June 19, 2019

Secure Pairing and Identification of BLE Devices

Adam Rodriguez

David Lazarov

Secure Pairing and Identification of BLE Devices

Abstract:

Today, pairing of Bluetooth Low Energy (BLE) capable devices with user devices is neither secure nor trivial. Secure pairing and identification of BLE devices is described. A service (*e.g.,* web service) provides a list of unique identifiers (UIDs) and an encrypted UID to a BLE device manufacturer without a decryption key. The manufacturer provisions each beacon of each BLE device with a UID generated by the service. The manufacturer also generates a quick response (QR) code to print on the BLE device. To pair with the BLE device, a user uses a camera or other scanner of the end-user device to simply scan the QR code. In response, the end-user device queries the service to resolve the UID, then scans for, identifies, and connects to the beacon. The end-user device also configures the beacon to broadcast an ephemeral identifier (EID), which changes over time, preventing third parties from identifying the paired beacon.

Keywords:

Beacon, Bluetooth Low Energy, BLE, BLE device, pairing devices, Internet-of-Things (IoT), ephemeral identifier, EID

Background:

Today, with advancements in wireless communication and with beacon technology embedded in a myriad of devices, the ability for devices to locate one another over a wireless personal area network (PAN), such as a Bluetooth Low Energy (BLE) network, to collect and/or exchange data or signals with one another is escalating. The low-energy signaling of BLE enables long battery life and proximity-sensing capabilities. Generally, a first device repeatedly broadcasts

an identifier (ID) that a second device can receive and, with the correct key, decode. However, simply broadcasting the same identifier over and over is not secure because it can be easily discovered by unauthorized devices.

To address these privacy concerns, further BLE developments include the use of an ephemeral ID, which is an encrypted identifier that changes periodically at a rate determined during initial registration with a web service. For example, the ephemeral ID may refer to the identity and MAC address of the beacon that change (*e.g.,* rotate) with regard to some Advanced Encryption Standard (AES) key and clock value of the beacon, making it non-trackable by third parties. The broadcast ephemeral ID can be resolved remotely by the service with which it was registered, but to other observers appears to be changing randomly. This system becomes less-secure, however, by providing the AES key to other entities, even manufacturers. Further, the ephemeral ID may become impossible to decrypt if either the key or the clock value is unknown, due to the constant rotation of the identity over time.

Description:

Beacon technology is a locating technology that relies on a small wireless device transmitting a short-range signal (a beacon) via a low energy communication protocol such as Bluetooth Low Energy. Such a signal typically includes a unique identifier (UID), which may be associated with a particular device and/or location, and indexed, along with information about the particular device and/or location, as part of a database. The signal can be detected by a mobile device, such as a smartphone, a smartwatch, a tablet, or the like, and, when detected, can serve to indicate that the mobile device is proximate to the particular location associated with the beacon.

The signal can alternatively or additionally serve to identify the particular BLE device that a user device can establish a wireless connection (*e.g.,* pair) with.

A general overview of a system for secure pairing and identification of BLE devices is depicted in Fig. 1. As illustrated, a service (*e.g.,* web service implemented at a server) provides, to a manufacturer, a list of UIDs and an encrypted form of the UID, which the manufacturer cannot decrypt without the proper key. The encrypted form of the UID may be implemented as a manufacturer-specific key generated by the service. The encrypted UID can be shortened by a URL service. Encryption is performed by the service using the manufacturer-specific key, which may require a one-time process of the service generating a key for each manufacturer that the service supports.

