ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38648—2020

信息安全技术　蓝牙安全指南

Information security techniques—Guideline to bluetooth security

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院大学、西安电子科技大学、南京理工大学。

本标准主要起草人:张玉清、王基策、何远、李意莲、杨毅宇、黄庭培、赵尚儒、冯翰滔、姚尧、王文杰、王鹤、付安民、伍高飞、李学俊。

信息安全技术　蓝牙安全指南

1　范围

本标准给出了蓝牙安全建议。

本标准适用于蓝牙 5.0 以下版本(含蓝牙 5.0),可对蓝牙设备的设计、开发、测试、使用提供指导。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

蓝牙　bluetooth

一种采用射频方式在近距离使用电子信息设备交换信息的无线接口技术。

3.2

蓝牙网络　bluetooth network

使用蓝牙技术将各种形式的蓝牙设备相互连接构成的无线网络。

4　缩略语

下列缩略语适用于本文件。

BD_ADDR:蓝牙设备地址(Bluetooth Device Address)

BR:基础速率(Basic Rate)

CSRK:连接签名解析密钥(Connection Signature Resolving Key)

ECDH:迪菲赫尔曼椭圆曲线(Elliptic Curve Diffie Hellman)

EDR:增强数据率(Enhanced Data Rate)

HS:高速数据速率(High Speed)

IRK:身份解析密钥(Identity Resolving Key)

LE:低功耗(Low Energy)

LTK:长期密钥(Long-Term Key)

MITM:中间人(Man-in-the-Middle)

PAL:协议适应层(Protocol Adaption Layer)

PIN:个人识别码(Personal Identification Number)

PKI:公钥基础设施(Public Key Infrastructure)

SDP:服务发现协议(Service Discovery Protocol)

SSP:安全简单配对(Secure Simple Pairing)

5 概述

蓝牙分为BR、EDR、HS和LE四种类型。蓝牙1.1和1.2版本支持BR,传输速率为1 Mbit/s;蓝牙2.0版本引入EDR,传输速率提高至3 Mbit/s;蓝牙3.0版本引入HS,最高传输速率可达24 Mbit/s;蓝牙4.0版本引入LE,保持最高传输速率的同时降低了能耗。蓝牙4.0至5.0版本均支持BR、EDR、HS和LE四种类型。

蓝牙安全机制参见附录A。BR、EDR、HS支持四种安全模式,LE支持两种安全模式。其中,BR、EDR、HS的安全模式4支持五种服务安全级别,LE的安全模式1支持四种加密级别,LE的安全模式2支持两种数据签名级别。蓝牙典型的安全漏洞和面临的威胁参见附录B。

6 安全建议

6.1 管理

在部署和维护蓝牙网络时宜关注以下事项,包括但不限于:

a) 制定蓝牙网络安全策略;
b) 在部署蓝牙网络前,掌握构成蓝牙网络设备的安全特性,如身份认证功能、数据加密功能等;
c) 定期对蓝牙网络的安全状态进行评估;
d) 记录接入蓝牙网络设备的信息,如蓝牙物理地址、蓝牙名称等;
e) 设置连续请求之间的时间间隔数值为指数级方式增长,防止攻击者重复验证身份。

6.2 技术

6.2.1 密钥配置

当采用蓝牙交换信息时,密钥配置宜关注以下事项,包括但不限于:

a) 配置加密密钥时,选择算法允许的最大长度;
b) 选择随机且达到最大允许长度的数字组合作为PIN;
c) 链路密钥不能基于网络中设备共享的单元密钥;
d) 设备验证的链路密钥宜在配对过程中产生;
e) 使用SSP的蓝牙2.1以上版本(含蓝牙2.1)设备使用口令输入模式进行配对时,采用随机且唯一的口令;
f) 提供应用级安全,如用户认证、端到端安全通信、审计等;
g) 使用如生物特征识别技术、智能卡、双因素认证或PKI等完成用户认证;
h) 通过配对设备中的随机数产生器生成认证密钥和加密密钥;
i) 蓝牙广播传输时使用基于主机链路密钥的加密密钥进行加密;
j) 使用LE技术的设备应采用主流加密算法;
k) 使用的密码技术应符合国家密码管理相关规定。

