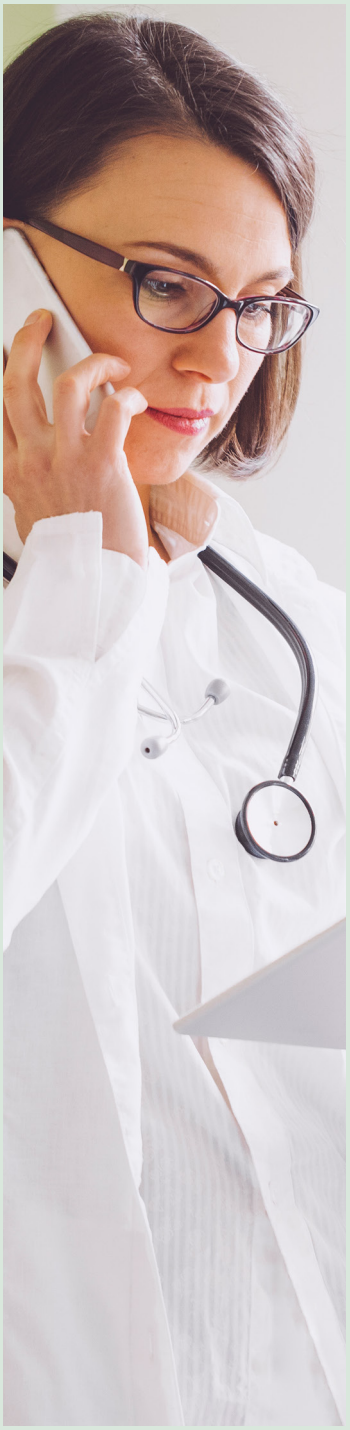
WHITE PAPER



BLE TECHNOLOGY FOR MEDICAL DEVICES

Infosys®
Navigate your next

Table of Contents

1.0 Introduction

This document evaluates the security considerations when using Bluetooth Low Energy or (BLE) technology in devices deployed in medical domains. Since these devices generate patient-specific data, there is significant importance attached to the security, integrity and privacy of the data. Hence essential design considerations come into play when using BLE for these applications, as they need to comply with the regulatory standards in the medical domains.

The document looks at the BLE Communication layer security and security for data-in-transit, the security infrastructure that the BLE protocol offers and gives a view on the BLE security challenges and how they can be overcome.

The document does not address any specific medical product type or application or address specific security considerations for BT profiles applicable to the medical domain, such as the insulin delivery profile. The reader can refer to the relevant BT Gatt Specification document to gain insights into what security should be adopted for a specific profile. This document does not focus on data-at-rest security.

2.0 Target audience

The document is aimed at medical application developers and medical product designers considering BLE as a communication protocol. It provides an insight into the data-in-transit security aspects to be considered in a BLE connection. It also presents potential design solutions derived from the author's experience.

3.0 BLE as a wireless connectivity option for medical devices

BLE technology is emerging as one of the popular options for wireless connectivity as it is more energy efficient than both Bluetooth classic and wi-fi. BLE technology is an open standard specified and developed by the Bluetooth Special Interest Group (SIG), based on the license-free 2.4GHz frequency band. By 2023, more than 1.6 billion BLE single mode devices will ship each year. The popularity of BLE for connecting data to applications and services is increasing. Industry analysts expect a 40% CAGR for Bluetooth connected healthcare devices through 2023. *Reference [4]

BLE is currently used in several application scenarios such as -

1. Blood pressure monitors
2. Fitbit-like devices
3. Class 3 devices like pacing systems
4. Blood glucose monitors

Many BLE Profiles and services are also available today that are Bluetooth SIG adopted, which can be utilized. Some of them are -

1. BLP/BLS: Blood Pressure Profile/Service
2. GLP/GLS: Glucose Profile/Service
3. HTP/HTS: Health Thermometer Profile/ Service
4. HRP/HRS: Heart Rate Profile/Service
5. LNP/LNS: Location and Navigational Profile/Service

3.1 Security capabilities provided by BLE

BLE includes a Security Manager component and a Security Manager Protocol (SMP). This protocol is involved in security procedures, such as pairing, which is the foundation of Bluetooth security. There are a variety of ways in which pairing may proceed. There are two distinct pairing methods available in devices running a BLE stack compliant with Bluetooth Core Specification version 4.2 or later. The first is called LE Legacy Pairing, and the second, a newer and substantially more secure method, is called LE Secure Connections.

