国家金融IC卡安全检测中心
National Financial IC Card Security Test Center
银行卡检测中心
Bank Card Test Center

不以小而不为

——从智能门锁信息安全问题引发的对智能家居产品信息安全的思考和建议

杨 波

Tuesday, June 19, 2018

目录

CONTENTS

第一部分

智能门锁安全问题分析

智能门锁概览、安全测评及问题分析

1.1 智能门锁概览

※ 定义

➢ 智能门锁是指在传统机械锁的基础上改进的，在用户安全性、识别性、管理性方面更加智能化、简便化的锁具。智能门锁是门禁系统中锁门的执行部件。智能门锁区别于传统机械锁，是具有**安全性、便利性、先进技术**的复合型锁具。

※ 常见智能门锁的物理组成部分

参见《2017中国智能锁应用与发展白皮书》

前面板

- 主电路板
- 密码按键
- 指纹模组
- 前把手
- 显示屏
- 射频卡识别模块
- 电机

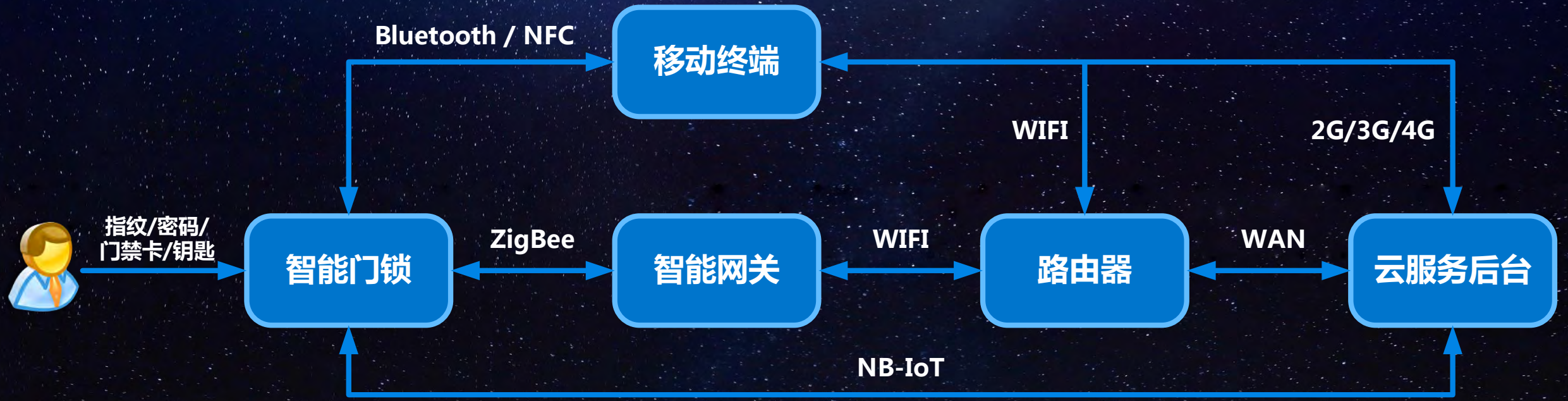
锁体

- 锁体
- 锁芯
- 电机（可选）

后面板

- 通讯模块（WIFI、蓝牙、ZigBee、NB-IoT等）
- 电池槽
- 反锁旋钮
- 后把手

1.2 常见应用模型


Bluetooth / NFC
移动终端
WIFI
2G/3G/4G
指纹/密码/
门禁卡/钥匙
智能门锁
ZigBee
智能网关
WIFI
路由器
WAN
云服务后台
NB-IoT

1.3 标准规范

※ **国际**

- 美国：《ANSI/UL 1034-2004 Burglary-Resistant Electric Locking Mechanisms》(防盗电子锁机械装置)
- 欧洲：EN2209:2003、EN1906:2002、EN1303:2005等检测标准

