November 2021

Sharing Bluetooth Accessories

Himanshu Rawat

Sharing Bluetooth Accessories

Abstract:

This publication describes methods of generating bonding information for connecting with a Bluetooth accessory and sharing the bonding information with another Bluetooth device to enable the other Bluetooth device to autonomously connect, pair, and bond with the Bluetooth accessory. In aspects, the methods include the generation of user keys, the generation of the shared secret, establishing ownership of the Bluetooth accessory, sharing ownership of the Bluetooth accessory, sharing usage of the Bluetooth accessory, and management of users/owners of the Bluetooth accessory.

Keywords:

Bluetooth, shared secret, user key, owner key, secret key, link key, bonding information, authentication data, shared random value, Bluetooth device, pair, ownership, sharing, connectivity, Bluetooth device address

Background:

Some types of Bluetooth accessories are frequently shared within a household. For example, a wireless speaker may be shared by multiple users of a household who have each individually paired their Bluetooth-enabled smartphones with the wireless speaker. Traditional Bluetooth pairing processes may present challenges to some users. For example, a person who lacks the technological skills necessary to understand and execute Bluetooth pairing instructions may struggle with understanding how to connect to and pair with the accessory. In addition, a person may have lost the user manual containing instructions for pairing with the accessory.

Description:

This publication describes methods of generating bonding information for connecting with a Bluetooth accessory and sharing the bonding information with another Bluetooth device to enable the other Bluetooth device to autonomously connect, pair, and bond with the Bluetooth accessory. The bonding information is used for generating the shared secret for Bluetooth pairing. Fig. 1, below, is an environmental view that illustrates a first Bluetooth device (a smartphone), a second Bluetooth device (a tablet computer), and a Bluetooth accessory (a wireless speaker) that may implement one or more of the methods described herein.

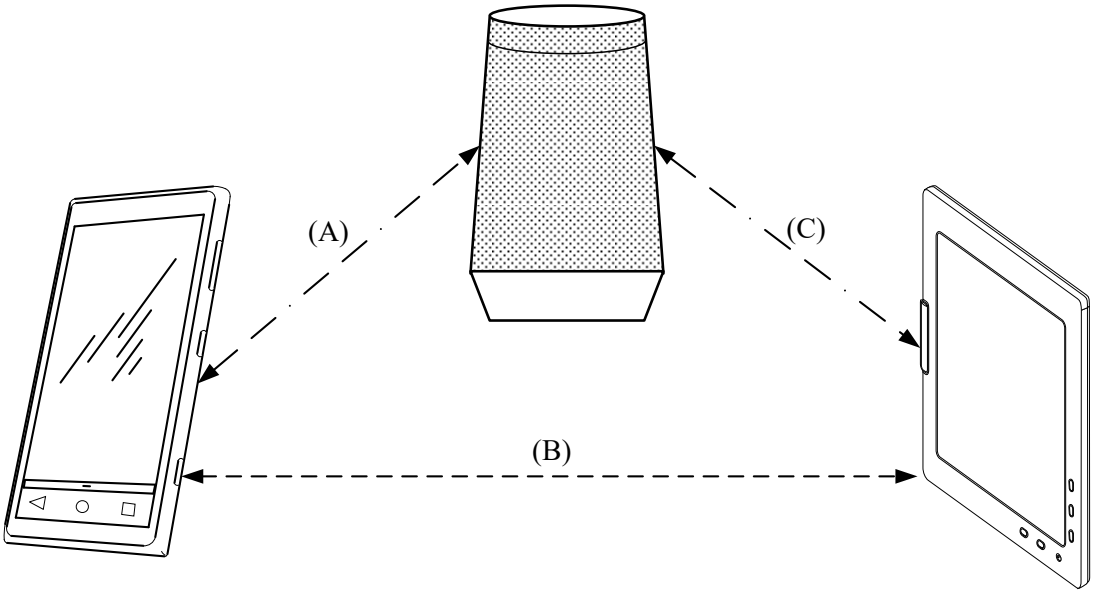

Fig. 1

In the example of Fig. 1, the first Bluetooth device establishes a Bluetooth connection (A) and pairs with the Bluetooth accessory. Later, the first Bluetooth device may share (B) bonding information with the second Bluetooth device for enabling the second Bluetooth device to autonomously connect, pair, and bond (through a second Bluetooth connection (C)) with the Bluetooth accessory.