Devices running a stack whose version is earlier than Bluetooth 4.2 will only use the LE Legacy Pairing method.

3.1.1 The difference between LE Legacy Pairing and LE Secure Connections

	LE Legacy Pairing	LE Secure Connections
Confidentiality during key distribution	It uses a simple process of exchanging confidential data to derive a symmetric key to encrypt the link during the key distribution phase.	It uses elliptic curve public key cryptography to allow a symmetric key to be securely derived. That key is then used to encrypt the link during the key distribution phase.
Association models	Just Works, Passkey Entry, OOB	Just Works, Passkey Entry, Numeric Comparison, OOB

Just Works: Involves no interaction with the user, and it is plug and play. It is the least secure of all models and not used for connections involving high security levels such as medical device applications.

Passkey Entry: Requires one device to display a six-digit random number and the user to enter it into the other device. It is not useful if the device has no display or input capability.

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, perhaps by pressing one button for yes and another for no. It cannot be used if the device has no display or input capability.

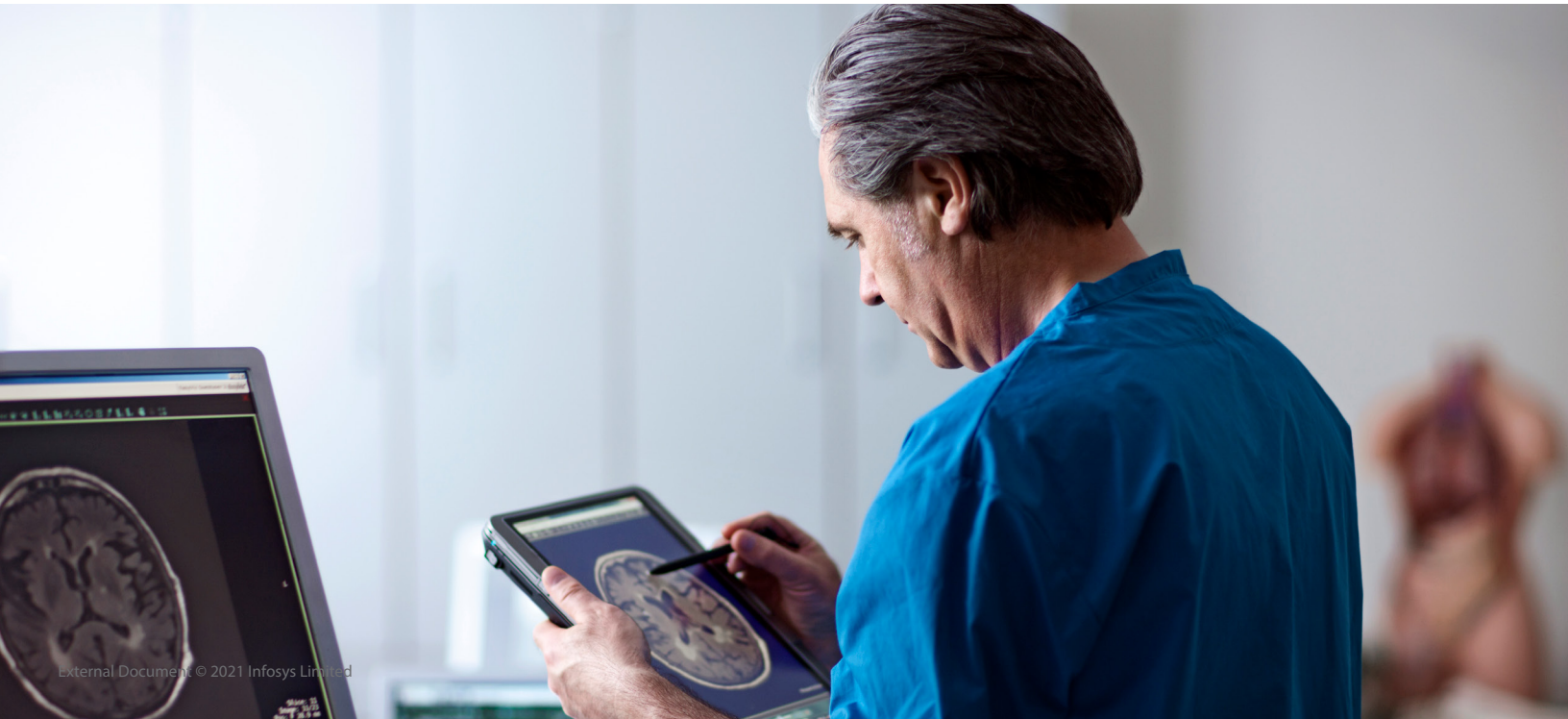
OOB: Out-of-band involves passing data between the two devices in either one direction or bi-directionally using a communication channel that is not Bluetooth. A full 128-bit key can be used here.