6.2.2 模式选择

配置蓝牙的通信模式时宜重点关注以下事项,包括但不限于:

a) 蓝牙2.0以下(含蓝牙2.0)版本的设备与其他版本的设备使用BR、EDR、HS通信时,采用安全模式3;

b) 蓝牙 2.1 以上(含蓝牙 2.1)版本的设备之间使用 BR、EDR、HS 通信时,采用安全模式 4;
c) 蓝牙 4.1 以上版本(含蓝牙 4.1)设备之间使用 BR、EDR、HS 通信时,采用安全模式 4 级别 4;
d) 蓝牙 4.0、4.1 版本的设备和蓝牙 4.0 以上版本(含蓝牙 4.0)设备使用 LE 技术通信时,采用安全模式 1 级别 3;
e) 蓝牙 4.2、5.0 版本的设备之间使用 LE 技术通信时,采用安全模式 1 级别 4;
f) 蓝牙 2.1 以上(含蓝牙 2.1)版本设备使用 SSP 策略时,不使用"Just Works"配对方式。

注:"Just Works"模式指不需要用户参与,设备发起连接即可配对目标设备,容易受到附录 B 中 B.2 g)的简单配对攻击。

6.2.3 连接及链路配置

配置蓝牙的连接及通信链路时宜关注以下事项,包括但不限于:

a) 设备之间的通信链路启用加密;
b) 设备之间的连接采用双向认证;
c) 设备需提示用户对蓝牙连接进行授权;
d) 限制蓝牙传输功率大小至仅能满足蓝牙设备间的通信需求,降低受到 B.2 h)侧信道攻击的风险。

6.3 操作

加入蓝牙网络的用户在进行信息交换等操作时宜重点关注以下事项,包括但不限于:

a) 减少配对次数,降低输入口令和蓝牙配对信息泄露的风险;
b) 不响应未知设备的 PIN 请求;
c) 不接受来自未知设备的信息,包括文件、图片等;
d) 修改设备的设置使其符合接入网络的安全策略;
e) 配置设备为非发现模式;
f) 为设备的蓝牙模块设置密码;
g) 若设备丢失,及时移除现有设备中与丢失设备的配对信息;
h) 不使用蓝牙时关闭蓝牙功能,停用不需要或未授权的服务或资源;
i) 定期升级蓝牙软件,及时更新蓝牙补丁和固件。

附 录 A
（资料性附录）
蓝牙安全机制

A.1 蓝牙安全服务

蓝牙技术提供了身份鉴别、保密、授权、消息完整性、配对五种基本的安全服务。

A.2 BR、EDR 和 HS 的安全模式

蓝牙 BR、EDR 和 HS 定义了四类安全模式，安全模式决定了蓝牙设备何时启用安全服务，蓝牙设备工作于其中一类模式下。四类安全模式定义如下：

a) 安全模式 1：设备或模块没有启用加密和认证功能。蓝牙 2.0 以下版本（含蓝牙 2.0）版本的设备支持安全模式 1，蓝牙 2.1 以上版本（含蓝牙 2.1）的设备可以使用安全模式 1 向下兼容之前版本的设备。

b) 安全模式 2：强制的服务级安全模式。安全功能在物理连接建立后，逻辑连接建立前启动。由本地安全管理器控制对特定服务的访问。本地安全管理器通过授权功能，决定一个设备是否被允许获得一项特定权限。在本地安全管理器中实现认证和加密机制。蓝牙 2.0 以下版本（含蓝牙 2.0）的设备支持安全模式 2，蓝牙 2.1 以上版本（含蓝牙 2.1）的设备可以使用安全模式 2 向下兼容之前版本的设备。

c) 安全模式 3：强制的链路级安全模式。安全功能在物理连接完全建立前启动。要求对所有接入设备进行验证和加密。一旦设备通过验证后通常不会再执行服务级的授权。蓝牙 2.0 以下版本（含蓝牙 2.0）的设备支持安全模式 3，蓝牙 2.1 以上版本（含蓝牙 2.1）的设备可以使用安全模式 3 向下兼容之前版本的设备。

d) 安全模式 4：强制的服务级安全模式（类似于安全模式 2）。安全功能在物理和逻辑连接建立后启动。使用 SSP 策略，在连接密钥生成时用椭圆曲线 ECDH 密钥协议取代传统的密钥协商协议，设备认证和加密算法与蓝牙 2.0 及早期版本中的算法相同。是否进行链路密钥验证取决于使用的 SSP 关联模型。安全模式 4 需要加密所有服务。为了兼容，当与蓝牙 2.0 以下版本（含蓝牙 2.0）不支持安全模式 4 的设备通信时，安全模式 4 的设备可以回落到任何其他三种安全模式之一。安全模式 4 下的服务又可以分为五种安全级别：级别 0 和级别 1 都没有任何安全要求，区别在于级别 0 只适用于 SDP 协议；级别 2 要求未认证的链路密钥；级别 3 要求已认证的链路密钥；级别 4 要求已认证的链路密钥并使用安全连接。

