Bluetooth Low Energy security analysis framework

Jennifer Ann Janesko

Technical Report

RHUL–ISG–2018–5

5 April 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

1 Project Introduction

1.1 Bluetooth Low Energy

Bluetooth low energy (BLE) is a wireless communication technology that allows the short range, wireless exchange of communication between devices. It is a special type of Bluetooth that was developed by the Bluetooth SIG with the specific goal to operate as efficiently as possible so that devices conserve battery power. It was introduced in version 4.0 of the Bluetooth specification. At the start of this project, the Bluetooth specification is at version 4.2. At the time of writing, the Bluetooth SIG started promoting version 5.0, although it had not officially been released.

Traditionally, Bluetooth has been used as a technology to organize devices wirelessly into networks called “piconets”. These piconets are often described as “ad hoc” because they can be built up and torn down quickly. “Ad hoc” has the connotation that the use of Bluetooth are impermanent and possibly only relevant for non-serious applications such as exchanging pictures between to mobile phones. But, the Bluetooth SIG has been marketing its Bluetooth low energy technology as a solution for Internet of things communications [B516].

Internet of things, or “IoT”, is a term that is used in the press, but is not clearly defined. Zielgedorf, et. al., outline a reference model by which IoT components can be categorized. IoT is described as “anyone and anything [that] is interconnected anywhere at any time via any network participating in any service.” While this definition seems overly broad, the authors refine it by describing five[1] types of entities that participate in an IoT application and their related information flows.

[1] Ziegeldorf, et.al., actually introduce four entities where “subjects” and “recipients” are combined into one entity under the category of “humans”. This is appropriate for their paper because their research focuses on the privacy challenges embedded in the use of IoT devices by human individuals in everyday life. This paper will use IoT in a broader sense to include subjects and recipients that are non-human which is fitting to smart home technologies and manufacturing automation technologies.

- Smart things: These are everyday devices that have been augmented with ICT components to collect data and share this data via services.
- Subjects: These are the entities from or about which smart things collect data for reporting.
- Services hosted on backends: These are services that collect data from the smart things and process that data for use in decision making.
- Recipients: These are the entities that receive feedback and information from the services on the backend.
- Infrastructure: These are the networks that allow communication between smart devices and their backend services. [JHZ13]

Take as a simple example, the logical representation of a smart climate management system in figure 1.

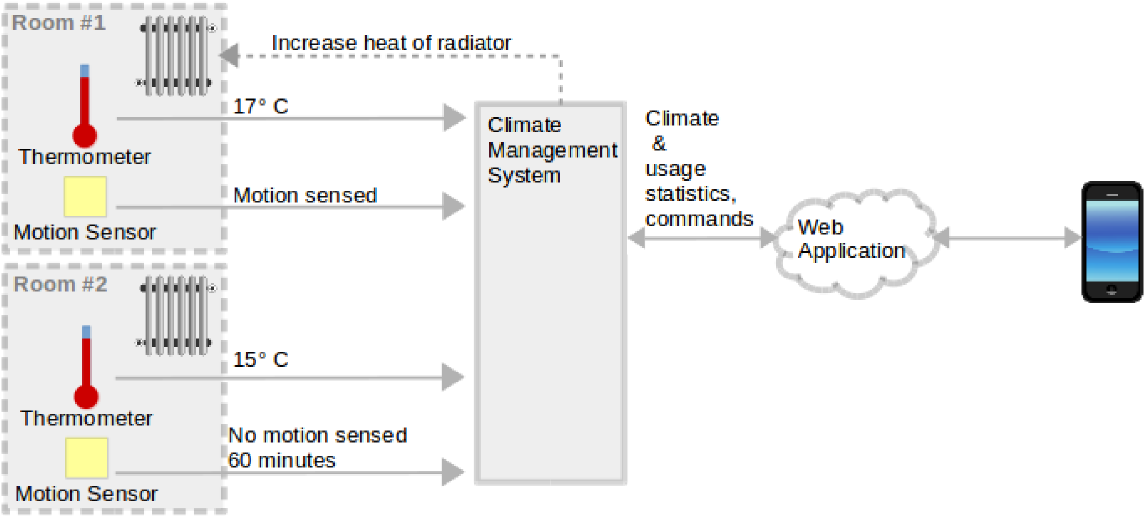
Room #1
Increase heat of radiator
17° C
Thermometer
Motion sensed
Motion Sensor
Climate Management System
Climate & usage statistics, commands
Web Application
Room #2
15° C
Thermometer
No motion sensed 60 minutes
Motion Sensor

Figure 1: Climate Management Example

This could be considered an IoT example. In the example there are smart things, the thermometers and motion sensors, that collect data from their subjects. In this case, the thermometers' subject is the room temperature. The motion sensors' subject is the (human) movement in the room. These smart devices communicate their data to the client, i.e., the backend client management system. This system reports statistics to an on-line web application which is viewable by the owner of the building. Based on input from the sensors and the climate and usage statistics over time, the climate management system determines whether to modify the climate controls in each individual room. This type of system has the advantages of being environmentally friendly as well as cutting heating costs.

