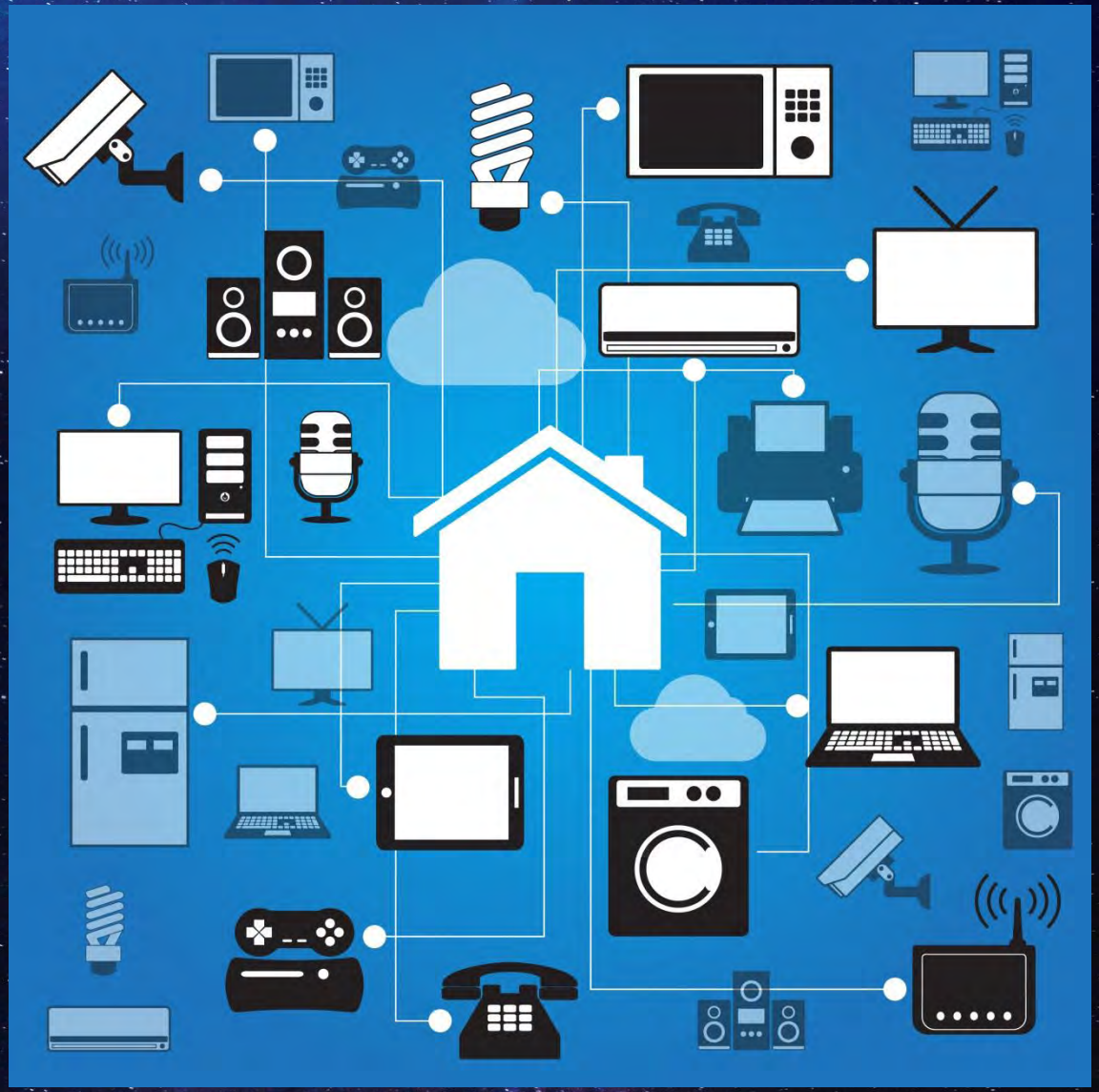
2.5 智能家居安全现状

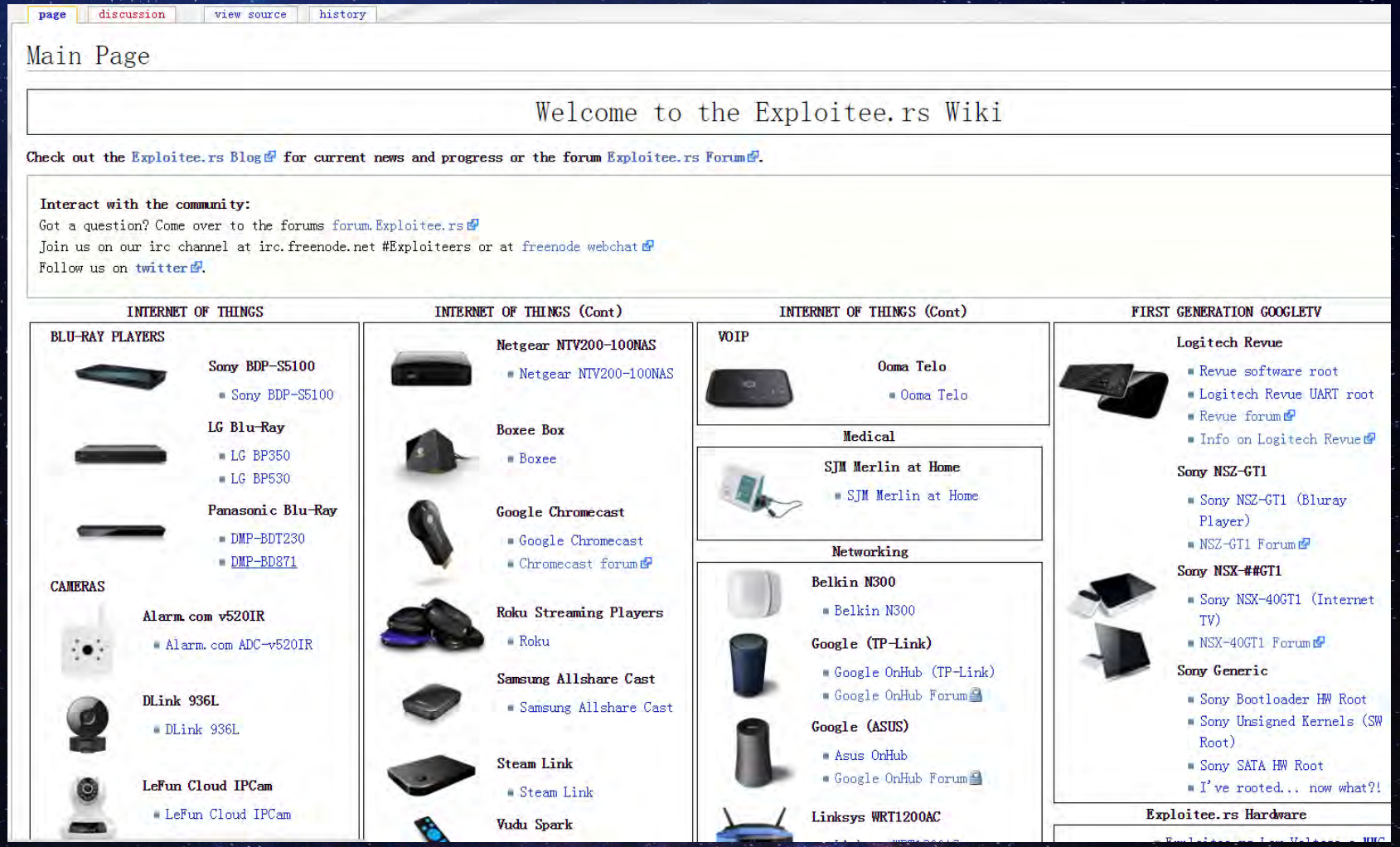
- 产业链条长
- 碎片化严重
- 聚焦于终端安全
- 涉及物联网端管云
- 缺乏安全防护设计
- 威胁难以控制



2.6 大量智能家居产品存在安全隐患

※ **国外某黑客网站**

- 批量公开了存在安全漏洞的物联网产品，信息丰富
- 公开了漏洞情况及攻击方法
- 绝大多数为智能家居产品
- 涉及的类型：蓝光播放器、摄像头、小家电、智能电视、数字机顶盒、音乐播放器、智能音响、智能网络设备、智能冰箱、家庭医疗设备等
- 涉及的品牌：Google、Sony、Samsung、Hisense、Moto、Western Digital、Amazon、Panasonic、Logitech、Asus...



