# Mitigating Risks in Internet of Things: A Short Analysis of Bluetooth Low Energy devices

Vu, Lan Anh
*Department of Computer Science*
*H-BRS University of Applied Science*
Sankt Augustin, Germany
lan.vu@smail.inf.h-brs.de

***Abstract*—In this scientific paper I want to give a short introduction in BLE and its weaknesses, which make it possible for outsiders to attack the system connected through BLE.**

***Index Terms*—BLE, sniffing, spoofing, smart home technology, security, Internet of Things**

## I. Introduction

In this day and age home automatisation turns into a more an more present aspect in everyday commodities, whether it's simple devices such as lamps or more complex devices such as refrigerators. The most commonly used wireless personal area network technology for this occasion is Bluetooth Low Energy (short: BLE) [1]. BLE was first introduced in 2010 in Version 4.0 of the Bluetooth specification to address the needs of applications in the Internet of Things (short: IoT) [2]. It focuses on low power consumption, which gives BLE its name, so battery powered devices could exhibit a longer battery life span than using Bluetooth (also known as Classic Bluetooth or Bluetooth Basic Rate/Enhanced Data Rate, short: BR/EDR). BLE operates in the industrial scientific and medical band (short: ISM band) — an unlicensed band used for short-range applications in the 2.4 GHz spectrum — which is the same spectrum occupied by Wi-Fi, Classic Bluetooth and other technologies [3].

## II. BLE Properties

### A. Range of BLE Communications

The maximum achievable range BLE allows varies depending on the configuration being used, which allows the user to configure BLE devices to their needs and the needs of specific applications in question. It can range from a few meters to over one kilometre line of sight. The specific mode utilises a method for data recovery called *forward error correction* (short: FEC), which increases the range without the need to increase the transmit power. [5]

### B. Power Consumption

To achieve a reduced power consumption BLE devices only activate the radio when needed, meaning it is only being used to send and receive data and turned off until the next data transfer happens. The peak power consumption of the radio heavily depends on the chipset being used but through this method a battery life span of months or even years in some cases can be achieved. [2]

### C. Data Throughput

A few configurations of a BLE device affect the maximum data throughput achievable. The highest data rate for the radio is the 2 Mbits mode in which the application data is slightly lower due to overhead and some other aspects but it can be expected to achieve up to 1.4 Mbits/sec applications data rate. The range and data throughput are mutually exclusive, meaning if a higher range needs to be achieved, it is affecting and reducing the data throughput that can be achieved and vice versa. [4]

### D. Adaptive Frequency Hopping

This property allows BLE devices to dynamically avoid collision and interferences with other devices and signals in the 2.4 GHz spectrum in real time by continously monitoring their environment for interference and changing the channel map to address interferences [2].

## III. Concepts in BLE

### A. Peripherals & Centrals

A *peripheral* is called the device that sends out advertisement data for other devices to discover it, whether it is to connect or to just read the data. A *central* is the device that discovers these advertisement packets and could connect to that device if the packet allows it. It is also in charge of controlling the timing and the parameters of a BLE connection and therefore consumes more power than a peripheral [2]. A BLE device, regardless of its role, can connect to multiple other devices, which means a central could connect to multiple peripherals and vice versa.

### B. Advertising & Scanning

*Advertising mode* is when a peripheral sends out data — called advertising packets — for other devices to discover it, which can lead to a connection or simply being used for discovery and reading some of the advertisement data. The central will be continuously scanning for advertising packets from other devices. [2] We will further explain this process later on.

### C. Connections

BLE allows connection oriented and connectionless communication. For a connection to occur several steps are needed:

- The peripheral needs to send out connectable advertisement packets.
- The central needs to be scanning for advertisement packets. [2]

We will further explain this process later on.

### D. Services & Characteristics

A *characteristic* represents a piece of information or data that a BLE device wants to expose to another device whereas a *service* is a grouping of one or more characteristics, usually logically grouped meaning related characteristics are grouped within one service. Both services and characteristics are called *attributes* which define how a BLE device organises and structures the data that it exposes to other devices to discover it. Each attribute consists of a value and three properties — an *attribute type* which is given by a universally unique identifier (short: UUID), an *attribute handle* which is a 16-bit number allowing a client to specify attributes in requests and *access permissions* which describe the possible accessibility of an associated value — associated with it [2].