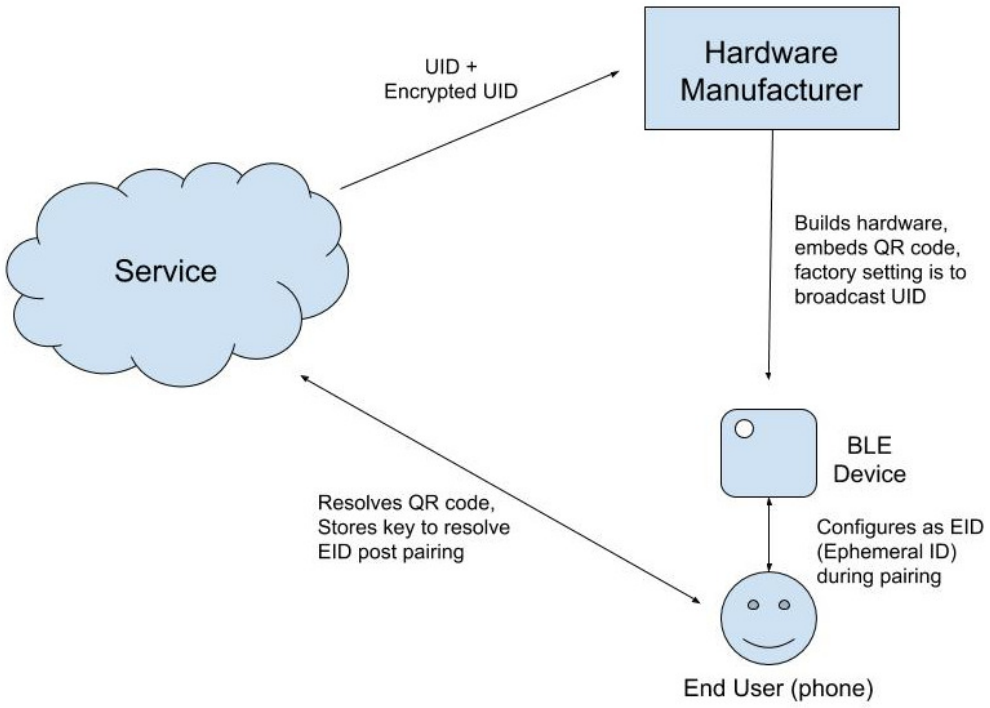

Fig. 1

When building hardware, such as a BLE device, the manufacturer may provision the hardware with a UID from the list, and embed or print a QR code on the BLE device. In some aspects, the manufacturer may generate new UIDs based on the encrypted UID (*e.g.,* UID encrypted with the manufacturer-specific key). The QR code may include a link (*e.g.,* URL) to a resolver service that allows an end-user device to query for the identity of the beacon. The QR code may also include a manufacturer-specific ID and the encrypted UID generated by the service. The resolver service may be the same as, or different from, the service that generated the list of UIDs.

To pair the end-user device with the BLE device, the end-user device first scans, using a scanner, the QR code of the BLE device. From the QR code, the end-user device obtains the link to the resolver service and issues a query to the resolver service to resolve the UID. The resolver service resolves the QR code using the stored key and transmits the UID of the BLE device to the end-user device. Then, the end-user device scans for the beacon, identifies the beacon using the UID, and connects to the beacon.

The end-user device, in response to connecting to the beacon, generates an AES key and configures the beacon to generate an ephemeral ID based on the AES key. For example, the end-user device generates a new Active Server Pages (ASP) exchange with the beacon over a wireless connection, such as a Generic Access Profile (GAP) connection. From this point on, the beacon broadcasts the ephemeral ID. The end-user device, or an application on the end-user device, generates an additional secret key to lock the connection between the beacon and the end-user device, or between the beacon and the application on the end-user device. The end-user device also transmits, to the resolver service, information sufficient for resolving (*e.g.,* decrypting) the ephemeral ID of the BLE device post pairing. The resolver service also registers the ephemeral

ID with an account associated with the end-user device or a user of the end-user device. The BLE device is configured to, during a lifetime of the beacon, broadcast the ephemeral ID if and only if the beacon is associated with a user account of the resolver service. If the BLE device is not associated with any such account, then its beacon broadcasts its factory-setting UID, which is easily discoverable.