A.3 LE 安全模式

蓝牙 LE 旨在支持计算和存储受限的设备，其安全性与 BR、EDR 和 HS 不同。另外，LE 还引入了诸如私有设备地址和数据签名等功能，分别由新的加密密钥——IRK 和 CSRK 来支持这些功能。这些密钥（LTK、IRK、CSRK）在 LE 配对期间生成并安全分发。

LE 安全模式类似于 BR、EDR 和 HS 的服务级安全模式，每个服务可以有自己的安全要求。而且，LE 还规定，每个服务请求也可以有自己的安全要求。LE 安全模式 1 和安全模式 2 的定义如下：

a) 安全模式 1：拥有四种加密级别，其中级别 1 不使用认证和加密；级别 2 使用加密、不使用配对

认证;级别3使用加密和配对认证;蓝牙4.2以上版本(含蓝牙4.2)添加了级别4,级别4使用特定加密算法进行加密和配对认证。

b) 安全模式2:提供了数据签名,数据签名提供了数据完整性,但不提供保密性。安全模式2拥有两种数据签名级别,其中级别1使用数据签名、不使用配对认证;级别2使用数据签名和配对认证。

如果不同的服务具有不同的安全模式或级别,则使用较强的安全要求。LE安全模式1级别4的安全性最高,安全模式1级别1的安全性最低。由于安全模式2不提供加密,安全模式1级别3和级别4优于安全模式2。对于4.2以上版本(含蓝牙4.2),建议使用安全模式1级别4。对于4.2以下版本,建议使用安全模式1级别3。

附 录 B
（资料性附录）
蓝牙漏洞与威胁

B.1 蓝牙漏洞

表 B.1 给出了蓝牙主要的安全漏洞信息、漏洞影响的版本以及可采取的安全建议。

表 B.1 蓝牙主要安全漏洞

序号	安全漏洞	说明	影响的版本	安全建议章条号
1	基于单元密钥的链路密钥是固定的，在每次配对中重复使用	使用单元密钥的设备在同其他设备配对时使用相同的链路密钥。这是一个严重的加密密钥管理漏洞	1.0 1.1	6.2.1 c)
2	使用基于单元密钥的链路密钥可能导致窃听和欺骗	当设备的单元密钥泄露后（即在它第一次配对时），那么具有该密钥的其他设备都可以欺骗该设备或者任何与该设备配对过的设备。此外，不管设备链路是否加密，该设备的链路都可被窃听	1.0 1.1 1.2	6.2.1 c)
3	安全模式 1 的设备不会初始化安全策略	使用安全模式 1 的设备是不安全的。对于蓝牙 2.0 及以下版本（含蓝牙 2.0）的设备，推荐使用安全模式 3	1.0 1.1 1.2 2.0	6.2.2 a)
4	使用较短的 PIN	在配对过程中 PIN 用来保护链路密钥，但较短的 PIN 可被轻易破解	1.0 1.1 1.2 2.0	6.2.1 b)
5	缺乏 PIN 管理	在用户众多的蓝牙网络中产生充足的 PIN 是困难的。PIN 的扩展经常导致安全问题产生。建议由配对设备中的随机数产生器生成 PIN	1.0 1.1 1.2 2.0	6.2.1 h)
6	加密密钥在使用 23.3 h 后仍重复使用	在 E0 加密算法中，加密密钥流由链路密钥、EN-RAND、主设备 BD-ADDR 和时钟决定。在一个特定的加密链接中只有发起连接的主设备的时钟才会改变。如果一个链接持续时间超过了 23.3 h，时钟值会被重置，因此生成的密钥将和早期连接中使用的密钥相同。重复密钥是一种严重的加密漏洞，攻击者可以据此定义出明文	1.0 1.1 1.2 2.0	6.2.1 a)

