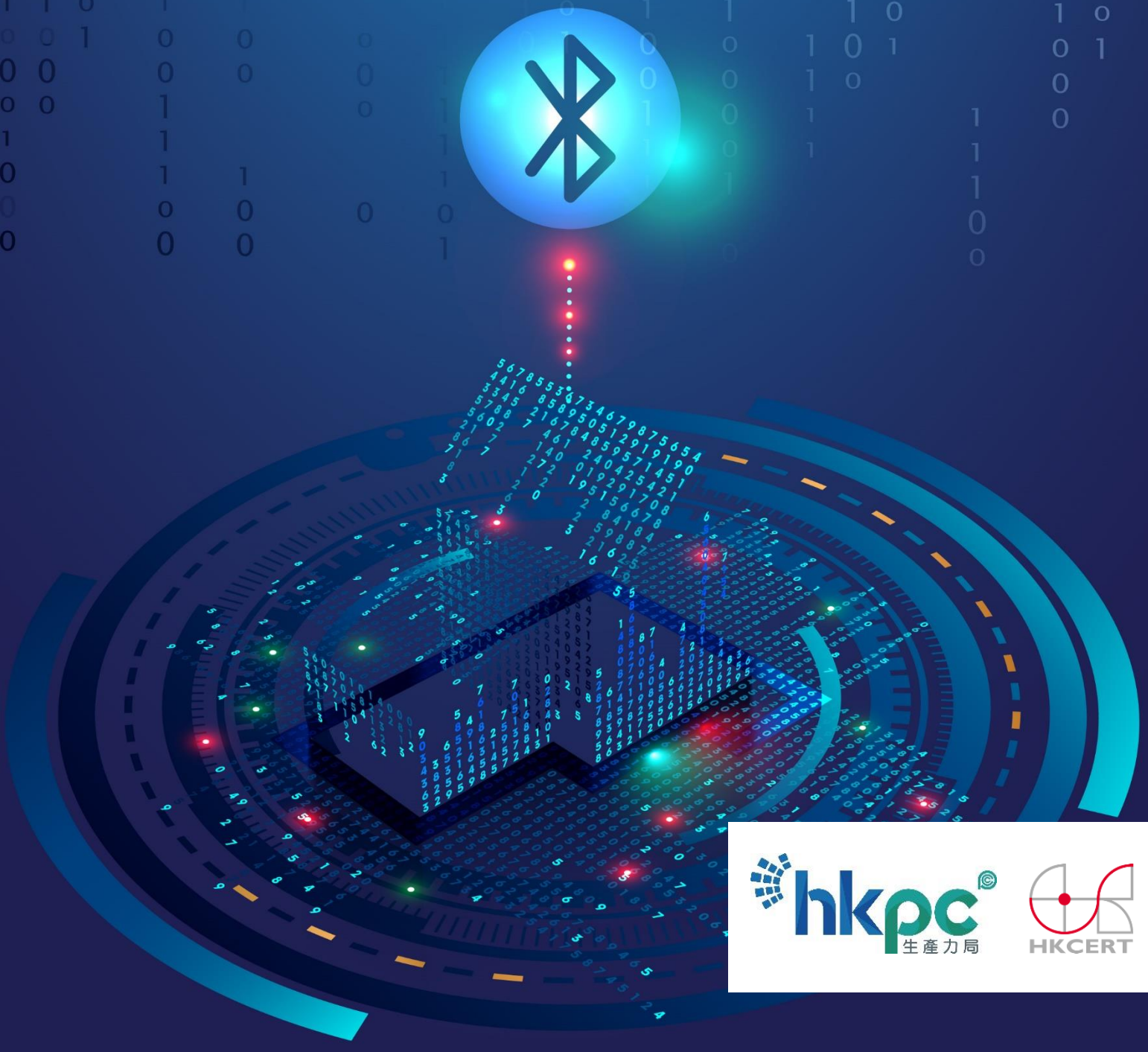
IoT Device (BLE) Security Study

February 2020



hkpc 生產力局

HKCERT

Disclaimer

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Productivity Council (HKPC) reserve the right to amend the document from time to time without prior notice.

