XCON2022

AIoT安全体系建设实践

夏良钊 百度AIoT安全研究负责人

CONTENT 目录

0 百度AIoT安全团队

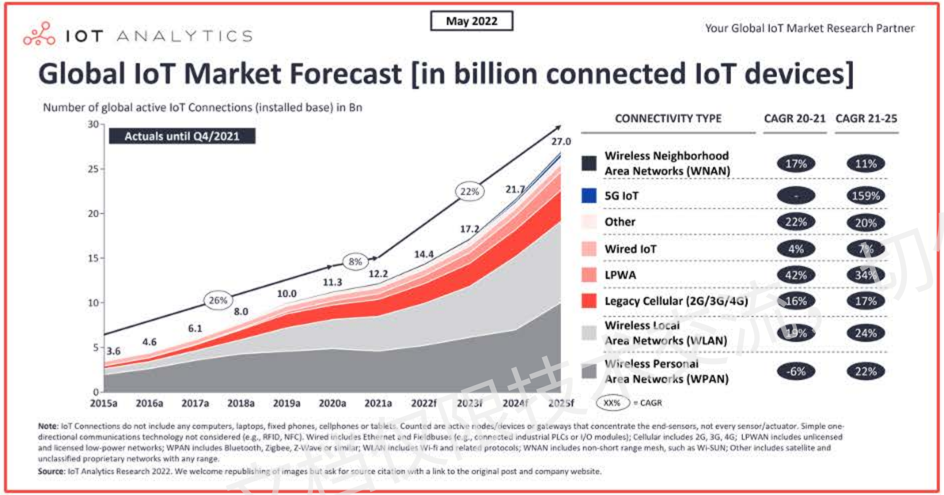
- 负责百度AIoT业务安全保障和体系建设，业务范围包括小度DuerOS生态、Apollo无人车及AI智能硬件
- 针对AIoT安全生态广泛开展安全研究，在上游内核模块、蓝牙&Wi-Fi等组件中累计获得300+CVE，获得谷歌、高通、联发科的多次致谢，团队成员多次受邀在BlackHat上发表演讲
- 打造业界领先的AIoT+移动安全解决方案，在OTA、入侵防护、应用检测与加固等场景中持续赋能外部客户