表 B.1（续）

序号	安全漏洞	说明	影响的版本	安全建议章条号
7	Just Works 模式在配对时不提供 MITM 攻击防护，会产生未验证的链路密钥	BR 或 EDR 设备在 SSP 过程中，需要拒绝使用由 Just Works 配对产生的未验证的链路密钥来防护 MITM 攻击	2.1 3.0 4.0 4.1 4.2 5.0	6.2.2 e)
8	在 SSP 过程中使用的 ECDH 密钥对是固定密钥对或弱密钥对	弱 ECDH 密钥对削弱了 SSP 的窃听保护，使攻击者容易获得链路密钥。设备应该拥有唯一并定期更新的强 ECDH 密钥对	2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 a)
9	固定的 SSP 密钥容易造成 MITM 攻击	设备应在每次配对时使用随机且唯一的密钥，降低在 SSP 过程中受到 MITM 攻击的风险	2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 a)
10	支持安全模式 4 的设备（蓝牙 2.1 及以上版本）可以降低自己的安全模式与不支持安全模式 4 的设备（蓝牙 2.0 及以下版本）进行连接	最差情况下，设备将降低到安全模式 1，即没有安全保护。建议支持安全模式 4 的设备只降低到安全模式 3	2.1 3.0 4.0 4.1 4.2 5.0	6.2.2 a)
11	可重复身份验证	为防止无限制的请求，需要将限制功能纳入规范。蓝牙协议通常要求连续重复请求间隔一段时间，该时间随着重复请求次数指数增长。但是它没有规定认证挑战请求之间的等待时间间隔，所以攻击者可以收集大量的挑战响应（使用秘密链路密钥加密过），从而可以收集链路密钥的信息	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.1 e)
12	蓝牙网络中的设备共享广播加密的主密钥	密钥由多方共享可导致伪装攻击	1.0 1.1 1.2 2.0 2.1 3.0	6.2.1 c)

表 B.1（续）

序号	安全漏洞	说明	影响的版本	安全建议章条号
13	蓝牙 BR 或 EDR 加密使用的 E0 流密码算法易被破解	使用蓝牙 LE 中要求的主流加密算法	1.0 1.1 1.2 2.0 2.1 3.0 4.0	6.2.1 j)
14	在蓝牙 BR 或 EDR 中，与特定用户关联的 BD_ADDR 被捕获可能会导致隐私泄露	当 BD_ADDR 关联到一个特定的用户，该用户的行为和地址可被跟踪	1.0 1.1 1.2 2.0 2.1 3.0	6.1 d)
15	在蓝牙 LE 中，与特定用户关联的 BD_ADDR 被捕获可能会导致隐私泄露	在蓝牙 LE 中，可以通过实施地址隐私来减少这种风险	4.0 4.1 4.2 5.0	6.1 d)
16	设备认证采用简单的单向挑战/响应密钥	单向的挑战/响应身份验证会受到 MITM 攻击。蓝牙提供双向验证，用于验证设备是否合法	1.0 1.1 1.2 2.0 2.1 3.0	6.2.3 b)
17	蓝牙 LE 配对不提供防窃听保护	窃听者可以捕获在 LE 配对期间分发的密钥（即 LTK，CSRK，IRK）	4.0 4.1	6.2.1 f)
18	蓝牙 LE 安全模式 1 级别 1 不要求任何安全机制（即不进行配对认证或加密）	类似于 BR 或 EDR 安全模式 1，这本质上是不安全的。推荐使用 LE 安全模式 1 级别 4（加密和配对认证）	4.0 4.1 4.2 5.0	6.2.2 d)
19	链路密钥存储不当	如果链路密钥没有被安全存储或增加访问控制，攻击者就可以读取或修改链路密钥	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 a)

表 B.1（续）

序号	安全漏洞	说明	影响的版本	安全建议章条号
20	伪随机数生成器的强度未知	伪随机数生成器可能产生固定或周期性的数字，这将减少认证模式的有效性。建议使用强伪随机数生成器	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 h)
21	加密密钥长度是可协商的	蓝牙 3.0 及以下版本允许设备协商的加密密钥长度最小为 1 字节	1.0 1.1 1.2 2.0 2.1 3.0	6.2.1 a)
22	没有用户认证	蓝牙标准只提供了设备认证。应用级安全（包括用户认证）可以由应用开发者加入	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 f)
23	没有执行端到端的安全	只是对单个链路进行加密和认证。中间节点会对数据解密。可以在蓝牙协议栈之上通过额外的安全控制来提供端到端的安全保障	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 f)

