
Architect
SACC
2022 中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2022
激发架构性能 点亮业务活力
云上会议 网络直播 | 2022年10月27-29日
ITPUB

AIoT安全与隐私自动化建设实践

小米集团智能终端安全实验室 吴明

目录

- 背景
- IoT安全自动化系统
- 挑战与突破
- 落地实践和成果
- 展望未来

简介

- BaCde

RapidDNS网站站长（rapiddns.io），小米智能终端安全实验室（原AIoT安全实验室）高级安全工程师。主要从事AIoT安全攻防研究和智能网联汽车安全研究方向。曾在CNCERT 2018、中国物联网大会2018、DTCC 2019、ISC 2021、Defcon 29（US） 等会议发表主题演讲。

- **智能终端安全实验室（原AIoT安全实验室）**

团队共20余人，涵盖车联网安全、嵌入式安全、无线电安全、编码安全、安全架构设计等多个方向。团队成员曾多次参与Pwn2own、Geekpwn、天府杯、补天杯等赛事并获大奖。

背景

物联网安全威胁

- 僵尸网络
- 中间人攻击
- 隐私泄露
- 隐私监听（监听或定位等）
- APT攻击
- 远程跳板

背景

2020年01月	英国发布《消费物联网安全基线要求》 草案
2020年05月	NISTIR 8259A 物联网设备信息安全基线能力
2020年06月	欧洲电信标准化协会发布《消费物联网产品网络安全/隐私保护标准》ETSI EN 303645
2020年12月	美国CTA消费者技术协会发布《设备和设备系统安全基线指南》
2020年12月	美国众议院通过《促进IoT安全改进法案》
2020年12月	全国信息安全标准化技术委员会GB/T 38632-2020《信息安全技术 智能音视频采集设备应用安全要求》
2021年02月	全国信息安全标准化技术委员会《智能家用电器的通用安全技术要求》征求意见稿
2021年05月	国内智能家电安全《智能家居终端安全 智能摄像头安全能力技术要求和测试方法》征求意见稿
2021年08月	欧洲电信标准化协会发布TS103701《消费物联网基线评估标准》
2021年12月	英国《产品安全和电信基础设施PSTI法案（草案）》

背景

国内个人信息保护立法体系

国家标准、行业标准

《信息安全技术 个人信息安全规范》（GB/T 35273-2020）
《信息安全技术 个人信息去标识化指南》（GB/T 37964-2019）
《信息安全技术个人信息安全规范》（GB/T 35273-2017）
《信息安全技术 网络安全等级保护基本要求》
《信息安全技术移动智能终端个人信息保护技术要求》（GB/T 34978-2017）
《信息安全技术 公共及商用服务信息系统个人信息保护指南》（GB/Z 28828-2012）
《个人金融信息保护技术规范》（JR/T 0171-2020）
《个人健康信息码 参考模型》（GB/T 38961-2020）
《个人金融信息保护技术规范》（JR/T 0171-2020）
《金融服务 生物特征识别 安全框架》（GB/T 27912-2011）
《信息安全技术 数据出境安全评估指南（征求意见稿）》
《信息安全技术 个人信息告知同意指南（征求意见稿）》
《信息安全技术关键信息基础设施安全控制措施（征求意见稿）》

规范性文件

《关于做好个人信息保护利用大数据支撑联防联控工作的通知》
《互联网个人信息安全保护指南》
《中国人民银行关于进一步加强征信信息安全管理的通知》
《App违法违规收集使用个人信息行为认定方法》
《App违法违规收集使用个人信息自评估指南》
《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》
《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请适用指南》
《网络安全实践指南—移动互联网应用基本业务功能必要信息规范（V1.0）》（TC260-PG-20191A）
《移动互联网应用程序（App）安全认证实施规则》（CNCA-App-001）
《网络安全标准实践指南—移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）》
《网络安全标准实践指南——移动互联网应用程序（APP）中的第三方软件开发工具包（SDK）安全指引（征求意见稿）》
《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南（征求意见稿）》

司法解释

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》

部门规章

《儿童个人信息网络保护规定》
《网络交易监督管理办法》
《网络安全审查办法》
《电信和互联网用户个人信息保护规定》
《中国人民银行金融消费者权益保护实施办法》
《网络交易监督管理办法（征求意见稿）》
《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》

法律

《刑法》、《刑法修正案（七）》、《刑法修正案（九）》
《民法典》
《网络安全法》
《电子商务法》
《消费者权益保护法》
《中华人民共和国出境入境管理法》
《反恐怖主义法》
《基本医疗卫生与健康促进法》
《全国人民代表大会常务委员会关于加强网络信息保护的决定》
《个人信息保护法（草案）》
《数据安全法（草案）》