## IV. Structure of BLE Protocol Stack

In this section we will explain the BLE protocol stack responsible for its connection ability.
A *protocol* is an universally agreed way to communicate between two devices and a protocol stack is a set of protocols that work together to transmit information from one device to another. The BLE protocol stack can be divided into two major groups: *controller* — which consists of lower layers handling time-critical tasks — and *host* — which contains layers performing high-level complex tasks. They communicate through the host controller interface (short: HCI) making it possible for the host to control lower layers through a command set and for the controller to send data to upper layers [2].

### A. Physical layer

The *physical layer* (short: PHY) contains the analog communication circuitry and is concerned with the actual transfer of data over air via radio. In BLE the operating band is divided into 40 radio frequency (short: RF) channels with 2 MHz spacing where three are designated as primary advertising channels used for advertising and connection establishment — which are equally distributed over the ISM band to avoid interference caused disruption of advertising — and the remaining channels are used as general purpose channels for the majority of communication. Additionally, the physical channel is changed every few packets during an established connection [2].

### B. Link layer

The *link layer* (short: LL) handles low-level tasks and all time-critical tasks to achieve a responsive RF communication which includes calculation and verification of cyclic redundancy check (short: CRC) values and message integrity code (short: MIC) as well as security related functions. Additionally it maintains the Bluetooth device address (short: BD_ADDR), a unique identifier which allows distinguish different communication partners. There are seven possible states a BLE device can achieve:

1) When a device does not send or receive data it is in *standby state* which is the default state.
2) When switching into *advertising state* a device becomes an advertiser which is usually performed by peripheral devices. It will send advertising packets on the three primary advertising channels and looking for connection requests in fixed intervals.
3) When switching into *scanning state* a device becomes a scanner scanning the three primary advertising channels for connection requests which is usually performed by central devices.
4) A scanner switches into *initiating state* upon reception of an undirected or directed advertisement packet and responds to the received advertising packet of an advertiser with a connection request.
5) When the scanner switches into *connection state*, the advertiser follows as soon as it receives the scanner's connection request. If the scanner sends any protocol data units (short PDUs) the connection is acknowledged and therefore the connection is considered established. The initiator device adopts the *central* role and the advertiser device the *peripheral* role.
6) Alternatively a *broadcaster* could send only non-connectable and non-scannable advertisement packets — making it impossible to establish a connection.
7) Additionally, there is also the *synchronisation state*, during which the observing device listens for periodic advertising packets and isochronous data packets [2].

### C. Host controller interface

A set of *host controller interface* (short: HCI) commands and events defines the communication between the two major groups. Implementations of the HCI vary based on the use case. [2]

### D. Logical link control & adaptation layer protocol

The *logical link control & adaptation layer protocol* (short: L2CAP) layer's main function is protocol multiplexing which is necessary since there is more than one upper layer protocol defined by BLE. By tagging packets with a protocol-specific channel identifier (short: CID) packets are correctly routed to upper layer protocols. [2]

### E. Security manager protocol

As the name indicates the *security manager* (short: SM) layer handles all parts regarding security which can be divided into a cryptographic toolbox — which contains all cryptographic functions for hash calculations and key generation — and methods for both pairing and key exchange. [2]

### F. Attribute protocol

The *attribute protocol* (short: ATT) is a client-server protocol, which allows a server to expose attributes and their associated values to the client. The generic attribute profile (short: GATT) on top of ATT defines a data abstraction model for attributes. [2]

### G. Generic access profile

The *generic access profile* (short: GAP) describes profile roles and defines modes and procedures for discoverability, connection and security of BLE devices. It guarantees interoperability between devices of different manufactures by utilising features provided by the other layers, defining which functionalities of other layers are mandatory or optional. [2]

## V. POSSIBLE ATTACK ON BLE DEVICES

In this section we will expatiate on BLE devices' security weaknesses on the basis of a Playbulb Candle by MiPOW — a smart home LED lamp possible of changing colors — and a eQ-3 temperature regulator to control the temperature of a heating element. Both devices are controlled by an application provided by the producer. We will introduce a way to gain control over these two devices by sniffing the connection, identifying the commands responsible for controlling them and gaining control externally.

