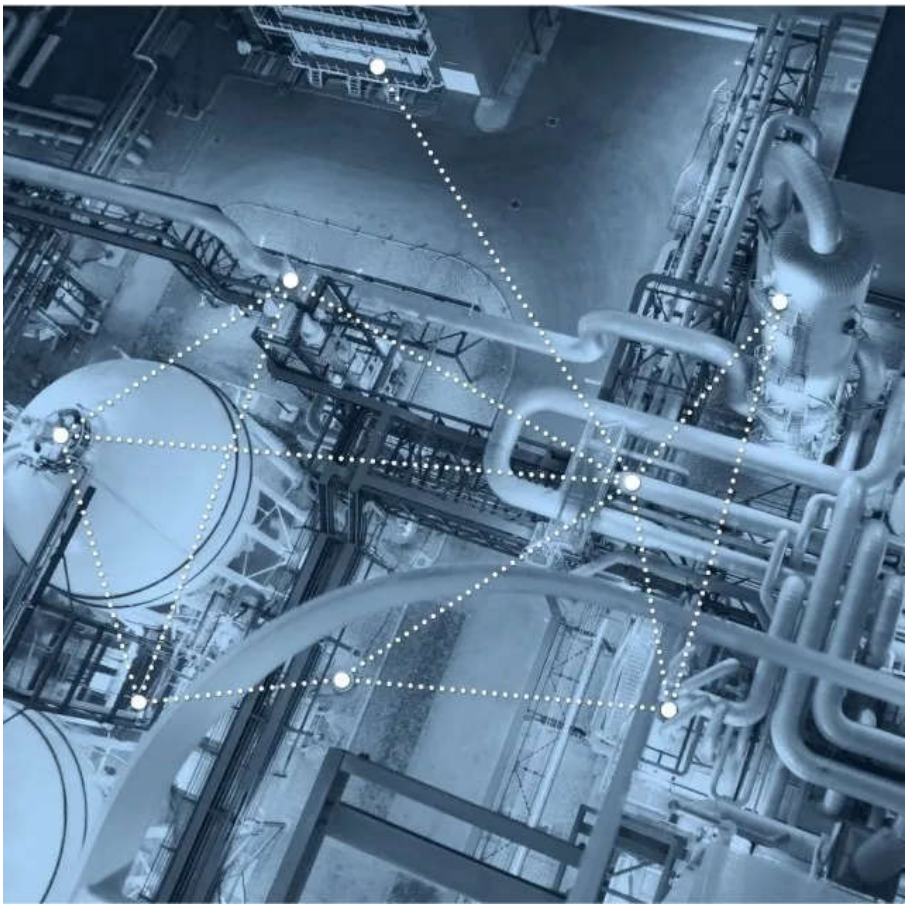
# 解密蓝牙mesh系列 | 第八篇

2017-10-27 任凯和小码哥 蓝牙技术联盟

## 蓝牙mesh网络
## 安全性概览



### 为何安全性如此关键？

安全性可谓是物联网（IoT）最受关注的问题之一。从农业到医院、从智能家居到商业智能建筑、从发电站到交通管理系统，物联网系统和技术将触及我们生活的方方面面。**物联网系统如果存在安全漏洞，就可能会导致灾难性的后果**。

蓝牙mesh网络的安全性从设计之初就是重中之重。**本文将着重分析主要的安全特性和现已被解决的安全问题**。本系列的后续文章也将持续详细地介绍蓝牙mesh网络安全性的各个方面。

### 蓝牙mesh网络强制使能安全性

低功耗蓝牙（Bluetooth Low Energy）GATT设备可实施蓝牙核心规格中定义的一系列安全措施。产品设计人员有责任决定采取哪些安全措施，也可以决定不采用任何既有的安全特性。换句话说，**低功耗蓝牙GATT的安全性配置是非强制性的**。如果我们谈论的是单一设备的安全性及其与另一台设备的连接，只要产品设计师正确地进行风险评估，那么他的决定就是合理的。**然而，蓝牙mesh网络中的安全性涉及的不仅是单一设备或对等设备之间的连接安全性；它关注的是整个设备网络的安全性，以及网络中各组设备的安全性。**

