解密蓝牙mesh系列 | 第九篇

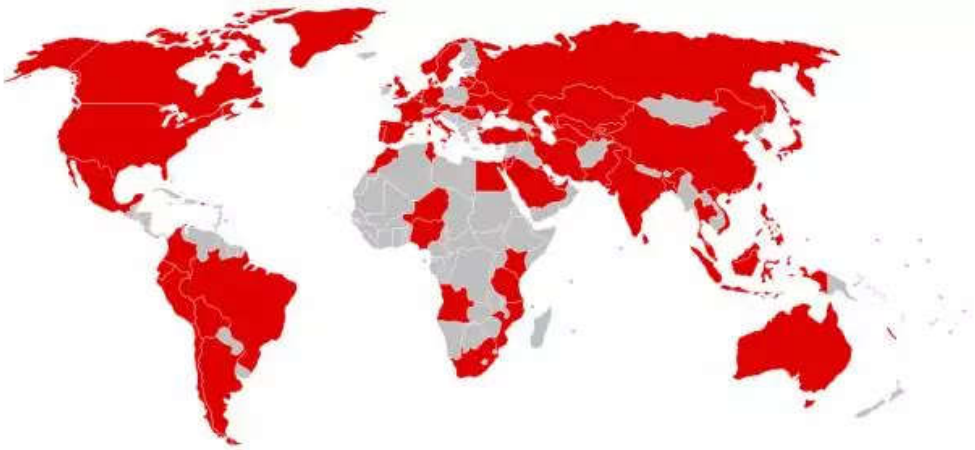
2017-11-03 任凯 蓝牙技术联盟

蓝牙mesh网络

启动配置Part1

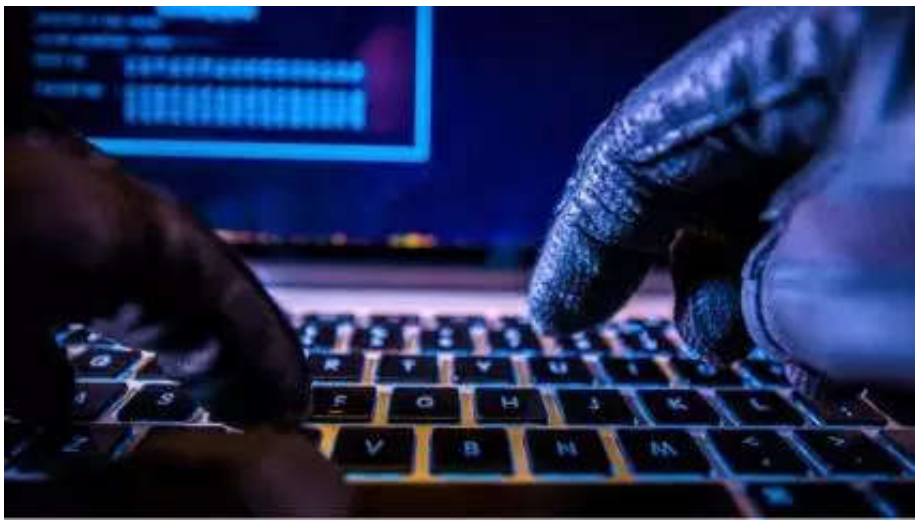
蓝牙技术联盟亚太区技术项目经理

任凯



受WannaCry攻击的国家地区

2017年5月，臭名昭著的勒索软件WannaCry向全球各地的电脑发起了攻击，并窃取了用户数据进行勒索。来自150个国家和地区的数百万台计算机遭受影响，勒索软件要求用户通过比特币这一加密电子货币的形式支付赎金。如果没有稳健的、基于标准的安全系统设计，物联网（IoT）可能也会发生类似情况。可以想象，如果没有完善的安全防护，今后物联网设备的用户也会迫不得已支付“赎金”让“黑客”打开自家的家门。



安全性是蓝牙mesh网络设计的核心，而且这种安全性是强制性的，网络中的每个数据包都会经过加密和认证。蓝牙mesh网络的安全性能够保护整个mesh网络免受各类威胁和问题的困扰，包括：

- **中继攻击（Replay attack）**：可通过正确使用序列号来保护网络不受中继攻击。
- **中间人攻击(Man-in-the-middle attack)**：采用非对称加密技术来进行抵御，例如通过椭圆曲线Diffie-Hellman（ECDH）来有效防范中间人攻击。
- **垃圾桶攻击(Trash Can attack)**：这种攻击利用的是废弃设备，必要时可通过刷新安全密钥来防止攻击发生。

