Learning from BLE Advertisements

It’s not machine learning (yet), relax.

Yibo Wei

Background

What does a BLE device advertise (usually)?

What does a BLE device advertise (usually)?

- Device name

What does a BLE device advertise (usually)?

- Device name
- Manufacturer data (with a company ID)

What does a BLE device advertise (usually)?

- Device name
- Manufacturer data (with a company ID)
- Service/Characteristic UUIDs

What does a BLE device advertise (usually)?

- Device name
- Manufacturer data (with a company ID)
- Service/Characteristic UUIDs
- Tx power level (for distance estimation)

What does a BLE device advertise (usually)?

- Device name
- Manufacturer data (with a company ID)
- Service/Characteristic UUIDs
- Tx power level (for distance estimation)
- …

What does a BLE device advertise (usually)?

- Device name
- Manufacturer data (with a company ID)
- Service/Characteristic UUIDs
- Tx power level (for distance estimation)
- …
- Many other things that are defined but rarely used

When does a BLE device advertise?

When does a BLE device advertise?

- To be paired with a central device
  - Wireless earbuds
  - Smartwatches

When does a BLE device advertise?

- To be paired with a central device
  - Wireless earbuds
  - Smartwatches
- To broadcast data to nearby devices
  - Temperature sensors
  - Beacons
  - Apple’s FindMy network

When does a BLE device advertise?

- To be paired with a central device
  - Wireless earbuds
  - Smartwatches
- To broadcast data to nearby devices
  - Temperature sensors
  - Beacons
  - Apple’s FindMy network

Reality:

When does a BLE device advertise?

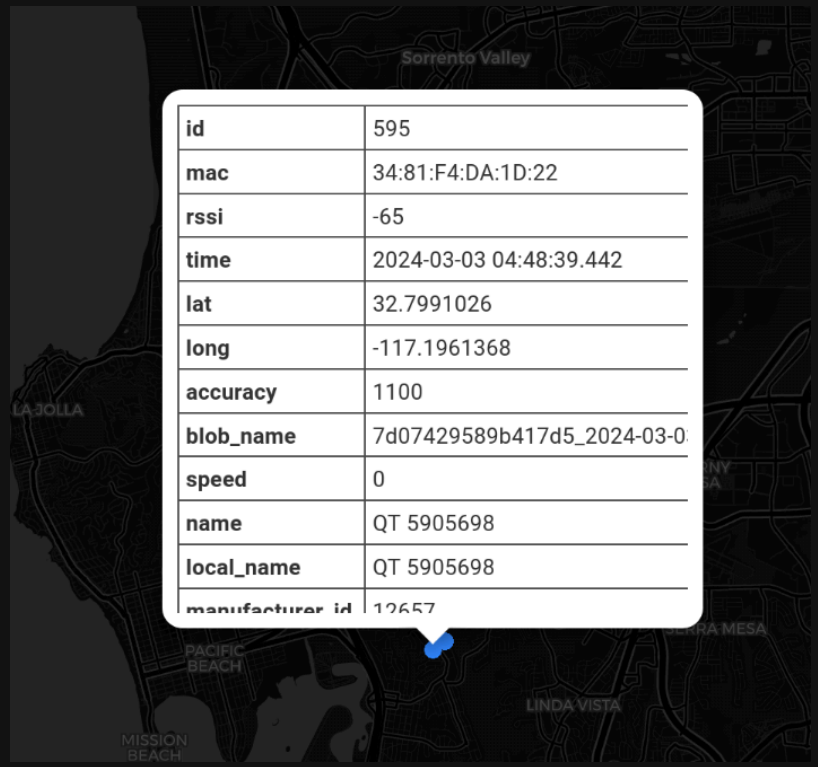
- To be paired with a central device
  - Wireless earbuds
  - Smartwatches
- To broadcast data to nearby devices
  - Temperature sensors
  - Beacons
  - Apple’s FindMy network

Reality:

When it shouldn’t

Example: CARR Alarm System

Don’t install this when your dealer tries to sell you one!



id	595
mac	34:81:F4:DA:1D:22
rssi	-65
time	2024-03-03 04:48:39.442
lat	32.7991026
long	-117.1961368
accuracy	1100
blob_name	7d07429589b417d5_2024-03-0
speed	0
name	QT 5905698
local_name	QT 5905698
manufacturer_id	12657

Example: MyQ Garage Door Opener

This device only needs to be paired once, but we found a lot of advertisements.

Example: Govee LED Strip

This is the worst one so far.