2.7 产品组件分解

终端软件	终端硬件	通信链路	云端应用
固件	MCU/AP	通信协议	基础设施
OS/COS	通信模块	密钥管理	密钥管理
应用软件	安全芯片	中继设备	数据存储

2.8 智能家居产品被攻破后的危害

2.9 攻击方式分析

※ 设备输入数据接口利用

※ 设备网络端口利用

※ 设备硬件调试接口利用

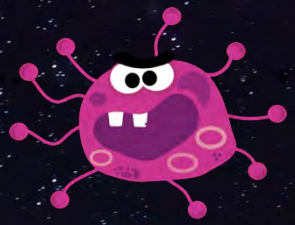
※ 设备已公开漏洞利用

※ 设备固件更新利用

※ 设备启动过程劫持

※ 设备处理输入数据的软件漏洞利用



第三部分

智能家居安全测评

安全测评的意义及相关技术

3.1 智能家居安全测评的意义

测评是确诊安全风险，对症下药

- 智能家居系统风险是客观存在的，也是可以被感知和认识从而进行科学管理的。如何确认系统的状态和发现系统中心存在的风险和面临的威胁，就需要进行信息安全测试评估

夯实安全根基，巩固智能家居安全大厦

- 可以帮助智能家居产品厂商了解潜在威胁，合理利用现有资源开展规划设计，让智能家居系统安全“赢在起跑线上”

测评是智能家居产品安全管理的“利器”

- 信息安全是高科技较量，没有科学的方法和手段，很难全面发现潜在的问题和威胁。“工欲善其事，必先利其器。”测试评估便是智能家居产品信息安全管理的“利器”

寻求适度安全和建设成本的最佳平衡点

- 安全是相对的，成本是有限的。测试评估为厂商算了一笔经济账，让我们认清智能家居产品面临的威胁和风险，以便在潜在风险损失与建设管理成本之间寻求一个最佳平衡点，力求达到预期效益最大化

3.2 智能家居产品安全检测技术

“云”测评技术

- 业务逻辑分析技术
- 接口安全分析技术
- 节点渗透攻击技术
- Web漏洞扫描技术
- SQL注入技术
- 跨站攻击技术
- 中间人重放技术
- HTTP(S)协议分析技术
- HTTP(S)协议还原技术
- DDOS测试技术
- 弱口令攻击技术
- ……

“管”测评技术

- 无线信号劫持技术
- 无线信号分析技术
- 网络协议分析技术
- 无线信号生成技术
- 无线信号重放技术
- USB协议通信技术
- 网络协议渗透技术
- 协议漏洞分析技术
- 网络协议解密技术
- 协议模糊测试技术
- 协议还原技术
- ……

“端”测评技术

- 固件逆向工程技术
- 固件漏洞分析技术
- 移动应用逆向技术
- Fuzzing分析技术
- 软件反编译技术
- 软件Hook技术
- 动态调试跟踪技术
- 软件静态分析技术
- 软件漏洞挖掘技术
- 软件脱壳技术
- 软件解密技术
- ……

3.3 智能家居安全测评对象

- **测评范围**
  - 物联网“云、管、端”，包括智能家居设备终端、移动设备、通信网络和云服务等

- **典型评估对象**
  - 终端芯片：AP、MCU、安全芯片（SE）、SIM等
  - 终端设备：空调、冰箱、洗衣机、智能摄像头、智能投影仪、智能网联汽车、智能机器人（家庭服务类）、VR设备等
  - 终端软件：移动终端APP、终端固件等
  - 通信协议：WIFI、ZigBee、Bluetooth、2G\3G\4G、NB-IoT、USB等
  - 物联网服务云：IIS、Tomcat、nginx、Webservice、Websocket、Hadoop等

