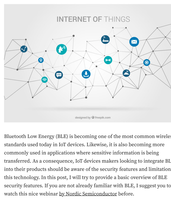
Published in Rhone IoT Security

Alexis Duque
Sep 3, 2018 · 11 min read · Listen

Deep Dive into Bluetooth LE Security



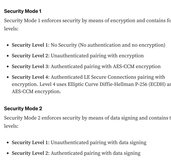
Bluetooth Low Energy (BLE) is becoming one of the most common wireless standards used today in IoT devices. Likewise, it is also becoming more commonly used in applications where sensitive information is being transferred. As a consequence, IoT devices makers looking to integrate BLE into their products should be aware of the security features and limitations of this technology. In this post, I will try to provide a basic overview of BLE security features. If you are not already familiar with BLE, I suggest you to watch this nice webinar by Nordic Semiconductor before.

Overview

A BLE connection is said to operate at a specific security mode for which there are several security levels. The required security mode/level of a connection may change from time to time, leading to procedures to increase that level. Note that each connection starts its lifetime in Security Mode 1, Level 1.

When two devices, which initially do not have security, wish to do something that requires security, the devices must first pair. This process is triggered by a *Central device* (e.g. a smartphone) that is attempting to access a data value (a "characteristic") on a *Peripheral device* that requires authenticated access. Pairing involves authenticating the identity of two devices, encrypting the link using a short-term key (STK) and then distributing long-term keys (LTK) used for encryption. The LTK is saved for faster reconnection in the future, that is termed *Bonding*.

This process is shown the following figure:



Bluetooth pairing process

The new security level of the connection is based on the method of pairing performed and its selection is based on the I/O capabilities of each device. The security level of any subsequent reconnections is based on the level achieved during the initial pairing.

The role each device plays is defined in the Security Manager (SM) portion of the BLE stack. They are the *Initiator* (the central), and the *Responder* (the peripheral).

Encryption and Authentication

The encryption in Bluetooth LE is based on 128-bit Advanced Encryption Standard — Counter with CBC-MAC (AES-CCM). LTK is used with this algorithm to create the 128-bit "shared secret" key.

Authentication is provided in Bluetooth (LE) by digitally signing the data using the connection Signature Resolving Key (CSRK). The sending device places a signature after the Data PDU. The receiver verifies the signature using the CSRK.

Security Modes and Levels of a Connection

For a BLE connection,the Generic Access Protocol (GAP) defines two security modes, along with several security levels per mode.

Security Mode 1

Security Mode 1 enforces security by means of encryption and contains four levels:

- **Security Level 1**: No Security (No authentication and no encryption)
- **Security Level 2**: Unauthenticated pairing with encryption
- **Security Level 3**: Authenticated pairing with AES-CCM encryption
- **Security Level 4**: Authenticated LE Secure Connections pairing with encryption, Level 4 uses Elliptic Curve Diffie-Hellman P-256 (ECDH) and AES-CCM encryption.

Security Mode 2

Security Mode 2 enforces security by means of data signing and contains two levels:

- **Security Level 1**: Unauthenticated pairing with data signing
- **Security Level 2**: Authenticated pairing with data signing

Mixed Security Mode

Mixed Security Mode is when a device is required to support both Security Mode 1 and 2, i.e., it needs to support signed and unsigned data. Secure Connection Only Mode is Secure Mode 1 with Security Level 4, meaning that all incoming and outgoing traffic in a Bluetooth device involve authenticated connections and encryption only.

Each connection starts its lifetime in Security Mode 1, level 1 and can later be upgraded to any security level by means of an authentication procedure discussed below. When pairing, the method/algorithm chosen determines if the pairing performed a strong authentication or not. Unauthenticated pairings occur in situations where the device could not authenticate itself (for example, if it has no input/output capabilities).

Further details are provided in Vol. 3, Part C, Section 10 of the BLE v4.2 Core Specification.

Pairing Modes

Pairing involves authenticating the identity of the 2 devices to be paired, usually through a process of sharing a secret. Once authenticated, the link is encrypted and keys are distributed to allow security to be restarted on a reconnection much more quickly. If these keys are saved for a future time, the devices are said to be Bonded. The pairing happens in 3 phases.

