Bluetooth blog

Management of Devices in a Bluetooth Mesh Network

Posted on August 28, 2017 by Martin Woolley

Chapter 6 of the Bluetooth Mesh Networking Series

This article is one of several in a series about Bluetooth mesh networking. Bluetooth® mesh is a new Bluetooth technology with new terminology and concepts. It is recommended that you read previous articles in the series first.

Introduction

A Bluetooth mesh network is like an exclusive club. If you're a member of the club, you can enter the club and make use of those facilities and services which your membership type allows. If you're not, you aren't allowed through the front door, no matter what you say.

A Bluetooth mesh device is either a member of a particular Bluetooth mesh network, or it is not. If it is a member, it has the right to communicate, in at least a basic way, with other devices that are also members of that network. If it's not a member, then anything and everything that device transmits will be ignored by other devices in the network.

A Bluetooth mesh device can be thought of as having a membership type as well, like having access to specific club amenities (gym, golf course, etc.), but not the entire club. It can only fully interact with certain devices in the network. The concept governing this is that of the application. For example, a Bluetooth mesh light switch can switch Bluetooth mesh lights on or off in the network as a consequence of each of those devices being part of the lighting application. The light switch cannot switch on the heating system because the heating system is not part of the lighting application.

For a device to become a member of a Bluetooth mesh network, it must be added to the network using a secure process called provisioning.

Security

Figure 1 - A Bluetooth mesh network

Security is central to Bluetooth mesh networking and we'll cover the subject in detail later in this series. Adding or removing a device to/from a Bluetooth mesh network are both processes which have security requirements at their very heart.

Bluetooth mesh networking uses a system of different security key types to secure the network as a whole, as well as to secure and separate individual applications within the network. Being a member of a network and having the right to participate in a particular application is, in both cases, a consequence of a device possessing the right security keys. All Nodes in a network possess a key called the network key or NetKey. It is possession of this key which makes a device a member of that network, i.e. one of its nodes.

Nomenclature

Earlier in the Bluetooth Mesh Networking Series, we introduced the formal, technical terms device and Node. You may recall that a device which is a member of a mesh network is called a node and one which is not is called a device. I'll now use "Device" with an uppercase "D" to denote a device which is not yet part of a mesh network and continue to use "device" as I have been so far, to mean an electronic item in the more general, informal sense.

The Provisioner

Provisioning transforms a humble Device into a Node, a full-fledged member of a Bluetooth mesh network. The process is accomplished using an application, which is typically provided by product manufacturers for use on smartphones or tablets, but may take other forms, such as desktop or web applications.

The device running the provisioning application is called the Provisioner. The Provisioner must be physically secure, as it has a very special role to play.

FEATURED RESOURCE

Bluetooth Mesh Networking - An Introduction for Developers

Download this comprehensive technology overview to learn more about the key concepts and terminology, system architecture, and security mechanisms, as well as the unique message publication and delivery technique behind Bluetooth mesh networking.

The Provisioning Protocol

During provisioning, the Provisioner and the Device to be provisioned communicate using a Bluetooth mesh protocol called the Provisioning Protocol. The Provisioner may use the Provisioning Protocol over either of the PB-ADV or PB-GATT bearers[i], ensuring that Provisioner applications may be implemented on older smartphones, only requiring that they have support for Bluetooth Low Energy (LE) and GATT.

Adding a New Device to the Network

Adding a device to the network is largely concerned with providing it with the network key which all the other Nodes of that network possess. And of course, that process must itself be secure so that malicious devices cannot eavesdrop on the communication which takes place whilst adding the new device and steal the NetKey.

When a new Device is purchased and it needs to be added to an existing Bluetooth mesh network, users will employ the Provisioner, together with instructions from the manufacturer of the new Device, to add it to the Bluetooth mesh network. This transforms the new Device into a Node and member of the Bluetooth mesh network.

The process involves several steps, depicted in the flow chart below.

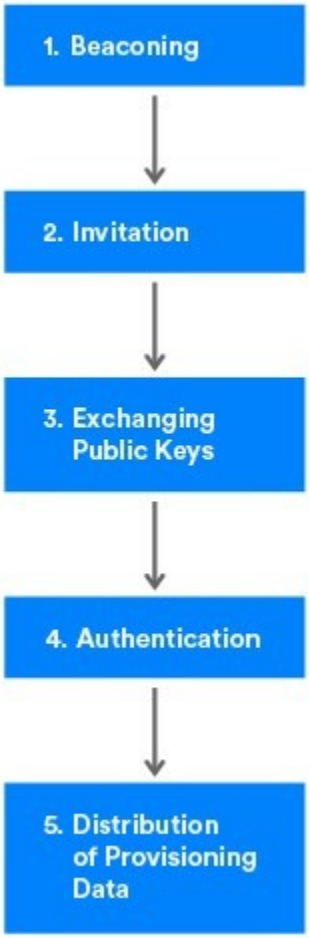

Figure 2 - the provisioning process

Step 1. Beaconing

The Bluetooth mesh network specification has introduced new GAP AD Types, including the <<Mesh Beacon>> AD Type[ii].

A Device indicates its availability to be provisioned by using the <<Mesh Beacon>> AD type to advertise itself as an unprovisioned Device. The user might need to start the new device advertising in this way by following a procedure described by the manufacturer, such as pressing a combination of buttons or holding down a button for a certain length of time.

The user will also start the “Add Device to Network” process within the Provisioner, and this will cause it to receive the advertising packets from the beaconing Device. Remember that the Provisioner is likely to be a smartphone or tablet application, so in practical terms, this involves unlocking the smartphone, launching the application, perhaps logging into the app (for extra security) and

employing its user interface to initiate looking for beaconing Devices. In this way, the Provisioner becomes aware of the new Device and its readiness to go through the remainder of the provisioning process.

