消费级物联网安全基线

小米AIoT安全实验室

2021.12

目　录
Contents

前　言

近年来，随着科技的发展，以及消费者对智能生活日益增长的消费升级需求，物联网（IoT）设备市场也开始蓬勃发展。从产品数量来看，根据 Statistics 的调研报告，预计 2021 年 IoT 设备数量将超过 310 亿，2025 年将超过 750 亿；从市场价值来看，根据 IoT analystic 的调研报告，2019 年，IoT 市场空间 170 亿美元，预计到 2025 年，IoT 市场空间将超过 810 亿美元；从 IoT 设备所产生的数据来看，根据 IDC 的调研报告，2018–2025 年间，由 IoT 设备产生的数据量将以 28.7% 的复合年增长率增长，预计到 2025 年，IoT 设备数据将达到 79.4ZB。

IoT 市场如此迅猛的增速，意味着物联网设备将迅速进入人们的日常生活并广泛应用于各种场景。不同于传统家电，消费级物联网设备具有感知物体、信息传输、智能处理的特点，其本质是互联网在用户各种生活场景的延伸，因此在方便人们生活的同时，也不可避免的会收集、传输、存储、处理大量的用户个人信息甚至个人敏感信息。国内外的监管机构与国际标准化组织也相继发布了针对 IoT 产品的安全与隐私法律法规和标准规范；与此同时，消费者对 IoT 设备的安全与隐私保护能力的要求也越来越高。

在 IoT 设备数量急速增加，所产生的数据急剧增加，监管，标准组织和用户对产品安全与隐私保护的关注度不断增加的背景下，企业应如何保证物联网设备的安全与隐私，让用户，监管和合作伙伴放心，信任其物联网产品，保障产品合规发展，成了企业首要解决的问题。但当前国内缺少一份可被公开查询、可落地的消费级物联网终端安全基线指南，来帮助企业提升其 IoT 终端产品的安全与保护能力。

小米 AIoT 安全实验室根据多年的安全测试经验积累、并结合国内外法律法规和标准规范，制定了本基线指南。本指南意在帮助国内物联网企业，在应对以上安全挑战时，可以有一个开放，便捷，落地的知识库，让企业在设计和开发消费级物联网终端产品时，可以对照此指南，规避一些基本的安全与隐私保护风险，以快速提升产品的安全与隐私保护能力。

范围

本基线主要描述了针对消费级物联网终端设备的安全基线要求。

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。

ETSI EN303645 《消费级物联网信息安全基本要求》

Cyber Security for Consumer Internet of Things: Baseline Requirements

GB/T35273-2020《信息安全技术 - 个人信息安全规范》

Information security technology—Personal information security specification

Regulation (EU) 2016/679《通用数据保护条例》

General Data Protection Regulation

01

设备硬件

1.1 物理调试接口

1.1.1 调试接口默认关闭

消费级物联网设备（下文简称“设备”）应在出厂时默认关闭 UART、JTAG、SWD 等调试接口。如因售后问题分析等原因需开启调试接口，应按需飞线通联或根据设备传感器等能力，做出特殊操作后开启（如特殊按键组合、私有 USB Dongle 串接使用、设备倾斜通电等），以减少不必要的物理调试接口暴露和信息传输。

1.1.2 PCB 板上调试接口丝印

设备应去除 PCB 板上的调试接口丝印（如明显的 TX、RX），以防止逆向工程。

1.1.3 调试接口默认关闭信息输入

调试接口因某些特定需要而开启后，默认不应开放调试接口的信息输入，防止设备固件被篡改或本地存储的敏感信息被读取。

1.1.4 调试接口打印敏感数据

调试接口在某些特定需要而开启后，应仅允许进行不包含用户与设备敏感信息的 log 输出（敏感信息包含敏感安全参数如 key、token，和个人敏感信息如 password、Wi-Fi 密码等，详见附录 C 个人敏感信息），如需输出完整数据流日志，需要将此类信息遮蔽展示（如：password：********）

1.2 本地数据存储

1.2.1 敏感信息加密

设备应将敏感信息加密存储在存储芯片（flash、nand、emmc 等），加密方案可通过采用集成安全芯片或操作系统分区加密来实现。

1.2.2 芯片读保护

设备 MCU 应开启芯片读保护机制，如尝试通过调试接口读取芯片内容 / 内存时报错等，以防止通过调试接口非授权读取设备信息。

1.3 通信链路数据传输

设备宜对硬件通信链路（IIC/SPI）中传输的通信数据本身进行加密。宜采用安全芯片来确保加密密钥的安全性，并结合真实与伪数据融合发送的机制，以防止攻击者通过硬件通道嗅探得到协商密钥以及芯片指令。

图 1 – 安全芯片

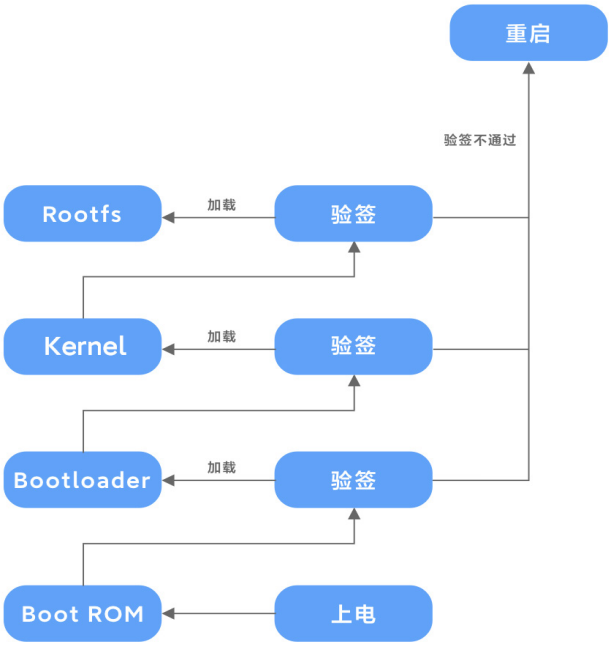

图 2 – 安全启动

1.4 安全启动

设备芯片宜支持安全启动（SecureBoot 原理如图），启动时对固件（uboot、kernel、rootfs）或 Flash 关键分区进行合法加载校验，确保存储芯片中的系统合法性和完整性校验通过后才能正常启动。