While we have made every attempt to ensure that the information contained in this document is obtained from reliable sources, HKCERT is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is intended to provide general information and for reference only. Reliance or use of this information shall be at the reader's own risk. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will HKCERT, HKPC or its partners, employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this document, or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Licence

Table of Contents

1. Background

The applications of the Internet of Things (IoT) are becoming more diverse with the rapid development of wireless technology. Each type of IoT devices has to adopt the appropriate wireless technology in accordance with their application requirements. Among various wireless technologies, Bluetooth Low Energy (BLE) has become one of the most widely used wireless technology for IoT devices due to its low power consumption, low cost and feasibility on applications. BLE is used in many fields, including smart home, healthcare, entertainment and industry, etc.

BLE devices bring convenience to their users but also come with potential cyber security vulnerabilities that the users need to be aware of. Attackers may try to control the device, steal sensitive information from it, execute code remotely, or even cause other substantial damage. In addition, there is the issue of privacy related to BLE devices which may make the devices being tracked.

HKCERT has, therefore, conducted a study on BLE devices and selected some of them for security testing. We hope to illustrate relevant security issues through the test results in order to help raise security awareness of the BLE devices among product developers and general users.

2. BLE Device Security Study

The use of BLE makes IoT devices more convenient and easier to use, and the connection between the devices and applications is simpler.

Since BLE chips are more affordable and easier for applications, different types of smart home appliances installed with the chips can easily connect to the mobile applications through BLE. Users can operate and customise the configuration of smart home devices with mobile applications, which not only brings convenience to users but also improves their experiences.

The application of BLE in healthcare equipment is common as well. Due to the small size and low power consumption of BLE chips, manufacturers can design wearable devices, such as smart bracelets, with sensors that monitor vital signs of their users. These devices can operate for months or years on a tiny battery to reduce the frequency of battery replacements. Users can purchase such devices and connect them to mobile applications for vital sign monitoring at any time.

2.1 Three Types of Attack Methods and Their Characteristics

Indeed, BLE devices bring more convenience to their users, but at the same time, incorrect BLE configuration will cause security issues being exploited by attackers. Overall, there are three types of attacks on BLE devices: passive attack, active attack and identity tracking. The following chart has more details.

Attack Method	Attack Characteristics
Passive attack	Eavesdrop passively on data transmission between devices to obtain information and operation commands in transit.
Active attack	Send data actively to the targeted device or tamper with the data as a man-in-the-middle, so that the targeted device receives incorrect data or runs illegal operation commands.
Identity tracking	By scanning and collecting the addresses of Bluetooth devices, generating the trajectory of device movements, inferring the users who hold these devices, and grasping their whereabouts and habits.

2.2 Application Types and Corresponding Defence Methods

As the applications of BLE devices are diverse, the security configuration of BLE devices needs to be adopted for hardware constraints and security requirements. Manufacturers can choose the correct security configuration to prevent attacks based on the characteristics of the application.

The following chart shows the application types, device examples and attack types that need to be defended against.

Application Type	Device Example	Defend Against Attack Type
Device that needs to transmit sensitive information	Communication device, critical equipment sensor, etc.	Passive attack
Device that can affect personal or environmental safety if operated illegally	Household appliances, medical and health equipment, transportation equipment, industrial operation equipment, etc.	Active attack
Device that needs to be carried around	Wearable device, mobile device, etc.	Identity tracking

For instance, if devices need to transmit sensitive data, a security configuration specifically to prevent passive attacks must be employed to avoid the theft of data in transit. For attacks that cause the device to run illegal operation commands resulting in personal safety or the environment being compromised, a security configuration that deals with active attack must be adopted. In addition, devices that will be carried around should avoid identity tracking and disclosing their users' whereabouts.

For a device with multiple features, such as portable healthcare equipment which may compromise personal safety, it needs a security configuration to address both active attack and identity tracking.

There are several corresponding security configurations in Bluetooth protocol to prevent the above attacks, which are pairing and encryption (for passive and active attacks), and privacy protection functions (for identity tracking). The followings will briefly introduce these two functions. At the same time, we will investigate the security level of BLE devices in these two aspects.