### A. Playbulb Candle by MiPOW

To receive BLE packages we used a *nRF52840 Dongle* and to record and analyse those packages we used the open source tool *Wireshark*. Whenever the colour of the candle was changed, the application sent a data package with the responsible command. While analysing the packages we discovered they could be identified by filtering using the ATT protocol. They include the attribute's UUID as well as a value representing the colour being displayed. The application sent eight hexadecimal numbers as values for its commands where the first two digits remain 00 and the last six digits in pairs represent red, green and blue — making it possible to display numbers from zero to 255. To create own commands we used the open source tool *bettercap* which displayed both the MAC address as well as the name of the device when searching and scanning for BLE devices meaning these values are being sent in its advertising packets. With both the discovered MAC address and UUID it was possible for bettercap to recreate a command to change the colour of the Playbulb Candle without using the provided application meaning it is irrelevant for the device whether the commands are sent by the application.

### B. eQ-3 temperature regulator

Since this device contains a display, it fulfils the requirements to apply the passkey entry method — a method where a four to six digit number is displayed to insert on the controlling device to maintain a secure connection. To use the application provided by the producer the four digit number displayed needs to be inserted into the application to establish a connection. After the established connection we proceeded similar to how we did with the Playbulb Candle. First we recorded the command data transfer while setting the temperature at 0 °C which is the lowest possible temperature. Next we analysed the data packages via Wireshark where we discovered that the temperature is provided by hexadecimal numbers. Thanks to the package sent when we set the temperature at 0 °C is was possible to determine the starting hexadecimal value 4100. The sent packages also consist of the Universal Unique Indentifier (short: UUID) needed to change the temperature. We were able to determine the MAC address via bettercap making is possible to recreate a command using the discovered MAC address and UUID. Additionally, we sent several command packets while constantly increasing the the hexadecimal value responsible for the temperature where we discovered that every increase would cause a temperature rise of 0.5 °C. The highest possible displayed temperature achieved by this method was 127.5 °C even though the maximum achievable temperature provided by the producer's application was 29 °C.

## VI. CONCLUSION

After testing both devices, we discovered that neither of the two devices could provide the security standard offered by BLE and are both easily breached by a few preceding steps mentioned in the previous section. This shows that producers do not set security as high value when producing smart home technologies like the two devices mentioned before. However, due to the ignorance of the average consumer it is very unlikely that manufacturers will put more effort and value into securing the connections established between their products and the applications provided to control those due to additional cost which prevent them to offer those products to an affordable price appealing for the wider masses. If or when this aspect will change is unclear even though it would make those products more attractive for professionals to use.

## REFERENCES

[1] K. FRÖHLICH, M. RADEMACHER, K. JONAS *Sicherheitsanalyse von Bluetooth Low Energy Geräten in der Heimautomatisierung* Mobilkommunikation - Technologien und Anwendungen. Vorträge der 24. ITG-Fachtagung, 15.-16. Mai 2019 in Osnabrück. ITG-Fachbericht, vol. 288, 2019, VDE Verlag, p. 99-104.

[2] M. CÄSAR, T. PAWELKE, J. STEFFAN, G. TERHORST *A survey on Bluetooth Low Energy security and privacy* Computer Networks vol.205, 14th March 2022, art. 108712, p. 1-18.

[3] S. M. DARROUDI, C. GOMEZ *Bluetooth Low Energy Mesh Networks: A survey* Sensors vol. 17, 2017, Switzerland: MDPI AG, p. 1467-1485.

[4] M. R. GHORI, T.-C. WAN, G. C. SODHY *Bluetooth Low Energy Mesh Networks: Survey of Communication and Security Protocols* Sensors vol. 20, 2020, Switzerland: MDPI AG, p. 3590-3625.

[5] M. WOOLLEY *The Bluetooth Low Energy Primer* 6th June 2022, Bluetooth SIG, Inc., p. 1-80.