CHAPTER 3
BLUE TOOTH SECURITY FEATURES

3.1. Prologue

Security issues have played a major role in the invention of Bluetooth Technology [82][131][132][133][134][135][139]. The Bluetooth SIG has put too much dedicated effort to make a Bluetooth a Secure Technology[23]. Different kinds of Security measures have been designed and implemented at different protocol phases but however basic Bluetooth security configuration dependent on the user’s Bluetooth Device who predicts about the discoverability and connection options [23][119]. In general Bluetooth discoverability and connection options are broadly categorized into three types such as[139]:

i. Silent: In this option the device does not accept any connections. Simply it tries to monitor the Bluetooth traffic[23].

ii. Private: In this option also the device cannot be discovered[139]. A Bluetooth address is represented by a 48-bit BD_ADDR is usually a normal unique address which always points to globally only one unique address[23][119].

iii. Public: In this option the device can be discovered and connected to. It is therefore called a discoverable device[23][119].

The Bluetooth Security Supports for three main steps such as

i. Authentication [23][119]

ii. Authorization [23]

iii. Optional Encryption [23][119]

In this chapter the various issues of Bluetooth security are addressed. The most technical aspects of security features of Bluetooth are defined for some time[82]. The Bluetooth core specification v3.0 which introduces the optional high speed feature. The high speed makes use of 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 [23][119]. As we already learnt Bluetooth is a radio frequency technology which operates in the unlicensed 2.4 GHz ISM band [139]. It was mainly designed by Ericsson as a substitute for RS-232 data cable and is mainly intended for short distance data
swapping usually 10 meters[82]. Bluetooth is also specified by the Bluetooth Special Interest Group (BSIG) from a collection of companies such as Intel, Nokia, Microsoft, Motorola, Ericsson, Toshiba and Lenovo. It was designed to be low power and low cost Bluetooth chips price few dollars and are very popular in instruments over the world. As we know that a new specification for a real low power radio which enables a device with a Bluetooth low energy radio to live a year without updating its battery[23][119]. The security is based in a link key exchange at the first connection between two devices. This technology is known as Bluetooth Pairing[139]. The Bluetooth pairing procedure is the mechanism of establishing a secure connection between two Bluetooth devices[23][119]. 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[139]. In this mechanism the Bluetooth instruments basically create and swap their link keys and stores them, so in further connections they don’t need to do everything again so reconnection happens without user interaction. When devices are paired they are said to be paired or bonded. The pairing mechanism is as follows [131][132][133][134].

i. First Connection

1) Host Controller Interface_PIN_Code_Beseech,
2) Host Controller Interface_PIN_Code_Supplicate_Riposte,
3) Host Controller Interface_Link_Key_Divulgence.

ii. Further Connections

1) Host Controller Interface_Link_Key_Supplicate,
2) Host Controller Interface_Link_Keyimplode_Rejoinder.

It is also possible to scan the PIN Number Rejoinder 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. Which can happen in removable controllers such as Bluetooth dongles if we plug it in another host[23][119]. There are some different techniques to run the pairing procedure which depends on kind of radio, the version of the specification the instrument 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. Bluetooth instruments implements the Bluetooth Core
Specifications prior version 2.1 do pairing through legacy pairing today. Legacy pairing was built for instruments which have limited resources and cannot do a lot of processing to create keys and encrypt the bluetooth link. Legacy pairing which uses SAFER+ for key derivation and E0 stream cipher encrypt. The authentication keys are 128 bits long and the secret to generate them are 1-16 bytes long. These secrets are usually called PIN code[23][119].

3.2. Legacy Pairing

In Legacy Pairing mechanism the entire encryption process and key generation is performed in the controller component. Legacy pairing operates in three different security modes which are also termed as,

i. **Security mode-1**: As already we know that Security mode-1 cannot provide any security[25].

ii. **Security mode-2**(*Service Level Security*): In this mode Bluetooth link can be established without encryption and authentication but when a service require security all the security procedures needs to be done[24][25].

iii. **Security mode-3**(*Device level security*): The Bluetooth needs to be encrypted at the moment of its creation. In this mode it is not allowed to run a Bluetooth link without encryption[23][25].

3.3. Various issues with Legacy Pairing

The design of legacy pairing is shown to be wrong and weak. Brute force for small PIN codes is not hard and the pin code is usually allocated to 4 bytes and many devices uses 0000 or 1234 and also pin is the only source of randomness for key generation. To the best of our knowledge and wisdom the E0 encryption cipher acts very weak. The link does not have any expiration date giving time for attacker the derivative key is small. There is no protection against the man in the middle attack[23][25][119].

3.4. Secure Simple Pairing (SSP)

Due to many problems with legacy pairing a new pairing scheme to be introduced[23][24][25]. The secure simple pairing is represented by Bluetooth Core Spec v2.1 and is compulsory requirement for any device which implements v2.1 or greater. However for compatibility reasons support for legacy pairing is also necessary. Encryption is also done in controller. Secure Simple Pairing was
introduced to simplify and improve Bluetooth security which uses elliptic curves Diffie Hellman which provides passive eavesdropping protection[119]. Also there is optional MITM protection. Even the simpler SSP Pairing model is more secure than legacy pairing. Secure Simple Pairing is also called as Security mode 4 but it does not have any technical relations with the security modes of legacy pairing. The SSP introduces the IO capabilities. It is a mechanism which takes in account the devices input and output capabilities and choose the pairing model based on these capabilities[23][24][25].

3.5. Categories of Pairing models

The pairing models are broadly divided into four Numeric comparison, Just works, Passkey entry and Out of band[26].

3.5.1. 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 digit number 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. By knowing the six digit number gives help in decrypting the encoded data[119].