1.5 防物理拆除

室外（公共区域：如大门外）设备宜具备在受到暴力移除或拆卸时的防护或预警机制：

- 外壳防拆除：设备不宜暴露可以将设备部分或全部拆除的螺丝孔或卡扣，设备室外外壳宜采用一体式结构设计；如因业务需要必须暴露螺丝或卡扣的，宜采用非常用类型固定螺丝来固定设备，并使用强度结构符合要求的结构胶对外壳螺丝封胶防护，以防止设备从室外被轻易拆除。
- 电子组件结构防护：设备具有控制功能的电子组件（包括但不限于 MCU，接口，线路）应具有足够强度的结构保护，如把此类电子组件设计在设备的室内部分，防止设备室外外壳被拆除后直接暴露。
- 拆除警报：如设备传感器具备检测设备被拆解的能力，宜发出警报铃声，记录并上报拆除事件至设备管理员。

注：门锁、门铃设备应满足此要求的所有内容。

1.6 防强电磁攻击

高安全等级设备应在芯片外加装电磁防护罩，以防止强电磁脉冲（EMP）攻击造成的设备逻辑或运行异常，进而导致逻辑错误，设备宕机或电路烧毁（如门锁设备遭遇强电磁攻击后可导致非授权开锁）。

1.7 智能门锁锁芯及门卡

- **真插芯**

智能门锁（真插芯）应将离合组件放置于门内锁体中，以保证即使外部锁体被破坏或舵机电平被控制时，锁芯依然空转无法解锁。防止智能

门锁锁芯被暴力或专用工具（已有专业开锁工具）通过外部锁体缝隙劫持锁芯开锁。强烈建议智能门锁产品采用真插芯，并且宜采用 C 级锁芯。

- **假插芯**

智能门锁（假插芯）应在钥匙孔与锁芯机关间用金属格挡并固定，门外锁体与门之间应用金属挡板全部封闭，以防止他人通过钥匙孔、锁体缝隙触动开锁机关开锁。

- **NFC**

智能门锁应使用 CPU 卡作为开锁门卡，不应使用易被嗅探、破解复制的 ID 卡或 M1 卡开锁。

卡类型	优点	缺点	推荐
CPU 卡	安全性高，用户空间大，读取速度快	价格稍贵	推荐使用
ID 卡	价格便宜	容易复制，安全性低	不应使用
M1 卡	可读可写	易被嗅探、破解并复制，价格稍贵	不应使用

1.8 设备唯一标识防篡改

设备端应存储唯一硬件标识，并采用一次性编程、安全芯片等技术防止被篡改。

02

设备软件

2.1 软件更新

2.1.1 固件升级包完整性与合法性

设备固件升级（OTA 远程或本地升级）前应先对固件包进行完整性哈希得到固件包摘要，再使用公私钥方式对摘要进行合法性签名和验签（可参考 Nordic 例程[1]），确认升级包完整性与合法性再进行更新，以防止固件包被篡改或替换。

固件升级包完整性哈希应采用安全的哈希算法（详见 5.1 加密与哈希算法），完整性凭据应在设备与服务端的加密通信通道内传输。

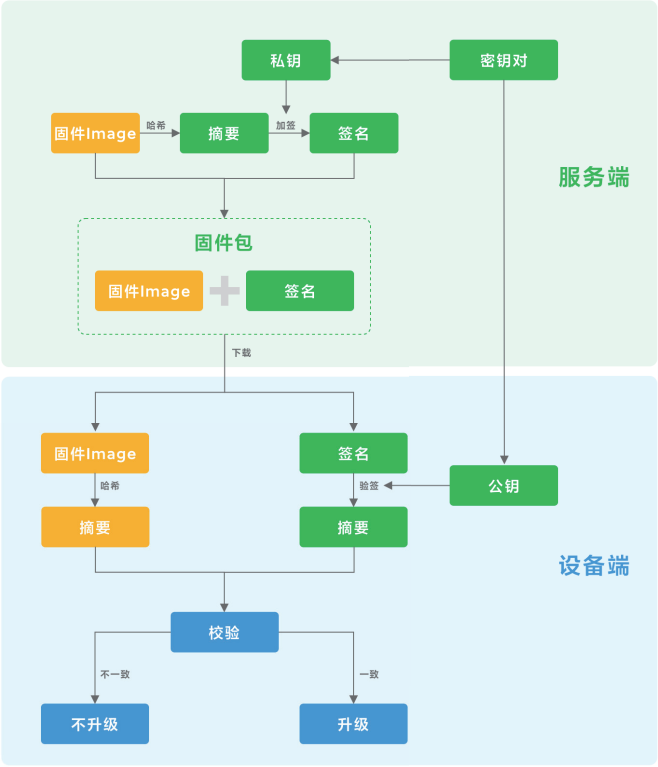

图 3 – 固件升级包合法性与完整性校验

2.1.2 防固件降级

通过 OTA 功能进行设备更新时，设备应拒绝旧版固件更新，以防止一些历史 BUG 或安全风险重新暴露被利用。特殊需求下（如：测试、维修等），可以通过 SD 卡或线刷等方式对固件验签后刷机。

2.1.3 软件更新失败后恢复机制

设备软件更新时可能遇到断电等特殊情况，导致设备升级失败。因此设备应具备 OTA 双分区备份机制，保障升级失败时能恢复到可用软件版本，防止升级失败损害设备可用性。

2.1.4 局域网 OTA 升级

设备应默认关闭局域网 OTA 升级能力，如需开启应满足 2.1.1 固件升级包完整性与合法性要求，以防止攻击者通过局域网对设备进行恶意固件 OTA 升级。

2.1.5 第三方组件更新

设备制造商在产品开发过程中应维护产品软硬件的第三方商用及开源组件清单，并将其用于持续监测已识别的软硬件组件的相关安全。

设备使用到的第三方软件 / 库应使用最新版本，如特殊需求不能使用最新版本，应经过安全评估。在明确安全漏洞的情况下，应及时更新到最新修复版本。

注：软件 / 库漏洞可前往：https://www.cvedetails.com/product-list.php 查询。

2.1.6 MCU IAP 更新机制

支持线刷设备的 MCU 应具备安全更新机制，如封装专用的 USB Dongle 确保对 MCU 的 IAP 过程进行了数据加密或签名验证，以避免 MCU 固件逻辑被篡改的风险。

