Secure Bluetooth Low Energy Temporary Key Exchange

Monjur Hasan, Brandon Chen, Mark Guindi, Sabrina Supapkooha, Jimmy Lauchoy

1. Abstract

Bluetooth Low Energy (BLE) protocol is a wireless network technology. It is designed to have a smaller power consumption and overall cost than its Bluetooth counterpart, while still maintaining a similar range to communicate with other devices. This is possible because BLE technology sends small packets through its connections instead of constantly scanning and transmitting data, and therefore uses less power. The traditional method of connection between two BLE-enabled devices involves a three phase pairing process. While effective in most use cases, sensitive data (passwords, credit card info, etc) can be intercepted through a passive eavesdropper, compromising the confidentiality of such data. Such compromises can further allow the attacker to manipulate and hijack devices, known as a Man-in-the-Middle attack.

We propose a long term key (LTK) exchange technique during the pairing process that utilizes other wireless technologies such as near-field communication (NFC). Not only does this ensure a secure channel for TK exchange, larger TK keys can be used for greater security and enhances immunity to passive eavesdropping.

Keywords - Bluetooth, Low Energy, pairing, Man-in-the-Middle, LTK, passive eavesdropping

2. Introduction

In a world of increasingly connected IoT devices, development of efficient data transmitting devices has been the goal of many companies and research institutions. In situations where large amounts of data need to be sent over a wireless network, battery consumption is not a big concern. However, small devices such as smartphones and smartwatches can send data over a wireless network but are limited by the capacity of their batteries. Therefore, radio devices need to be developed to deliver a reasonable amount of data with as little power consumption possible while keeping it secure against most vulnerabilities.

Bluetooth Low Energy (BLE) is a subset of the Bluetooth protocol, integrated into any mobile platform requiring secure data transfers. A Generic Access Profile (GAP) defines roles for the type of device, mainly peripheral and central roles. This unique device GAP makes a device visible to other devices, and controls the interactions between two devices. Advertising data payload can contain up to 31 bytes of data, which is constantly transmitted from the device for visibility. One feature of the Bluetooth Low Energy protocol is Broadcasting, the ability to send one-way data to multiple devices in listening range.

A more common use case is data transfer between two devices, which is managed by a Generic Attribute Profile (GATT) using Services and Characteristics. GATT connections are exclusive to the specific connected devices and will stop broadcasting advertising data payloads once a connection is established. A GATT client initiates a request from the GATT server to initiate Attribute Protocol (ATT) lookup data, which contain nested objects. Services are containers for characteristics, labeled by a 16-bit unique numeric ID (UUID). Characteristics within a service contain single data points such as latitude, longitude data from a GPS sensor, and have UUIDs defined by the Bluetooth Special Interest Group [8].

3. Background

First introduced as Wibree by Nokia in 2006 [6], this low energy wireless protocol had a theoretical transfer speed of 1 Megabyte per second, but at one-tenth the power cost compared to Bluetooth technology. This technology enabled new use-cases and growth potential in the market of mobile devices. Wibree merged with the Bluetooth SIG in 2007 to standardize the Bluetooth user experience, which would further push BLE into the mainstream [7]. Apple Corporation's iPhone 4S was the first commercialized product to have BLE 4.0 implemented, with a slew of manufacturers following suit by 2012. BLE Core Specifications 4.0 and 4.1 utilized LE Legacy Pairing, while version 4.2 is capable of creating LE Secure Connections via a Long Term Key (LTK) for encryption [3]. Generated using Elliptic Curve Diffie Hellman (EDCH) public key cryptography, LTKs provide a more secure authentication channel during the pairing process. Version 5.0 increases connectivity range and data broadcasting capacity for IoT appliances for connected homes.

In order to mitigate threats against BLE by Bltejacking, OOB (out-of-band) pairing is a simple solution which doesn't require bluetooth and also allows developers to integrate their own security models. However, one downside is that it requires large amount energy to run which can be a burden for low energy capabilities bluetooth device. Fortunately, Near Field Communication protocol (NFC), OOB pairing can be used by bluetooth devices which is a set of communications protocol that allow devices to exchange data over a short distance. This short proximity makes sure that cryptographic keys can be exchanged without an attacker receiving it as well. While only small amount of data can be exchanged, the advantages of NFC outweighs the minor setbacks.

4. Threat Model

The OOB (out-of-band) pairing is poised to be a fairly adequate solution to the threats posed by Bltejacking since it not only provides users the option to initiate connections without using bluetooth but also is flexible enough to allow developers to formulate their own security mechanisms. Displayed below: the attack tree demonstrating a broad view of threats (for reference) and solutions provided by OOB pairing.

