Sprint 2 Boeing Bluetooth Protocol Analytical Research

By: Caroline Terre, Matthew Irvin, Gianna Scarangelli, Jonah Rowell, Connal Grace

EMBRY-RIDDLE
Aeronautical University

Bluetooth

- Short range wireless data transfer standard
- Operates at around 2.4 GHz
- Used in tables, smartphones and laptops
- Used for high data transfer rate applications

Zigbee

- Operates around 2.4 GHz and 900 MHz
- IEEE 802.15.4-based
- Often used for low power, low data and low cost
- Commonly used in mesh networks

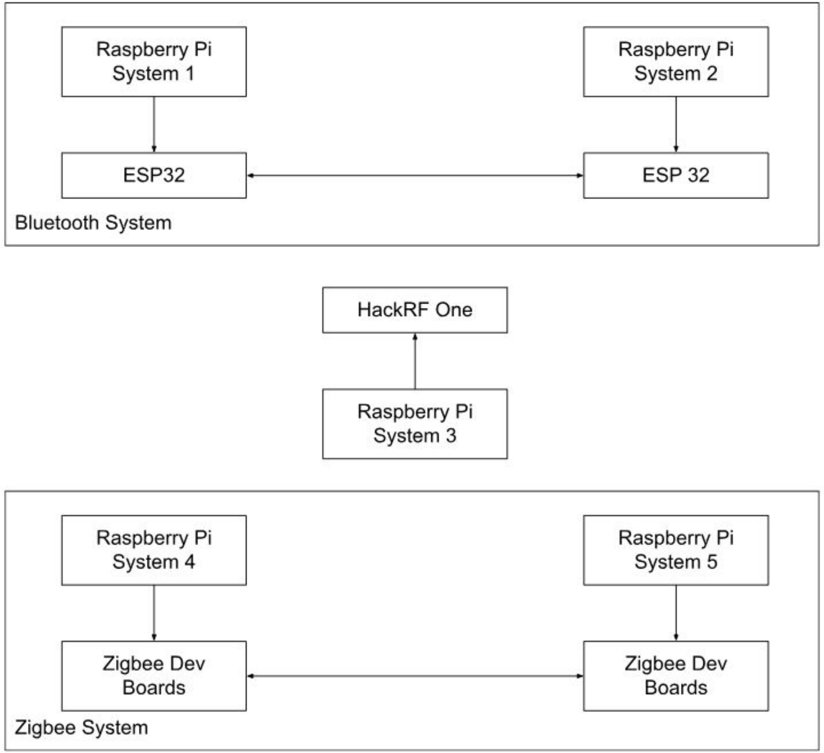
Devices

ESP32

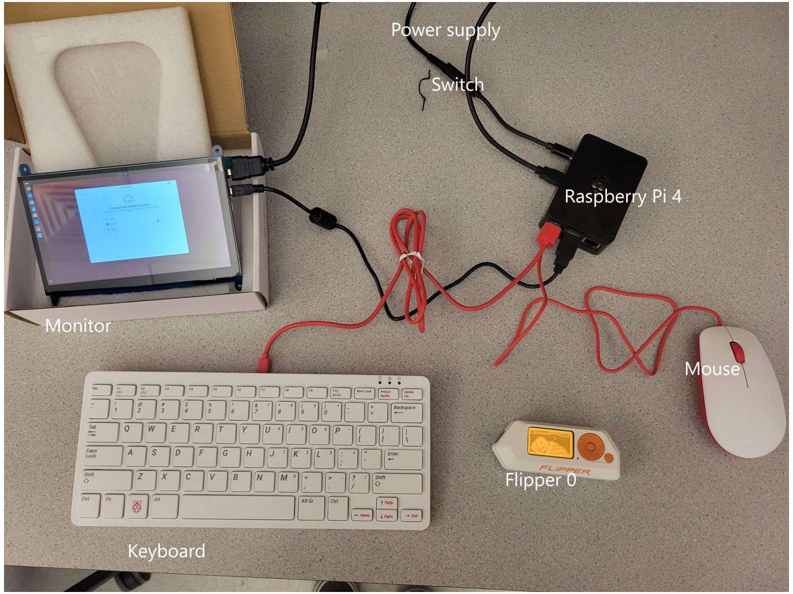
HackRF One

Zigbee Dev Board

Testbed



Raspberry Pi System 1
Raspberry Pi System 2
ESP32
ESP 32
Bluetooth System
HackRF One
Raspberry Pi System 3
Raspberry Pi System 4
Raspberry Pi System 5
Zigbee Dev Boards
Zigbee Dev Boards
Zigbee System



