Low Energy Bluetooth

Fingerprinting & Patterns of Life Analysis

Faculty Sponsor: Dominick Foti

Frederick Berberich III

MARIST

Introduction

Bluetooth low energy (BLE) are short-range wireless technologies that use public non encrypted advertising channels to announce their presence to other devices. BLE uses a MAC randomization protocol to protect devices from hackers.

Image of nRF52840 Dongle

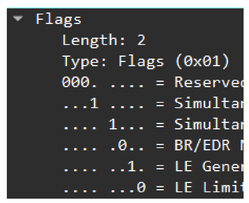
Methods

During the time of my research, the testbed included different generations of air pods, iPhone, and a JBL Flip 5 speaker to study the BLE packets. With the air pods still in the case, I would flip open the case so the device would start broadcasting. I would make sure my JBL speaker was on and connected to my iPhone, lastly, I would make sure my iPhone screen was on. I repeated these steps in a private area where the same stationary devices were in the area, so BLE packets from devices in a different area wouldn't be picked up from the BLE dongle and cause some of the data to be different. After making sure all the devices were broadcasting, I would then set up each device to a specific RSSI number, so I can keep track of each device as the MAC address would change every 15 minutes. For the dongle, we decided to use Nordic Semiconductor's BLE dongle. It's called a nRF5280 dongle. Nordic created a Wireshark add-on that makes it relatively easy to use and receives an additional attribute from BLE packets called RSSI.

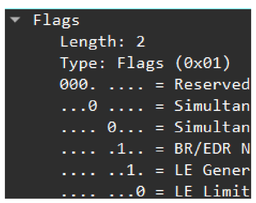
Data Analysis

Various attributes found in BLE packets were proven to be quite useful when trying to track BLE devices through their MAC randomization protocol

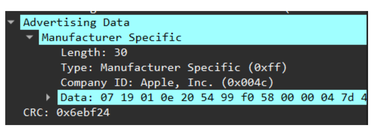
- **Device name:** The name if device was named by a user
- **Company ID:** A standard company code that each company that creates BLE devices associates with
- **Length:** length of BLE section of packet
- **Power Level:** What power level (measured in dBm) packet was detected as
- **RSSi:** How far the packet was sent from the BLE dongle
- **Flags:** Functions that are enabled for each specific BLE device



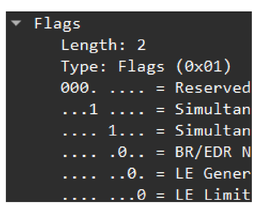
iPhone, Android, & Apple Watch flags



Laptop Flags



Air pods length



JBL Speaker Flags

Results

While some companies such as JBL have the device name public within the BLE broadcasting packet, companies such as Apple like to keep all their device's information private and encrypted. This means we must find more ways to identify a device other than its device name. The first way is to see if a device has the *flags* attribute within its *Advertising data* section. If a device does not have any flags, there is a chance that it may be Bluetooth headphones. If it does, then it is a mobile device. Within the flags attribute itself, has 5 categories total but the main 3 to pay attention to are the *Host*, *Controller*, and *BR/EDR Not Supported* sections. They are labeled as enabled or disabled with a 1 or a 0. The flag attributes coming from a smartphone or smartwatch will have the values 1,1,0, laptops would be 0,0,1.

Source	Destination	Protocol	Length	Company ID	Device Name	Length	Power Level (dBm)	RSSI
5a:71:7f:67:0b:63	Broadcast	LE LL	51	Apple, Inc.		2,2,12	8	-43 dBm

BLE packet from an iPhone

Source	Destination	Protocol	Length	Company ID	Device Name	Length	Power Level (dBm)	RSSI
54:6d:69:f5:ad:9a	Broadcast	LE LL	49	Apple, Inc.		2,2,10	9	-85 dBm

BLE packet from an Apple Watch

Source	Destination	Protocol	Length	Company ID	Device Name	Length	Power Level (dBm)	RSSI
76:b5:7d:66:61:45	Broadcast	LE LL	63	Apple, Inc.		30		-33 dBm

BLE packet from Air pods

Another identifier is a BLE packet's power level. A BLE packet's power level is the strength a packet was sent out. It's measured in dBms and smartphones such as iPhone typically have a power level of 8 while smartwatches such as Apple watches have a power level of 9. You can identify a device based off of their packet length found in the *Manufacturer Specific* section. BLE headphones such as air pods almost always have a length of 30 while smartphones will have a length of 12 and smartwatches will have a length of 10. While manufacturer length is great for identifying headphones, it is not as trustworthy as smartphones and smartwatches because the length can change depending on what each device is transmitting.

Source	Destination	Protocol	Length	Company ID	Device Name	Length	Power Level (dBm)	RSSI
JingxunSoftw_09:5e:…	Broadcast	LE LL	61	Harman Inter…	JBL Flip 5	2,9,3,11		-28 dBm

BLE packet from a JBL Flip 5 Speaker

Source	Destination	Protocol	Length	Company ID	Device Name	Length	Power Level (dBm)	RSSI
SiliconLabor_87:aa:…	Broadcast	LE LL	53			2,17		-84 dBm

BLE packet from a MacBook

Conclusion

Having additional understanding in Bluetooth Low Energy can be applied to make devices we use on a day-to-day basis communicate more securely, enhance our capability to monitor their communications, and identify those that are behaving outside of the norm. Overall being able to monitor Bluetooth Low Energy packets is a benefit to everyone.

MARIST
SCHOOL OF SCIENCE

MARIST | SCHOOL OF SCIENCE

MARIST

MARIST