Phase 1

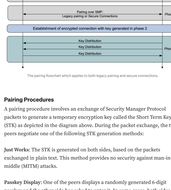
In phase one, the two devices let each other know what they are capable of doing. The values they are sending are Attribution Protocol (ATT) values and live at layer 4 with L2CAP. They are not encrypted. These values determine which pairing method is going to be used in phase two and what the devices can do and what they expect. For instance, the peer's input and output capabilities which are selected from one of the following possibilities determine the connection security level. These capabilities are communicated between the devices by using the Security Manager (SM) Pairing Request message. They are: No Input No Output, Display Only, Display Yes/No, Keyboard Only and Keyboard Display.

Phase 2

In phase 2, the purpose is to generate a Short Term Key (STK). This is possible with the devices agreeing on a Temporary Key (TK) mixed with some random numbers which gives them the STK. The STK itself is never transmitted between devices. The use of STK is commonly known as LE legacy pairing. However, if the Secure Connection Only Mode is being used, a Long Term Key (LTK) is generated at this phase (instead of an STK) and this is known as LE Secure Connections.

Phase 3

In phase 3, the key from phase two is used to distribute the rest of the keys needed for communications. Whereas on LTK wasn't generated in phase two, one is generated in phase three. In this phase, data like the Connection Signature Resolving Key (CSRK) for data signing or the Identity Resolving Key (IRK) for private MAC address generation and lookup are generated.



The pairing flowchart which applies to both legacy pairing and secure connections.

Pairing Procedures

A pairing procedure involves an exchange of Security Manager Protocol packets to generate a temporary encryption key called the Short Term Key (STK) as depicted in the diagram above. During the packet exchange, the two peers negotiate one of the following STK generation methods:

Just Works: The STK is generated on both sides, based on the packets exchanged in plain text. This method provides no security against man-in-the-middle (MITM) attacks.

Passkey Display: One of the peers displays a randomly generated 6-digit passkey and the other side has asked to enter it. In some cases, both sides enter the key if no display is available. This method provides protection against MITM attacks.

Out of Band (OOB): In this method, the additional data can be transferred by other means than the BLE radio (such as another wireless technology like NFC). This method also provides protection against MITM attacks.

Numeric Comparison (LE Secure Connections Pairing) and only with BLE 4.2: This method uses an algorithm called Elliptic curve Diffie-Hellman (ECDH) for key generation and a new pairing procedure for the key exchange. The link is encrypted using LTK from Phase 2

The table below is a reference to determine/for determining the pairing method based on the two devices I/O capabilities and the role each device plays in the process.

		Initiator				
	I/O Capabilities	DisplayOnly	DisplayYes/No	Keyboard Only	NoInputNoOutput	Keyboard Display
Responder	DisplayOnly	Just Works	Just Works Passkey Display: (responder displays, initiator inputs)	Just Works Passkey Display: (responder displays, initiator inputs)	Just Works	Just Works Passkey Display: (responder displays, initiator inputs)
		Unauthenticated	Unauthenticated	Authenticated	Unauthenticated	Authenticated
	DisplayYes/No	Just Works	Just Works Out of band (OOB) Numeric Comparison (for LE Secure Connections Pairing)	Passkey Display: (responder displays, initiator inputs)	Just Works	Passkey Display: (responder displays, initiator inputs) Out of band (OOB) Numeric Comparison (for LE Secure Connections Pairing)
		Unauthenticated	Unauthenticated	Authenticated	Unauthenticated	Authenticated
	Keyboard Only	Unauthenticated Passkey Display: (initiator displays, responder inputs)	Unauthenticated Passkey Display: (initiator displays, responder inputs)	Authenticated Passkey Display: (initiator displays, responder inputs)	Unauthenticated Just Works	Unauthenticated Passkey Display: (initiator displays, responder inputs)
		Authenticated Just Works	Authenticated Just Works	Authenticated Just Works	Unauthenticated Just Works	Authenticated Just Works
	NoInputNoOutput	Just Works	Just Works	Just Works	Just Works	Just Works
		Unauthenticated	Unauthenticated	Unauthenticated	Unauthenticated	Unauthenticated
	Keyboard Display	Passkey Display: (initiator displays, responder inputs)	Passkey Display: (initiator displays, responder inputs) Out of band (OOB) Numeric Comparison (for LE Secure Connections Pairing)	Passkey Display: (initiator displays, responder inputs)	Just Works	Passkey Display: (initiator displays, responder inputs) Out of band (OOB) Numeric Comparison (for LE Secure Connections Pairing)
		Authenticated	Authenticated	Authenticated	Unauthenticated	Authenticated

