: 5730 bytes on wire (45840 bits), 5730 bytes captured (45840 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_2e:08:e3 (08:00:27:2e:08:e3)
▸ Internet Protocol Version 4, Src: 13.33.37.196, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 35450, Seq: 1, Ack: 1, Len: 5676
  Secure Sockets Layer
```

```
0000  08 00 27 2e 08 e3 52 54  00 12 35 02 08 00 45 00   ..'...RT ..5...E.
0010  16 54 bf f2 00 00 40 06  65 be 0d 21 25 c4 0a 00   .T....@. e..!%...
0020  02 0f 01 bb 8a 7a 20 75  72 ab dd ca dd 55 50 18   .....z u r....UP.
0030  ff ff 55 3a 00 00 f5 ab  db 92 76 ee 4b a0 b5 d1   ..U:.... ..v.K...
0040  d8 f7 d4 a8 d4 e6 72 d7  a9 a5 46 71 b8 92 13 5f   ......r. ..Fq..._
0050  f7 9e 5c 9d 8e e7 4e c2  7a aa 2b 57 be da 02 79   ..\...N. z.+W...y
0060  27 01 4e e2 b5 29 a9 cb  78 91 b6 12 65 fa 81 5e   '.N..).. x...e..^
0070  0b 18 ff 71 c1 63 92 30  75 72 45 e3 e9 cf 54 7d   ...q.c.0 urE...T}
0080  04 66 02 83 11 6d bc 8b  71 a6 f8 ae de 7f 62 9c   .f...m.. q.....b.
0090  7f 4e 5e 71 6a cd 61 de  85 7f b6 7d f3 b3 c5 6f   .N^qj.a. ...}...o
```

enp0s3: <live capture in progress>   Packets: 67 · Displayed: 67 (100.0%)   Profile: Default

This Coming Week

- Figure out how to use GNU Radio and Software-Defined Radios
- Read packets captured by Wireshark
- Learn about Z-wave attacks with EZ-wave

First Attack !!!!!!!!!