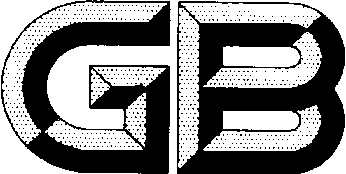
ICS 35.040

L80



中华人民共和国国家标准

GB/T XXXXX—20XX

|  |
| --- |
|  |

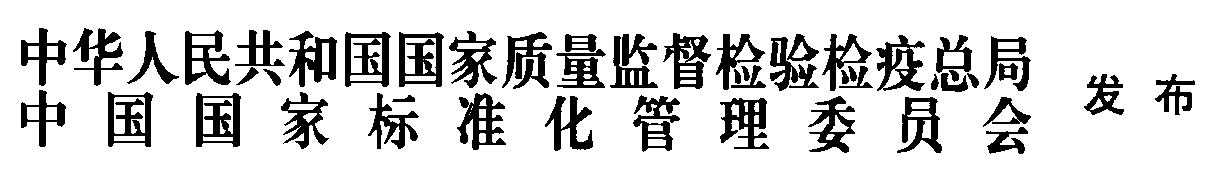
信息安全技术 蓝牙安全指南

Information security technology--Guide to Bluetooth usage security

|  |
| --- |
| （征求意见稿） |
| 2018-05-15 |

20XX - XX - XX发布

20XX - XX - XX实施



目次

[目次 I](#_Toc515993699)

[前言 III](#_Toc515993700)

[引言 IV](#_Toc515993701)

[1 范围 1](#_Toc515993702)

[2 规范性引用文件 1](#_Toc515993703)

[3 术语和定义 1](#_Toc515993704)

[4 缩略语 2](#_Toc515993717)

[5 蓝牙技术概述 2](#_Toc515993718)

[5.1 蓝牙技术的特点 2](#_Toc515993719)

[5.2 蓝牙网络的结构 2](#_Toc515993720)

[6 蓝牙安全使用建议 4](#_Toc515993721)

[6.1 管理建议 4](#_Toc515993722)

[6.2 技术建议 4](#_Toc515993723)

[6.3 操作建议 4](#_Toc515993724)

[附录A（资料性附录）蓝牙漏洞与威胁 6](#_Toc515993725)

[A.1 蓝牙漏洞 6](#_Toc515993728)

[A.2 蓝牙威胁 9](#_Toc515993729)

[参考文献 10](#_Toc515993730)

前言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国科学院大学国家计算机网络入侵防范中心、西安电子科技大学

本标准主要起草人：张玉清、王基策、何远、黄庭培、王文杰、王鹤、伍高飞、李学俊

引言

本指南参考IEEE 802.11和IEEE 802.15.1-2002两个国际标准的部分内容以及相关行业技术发展和实践经验制定而成。

蓝牙是一种短距离无线射频通信的开放标准，广泛应用于各种类型的企业与消费电子设备中。它容易遭受窃听、拒绝服务攻击、中间人攻击、消息篡改和资源盗用等一般无线网络威胁，同时还受到与蓝牙相关的，针对蓝牙标准与实现中已知安全漏洞的威胁。因此，为了缓解蓝牙安全风险，蓝牙使用需要相应的指导。

蓝牙安全指南

1. 范围

本指南为各组织安全有效地使用蓝牙技术提供建议。安全建议涵盖了目前已发布的蓝牙标准1.1、1.2、2.0、2.1、3.0和4.0、4.1、4.2等多个版本。

本指南适用于所有使用蓝牙技术的政府组织或非政府组织。

1. 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，仅所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。