In the example above, the infrastructure is the network that is set up between the sensors and the server and the server and the external web application. These infrastructures most likely rely on different protocols for communication. The infrastructure that provides a connection to the Internet is often TCP/IP-based. For manufacturing automation, the long-distance communication protocol may be specific to the application. The communication between the smart things and the server usually take place over a wireless protocol.

Wireless protocols provide a few advantages over cabled protocols. Setting up a wireless communications network is usually less costly and requires less effort for physical installation. In addition to this, wireless devices can be installed in areas where it might be a challenge to install cabling. In the IoT market, there are a small number of wireless protocols that are often mentioned: Zigbee, BLE and Thread [VT14]. Zigbee is a proprietary protocol that has been on the market since 2004. Thread is a newcomer (2014) and is backed by IT-giants like Google and NXP. BLE came to the market in 2013, was delivered on 165 million devices by 2014 and is expected to reach 1.2 billion devices by 2018. [RQ15]

Initially, BLE was known for being the communication protocol for smart devices like Apple’s iBeacon or for fitness trackers such as a Fitbit. But, BLE’s low power consumption has also made it ideal for health monitoring devices and home automation. The fact that BLE is an open standard coupled with its prevalence on users’ mobile devices has helped its proliferation [PMGL16][GL16]. In 2016, there was a big move in the controller industry to incorporate BLE for use in applications where reliability is required. Silicon Labs, NXP and Cypress have incorporated BLE into their PSoC offerings

[SLG16][JY16][PM16][GL16]. Open RTOS implemented a BLE stack [RM16]. Telit, an important competitor in the automation market, acquired a BLE stack in January 2016 [TAW16]. They provide equipment in the fields of condition monitoring, industrial automation, predictive maintenance, asset tracking, supply chain management and telematics and fleet management.

BLE is positioned to be a core IoT infrastructure component. And, whether is it used for tracking personal fitness, manging a home or managing factory automation, the question of BLE's security must be considered when developing a device. At the time of this project's writing, there has been little released to provide guidance with respect to IoT. OWASP has an emerging security testing guide for IoT, but at the time of writing, it focuses on the communication between an IoT device and an Internet service. The NIST has provided a set of security guidelines for the use of Bluetooth. These guidelines do include BLE, but the guidelines refer to BLE 4.0 [MSKS13]. In addition to this, there has been piecemeal research into the security aspects of BLE (see Chapters 4), but no structured approach to testing the security of a BLE device has been developed.

1.2 Project scope

The goal of this project to to provide a security analyst with the necessary information to perform a comprehensive security analysis of a device that uses Bluetooth Low Energy (BLE) for communication. To accomplish this task the paper is broken down into the following major sections:

- Introduction to the Bluetooth low energy concepts
- Enumeration of the generic Bluetooth low energy attack surface
- Development of a generic Bluetooth low energy threat model
- Outlining of an approach to BLE security testing

Although the Bluetooth Low Energy communication can be regarded as relatively simple, there is a considerable amount of detail in the specification that is relevant for a security review. To preserve the readability of this paper, the core body of the text in chapter 2 will be dedicated to elucidating core BLE concepts to the reader that were deemed relevant for security. The appendix of this document will contain a series of tables and listings that will provide necessary detail if a reader plans to use this document as a framework for an actual testing scenario.

1.3 Project Limitations

There are three modes of Bluetooth: BLE, EDR/BR and EDR/BR/BLE.

- BLE, as mentioned above, is Bluetooth Low Energy. BLE was introduced in the 4.0 Bluetooth specification. BLE is also marketed as “Bluetooth Smart”.
- EDR/BR is the version of Bluetooth that has been available since the first release of the Bluetooth specification. EDR/BR is often simply referred to as “Bluetooth” or “classic Bluetooth”. EDR/BR has enough differences from BLE on the host and controller that its communication is not compatible with BLE.
- EDR/BR/BLE devices have both the EDR/BR and BLE stacks built into them. These are also referred to as “dual mode” devices.

This project will only focus on providing a framework for BLE mode testing. EDR/BR and EDR/BR/BLE modes are not in scope for this project. That being said, there is a great deal of overlap in the specification between BLE and EDR/BR modes, and there has been significant research into the security of EDR/BR. Where applicable, results from EDR/BR research will be taken into consideration for this paper.

In addition to this, the version of the Bluetooth specification that was available at the beginning of this project was version 4.2. This project will focus on the analysis of the contents of the 4.2 specification.

1.4 Note on Referencing

Throughout the course of this work, the type of in-text referencing is used where the first 3 letters of the author's name is referenced plus the last two digits of the year of the referenced publication. No page number is provided with this type of referencing.

It is the author's intent to make the Bluetooth specification more accessible for others, and when referencing the Bluetooth specification, the following conventions will be used.

- BLE-LL refers to volume 6 part E of the specification.
- BLE-GAP refers to volume 3 part C of the specification.
- BLE-ATT refers to volume 3 part F of the specification.
- BLE-GATT refers to volume 3 part G of the specification.
- BLE-SMP refers to volume 3 part H of the specification.
- BLE-Supp refers to the Core Specification Supplement version 4 (CSS)

When the specification is referenced, the page numbers of the respective volumes will be included so that it is easier to locate the information and gain further background information.