BLUETOOTH Secure Simple Pairing

The Bluetooth Secure Simple Pairing feature in the 2.1+EDR Specification will help Bluetooth be adopted in newer domains, which require more security than the legacy Bluetooth could have provided.

By Anindya Bakshi, MindTree Consulting

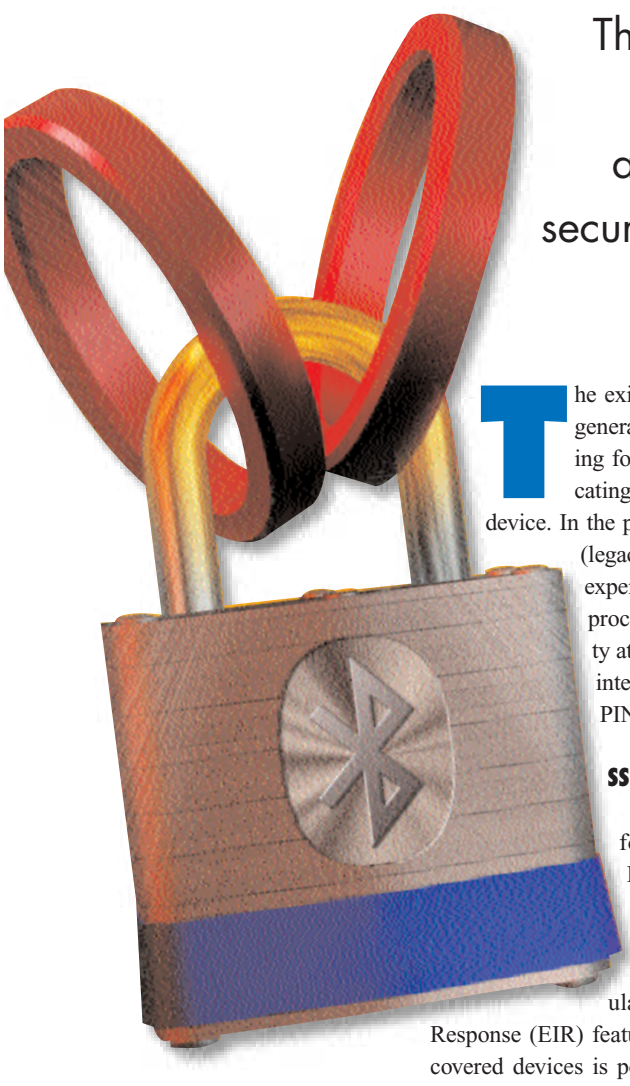

Illustration by Bill Yermal

The existing method of pairing Bluetooth devices generally consists of several steps, such as searching for the device, connecting to it and authenticating the device to make sure it is the correct device. In the pre- 2.1+EDR compliant Bluetooth devices (legacy devices), in order to simplify the user experience, the products used an authentication procedure, which is vulnerable to simple security attacks. Bluetooth devices with minimal user interfaces, most of the time, relied on a fixed PIN (shared secret), causing security concerns.

SSP vs. Legacy Bluetooth Pairing

Secure simple pairing (SSP) achieves the following advantages over the legacy Bluetooth pairing:

- It reduces the number of steps with minimal or no user action. The user will have a smaller set of devices to access a particular service. With the Extended Inquiry Response (EIR) feature of 2.1+EDR, efficient filtering of discovered devices is possible based on the service class UUIDs present in the response, compared to the legacy Class of Device (CoD) based filtering. Apart from that, using EIR the "Friendly Name" of the peer device can be received. This eliminates the need of paging the device to perform Remote Name Request, and in the process, reduces the overall connection time.

During the pairing phase, the user does not need to remember a PIN key. In Secure Simple Pairing, a user has to perform one of following three things to perform pairing:

1. Select "yes" or "no"
2. Compare six digit numbers displayed in both the devices and answer with "yes" or "no"
3. Enter a six digit number from an input only capable device, when the other device has display capability

- Improved the Bluetooth security without additional user overhead:

Secure Simple Pairing protects against passive eavesdropping and also against man-in-the-middle (MITM) attacks. SSP uses Elliptic Curve Diffie Hellman (ECDH) public key cryptography to protect against passive eavesdropping attacks.

In MITM attacks, the attacking device relays information between the two devices creating the illusion that those two devices are connected to each other. In this attack, the information exchanged between those two devices is compromised to the attacker. Secure Simple Pairing provides two methods: numerical comparison and passkey entry to protect Bluetooth devices against MITM attack.