IEEE 802.15.1-2002 电气和电子工程师协会 蓝牙标准

IEEE 802.11 电气和电子工程师协会 无线局域网 AP标准

1. 术语和定义

下列术语和定义适用于本标准。



接入点 access point

将各个无线客户端设备在逻辑上相互连接起来，并提供对分布式系统的访问，例如对企业有线网络的访问。



无线个域网 wireless personal area network

一个短距离的需要很少或不需要基础设施运营的小型无线网络。无线个域网通常用于单独房间内几个设备间的无线连接。



干扰台 jamming

一个在无线网络工作的频段发射电磁波信号来干扰无线网络的正常使用的设备。



校验机 verifier

在蓝牙连接过程中验证申请者身份的蓝牙设备。



微微网 piconet

通过以Ad Hoc方式建立起来的一种微型蓝牙网络。



分布式网络 scatternet

由多个独立、非同步的微微网形成的网络

1. 缩略语

BR 基础速率（Basic Rate）

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

EDR 增强数据率（Enhanced Data Rate）

FHSS 跳频扩频（Frequency Hopping Spread Spectrum）

HS 高速数据速率（High Speed）

LE 低功耗（Low Energy）

PDA 掌上电脑（Personal Digital Assistant）

ad hoc 点对点

1. 蓝牙技术概述
   1. 蓝牙技术的特点

蓝牙是一种低成本、低功耗技术，提供了建立小型无线网络（微微网）的机制。微微网由在同一操作通道、使用相同跳频序列、物理上非常接近的两个或多个蓝牙设备组成，如基于蓝牙的手机和耳机之间的连接就是一个微微网。蓝牙技术的主要优点是：不需电缆、易于文件共享、自动无线同步和共享互联网连接。

蓝牙工作在全球通用的2.4GHz到2.4835GHz的工业、科学、医学频段、采用跳频技术（FHSS）、蓝牙提供了无线链路功能控制策略，使设备能够根据信号强度，协商和调整其无线功率。跳频方案与无线链路功率控制的结合为蓝牙提供了有限的，避免窃听和恶意访问的保护。

蓝牙设备可以通过可发现和可连接模式找到彼此并建立通信。在可发现模式中、设备定期监测一个查询扫描物理信道，并用其设备地址、本地时钟（计数器）值、以及其他寻呼和随后连接所需的特征响应此信道上的寻呼，启动网络连接。

* 1. 蓝牙网络的结构

拥有蓝牙功能的设备可以建立一个ad hoc网络。ad hoc网提供了一个能够让在同一个区域的移动设备（比如在同一个房间）简单的直接连接方式，此连接方式不需要网络基础设施。一个拥有蓝牙发射器并且有软件协同蓝牙协议栈和接口进行工作的设备就是一个简单的蓝牙客户端。

蓝牙标准规定主机和主机控制器之间独立地去执行协议栈功能。主机负责更高层的协议比如：逻辑链路控制及适配协议（L2CAP）和服务发现协议（SDP）。主机是一个拥有计算功能的设备比如笔记本电脑或者桌面电脑。主机控制器主要负责较低层的协议包括发射、基带和链路管理协议（LMP）。主机控制器的主要功能是由一个整合的或者是外部的蓝牙适配器完成的。主机和主机控制器通过主机控制器接口（HCI）进行通信。通常情况下主机和主机控制器被整合在一个设备上，比如蓝牙耳机。

图1描述了基本的蓝牙网络拓扑结构。在一个微微网中，有一个设备作为主设备，其他的设备作为从设备。一个微微网中可以拥有7到255个活动的从设备。



图1 蓝牙自组网拓扑结构

主设备负责建立并控制网络，包括定义网络的跳频序列方案。尽管一个微微网只有一个主设备，但是在采用时分复用（TDM）机制时，允许一个蓝牙设备在一个微微网中作为从设备，且同时在另一个网络中作为主设备，从而形成一个链状网络，称为分布式网络。分布式网络允许多个设备在一个扩展的距离范围内建立一个动态的网络拓扑结构，每次会话都可以改变整个网络的拓扑结构。当一个设备远离或者靠近一个主设备时，网络拓扑结构和网络设备关系都将发生变化。图2描述了一个包含由3个微微网构成的分布式网络。