※ **国内**

- 国家标准： GB 17565-2007 防盗安全门通用技术条件、GB/T 35735-2017公共安全 指纹识别应用 采集设备通用技术要求
- 公安行业： GA 374-2001 电子防盗锁 、 GA 701-2007 指纹防盗锁通用技术条件
- 企业规范：智能家用电器信息技术安全框架、网络智能家用电器信息技术安全认证实施规则

※ **正在制定**

- 国家标准：《建筑及居住区数字化技术应用 智能门锁安全》

1.4 智能门锁与终端机具对比

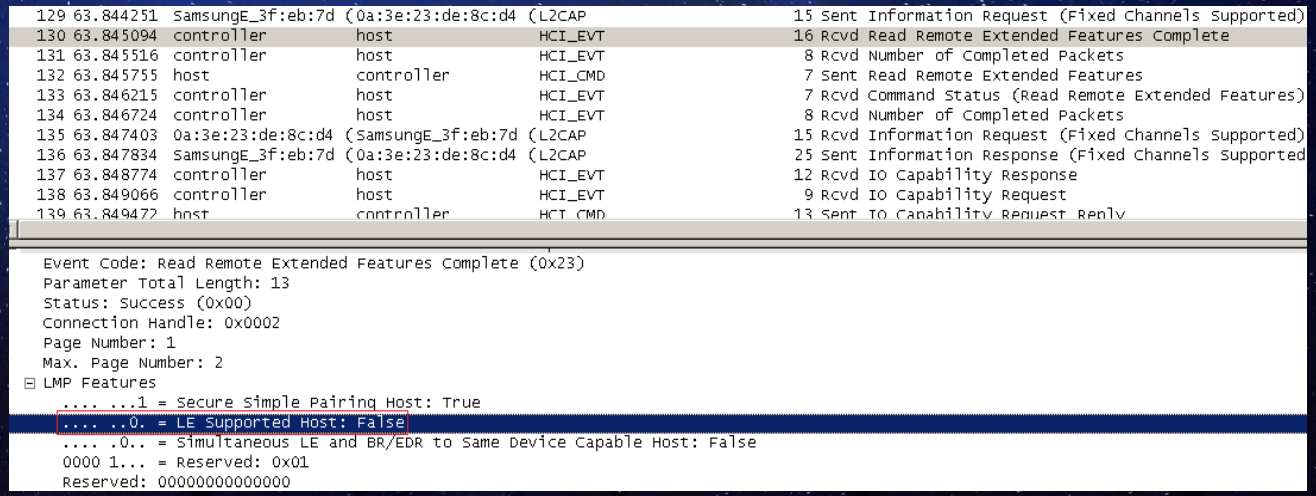
安全要求	智能门锁	终端机具
物理安全	√	√
系统安全	√	√
通信安全	√	√
芯片安全	√	√
卡片安全	√	√
显示安全	√	√
PIN输入安全	√	√
生物认证安全	√	--

1.5 智能门锁检测方案

物理安全	• 防移除、防入侵
逻辑安全	• 设备自检，安全审计，逻辑异常，固件认证，固件更新，敏感服务控制，内存清除，随机数，密码算法，密钥管理
PIN安全	• 输入时的音调，输入超时，复杂度要求，防穷举，传输安全，临时PIN安全
RFID安全	• 识别ID，防复制，防重放
指纹安全	• 传感器精度，传感器认证，防复制，指纹数据存储，指纹数据传输
通信安全	• 安全协议，远程密钥发布
脆弱性分析	• 渗透测试

