解密蓝牙mesh系列 | 第六篇

2017-10-13 小码哥 蓝牙技术联盟

蓝牙mesh网络
设备管理

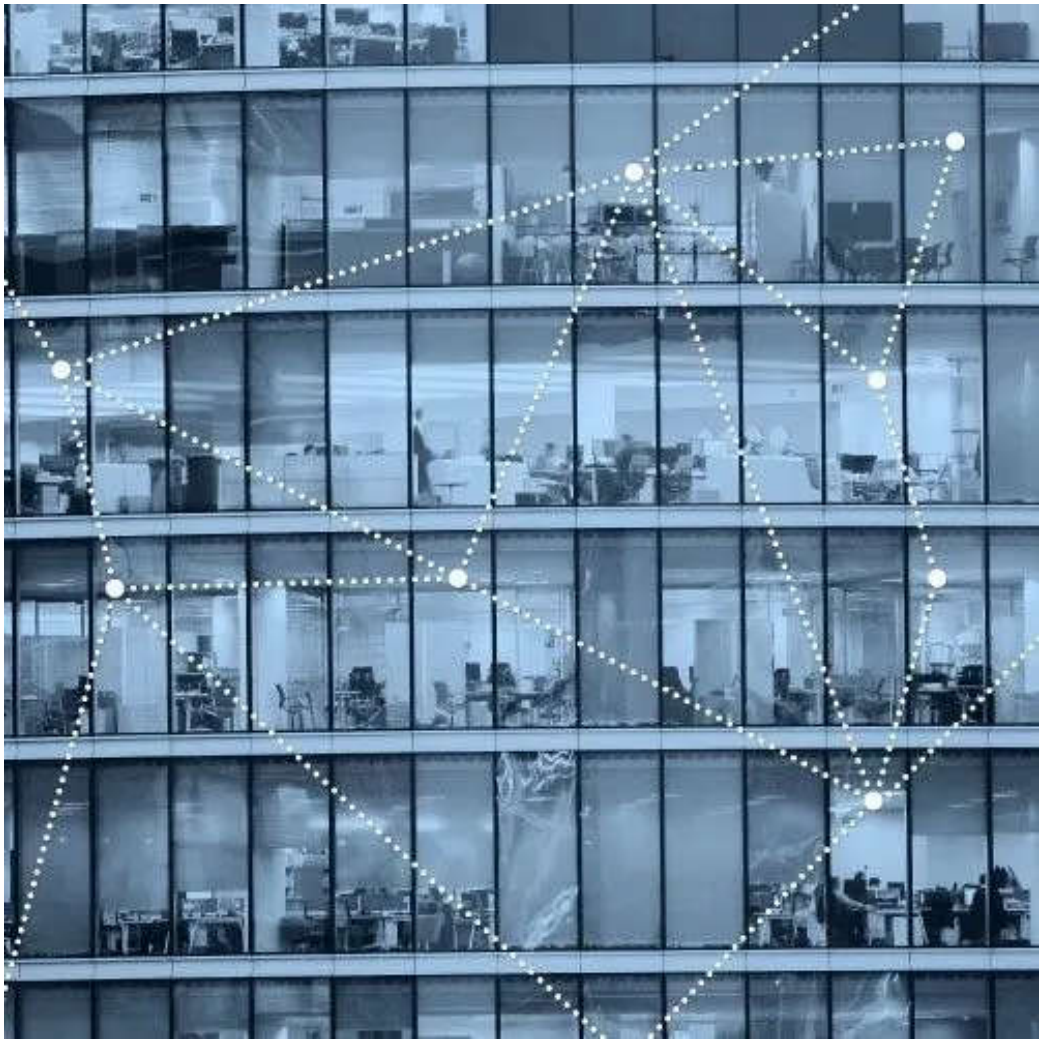
蓝牙技术联盟EMEA技术项目经理
Martin Woolley
小码哥

前言

蓝牙mesh网络好比是一个VIP俱乐部。如果您是这个俱乐部的会员，就可以随意进入，享受与会员类别相对应的设施和服务。如果您不是会员，便无论如何也过不了门卫这一关。

蓝牙mesh设备有可能是某一特定蓝牙mesh网络的成员，也有可能不是。如果它是成员，则有权与同为该网络成员的其他设备进行通信（至少以一种基本的方式）。如果它不是成员，那么该设备**传输的所有内容都将被网络中的其他设备忽略。**

其实可以理解为蓝牙mesh设备也拥有不同的会员类型，例如可以使用某些特定的俱乐部服务设施（如健身房、高尔夫球场等），但不是全部。它只能与网络中的某些设备进行充分的交互。**而对其进行管理的就是“应用”（application）这一概念。**例如，蓝牙mesh照明开关可以在网络中打开或关闭蓝牙mesh照明灯，因为所有这些设备都是照明应用的一部分。而由于供暖系统并非照明应用的一部分，因此照明开关就无法打开供暖系统。