3. Security Analysis of Pairing and Encryption of BLE

3.1 Introduction

BLE devices require pairing to establish a connection. There are two distinct pairing methods - LE Legacy Pairing and LE Secure Connections Pairing (for Bluetooth 4.2 or later). The latter uses Elliptic Curve Diffie–Hellman (ECDH) to generate keys to encrypt the connection, which is more secure than the former and can effectively prevent passive attack.

LE Legacy Pairing has three available association models, known as Just Works (JW), Passkey Entry (PKE), and Out of Band (OOB). LE Secure Connections Pairing has one more available association model, which is Numeric Comparison (NC). The following chart shows the characteristics and security of various pairing association models.

Association Model	LE Legacy Pairing	LE Secure Connections Pairing	Pairing Characteristic	Scope of Application	Security Level
Just Works	✓	✓	Involves no interaction with the user.	No display, no input device.	In LE Legacy Pairing mode, it cannot defend against both passive and active attacks. In LE Secure Connections Pairing mode, it can defend against passive attack, but not active attack.
Passkey Entry	✓	✓	Requires one device to display a six-digit random number and the user to enter it into the other device.	The device that initiates the connection needs to have input, and the connected device needs to have display.	In LE Legacy Pairing mode, it can defend against active attack. However, as the pairing key can be brute forced, it cannot completely prevent passive attack. In LE Secure Connections Pairing mode, it can defend

Association Model	LE Legacy Pairing	LE Secure Connections Pairing	Pairing Characteristic	Scope of Application	Security Level
					against both passive and active attacks.
Out Of Band	✓	✓	Involves exchanging pairing key using a communication channel other than Bluetooth (such as NFC).	Devices with wireless technologies other than Bluetooth (such as NFC).	In LE Legacy Pairing and LE Secure Connections Pairing mode, it can defend against both passive and active attacks.
Numeric Comparison	×	✓	The same six-digit random number is displayed to the user on both devices. The user must indicate whether the two numbers are identical.	Device with display and YES/NO input.	In LE Secure Connections Pairing mode, it can defend against both passive and active attacks.

Regarding the three types of applications mentioned in Section 2.2, HKCERT recommends that developers refer to the following guidelines to configure pairing encryption methods with corresponding security levels:

- LE Secure Connections Pairing must be used to defend against passive attack for device that needs to transmit sensitive information. If only LE Legacy Pairing mode is available, Out Of Band model must be used.
- Passkey Entry, Out Of Band or Numeric Comparison pairing association models must be used to defend against active attack on device that can compromise personal or environmental safety if operated illegally.
- Just Works pairing association model can be used for device that does not compromise personal or environmental safety or comes without display and input. It is recommended that manufacturers use LE Secure Connections Pairing method and set the Bluetooth switch. When Bluetooth is not in use, the user can turn off Bluetooth to avoid active attack.

3.2 Security Analysis

Our investigation into the security of the pairing encryption of BLE devices found that some of them used the incorrect pairing encryption method, exposing the devices to the risk of hacking that could incur substantial damage.

We tested a BLE smart straightener, and found that it has an electronic display, but it uses the Just Works association model of LE Legacy Pairing method without an independent Bluetooth switch. We use the test platform to eavesdrop on the data transmission, finding the Handle value that adjusts the temperature and heating time, and then write the corresponding value to change the temperature and heating time through active connection with the device. We can also perform man-in-the-middle attack on it to tamper with the user's operation instructions on the straightener. This vulnerability will cause the straightener to be set at the wrong temperature and heating time. For instance, the straightener is set at a maximum temperature of 235 degrees Celsius and heat for 20 minutes. If placed next to flammable materials, it may cause a fire.

If the product is operated illegally, it could compromise personal or environmental safety. Therefore, a pairing encryption method that can prevent active attack should be used. Furthermore, for products with a display, the manufacturer should choose the Passkey Entry pairing method instead of Just Works. Obviously, using the incorrect pairing encryption method will increase the risk of the device being attacked successfully and may substantially compromise personal or environmental safety.

Refer to Section 7.1 for test details.

