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)