Establishing Bluetooth Connection (A)

Through a standard Bluetooth pairing process, the first Bluetooth device and the Bluetooth accessory establish an initial wireless protocol link, connect, pair, and bond. Through the pairing process, a link key (encryption key) is generated by the first Bluetooth device and the Bluetooth accessory.

Taking Ownership of the Bluetooth Accessory

When a Bluetooth accessory and the first Bluetooth device are paired for the first time, the first Bluetooth device can take ownership of the Bluetooth accessory by configuring an Ownership service on the Bluetooth accessory. In an example, the first Bluetooth device generates a unique owner key and shares it with the Bluetooth accessory, which subsequently stores the owner key. Through this process, the owner key is set, thereby establishing ownership of the Bluetooth accessory by the first Bluetooth device. The first Bluetooth device stores the identity information (e.g., the Bluetooth device address) of the Bluetooth accessory and also stores the owner key. After the initial pairing, the first Bluetooth device can configure a pairing model on the Bluetooth accessory. For example, the first Bluetooth device can configure the Bluetooth accessory to only pair with Bluetooth devices in the future using an out-of-band (OOB) pairing method or Passkey entry.

Sharing Ownership and Use

The first Bluetooth device shares bonding information with the second Bluetooth device. If the owner of the first Bluetooth device desires to share the ownership of the Bluetooth accessory with a second Bluetooth device, then the owner key can be included in the bonding information

shared by the first Bluetooth device with the second Bluetooth device. The bonding information shared by the first Bluetooth device with the second Bluetooth device also includes the identity information of the Bluetooth accessory.

A Bluetooth device with ownership over a Bluetooth accessory may share the owner key or a user key with one or more additional Bluetooth devices. For example, a second Bluetooth device with ownership privileges over the Bluetooth accessory may grant a third Bluetooth device ownership privileges over the Bluetooth accessory by sharing the owner key with the third Bluetooth device.

If the owner of the first Bluetooth device only desires sharing the use of the Bluetooth accessory with a second Bluetooth device, then the owner key will not be included within the bonding information provided to the second Bluetooth device. In such an instance, the first Bluetooth device shares bonding information with the second Bluetooth device, which includes the identity information of the Bluetooth accessory, and the user key.

Generator Functions

A generator function (e.g., a user key generator function, a shared secret generator function) is used to generate one or more elements of the bonding information that are used for generating the shared secret for pairing.

User Key Generator Function

Fig. 2, below, illustrates a user key generator function implemented on a Bluetooth device. The function may be implemented on the first Bluetooth device and used to generate a user key for the second Bluetooth device. The function utilizes the owner key generated by the first

Bluetooth device and the device address (e.g., identity information, Bluetooth device address) of the second Bluetooth device to generate a user key for the second Bluetooth device. The device address can be determined by the first Bluetooth device or can be received by the first Bluetooth device from the second Bluetooth device. The first Bluetooth device can then share the user key with the second Bluetooth device as bonding information. The second Bluetooth device stores the bonding information for use in connecting with the Bluetooth accessory.

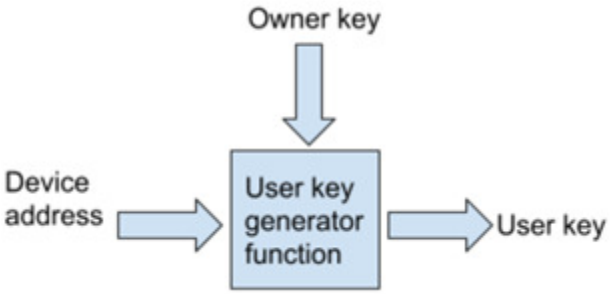

Fig. 2

The user key generator function may also be implemented on the Bluetooth accessory. Upon the second Bluetooth device initiating a Bluetooth connection with the Bluetooth accessory, as described below, the Bluetooth accessory can apply the device address of the second Bluetooth device and the owner key in the function to generate a user key for the second Bluetooth device. The generated user key can then be utilized by the Bluetooth accessory in generating the shared secret, as discussed below.

The user key generator function may also be implemented on the second Bluetooth device, for example, where ownership of the Bluetooth accessory was shared with the second Bluetooth device. In this example, the second Bluetooth device implements the function, along with the owner key received from the first Bluetooth device and the device address of the second Bluetooth device to generate the user key. The user key is then used by the second Bluetooth device to generate the shared secret, as discussed below.