4. Introduction and Security Analysis of Privacy Protection of BLE

4.1 Introduction

Bluetooth devices use an address called the Bluetooth device address (BD_ADDR) as an identifier. When the Bluetooth device is in idle state, the address will be broadcasted to other devices for connection. Once the connection is established, the address will be used as the address for receiving and sending data. There are privacy risks that attackers could build a footprint of the movements of devices and, by inference, the whereabouts and habits of the actual users of those devices, through scanning for and collecting such addresses over time.

The Bluetooth privacy feature is designed to mitigate this risk. When using the privacy feature, devices have two addresses. The first one is the identity address, which acts as an unchanging identifier of the Bluetooth device. The second one is the private device address, which changes periodically. Private addresses disguise the identity of a device and when in use, it is the private address which is disclosed in over the air packets, not the identity address.

4.2 Security Analysis

After testing, we found that there are some BLE portable devices, such as smart bracelets, that do not use the BLE privacy protection function, and their Bluetooth device addresses do not change periodically. If the user uses his or her name to set the smart bracelet's device name (e.g. someone's bracelet), and the data broadcasted by the smart bracelet includes the device name, attackers can grasp the user's name and whereabouts to push advertisements or scam.

Refer to Section 7.1 for test details.

5. Recommendations

5.1 End Users

- Purchase BLE devices from official channels. Before purchasing, search for information like whether the BLE device has security vulnerability, and whether the vendor provides firmware update in official website, etc.
- Please turn on the device only when in use and connect the device immediately after it is turned on. Please turn off the device when it is idle.
- Check and update the device firmware regularly.
- Do not disclose personal information (such as name, ID, phone number, etc.) when setting the device name.

5.2 Product Developers

- Use the self-assessment checklist of the HKCERT "IoT Security Best Practice Guidelines" section 4.2.4.1 wireless security to assess the product, and improve product BLE security.
- Select the recommended security configuration based on product characteristics. (Refer to section 5.3 for details).
- Timely rollout of updates to fix BLE product vulnerabilities.

5.3 Security Configuration Advice Based on Product Characteristics and Application Types

- End users and product developer can refer to the following guidelines to purchase or develop BLE devices.

Application Type	Device Example	Type of Attack Defend Against	Security Configuration Advice
Device that needs to transmit sensitive information	Communication device, critical equipment sensor, etc.	Passive attack	Select LE Secure Connections Pairing. If only LE Legacy Pairing mode is available, select Out Of Band model.
Device that can affect personal or environmental safety if operated illegally	Household appliances, medical and health equipment, transportation equipment, industrial operation equipment, etc.	Active attack	Select Passkey Entry, Out Of Band or Numeric Comparison pairing association models.
Device that does not affect the safety of the person or the environment or without display and input	Harmless entertainment appliances	None	Recommend to use Just Works pairing association model of LE Secure Connections Pairing method and provide Bluetooth on/off function, such that users can turn off Bluetooth signal when not requiring Bluetooth operation.
Device that needs to be carried around	Wearable device, mobile device, etc.	Identity tracking	Enable the privacy protection function to avoid devices being tracked and leak user privacy.

6. Summary

- As the number of BLE devices continues to grow over the next few years, attacks against such devices will also surge.
- The developers should select the correct pairing encryption method based on product application characteristics to prevent passive and active attacks.
- Device that needs to transmit sensitive information needs defence against passive attack, and avoids being eavesdropped passively on data transmission.
- Active attack on BLE devices that involve personal and environmental safety can cause substantial damage.
- Possible to be tracked, the portable BLE device should enable privacy protection function.
- Developers can use the self-assessment checklist of the HKCERT “IoT Security Best Practice Guidelines” to assess the products in order to improve product BLE security.

7. Appendix

7.1 BLE Smart Straightener Security Test

We tested a BLE smart straightener.

In addition to using physical buttons to operate, this straightener allows users to perform remote operations through the mobile application via Bluetooth. Our test mainly involves eavesdropping data and active attacks. The flow of attack scenario can be referred to the diagram below.