图2 蓝牙网络（多个分散网络）

由于低功耗蓝牙技术不支持相关特性，因此，目前仅有BR/EDR设备可用于组建分布式网络。

1. 蓝牙安全使用建议
   1. 管理建议

（1）制定一个无线网络安全策略用于增强蓝牙无线网络的安全性。

（2）确保蓝牙网络用户对蓝牙使用的安全相关责任有所了解。

（3）定期执行全面的安全评估，以便于充分了解组织的蓝牙安全状态。

（4）保证无线网络中的蓝牙设备在网络架构上便于识别，并能用文档描述出来。

（5）给用户提供一系列的安全措施，他们可以使用这些措施更好地保护手持蓝牙设备不被盗窃。

（6）维护一个完整的清单，清单包括所有具备蓝牙功能的无线设备和地址(BD\_ADDR)。

* 1. 技术建议

（1）改变蓝牙设备的默认设置值，实施组织制定的的安全策略。

（2）把蓝牙设备的功率设置为正好可满足大小，以便于传输只在安全参数允许范围内进行。

（3）选择一个随机的足够长的私有PIN码，避免静态的和较弱的PIN码，比如全0。

（4）确保链路密钥基于组合密钥而不是单元密钥。

（5）对于v2.1设备使用安全简易配对。避免使用“Just Work”模式。

（6）设备必须验证可靠的链路密钥在配对过程中产生。

（7）对于v2.1和更高版本且使用SSP的设备，在密钥输入模式中必须在每次配对过程中使用随机且唯一的密钥。

（8）使用安全模式4的蓝牙v2.1和更高版本的设备在于v2.0及更低版本设备兼容时，只能降低到安全模式3。

（9）v4.0和v4.1使用低功耗技术的设备和服务应尽可能使用安全模式1级别3。低功耗安全模式1级别3为v4.0和v4.1低功耗设备提供最高的安全性。

（10）使用低功耗功能的蓝牙v4.2设备和服务应尽可能使用安全模式1级别4。低功耗安全模式1级别4实现安全连接模式，并为4.2低功耗设备提供最高安全性。

（11）v4.1 BR/EDR设备和服务应尽可能使用安全模式4级别4，因为它提供了可用于v4.1及更高版本BR/EDR设备的最高安全性。

（12）应锁定不需要和未授权的服务和资源。

（13）蓝牙设备应采用并保持默认配置，除了需要配对以外应该适中处于非发现模式。

（14）在所有蓝牙连接中使用链路加密。

（15）如果多跳无线通信正在使用，确保在通信链中每一个链接上加密。

（16）确保所有访问之前都要在相互之间进行认证。

（17）为所有广播传输执行加密（加密模式3）。

（18）配置最大允许长度的加密密钥。

（19）在允许任何进入的连接请求进行之前，蓝牙设备必须提示用户授权所有传入的蓝牙连接请求。

（20）对敏感信息的传输使用应用程序级（蓝牙协议栈的顶端）认证和加密。

（21）使用如如生物识别技术、智能卡、双因素认证或公钥基础设施（PKI）完成用户认证。

如果使用了移动设备管理方案，应确保蓝牙安全策略在该方案中正确实施。

* 1. 操作建议

（1）不使用蓝牙设备时，应关闭它们。

（2）尽可能少的执行配对，最好在一个安全的地方进行配对，在这个地方攻击者不能实际地观察输入口令和拦截蓝牙配对信息。（注：“安全区”的定义是非公共区域，室内远离窗户的位置，在物理上可控制访问的地方）用户不应对任何请求PIN码的消息做出响应，除非用户已建立一个对，并确定PIN请求来自用户设备。

（3）BR/EDR服务级的安全模式（即安全模式2或4 ）应只用于已经控制并且已充分了解的环境。

（4）确保为具有蓝牙接口的便携式设备设定一个密码 。

（5）如果一个蓝牙设备丢失或被盗，用户应立即从所有其它与它曾配对的蓝牙设备中解开配对。

（6）如果开启蓝牙的主机支持安装安全软件，那么应安装杀毒软件。

（7）充分测试并部署蓝牙软件补丁，定期升级。

（8）用户不应该接受来自未知或者可疑设备的任何形式的传输，这些传输的形式包括消息，文件，和图片。

（9）在部署前充分了解其产品和安全特征。

（10）指定一人追踪蓝牙安全产品和安全标准的进展（可能是通过蓝牙技术联盟）以及该技术的威胁和漏洞。

附录A

(资料性附录)