Pairing procedure and I/O capabilities

Bonding Modes and Procedure

There are two modes:

- **Non-Bondable Mode**: this is the default bondable mode for devices. This means the device will not accept bonding. No keys will be exchanged or stored by the device.
- **Bondable Mode**: to accept a bonding request, the Peripheral must set the bonding bit in the authentication requirements of the Pairing Request message during pairing. The device exchanges security keys and stores them.

If a Central wants to bond with a Peripheral device it believes is bondable, it uses the bondable procedure. It initiates pairing with the same bonding bit set in the authentication requirements of the Pairing Request message. If the Peripheral device is bondable, it will respond with the bonding bit set. If all this happens, the keys will be distributed after the link is encrypted and then the keys are stored. Once the keys have been distributed and stored, the pair of devices are said to be Bonded.

Conclusion

BLE offers several features for securing communication between devices, each with its own advantages and limitations.

As IoT devices makers, we take care of implementing BLE features into their designs. We are aware of the specific security threats facing BLE and make our best effort to leverage BLE's security features to mitigate them.

Annexe 1: Summary of 4.0 and 4.2 differences

Bluetooth 4.2 introduced a new security model, LE Secure connections. LE Secure Connections use an algorithm called Elliptic curve Diffie-Hellman (ECDH) for key generation and a new pairing procedure for the key exchange.

Using LE Secure Connections with the ECDH algorithms to generate public/private keys pairs, the Security Manager protects the communication from passive eavesdropping regardless of the I/O capabilities and pairing methods (Numeric Comparison, Just Works, Passkey Entry, and Out Of Band). It will provide protection from Man-In-The-Middle (MITM) attacks if the application uses Numeric Comparison, Passkey Entry, and Out Of Band as the pairing method.

References

Bluetooth Core Specification, ver. 4.1, Bluetooth SIG, December 2013

Bluetooth Core Specification, ver. 4.2, Bluetooth SIG, December 2014

Bluetooth Pairing https://blog.bluetooth.com/bluetooth-pairing-passkey-entry August 2016

Rosa, T. (2013, May 23). *Bypassing Passkey Authentication in Bluetooth Low Energy*. Retrieved August 01, 2016, from https://eprint.iacr.org/2013/309.pdf

Ryan, M. (2013). *Bluetooth: With Low Energy Comes Low Security*. Retrieved August 01, 2016, from http://www.usenix.org/conference/woot13/workshop-program/presentation/ryan

This post has been posted on Rhone blog. I would like to thanks Jenny Bazar for the review.

139 139

More from Rhone IoT Security
Blog about IoT security by Rhone IT Nexus.
Alexis Duque · Aug 28, 2017
Make your Bluetooth Low Energy IoT device more secure with Visible Light Communication
About IoT security Since the Internet of Things is still in the emerging phase, ensuring security and privacy is an important issue that must b...
Internet Of Things · 4 min read

Read more from Rhone IoT Security.

Get unlimited access

Search

Alexis Duque
51 Followers
Director of Research @Rhone_IoT | Ph.D. VP of Eng. @NetVX. Research Associate @ 5 Edinburgh Bio & Eng. Ex-pharmacist by Royal Charter. Rhone IoT Security
Follow

More from Medium
Joseph Nathaniel in NerdCouch
YouTube is Dead and Something Now is Coming
Ibrahim Jabbi
8 Must Have Google Chrome Extensions to Save Hours of Work Into Minutes
Arshad Sogi in Better Humans
4 Uneasy One-Minute Habits That Save Me 20+ Hours Every Week
Liam Zaudtke in Curiosity
10 Unified New Apps to Explore Immediately (September 2022 Edition)
Help Status Writers Blog Careers Privacy Terms About Knowable