Power supply
Switch
Raspberry Pi 4
Monitor
Mouse
Flipper 0
Keyboard

Requirements

- External Interface
  - User Interfaces
  - Hardware
  - Software
  - Communications
- System Features
  - Test Plan
  - Bluetooth Connectivity
  - Zigbee Connectivity
- Nonfunctional Requirements
  - Performance
  - Safety
  - Security

Operating Systems

Kali Linux (Caroline and Connal)

- Linux distribution designed for cybersecurity and penetration testing

Ubuntu (Matt)

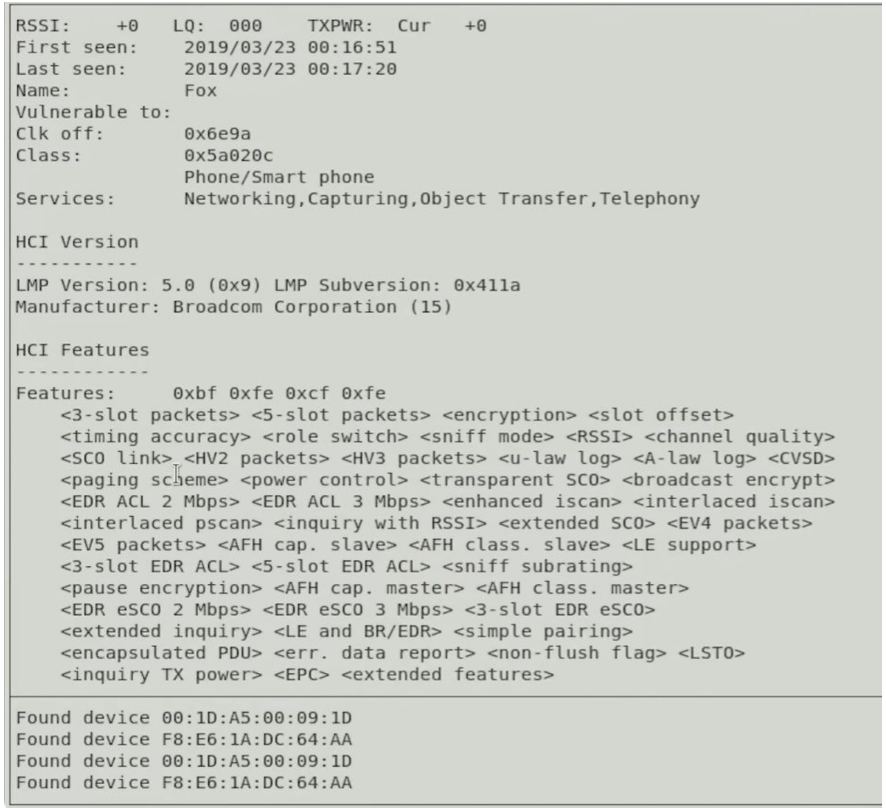
- Open-source linux distribution
- General purpose operating system

Raspberry Pi OS (Jonah and Gia)

- Based on Debian-Linux distribution
- Optimized for the Raspberry Pi architecture

