Bluetooth Security

Gustavo Padovan
University of Campinas - Brazil
gustavo@padovan.org

July 4, 2011

This article talks about Bluetooth Security, explaining the mechanisms used by Bluetooth over time to achieve its securities requirements.

1 What is Bluetooth?

Bluetooth is a radiofrequency technology that operates in the unlicensed 2.4GHz ISM band, it was designed by Ericsson as a replacement for the RS-232 data cable and is intended for short distance data exchange, usually 10 meters, but there are variants for a small 1 meter range and for 100 meters range.

Today there are many use cases for Bluetooth. Formally called "Profiles", they provide things like the Human Input Device Profile, for use in Bluetooth keyboards and mouses. Handsfree Profile, for control your cellphone calls from via a Bluetooth link, Advanced Audio Distribution Profile, for high quality audio, Audio/Video Remote Control Profile, for remote control via a Bluetooth link for commands like "Play", "Stop", etc, and informations about the current track. Personal Area Network Profile and Dial-up Network Profile, that enable sharing of an internet connection via Bluetooth. There are many others: File Transfer Profile, Message Access Profile, SIM Access Profile, etc. Check [1] for more information.

Bluetooth is specified by the Bluetooth Special Interest Group [2]. A Group formed by the companies Intel, Nokia, Microsoft, Motorola, Ericsson, Toshiba and Lenovo.

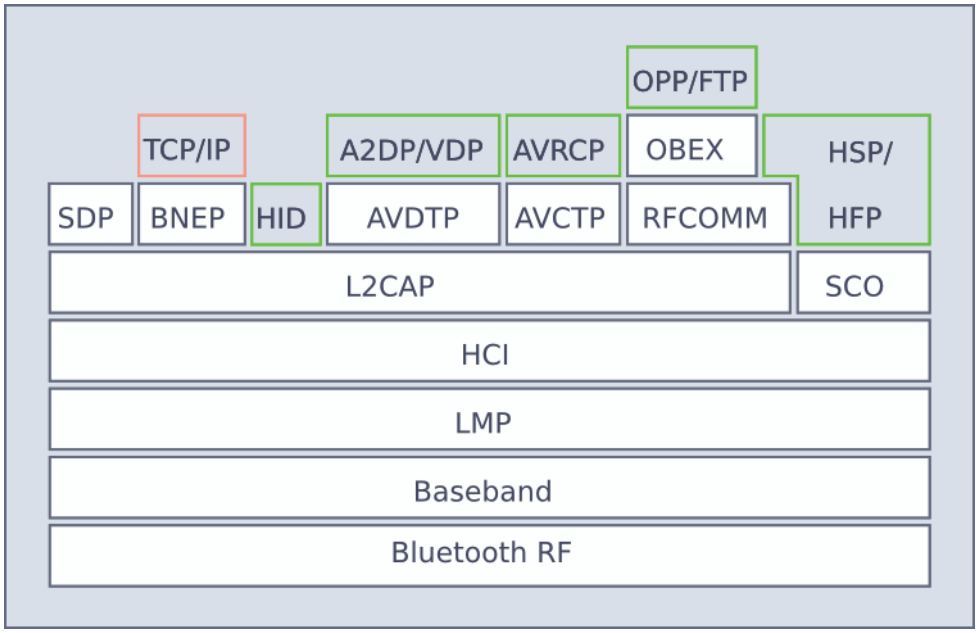
It was designed to be low power and low cost, Bluetooth chips cost few dollars and are very popular in devices over the world. Since 2010 there is a new specification for a real low power radio, that enables a device with a Bluetooth Low Energy radio to live a year without changing its battery.

The security is based in a link key exchange at the first connection between two devices. This process is called Pairing and it will be explained further.

1.1 Bluetooth Radios

There are 3 different Bluetooth radios. The default radio is the Basic Rate Radio (BR/EDR) which is the most used radio. And in the recent years the Low Energy Radio(LE) was added. Bluetooth also uses a 802.11 radio, to feature the Bluetooth High Speed technology. This radio needs to be combined to a BR/EDR radio in its usage.

1.2 Bluetooth Stack



The stack is primary divided into a Controller part and a Host part. The Controller comprehends the Bluetooth Radio, Baseband and the Link Manager Protocol. It is done in hardware for obvious reasons. Host deals with high level data, and is usually built in software. Between the Host and the Controller there is an Host/Controller Interface, but some implementations may not implement this interface and just bypass everything directly to the Link Manager Protocol by implementing the whole stack on the chip.

2 Pairing

The Pairing procedure is the process of establish a secure connection between two Bluetooth devices. The pairing process is always done at the first connection attempt between two devices and enables the security requirements requested and/or supported by each connecting device.

In this procedure devices basically generate and exchange their link keys and stores them, so in further connections they don't need to do everything again so reconnection (or even auto-reconnection when devices are near each other) happens without user interaction. When devices are paired they are said to be "Paired" or "Bonded".