2.2 服务与端口最小化

设备应默认关闭 FTP、SSH、Telnet、HTTP、ADB 等高风险管理服务或信息数据服务，也应关闭非数据交互与控制实现所必要的 IoT SDK 控制服务端口。

2.3 代码库管理

设备相关代码库不应在未经允许的情况下上传至 Github、Gitee 等公用代码仓库或百度网盘等公开、半公开服务，防止源代码泄露。

03

设备 OS

3.1 通用 OS

3.1.1 Bootloader 启动

设备 BootLoader 不应在系统启动前预留中断时间，Delay 需设置为 0，防止通过修改启动参数进入 SHELL 界面获得设备控制权。

当设备操作系统引导加载程序（Bootloader/U-Boot）启动异常后，设备操作系统应自动重启，避免启动异常后暴露操作系统引导加载控制台（Console）界面，以防止攻击者通过错误植入进入到控制台界面，来获得篡改设备启动参数的权限，从而控制设备。

3.1.2 用户账户密码（有登录 UI）

对具有用户注册 / 登录界面的设备，如果用户注册 / 登录设备的用户账户 / 管理后台预置了默认密码，则该密码应为随机生成且一机一密的高强度密码，并在用户首次登陆时强制要求修改默认密码；如果设备不为用户注册 / 登录设备的用户账户 / 管理后台预置默认密码，则设备应要求用户注册或首次登录时自行设置高强度密码。

高强度密码：长度为 10-14 位，包含大写字母、小写字母、符号和数字其中三类字符的密码。

3.1.3 防暴力破解

设备登录密码应具备暴力破解机制，如验证码等人机交互机制、登录验证失败递增等待时间和登录验证失败超过一定次数锁定账号等。

3.1.4 验证输入数据

设备应验证通过用户界面和 API 接口输入的数据，以防止设备执行外部恶意攻击代码。数据验证方法包括过滤超出处理范围的数据、过滤和转义非预期的数据类型，及部署 fuzz 工具检测程序是否存在输入数据验证不足而出现的潜在漏洞等。

3.1.5 特权功能接口

设备应默认关闭可直接进入设备系统的特权能力或接口（如工厂 OTA、未公开功能接口、调试后门等），如实属业务必要，应具备鉴权机制。

3.2 嵌入式 Linux OS

3.2.1 串行端口绑定 SHELL

设备不应将系统 SHELL 绑定在 UART 等串行调试接口，防止通过接线获取设备控制权。如有特殊需要，需满足 3.2.2 要求。

3.2.2 系统默认账户密码（无登录 UI）

嵌入式 Linux 系统默认用户（如 root、admin 等）需设置高强度密码，并且保证一机一密，不应在代码中为所有设备写入相同密码或空密码。

高强度密码：长度为 10–14 位，包含大写字母、小写字母、符号和数字其中三类字符的密码。

3.2.3 基础文件系统权限

设备嵌入式 Linux 的基础文件系统（如 /etc/ 等存有启动项的目录）应使用只读文件系统（如 squashfs），以防止攻击者在篡改运行状态的操作系统。

3.2.4 外部存储的程序和脚本

设备嵌入式 Linux 操作系统默认不应运行外部存储（SD 卡、U 盘、网络存储等）中程序或脚本。如有特殊需要，应进行公私钥签名验证，以防止系统被植入恶意软件或脚本。

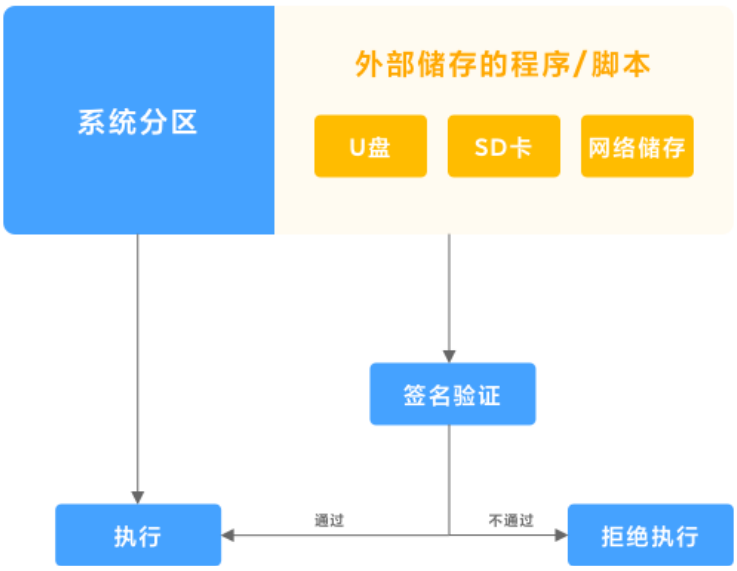

图 4 – 外部程序和脚本签名验证

3.2.5 地址空间布局随机化

嵌入式 Linux 系统的设备应开启地址空间布局随机化（ASLR）保护措施，以防止缓冲区溢出。

开启方式：在 /etc/sysctl.conf 中添加kernel.randomize_va_space = 2（Kernel >=2.6.12）
参数 2 代表除了库与栈外，堆也进行随机化保护，但需要注意，ASLR不负责代码端以及数据端的随机保护，
该项工作需要通过编译器PIE 实现，参见： 3.2.6