Association Models

Secure Simple Pairing defines the following association models based on the Input/Output (I/O) capabilities of the two devices:

- Numeric Comparison: designed to be used when both devices are capable of displaying a six-digit number and user input of "yes" or "no". A typical example could be two cell phones pairing with each other. The six-digit number displayed in this model is an output of the underlying security algorithm.
- Just Works: designed to be used when at least one of the devices does not have display capability of six digits and also is not capable of entering six decimal digits using a keyboard or any other means. This model does not provide protection against MITM attacks. Compared to the legacy headsets with a fixed PIN, the security level provided by this model is much higher.
- Out of Band: designed for devices capable of using Out of Band (OOB) mechanisms to exchange secretes to be used in the pairing process. Near Field Communication (NFC) to exchange the cryptographic information by touching two devices is an example.
- Passkey Entry: designed to be used when one of the devices does not have display capability of six digits, but has the input capability and the other device has output capability. PC and

keyboard is a typical example of this model. The user is shown a six-digit number and then asked to enter from the device with only input capability.

In the Bluetooth 2.1+EDR specification, a new security mode 4 is defined for the Secure Simple pairing. Usage of Security mode 1 (no security) and Security mode 3 (link level security) are excluded from the specification for 2.1+EDR devices. Usage of Security mode 4 is mandatory for all 2.1+EDR compliant devices, with only one exception. In the case when the remote legacy device does not support Secure Simple Pairing, Security mode 2 is to be used.

Secure Simple Pairing Process

Let us look into the Secure Simple Pairing process, with an example of Bluetooth SIM Access Profile (SAP), which has strict security requirements.

- *Device discovery*: The SAP Client will start Bluetooth Device discovery to find devices which support SAP Server role. Bluetooth Device Address (BD_ADDR) is the minimum requirement for that and which can be received using Bluetooth Inquiry (with or without EIR tags). With EIR tag, the SAP Client will be able to better filter the possible SAP Server devices by looking for the SIM Access UUIDs in the service class UUIDs received with the EIR tag. Apart from that, the name of the devices can also be received over EIR, which will help the user easily identify the known SAP server.
- *Connection establishment*: The user on the SAP Client end will select one of the device possible SAP Server to connect with and perform Bluetooth Service Discovery to be absolutely sure that the peer device really supports SAP Server and to retrieve the RFCOMM Server Channel required to establish SAP connection. The host application needs to initiate the authentication procedure before any L2CAP Channel establishment, with the exception of SDP. After the SDP query, once the SAP Client finds the peer device supports SAP Server, SAP server needs to initiate authentication before initiating L2CAP Channel establishment procedure for RFCOMM. If the SAP server receives an L2CAP connection request for RFCOMM, without the link being authenticated and encrypted, the request will be rejected.
- *IO capability and public key exchange:* After the connection establishment, if both the devices support SSP, they will exchange the IO capabilities, followed by exchange of public keys. Based on the IO capabilities, the association model will be decided.

Using HCI_Write_Simple_Pairing_mode command, the host has to enable the Simple Pairing Mode, which is done before making the 2.1+EDR devices connectable or before initiating connection with another device. Simple pairing is started by calling the HCI_Authentication_Requested command. The simple pairing process causes the IO Capability Request event being generated and Host to respond to this event with HCI_IO_Capability_Request_Reply command. IO Capability Response event finally indicates the IO capability and Authentication Requirement of the remote device to the host.

Authentication Stages

•*Authentication Stage 1*: This stage varies slightly for numeric comparison, OOB and passkey entry. Let us assume, that based on the IO Capability of both the devices, one side displays a six digit number for the other device to enter. After this stage the Authentication Stage 2 starts.

• Authentication Stage 2: At this stage, the results of the cryptographic functions are compared and if it is successful, the host receives Simple Pair Complete event and then the link key computation starts.

- *Link key calculation*: At this stage, a Link Key is calculated and mutual authentication is performed to make sure both the devices have the same link key. Similar to the legacy implementation, Link Key Notification event is generated on both the initiator and responder of the Simple pairing procedure. On the initiator end, HCI_Authentication_Complete event is generated at the end of this phase.
- *Enable Encryption*: The encryption phase is the same as the legacy implementation. The link level encryption can be enabled using HCI_Set_Connection_Encryption command. Once the link is encrypted, the SAP Client will start the L2CAP Channel establishment procedure for RFCOMM. Finally, SAP connection will be made over the RFCOMM Channel.

Another user senario could be that a link is authenticated without MITM protection. Now between the same pair of devices, a SAP connection is attempted, which will initiate authentication with MITM protection before initiating SAP connection.

Conclusion

The Bluetooth Secure Simple Pairing feature in the 2.1+EDR Specification will help in wider adaptation of Bluetooth because of the simplified user experience. The increased security level will help Bluetooth be adopted in newer domains, which require more security than the legacy Bluetooth could have provided.

WDD

About the Author

Anindya Bakshi is a senior technical member within the R&D group of MindTree Consulting, a global IT and R&D Services company co-headquartered in the U.S. and India. His core expertise areas include wireless systems design and architecture, implementation of communication protocols, and string processing algorithms. Currently, he is a member of Bluetooth Core Specification Working Group. He can be reach at b_anindya@mindtree.com.