Recommendation: LE Secure Connections pairing is significantly more secure than LE Legacy Pairing. If two devices can use LE Secure Connections pairing, then it is mandatory to do so.

3.2 Known security issues to be aware of when using BLE in Medical devices

The Bluetooth Specification Group (SIG), the official custodians of the BT technology, have identified two known security flaws and ways to mitigate it. They are -

Vulnerability	Publication Date	Details	Specifications Affected	CVE [NVD]
Key negotiation of Bluetooth	08/13/2019	SIG Statement	Core Specification, v4.2, v5.0 and v5.1	CVE-2019-9506
Validation of Elliptic Curve Parameters	07/23/2018	SIG Statement	Core Specification, v2.1 to v5.0	CVE-2018-5383



3.2.1 Key negotiation of Bluetooth

Researchers at the Center for IT-Security, Privacy and Accountability (CISPA) have identified a security vulnerability related to encryption on Bluetooth BR/EDR connections. They identified that an attacking device could interfere with the procedure used to set up encryption on a BR/EDR connection between two devices in such a way as to reduce the length of the encryption key used. In addition, since not all Bluetooth specifications mandate a minimum encryption key length, it is possible some vendors could develop Bluetooth products where the length of the encryption key used on a BR/EDR connection could be set by an attacking device down to a single octet. The attacking device could then initiate a brute force attack and have a higher chance of cracking the key and then be able to monitor or manipulate traffic.

Mitigation:

To remedy the vulnerability, the Bluetooth SIG has updated the Bluetooth Core Specification to recommend a minimum encryption key length of seven octets for BR/EDR connections. The Bluetooth SIG will also include testing for this new recommendation within the Bluetooth Qualification Program. In addition, the Bluetooth SIG strongly recommends that product developers update existing solutions to enforce a minimum encryption key length of seven octets for BR/EDR connections. Many companies have implemented this in the latest updates to their devices.

3.2.2 Validation of Elliptic Curve Parameters

Researchers at the Israel Institute of Technology identified a security vulnerability in two related Bluetooth® features: Secure Simple Pairing and LE Secure Connections.

Bluetooth firmware or operating system software drivers may not sufficiently validate elliptic curve parameters used to generate public keys during a Diffie-Hellman key exchange, allowing a remote attacker to obtain the encryption key used by the device.

Bluetooth utilizes a device pairing mechanism based on elliptic-curve Diffie-Hellman (ECDH) key exchange for allowing encrypted communication between devices. The ECDH key pair consists of a private and a public key, and the public keys are exchanged to produce a shared pairing key. The devices must also agree on the elliptic curve parameters being used.

In some implementations, not all elliptic curve parameters are validated by the cryptographic algorithm implementation allowing a remote attacker within the wireless range to inject an invalid public key to determine the session key with high probability. Such an attacker can passively intercept and decrypt all device messages forge and inject malicious messages.