1.6 检测过程

拆解试验-物理静态分析



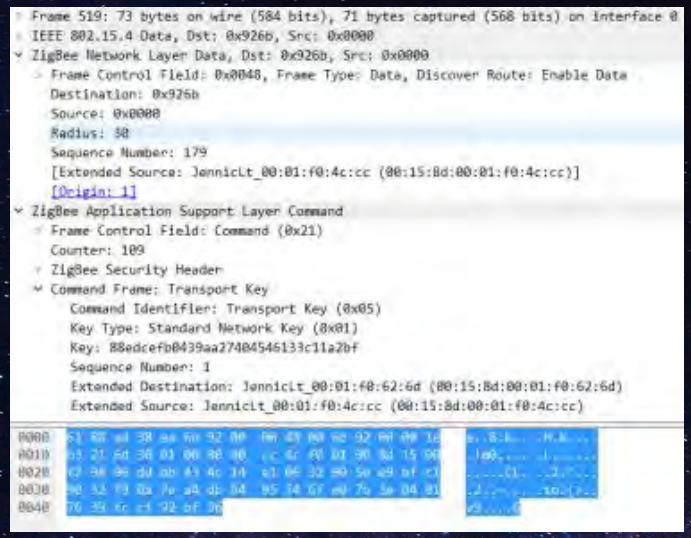
```
129 63.844251  SamsungE_3f:eb:7d (0a:3e:23:de:8c:d4 (L2CAP                15 Sent Information Request (Fixed Channels Supported)
130 63.845094  controller         host               HCI_EVT              16 Rcvd Read Remote Extended Features Complete
131 63.845516  controller         host               HCI_EVT               8 Rcvd Number of Completed Packets
132 63.845755  host               controller         HCI_CMD               7 Sent Read Remote Extended Features
133 63.846215  controller         host               HCI_EVT               7 Rcvd Command Status (Read Remote Extended Features)
134 63.846724  controller         host               HCI_EVT               8 Rcvd Number of Completed Packets
135 63.847403  0a:3e:23:de:8c:d4 (SamsungE_3f:eb:7d (L2CAP                15 Rcvd Information Request (Fixed Channels Supported)
136 63.847834  SamsungE_3f:eb:7d (0a:3e:23:de:8c:d4 (L2CAP                25 Sent Information Response (Fixed Channels Supported
137 63.848774  controller         host               HCI_EVT              12 Rcvd IO Capability Response
138 63.849066  controller         host               HCI_EVT               9 Rcvd IO Capability Request
139 63.849472  host               controller         HCI_CMD              13 Sent IO Capability Request Reply

  Event Code: Read Remote Extended Features Complete (0x23)
  Parameter Total Length: 13
  Status: Success (0x00)
  Connection Handle: 0x0002
  Page Number: 1
  Max. Page Number: 2
⊟ LMP Features
    .... ...1 = Secure Simple Pairing Host: True
    .... ..0. = LE Supported Host: False
    .... .0.. = Simultaneous LE and BR/EDR to Same Device Capable Host: False
    0000 1... = Reserved: 0x01
    Reserved: 00000000000000
```

蓝牙试验-动态拦截分析

银行卡检测中心

检 测 报 告

检测报告



```
Frame 519: 73 bytes on wire (584 bits), 71 bytes captured (568 bits) on interface 0
IEEE 802.15.4 Data, Dst: 0x926b, Src: 0x0000
ZigBee Network Layer Data, Dst: 0x926b, Src: 0x0000
  Frame Control Field: 0x0048, Frame Type: Data, Discover Route: Enable Data
  Destination: 0x926b
  Source: 0x0000
  Radius: 30
  Sequence Number: 179
  [Extended Source: JennicLt_00:01:f0:4c:cc (00:15:8d:00:01:f0:4c:cc)]
  [Origin: 1]
ZigBee Application Support Layer Command
  Frame Control Field: Command (0x21)
  Counter: 109
  ZigBee Security Header
  Command Frame: Transport Key
    Command Identifier: Transport Key (0x05)
    Key Type: Standard Network Key (0x01)
    Key: 88edcefb0439aa2740454613 3c11a2bf
    Sequence Number: 1
    Extended Destination: JennicLt_00:01:f0:62:6d (00:15:8d:00:01:f0:62:6d)
    Extended Source: JennicLt_00:01:f0:4c:cc (00:15:8d:00:01:f0:4c:cc)
```