The Pairing Procedure:

- First Connection
  1. > HCI_Pin_Code_Request
  2. < HCI_Pin_Code_Request_Reply
  3. > HCI_Link_Key_Notification
- Further Connections
  1. > HCI_Link_Key_Request
  2. < HCI_Link_Key_Request_Reply

We can see the PIN Code Request at the first connection and the request the Link Key for further connections.

Devices must store the link key received in the Host, to prevent the use of the link with a different host, this can happen in removable Controllers, like Bluetooth dongles if we plug it in another Host.

There are some different ways to run the Pairing procedure that depends on the type of the radio, the version of the specification the device implements and the input/output capabilities. First it will be described the Legacy Pairing, then Secure Simple Pairing. Then we change radios and talk about Pairing in Low Energy and High Speed technologies.

2.1 Legacy pairing, the old way

Bluetooth devices that implements the Bluetooth Core Specifications prior version 2.1 do pairing through what we call "Legacy Pairing" today. Legacy Pairing was built for devices that have limited resources and can't do a lot of processing to generate keys and encrypt the Bluetooth link.

Legacy pairing uses the SAFER+(Massey et al 1998) for key derivation and E0 stream cipher for encrypt. The authentication key are 128 bits long and the secrets to generate them are 1-16 bytes long. These secrets are usually called PIN code. For Legacy Pairing all the encryption and key generation is done in the Controller.

Legacy Pairing has three different security modes:

- Security Mode 1: There is no security in this mode.
- Security Mode 2: It's also called Service Level Security. In this mode a Bluetooth link can be established without encryption and authentication but when a service require security all the security procedures needs to be done.
- Security Mode 3: It's the Device Level Security. The Bluetooth link needs to be encrypted at the moment of it creation. In this mode it is no allowed to run a Bluetooth link without encryption.

2.1.1 Issues with Legacy Pairing

The design of Legacy Pairing proved to be wrong and weak. Brute force for small PIN codes is not hard and the PIN code is usually fixed to 4 bytes, many devices uses 0000 or 1234, also the PIN is the only source of randomness for key generation. The E0 encryption cipher is weak, there is no expiration date for the link key, giving time for attacker derivate the key. And no protection against the man-in-the-middle attack.

2.2 Secure Simple Pairing (SSP)

Due to the many problems with Legacy Pairing a new Pairing scheme had to be introduced. The Secure Simple Pairing is specified by Bluetooth Core Spec v2.1 and is mandatory for any device that implements v2.1 or greater. However for compatibility reasons support for Legacy Pairing is also required. Encryption is still done in controller.

SSP was introduced to simplify and improve the Bluetooth Security, it uses Elliptic Curves Diffie-Hellman that provides passive eavesdropping protection. Also there is optional MITM protection. Even the simpler SSP Pairing Model (JustWorks Pairing) is more secure than Legacy Pairing.

Secure Simple Pairing is called Security Mode 4 but it doesn't have any tecnical relations with the Security Modes of Legacy Pairing.

SSP introduces the concept of IO Capabilities. It is a mechanism that takes in account the devices' Input and Output Capabilities and choose the Pairing Model based on these Capabilities.

2.3 Pairing Models

SSP uses four different Pairing Models: Numeric Comparison, Just Works, Passkey Entry and Out Of Band.

2.3.1 Numeric Comparison

It is designed for scenarios where both devices can display a six digit number and are capable of having the user enter "Yes" or "No". When pairing, a six number digit is displayed in both sides and the users have to compare them and reply "Yes" if they are equal or "No" otherwise. In this model there is protection against MITM. Knowing the six digit number gives no help in decrypting the encoded data.

2.3.2 Just Works

This model is ideal for situations where both devices doesn't have any input and output capabilities. It uses the same protocol as Numeric Comparison but it doesn't display any number to the user and doesn't ask for confirmation of these numbers. Doesn't offer protection against MITM.

2.3.3 Passkey Entry

Designed for scenarios where one device has a numeric keyboard but doesn't have a display and the other device has at least numeric output. In the pairing process the side with display shows a 6 digits number that have to be entered in the other side through its keyboard.

It is worth to note that Passkey Entry in fundamentally different from PIN code entry of Legacy Pairing. While in Legacy Pairing the PIN Code is the only source of randomness for the key generation, in the Passkey Entry the six digit number is just an artifact of the security algorithm and not a input to it. Knowing the six digit number gives no help in decrypting the encoded data. Passkey Entry protects against MITM.

2.3.4 Out Of Band

Out Of Band Pairing allow pairing over a different technology such as NFC [3]. With NFC Bluetooth Pairing the devices just need to be put together

and they will be paired. For its MITM protection Out Of Band Pairing relies on the protection against MITM of the Out Of Band mechanism used.

2.4 IO Capabilities

Choosing a Pairing Model depends on the devices' Input and Output capabilities. Let's first explain them and afterwards see how devices interact to choose the Pairing model to be used.