因此，**蓝牙mesh网络中强制性使用安全性**。

### 蓝牙mesh网络安全性的基本概念

以下基本的安全性说明适用于所有蓝牙mesh网络：

| | |
|---|---|
| 加密与认证 | 所有mesh消息都经过加密和认证。 |
| 安全分级考量 | 网络安全性、应用安全性和设备安全性彼此独立。详见下方的“安全分级考量”。 |
| 区域隔离 | 蓝牙mesh网络可分为若干子网，每个子网密钥不同，独立于其他子网，各自都是安全的。 |
| 密钥刷新 | 通过密钥刷新过程，可以在蓝牙mesh网络的整个生命周期内更改安全密钥。 |
| 消息模糊化 | 消息模糊化的作用是让外界难以跟踪网络内所发送的消息，进而提供了一种隐私保护机制，难以让外界跟踪节点（Node）的网络活动。 |
| 中继攻击防护 | 蓝牙mesh安全性可保护网络免受中继攻击。 |
| 垃圾桶攻击防护 | 节点可从网络中安全地移除，此方式也能防止垃圾桶攻击(Trash Can Attack)。 |
| 安全设备启动配置 | 设备添加到蓝牙mesh网络以成为节点的过程是一个安全的过程。 |

### 安全分级考量与安全密钥

**蓝牙mesh安全性的核心是三类安全密钥**。这些密钥为mesh网络的不同方面提供了安全性，并实现了蓝牙mesh网络安全性中的关键性能，即“**安全分级考量**”。

以可用作中继（Relay）节点的mesh照明灯为例，它能够作为中继，处理与楼宇中蓝牙mesh门窗安全系统相关的消息。照明灯完全不涉及对这些消息内容细节的访问和处理，但却会将消息中继至其他节点。

为处理这种潜在的利益冲突，**蓝牙mesh采用称为“应用密钥（AppKey）”的安全密钥来保护应用层消息**，它不同于用于保护特定应用（如照明、物理安全、温控等）相关数据安全的密钥。

蓝牙mesh网络中的所有节点都拥有一个或多个网络密钥（NetKey），每个网络密钥对应一个子网，它也可能是主要子网。**节点必须拥有网络密钥，才能成为网络中的成员。网络加密密钥(Encryption Key)和隐私密钥(Privacy Key)直接源于网络密钥**。

拥有NetKey让节点能够对网络层的数据进行解密和验证，以便执行诸如中继等网络功能。但应用程序数据不可被解密。

每个节点还拥有一个唯一的安全密钥，称为设备密钥（DevKey），用于节点的启动配置（Provisioning）和配置流程。

### 区域隔离

节点拥有了主要NetKey ，就意味着它具备了蓝牙mesh网络成员资格和访问权限。但也可以将网络划分成不同的子网，每个子网都有自己的子网密钥。这意味着**只有拥有指定子网密钥的设备才能与该子网中的其他成员设备进行通信。也可以临时创建并分配子网密钥**，例如，酒店中位于不同客房的节点的隔离。

### 节点移除、密钥刷新与垃圾桶攻击

如上所述，节点包含各种蓝牙mesh安全密钥。如果一个节点发生故障并需要处理，或者如果所有者决定将节点出售给其他人，那么**重要的是确保该设备及其所包含的密钥不会被盗用，避免向节点原本所在的网络发动攻击**。



蓝牙mesh网络确保设备可被安全地进行丢弃处理

从网络中删除节点的程序现已有明确定义。**通过启动配置设备（Provisioner）应用程序，可将节点添加至黑名单，然后启动密钥刷新程序（Key Refresh Procedure）**。

密钥刷新程序会向网络中除黑名单成员以外的所有节点发放新的网络密钥、应用密钥、以及所有相关的派生数据。也就是说，**构成网络和应用程序安全性基础的整套安全密钥将被替换**。

因此，已从网络中移除的、包含原有NetKey 和AppKey的节点将不再是网络成员，换句话说，上述这些不被授信的节点将从网络当中剔除出去，因此也无法再构成威胁。

### 隐私

由NetKey导出的隐私密钥(Private Key)用于对网络PDU (Payload Data Unit)的报头值进行模糊化，例如源地址（source address）。**模糊化可以确保无法通过随机的被动窃听来跟踪节点及其使用者，也使得基于流量分析的攻击难以实施**。

### 中继攻击

在网络安全方面，**中继攻击是窃听者拦截并捕获一个或多个消息、稍后重新进行传输的一种技术，目的是欺骗接收者，执行未经被攻击设备授权的任务**。常见的例子就是汽车的无钥匙进入系统被攻击者所击破，攻击者就能拦截汽车车主和汽车之间的认证序列，然后对这些消息进行中继，以进入汽车并将其偷走。