zigbee试验-动态拦截分析

1.7 攻击面分析

云端安全

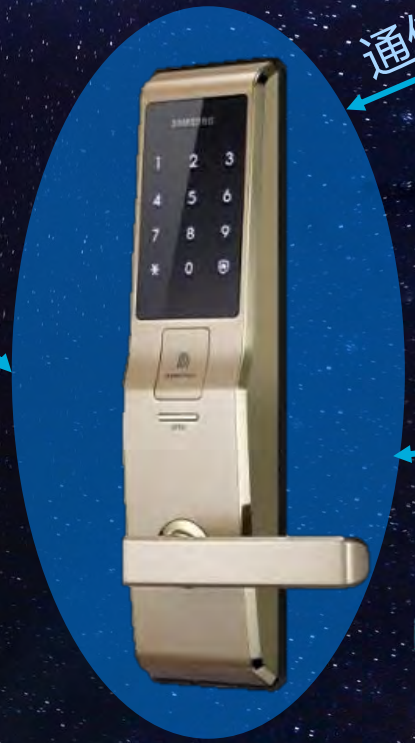
APP安全

通信安全

通信安全

通信安全

安全认证



本地安全

安全认证

功能越多，风险越多

1.8 典型风险—物理安全

※ 风险分析

- 门锁部分外壳为非金属材料（如触摸按键），破拆后可触及开锁信号线
- 外部暴露充电接口，容易遭受电源操纵攻击（拒绝服务、故障注入等）

※ 攻击过程举例

- 破拆指纹模块
- 使用钩具将信号线勾出
- 剪断信号线
- 使用外部电源为信号线供电
- 产生高电平后开锁成功

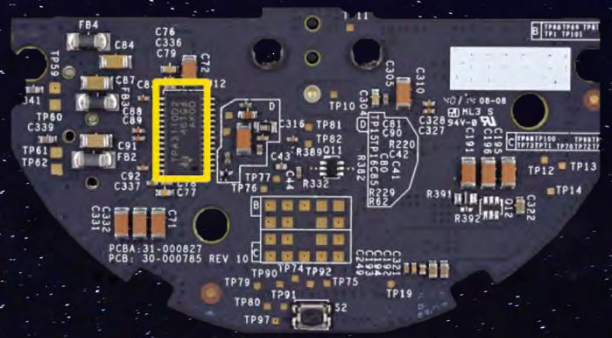
1.9 典型风险—固件安全

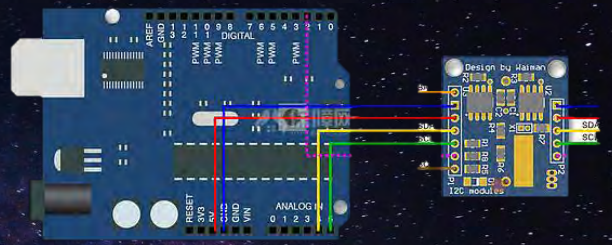
※ 风险分析

- JTAG、调试接口未封禁，固件可被提取分析，以寻找可利用的漏洞
- 固件认证保护机制脆弱，固件可被篡改后安装于门锁留下后门

※ 攻击过程举例

- 将门锁拆卸，暴露主电路板调试接口
- 使用外接连接线和设备连接调试接口
- 读取主电路板上的固件代码或程序
- 使用逆向工具破解固件代码，分析漏洞
- 利用漏洞实施攻击