概述

启动配置（Provisioning）是向蓝牙mesh网络（如灯泡）添加新的未经启动配置设备的过程。该过程由启动配置设备(Provisioner) 进行管理。启动配置设备和未经启动配置设备遵循蓝牙mesh规格中定义的固定过程。**启动配置设备向未经启动配置设备提供使其成为蓝牙mesh节点的启动配置数据（provisioning data）。**

启动配置设备通常是运行启动配置应用程序的智能手机或其它移动计算设备。尽管每个网络只需要一台启动配置设备来执行启动配置，但可用的启动配置设备可以有多台。

启动配置协议

蓝牙mesh规格中定义了启动配置协议，该协议定义了启动配置流程中用于在启动配置设备和新的未经启动配置设备之间进行通信的标准流程以及PDU。图1描绘了完整蓝牙mesh协议栈之外的启动配置协议栈。

图1: mesh系统架构与启动配置协议栈

从下到上的组件如下：

启动配置承载层(Provisioning Bearer)

启动配置承载层实现了启动配置PDU在启动配置设备和未经启动配置设备之间的传输。定义的**两个启动配置承载层包括**：

- **PB-ADV**：指通过蓝牙广播信道进行设备启动配置的启动配置承载层。PB-ADV承载层用于发送通用启动配置（Generic Provisioning）PDU。支持PB-ADV的设备应尽可能执行占空比接近100％的被动扫描，以避免遗漏任何发送来的通用启动配置PDU。

- **PB-GATT**：指使用来自代理协议的蓝牙mesh代理（proxy）PDU来进行设备启动配置的启动配置承载层。“代理协议能使节点通过面向连接的低功耗蓝牙（Bluetooth Low Energy）承载层来收发网络PDU、mesh Beacon、代理配置消息和启动配置PDU。PB-GATT在GATT操作中包含了启动配置PDU，涉及GATT启动配置服务，同时能在启动配置设备不支持PB-ADV时供其使用。

启动配置协议

定义对于启动配置PDU、行为和安全性的要求。了解启动配置协议将有助于您根据应用需求选择合适的验证方法。

启动配置协议定义了**10种启动配置PDU**：

1. 启动配置邀请 (Provisioning Invite)
2. 启动配置能力 (Provisioning Capabilities)
3. 启动配置状态 (Provisioning State)
4. 启动配置公钥 (Provisioning Public Key)
5. 启动配置输入完成 (Provisioning Input Complete)
6. 启动配置确认 (Provisioning Confirmation)
7. 启动配置随机 (Provisioning Random)
8. 启动配置数据 (Provisioning Data)
9. 启动配置完成 (Provisioning Complete)
10. 启动配置失败 (Provisioning Failed)

开发者若想了解有关这些PDU的详细信息，请参考**蓝牙mesh规格的5.4.1节**（详见：https://www.bluetooth.com/specifications/mesh-specifications）。

完整的启动配置过程必须在更高的层面完成两项重要任务：

1. **验证未经启动配置的设备。**在蓝牙mesh网络中，一个小空间中可能存在几台、几十台或数百台设备。执行认证是为了确保与启动配置设备进行交互的设备就是用户想要启动配置的设备。

2. **与未经启动配置的设备建立安全链接，并与之共享相应的信息。**在流程的最后，原本未经启动配置的设备将成为蓝牙mesh网络中的节点。

启动配置流程包括五个阶段：

① **发送Beacon信号**

② **邀请**

③ **交换公共密钥**

④ **认证**

⑤ **启动配置数据分发**

这里将介绍**前三个阶段**。我们将在“蓝牙mesh网络启动配置Part2”中介绍最后两个阶段。

① 发送Beacon信号

Beacon是低功耗蓝牙的传统应用场景。想象一下，一个GAP外设（如智能手表或活动跟踪器）希望与GAP中央设备（如智能手机或平板电脑）连接。 GAP外设切换到广播状态并开始发送其广播数据包。GAP中央设备扫描广播数据包以发现其它设备并接收相关基本信息。**蓝牙mesh启动配置使用的也是相同的广播机制**。

如果未经启动配置的设备支持PB-ADV承载层，则其作为未经启动配置设备Beacon进行广播。这涉及指定的数据包格式，且未经启动配置设备通过此方式来使自身被启动配置设备 (Provisioner) 发现。

当未经启动配置设备使用PB-GATT承载层时，一项称为“mesh启动配置服务”的GATT服务会支持整个启动配置程序，同时支持与启动配置设备的交互。在发送Beacon信号阶段，未经启动配置设备会发送包括mesh启动配置服务UUID的广播数据包，它会被启动配置设备通过标准的低功耗蓝牙扫描程序发现。