Mitigation:

After the vulnerability was identified, the Bluetooth SIG has updated the Bluetooth specifications to require validation of any public key received as part of public key-based security procedures, thereby providing a remedy to the vulnerability from a specification perspective. In addition, the Bluetooth SIG has added testing for this vulnerability within its Bluetooth Qualification Program.

3.3 Key design aspects to be considered by application developers in using BLE connections in medical devices

Medical device application developers can consider these design choices when connecting the medical devices using BLE to the gateways or device managers.

1. Ensuring that the BLE device connects to a known gateway only
2. Information is encrypted at both link layer and application and out-of-band communication of the encryption keys- (Out-of-band pairing mechanism)
3. Information integrity
4. Optimize connection duration to save battery life
5. Mitigate malicious attacks on the device

3.3.1 Ensuring that the BLE device connects to a known edge gateway only

For two BLE devices to connect, the peripheral starts to advertise, and the master device needs to scan for the advertisements during the time the peripheral advertises.

The application can be designed to ensure that the master connects only to a safe or known peripheral. It can be achieved in the following manner -

- The master needs to know which UUID it needs to scan.
- Before attempting a BLE communication the master sends an Initiate BLE communication request on an out-of-band communication link such as NFC or any other close range proprietary wireless technology.
- The peripheral then creates a uniquely generated UUID and passes this information to respond to the Initiate BLE communication request.
- The master uses the UUID and scans for this UUID before sending a connection request.
- The peripheral will use this UUID in its advertising data. This advertising message would be picked up by the master, which then initiates a BLE connection request to the peripheral.
- The peripheral could have a list of approved masters it could receive BLE connections from and then accept the connections from only those masters.

3.3.2 Information is encrypted at both link layer and application and out-of-band communication of the encryption keys- (out-of-band pairing mechanism)

There should be a dual encryption policy followed, with one at the BLE link layer as well as the application layer. The master would send an Initiate BLE communication request to the peripheral, an out-of-band communication link such as NFC or any other close range proprietary wireless technology. As part of the response to this request, information such as ephemeral AES key that would be used by both the parties for application layer encryption, the random number to be used with the AES key in addition to the link layer encryption key along with the random number to be used with this key is sent. The keys used will be a minimum encryption key length of seven octets. This approach helps us to mitigate the security risk "Key Negotiation of Bluetooth" clearly.

The mechanism described above is an out-of-band pairing mechanism that is the most secure; a close range wireless communication technology such as NFC could be used. The use of a 128 bit AES key would significantly enhance the security of the connection.

BLE Diagram

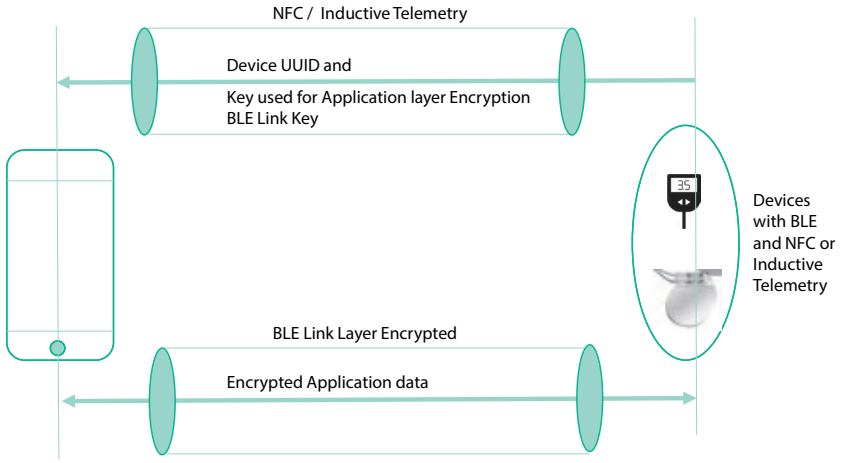


Figure 1 describes the scenarios in Section 3.3.1 and 3.3.2

3.3.3 Information integrity

It is always preferred to packet size data and perform a CRC check for each packet to ensure data integrity. This can be done at the application layer.

The application should use the data integrity mechanism provided by the BLE protocol at the link layer. If a BLE data packet is corrupt, then the data transfer will need to be retried.