Step 2. Invitation

Next, the Provisioner sends an invitation message to the device to be provisioned. The invitation takes the form of a Provisioning Invite PDU, which is part of the Provisioning Protocol. The Beaconing device responds with information about itself in a Provisioning Capabilities PDU.

The Provisioning Capabilities PDU provides information such as the number of Elements it has and the provisioning-related algorithms it supports. It also indicates the types of input and output capabilities the Device has, information which is used in the Authentication step.

Step 3. Exchanging Public Keys

All Bluetooth mesh devices, including the Provisioner, support the FIPS P-256 Elliptic Curve Algorithm and therefore must have a public key. Asymmetric cryptography, based on this algorithm, is used to create a secure channel over which to perform the remainder of the provisioning process. To this end, the Provisioner and Device exchange their public keys. Note that the Device may provide its public key via an out-of-band method, such as a QR code. We'll focus on mesh security, including provisioning security, in a later article in the Bluetooth Mesh Networking Series.

Step 4. Authentication

The Provisioner makes use of its knowledge of the new Device's capabilities and sends a message to it, which instructs it to output either a single or multi-digit value in response to one of various supported user actions, such as pressing a button. The form that the value takes when output will vary, according to the device. One device might display a three-digit, numeric value on an LED panel while another might flash a red LED a number of times, the number of flashes being the output authentication value. The user of the Provisioner will observe the value output by the Device and enter it into the Provisioner user interface.

The Device and Provisioner then exchange a cryptographic hash, derived from data which includes the random value which was output by the Device, allowing them to complete the authentication of their peer.

Step 5. Distribution of the Provisioning Data

After authentication has successfully completed, a session key is derived by each of the two devices from their private keys and the exchanged, peer public keys. The session key is then used to secure the subsequent distribution of the data required to complete the provisioning process, including a NetKey and a unique address for the device, known as the Unicast Address.

After provisioning has completed, the provisioned device possesses the network's NetKey, a Bluetooth mesh security parameter known as the IV Index and it has a Unicast Address[iii], allocated by the Provisioner. The new device is now officially a Node and a member of the Bluetooth mesh network.

Removing a Node from the Network

There will come a time when a Node of a Bluetooth mesh network needs to be removed. The device might have broken and needs replacing or it might need to be moved to another Bluetooth mesh network in another of the company's offices in a different city. Equally, the device might have been sold with the expectation that the new owner will add the device to their own Bluetooth mesh network, using the provisioning process described above.

Figure 3 - Sometimes things break!

If a device malfunctions and cannot be repaired, you might be tempted to simply throw it in the trash. If you sell a device to someone, you could equally be tempted to simply take the money and forget about your old device. That would be unwise, however.

Nodes contain security keys which they were provided with through the provisioning process. Remember, that it is possession of the main NetKey which determines that a device is a member of a network and therefore has access to it. Leaving the keys relating to your Bluetooth mesh network inside a device when you throw it away or sell it could leave your network vulnerable to a trash can attack. Therefore, a secure procedure for removing nodes, which eliminates this concern, has been defined and will be described here.

Removing a Node from a network involves two steps. First, the Provisioner application is used to add the node to be removed to a “black list”. Second, a process called the Key Refresh Procedure is initiated.

The Black List

Using the Provisioner, the user must add the Node to be removed to its black list. The purpose of the black list is simply to act as a list of those nodes which must not be issued with new security keys when the Key Refresh Procedure is initiated.

The Key Refresh Procedure

The Key Refresh Procedure results in all Nodes in the network, except for those which are members of the black list, being issued with new network keys, application keys and all related, derived data. In other words, the entire set of security keys which form the basis for network and application security are replaced.

The user initiates Key Refresh using the Provisioner and the Provisioner creates and sends new keys to every Node in the mesh network using configuration messages, except for those which are members of the black list.

Low Power Nodes will receive the new keys from their Friend. As such, it may be some considerable time before they receive them and therefore, for the whole network to have its keys replaced.

Due to the fact that every Node will not receive its new keys at exactly the same time, the Key Refresh Procedure defines a transition period known as “Phase 2”, during which both the old keys and the new keys are used. Specifically, transmission uses the new keys, but nodes that support receiving messages use both the old and the new keys.

The Provisioner informs all Nodes that they should revoke the old keys when Phase 2 has completed and each node that is not black listed has received its new keys.

At this point, the Node which was removed from the network and which contains an old NetKey and an old set of AppKeys is no longer a member of the network and consequently, poses no threat.

Conclusion

Security is at the very core of the design of Bluetooth mesh networking technology. We've seen how this has manifested itself in those most fundamental of network management scenarios, adding new devices to the Bluetooth mesh network and removing them.

If that's whetted your appetite for more information on Bluetooth mesh network security, you'll enjoy the next in our series of Bluetooth mesh articles where we give you a detailed tour of some of the most important Bluetooth mesh security features.

ON-DEMAND WEBINAR

What Makes Bluetooth Mesh so Disruptive?

The behind-the-scenes story of the making of Bluetooth mesh

Watch our free on-demand webinar to discover how Bluetooth mesh is disrupting building automation, wireless sensor networks, asset tracking, and more.

[i] Bearers are discussed in Part 1 of the series, An Introduction to Bluetooth mesh.

[ii] If you're not clear what "GAP" is or what an "AD Type" is, GAP is the Generic Access Profile, a part of the Bluetooth LE architecture and it defines how Bluetooth devices can operate in a connectionless mode, using "advertising" to broadcast data and "scanning" to receive it. "AD Types" are Advertising Data Types, fields of data which may be included in advertising packets. The Bluetooth Core Specification and Bluetooth Core Specification Supplement define GAP and AD Types in detail.