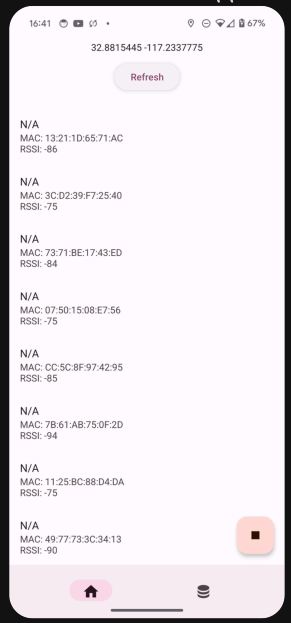
We want to find more bad devices like these.

We want to find more bad devices like these.

Our work

Data sources

Cluetooth App

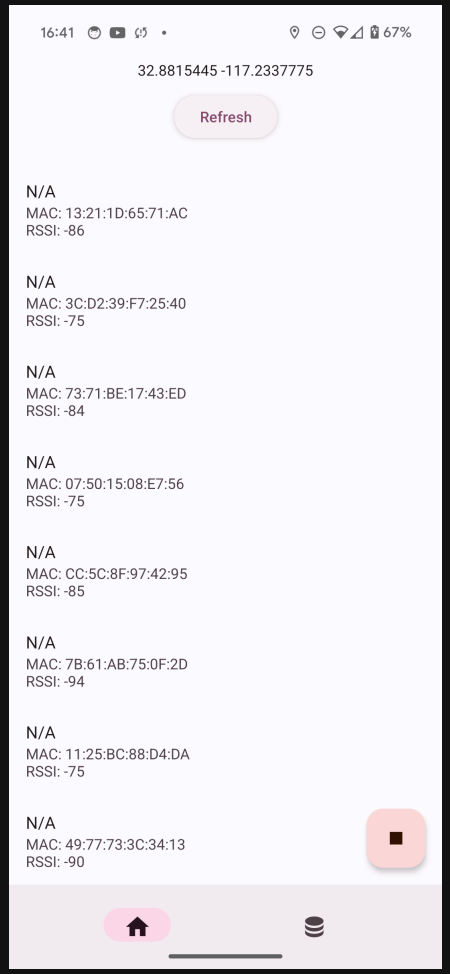


PostgreSQL

Apkpure

JADX

Bluetooth SIG Assigned Numbers



Cluetooth App

BLE scanner that uploads data to our server

Sample Data:

```
{
  "mac": "00:11:22:33:44:55",
  "rssi": -50,
  "time": "2024-03-03T12:34:56Z",
  "name": "My Device",
  "manufacturer_id": 12657,
  "lat": 37.7749,
  "lon": -122.4194,
  "accuracy": 10,
  "uuids": ["0000180D-0000-1000-8000-00805F9B34FB"],
  ...
}
```

Extracting UUIDs from APKs

Fully automated APK uuid extraction workflow:

Keyword based search


```
[
  {
    "name": "Govee Home"
    "app_id": "com.govee.home",
    "description": "Govee Home is an app to help you manage your smart devices."
  },
   ...
]
```



```
[
  {
    "uuid": "00010203-0405-0607-0809-0a0b0c0d2b11",
    "variable": "f22453y",
    "path": "com/govee/barelightv1/ble/BleComm.java"
  },
   ...
]
```

Assigned Numbers

16-bit UUIDs are assigned by the Bluetooth SIG

```yaml
- uuid: 0x1809
  name: Health Thermometer
  id: org.bluetooth.service.health_thermometer
- uuid: 0x180A
  name: Device Information
  id: org.bluetooth.service.device_information
- uuid: 0x180D
  name: Heart Rate
  id: org.bluetooth.service.heart_rate
- uuid: 0x180E
  name: Phone Alert Status
  id: org.bluetooth.service.phone_alert_status
- uuid: 0x180F
  name: Battery
  id: org.bluetooth.service.battery_service
```

More details:

https://bitbucket.org/bluetooth-SIG/public/src/main/assigned_numbers/uuids/

Assigned Numbers

16-bit UUIDs are assigned by the Bluetooth SIG

```yaml
- uuid: 0x1809
  name: Health Thermometer
  id: org.bluetooth.service.health_thermometer
- uuid: 0x180A
  name: Device Information
  id: org.bluetooth.service.device_information
- uuid: 0x180D
  name: Heart Rate
  id: org.bluetooth.service.heart_rate
- uuid: 0x180E
  name: Phone Alert Status
  id: org.bluetooth.service.phone_alert_status
- uuid: 0x180F
  name: Battery
  id: org.bluetooth.service.battery_service
```