蓝牙mesh网络

设备要想成为蓝牙mesh网络的成员，则必须经过一个称为“启动配置(provisioning)”的安全流程，将设备添加到网络中。

安全性

安全性是蓝牙mesh网络的核心，我们将在本系列的后续文章中详细介绍这一主题。将设备添加到蓝牙mesh网络、或从中移除设备的过程都将严格遵循安全性要求。

蓝牙mesh网络使用一套包含各类安全密钥的系统，从整体上保护网络，同时保护网络内的各个应用并将其彼此分离。拥有正确的安全密钥，设备才能成为网络成员并有权参与特定应用。**网络中的所有节点（node）都拥有一个名为“网络密钥”或“NetKey”的密钥。**只有设备拥有了这个密钥，才能成为该网络的成员，即成为其中的节点之一。

命名法

在解密蓝牙mesh系列之前的文章中（第一篇、第二篇、第三篇、第四篇、第五篇），我们介绍了“设备”（Device）和“节点”（Node）这两个正式的技术术语：**作为mesh网络成员的设备称为“节点”，而不构成节点的设备就称为“设备”。**本文将用英文首字母大写“D”的“设备（Device）”一词来代指非mesh网络成员的设备，用全部字母小写的“设备（device）”来代指一般的日常电子设备。

启动配置设备（Provisioner）

启动配置的流程会将普通的“设备（Device）”变身为“节点（Node）”，使其正式成为蓝牙mesh网络的成员。这一流程通常需要通过一个应用程序来实现，该程序一般由产品制造商所提供，可在智能手机或平板电脑上使用，但也可以采用其他形式，例如桌面或Web应用程序。

运行启动配置应用程序的设备称为“启动配置设备（Provisioner）”，由于它的作用至关重要，因此在物理上必须要保证它的安全性。

启动配置协议(Provisioning Protocol)

在启动配置期间，启动配置设备会采用称为“启动配置协议”的蓝牙mesh协议，与将要被启动配置的设备进行通信。**启动配置设备可通过PB-ADV或PB-GATT承载层**[i]**两者中的任何一个使用启动配置协议**，确保在较早版本的智能手机上亦可实施启动配置设备的应用程序，只要它们支持低功耗蓝牙(Bluetooth Low Energy)和GATT。

向网络中添加新设备

将设备添加至网络的过程中，**最重要的一点是要为其提供网络所有其他节点拥有的网络密钥。**当然，这一过程本身必须是安全的，这样恶意设备才无法窃取添加新设备时进行的通信，也无法窃取NetKey。

当购买了新的设备（Device）并需要将其添加至当前蓝牙mesh网络时，用户将使用启动配置设备（ Provisioner），同时参考这一新设备制造商的说明，将其添加至蓝牙mesh网络。这样，新设备（Device）就变身为节点（Node），成为蓝牙mesh网络的成员。

该流程涉及几个步骤，见下方流程图：

启动配置流程

1 Beacon广播

蓝牙mesh网络规格中介绍了新的GAP广播类型，包括 <<Mesh Beacon>> 广播类型[ii]。

设备（ Device ）可采用<<Mesh Beacon>> 广播类型来发出广播，声明自己是未经启动配置的设备，可被启动配置。用户可能需要根据制造商的说明，按照一定的流程，例如键入一组按钮，或将某一按钮长按一段时间等，以此方式启动新设备的广播。

用户还需要在启动配置设备中启动“添加设备到网络”的流程，以便从Beacon设备（Device）接收广播数据包。需要记住的一点是，启动配置设备可能是智能手机或平板电脑应用，因此在实际操作中会涉及到智能手机解锁、应用程序启动、也许还需要登录应用程序（为了进一步确保安全性），并通过其用户界面启动Beacon设备（Devices）搜寻。这样，启动配置设备就会意识到新设备（Device）的存在和准备就绪状态，可进入后续的启动配置流程。

2 邀请

接下来，**启动配置设备将以启动配置邀请PDU（Provisioning Invite PDU）的形式向要进行启动配置设备发送邀请，这是启动配置协议的一部分。**Beacon设备会在启动配置功能PDU中回应有关自身的信息。

启动配置功能PDU可提供一系列信息，例如其所拥有的元素数量、所支持的启动配置相关算法等。它还能指示设备（Device）拥有的输入输出功能类型，这些信息将用于认证（Authentication）步骤。

3 交换公共密钥(Public Key)

包括启动配置设备在内的所有蓝牙mesh设备都支持FIPS P-256椭圆曲线算法，因此必须拥有公共密钥。可通过基于该算法的非对称加密来创建安全通道，以完成剩余的启动配置流程。为此，启动配置设备会与将被启动配置的设备（Device）交换公共密钥。**需注意的是，将被启动配置的设备（Device）可以通过带外方式(Out of Band)，例如QR码，来提供公共密钥。**本系列的后续文章将重点讨论mesh安全性，包括启动配置的安全性。

4 认证（Authentication）

启动配置设备基于对新设备（Device）功能的了解，向其发送消息，指示其输出单一或多位数值，对其所支持的多种用户操作（例如按下按钮）作出响应。值的形式会因设备差异而有所不同。一台设备可能会在LED面板上显示一个三位的数值，另一台设备则可能是红色LED灯闪烁几次，闪烁的次数就是输出的验证值。启动配置设备的用户将观察到设备（Device）输出的值，并将值输入启动配置设备的用户界面。