② 邀请

在发送Beacon信号之后，启动配置设备和未经启动配置设备会建立PB-ADV或PB-GATT启动配置承载层（provisioning bearer）。然后，启动配置设备发送一个启动配置邀请 PDU，设备通过启动配置功能PDU对其作出响应。

启动配置邀请PDU包括**Attention Duration**字段，其指示了未经启动配置设备的主要元素应采用某种视觉指示方式，并在多长的时间内吸引用户的注意力。

启动配置功能PDU包括：

- 设备支持的元素数量；
- 支持的一组安全算法；
- 使用带外（OOB）技术实现的公共密钥可用性；
- 该设备向用户输出值的能力。
- 该设备允许用户输入值的能力。

图 2 – 启动配置邀请

图2中的流程图让人联想到低功耗蓝牙中的配对过程，这在此前的文章《蓝牙配对 - 第一篇：配对特性交换（Pairing Feature Exchange）》中有所介绍。低功耗蓝牙配对采用的配对特性交换类似于蓝牙mesh启动配置程序中的启动配置邀请阶段。**在启动配置邀请阶段，目的是向启动配置设备(Provisioner)提供有关未经启动配置设备功能的信息。**有了这些信息，启动配置设备就能决定下一步该如何进行。

③ 交换公共密钥

信息加密涉及两项基本技术：**对称加密**（也称为密钥加密）和**非对称加密**（也称为公钥加密）。

对称加密采用相同的密钥进行加密和解密。只要发送设备和接收设备都知道密钥，就能够解密所有使用此密钥加密的信息。然而，很难安全地通过链路交换密钥并防止其落入坏人之手。

非对称加密使用两个相关的密钥（即一个密钥对）来解决上述问题：公钥和私钥。公钥免费提供给任何可能想向您发送消息的人。私钥则为保密，只有你自己知道。使用公钥加密的任何消息（文本、二进制文件或对称密钥）只能通过应用相同的算法、且仅能使用与之匹配的私钥进行解密。这意味着您不必对通过链接传递公钥的过程有任何担忧，因为它们仅用于加密而非解密。然而，非对称加密比对称加密慢一些，且需要更高的处理能力来进行消息内容的加密和解密。

在蓝牙mesh用例中，大多数设备基于嵌入式芯片组或模块，因此无法使用计算成本昂贵的非对称加密技术来对每个消息进行加密/解密。对称加密更适合于不具备非对称加密所需处理能力的设备，但如何安全地交换并使用密钥仍然是一大问题。蓝牙mesh采用了非对称和对称加密结合的方式来解决这一问题。

- **非对称加密**：椭圆曲线Diffie-Hellman（ECDH）是一种匿名密钥协商协议，允许具有椭圆曲线公私密钥对的双方在非安全信道上建立共享保密信息。ECDH在蓝牙mesh启动配置中的目的是在启动配置设备和未经启动配置设备之间创建安全链路。它使用公钥和私钥来分发对称性密钥，两台设备随后可将其用于后续消息的加密和解密。

- **对称加密**：在蓝牙mesh网络中传输的每个消息都使用AES-128密码加密。 AES-128算法是常用的对称加密/解密引擎，常用于嵌入式平台。

在交换公钥阶段，有两种交换ECDH公钥的可能方式。它们可以通过蓝牙链路、或OOB隧道进行交换。在启动配置邀请阶段，未经启动配置的设备已经报告了是否支持通过OOB隧道发送自身公钥。如果是，则启动配置设备可继续使用它，并通过发送启动配置开始PDU来通知未经启动配置的设备。

如果未经启动配置设备的公钥可通过OOB隧道获得，则临时公钥从启动配置设备发送到设备，并采用合适的OOB技术（例如二维码），从未经启动配置的设备中读取静态公钥，如图3所示。

图 3 – 未经启动配置设备采用OOB方式进行的公钥交换

否则，双方的公钥都会经由图4中所示的蓝牙链路进行交换。

图 4 – 未经启动配置设备的公钥未知时的公钥交换

ECDHSecret = P-256 (私钥，对等公钥)

在该等式中，P-256即FIPS 186-3中定义的FIPS-P256曲线。

本文的Part2将介绍启动配置程序的最后两个阶段：启动配置数据的认证和分发。我还会对蓝牙mesh网络中会用到的安全工具箱进行介绍。

点击“**阅读原文**”，下载超全**mesh技术概览**！

程吗？没有oob的那种情况的

2017年11月3日

作者回复

Hi Zecw，如果使用PB-GATT进行provisioning，入网设备和provisioner需要建立连接，但是对于“配对pair”没有强制要求。

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