海外个人信息保护立法

俄罗斯

108/81，《关于自动处理个人数据的个人保护公约》
《关于保护个人数据自动处理的个人的公约的议定书》
2006年7月联邦法第152-FZ号，《个人资料法》
2006年7月联邦法第149-FZ号，《信息技术和信息保护法》
2001年12月30日第197-FZ号，《俄罗斯联邦劳动法》
2004年7月26日联邦法第98-FZ号，《关于商业秘密》
2017年7月联邦第187-FZ号，《关键信息基础设施的安全性法》
2020年4月24日联邦法第123-FZ号，《关于建立特殊法规的实验法》
2020年7月1日生效，《联邦个人数据法》
2001年12月30日第195-FZ号，《行政犯罪法典》
第146号政府法令，《关于批准组织和实施国家控制和监督上的个人数据的处理规则》
第687号政府法令，《关于批准关于不使用软件的个人数据处理属性的规定》
第512号政府法令，《关于批准对生物特征识别个人数据有形载体以及在个人数据信息系统外部进行此类数据存储的要求》

欧盟

《通用数据保护条例》《电子隐私指令》《治安数据保护指令》《电子商务指令》
EDPB发布的指南
关于补充转移工具以确保遵守欧盟个人数据保护水平的措施的第01/2020号建议
关于根据《条例》第2016/679条提出相关及合理反对意见的第09/2020号指引
关于GDPR中控制者和处理者概念的第07/2020号指南
关于根据第2016/679号条例同意的第05/2020号准则
关于在爆发COVID-19的情况下使用位置数据和接触者追踪工具的第04/2020号准则。
关于在COVID-19爆发的情况下为科学研究目的处理健康数据的第03/2020号准则。
关于第2016/679号条例第46(2)(a)条和第46(3)(b)条的第2/2020号准则，涉及欧洲经济区和非欧洲经济区公共当局和机构之间的个人数据转移
关于在联网车辆和移动性相关应用中处理个人数据的第1/2020号准则
关于GDPR下搜索引擎案例中被遗忘权标准的准则5/2019（第1部分）
关于第25条通过设计和默认方式保护数据的第4/2019号指引
关于通过视频设备处理个人数据的第3/2019号指引
关于欧洲数据保护监督员名单草案的第01/2019号建议，涉及需要进行数据保护影响评估的处理操作
关于在向数据主体提供在线服务的情况下根据《国内生产总值条例》第6(1)(b)条处理个人数据的第2/2019号指引
关于第2016/679号条例规定的行为守则和监督机构的第1/2019号准则
关于根据《一般数据保护条例》(2016/679)第43条认可认证机构的第4/2018号准则
关于GDPR地域范围的第3/2018号准则(第3条)
关于根据第2016/679号条例克减第49条的第2/2018号准则。
WP29工作组发布的指南
关于第2016/679号条例下的同意的第05/2020号准则
第2016/679号条例下的透明度准则
2016/679号条例下的自动个人决策和剖析指南
第2016/679号条例下的个人数据泄露通知指南
第2016/679号法规下的数据可携性权利指南
关于数据保护影响评估(DPIA)及确定处理是否 "可能导致高风险 "的准则2016/679条例
数据保护官员（DPO）指南
确定控制者或处理者的主要监管的指引

日本

《个人信息保护法》（2020年修订）
《信用信息法的使用和保护》
《促进信息和通信网络利用和信息保护法》
《数据保护法律和法规解释指南》
《取消个人数据识别准则》
《个人数据假名化指南》
《金融领域个人数据的假名和匿名化手册》

韩国

《个人信息保护法》（2020年修正）
《行政程序中使用数字识别特定个人的法令》
《个人信息保护法通用指南》
《个人信息保护法指南》（用于向外国转让给第三方）
《个人信息保护法指南》（对向第三方的转移进行检查和记录）
《个人信息保护法指南》（用于匿名信息）
《个人信息保护法指南》（用于数据泄漏）
《关于正确处理特定个人信息的准则》
《有关适当处理金融业务中特定个人信息的准则》

印尼

《个人数据保护法（草案）》
2008年第11号法令，《关于电子信息交易》
2016年第20号，《关于电子系统中个人数据保护》
2012年第82号政府法规，《关于电子系统和交易实施》
2019年第71号政府法规，《关于实施电子系统和交易》
第1 / POJK.07 / 2013号法规，《关于金融消费者保护》
第16/1 / PBI / 2014号条例，《关于支付系统服务消费者保护》

印度

《信息技术（合理的安全措施和程序以及敏感的个人数据或信息）规则》
《信息技术法》
《个人数据保护法案（草案）》
《电子通讯法》

内部挑战：AIoT安全隐私评估

- 产品量大，测试周期长 测试一款设备，我们的工程师需要 2-3 周 时间。2021年，提测 IoT 产品数量多达 300 余款。
- 测试标准不统一，安全测试纯靠工程师经验。 测试结果不统一，容易出现疏漏。
- 如何保障每一款 IoT 产品的安全与隐私呢？