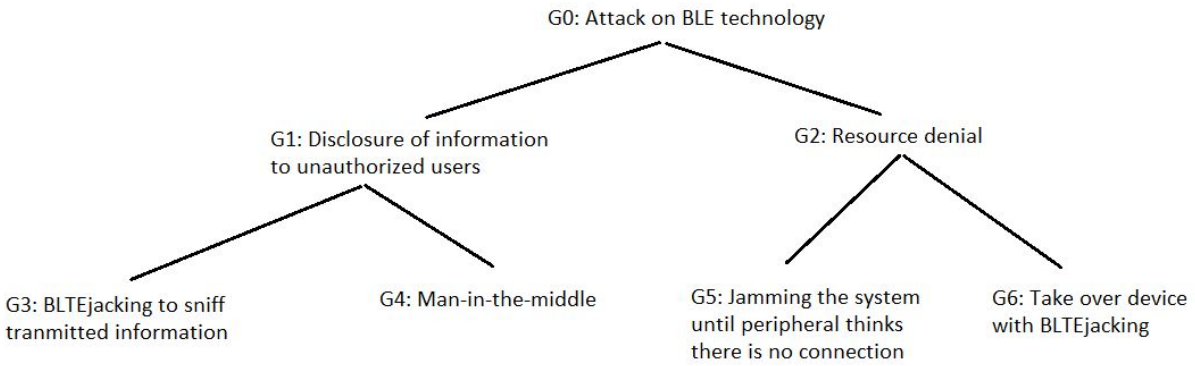

Figure 1. Attack Tree of Btlejacking Threats.

Threat	**Solution Proposed by OOB Pairing**

G3 Packet Sniffing/Injection	OOB pairing prevents packet altercation by giving developers the option to attach unique identification to packets and have devices only receive packets with authorized identification. Thus, if attackers send harmful packets with unauthorized identification, the attack would be nulled since the identification is incorrect.
G4 Man-In-The-Middle Attack	Developing their own security mechanisms, users can have devices generate unique and uncrackable keys at the beginning of a session so that any attacks after initialization would be blocked since attackers would not have the key(s); thus, preventing any successful hijacking/jamming attempts.
G5, G6 Hijacking/Jamming Session	OOBA (out-of-bound authentication) can guard against hijacks and jams by having two channels communicate over a 3G or 4G wireless network instead of the Internet. Therefore, hackers with keyloggers or other types of equipment would not be able to intercept the SMS message. Once the message is sent, the OOB pairing encrypts the channels to prevent any attack.

OOB pairing provides the capabilities for developers to essentially build their protection, therefore, allowing developers to fine-tune their defenses in the case that they need to protect from a specific attack - however, that does not suggest that devices are fully protected from attacks. Sophisticated attacks, such as the man-in-the-middle attack, can still penetrate devices such that:

1. Attackers are able to obtain the necessary key(s) before encryption.
2. Attackers are able to trick devices into a connection by establishing and promoting a fake network as a legitimate network.

5. Design

In the framework of OOB pairing, the field is defined as a flag and consists of values that indicate whether or not OOB authentication data is available. The OOB flag field is made up of one byte. The value of 0/1 is used to determine whether the OOB pairing is supported, while the remaining values are reserved for future use.

On devices connecting with BLE legacy pairing, the OOB flags of both devices are checked. Only if the OOB flag of *both* devices is set will the devices proceed to connect using OOB, as described below. Otherwise, the devices will continue to connect without OOB pairing (either using a mapping of each devices I/O capabilities, or using "Just Works" as a pairing method).

The OOB pairing begins with a method similar to the low energy legacy pairing passkey method, in which a temporary key (TK) is generated and shared between the primary and secondary devices. The OOB mechanism can aid in device discovery by delivering the TK and device address. The primary device will ask the secondary device to input the TK to insinitate OOB pairing.

Once the TK has been established, exchanged, and inputted, the security managers of both devices will:

1. Create a random value on both sides, *Mrand* and *Srand*.
2. Using Mrand and Srand, compute *Mconfirm* and *Sconfirm*.
3. With *Mconfirm* and *Sconfirm* established, the primary device sends *Mconfirm* to the secondary device. Secondary device sends the Sconfirm to the primary device in response to receiving the *Mconfirm*. Likewise, the primary device sends the *Mrand* to the secondary device.
4. Using the *Mrand*, the secondary device verifies the value of the Mconfirm by utilizing a built-in function with the *Mrand* value as input.
    a. If the calculated *Mconfirm* value does not match the received *Mconfirm* value, the pairing process fails and communications terminated.
    b. If the calculated *Mconfirm* value does match the received *Mconfirm* value, the secondary device sends *Srand* to the primary device.
5. Similar to the aforementioned step, the primary device verifies the *Sconfirm* value by using a function with the *Srand* as input.
    a. If the *Sconfirm* value does not match the received *Sconfirm* value, the pairing process will fail and communications will be terminated.
    b. If the calculated *Sconfirm* value does match the received *Sconfirm* value, the primary device computes a Short Term Key (STK) and alerts the controller to enable encryption.
6. The creation of the STK and channel encryption signifies that a connection has been established between the two devices. As mentioned before, the encryption prevents attackers from hijacking and/or tampering with the channel.