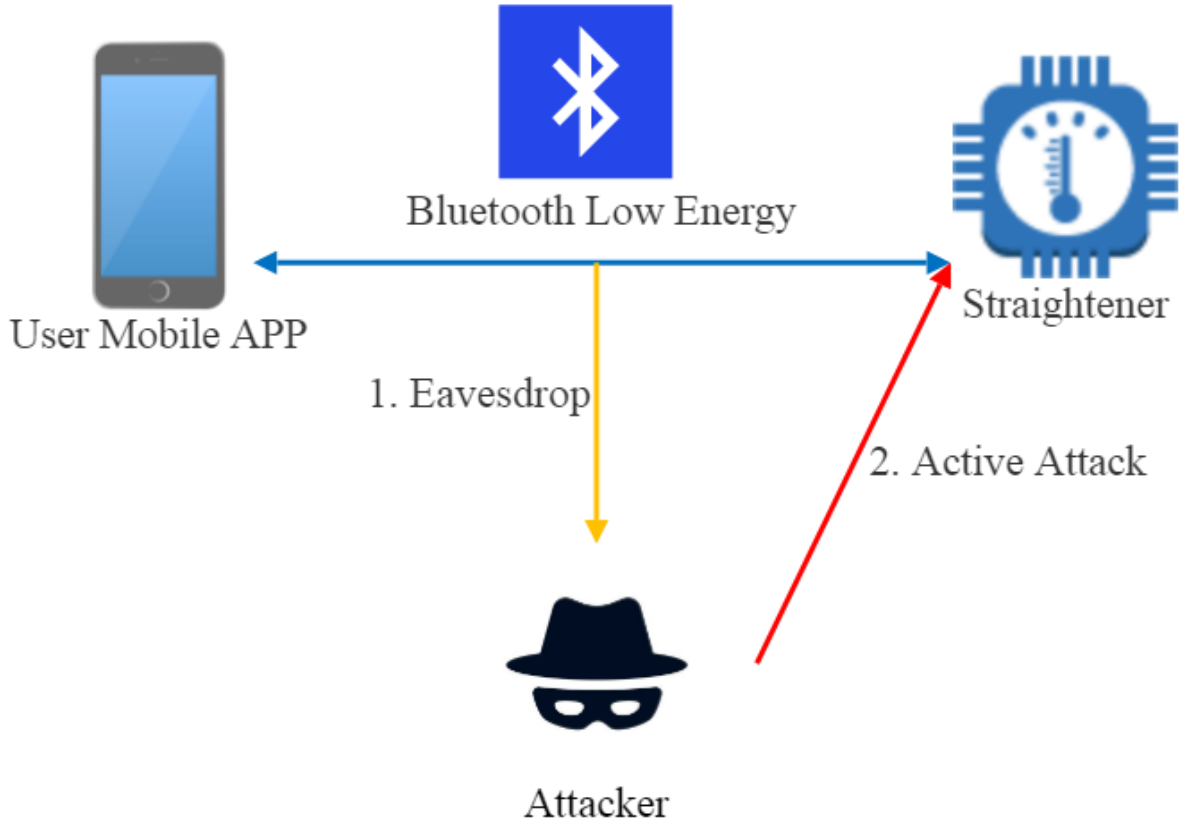


Fig. 7.1.1 Scenario diagram on the flow of attack

After turning on the straightener, we used our test platform to scan Bluetooth devices nearby and found the straightener can be scanned.

Fig. 7.1.2 BLE device scan result

We investigated the GATT file of the straightener and found that the Handle value of 0015 is writeable, indicating that we could control the straightener by writing value to this handle.

```
000e          |   Service Changed ( 00002a05-0000-1000-8000-00805f9b34fb )
                  | READ INDICATE  |

              |
                  |               |

0010 -> 0015  | 0783b03e-8535-b5a0-7140-a304f013c3b7
                  |               |

0012          |   0783b03e-8535-b5a0-7140-a304f013c3b8
                  | NOTIFY        |

0015          |   0783b03e-8535-b5a0-7140-a304f013c3ba
                  | WRITE         |

              |
```

Fig. 7.1.3 Read and write permissions of Handle value

By analysing the communication between the straightener and the mobile application, we inferred the value that controls the action of the hair straightener.