3.2.6 基址随机加载保护

应用应开启 PIE 应用基址随机加载保护选项。

> 方法：gcc 编译参数-pie -fPIE（注意大小写），同时需要系统 ASLR 支持，参见：3.2.5

3.2.7 栈 Cookie 防溢出

在编译 Linux 程序代码时，应开启 Linux 程序的 CANARY 栈溢出保护选项。

> 开启方法：添加gcc编译参数 -fstack-protector-all

3.2.8 栈不可执行

在编译 Linux 程序代码时，应开启 Linux 程序的 NX 栈不可执行保护选项。

> 开启方法：添加gcc 编译参数 -z noexecstack

3.2.9 删除调试符号表

在编译 Linux 程序代码时，需使用 Strip 函数删除调试符号表，以提升逆向分析难度并减少程序体积。

04

设备通信

4.1 通用通信

4.1.1 密钥硬编码

设备不应将用于传输加密或鉴权的密钥硬编码在程序代码中，应采用一机一密（PSK）或通过 PSK 密钥导出等方式生成密钥。

4.1.2 通信信道加密

设备应将与其他设备或应用通信的信道进行加密，并在会话结束时及时销毁会话密钥。针对不同通信方式的加密方案可参考 4.2，4.3，4.5

4.1.3 通信双向认证

设备通信时应在数据传输之前进行双向认证，验证双方真实身份是否合法，检查控制权限是否与身份匹配，以防止越权或非授权控制。设备应使用以下列举的米家标准双向认证通信协议，如因特殊原因需使用非标准协议的，应经过安全评估。

- 设备验证服务端：

以太网设备通过米家 OTS 协议（基于 TLS/DTLS）与服务端通信时会先向 CA 校验服务端证书是否合法。

蓝牙设备通过米家蓝牙安全认证协议绑定流程中的 OOB 信息验证服务端 /APP 是否合法。

- 服务端验证设备：

服务端通过校验设备的三元组信息（中、低安全等级设备）或米家安全芯片中的设备唯一标识（高安全等级设备）验证设备身份是否合法。

4.1.4 防重放

设备通信应使用滚动码或计数器机制，当请求操作计数大于设备计数才准许设备执行该操作指令，以防止他人通过抓包重放控制请求来对设备进行非授权的控制。

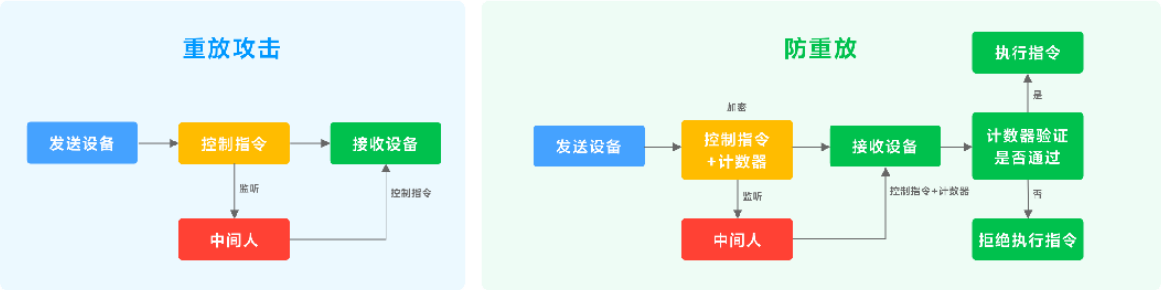

图 5 – 重放攻击和防重放

不同通信协议下的防重放可参考以下方案：

- **ZigBee：**设备应开启 Zigbee 协议帧计数器（framecounter）

  开启方法：设置 nwkAllFresh 为 TRUE

- **射频：**设备使用滚动码方式进行通信，参考 keeloq、DST40、Hitag2 等业界成熟方案[2]

- **Wi-Fi：**采用 HTTPS TLS1.2+ 传输协议默认支持的数据包序列号计数器防重放功能

- **蓝牙：**采用米家蓝牙认证协议默认支持的帧计数器和加密功能，或采用标准 BLE SM（Security Manager）模块的数据包计数器（packetCounter）和链路层加密

4.1.5 非授权通信协议

设备使用的通信协议应经过安全评估，不应使用非授权通信协议，以防止非授权协议存在安全漏洞或后门影响设备通信安全。

4.2 以太网

4.2.1 通信信道加密

设备应使用加密的传输协议对通信进行加密，应采用 TLS（1.2+）传输协议的安全加密套件。避免因使用 MQTT、HTTP 等明文传输协议而导致信息泄露或被篡改的风险。

注：TLS 加密套件的安全性可在 https://ciphersuite.info/cs/ 查询。

4.2.2 敏感信息传输加密

设备在传输敏感信息时应使用安全的加密算法对敏感信息进行额外的加密。

注：加密算法的安全性可参考 5.1 加密与哈希算法。

4.2.3 HTTPS 证书校验

设备使用 HTTPS 协议时，应进行严格的证书校验，不能忽略检查。

- Linux 系统

设备应严格验证服务端证书合法性，不应使用参数跳过证书验证或忽略证书验证错误。

工具 / 库	参数使用建议
curl	不应使用 -k 参数
wget	不应使用 --no-check-certificate 参数
libcurl	应将 CURLOPT_SSL_VERIFYPEER 和 CURLOPT_SSL_VERIFYHOST 设置为 True

- Android 系统

设备应用使用 SSL 加密通信服务应严格校验服务端和客户端证书，不应信任任意证书，不应忽略异常事件（如 return 空或者 null）；如需自定义 SSLx509 TrustManager，重写 checkServerTrusted 方法，方法内必须严格判断服务端的证书校验，以防止通信内容被劫持导致通信数据泄漏或被篡改。

4.2.4 Wi-Fi 接入点口令

设备使用 WiFi Direct 接入点与控制应用连接的功能应严格评估必要性，如确有必要，设备端 WiFi Direct 接入点口令不应使用固定密码或空密码，应遵循一机一密或者每次使用真随机生成密码，并显示在屏幕上（带屏设备）或在绑定时由用户提前设置并存储（无屏设备），以防止 Wi-Fi 被非法接入。

4.2.5 Wi-Fi 接入点用途

设备建立的 Wi-Fi 接入点应只允许与设备本身通信，不应访问设备外部网络（如家庭网或互联网），以防止攻击者通过设备 Wi-Fi 向家庭网渗透。

4.3 低功耗蓝牙（BLE）

4.3.1 蓝牙配对

有物理按键的蓝牙设备应通过物理按键进行绑定确认或开启绑定窗口，以避免设备重复绑定或在用户不知情的情况下被他人绑定的风险。

4.3.2 蓝牙控制指令合法性校验

对于支持蓝牙的设备，应每次登录协商会话密钥，设备与控制应用间应使用会话密钥加密传输控制指令。

4.3.3 传感器设备蓝牙广播

部分设备通过蓝牙将传感器采集的数据进行广播传输，通过蓝牙网关解析广播内容进行设备联动，或根据广播数据作为控制指令，从而影响其他设备。此类设备的蓝牙广播应使用安全的通信协议，并使用绑定时产生的 beaconkey 对广播数据内容进行加密。