BLE uses the AES-CCM cipher with 128-bit key length to provide data encryption and integrity over the wireless link. The key is generated using the Diffie-Hellman method with elliptic curve cryptography (ECC). Each device generates the same AES-CCM key at its end using the ECC public key received from the peer and its own secret ECC private key.

The BLE Data Channel PDU has a Data PDU header and the L2CAP data packet and the MIC (Message Integrity Check). These are the inherent data integrity check mechanisms available at the link layer that can be utilized.

3.3.4 Optimize connection duration to save battery life

The medical device must ensure that its battery life is maximized as it can be implanted in the body. For maximum battery life, the medical device should log and analyze its BLE connectivity usage in terms of, say, hours per day and then turn off the BLE advertising longevity after the hourly usage threshold is met for the day. It is also possible to experiment with the advertising frequency to ensure minimal battery is used. With this, the tradeoff would ensure that the time required to set up the BLE connection is acceptable.

3.3.5 Malicious attacks on device resulting in battery drain

The peripheral device could be subject to malicious attacks. One way to mitigate an attack is for the peripheral device to discard the data when it finds the received data is invalid when opening a connection. The validity of the data is determined by failure to decrypt. The termination of the connection could be done based on repeated occurrences of receipt of invalid data.

As part of the messaging protocol, a data counter could be maintained that keeps count of the received packets. If the counter of the data packet received is higher than the data counter stored, the peripheral device could update its counter. However, if the counter of the packet received is lower than the stored counter, it will likely be a stale message and discarded. Receipt of repeated stale messages could be construed as an attack resulting in the termination of the connection.

Man in the Middle Attack: This is mitigated by the out-of-band pairing mechanism described in the previous section, using short range wireless communication such as NFC.

3.4 BLE co-existence with other networks

Bluetooth sends signals over a 2.4GHz radio frequency. This becomes an issue when other nearby devices are also using the same frequency. Wi-fi is perhaps the biggest challenge. Interference can result in causing many Bluetooth connections to drop and is a crucial factor to be considered in medical applications. In such instances, the following approach may be used to mitigate the issue.

Both Bluetooth and wi-fi devices use the 2.4 GHz band, but many wi-fi devices can use the 5 GHz band instead. If the wi-fi router supports both bands, it helps connect the wi-fi devices to the 5GHz band.

4.0 Summary.

- Some of the best practices addressed in the document include:
    - Adopt a dual encryption policy, with one at the BLE link layer as well as the application layer
    - Use an out-of-band BLE pairing mechanism with a close range wireless communication technology such as NFC, or any proprietary short range wireless technology
    - Use a 128 bit AES key to enhance the security of the BLE connection
    - Use CRC check to ensure application data integrity

BLE is, thus, a good open wireless standard that can be used in the medical device connectivity landscape. It is optimized for low power and brings in the latest encryption technologies (AES-128 encryption), robust data integrity mechanisms with 24-bit CRC, 32-bit message integrity check (MIC) with fast connection setup times and several in-built profiles (mesh profile, healthcare profiles, fitness profiles, etc.) that can be used in medical devices. With proper usage of the BLE security mechanisms, companies are building medical devices incorporating BLE communication protocol.

References:

[1] https://www.fda.gov/medical-devices/digital-health/wireless-medical-devices

[2] https://www.networkcomputing.com/wireless-infrastructure/iot-security-using-ble-encryption

[3] https://support.apple.com/en-us/HT201542

[4] https://www.bluetooth.com/bluetooth-resources/2019-bluetooth-market-update/

[5] https://www.bluetooth.com/security/

About the Author

Balaji

Senior Principal Technology Architect in Infosys and focuses on Cardiac Rhythm Management device softwares

Balaji has close to 30 years of industry experience in areas of Class 3 medical application development, wearable devices creation, mobile handset and mobile tablet realization, VOIP protocol development and embedded software. He has expertise in consultancy, practice management, software architecture and software development. Currently, Balaji is a Senior Principal Technology Architect in Infosys and focuses on Cardiac Rhythm Management device softwares.

For more information, contact askus@infosys.com

Infosys®
Navigate your next