Boeing Bluetooth Protocol Analytical Research, Semester 2 Sprint 1

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

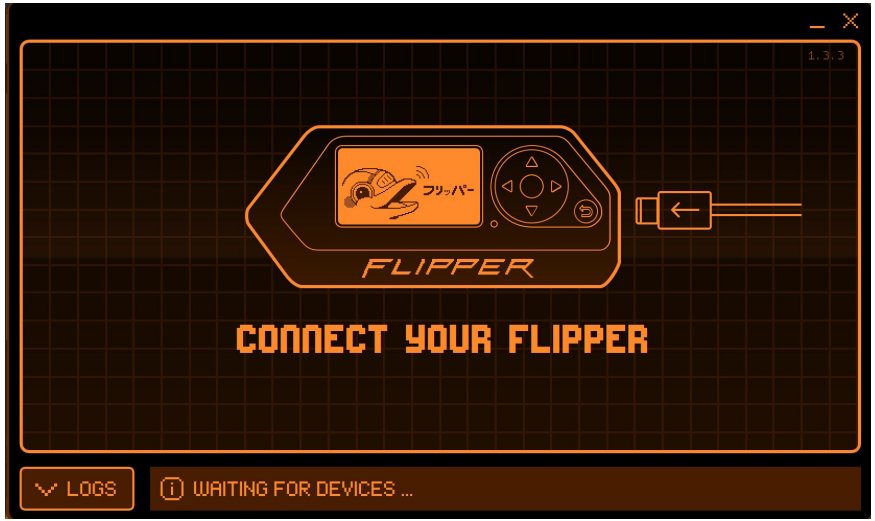
EMBRY-RIDDLE
Aeronautical University

Sprint Overview

- Ordered new equipment
- Focusing on Flipper Zero research
- Receiving and decoding Bluetooth Low Energy packets
- Collecting data from last semester

Flipper Zero

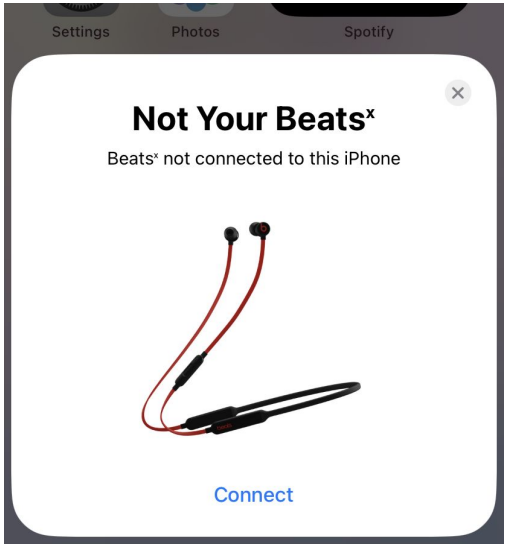
- Virtual Pet Game: various emulating capabilities
- Capitalizing off of its Bluetooth Low Energy Capabilities
  - Has Bluetooth to connect to iPhone app, for example, but cannot use Bluetooth otherwise



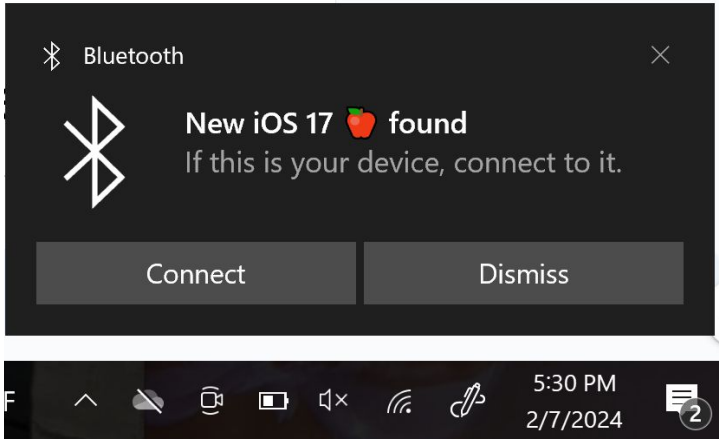
Flipper Zero

- Firmware from Github with excellent document
- Allows BLE attacks such as:

iOS 17 Lockup Crash



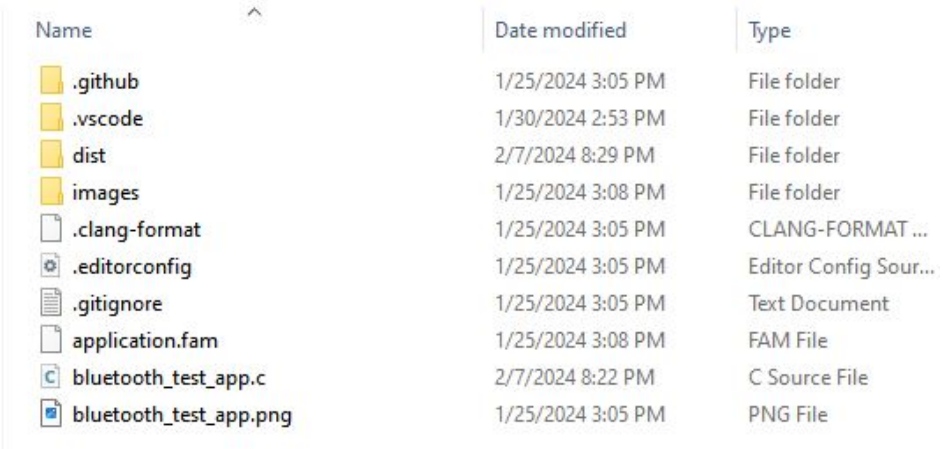
Apple Device Popup



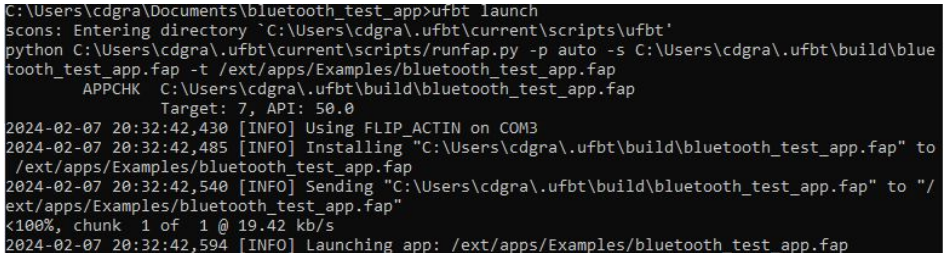
Windows Device Found

Flipper Zero Apps

- Flipper Zero apps - custom programs for the flipper zero that can interact with the Flipper Zero's built in Bluetooth
- uFBT - a python library that simulates the Flipper Zero's firmware to help create apps



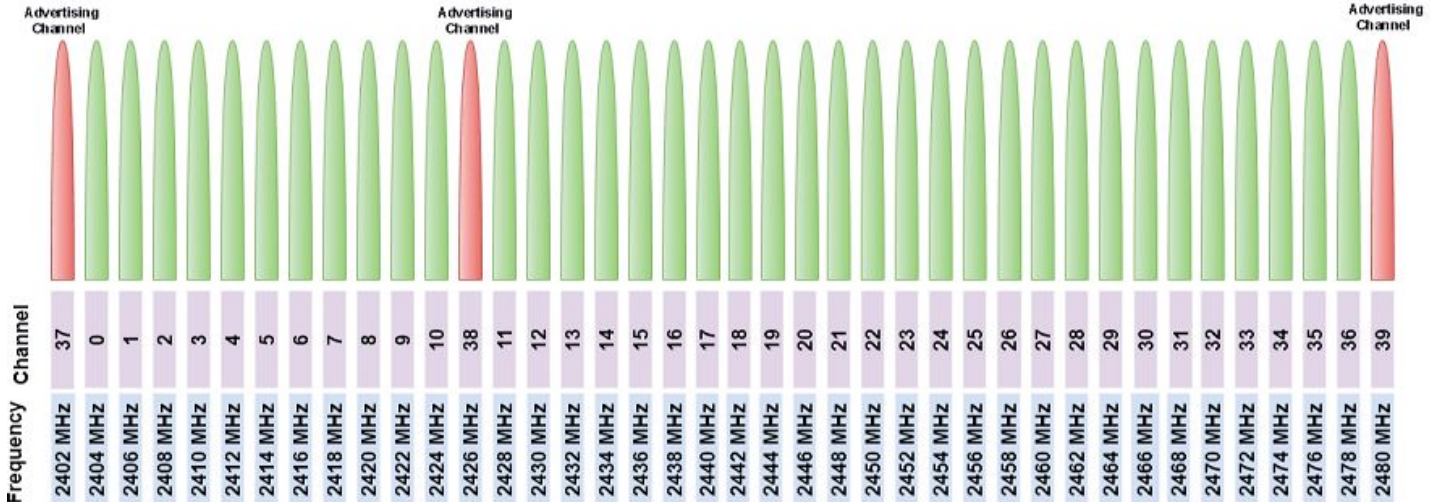
Name	Date modified	Type
.github	1/25/2024 3:05 PM	File folder
.vscode	1/30/2024 2:53 PM	File folder
dist	2/7/2024 8:29 PM	File folder
images	1/25/2024 3:08 PM	File folder
.clang-format	1/25/2024 3:05 PM	CLANG-FORMAT ...
.editorconfig	1/25/2024 3:05 PM	Editor Config Sour...
.gitignore	1/25/2024 3:05 PM	Text Document
application.fam	1/25/2024 3:08 PM	FAM File
bluetooth_test_app.c	2/7/2024 8:22 PM	C Source File
bluetooth_test_app.png	1/25/2024 3:05 PM	PNG File



```
C:\Users\cdgra\Documents\bluetooth_test_app>ufbt launch
scons: Entering directory `C:\Users\cdgra\.ufbt\current\scripts\ufbt'
python C:\Users\cdgra\.ufbt\current\scripts/runfap.py -p auto -s C:\Users\cdgra\.ufbt\build\blue
tooth_test_app.fap -t /ext/apps/Examples/bluetooth_test_app.fap
        APPCHK  C:\Users\cdgra\.ufbt\build\bluetooth_test_app.fap
                Target: 7, API: 50.0
2024-02-07 20:32:42,430 [INFO] Using FLIP_ACTIN on COM3
2024-02-07 20:32:42,485 [INFO] Installing "C:\Users\cdgra\.ufbt\build\bluetooth_test_app.fap" to
 /ext/apps/Examples/bluetooth_test_app.fap
2024-02-07 20:32:42,540 [INFO] Sending "C:\Users\cdgra\.ufbt\build\bluetooth_test_app.fap" to "/
ext/apps/Examples/bluetooth_test_app.fap"
<100%, chunk  1 of  1 @ 19.42 kb/s
2024-02-07 20:32:42,594 [INFO] Launching app: /ext/apps/Examples/bluetooth_test_app.fap
```