4.3.4 蓝牙 mesh 协议

蓝牙 mesh 设备应使用安全的通信协议与 mesh 设备、网关及手机进行双向认证，对传输的敏感数据使用会话密钥加密。

4.3.5 蓝牙协议版本

低功耗蓝牙 BLE 设备（如鼠标、音箱）采用蓝牙链接层加密时应使用 4.2 及以上低功耗蓝牙协议版本，以防止设备在绑定阶段泄露蓝牙连接层密钥（LTK），从而导致隐私泄露或设备伪造的风险。

4.3.6 蓝牙控制指令鉴权

设备使用蓝牙芯片厂商提供的 OTA 例程指令前应判断控制应用的蓝牙绑定状态，防止因例程中可能支持未授权指令控制设备的逻辑，从而导致设备拒绝服务（例如芯片重启、切换工作空间、进入 DFU 升级模式等等）的风险。

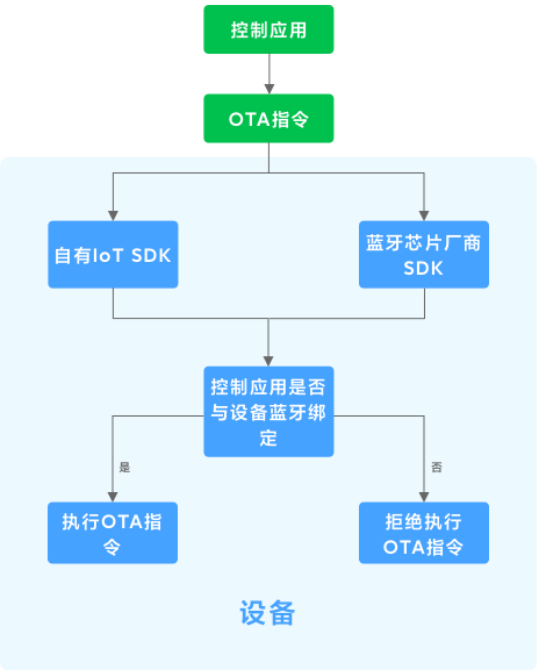

图 6 – 蓝牙控制指令鉴权

4.3.7 蓝牙广播防追踪机制

设备宜使用随机蓝牙 MAC 地址，并对蓝牙广播内容进行加密；如需通过 beacon 信标广播可识别身份的信息，应定时变换设备蓝牙 MAC 地址，以防止他人通过部署足够多的探测设备对广播内容进行分析，并跟踪设备的移动轨迹。

4.3.8 蓝牙敏感信息通信

设备在使用 BLE 与控制应用（安卓）通信时，应对敏感信息内容本身进行应用层加密，以防止用户使用 BLE 将手机与其他智能设备配对进行数据传输时，手机上的所有应用都可以访问这两个设备间传输的数据。

In contrast to Classic Bluetooth, Bluetooth Low Energy (BLE) is designed to provide significantly lower power consumption. This allows Android apps to communicate with BLE devices that have stricter power requirements, such as proximity sensors, heart rate monitors, and fitness devices.

Caution: When a user pairs their device with another device using BLE, the data that's communicated between the two devices is accessible to **all** apps on the user's device.

For this reason, if your app captures sensitive data, you should implement app-layer security to protect the privacy of that data.

风险描述参见安卓 4.3 引入蓝牙 BLE 时的开发文档[3]:

4.4 Zigbee

4.4.1 Zigbee 协议版本

Zigbee 设备应使用 Zigbee 3.0 协议栈版本，并使用官方 install code 方案[4]，以防止攻击者利用旧协议版本的默认 TCLK 密钥进行攻击。

4.5 射频

4.5.1 射频通信数据包序列号长度

设备的射频通信数据包应使用四字节作为序列号变量空间，避免使用较短序列号长度，以防止通信内容可在短时间暴力破解的风险。

4.5.2 通信密钥硬编码

设备射频通信密钥应通过发射器和接收器配对交换生成，不应预置密钥在代码中。

4.5.3 通信频率

设备应使用跳频机制进行通信，以防止因射频通信频点固定造成信道拥堵，导致设备无法正常通信。

05

数据安全与隐私

5.1 加密与哈希算法

● **加密算法：**设备应使用安全的加密算法且密钥长度符合对应算法的最低要求（见下表），不应使用 DES、TDES、RC4 等不安全加密算法。

● **哈希算法：**设备应使用 256 bit 以上的安全 hash 函数，如 sha256，sha512 等，不应使用已有安全风险的 hash 函数，如 md5 或 sha1。

算法	**密钥 / 哈希值 长度（bit 位）**
AES	128 / 192 / 256
ECDSA / ECDH	256/384/512
RSA	2048 /3072/ 4096
DSA	Prime P: 2048 /3072/4096
	Prime Q: 256/384/512
SM4	128
SHA	256/384/512

5.2 随机数生成函数

设备系统及应用应使用真随机或强伪随机算法产生认证或加密所需的随机数。

类型	**生成方式**	**建议**
真 / 强伪随机	/dev/urandom 芯片支持的熵随机能力	推荐
伪随机	srand()、rand() 并使用 time(0) 为种子生成	不推荐

5.3 日志上报

设备、系统及应用打印的日志不应上传任何明文或加密的敏感信息(如Wi-Fi SSID、密码、手机 IMEI、地理位置等敏感信息)。如经评估需要上报使用，应在隐私声明中明示作用与存储方式。

