Application Note

ZLG52810P0-1-TC 安全机制介绍

蓝牙模块

AN02040200 1.0.05 Date:2020/12/17

类别	内容
关键词	低功耗蓝牙 安全机制
摘要	介绍模块的安全机制，帮助用户选择合适的安全等级

修订历史

版本	日期	原因
V1.0.00	2018/04/09	创建文档
V1.0.01	2018/05/09	修订安全机制相关
V1.0.02	2018/10/19	修订原理说明以及每种模式的使用情况
V1.0.03	2019/03/08	修改企业名称
V1.0.04	2020/03/03	更新文档模板
V1.0.05	2020/12/17	更新文档模板

目 录

1. 简介

1.1 概述

用户开发的产品有的对安全性尤为敏感，但是要快速掌握 BLE 协议栈的繁杂安全机制又显得太浪费时间，这里我们会将最常用以及当前 BLE 最新的安全机制进行简单的封装，给用户提供简单的 AT 指令接口，只需要简单的配置，就能达到自己想要的效果。

注：许多用户喜欢采用静态配对码的方式进行认证，但是其实这种方式是存在很大的安全隐患的，我们强烈建议用户使用动态配对码的方式进行认证，具体配置方法在下文介绍。

1.2 简单原理说明

BLE 协议栈的配对、认证、加密、绑定等安全机制都是基于已经“连接”的两个 BLE 设备之间，也就是说两个 BLE 设备首先会连接，然后再运行相关的安全机制，而不是先运行相关安全机制，然后再决定是否连接。

需要注意的是，本模块支持大部分安全机制，但是当前版本模块本身并不具备主动发送安全请求的功能，也就是配对/加密请求必须由主机端发起，模块会做相应的反馈。

与模块安全机制相关的有三条指令：AT+SECL、AT+LESC、AT+PASS。

“认证”（Authentication）：当模块的 SECL 设置为 1 或者 3 的时候，手机希望与模块进行透传必须要先通过认证。AT+LESC 决定认证时候使用静态配对码还是动态配对码，如果 LESC 为 0，则认证时候采用静态配对码，如果 LESC 为 1，则认证时候采用动态配对码，所谓静态配对码即用户使用 AT+PASS 设置的 6 个字节，所谓动态配对码即在配对过程中模块随机生成的 6 个字节，无论是静态配对码还是动态配对码，都会在配对过程中被模块通过串口输出，如 AT+PASK:123456。若配对过程失败，模块主动断开连接。

注：再次强调，BLE 规范本身没有考虑使用静态配对码的情况，所以这种方式是有安全隐患的，如果安全要求不高可以使用，但是如果安全要求高，建议使用动态配对码方式。

“加密”（Encryption）：加密指的是对两个已连接设备之间的通信数据进行加密，使之成为密文，让第三方抓到空中包也不知道具体是什么意思，该功能不需要额外配置，自动使能。

“绑定”（Bonding）：使用绑定，模块与某个设备配对、认证、加密过程的信息都会保存起来，以便下一次这个设备再次对模块发起配对加密时，能够以最快速度完成加密，通过 AT+SECL 使能。

同时，BLE 的安全机制是由从机和主机共同决定的，模块的 IO 能力如下表。

表 1　不同配置下模块的 IO cap

AT+SECL	IO capability
0	NoInput NoOutput
1	Display Only
2	NoInput NoOutput
3	Display Only

模块作为从机只能最大程度上兼容安全功能，而要达到用户想要的效果，还需要主机配合，这里针对用户常用的几种安全机制进行说明，并且提供一些对应主机如何配置的建议。

1.3 举例

1.3.1 不认证，不绑定，不启用 LE secure Connections （BLE4.0 特性）

第一步，用户输入以下指令：

```
AT+SECL:0
```

第二步，用户输入以下指令：

```
AT+LESC:0
```

只要 BLE 主机支持加密功能，几乎都能支持这种模式。该种模式虽然有加密，但是很容易被破解。

1.3.2 认证，不绑定，不启用 LE secure Connections（BLE4.0 特性）

第一步，用户输入以下指令：

```
AT+SECL:1
```

第二步，用户输入以下指令：

```
AT+LESC:0
```

该模式支持认证和加密，两个设备的认证基于用户设定的静态配对码，通信加密算法也基于用户设定的配对码，也就说第三方抓取空中包数据后，如果不知道配对码，也就无法破解两个设备之间的通信数据，但是由于配对码是 6 个字节的字符的排列组合（‘0’ ~ ‘9’），所以依然可以用穷举法来猜测用户设定的配对码，破解加密，这也是 BLE4.0 协议上的硬伤。

如果主机没有足够的 IO 能力支持认证，规范规定双方设备会默认使用不认证的方法加密，这样就会导致模块判断为认证不通过，模块会自动断开连接，如果客户希望工作在该模式下，主机至少应该满足 IO capabilities：Keyboard Only / Keyboard Display，一般手机都是 IO capabilities = Keyboard Display。

1.3.3 不认证，不绑定，启用 LE secure Connections（BLE4.2 特性）

第一步，用户输入以下指令：

```
AT+SECL:0
```

第二步，用户输入以下指令：

```
AT+LESC:1
```

该模式不支持认证，但支持 BLE4.2 的新安全特性，其中最主要的是 ECDH 密钥交换协议和 AES-CMAC 算法，机密性得到很大的增强。

这个工作模式需要主机也支持 BLE4.2 的 LE secure Connections 特性，一般支持 BLE4.2 的手机都支持。

1.3.4 认证，不绑定，启用 LE secure Connections（BLE4.2 特性）

第一步，用户输入以下指令：

```
AT+SECL:1
```

第二步，用户输入以下指令：

```
AT+LESC:1
```

根据主机不同的 IO capabilities 和 BLE 版本，这种模式下会有以下现象：

主机 IO capabilities	主机版本	
	BLE4.0/BLE4.1	BLE4.2/BLE5.0
Display Only	Just Works（BLE4.0）	Just Works（BLE4.2）
Display YesNo	Just Works（BLE4.0）	Just Works（BLE4.2）
NoInput NoOutput	Just Works（BLE4.0）	Just Works（BLE4.2）
Keyboard Only	Passkey Entry（BLE4.0）	Passkey Entry（BLE4.2）
Keyboard Display	Passkey Entry（BLE4.0）	Passkey Entry（BLE4.2）

Just Works（BLE4.0）：和 1.4.1 情况是一样的；

Just Works（BLE4.2）：和 1.4.3 情况是一样的；

PasskeyEntry（BLE4.0）：和 1.4.2 情况是一样的；

PasskeyEntry（BLE4.2）：和 1.4.2 情况不同的是，这时候的配对码使用的是动态配对码，由于静态的配对码事实上是无法提供 MITM 保护的，所以为了提供一个最高安全模式，取消了静态配对码。

2. 免责声明

本着为用户提供更好服务的原则，广州致远电子股份有限公司（下称“致远电子”）在本手册中将尽可能地为用户呈现详实、准确的产品信息。但介于本手册的内容具有一定的时效性，致远电子不能完全保证该文档在任何时段的时效性与适用性。致远电子有权在没有通知的情况下对本手册上的内容进行更新，恕不另行通知。为了得到最新版本的信息，请尊敬的用户定时访问致远电子官方网站或者与致远电子工作人员联系。感谢您的包容与支持！