Bluetooth Low Energy

- Designed for low power and short range applications
- Operates in the 2.4GHz band with range of 100 meters
- Uses 40 channels compared to 80 with classic Bluetooth
- Channels 37, 38, 39 are used for advertising



BTLE Packet Analyzer

- Open source software developed by Jiao Xianjun
- BTLE monitor and transmitter
- Sniffs BTLE packets and provides corresponding data
- Uses HackRF SDR

```
0000127us Pkt001 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0a8eba851db0 Data:16ff0600010f300270ae9a7afd3f73e8894b11d76167e48cc486e456eb51a8 CRC1
0032191us Pkt002 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:5eff060001093022fc97c8fec10efa01e5a7562fe3629b679f30a6ce32a118 CRC1
0263710us Pkt003 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0a8bbe851cb0 Data:1eff0600010f200270ae9e7afd3d73e88b4b11d76167e58cc486e456eb51b8 CRC1
0129590us Pkt004 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL37 AdvA:0a8bba851cb4 Data:1eff0600010f200270ae9e7afd3d73e8894b11d7e167e58cc4866456eb51a8 CRC1
0001452us Pkt005 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060801092022fc97c8fec10efa01e5a7562fe3639b279f30a2ce3261d0 CRC1
0163411us Pkt006 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:20a7bc260639 Data:1eff060001092026b3c4ddce90cadc0f5ca33e638f3998f5b2f4556c4eb919 CRC1
0129692us Pkt007 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:20a7bc260639 Data:1eff060001092026b3c4ddce90cadc0f5ca33c8b86f8fe6aed15bca6e79e54 CRC1
0132115us Pkt008 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060001092022fc97c8fec10efa01e5a7562fe3629b279f30a2ce3261d0 CRC0
0196345us Pkt009 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0a8bba851cb4 Data:1eff0600810f200270ae9e7afd3d73e8994b11476167e5c8c6946452eb51a8 CRC1
0098678us Pkt010 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:28b2ba851cb0 Data:14f90600010f200270ae9e7afd3d73e8895b11d76167e58cc486e456eb51a8 CRC1
0033510us Pkt011 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060001092022fc97c8fec10efa01e5a7562fe3629b279f30a2ce3261d0 CRC0
0196462us Pkt012 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:0ccd55ffd0eb Data:1eff060001092022fc97c8fec10efa01e5a7562fe3629b279f30b2ce3261d0 CRC1
0261563us Pkt013 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL37 AdvA:20a6bc360639 Data:1eff068011090026b3c4ddce90cbdc0f5ea33eab82f8fe6aed95bca6e79e54 CRC1
0033528us Pkt014 Ch37 AA:8e89bed6 ADV_PDU_t2:ADV_NONCONN_IND T1 R0 PloadL23 AdvA:473685b8d6c4 Data:02011b0dff4c08160811aaec6dbb8c58bd CRC1
```

BTLE Packet Analyzer

0032191us Pkt1002 Ch37 AA:8e89bed6 ADV_PDU:t2:ADV_NONCONN_IND TxAdd:1 R0 Pload:37 AdvA:0a0ceba851db0 Data:1eff0600010f30027

1. 0032191us
2. Pkt1002
3. Ch37
4. AA:8e89bed6
5. ADV_PDU:t2:ADV_NONCONN_IND
6. TxAdd:1
7. R0
8. Pload:37
9. AdvA:0a0ceba851db0
10. Data:1eff0600010f30027

ESP 32 Test Bed

- Connection Verification
  - Server: Call and Response
  - Client: Message Prediction

- Data Collection
  - Statistical Analysis

Difficulties with Sprint 1

- Still understanding Flipper Zero & how to customize
- Very little official documentation on how to make apps for the Flipper Zero
- Still waiting on equipment that we already have plans for

Future Goals

- Monitor all 40 BTLE channels and record packet data
- Decode and track BTLE channel hopping
- Continue understanding what we can do with the Flipper Zero and further see how can we utilize these capabilities ourselves
- Produce final white paper