Shared Secret Generator Function

For the second Bluetooth device to automatically connect, pair, and bond with the Bluetooth accessory, both the second Bluetooth device and the Bluetooth accessory need to possess and/or generate the relevant bonding information. For example, the second Bluetooth device and the Bluetooth accessory both need to be able to generate an identical shared secret that is utilized in the Bluetooth pairing process. The shared secret can be used as a passkey value or as out-of-band data, depending on the Bluetooth pairing method performed.

When the second Bluetooth device, performing a Bluetooth scanning process searching for the device address of the Bluetooth accessory included in the bonding information, locates the Bluetooth accessory it will initiate a Bluetooth connection with the Bluetooth accessory. Fig. 3, below, illustrates a shared secret generator function implemented on a Bluetooth device. The function is implemented by the second Bluetooth device and the Bluetooth accessory to generate the shared secret that is used in the Bluetooth pairing process.

The second Bluetooth device and the Bluetooth accessory each utilize the shared secret generator function with the user key and a shared random value to generate an identical shared secret. The shared secret is then used in the Bluetooth pairing process to pair the second Bluetooth device and the Bluetooth accessory. The shared random value includes connection specific information to ensure that a different shared secret is generated for pairing between the Bluetooth accessory and a Bluetooth device. The shared random value provides an additional layer of protection against repetition attacks. The Bluetooth accessory may generate a new shared random value when a connection occurs.

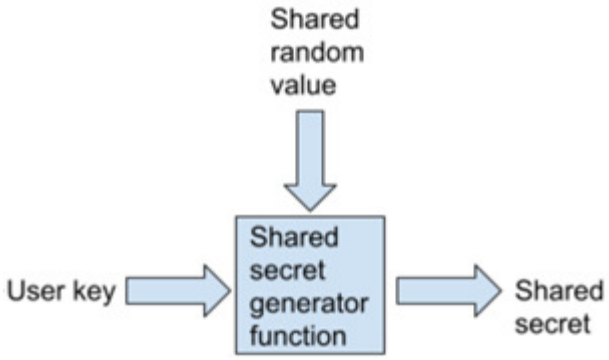

Fig. 3

In an example of the Bluetooth pairing process between the second Bluetooth device and the Bluetooth accessory, the second Bluetooth device performs a Bluetooth scanning process to find the Bluetooth accessory at a known address (e.g., the stored Bluetooth address of the Bluetooth accessory received in the bonding information from the first Bluetooth device). The second Bluetooth device then initiates a Bluetooth connection process with the Bluetooth accessory.

The second Bluetooth device either generates the user key (if an owner, using the user key generator function) or uses a stored user key provided by the first Bluetooth device. The user key is used to generate the shared secret via the shared secret generator function. The Bluetooth accessory, as described above, also generates the shared secret that is utilized by the user key generator function and the shared secret generator function. Upon both devices generating the shared secret, the second Bluetooth device and the Bluetooth accessory pair through an OOB pairing method.

Removing Users/Owners

Access to the Bluetooth accessory may be managed through a device policy manager implemented on the Bluetooth accessory. The device policy manager may register and store information regarding the owner device and the device policy manager can be used to alter user

restrictions and permission policies on the Bluetooth accessory. For example, to restrict access and/or use of the Bluetooth accessory. The device policy manager can be further used to set, change, or clear (collectively "modify") the owner key, thereby removing ownership privileges for other Bluetooth devices. Modifying an owner key invalidates the previous, original owner key, causing Bluetooth devices storing the original owner key to lose ownership and/or user access to the Bluetooth accessory. A Bluetooth device with the new owner key can generate and share the new owner key with additional Bluetooth devices, as described above.

References:

[1] Patent Publication: US20190260660A1. Uniform Communication Protocols for Communication Between Controllers and Accessories. Priority Date: February 5, 2014.

[2] Patent Publication: US20200008035A1. Cloud-based Proximity Pairing and Switching for Peer-to-Peer Devices. Priority Date: June 5, 2015.

[3] "Bluetooth Pairing Part 5: Legacy Pairing – Out of Band," Bluetooth® Technology Website. Bluetooth.com, (April 7, 2017). https://www.bluetooth.com/blog/bluetooth-pairing-part-5-legacy-pairing-out-of-band/.

[4] "Enabling Bluetooth Out-Of-Band Pairing through NFC," Invia. (July 17, 2021). https://www.invia.fr/Pages/Tutorials/enabling-bluetooth-out-of-band-pairing-through-nfc.aspx.

[5] "Google Fast Pair Service," Google Developers. (Updated June 07, 2021). https://developers.google.com/nearby/fast-pair/spec.