September 2021

Pairing Bluetooth Devices via QR Code

Martin Brabham

Myles Watson

Pairing Bluetooth Devices via QR Code

Abstract:

The out-of-band pairing of Bluetooth devices utilizing a quick response code provides a novel method for pairing Bluetooth devices. Pairing two devices over Bluetooth can be challenging for a user and presents security issues. The utilization of out-of-band Bluetooth pairing via a quick response code overcomes security problems presented by in-band pairing and does not require internet connectivity or an established server infrastructure to accomplish the Bluetooth pairing, providing a user-friendly experience over traditional pairing techniques.

Keywords:

Bluetooth, pairing, out-of-band (OOB) pairing, bonding, quick response (QR) code, Bluetooth Low Energy (BLE), Zigbee

Background:

Currently, pairing two devices over Bluetooth through in-band pairing or out-of-band (OOB) pairing can present challenges for a user attempting to pair the two devices. Multiple steps in the pairing process introduce opportunities for user error and add to the difficulty of pairing the devices. In addition, compromised Bluetooth pairing may present potential security risks to information transmitted between devices, as an intermediary may attempt to intercept data transmission between the devices or redirect the flow of data to a third-party device.

In some implementations, Bluetooth pairing may be performed using “Numeric Comparison,” which requires an advertising device to advertise that it is ready for pairing and a

scanning device to scan for the advertisement of the advertising device. Once the first device scans and detects the advertisement from the second device, the scanning device may establish a connection to the advertising device. Once a connection is established, both the advertising device and the scanning device will start checking for authentication data. If no authentication data is found, then both devices will ask the user to manually select "pair" through a user interface displayed as a dialog. Thereafter, each device must supply input to proceed and maintain the pairing.

In other implementations, Bluetooth pairing may be performed through a "non-bonded" generic attribute profile (GATT) connection. For example, the "non-bonded" generic attribute profile connection method may include sending data encrypted with a pre-shared advanced encryption standard (AES) cipher block chain (CBC) passphrase and initialization vector (IV) such that a first device can encrypt using the CBC passphrase and initialization vector (e.g., "12345678901234567") and a second device may decrypt using the same passphrase and IV. The added step of encryption and decryption requires the devices to access a server outside of the application.

Description:

Users of Bluetooth-capable devices often have difficulty during the Bluetooth pairing process because predominant pairing techniques require too much user interaction, which frequently results in user error. Out-of-band pairing for Bluetooth devices via a quick response (QR) code requires less user interaction, simply requiring the user to direct a camera at the QR code, thereby simplifying the process for a more fluid and easier user experience. The QR code contains the necessary instructions for initiating pairing and maintaining a Bluetooth connection

across devices. User-initiated out-of-band pairing eliminates the requirement of a device to show the user a dialog for verification because the verification automatically occurs through a confirmation key contained in the QR code.

The user experience of out-of-band Bluetooth pairing using a QR code provides an advantage over traditional means of Bluetooth pairing. Traditional means for pairing require a first device to advertise that it is ready for pairing and a second device to scan for the advertisement of the first device. Once the second device scans and detects the advertisement from the first device, the second device may establish a connection to the first device. Once a connection is established, both the first device and the second device will start checking for authentication data. If no authentication data is found, then both devices will ask the user to manually select "pair" on a user interface dialog. Each device must supply input to proceed and maintain the pairing. Each of these steps in the traditional Numeric Comparison technique introduces opportunity for user error. In contrast, OOB pairing using a QR code does not require the user to input numbers to accomplish the pairing. Instead, the user views the QR code through a camera or other image viewing application on their computing device.

FIG. 1, below, illustrates an example computing device and elements of the computing device that support pairing Bluetooth devices via a QR code. While the computing device illustrated in FIG. 1 is a smartphone, other types of computing devices can also support the techniques and systems described in this publication.