6. Implementation

OOB pairing requires a large amount of energy to run - a burden that appears to be too much for the low energy capabilities of bluetooth devices. But, with the aid of the Near Field Communication protocol (NFC), OOB pairing can be utilized by bluetooth devices. The NFC is a set of communications protocols that allows devices to exchange data over a short distance of approximately ten centimeters (four inches). Though the amount of data that can be exchanged is small, NFC has a few advantages that balances out the small setback. The NFC:

1. Requires much less energy than either bluetooth or WiFi, therefore less battery drain.
2. Establishes connections quickly and requires no setup.
3. Receives and sends data.
4. Has three modes of operation:
    a. Peer-to-Peer: Two NFC devices exchange data between each other.
    b. Read/Write: Only one NFC device is active and can receive data.

c. Card Emulation: Turns NFC into a contactless card that can be used for transactions by holding the device to a compatible NFC reader.

Additionally, NFC adds another layer of protection from attacks since attackers would need to be in close proximity to the already short distance between the primary and secondary devices. Likewise, NFC devices designed to be tapped before exchanging data helps ensure that only the tapped devices will exchange data. Thus, due to its low energy and efficient functionality, the NFC acts a grounded foundation (interface) for OOB pairing. When pairing via OOB, NFC can be utilized to send the TK to the secondary device by including it in the payload of the NFC data exchange format (NDEF) message.

In short, NFC ensures that, due to the required proximity of the devices, cryptographic keys can be exchanged without an attacker receiving them as well (or, at least, an *extremely low likelihood* that an attacker can receive them). Thus, any further communications over BLE will be fully encrypted, and an attacker cannot view any of the data being sent, nor can the attacker hijack the connection.

7. Evaluation

While OOB pairings offer flexibility in security implementations, its high power consumption makes it less appealing to consumers. NFC provides a solution to the power hungry OOB pairing, but its main shortcoming - the limited connection range - severely hampers its ability to be a overall practical solution. With a maximum connection range of just four centimeters, NFC can be very secure, as any attack can only attack a connection if they too are 4 centimeters away, which is high impractical. Unfortunately, this impracticality also applies to its intended users as well. Because of its limited range, NFC will effectively render "wireless" useless for various everyday usage. Any headphones will need the main devices to be close to it, at which point one might as well just listen through the main device. Any remote devices will require users to be very close to the device itself, making the remote impractical.

8. Related Solutions

- BLE Specification - This mechanism involves adding an authentication code to all packets sent and received by Bluetooth devices. This way, if a attacker tries to add their own packets in order to jam the system or inject their own code, their packets, which will not have the correct authentication code, will be ignored by the system and will not have any effect.
- "Pitched as an alternative to Near Field Communication (NFC), **NearBytes** sees the transmitting device encrypt the data and send it as a series of chirps that sound similar to a cricket. The receiving device then captures these sounds and decodes the data. As it relies only on the devices' microphone and speaker, NearBytes doesn't require any special hardware." [9]

9. Conclusion

Bluetooth Low Energy (BLE) is a subset of the Bluetooth protocol, integrated into any mobile platform requiring secure data transfers. The primary flaw of BLE protocols - the "sweet spot" for risks to occur - is that the possibility of an attack to occur between an exchange of packets. Unencrypted packets exchanged between devices can be intercepted and observed by means of sniffing , jamming, BTEjacking or by man-in-the-middle attack. OOB pairing solves many of these problems by defining field as flag and consists of values that indicate whether or not OOB authentication data is available. However this whole process is not energy efficient. Fortunately, Near Field Communication protocol (NFC), OOB pairing can be used to overcome this problem but only downside is the it's range is very limited, so in future, a new method of BTE data transfer need to be developed which can transfer data securely over a large distance while remaining extremely energy efficient.

10. References

1. Bluetooth Pairing Part 5 - Legacy Pairing - Out of Band
https://blog.bluetooth.com/bluetooth-pairing-part-5-legacy-pairing-out-of-band

2. Leveraging Near Field Communication (NFC) to Connect with BLE Smart Sensors
https://www.digikey.com/en/articles/techzone/2017/nov/leveraging-nfc-to-connect-with-ble-smart-sensors

3. A Basic Introduction to BLE Security
https://www.digikey.com/eewiki/display/Wireless/A+Basic+Introduction+to+BLE+Security

4. Out-of-Band Authentication
https://www.techopedia.com/definition/29532/out-of-band-authentication-ooba

5. What's NFC and why should you care?
https://www.jabra.com/blog/whats-nfc-and-why-should-you-care/

6. Bluetooth rival unveiled by Nokia
http://news.bbc.co.uk/2/hi/technology/5403564.stm

7. "Wibree forum merges with Bluetooth SIG" (PDF) (Press release). Nokia. 12 June 2007.

8. Introduction to Bluetooth Low Energy
https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

9. NearBytes sounds like an NFC alternative
https://newatlas.com/nearbytes-communication-proximity/28347/