When a user disconnects a BLE device from the end-user device, the process is essentially reversed. For example, the end-user device scans for the ephemeral ID, locates the beacon, and resets the beacon to manufacturer settings (*e.g.,* factory reset to original state). The end-user device also informs the resolver service of the disconnection, which enables the resolver service to delete stored information associated with that beacon from the user's account.

These techniques provide many benefits, some of which include a simplified method of pairing devices for the user by simply scanning a QR code, prevention of unauthorized pairing with the BLE device, and enhanced security of private information such as the user's identity. These techniques prevent third-party entities from resolving the ephemeral ID. Because the end-user device's identity is not provided to the manufacturer, there is little chance of that private information being revealed to a third party. In fact, the service does not provide any secret or private information to the manufacturers. The manufacturer itself does not generate and does not maintain any secret key. If the information provided to the manufacturer leaks, then while a single counterfeit beacon could be created utilizing the leaked encrypted UID, the end user device's identity cannot be revealed or determined by a third party. Therefore, private information is safeguarded by the service. At any point in time, the owner of the beacon may identify their beacons by scanning the QR code again on a paired BLE device and the resolver service can expose the beacon's owner and name if the user who scanned the QR code is the owner or if the owner

has explicitly made the beacon public. Further, after the owner disconnects the beacon, the owner can no longer track the beacon if another user pairs a user device to it because the beacon has been configured with a new AES key. Thus, the beacon is protected from unauthorized access, even by a previous owner.

In aspects, the service and/or the resolver service are implemented as one or more software services with a specification, which other entities (*e.g.,* BLE device manufacturers) can implement to be compatible with the one or more software services. The BLE device may include any suitable device capable of executing BLE techniques, including keychains, laptops, sensors, actuators, cellphones, and other small devices that are configured to utilize, or are limited to, low power consumption. Other BLE devices may include devices configured with Internet-of-Things (IoT) functionality, which refers to communications and exchange of data across the myriad of devices either directly, in a machine-to-machine environment, or indirectly over a network.

The end-user device may execute an application program configured to intercept the scanning of the QR code and, responsively, query the resolver service. The application program may be used to perform the functions described above with respect to the end-user device. If the application program is not installed on the end-user device, then upon scanning the QR code for pairing with the BLE device, the end-user device may responsively initiate a browser application that is directed to an installation page for downloading and installing the application program.

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 or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one

or more ways before it is stored or 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 (such as 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 what information is collected about the user, how that information is used, and what information is provided to the user.

In conclusion, secure pairing and identification of BLE devices, using techniques and systems described above, addresses privacy and security concerns associated with accessing beacon identity information of a paired beacon. The techniques described herein provide a simple pairing mechanism compared to other Bluetooth pairing mechanisms. These techniques also provide enhanced security of beacon identifiers of BLE devices and prevent unauthorized access to the identifiers, including by the manufacturer of the BLE devices. Further, using these techniques, a user can easily identify their paired devices by querying the service because the user's paired devices are associated with a user account maintained by the service.

References:

[1] Juels, Ari. Systems and Methods for Detection of Wireless Beacon Cloning. WIPO Pub. WO201809363, filed November 10, 2017, and published May 24, 2018.

[2] Krieger, Ken, and Michel Weksler. Generating and Using Ephemeral Identifiers and Message Integrity Codes. US Patent 9,043,602, filed December 3, 2014, and issued May 26, 2015.

[3] Coli, Vincent J., and Leonard Ott. Beacon-Activated Automatic Generation of Scan Targets and Scan Responses. US Pub. 20190026768, filed January 13, 2017, and published January 24, 2019.

[4] Hassidim, Avinatan, Yossi Matias, Moti Yung, and Alon Ziv. "Ephemeral Identifiers: Mitigating Tracking & Spoofing Threats to BLE Beacons." Google AI. January 01, 1970. Accessed June 14, 2019. https://ai.google/research/pubs/pub45367.