Bluetooth Packet Sniffing

1 Key Objectives

- Reinforce your concept about Bluetooth workflow.
- Get familiar with Bluetooth security and privacy .
- Learn how to use tools to sniff Bluetooth traffic.

2 Installing nRF Connect for Mobile

- Please open your Apple App Store (or Google Play for Android users) and search a mobile app named nRF Connect for Mobile (See Figure 1).
- Install the app to your iPhone or Android Phone. nRF Connect for Mobile is a tool that enables Bluetooth Low Energy traffic analysis.

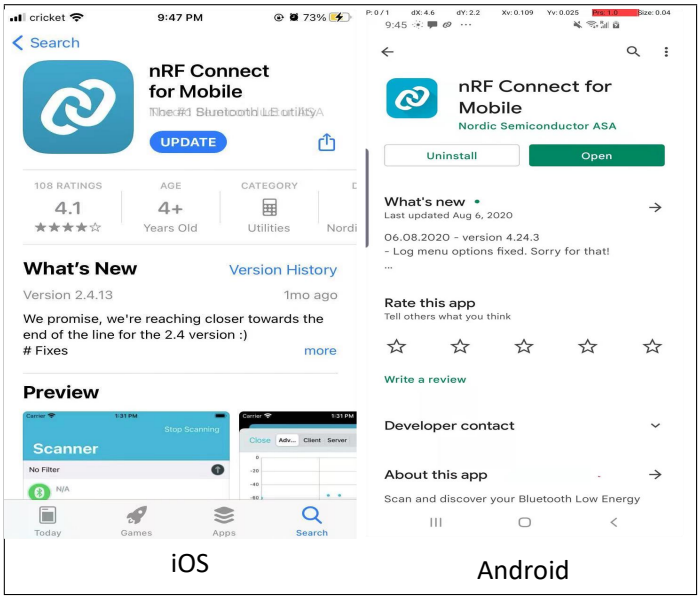

Figure 1: nRF Connect for Mobile

3 Using a mobile sniffer to observe the nearby BLE devices

- **Step-I.** Open nRF Connect for Mobile, which will list the nearby BLE devices.
- **Step-II.** Check the sniffed Bluetooth devices.

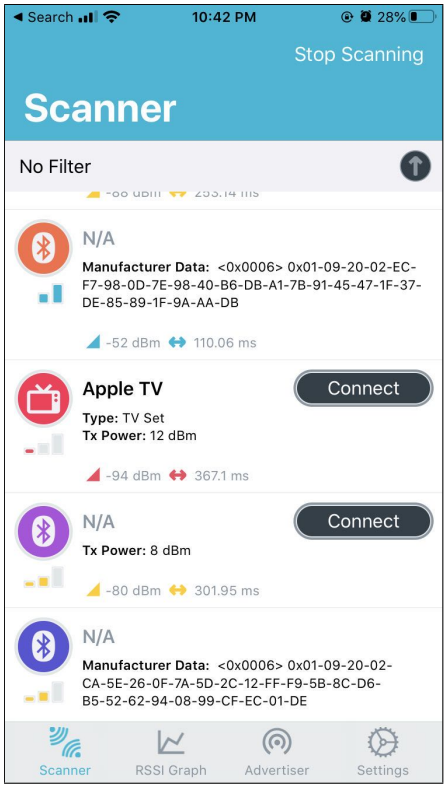

Figure 2: Nearby Bluetooth devices discovered by nRF Connect for Mobile (iOS)

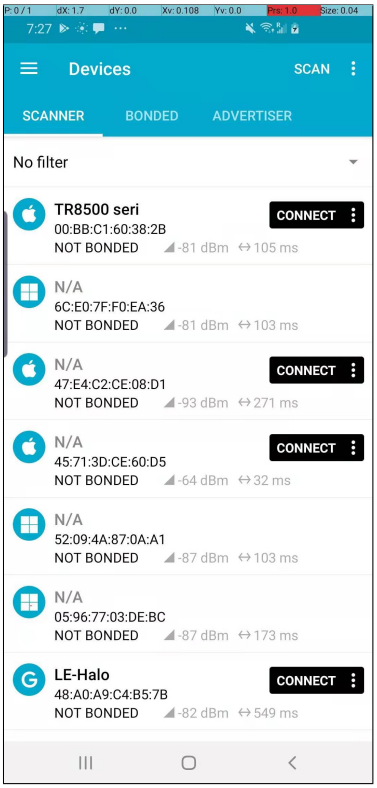

Figure 3: Nearby Bluetooth devices discovered by nRF Connect for Mobile (Android)

Warning: Do not attempt to BLE devices owned by others, since this be considered as a intrusion.

4 Results: what you have observed

- Check the icons of the collected devices, which will indicate what are the manufactures of devices, as shown in Figure 2 (iOS) and Figure 3 (Android).
- Check the manufacture data of nearby BLE devices. Please note that Android does not support to view the manufacture data of other BLE devices, as shown in Figure 3.
- Check the and MAC addresses of Bluetooth devices. Please note that iOS does not support to view the MAC addresses of other BLE devices, as shown in Figure 2.

UUID	Represented Services
0x181B	Body Composition
0x181C	User Data
0x181D	Weight Scale
0x181E	Bond Management
0x181F	Continuous Glucose Monitoring
0x1820	Internet Protocol Support
0x1821	Indoor Positioning
0x1822	Pulse Oximeter
0x1823	HTTP Proxy
0x1824	Transport Discovery
0x1825	Object Transfer
0x1826	Fitness Machine
0x1827	Mesh Provisioning
0x1844	Volume Control
0x184C	Generic Media Control Service
0x183A	Insulin Delivery
0x183B	Binary Sensor
0x183E	Physical Activity Monitor
0x1843	Audio Input Control
0x183C	Emergency Configuration
0x1845	Volume Offset Control
0x1846	Coordinated Set Identification Service
0x1847	Device Time
0x184B	Telephone Bearer Service

Table 1: A list of common UUIDs and their represented services (more details can be found in [2])

- Check the services provided by the devices, which will indicate the UUID of the devices. *"A UUID is a universally unique identifier that is guaranteed to be unique across all space and all time"*. Bluetooth SIG [1] reserved UUIDs to represent different services the devices provide. For example, UUID for contact tracing is *0xFD6F*. A list of UUIDs and their represented services can be found in Table 1.
- Check the names of the Bluetooth devices (e.g., some devices may be given a tractable name, Alice's phone)

References

[1] S. Bluetooth, "Bluetooth core specification version 5.2," *Specification of the Bluetooth System*, 2020.

[2] Bluetooth SIG, "16-bit uuid numbers document," https://btprodspecificationrefs.blob.core.windows.net/assigned-values/16-bit%20UUID%20Numbers%20Document.pdf, 2021.