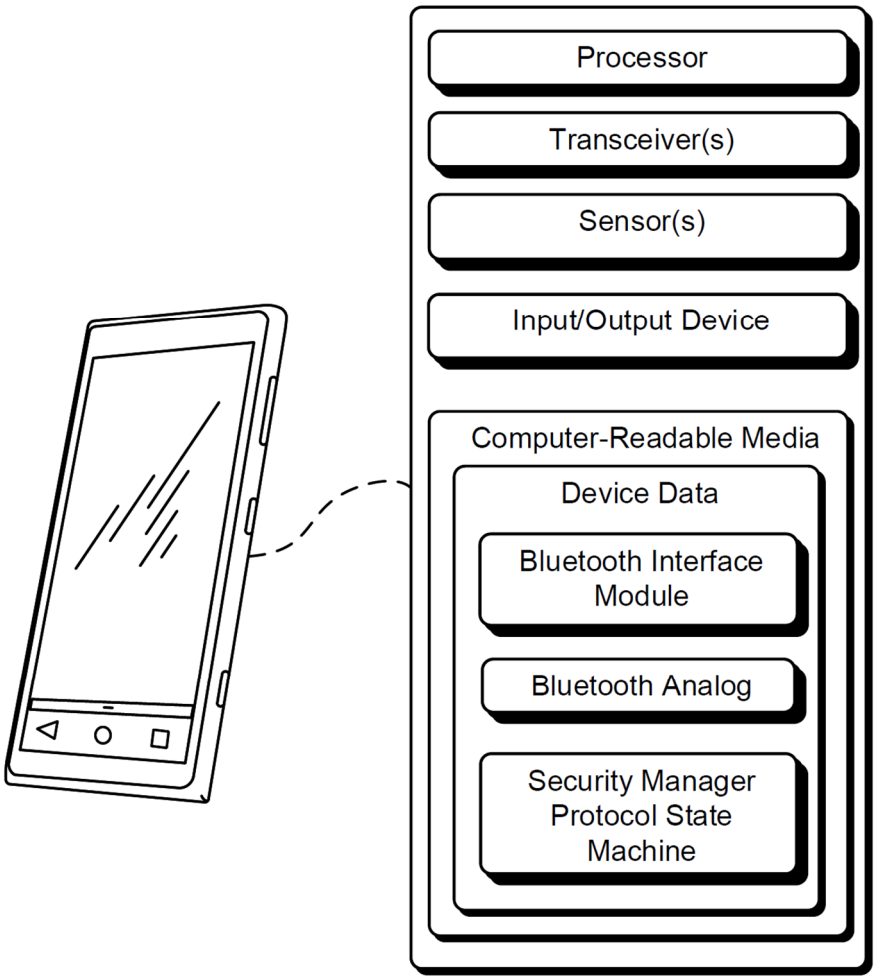

FIG. 1

The computing device includes a processor, transceiver(s), sensor(s) (e.g., camera sensor), and input/output device (e.g., a display). The computing device also includes a computer-readable medium (CRM). Device data (e.g., user data, applications, a Bluetooth Interface Module for interpreting QR code instructions, a Bluetooth Analog for converting digital instructions, a security manager protocol state machine for processing the instructions, and/or an operating system of the mobile device) is stored on the CRM. The device data may include instructions that, responsive to execution by the processor, cause the processor to perform operations to pair Bluetooth devices

via a QR code. In aspects, the operations include scanning a QR code, creating a connection between Bluetooth devices, generating a set of security keys, and exchanging OOB security keys so that pairing between the Bluetooth devices occurs. After Bluetooth pairing occurs, long-term keys may be saved to ensure faster pairing in the future between the same devices.

The computing device translates the associated Bluetooth pairing instructions in the QR code for the user and initiates the pairing. User-initiated out-of-band pairing eliminates the requirement of a device to show the user a dialog for verification because the verification has already happened with a confirmation key contained in the QR code. Out-of-band pairing for Bluetooth devices via a quick response code provides a novel method for pairing Bluetooth devices. FIG. 2, below, illustrates such a method.

In FIG. 2, first, a QR code is scanned using a camera or other similar hardware component of a computing device. The QR code may provide instructions for the transmission of data used to perform Bluetooth pairing between devices. A Bluetooth Interface Module on the computing device interprets the instructions from the QR code, and a Bluetooth Analog converts digital instructions for processing by a Security Manager Protocol State Machine. The QR code includes pairing initiation data which will prompt an indication at the user interface that a Bluetooth pairing process has been initiated. The OOB QR code contains the necessary instructions to create temporary “Diffie-Hellman” security keys during pairing. Pairing, as shown in FIG. 2, describes the exchange of temporary security features to establish a long-term bond. After a QR code containing the necessary instructions has been scanned, a bond may be created between the devices. Specifically, the pairing process utilizes out-of-band pairing, resulting in the two devices establishing a long-term key and allowing for bonding between the devices. The bond may be established once the connection has been encrypted for storage and use for the next time a

connection needs to be initiated. In other aspects, a barcode could be used for identifying a media access control (MAC) address of one or more of the Bluetooth devices instead of a QR code.

