CS397/497, Spring 2024
Homework: BLE Packets

This is an **individual** assignment. Submission is through Gradescope. You can submit a scanned version of this document, a computer edited version, or simply paper with the answers. Please be careful to ensure that answers are labeled and legible.

The goal of this homework is to practice interacting with BLE advertisement payloads. Useful aspects of this are decoding TLV data, interpreting fields, and investigating meaningful BLE values (Assigned Numbers).

I don't want busy work, so we're going to keep this assignment short. Long enough to force you to engage a little, but hopefully doesn't take more than an afternoon. If you run into issues on this homework, please reach out to the professor!

BLE Advertisement Background & Resources

- Advertisement TLV format
  - For BLE advertisements, the format of data is Length-Type-Value
    - Where Length is the number of bytes for the Type + Value (doesn't count itself)
  - These "Advertisement Data" TLVs are concatenated together to create a full advertisement payload.
  - Type numbers are defined in the Generic Access Profile document
  - Value fields have their own layout, defined in the Core Specification Supplement
    - 16-bit Service UUIDs are defined in the 16-bit UUID Numbers document
- Advertisement decoding example: https://community.silabs.com/s/article/kba-bt-0201-bluetooth-advertising-data-basics?language=en_US
- To determine what a device is, you will likely have to do a little googling. Usually, a name of a device, or the service UUID and the word "BLE", can get you pretty far.
- Eddystone URL beacon encoding
  - Eddystone payloads use the service UUID 0xFEAA. The service data attached is then further specified by protocol documentation:
  - https://github.com/google/eddystone/blob/master/protocol-specification.md
  - https://github.com/google/eddystone/tree/master/eddystone-url

Q1: Simple BLE Advertisements [20pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	04	09	48	69	21	02	0A	00
8	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement?

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc.

Q2: Real-world BLE Advertisement 1 [25pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	03	03	03	FE	0E	09	4C	45
8	5F	57	48	2D	31	30	30	30
16	58	4D	34	--	--	--	--	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement?

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc.

3. What is this device and why does it have that service?

Q3: Real-world BLE Advertisement 2 [25pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	02	01	01	03	03	EC	FE	0B
8	09	56	65	6E	75	65	2D	54
16	69	6C	65	--	--	--	--	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement?

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc.

3. What is this device and why does it have that service?

Q4: Eddystone Advertisement [30pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	02	01	06	03	03	AA	FE	0F
8	16	AA	FE	10	BA	03	78	6B
16	63	64	00	32	30	35	35	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement?

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc.

3. What is the Eddystone URL here?