表 B.1（续）

序号	安全漏洞	说明	影响的版本	安全建议章条号
24	有限的安全功能	审计、不可否认性和其他的一些功能没有在蓝牙标准中体现。如果需要，这些服务可以由应用开发者加入	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.2.1 f)
25	长时间处于可发现或可连接模式的设备容易受到攻击	设备为了完成配对或连接，必须进入发现模式或者连接模式，这一过程应尽可能在最短时间内完成。设备不能一直处于这两个模式中	1.0 1.1 1.2 2.0 2.1 3.0 4.0 4.1 4.2 5.0	6.3 e)
26	Just Works 配对方法不提供 MITM 攻击保护	MITM 攻击者可以捕获和操纵设备之间传输的数据。LE 设备应在安全的环境中进行配对，以降低窃听和 MITM 攻击的风险。在蓝牙 LE 中不使用 Just Works 配对方式	4.0 4.1 4.2 5.0	6.2.2 e)
27	在安全模式 3 和安全模式 4 下，两个已配对的 BR、EDR 或 HS 设备可能不会发生双向认证	对于已经配对的两个设备 A 和 B，假设 A 是 B 的认证发起者，加密设置将在初始认证之后开始，如果加密设置的安全程度满足 B 的要求，那么 B 无需再尝试认证 A	1.0 1.1 1.2 2.0 2.1 3.0	6.2.2 a)

B.2 安全威胁

蓝牙设备易受到常见的各类无线网络威胁，比如拒绝服务攻击、窃听、消息篡改及资源盗用等。蓝牙设备也容易受到以下特定威胁，包括但不限于：

a) 蓝牙诱捕：攻击者利用蓝牙设备的固件漏洞入侵开启蓝牙的设备。这种攻击通过非法建立与蓝牙设备的连接来获取该设备上包括国际移动设备识别码在内的任意存储数据。国际移动设备识别码是区别移动设备的标志。攻击者可以利用国际移动设备识别码将受害用户设备上的所有来电转接到攻击者的设备。

b) 蓝牙劫持:攻击者可以向受害蓝牙设备发送消息发起蓝牙劫持攻击。该消息并不会直接导致蓝牙设备受到侵害,而是诱使用户以某种方式做出回应或在设备地址簿中添加新联系人。类似于对电子邮件用户进行的垃圾邮件和网络钓鱼攻击。

c) 蓝牙窃听:攻击者利用某些早期蓝牙设备的固件漏洞获取该设备的访问和控制权限。该攻击可以在用户未察觉的情况下控制蓝牙设备,访问存储数据、拨打电话、窃听通话、发送短信息、以及修改其他设备服务。

d) 拒绝服务攻击:蓝牙易受拒绝服务攻击。其影响包括使设备的蓝牙接口不可用和消耗掉移动设备的电池。该类型的攻击威胁不大,因为蓝牙只有在一定距离内才能工作,所以只需要离开攻击源即可避免。

e) 模糊攻击:蓝牙模糊攻击包括发送畸形或者不标准的数据给蓝牙设备,然后观察设备的反应。如果设备的响应很慢或者完全停止,说明协议栈中存在一个潜在的严重漏洞。

f) 配对过程窃听:PIN 配对方法(蓝牙 2.0 及以下版本)和 LE 配对方法(蓝牙 4.0)容易受到窃听攻击。如果窃听者收集到所有的配对包,就可以确定密钥,从而伪装成可信设备,并进行主动或被动的数据解密。

g) 安全简单配对攻击:Just Works SSP 没有提供抵抗 MITM 攻击的保护,很多技术可以强迫远程设备使用该模式进行配对(例如,攻击设备声明自己没有输入输出能力)。此外,固定的密钥也可允许攻击者实施 MITM 攻击。

h) 侧信道攻击:针对电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息泄露而对设备进行攻击的方法被称为侧信道攻击。

参 考 文 献

[1] Padgette,John & Scarfone,Karen & Chen,Lily.NIST Special Publication 800-121 Revision 1, Guide to Bluetooth Security

[2] IEEE Std 802.11—2016 IEEE Standard for Information technology—Telecomm-unications and information exchange between systems Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[3] Defense Information Systems Agency. DoD Bluetooth Peripheral Device Security Requirements, 16 July 2010

[4] National Security Agency, Bluetooth Security Factsheet, December 2005

[5] Bluetooth Core Specification v5.0