**蓝牙mesh可保护网络免受中继攻击。这种保护是基于分别称为序列号（SEQ, Sequence Number）和IV索引(IV Index)的两个网络PDU字段**。每次发布消息时，元素会增加SEQ值。节点从元素接收消息，如果元素包含的SEQ值小于或等于上一个有效消息中的SEQ值，则节点会将消息丢弃，因为这则消息可能与中继攻击有关。IV索引是一个单独的字段，需与SEQ一同纳入考量。来自给定元素的消息中的IV索引值必须始终等于或大于该元素的上一个有效消息。

### 加密工具箱

蓝牙mesh网络的大多数安全特性都有赖于业内标准的加密算法和程序，这在本系列的其他安全性相关文章中也会提及，本文还是着重解释最重要的内容。

**蓝牙mesh协议栈中采用的两项关键的安全功能是AES-CMAC和AES-CCM**。这些是基本的加密和认证功能，所有用于密钥生成的其他功能都是基于上述两

者。

### AES-CMAC

基于密码的消息认证码（CMAC）是一种算法，能够生成固定长度的128位消息认证值，并将其用于任何变量长度输入。使用AES-CMAC算法生成消息认证码MAC的公式为：



AES-CMAC具有出色的错误检测能力。涉及验证校验和或者使用错误检测代码的其他技术只能检测数据的意外修改。**AES-CMAC旨在检测有意的、未经授权的数据修改，以及意外修改**。如果您有意向了解更多关于此功能的信息，请参考RFC4493 中的详细定义：https://tools.ietf.org/html/rfc4493

向 AES-CMAC输入:

- **k – 128位的密钥**
- **m – 将被认证的可变长度数据**

### AES-CCM

**AES-CCM是一种通用的、认证的加密算法，使用时需要加密块密码**。在蓝牙mesh规格中，AES-CCM在所有情况下都能被用作基本的加密和认证功能。其使用公式如下：



向AES-CCM输入四项内容:

- **k – 一个128位的密钥**
- **n – 一个104位的随机数**
- **m – 将被加密和认证的可变长度数据**
- **a – 将被认证、但不加密的可变长度数据，也被称为“附加数据（Additional Data）”，这一输入参数长度可以为0字节。**

从 AES-CCM有两项输出:

- **密文 - 加密后的可变长度数据**

- **MIC – m和a的消息完整性检查值**

下图显示了可能来自蓝牙mesh网络层（network layer）或上层传输层(upper transport layer) 的**纯文本有效载荷（Payload）**，由具有**输入加密密钥(Key)**、**随机数(Nonce)**和**纯文本有效载荷的AES-CCM**进行处理。其输出为**加密的有效载荷(Encrypted Payload)** 和**MIC**。



用于数据包有效负载加密和认证的AES-CCM

### SALT生成

蓝牙mesh安全性定义了SALT 生成函数s1，它采用AES-CMAC功能。如上所述，AES-CMAC具有两个输入参数：k和m。当用于SALT生成时，只有输入参数m发生变化。 K一直被设置为一个128位的值，即0x0000 0000 0000 0000 0000 0000 0000 0000，它在蓝牙mesh规格中被称为ZERO。



SALT生成函数

向 SALT生成函数输入：

- **m – 一个长度非零的八位字节数组或ASCII编码字符串**

其输出为一个128位的MAC值，s1公式 如下:

### 其它安全性函数

在蓝牙mesh网络规格第3.8.2章节的“安全工具箱（Security Toolbox）”部分中，可以找到对其他安全函数的定义，例如各种关键性的派生函数。所有这些都是基于AES-CMAC和SALT生成函数s1（SALT生成函数也是基于AES-CMAC）。
（https://www.bluetooth.com/specifications/mesh-specifications）

### 未完待续！

安全性是蓝牙技术的首要问题，我们将在解密蓝牙mesh系列中持续探讨这一话题。读完本文，对于蓝牙mesh网络主要的安全特性以及一些基本的加密技术，您应该已经有了较为深入的了解，敬请期待下周的解密蓝牙mesh系列！

---

**本期笔者**


**任凯**

蓝牙技术联盟亚太区技术项目经理

**Martin Woolley小码哥**

蓝牙技术联盟EMEA技术项目经理


---

点击“**阅读原文**”，下载超全**mesh技术概览**！

精选留言

写留言

淡定⊙▿⊙ 1

蓝牙也用中继延伸距离在，运用中会更广

2017年10月27日

城东

你好，我是蓝牙芯片原厂工程师，我们公司的新片要加上mesh的功能，但是我们没有什么经验，请问你们对我们这种情况有什么好的建议吗

2017年12月11日

高校无线网+创客...

很想了解用蓝牙技术做立体空间定位功能

2017年11月23日

以上留言由公众号筛选后显示

了解留言功能详情