1.10 典型风险—指纹认证安全

※ **风险分析**

- 指纹传感器普遍不具备活体检测功能，无法防御指纹膜攻击
- 使用市面上售卖的工具即可有效复制出能够通过认证的指纹套

※ **攻击过程举例**

- 购买指纹复制工具
- 获取合法用户的指纹
- 使用工具制作用户的指纹膜
- 非法用户配带指纹膜尝试指纹开锁

1.11 典型风险—门禁卡认证安全

※ **风险分析**

- 门禁卡若采用ID卡或 Mifare 1（M1）卡，几分钟内可完成复制过程
- 复制工具可在市面上购买

※ **攻击过程举例**

- 购买相应的卡片复制工具
- 获取合法用户的门禁卡
- 使用工具和空白卡复制出克隆卡
- 使用克隆卡尝试刷卡开锁

1.12 典型风险—ZigBee认证安全

※ **风险分析**

- ZigBee通信时采用默认密钥，临时密码下发时可被窃听
- 监听设备易于购买和配置

※ **攻击过程举例**

- 购买和配置无线监听模块
- 在门锁正常联网工作时，开启监听模块获取通讯源数据
- 分析源数据，使用默认密钥破解敏感信息
- 窃取通讯过程中下发的临时密码
- 使用密码开锁

1.13 其他风险

密码防穷举能力弱	APP与后台通信协议安全性弱	未有效清除内存数据	门锁缺乏详细的安全审计功能
• 门锁密码验证使用了虚位密码 • 未对输入长度进行限制和检查 • 攻击者可以尝试一次性输入多种密码猜测组合	• 手机APP与后台之间使用了http协议 • 攻击者可以尝试监听或窜改APP与后台之间的通信 • 威胁临时密码下发的过程	• 输入密码超时后未直接将输入数据清除，超时后仍进行了密码校验比对 • 攻击者可以利用合法用户正确输入但未按确认键后即离开的情况非法打开门锁	• 门锁未记录和审计连续多次开锁失败等敏感事件

第二部分

智能家居安全威胁

从物联网角度分析智能家居的安全威胁

2.1 安全事件——源于物联网设备

2016年10月21日 美国史上最严重的DDoS攻击

■ 事件经过

2016年9月，黑产世界公布了Mirai攻击的源码

10月，安全人员发布了物联网恶意代码Mirai分析报告

IoT僵尸网络 Mirai分析	恶意软件Mirai感染全 球物联网设备	Mriai IoT DDoS木马瞄准蜂窝网络设备	国外黑客发现国产摄像机存在漏洞	利用Mirai发动DDoS攻击并公布源码

源码公开一天后，10月21日黑客发动了DDoS攻击

黑客操控数百万网络摄像头及相关DVR录像机作为“肉鸡”通过Mirai僵尸网络以DDoS劫持攻击方式瘫痪了美国主要域名服务器供应商Dyn公司的服务器	导致大量美国知名网站无法访问，半个美国陷入断网状态

■ 事件分析

1

Mirai病毒

- 高效扫描物联网系统设备，通过感染存在漏洞（采用出厂密码设置或弱口令）物联网设备，像“寄生虫”一样存在设备中，进行操控。
- 被病毒感染后，设备成为僵尸网络机器人，在黑客命令下针对目标网络发动高强度攻击。通过Mirai僵尸网络病毒每次可以发动38万个IoT机器人参与攻击。

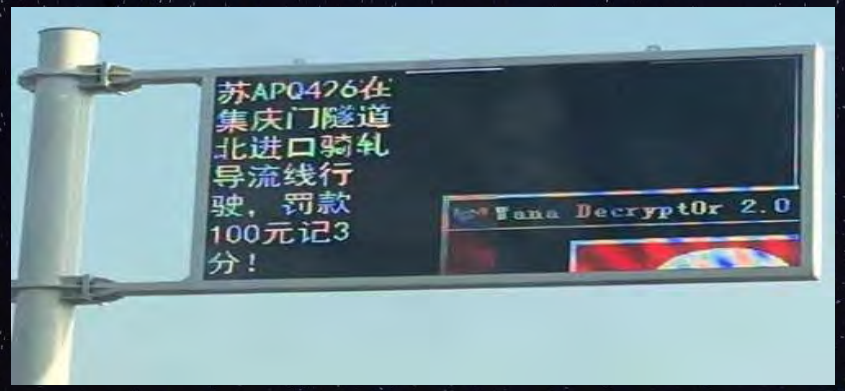
2

攻击目标

- 通过路由器、网关等连网设备都可能成为Mirai的攻击目标
- 网络摄像头、DVR、路由器、其它家用网络设备包括门窗、灯泡等可以通过物联网进行控制的都可能成为Mirai僵尸网络的“猎物”