2.4.1 Input Capabilities

There are three possible input capabilities:

- No Input: When a device has no mechanism of input
- Yes/No: When the user can enter "Yes" or "No"
- Keyboard: When the user can enter a six digit number

2.4.2 Output Capabilities

There are two different output capabilities:

- No Output: When the device can't display a six digit number
- Numeric Output: When the device can display a six digit number

2.4.3 Mapping of Input / Output Capabilities to IO Capability

IO Capabilities can be mapped this way:

Local Output Capacity / Local Input Capacity	No Output	Numeric Output
No input	NoInputNoOutput	DisplayOnly
Yes / No	NoInputNoOutput	DisplayYesNo
Keyboard	KeyboardOnly	DisplayYesNo

This defines the devices regarding their input and output capabilities.

2.4.4 Choosing the Pairing Model

Now that we know the IO Capabilities we can use this info to choose the Paring Model between devices. Let's first define Initiator as the device that sends the pairing request and Responder as the device that receives the pairing request.

The next table shows how to choose the pairing mode and if devices are able to authenticate with each other. Authentication here basically means MITM protection and "Numeric Comparison with automatic confirmation on both devices" is the Just Works Pairing.

Initiator A / B Responder	**Display Only**	**DisplayYesNo**	**KeyboardOnly**	**NoInputNoOutput**
DisplayOnly	Numeric Comparison with automatic confirmation on both devices. Unauthenticated	Numeric Comparison with automatic confirmation on device B only. Unauthenticated	Passkey Entry: Responder Display, Initiator Input. Authenticated	Numeric Comparison with automatic confirmation on both devices. Unauthenticated
DisplayYesNo	Numeric Comparison with automatic confirmation on device A only. Unauthenticated	Numeric Comparison: Both Display, Both Confirm. Authenticated	Passkey Entry: Responder Display, Initiator Input. Authenticated	Numeric Comparison with automatic confirmation on device A only. Unauthenticated
Keyboard Only	Passkey Entry: Initiator Display, Responder Input. Authenticated	Passkey Entry: Initiator Display, Responder Input. Authenticated	Passkey Entry: Initiator and Responder Input. Authenticated	Numeric Comparison with automatic confirmation on both devices. Unauthenticated
NoInputNoOutput	Numeric Comparison with automatic confirmation on both devices. Unauthenticated	Numeric Comparison with automatic confirmation on device B only. Unauthenticated	Numeric Comparison with automatic confirmation on both devices. Unauthenticated	Numeric Comparison with automatic confirmation on both devices. Unauthenticated

3 Bluetooth High Speed

The Bluetooth Core Specification v3.0 introduces the optional High Speed feature. High Speed make uses of the 802.11 technology to increase Bluetooth transfer bandwidth. After the Bluetooth link is established in the default BR/EDR radio the data transfer can be moved to the 802.11 radio for a faster transfer. It's also called Alternate MAC/PHY(AMP).

3.1 Bluetooth High Speed Security

Due to the fact that the connection is first established in the BR/EDR radio High Speed relies on Secure Simple Pairing for its security. From the user point of view there is no difference from v2.1 radios.

To protect the data over the 802.11 link AMP uses 256 bits key generated from the BR/EDR link key.

4 Bluetooth Low Energy (LE)

Bluetooth Low Energy is specified by Bluetooth Core Specification v4.0 and introduces a new radio with reduced low power consumption. This radio can be used along with the default BR/EDR radio or alone, this defines a dual mode device or a single mode device respectively. To reduce power usage and cost Low Energy has very limited resources.

4.1 Bluetooth Low Energy Security

Due to its very limited resources the encryption through Elliptic Curves Diffie-Hellman could not be used here, thus passive eavesdropping protection is not present in LE. LE uses AES-CCM[4] that is also used in Wireless LAN. The encryption is still in the Controller but the key generation is in the Host, this way the algorithm for key generation can be changed without change the hardware.

It uses a similar IO Capabilities mechanism with the exception that Numeric Comparison is not available. The decision of which Pairing Model to use is similar to Secure Simple Pairing on BR/EDR. But the have a lot of difference on the quality of the security provided. Neither JustWorks or Passkey Entry Pairing provide protection against passive eavesdropping.

Bluetooth Low Energy introduces a Privacy feature where devices can hide they real address and uses random bluetooth address that changes after a period of time. Thus the privacy is guaranteed by not revealing the real

address. There is two different type of random address. One that is not resolvable, i.e., the peer will never discover the real address of device and one that is resolvable, in this type the peer can derivate the real address using the random address and the link key of the connection.

5 Credits

- The New Security Model Of Bluetooth, Marcel Holtmann, 2007.
  http://www.securitytube.net/video/1974
- Linux Bluetooth Developers
- Bluetooth Core Specification v4.0.
  https://www.bluetooth.org/docman/handlers/do wnloaddoc.ashx?doc_id=229737

References

[1] http://en.wikipedia.org/wiki/Bluetooth_profile

[2] http://bluetooth.org

[3] http://en.wikipedia.org/wiki/Near_field_communication

[4] http://en.wikipedia.org/wiki/CCMP