PART A

AIoT安全的现状和趋势

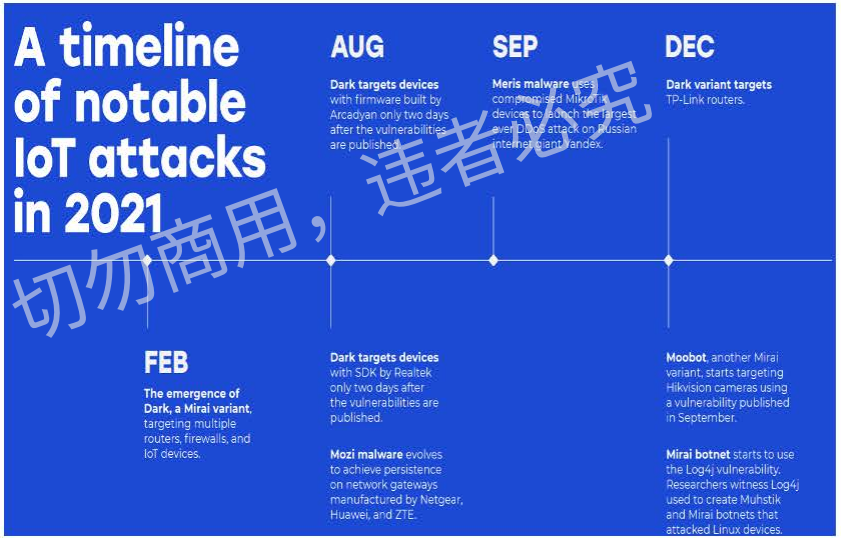
IoT安全态势

A IoT发展趋势



- **2022，预计达到144亿，增长率18%**
- **2025，预计达到270亿，增长率22%**

A IoT安全态势



- IoT恶意软件增长700% --- Zscaler
- 每年十亿级 IoT 设备被攻击 --- Securingsam Network

小度DuerOS助手

- **通过自然语言对话交互方式，可实现在不同场景下信息查询、生活服务出行路况、影音娱乐等数百项功能服务**

中国最大的对话式人工智能操作系统

66亿
单月语音交互次数

2亿+台
IoT智能家居设备连接

繁荣的合作伙伴生态及开发者社区

500+家
知名企业合作伙伴

5.2万名
开发者

35万+间
合作酒店客房

5200+项
技能支持

A 种类繁多的设备

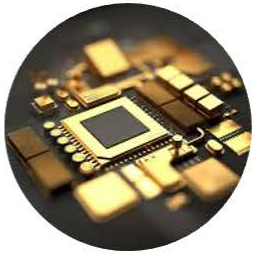
- 不同的安全要求
- 不同的攻击面
- 不同的策略

A 接口丰富的云端

面临的风险

业务安全

账号体系攻击
恶意调试刷机
远程静默监控



供应链安全

内核驱动漏洞
射频通讯模组漏洞
三方技能/SDK漏洞