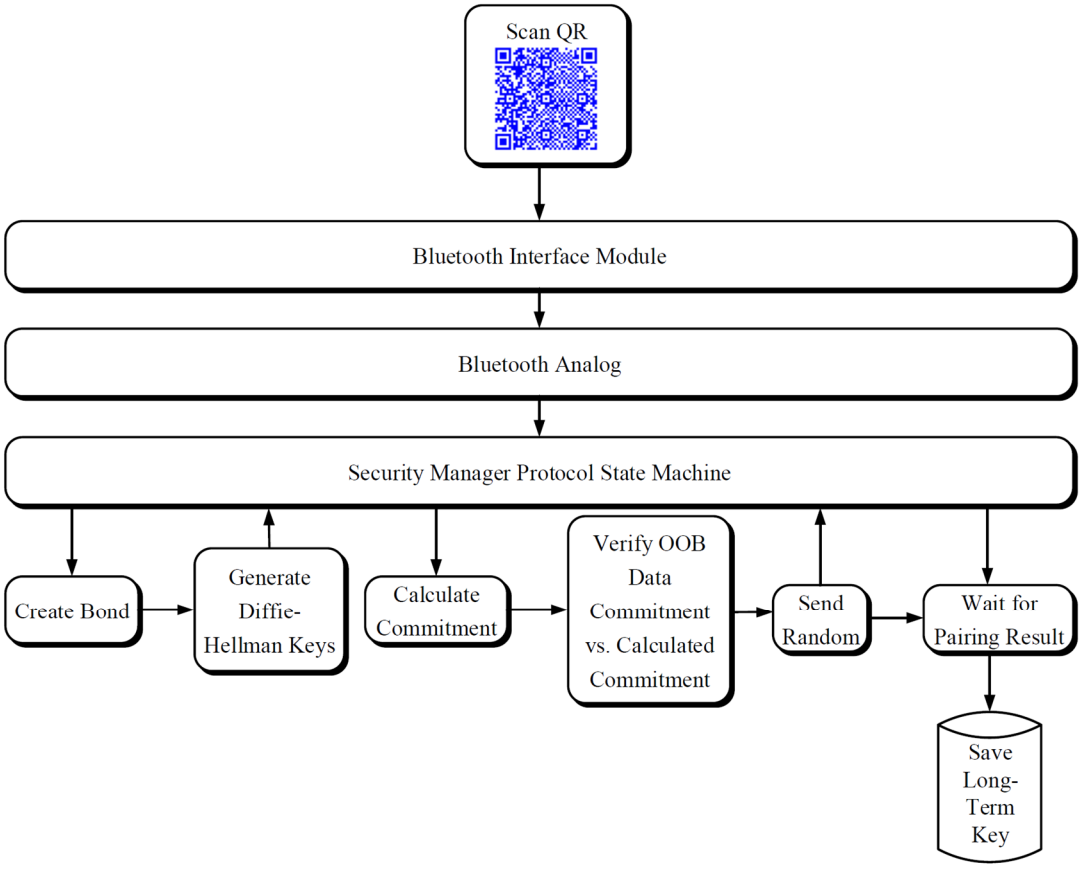

FIG. 2

The method of FIG. 2 includes saving any long-term keys (LTK) derived from a pairing process involving scanning a quick response code by the two Bluetooth devices. Saving the long-term keys simplifies future discovery and pairing processes.

Throughout this disclosure, examples are described where a computing system (e.g., a user equipment (UE), a client device, a server device, a computer, or another type of computing system) may analyze information (e.g., Bluetooth data) associated with a user. Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if

and when systems, programs, and/or features described herein may enable collection of information (e.g., information about a user's social network, social actions, social activities, profession, a user's preferences, a user's current location), and if the user is sent content or communications from a server. The computing system can be configured to only use the information after the computing system receives explicit permission from the user of the computing system to use the data, for example, in situations where the computing system analyzes Bluetooth data associated with a user's device or a user account. Further, individual users may have constant control over what programs can or cannot do with the information. In addition, information collected may be pre-treated in one or more ways before it is transferred, stored, or otherwise used so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (for example, to a city, ZIP code, or state level) so that a particular location of a user cannot be determined. Thus, the user may have control over whether information is collected about the user and the user's device and how such information, if collected, may be used by the computing device and/or a remote computing system.

The out-of-band pairing method for pairing Bluetooth devices via a QR code provides an advantage over utilizing a "non-bonded" GATT connection because the QR code does not require use of a server. For example, the "non-bonded" GATT connection method may include sending data encrypted with a pre-shared AES CBC passphrase and IV such that a first device can encrypt using the CBC passphrase and IV (e.g., "12345678901234567") and a second device can decrypt using the same passphrase and IV. However, the added step of encryption and decryption requires the devices to access a server outside of the application, thereby adding an additional layer of

indirection and complexity in the pairing process. In contrast, a user viewing a QR code containing necessary encryption keys through a camera or other image viewing application on their computing device does not require access to the internet or use of a server.

The disclosed out-of-band pairing processes may utilize a library (e.g., ZXING) to generate and capture the QR code data and/or may utilize a specific format of QR code data (e.g., JSON data with Base64 encoded string values and regular integer values). Further, two-dimensional (2D) barcodes (e.g., barcode symbologies that employ 2D patterns of squares, dots, or other geometric patterns to represent data) may be utilized by an OOB pairing process instead of a QR code. Examples of common 2D barcode symbologies may include Datamatrix, Maxicode, Quick Response (QR) Code, Aztec Code, Semacode, and the like.

In this way, the disclosed methods provide an improved version of Bluetooth pairing that uses out-of-band pairing for Bluetooth devices via a quick response code to enhance the user experience and increase security.

References:

[1] Patent Publication: US20110081860A1. Methods and devices for facilitating Bluetooth pairing using a camera as a barcode scanner. Priority Date: October 2, 2009.

[2] Patent Publication: US20200229248A1. Association between devices. Priority Date: August 18, 2017.

[3] Patent Publication: US20150098706A1. Light sequence out-of-band Bluetooth pairing. Priority Date: October 7, 2013.

[4] Patent Publication: KR20120045848A. Device and method for pairing between Bluetooth devices. Priority Date: November 1, 2010.