蓝牙漏洞与威胁

A.1 蓝牙漏洞

表A.1 蓝牙固有的核心安全问题

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 安全问题或漏洞 | 备注 | | 影响的版本 |
| 1 | 基于单元密钥的链路密钥是固定的，在每次配对中重用 | | 使用单元密钥的设备将和每个与之配对的设备使用相同的链路密钥。这是一个严重的加密密钥管理漏洞 | v1.0  v1.1 |
| 2 | 使用基于单元密钥的链路密钥可导致窃听和欺骗 | | 当设备的单元密钥泄露之后（即在它第一次配对时），那么任何其他设备都可以欺骗该设备或者任何与之相连的设备。此外，不管是否加密，该设备的链路可被窃听 | v1.0  v1.1  v1.2 |
| 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v2.0版本和稍早的设备，推荐使用安全模式3（链路级别安全）。 | v1.0  v1.1  v1.2  v2.0 |
| 4 | 使用较短的PIN码 | | 保护链路密钥产生的脆弱PIN码可被轻易的破解，而人们倾向于使用短小的PIN码 | v1.0  v1.1  v1.2  v2.0 |
| 5 | 缺乏PIN码管理 | | 在一个用户众多的企业网络中里产生充足的PIN码可能较困难，扩展性问题经常导致安全问题产生。目前比较好的方法是由配对设备中的随机数产生器来生成PIN码 | v1.0  v1.1  v1.2  v2.0 |
| 6 | 加密密钥在使用23.3小时之后仍重复使用 | | 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小时，时钟值会被重置，因此生成的密钥流将和早期连接中使用的密钥流相同 | v1.0.  v1.1  v1.2  v2.0 |
| 7 | Just Work模式在配对时不提供MITM攻击保护，这将导致不可靠的链路密钥 | | 为了更高的安全性，设备在SSP过程中应当需要MITM攻击保护，拒绝使用由Just Work配对产生的不可靠链路密钥 | 2.1  v3.0  v4.0  v4.1  v4.2 |
| 8 | SSP ECDH密钥对是固定的或者很脆弱 | | 弱ECDH密钥对削弱了SSP的窃听保护，这可能使得攻击者确定链路密钥。所有的设备应该拥有唯一健壮的ECDH密钥对 | v2.1  v3.0  v4.0  v4.1  v4.2 |
| 9 | 固定的SSP密钥容易造成MITM攻击 | | 在SSP过程中，密钥提供MITM保护。设备应在每次的配对中使用随机唯一的密钥 | v2.1  v3.0  v4.0  v4.1  v4.2 |
| 10 | 安全模式4的设备（即v2.1版本及稍后版本）降低自己的安全模式与不支持安全模式4的旧设备（即v2.0版本及以前版本）进行相连 | | 最差情况是设备降低到安全模式1，即没有安全保护 | v2.1  v3.0  v4.0  v4.1  v4.2 |
| 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。蓝牙标准通常要求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，所以攻击者可以收集大量的挑战回应（使用秘密链路密钥加密过），从而可以收集链路密钥的信息 | All |
| 12 | 用于广播加密的主密钥在微微网中所有的设备共享 | | 密钥由多方共享可导致伪装攻击 | v1.0  v1.1  v1.2  v2.0  v2.1  v3.0 |
| 13 | 蓝牙BR/EDR加密使用的E0流密码算法较弱 | | 低功耗蓝牙中使用AES-CCM算法 | v1.0  v1.1  v1.2  v2.0  v2.1  v3.0  v4.0 |
| 14 | BR/EDR模式中，与特定用户关联的蓝牙设备地址（BD\_ADDR）被捕获，可能导致隐私泄漏 | | 当BD\_ADDR关联到一个特定的用户，那么该用户的行为和地址就可被跟踪 | v1.0  v1.1  v1.2  v2.0  v2.1  v3.0 |
| 15 | LE模式中，与特定用户关联的蓝牙地址被捕获，可能导致隐私泄漏 | | 对于低功耗来讲，可以通过实施地址隐私以减少这种风险 | v4.0  v4.1  v4.2 |
| 16 | 设备认证采用简单的共享密钥挑战/响应 | | 单向挑战/响应身份验证会受到MITM攻击。 蓝牙提供双向验证，用于验证设备是否是合法的 | v1.0  v1.1  v1.2  v2.0  v2.1  v3.0 |
| 17 | LE模式配对不提供防窃听保护 | | 如果成功，窃听者可以捕获在低功耗配对期间分发的密钥（即LTK，CSRK，IRK） | v4.0  v4.1 |
| 18 | LE安全模式1/1级不要求任何安全机制（即不进行身份验证或加密）。 | | 类似于BR / EDR安全模式1，这本质上是不安全的。 强烈推荐LE安全模式1/4（加密和认证配对）。 | v4.0  v4.1  v4.2 |
| 19 | 链路密钥存储不当存储 | | 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 | All |
| 20 | 挑战应答伪随机数生成器的强度未知 | | 随机数生成器器（RNG）可能产生静态固定的或周期性数字，将减少认证模式的有效性。蓝牙实现应该使用强PRNG | All |
| 21 | 加密密钥长度是可协商的 | | v3.0标准允许设备协商加密密钥，加密密钥最小可为一个字节。低功耗蓝牙需要至少7字节的密钥。推荐在BR/EDR（E0）和LE（AES-CCM）中使用128位密钥长度 | v1.0  v1.1  v1.2  v2.0  v2.1  v3.0 |
| 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），可以由应用开发者通过覆盖加入 | All |
| 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 | All |
| 24 | 有限的安全服务 | | 审计，不可否认性和其他的一些服务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以覆盖方式嵌入 | All |
| 25 | 可发现或可连接的设备容易受到攻击 | | 设备为了完成配对，必须进入发现模式或者连接模式，这一过程应该尽可能在最短时间内完成。任何设备都不能一直处于这两个模式中 | All |
| 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在可信设备之间传输的数据。低功耗设备应在安全的环境中进行配对，以尽量减少窃听和MITM攻击的风险。 Just Works配对不能用于低功耗。 | v4.0  v4.1  v4.2 |
| 27 | 使用两个已配对的BR / EDR / HS设备，安全模式3和4可能并不总是发生双向认证 | | 如果设备A已经配对，如果设备A是认证发起者B，加密设置将在初始认证之后开始，加密设置的成功程度足以满足B的要求，以至于B无法尝试认证A | v1.0  v1.1  v1.2  v2.0  v2.1  v3.0 |