2.2 安全事件——殃及物联网设备

2017年5月7日 勒索病毒 Wannacry



一款勒索病毒引发的“血案”

2.3 物联网市场安全现状

物联网市场发展迅速，终端数量剧增，安全隐患大

物联网终端安全高危漏洞

- 80%的设备采用简单密码
- 70%的通信过程未加密
- 90%固件存在安全隐患
- 大量设备没有更新补丁，甚至无法更新，telnet不能禁用且使用硬编码密码

物联网终端安全防护措施不足

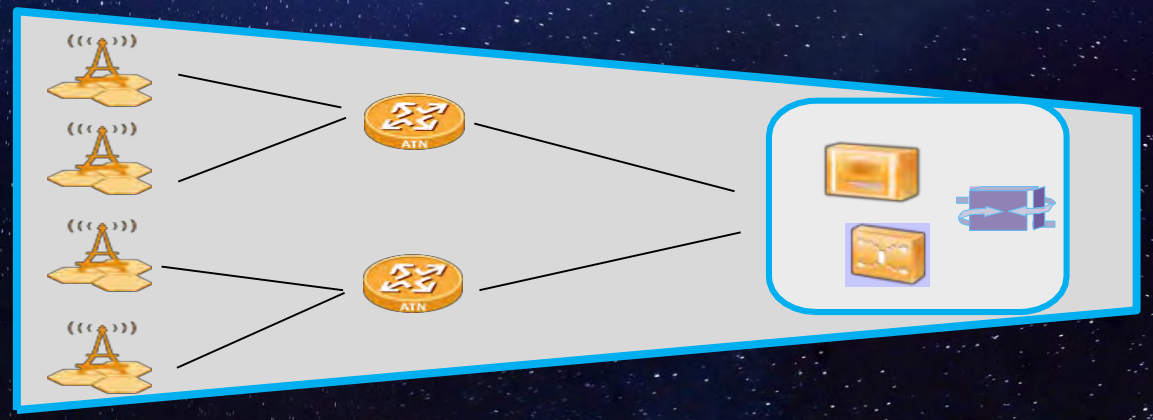
- 物联网设备的专用性、低成本、轻量级，导致很少防病毒软件能适配安装
- 出厂未进行安全检查
- 物联网终端在室外分散安装，导致物理攻击、篡改和仿冒

物联网产业链中安全环节占比低

物联网产业包括设备制造商、互联网厂商、运营商等多个环节。同时， 物联网安全风险无处不在，大到网络系统和平台，小到传感器等终端设 备。任何一处风险都有可能使得威胁扩散到整个网络与核心系统。各环节在立足市场，抢占入口的同时，较少关注产品的安全问题，也不愿投入成本解决这些安全问题。

2.4 物联网安全威胁分析

端、管、云面临非法入侵、恶意代码、流量攻击等安全威胁



接入网+核心网

应用云平台

终端面临的威胁

1、非法入侵 由于终端侧自身的漏洞导致的设备被非法入侵和控制

2、恶意代码 多数物联网终端由于成本受限、处理性能不高等原因，自有安全防护能力差

网络面临的威胁

1、流量攻击 物联网接入网和核心网面临着来自终端和互联网的双向流量攻击威胁

2、非法入侵 攻击者可能利用运维管理上的漏洞，对核心网元和系统发起入侵、感染病毒和篡改重要业务数据

平台面临的威胁

1、流量攻击 对平台实施DDoS攻击

2、入侵攻击 由于安全漏洞，攻击者可以从入侵平台设备

3、恶意代码 平台软件系统可能感染来自互联网的恶意代码