第四部分

智能家居安全防护技术

安全技术介绍与产品防护建议

4.1 智能家居安全技术

※ 已有技术在物联网环境中的应用

- 异常行为检测、代码签名、白盒密码、空中下载技术（over-the air，OTA）、深度包检测（ DPI ）技术、防火墙、访问控制

※ 新技术的探索

- 区块链（通过去中心化和去信任的方式集体维护一个可靠数据库）

※ 物联网相关设备、平台、系统的漏洞挖掘和安全设计

- 物联网平台漏洞挖掘
- 物联网协议的0Day 漏洞主动挖掘技术
- 物联网操作系统漏洞挖掘
- 嵌入式设备安全框架

4.2 智能家居产品防护措施及建议

※ 物理安全

- 防破拆面板，增加拆除后状态锁定装置

※ 固件安全

- 封禁JTAG等调试接口
- 增加固件认证机制，验证固件来源及固件完整性

※ 指纹认证安全

- 使用具有活体检测的指纹识别模块
- 借助其他技术

※ 标识卡认证安全

- 使用CPU卡（IC卡），并启用安全认证技术

4.3 防护措施及建议（续）

※ **ZigBee认证安全**

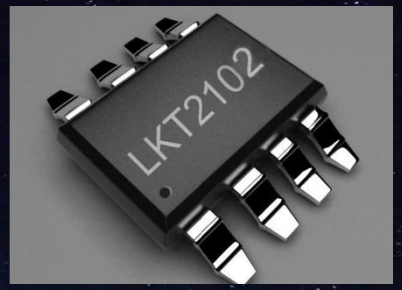
- 使用规范中高安全等级的方案
- 缩短临时密钥的使用周期

※ **芯片安全**

- 使用安全芯片处理和存储安全敏感信息

※ **逻辑与协议安全**

- 设计与使用安全的通信协议
- 接受严格的安全检测，发现可能的安全隐患

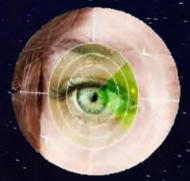


4.4 身份认证技术

※ **生物识别技术**

- 指纹、人脸、虹膜、掌纹、声纹、静脉





※ **人工智能识别**

- 多因子组合认证
- 认证因子的采集、存储、传输、计算符合安全规范



※ **身份认证组织**

- FIDO联盟（线上快速身份验证联盟）
- IFAA联盟（互联网金融身份认证联盟）
- BCTC是FIDO授权的安全检测实验室
- BCTC是IFAA正式成员，IoT安全工作组组长

4.5 TEE技术

※ **可信执行环境（TEE）在IoT设备的应用**

- 保护安全敏感数据的计算和存储
- 与身份认证技术相结合

※ **硬件支持**

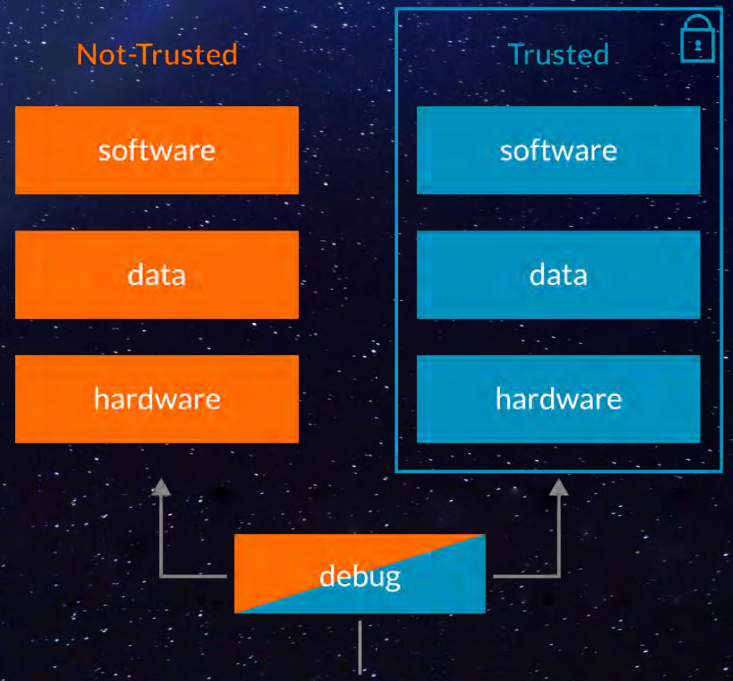
- ARM Cortex-M23/33 /35P 支持简化的TrustZone技术
- 由TrustZone实现TEE

※ **解决方案**

- 多个安全厂商已有成熟的TEE方案

※ **标准化与检测**

- GlobalPlatform（GP）
- BCTC是GP的功能检测与安全检测授权实验室



第五部分

中心情况简介

银行卡检测中心（国家金融IC卡安全检测中心）以及中心综合服务能力介绍

5.1 中心简介

银行卡检测中心（国家金融IC卡安全检测中心）

面向广大金融及非金融行业，提供**国际**、**国家**和**行业级**的**合规性检测**与**信息安全专业化服务**

※ 经中国人民银行总行批准，于1998年4月成立的**服务于金融行业的独立第三方专业技术服务机构**，注册资金3亿元人民币

※ 为支付产业各方提供银行卡、安全芯片、终端机具、客户端软件、信息系统等产品的功能与安全检测服务及相关技术支持

※ 2013年建成**国家金融 IC 卡安全检测中心**，填补了国内芯片检测领域的空白

※ 总部设在北京，在深圳和上海设有分公司，北京与深圳检测环境约为1.5万平米，公司实验室用地近2万平米

※ 国内唯一一家同时被Visa、MasterCard、EMVCo、中国银联、Discover、PCI、GlobalPlatform等国际机构与卡组织授权的检测机构，也是同时具备金融行业、通信行业、卫健委、住建部、交通部、石油石化等多行业检测能力的专业技术服务机构