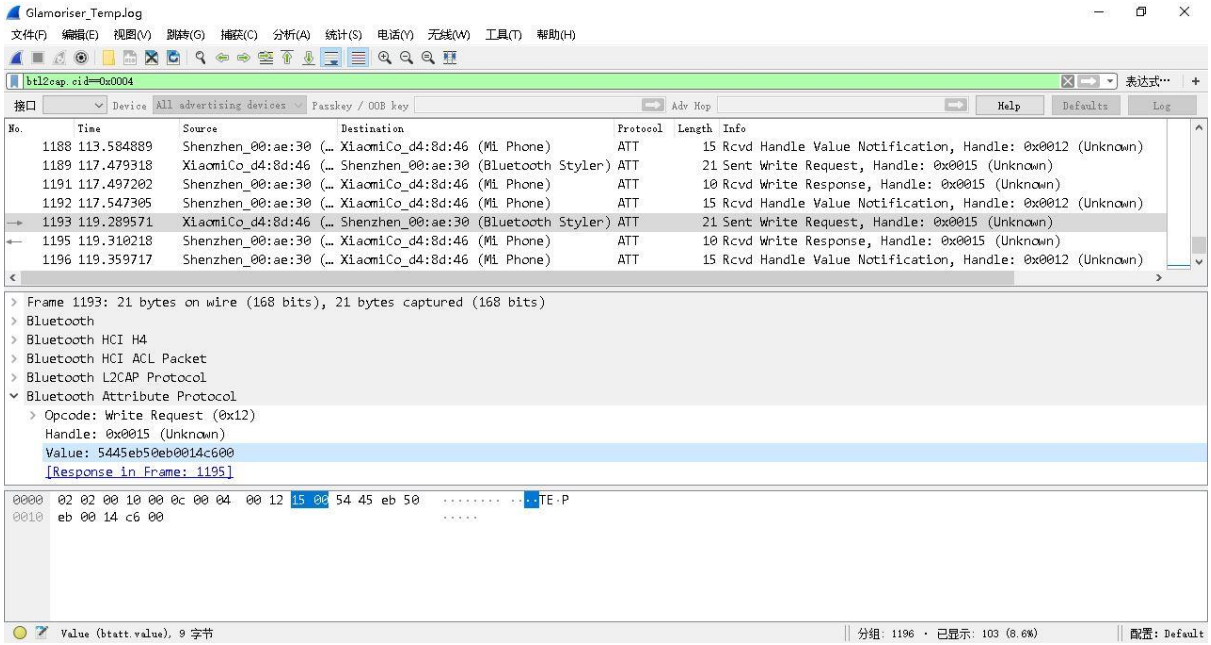


Fig. 7.1.4 Raw data communication between straightener and mobile application

We wrote the value representing the temperature of 235 degrees Celsius to the corresponding Handle value through the test platform.

```
[    ][f0:13:c3:00:ae:30][LE]> connect
[CON][f0:13:c3:00:ae:30][LE]> char-write-req 0015 5445eb50eb0014c600
[CON][f0:13:c3:00:ae:30][LE]> Characteristic value was written successfully
```

Fig. 7.1.5 Write the corresponding Handle value to straightener

The initial heating temperature of the straightener was 80 degrees Celsius.

Fig. 7.1.6 Initial temperature of the straightener before writing the Handle value

After receiving the command, the heating temperature of the straightener rose to 235 degrees Celsius.

Fig. 7.1.7 The temperature of the straightener after writing the Handle value

The straightener can be set with the heating time up to 20 minutes. If it is set to 235 degrees Celsius and placed next to flammable items, it is likely to cause a fire.

We use the self-assessment checklist of HKCERT "IoT Security Best Practice Guidelines" section 4.2.4.1 wireless security to assess the BLE transmit security of the straightener.