数据安全

不安全的传输
关键数据未加密
缺乏权限控制与审计

AI安全

人脸识别绕过
声纹脸纹突破
海豚音攻击

监管及舆论

法律监管
各大破解比赛
负面新闻及报道

安全的挑战

上游供应链冗长

时刻关心个人隐私

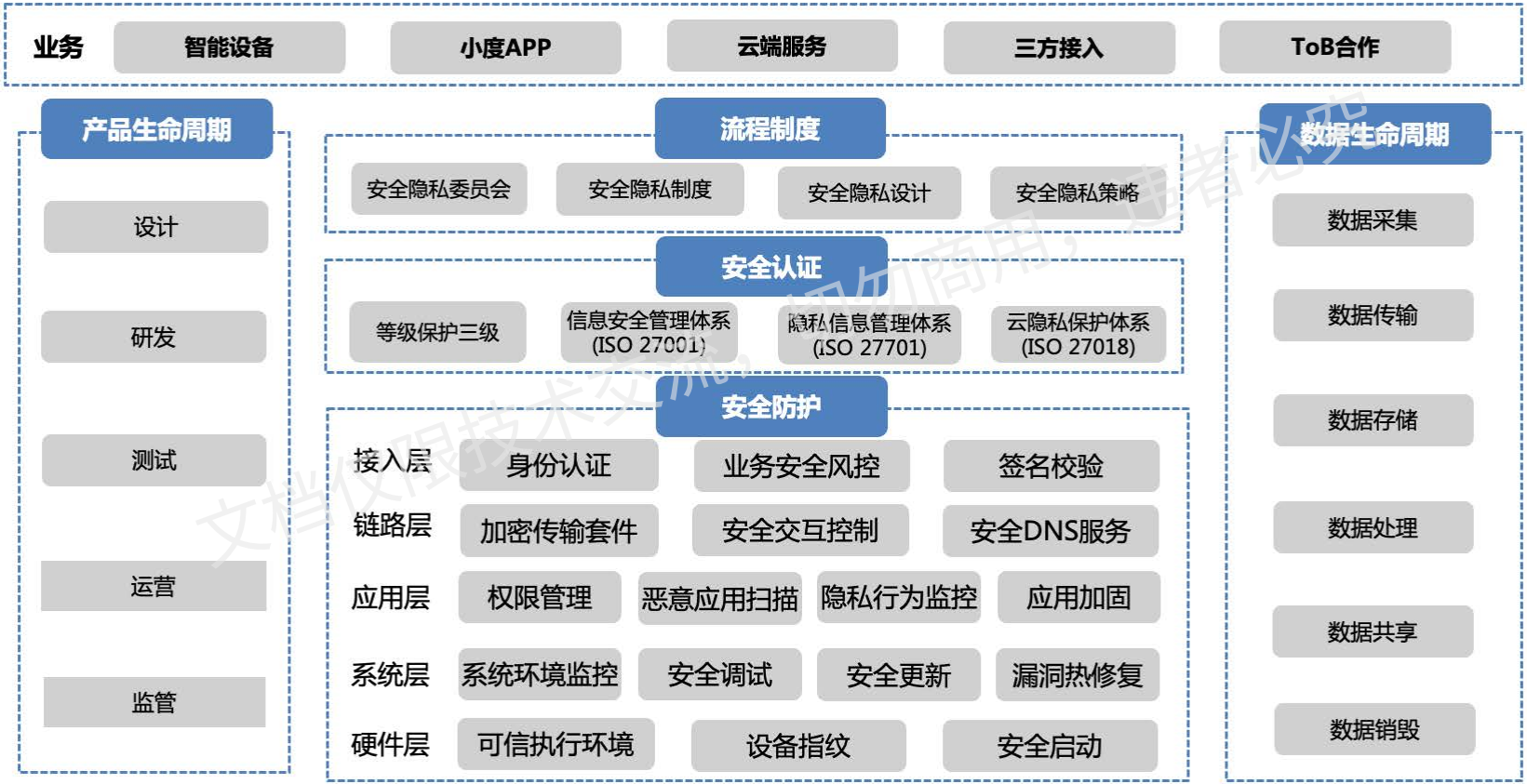
处理大量个人数据

PART B

百度AIoT安全体系框架

全生命周期主动安全体系

B 百度AIoT安全保障框架



B 产品生命周期防护

设计阶段	研发阶段	测试阶段	运营阶段	监管阶段
产品安全基线	安全基础组件	应用安全扫描	安全应急响应	产品口径库
安全编码规范	SDK安全准入	固件安全扫描	安全补丁管理	安全标准参与
业务安全培训	三方应用集成	数据安全扫描	系统安全防护	安全隐私认证
安全方案评审	代码安全扫描	设备渗透测试	业务安全风控	企业安全白皮书

B 数据生命周期防护

网络安全法　　个人信息保护法　　数据安全法

业务

- 唤醒控制
- 回家看看
- 音视频通话
- 看护助手
- 脸纹识别
- 声纹识别
- 家庭相册

政策协议

隐私政策	儿童隐私政策	网盘同步隐私说明	隐私问答
用户协议	儿童服务协议	个人语音服务协议	看护助手协议
声纹服务协议	面容服务协议	看护助手协议	三方信息数据共享