然后，**设备（Device）和启动配置设备交换密码散列**，这些数据来源包括设备（Device）输出的随机值，**允许它们完成对彼此的验证**。

5 启动配置数据的分配

认证成功完成之后，会通过两台设备的私有密钥（Private Key）和交换的对等公共密钥生成会话密钥（Session Key）。随后，会话密钥即可用于保护完成启动配置流程所需数据的后续分发，包括网络密钥（NetKey）和设备的唯一地址，即单播地址（Unicast Address）。

启动配置完成后，启动配置设备就会拥有网络的NetKey，这是一个称为“IV索

引（IV Index）”的蓝牙mesh安全性参数，且拥有一个由启动配置设备分配的单播地址[iii]。**至此，新设备就正式成为了节点，即成为蓝牙mesh网络中的一员。**

从网络中移除节点

有时会需要从蓝牙mesh网络中移除节点。**设备可能已经损坏并需要更换，或者可能需要将它移到另一蓝牙mesh网络**，如公司位于其他城市的另一个办公室。**同样，设备可能已经被出售**，新的设备所有者可能会采用上述启动配置流程，将设备添加至自己的蓝牙mesh网络。

设备有时会破损

如果设备故障无法修复，你可能只会想简单粗暴将它丢进垃圾桶。如果把某个设备卖给别人，同样你可能只会简单地想到收款，而忽略故障设备的问题。然而，这种做法并不明智。

节点包含通过启动配置流程提供的安全密钥。请记住，设备必须拥有主网络密钥（NetKey），通过这一点才能确定它是网络的成员、并有权访问网络。**当您丢弃设备或将其出售时，如果还将蓝牙mesh网络的相关密钥留在其中，就可能导致网络遭受垃圾桶攻击。**因此，这里所定义和描述的移除节点的安全程序，能够避免网络被攻击。

从网络中移除节点涉及两个步骤：

1. 首先，使用启动配置设备应用，将想要移除的节点添加至“黑名单”。
2. 其次，启动一项称为**密钥刷新程序（Key Refresh Procedure）**的流程。

黑名单

使用启动配置设备，用户必须将想要移除的节点添加至黑名单。黑名单的目的很简单，就是当启动密钥刷新程序时，确保新的安全密钥不会被发放至黑名单中的节点。

密钥刷新程序

通过密钥刷新程序，除了黑名单中的节点，网络中的所有节点都会被发放新的网络密钥、应用密钥、以及所有相关衍生数据。也就是说，构成网络和应用安全性基础的整套安全密钥都会被替换。

用户可使用启动配置设备启动密钥刷新，启动配置设备会创建新密钥，并通过配置消息向mesh网络中的所有节点发送新密钥，但黑名单中的成员除外。

低功耗节点（Low Power Node）将从好友节点处接收到新密钥，因此它们可能需要经过相当长的一段时间才会接收到新密钥，随后整个网络将全部更换密钥。

由于所有节点不会在同一时间接收到新密钥，因此密钥刷新程序定义了一个称为“第二阶段”的过渡周期，在此期间新旧密钥均可使用。具体来说，传输过程中会使用新密钥，但支持消息接收的节点会同时使用新旧密钥。

第二阶段完成之后，启动配置设备会通知所有节点废除它们的旧密钥。至此，黑名单之外的每个节点都收到了新密钥。

此时，从网络中移除的节点、以及包含旧网络密钥（NetKey）和旧应用密钥（AppKey）的节点将不再是网络中的成员，因此也无法构成任何威胁。

结论

安全性是蓝牙mesh网络技术设计的核心。这在网络管理场景中的一些最基本的层面已有充分体现：向蓝牙mesh网络中添加或移除设备。

想了解有关蓝牙mesh网络安全性的更多信息吗？在下一篇解密蓝牙mesh系列中，我们将选取部分最重要的**蓝牙mesh网络安全特性**为大家做详细介绍，敬请期待！

References:

[i] 关于承载层，请参考 解密蓝牙mesh系列 | 第二篇 。

[ii] 什么“GAP”，什么是“广播类型”？GAP是通用访问配置文件（Generic Access Profile）的缩写，它是低功耗蓝牙架构的一部分，定义了蓝牙设备如何通过“广播”来发送数据、通过“扫描”来接收数据，从而以无连接模式进行操作。“广播类型”是广播数据类型（Advertising Data Types）的缩写，它指的是可被包括在广播数据包中的数据字段。蓝牙核心规格和蓝牙核心规格附录对GAP和广播类型给出了详细的定义。

[iii] 关于蓝牙mesh采用的寻址机制，请参考 解密蓝牙mesh系列 | 第四篇。

点击“**阅读原文**”，下载超全mesh技术概览！

精选留言

写留言

米米

请问如何确认蓝牙mesh的连接性？有测试标准和一起吗？

2017年10月27日

作者回复

关于mesh的测试标准，请参考 https://www.bluetooth.com/specifications/qualification-test-requirements ，内涵最新的test case reference list(TCRL): TCRL 2017-1.

2017年11月7日

以上留言由公众号筛选后显示

了解留言功能详情