Wireless security self-assessment checklist

Self-Verification Checklists	Assessment Result
☐ Encryption is enabled in all wireless communications.	**No.** The pairing encryption method of this product is Just Works of LE Legacy Pairing, which cannot prevent eavesdropping. It is equivalent to no encryption. This product does not transmit sensitive data and does not need to be protected from passive attack. However, the attacker will obtain the operation command through passive attack and analyse the command format in reverse. Therefore, it is recommended to use LE Secure Connections Pairing.
☐ Data is encrypted in application layer before transmission through wireless protocols without encryption features.	**No.** The product data is not encrypted at the application layer, and the values of the control command are fixed. This product does not transmit sensitive data and does not need to be protected from passive attack. However, the attacker will obtain the operation command through passive attack and analyse the command format in reverse. If it is not encrypted at the link layer, it is recommended to be encrypted at the application layer.
☐ Due to limited device computation power, content in wireless data stream is still secured from trivial eavesdropping with alternative encryption methods.	**No.** The pairing encryption method of this product is Just Works of LE Legacy Pairing, which cannot prevent eavesdropping. Can use the two improved methods above to prevent eavesdropping.
☐ User interaction is required in initial pairing process to avoid unintended pairing to unauthorised remote party.	**No.** The pairing encryption method of this product is Just Works of LE Legacy Pairing, which does not need user interaction during pairing. This product will cause damage to personal or environmental safety due to illegal operation, so be sure to prevent the active attack of unauthorized third party. The pairing process requires user interaction. Because the product has an electronic display, it is recommended to use the Passkey Entry pairing method.
☐ Default wireless passphrase is only used once during initial pairing process and enforced to be changed for proceeding to normal service.	Not applicable.

From the above assessment results, if the product can adopt the best practices of the guidelines, the wireless security of the related products can achieve effective improvement.

7.2 Smart Bracelet Privacy Security Test

We tested the privacy security of a BLE smart bracelet and found that it is not enabled for privacy protection with the failure of the Bluetooth device address to change periodically. If the user inputs the his name as the device name in the setting, attackers can scan and collect the Bluetooth device address to create a footprint of the device's movement and grasp the user's whereabouts and habits.

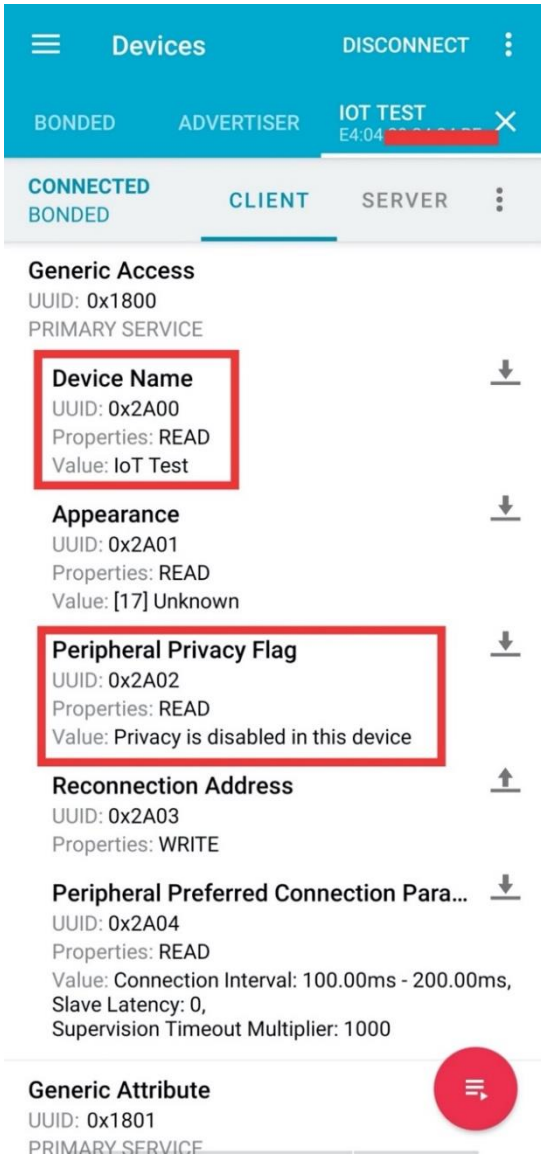


Fig. 7.2.1 Smart bracelet privacy security configuration issue