3.5.2. Just Works:

This model is suitable for situations where both devices does not have any input and output capabilities. Just works uses the same protocol as similar to the numeric comparison but it does not display any number to the user and does not ask for confirmation of these numbers. It also does not offer protection against MITM[119][23][24][25][26].

3.5.3. Passkey entry:

This one is 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 six digit number which has to be entered in the other side through its keyboard. It is worth to note that Passkey entry is fundamentally different from PIN code entry of legacy pairing. While in legacy pairing the PIN code is the only source of randomness for a key creation. As we know that in the Passkey entry the six digit number is just an artifact of the security
algorithm and not an input to it. The passkey entry is one which protects against
MITM[119].

3.5.4. Out of Band:

Out of Band pairing allows pairing over a different technology like NFC. By
using NFC Bluetooth pairing the devices just need to be put together and they will be
paired. In MITM protection out of band pairing relies on the protection against MITM
of the out of band technique used[119].

3.6. I/O (Input/ Output) capabilities

First of all choosing a secure pairing model for Bluetooth relies on the devices
input and output capabilities. In this research work we are first planning to explore all
the Input and Output Capabilities. The Input capabilities in Security concepts of
Bluetooth are partitioned into 3 kinds such as:

3.6.1. Input capabilities:

There are three possible input capabilities.

i. No input: When a device has no mechanism of input.

ii. Yes/No: When the user can enter Yes/No

iii. Keyboard: When the user can enter a six digit number[119].

3.6.2. Output Capabilities:

The output capabilities are broadly categorized into two types such as

i. No output: When the device cannot display a six digit number.

ii. Numeric output: When the device can display a six digit number[119].

3.7. Mapping of Input/Output capabilities to I/O capability

The I/O capabilities can be mapped in this way.

<table>
<thead>
<tr>
<th>Local Output Capacity</th>
<th>No Output</th>
<th>Numeric Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local input capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No input</td>
<td>No input No Output</td>
<td>Display Only</td>
</tr>
<tr>
<td>Yes/No</td>
<td>No input No Output</td>
<td>Display Yes No</td>
</tr>
<tr>
<td>Keyboard</td>
<td>Keyboard only</td>
<td>Display Yes/No</td>
</tr>
</tbody>
</table>
3.8. How to choose the Pairing model

We know that Input Output Capabilities can use this information to choose the pairing model between devices. Let's first define initiator as the device which sends the pairing request and responder as the device that receives the pairing request. The Table-2 shows how to choose pairing mode and if devices are able to authenticate with each other[131][132][133][134]. Here authentication means MITM protection and numeric comparison with automatic confirmation on both devices is the just works pairing[119].

**Table 2: Picking of pairing mode and how devices are able to authenticate**

<table>
<thead>
<tr>
<th></th>
<th>Display only</th>
<th>Display Yes No</th>
<th>Keyboard Only</th>
<th>No input</th>
<th>No output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display only</td>
<td>Numeric comparison with automatic confirmation on both the devices.</td>
<td>Numeric comparison with automatic confirmation on device B only.</td>
<td>Passkey entry: Responder display, initiator input.</td>
<td>Numeric comparison with automatic confirmation on both the devices.</td>
<td>Un authenticated.</td>
</tr>
<tr>
<td>Display Yes No</td>
<td>Numeric comparison with automatic confirmation on device A only.</td>
<td>Both display, Both confirm.</td>
<td>Passkey entry: Responder display, initiator input.</td>
<td>Numeric comparison with automatic confirmation on device A only.</td>
<td>Un authenticated.</td>
</tr>
</tbody>
</table>
3.9. How Bluetooth Supports for High Speed

Due to the connection created in the BR/EDR Radio High Speed is standing on Secure Simple Pairing (SSP) for its Security[131][132]. According to the user point of view there is no difference from v2.1 radios. In order to Protect data over the 802.11 Link the AMP cooperates 256 bits key created from the BR/EDR Link Key[37].

3.9.1. Low Energy in Bluetooth Security:

As we know that the Bluetooth is one which supports for limited resources, the encryption through Elliptic Curve Diffie Hellman is not possible to use here. Due to this genuine reason Passive eaves dropping protection is not available in LE[131]. The LE is one which is dependent on AES-CCM which is also used in Wireless LAN[131][132][133][134]. The encryption lies in controller but the Key-Generation is in the host. In this way algorithm for key generation can be updated without changing the Hardware[38]. Bluetooth Low energy introduces a Privacy feature where devices can protect the real address and it uses a random Bluetooth address which updates after a period of time. We are using two different types of random addresses. One i.e. not resolvable (Where Peer is not able to discover the real address of the device and one more address is not resolvable)[37].

3.9.2. Bluetooth Radios:

Bluetooth radios are broadly divided into three types, such as:

i. The default radio of Bluetooth is Basic Rate Radio (BR/EDR)[131][132][133][134]. BR/EDR is the most widely used radio in bluetooth technology.
ii. The second type of radio supported by bluetooth technology is Low Energy Radio (LER)[37][38].

iii. The third kind of radio supported by bluetooth technology is 802.11 radio which uses high speed technology [37][38][66].

3.9.3. Bluetooth Stack

The bluetooth stack is one of the important part of bluetooth technology[23]. The bluetooth stack is mainly partitioned into a controller part and a host part. The controller part consists of bluetooth radio, baseband and the link manager protocol[119], which is done in hardware for obvious reasons. Host always handles High level data and it is usually implemented by software[131]. In between host and the controller there is a Host Controller Interface[37][38]. The different types of hardware devices does not implement host/controller interface and just forwards everything to the Link Manager Protocol (LMP) by implementing the whole stack on the chip[119][131].