5.4 跨境网络请求

设备或控制应用应识别当前用户所属国家或地区，根据不同国家或地区的隐私合规要求发送网络请求，以防止数据跨境传输带来的隐私风险。

5.5 云端存储安全

通过设备采集的用户敏感数据（视频、音频、图片、文档等）应加密存储于业务云端存储服务器。

5.6 云端数据删除功能

物联网平台应向用户提供便捷的删除云端数据的功能，删除范围包括用户在使用设备及其关联服务过程中产生并存储在云端的个人信息。

5.7 恢复出厂设置

设备恢复出厂设置后应完全清除设备中所有用户数据、设置（如用户使用记录、设置、NFC 门卡、eSIM 卡记录等）。

06

业务逻辑

6.1 设备可绑定状态

未绑定设备上电 30 分钟后仍未绑定应关闭待绑定状态，待重新上电后重新进入绑定状态，避免设备始终允许接受绑定请求而被恶意绑定的风险。

6.2 绑定确认

室内高安全级别设备绑定时宜在产品能力允许的情况下，要求用户在设备端进行绑定确认；室外交通工具和室外高安全级别设备（如滑板车、门铃、门锁、室外监控摄像机）应使用 OOB 绑定方式，防止设备被恶意绑定。

6.3 防重复绑定

对于具备重置能力的设备，应被重置后才可再次接受绑定请求，以防止被其他用户重复绑定或恶意绑定控制。

6.4 强绑定关系

室外高安全级别设备应在云端将设备和账户建立强绑定关系，即云端记录设备 ID 与用户 ID 的绑定关系。设备绑定时应先验证云端记录，仅允许在云端没有绑定记录的设备的绑定请求，并且设备端重置不应清除云端绑定记录，仅当设备所有者（在云端有绑定记录的用户 ID）在控制端应用上主动解绑时才清除绑定关系，以防止设备重置后被非法绑定控制。

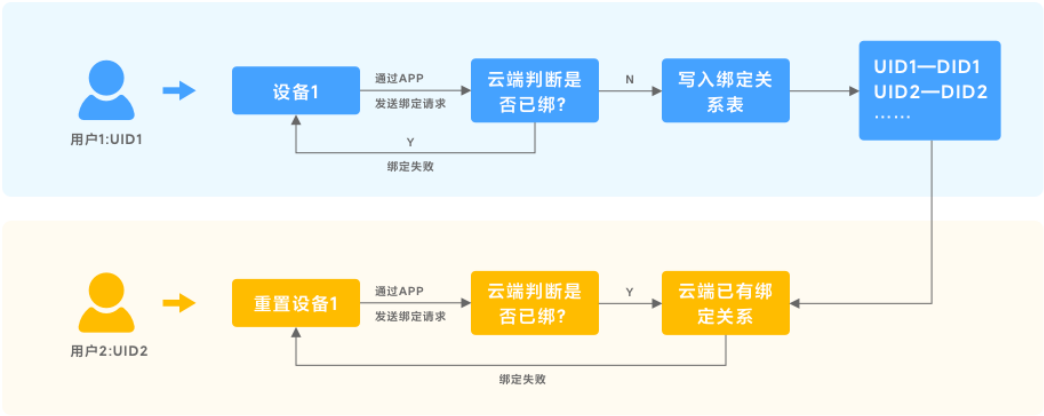

图 7 – 强绑定

6.5 设备日志安全监控

物联网平台应从设备端收集关键日志（如设备联网状态、使用状态、升级状态等），应将此类设备日志用于安全监控。通过统计和分析日志信息发现异常，从而发现潜在的设备或物联网平台安全风险。

6.6 安全设置指南

设备如果具备安全功能，应采取以下方式之一帮助用户简便地开启这些安全功能：

- **默认设置：**设备初始化时自动默认开启必要的安全功能。

- **软件引导：**设备软件或控制应用通过软件 UI 提供相关安全功能开关和说明，或通过弹窗等形式引导用户开启。

- **说明书：**通过纸质或电子版产品安全设置指南告知用户开启产品安全功能的方式和步骤。

术语和定义

下列术语和定义适用于本文件

1 消费级物联网设备 Consumer IoT Device

网络连接（和网络连接）设备（本文简称“设备”），该规范内消费级物联网终端设备指具有无线（ Wi-Fi、BLE/Mesh、Bluetooth classic、Zigbee、NFC、RF 射频 ）、有线（ RJ45 ）联网与组网能力，或具有固件逻辑更新能力的任意智能终端产品。

注 1: 消费级物联网设备也通常用于商业环境。这些设备仍然被归类为消费级物联网设备。

注 2: 消费级物联网设备通常可供消费者在零售环境中购买。消费级物联网设备也可以委托和 / 或专业安装。

2 用户 User

自然人或组织。

3 关键安全参数 critical security parameter

与安全相关的秘密信息，这些信息被泄露或被修改后会危及智能家居安全性。例如后台系统管理员认证信息、操作系统登录认证信息，网络设备认证信息等。

4 公共安全参数 public security parameter

与安全相关的公共信息，其修改会损害安全模块的安全性。

示例 1: 验证软件更新的真实性 / 完整性的公钥。

示例 2: 证书的公共组件。

5 敏感安全参数 sensitive security parameters

公共安全参数和关键安全参数。

6 个人信息 personal data

与已识别或可识别的自然人有关的任何资料。

7 敏感信息 Sensitive information

敏感信息为敏感安全参数与个人信息的统称。

8 调试接口 debug interface

制造商在开发过程中用于与设备通信的物理接口，或用于对设备的问题进行分类 . 例如：测试点，UART，SWD，JTAG。

9 逻辑接口 logical interface

利用网络接口通过信道或端口在网络上通信的软件实现。

10 网络接口 network interface

可用于通过网络访问消费者物联网功能的物理接口。

11 物理接口 physical interface

物理端口或空气接口（如无线电、音频或光学接口），用于与物理层的设备通信，如：收音机、以太网端口、USB 等串行接口和用于调试的接口。

12 安全更新 security update

解决制造商发现或报告给制造商的安全漏洞的软件更新。

注：如果漏洞的严重程度需要更高的优先级修复，软件更新可以是纯粹的安全更新。

13 日志 telemetry

来自设备的数据，可以提供信息，帮助制造商识别与设备使用有关的问题或信息。例如：消费者物联网设备向制造商报告软件故障，使他们能够识别和补救原因。

14 鉴权 authentication mechanism

用于证明实体真实性的方法"实体"既可以是用户，也可以是机器。例如：认证机制可以是请求密码、扫描二维码或使用生物特征指纹扫描仪。

15 闪存 Flash

Flash 是存储芯片的一种，通过特定的程序可以修改里面的数据。FLASH 在电子以及半导体领域内往往表示 Flash Memory 的意思，即平时所说的"闪存"，全名叫 Flash EEPROM Memory。