数据生命周期安全保护

采集 → 传输 → 存储 → 使用 → 共享 → 销毁

合规红线	分类分级	权限管理	安全流通
数据鉴别	数据脱敏	可信加密	数据沙箱
安全存储	联邦学习	日志审计	安全销毁

原则

- 公开透明
- 知情同意
- 最少够用
- 确保安全
- 数据质量
- 用户体验

PART C

纵深防御方案建设

安全合规技术

C 供应链漏洞管理与运营

发现

审计 + 逆向 + Fuzzing

应用

三方应用 | 三方SDK | 三方技能

系统

android | Linux | freeRTOS

硬件

MEDIATEK | Allwinner | Qualcomm | UNISOC | Rockchip | Amlogic

管理

流程 + 方案

三方应用准入规范 | 三方SDK准入规范

供应链安全扫描（应用+SDK+技能+固件）

系统补丁计划 + 芯片补丁计划

补丁筛选 → 补丁验证 → 补丁维护

运营

热修复 + OTA

热补丁制作 → 热补丁下发

官方补丁包 → 官方补丁下发



C

供应链漏洞管理与运营

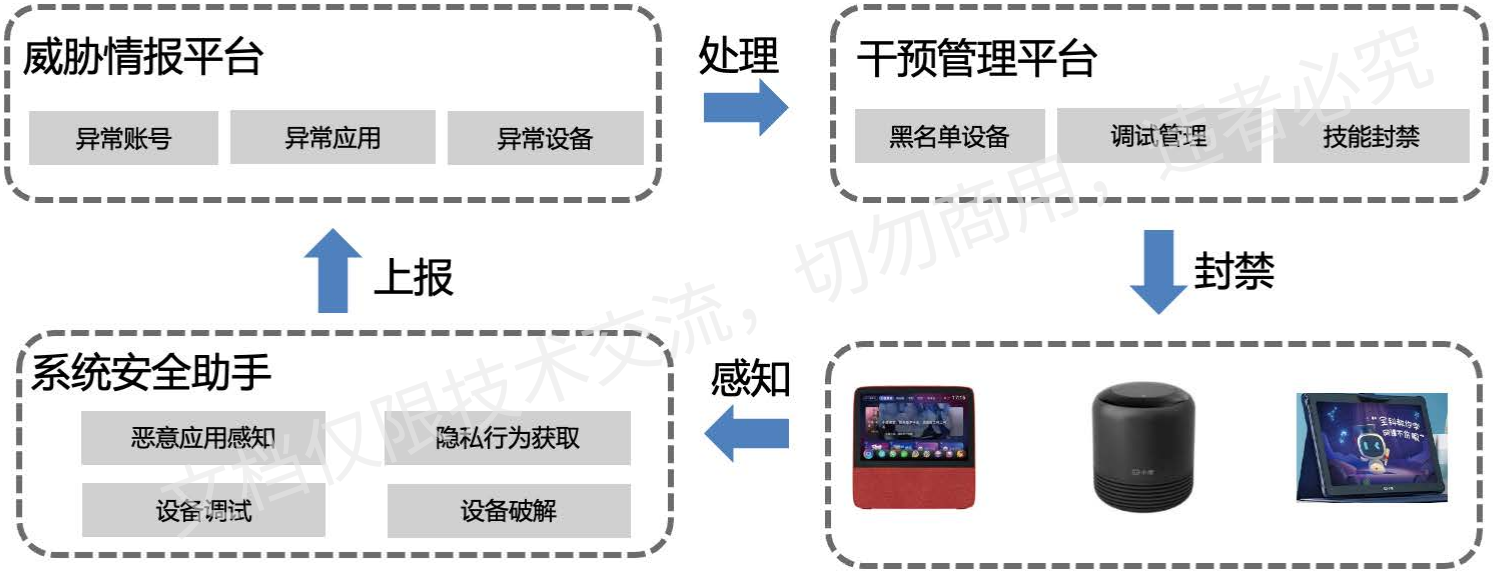
300+
供应链漏洞

50+
热修复补丁

500+
官方补丁合入

2000w+
热修复能力覆盖

C 设备风险感知与响应



设备风险感知与响应

总览设备问题-设备维度

sn	存在恶意app（病毒app）	root	magisk
9505	否	是	否
9505	否	是	否
9505	否	是	否
9505	否	是	否
9505	否	是	否
9505	否	是	否
9504	否	是	否
9504	否	是	否

总览app维度-app访问隐私权限行为

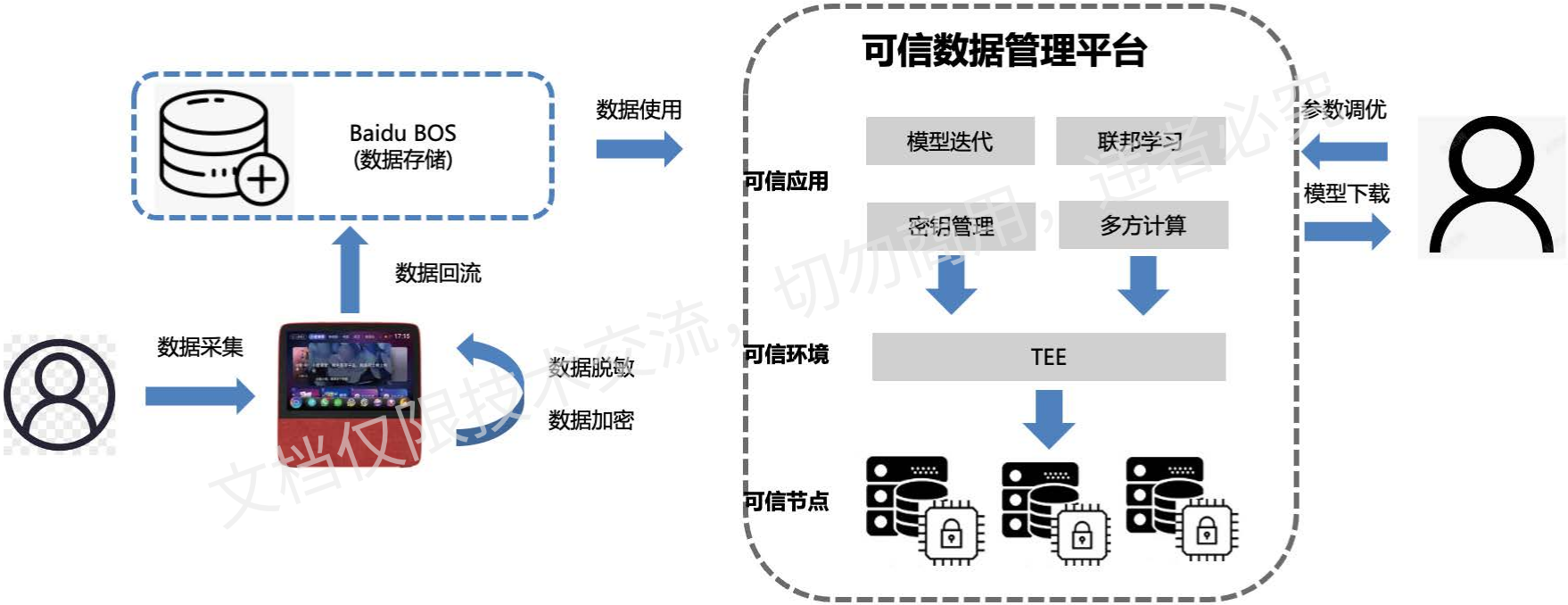
隐私权限调用应用名称	隐私权限调用总次数	隐私权限调用总设备量	摄像头调用次数	摄像头调用设备量	麦克风调用次数	麦克风调用设备量	地理位置调用次数	地理位置调用设备
com.a	2	2	2	2	0	0	0	
com.s	2	1	0	0	0	0	2	
com.u	2	1	0	0	0	0	2	
com.r	0	0	0	0	0	0	0	
com.b	0	0	0	0	0	0	0	

