Preventing the Man in the Middle Attack on a Bluetooth Connection Using BlueZ Software

Cameron Bertram, Moradeke Olumogba

Prof. Vincent Mooney

Vertically Integrated Projects

Secure Hardware

December 5, 2017

I. Background

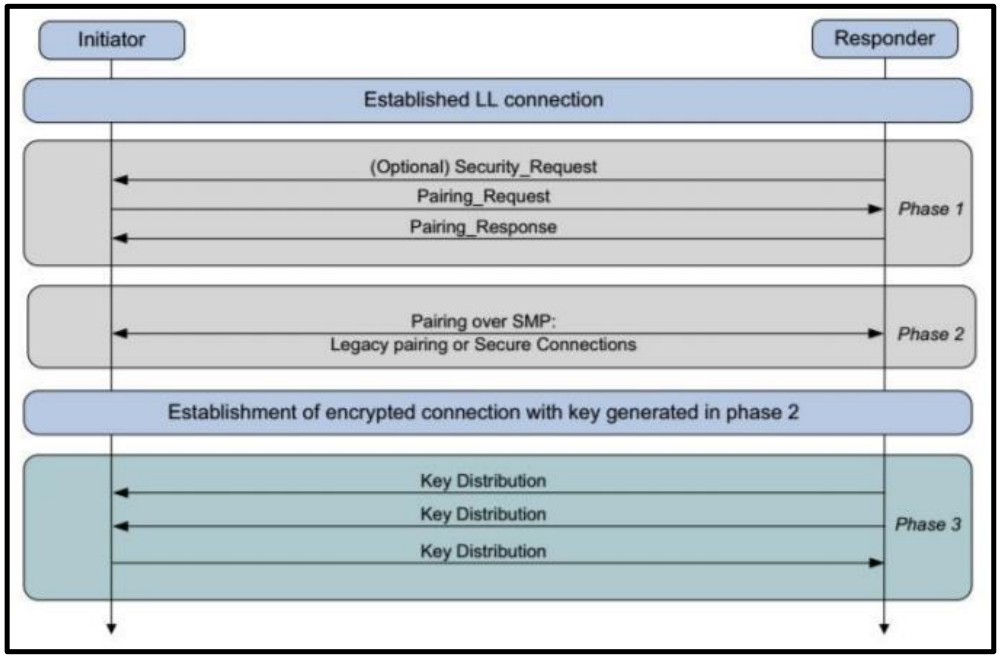
This group involves two of the same team members as that of Spring 2017 therefore rather than write a brand new report this semester we decided to update the previous one from the Spring.

A. Bluetooth Background

Bluetooth is a protocol for short range, wireless communication between two devices. It has become one of the most popular standards for wireless data transfer in the world due to its ease of use and very low energy cost. Bluetooth operates in the 2.4 GHz frequency of the industrial, scientific, and medical radio (ISM) band. This semester our team had access to a Pandora Bluetooth Nano Adapter that uses Bluetooth 4.0 or Bluetooth Low Energy. Bluetooth 4.0 is currently the most common version of Bluetooth. As such, this paper's description of Bluetooth will only pertain to Bluetooth 4.0. The most important processes of Bluetooth that pertain to security are the steps that two devices go through to pair with each other.

1. Discovery/Inquiry Phase

The first phase that any two Bluetooth devices go through before they begin the pairing process is the discovery phase [10]. In this phase, the two devices become aware of each other's presence and learn the basic services they offer to the user. Any active Bluetooth device is broadcasting a General Inquiry Access Code (GIAC) that contains the Bluetooth address of the sender as well as some basic information about the services the device offers. When another device receives a GIAC, it uses the Bluetooth address to send its own GIAC to the inquiring device.



V. Results

A. User-defined link key

The link key was manually written into the file ‘linkkeys’. The syntax is <bluetooth address> <32-hexadecimal digit link key> <channel> … The bluetooth address refers to the other device paired with the computer. The syntax was discerned by comparing it with the manual for ‘rfcomm’. As the bluetooth address and channel is like that in rfcomm man and a 32-bit link was expected as read in bluetooth documentations were able to understand the syntax.

```
config   eir  lastseen  linkkeys  names          sdp
[molumogba3@ivy 00:1A:7D:DA:71:02]$ more linkkeys
28:18:78:43:4E:9C 098A3BCA38B7CDE16D013D8FE2097057 5 -1
[molumogba3@ivy 00:1A:7D:DA:71:02]$
```

A screenshot from the computer was sent via bluetooth and it successfully transferred to the other device.