16 Bootloader

在嵌入式操作系统中，BootLoader 是在操作系统内核运行之前运行，可以初始化硬件设备、建立内存空间映射图，从而将系统的软硬件环境带到一个合适状态，以便为最终调用操作系统内核准备好正确的环境。

17 U-boot

U-Boot 是一个主要用于嵌入式系统的引导加载程序，可以支持多种不同的计算机系统结构，包括 PPC、ARM、AVR32、MIPS、x86、68k、Nios 与 MicroBlaze。

18 Kernel

嵌入式内核是在嵌入式硬件和软件之间的抽象层，在 Linux 的术语中被称为"内核"，也可以称为"核心"。Linux 内核的主要模块（或组件）分以下几个部分：存储管理、CPU 和进程管理、文件系统、设备管理和驱动、网络通信，以及系统的初始化（引导）、系统调用等。

19　蓝牙信标 Beacon

蓝牙信标(Beacon)是建立在低功耗蓝牙协议基础上的一种广播协议。

20　地址随机化 ASLR

地址随机化（ASLR）是一种针对缓冲区溢出的安全保护技术，通过对堆、栈、共享库映射等线性区布局的随机化，通过增加攻击者预测目的地址的难度，以防止攻击者直接定位攻击代码位置，达到阻止溢出攻击的目的。

21　ID 卡 Identification Card

ID 卡全称为身份识别卡（Identification Card），是一种不可写入的感应卡，含固定的编号，主要有台湾 SYRIS 的 EM 格式、美国 HIDMOTOROLA 等各类 ID 卡。ID 卡与磁卡一样，都仅仅使用了“卡的号码”而已，卡内除了卡号外，无任何保密功能，其“卡号”是公开、裸露的。所以说 ID 卡就是“感应式磁卡”。

22　M1 卡 M1 card

M1 芯片卡，是指飞利浦下属子公司恩智浦出品的芯片缩写，全称为 NXP Mifare1 系列，常用的有 S50 及 S70 两种型号。常见的有卡式和钥匙扣式。

23　真插芯

智能门锁的真插芯是指锁芯直接固定在再锁体结构上，利用锁芯上的拨片直接驱动锁体，使其实现开关效果的一种组合方式，直观表现为：使用钥匙时，钥匙与门面为垂直关系。

24 假插芯

智能门锁的假插芯是将锁芯与锁体位置分离，锁芯转动时，利用齿轮箱和连接杆，将动力传送给锁体，从而实现锁体开关效果的一种新型组合方式，直观表现为：使用钥匙时，钥匙与门面为平行关系。

25 例程 Routine

例程是某个系统对外提供的功能接口或服务的集合。比如操作系统的 API、服务等就是例程。

缩略语

下列缩略语适用于本文件。

API	应用编程接口（Application Programming Interface）
IoT	物联网（Internet of Things）
IP	网络协议（Internet Protocol）
JTAG	联合测试工作组（Joint Test Action Group）
OTA	空中下载（Over The Air）
UART	通用异步收发传输器（Universal Asynchronous Receiver-Transmitter）
USB	通用串行总线（Universal Serial Bus）
SSH	安全外壳协议（Secure Shell）
MAC	介质访问控制地址（Media Access Control）
TLS	安全传输层协议（Transport Layer Security）
TCP	传输控制协议（Transmission Control Protocol）
UDP	用户数据报协议（User Datagram Protocol）
FTP	文件传输协议（File Transfer Protocol）
UID	用户名（User ID）
DID	设备标识码（Device ID）
SWD	串行线调试（Serial Wire Debug）
NAND	与非门逻辑电路（Not And）
EMMC	Embedded Multi Media Card
MQTT	消息队列遥测传输（Message Queuing Telemetry Transport）
TCLK	信任中心链接密钥（Trust Center Link Key）
ASLR	地址空间布局随机化（ASLR）
NX Stack	栈不可执行（No Execute Stack）
PIE	位置独立的可执行文件（Position Independent Executables）
OOB	带外数据（Out of Band）
XML	可扩展标记语言（eXtensible Markup Language）
AES	高级加密标准（Advanced Encryption Standard）
DES	数据加密标准（Data Encryption Standard）
RSA	一种非对称加密算法，以此算法的三位共同提出者姓氏开头字母拼在一起而命名
TX	发送（transmit）
RX	接收（Receive）
PSK	预共享密钥（Pre-Shared Key）
ADB	安卓调试桥（Android Debug Bridge）
JSAPI	JavaScript 应用编程接口（JavaScript Application Programming Interface）

附录 A

产品安全等级：

根据产品的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）收到损害时对设备、用户及物联网平台可能造成的最大影响程度，把物联网产品分为高、中、低三个安全等级。设备安全等级判断的核心关注点及对应影响等级见下表：

安全属性	关注点	影响程度			备注
		低	中	高	
保 密 性 Confidentiality	设备收集的个人信息的敏感程度越高，保密性受到损害时对用户的影响越大				
	个人基本资料	√			
	个人教育工作信息	√			
	个人常用设备信息	√			
	个人通信信息		√		
	联系人信息		√		
	个人身份信息			√	
	个人生物识别信息			√	
	网络身份标识信息			√	
	个人健康生理信息			√	
	个人财产信息			√	
	个人上网记录			√	
	个人位置信息			√	
	其他敏感信息			√	
完 整 性 Integrity	综合设备或 APP 端可能发生的恶意篡改或其他完整性被破坏的情况下，对用户人身安全、财产安全、精神上可能带来的影响程度				
	影响轻微	√			
	影响有限		√		
	影响严重			√	
可 用 性 Availability	在设备及相关服务完全不可用的情况下，对用户或在舆论上带来的影响程度				
	影响轻微	√			
	影响有限		√		
	影响严重			√	