200+
异常应用

160+
异常设备

100w+
能力覆盖

基于可信环境的数据保护



PART D

行业影响力建设

共建行业安全生态

漏洞挖掘

February

Researchers	CVEs
Lewei Qu(曲乐炜) and Dong xiang Ke(柯懂湘) of Baidu AIoT Security Team	CVE-2021-39616,CVE-2021-39635,CVE-2021-39658

January

Researchers	CVEs
Lewei Qu(曲乐炜) of Baidu AIoT Security Team	CVE-2021-1049

MediaTek components

These vulnerabilities affect MediaTek components and further details are available directly from MediaTek. The severity assessment of these issues is provided directly by MediaTek.

CVE	References	Severity	Component
CVE-2022-20024	A-209705228 M-ALPS06219064*	High	System service
CVE-2022-20025	A-209700749 M-ALPS06126832*	High	Bluetooth
CVE-2022-20026	A-209705229 M-ALPS06126827*	High	Bluetooth
CVE-2022-20027	A-209702508 M-ALPS06126826*	High	Bluetooth
CVE-2022-20028	A-209702509 M-ALPS06198663*	High	Bluetooth

MIUI 某系统服务存在指针重复释放漏洞

内部标识	CVE编号	CVSS分数	发布时间
MiSVD-2022-134	CVE-2020-14123	4.2 中危	2022-04-22

漏洞描述及影响

MIUI 某系统服务存在指针重复释放漏洞。在函数调用时，内存指针拷贝给两个功能模块，攻击者
受影响模块崩溃，影响正常功能，如果成功利用该漏洞可造成权限提升。

CVE-2020-11836 MTK AEE module is in debug mode

2021-02-04

OPPO security team sincerely appreciates these security researchers' efforts to help us improve t
more security researchers to apply for CVE IDs.

Acknowledgements

Vulnerabilities Submitted by: Qu Lewei, Baidu AIoT security team

Vulnerability submission time: November, 2020

顶会论文

D 行业标准

国家标准

《智能人体温度检测与识别系统技术要求和测试评价方法》
《物联网 参考体系结构》修订GB/T33474-2016
《汽车整车信息安全技术要求》
《汽车数字证书应用规范》
《汽车软件升级通用技术要求》
《信息安全技术 关键信息基础设施安全测评要求》
《信息安全技术 公钥基础设施 PKI系统安全技术要求》
《信息安全技术 边缘计算安全技术要求》
《信息安全技术 汽车采集数据的安全要求》

行业标准

《智能终端设备 数据安全技术要求》
《智能显示设备适老化技术要求评测方法》
《智能终端设备个人信息安全技术规范》
《移动智能终端个人信息分类分级》
《云游戏X86终端技术要求和测试方法》

团体标准

《智能终端设备 数据安全技术要求》
《智能显示设备适老化技术要求评测方法》
《智能终端设备个人信息安全技术规范》
《移动智能终端个人信息分类分级》
《云游戏X86终端技术要求和测试方法》

D 产业联盟

智能终端安全生态联盟（Open AI System Security Alliance）

国内首个致力于提升智能终端生态安全的联合组织，由信通院、华为、百度联合发起成立，由安全厂商、终端厂商、高校科研机构、政府机构共同组成。联盟宗旨是希望引导一个开放、共享、合作、共建的安全生态链，促进智能终端厂商与安全厂商之间建立良性的互动与合作，共同推进智能终端安全生态的建设。

THANK YOU