Kali Linux

btscanner on Kali Linux



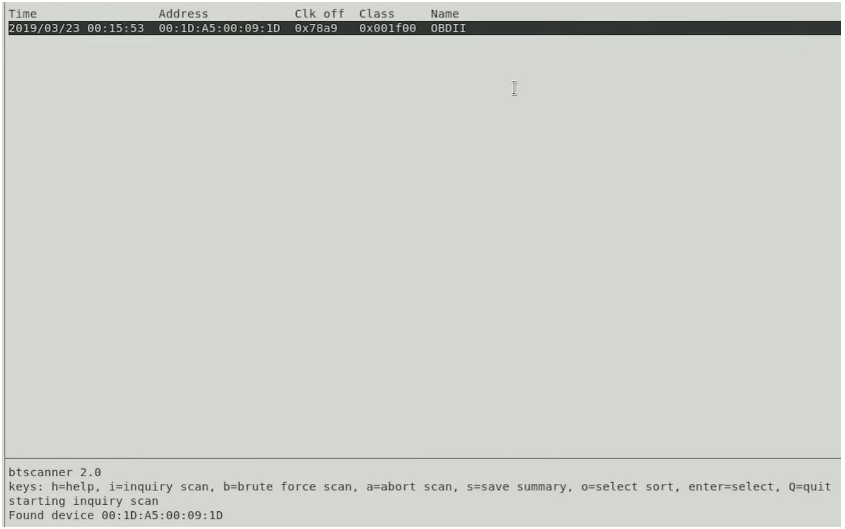
```
RSSI:    +0    LQ:  000    TXPWR:  Cur   +0
First seen:    2019/03/23 00:16:51
Last seen:     2019/03/23 00:17:20
Name:          Fox
Vulnerable to:
Clk off:       0x6e9a
Class:         0x5a020c
               Phone/Smart phone
Services:      Networking,Capturing,Object Transfer,Telephony

HCI Version
-----------
LMP Version: 5.0 (0x9) LMP Subversion: 0x411a
Manufacturer: Broadcom Corporation (15)

HCI Features
------------
Features:     0xbf 0xfe 0xcf 0xfe
    <3-slot packets> <5-slot packets> <encryption> <slot offset>
    <timing accuracy> <role switch> <sniff mode> <RSSI> <channel quality>
    <SCO link> <HV2 packets> <HV3 packets> <u-law log> <A-law log> <CVSD>
    <paging scheme> <power control> <transparent SCO> <broadcast encrypt>
    <EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan> <interlaced iscan>
    <interlaced pscan> <inquiry with RSSI> <extended SCO> <EV4 packets>
    <EV5 packets> <AFH cap. slave> <AFH class. slave> <LE support>
    <3-slot EDR ACL> <5-slot EDR ACL> <sniff subrating>
    <pause encryption> <AFH cap. master> <AFH class. master>
    <EDR eSCO 2 Mbps> <EDR eSCO 3 Mbps> <3-slot EDR eSCO>
    <extended inquiry> <LE and BR/EDR> <simple pairing>
    <encapsulated PDU> <err. data report> <non-flush flag> <LSTO>
    <inquiry TX power> <EPC> <extended features>

Found device 00:1D:A5:00:09:1D
Found device F8:E6:1A:DC:64:AA
Found device 00:1D:A5:00:09:1D
Found device F8:E6:1A:DC:64:AA
```

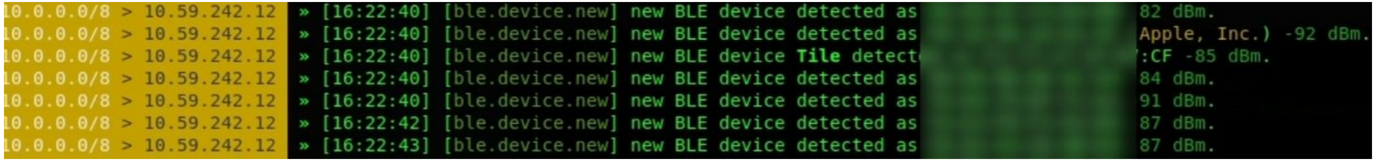
This image displays detailed specifications of a Bluetooth device, showcasing its name, manufacturer, supported services, and various HCI features. Utilizing this utility to understand the characteristics of Bluetooth devices can also highlight potential vulnerabilities or susceptibility to specific cyber threats



```
Time                 Address            Clk off  Class     Name
2019/03/23 00:15:53  00:1D:A5:00:09:1D  0x78a9   0x001f00  OBDII

btscanner 2.0
keys: h=help, i=inquiry scan, b=brute force scan, a=abort scan, s=save summary, o=select sort, enter=select, Q=quit
starting inquiry scan
Found device 00:1D:A5:00:09:1D
```