More details:

https://bitbucket.org/bluetooth-SIG/public/src/main/assigned_numbers/uuids/

Assigned Numbers

16-bit UUIDs are assigned by the Bluetooth SIG

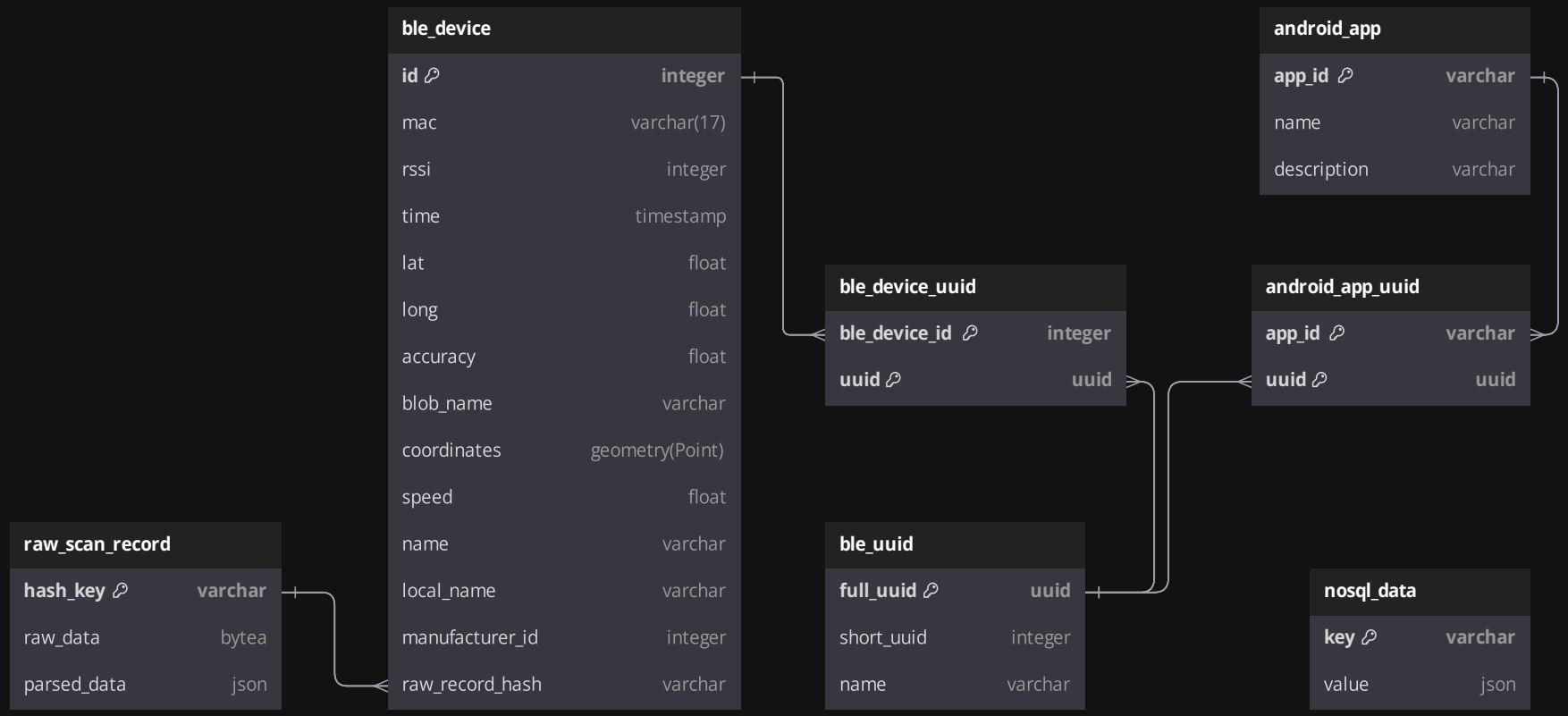
```yaml
# Assigned 16-bit UUIDs converted to 128-bit UUIDs
- uuid: 00001809-0000-1000-8000-00805F9B34FB
  name: Health Thermometer
  id: org.bluetooth.service.health_thermometer
- uuid: 0000180A-0000-1000-8000-00805F9B34FB
  name: Device Information
  id: org.bluetooth.service.device_information
- uuid: 0000180D-0000-1000-8000-00805F9B34FB
  name: Heart Rate
  id: org.bluetooth.service.heart_rate
- uuid: 0000180E-0000-1000-8000-00805F9B34FB
  name: Phone Alert Status
  id: org.bluetooth.service.phone_alert_status
- uuid: 0000180F-0000-1000-8000-00805F9B34FB
  name: Battery
  id: org.bluetooth.service.battery_service
```

More details:

https://bitbucket.org/bluetooth-SIG/public/src/main/assigned_numbers/uuids/

Database

We use UUIDs to associate scanned devices with Android apps.



Future work

Future work

- Scan a lot more

Future work

- Scan a lot more
- Data analysis

Future work

- Scan a lot more
- Data analysis
- Machine learning?

Questions?

About this presentation

I hate PowerPoint and Google Slides.

- Slides are made with Slidev
- Diagrams are made with Excalidraw
- The database schema diagram is made with dbdiagram.io (Non-free)

Thank you!