A.2 蓝牙威胁

蓝牙及其相关的设备易受无线网络威胁，比如拒绝服务攻击、窃听、消息篡改及资源盗用等，也容易受到蓝牙相关的特定威胁，列举如下：

1. 蓝牙诱捕：攻击者利用早期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（IMEI）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IMEI码将受害用户设备上的所有来电转接到攻击者的设备。
2. 蓝牙劫持：对开启了蓝牙功能的移动设备（如手机）进行攻击。攻击者通常通过向受害蓝牙设备的用户发送消息发起蓝牙劫持攻击。该消息并不会直接导致用户蓝牙设备受到侵害，而是诱使用户以某种方式作出回应或在设备地址薄中添加新联系人。类似于对电子邮件用户进行的垃圾邮件和网络钓鱼攻击，当用户响应一个恶意的蓝牙劫持消息时，可能遭受损害。
3. 蓝牙窃听：攻击者利用某些早期蓝牙设备的固件漏洞获取对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、以及修改其它设备服务。
4. 汽车窃听：通过一款软件工具，利用安装在汽车上的免提蓝牙车载套件中的一个关键问，攻击者将音频传输到汽车喇叭，并从车内的麦克风接受（窃听）声音。
5. 拒绝服务攻击： 蓝牙易受DoS攻击。其影响包括使设备的蓝牙接口不可用和耗掉移动设备的电池。这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。
6. Fuzzing攻击： 蓝牙Fuzzing攻击包括发送畸形或者不标准的数据给设备蓝牙设备，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。
7. 配对过程窃听：PIN配对方法（蓝牙v2.0和稍早版本）和LE配对方法（蓝牙4.0版本）容易受到窃听攻击。如果窃听者收集到所有的配对包，那么就可以确定密钥，从而就可伪装成可信设备，并进行主动或被动的数据解密。
8. 安全简单配对攻击：Just Work SSP没有提供抵抗MITM的保护，而存在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。

参 考 文 献

1. Bluetooth Special Interest Group, Bluetooth specifications. https://www.bluetooth.org/Technical/Specifications/adopted.htm
2. Bluetooth Special Interest Group, “Bluetooth Security White Paper”, May 2002. http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth\_24Security\_Paper.pdf
3. Padgette J. Guide to bluetooth security[J]. NIST Special Publication, 2017, 800: 121.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

1. C. Gehrmann, J. Persson, and B. Smeets, Bluetooth Security, Artech House, 2004
2. Defense Information Systems Agency, “DoD Bluetooth Peripheral Device Security Requirements”, 16 July 2010 http://iase.disa.mil/stigs/downloads/pdf/dod\_bluetooth\_requirements\_spec\_20100714.pdf
3. National Security Agency, “Bluetooth Security Factsheet”, December 2005 http://www.nsa.gov/ia/\_files/factsheets/I732-016R-05.pdf
4. Y. Lu, W. Meier, and S. Vaudenay, “The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption”, http://lasecwww.epfl.ch/pub/lasec/doc/LMV03.pdf
5. Y. Shaked and A. Wool, “Cracking the Bluetooth PIN”, In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys), pages 39–50, Seattle, WA, June 2003. http://www.usenix.org/event/mobisys05/tech/full\_papers/shaked/shaked.pdf