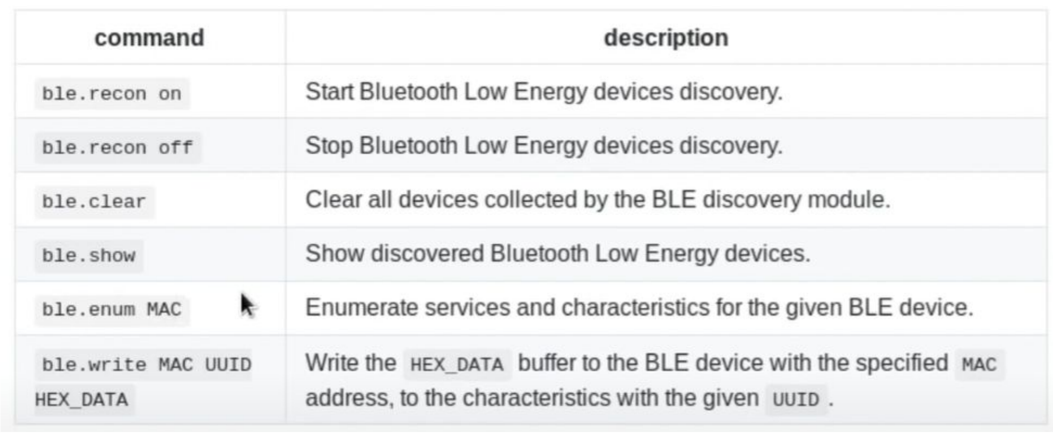
Kali Linux



```
10.0.0.0/8 > 10.59.242.12  » [16:22:40] [ble.device.new] new BLE device detected as [redacted] 82 dBm.
10.0.0.0/8 > 10.59.242.12  » [16:22:40] [ble.device.new] new BLE device detected as [redacted] Apple, Inc.) -92 dBm.
10.0.0.0/8 > 10.59.242.12  » [16:22:40] [ble.device.new] new BLE device Tile detect[redacted]:CF -85 dBm.
10.0.0.0/8 > 10.59.242.12  » [16:22:40] [ble.device.new] new BLE device detected as [redacted] 84 dBm.
10.0.0.0/8 > 10.59.242.12  » [16:22:40] [ble.device.new] new BLE device detected as [redacted] 91 dBm.
10.0.0.0/8 > 10.59.242.12  » [16:22:42] [ble.device.new] new BLE device detected as [redacted] 87 dBm.
10.0.0.0/8 > 10.59.242.12  » [16:22:43] [ble.device.new] new BLE device detected as [redacted] 87 dBm.
```

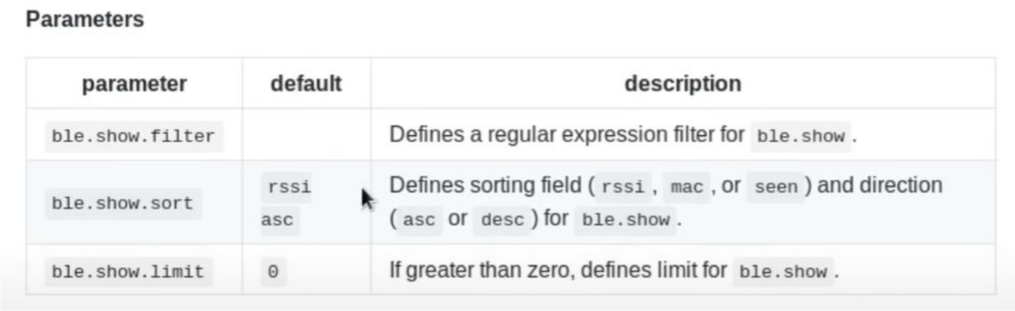
Bettercap on Kali Linux

Commands



command	description
`ble.recon on`	Start Bluetooth Low Energy devices discovery.
`ble.recon off`	Stop Bluetooth Low Energy devices discovery.
`ble.clear`	Clear all devices collected by the BLE discovery module.
`ble.show`	Show discovered Bluetooth Low Energy devices.
`ble.enum MAC`	Enumerate services and characteristics for the given BLE device.
`ble.write MAC UUID HEX_DATA`	Write the `HEX_DATA` buffer to the BLE device with the specified `MAC` address, to the characteristics with the given `UUID` .

Parameters



parameter	default	description
`ble.show.filter`		Defines a regular expression filter for `ble.show` .
`ble.show.sort`	`rssi asc`	Defines sorting field (`rssi` , `mac` , or `seen`) and direction (`asc` or `desc`) for `ble.show` .
`ble.show.limit`	`0`	If greater than zero, defines limit for `ble.show` .

Difficulties with Sprint 2

- Getting equipment from the IT department
- Cannot openly access information on Bluetooth and Zigbee vulnerabilities
- Attend two rooms now when meeting
- Setting up Raspberry Pi's
  - Length of time setting up Raspberry Pi's
  - Installing operating systems
  - Missing SD cards for Flipper 0's

Future Goals

- Finish setting up systems on all Raspberry Pi’s
- Set up HackRF One with Kali
- GNU Radio software set up
- Figure out how to adapt software to hardware for use
- Get bluetooth connection functioning
- Have fully set up test-bed according to our system requirements standards