各类个人信息及敏感信息的定义及举例见附录 C

附录 B

不同安全等级的设备需满足的要求如下：

章节	标题	低	中	高	适用条件
设备硬件	**1.1 物理调试接口**				
	1.1.1 调试接口默认关闭		√	√	
	1.1.2 PCB 板上调试接口丝印			√	
	1.1.3 调试接口默认关闭信息输入		√	√	
	1.1.4 调试接口打印敏感数据		√	√	
	1.2 本地数据存储				
	1.2.1 敏感信息加密存储		√	√	
	1.2.2 芯片读保护			√	
	1.5 防物理拆除			√	智能门锁、门铃
	1.6 防强电磁攻击			√	智能门锁
	1.7 智能门锁锁芯及门卡			√	智能门锁
	1.8 设备唯一标识防篡改			√	
设备软件	**2.1 软件升级**				
	2.1.1 固件升级包完整性与合法性	√	√	√	
	2.1.2 防固件降级			√	
	2.1.3 软件更新失败后恢复机制		√	√	
	2.1.4 局域网 OTA 升级指令	√	√	√	
	2.1.5 第三方组件更新		√	√	
	2.1.6 MCU IAP 更新机制			√	
	2.2 服务与端口最小化	√	√	√	
	2.3 代码库管理	√	√	√	
设备 OS	**3.1 通用 OS**				
	3.1.1 Bootloader 启动		√	√	
	3.1.2 用户账户密码（有登录 UI）	√	√	√	
	3.1.3 防暴力破解	√	√	√	
	3.1.4 验证输入数据	√	√	√	
	3.1.5 特权功能接口		√	√	
	3.2 嵌入式 Linux OS				
	3.2.1 串行端口绑定 SHELL		√	√	
	3.2.2 系统默认账户密码（无登录 UI）			√	
	3.2.3 基础文件系统权限		√	√	
	3.2.4 外部存储的程序和脚本		√	√	
	3.2.5 地址空间布局随机化		√	√	
	3.2.6 基址随机加载保护		√	√	
	3.2.7 栈 Cookie 防溢出		√	√	
	3.2.8 栈不可执行		√	√	
	3.2.9 删除调试符号表	√	√	√	

章节	标题	低	中	高	适用条件
设备通信	**4.1 通用通信**				
	4.1.1 密钥硬编码		√	√	
	4.1.2 通信信道加密	√	√	√	
	4.1.3 通信双向认证			√	
	4.1.4 防重放		√	√	
	4.1.5 非授权通信协议	√	√	√	
	4.2 以太网				
	4.2.1 通信信道加密	√	√	√	
	4.2.2 敏感信息传输加密		√	√	
	4.2.3 HTTPS 证书校验	√	√	√	
	4.2.4 Wi-Fi 接入点口令		√	√	依赖设备建立 Wi-Fi 热点进行连接控制 （如行车记录仪、运动相机等）
	4.2.5 Wi-Fi 接入点用途		√	√	
	4.3 低功耗蓝牙（BLE）				
	4.3.1 蓝牙配对	√	√	√	
	4.3.2 蓝牙控制指令合法性校验	√	√	√	
	4.3.3 传感器设备蓝牙广播	√	√	√	
	4.3.4 蓝牙 mesh 协议	√	√	√	
	4.3.5 蓝牙协议版本	√	√	√	
	4.3.6 蓝牙控制指令鉴权	√	√	√	
	4.3.8 蓝牙敏感信息通信			√	
	4.4 Zigbee				
	4.4.1 Zigbee 协议版本	√	√	√	
	4.5 射频				
	4.5.1 射频通信数据包序列号长度	√	√	√	
	4.5.2 通信密钥硬编码		√	√	
	4.5.3 通信频率			√	
数据安全与隐私	5.1 加密与哈希算法	√	√	√	
	5.2 随机数生成函数		√	√	
	5.3 日志上报	√	√	√	
	5.4 跨境网络请求	√	√	√	
	5.5 云端存储安全	√	√	√	
	5.6 云端数据删除功能	√	√	√	
	5.7 恢复出厂设置	√	√	√	
业务逻辑	6.1 设备可绑定状态	√	√	√	
	6.2 绑定确认			√	
	6.3 防重复绑定	√	√	√	
	6.4 强绑定关系			√	室外设备
	6.5 设备日志安全监控	√	√	√	
	6.6 安全设置指南			√	

附录 C

个人信息

个人信息是指以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映自然人活动情况的各种信息。

表A.1　个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

[来源：GB/T35273-2020《个人信息安全规范》附录 A]

个人敏感信息

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

表B. 1　个人敏感信息举例

个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

[来源：GB/T35273–2020《个人信息安全规范》附录 B]

特殊类型的个人信息

揭示种族或民族血统、政治观点、宗教或哲学信仰或工会会员资格的个人数据，以及处理基因数据、用于唯一识别自然人的生物识别数据、有关健康的数据或有关自然人的性生活或性取向的数据。

[来源：General Data Protection Regulation – Article 9]

附录 D

修订记录

版本号	修订时间	修订人	修订内容
1.0	2020.12	信息安全与隐私部	初版
2.0	2021.12	信息安全与隐私部	1. 优化描述，移除不适用内容； 2. 增加产品安全等级定义方法及关注点； 3. 增加基线要求分级适用表，明确各安全等级产品需满足的不同要求；

参考资料

【1】 Nordic OTA 例程

https://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.sdk5.v15.3.0%2Fexamples_bootloader.html&cp=5_1_4_4

【2】 滚动码

滚动码被用于设备通信身份验证，防止重放攻击。

https://ww1.microchip.com/downloads/en/Appnotes/Atmel-2600-AVR411-Secure-Rolling-Code-Algorithm-for-Wireless-Link_Application-Note.pdf

- 业界成熟方案：

Keeloq：https://blog.csdn.net/kangweijian/article/details/43491047

DST40：https://en.wikipedia.org/wiki/Digital_signature_transponder

Hitag2：https://blog.csdn.net/spenghui/article/details/71930428

【3】 安卓 4.3 引入 BLE 时的开发者文档：

https://developer.android.com/guide/topics/connectivity/bluetooth-le

【4】 Zigbee 3.0 官方 Install code 方案：

https://zigbeealliance.org/solution/zigbee/