行业难题：AIoT安全隐私评估

- 检测时间长 由于 IoT 安全测试的复杂性，外部大多采 用人工测试方式。BSI 测试一款设备需要 4-6周时间，项目组需要2-3个全职人员。
- 检测成本高 外部公司检测一款 IoT 设备的安全性，费 用至少为几万元，BSI 测试一款设备需要花 费30万元
- 缺乏优秀实践标准 整个行业目前没有一家企业或者机构同时 发布 IoT 安全和隐私方面的实践标准。
- 自动检测维度单一 行业内，诸如微软、阿里、腾讯等国内外大 厂，只有固件安全检测产品，而固件安全只 是IoT安全的冰山一角。

IoT安全自动化系统

我们的目标

做一个人人都可以用的AIoT安全自动化检测系统

覆盖全生命周期

从设备上电到出报告过程全自动化

测试依据

EN 303645 Cyber Security for Consumer Internet of Things: Baseline Requirements

OWASP IoT Top10 2018

IoT Security Foundation IoT Cybersecurity Framework checklist 2.0

GB/T 信息安全技术 智能家居安全通用技术要求和测试评价方法（征求意见稿）

TAF-FG1-AS0030-V1.0.0 2019 智能门锁信息安全技术要求和评估方法-信息采集单元

GB/T35273-2020 《信息安全技术 - 个人信息安全规范》

物联网安全基线

硬件安全
Linux嵌入式
射频安全
ZigBee安全
数据安全
蓝牙安全
逻辑安全
移动安全
通信安全
以太网通信
系统安全
编码安全

https://github.com/MiSecurity/Cyber-Security-Baseline-for-Consumer-Internet-of-Things

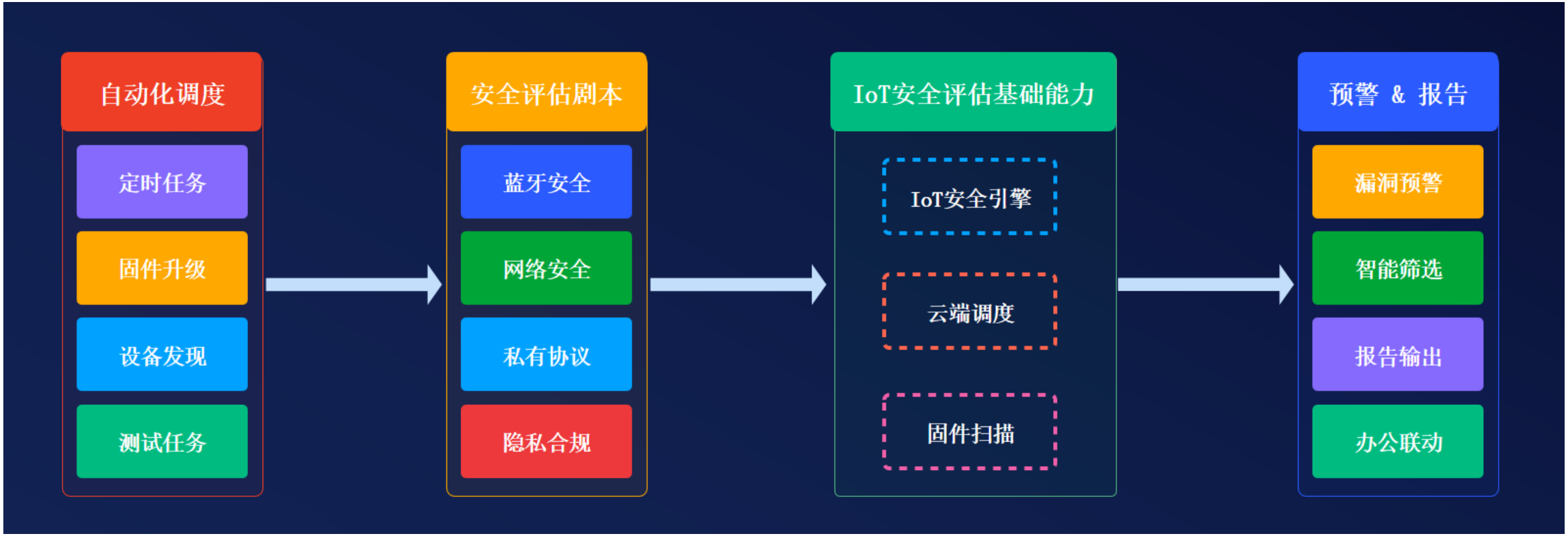
物联网安全基线

需要具备的能力

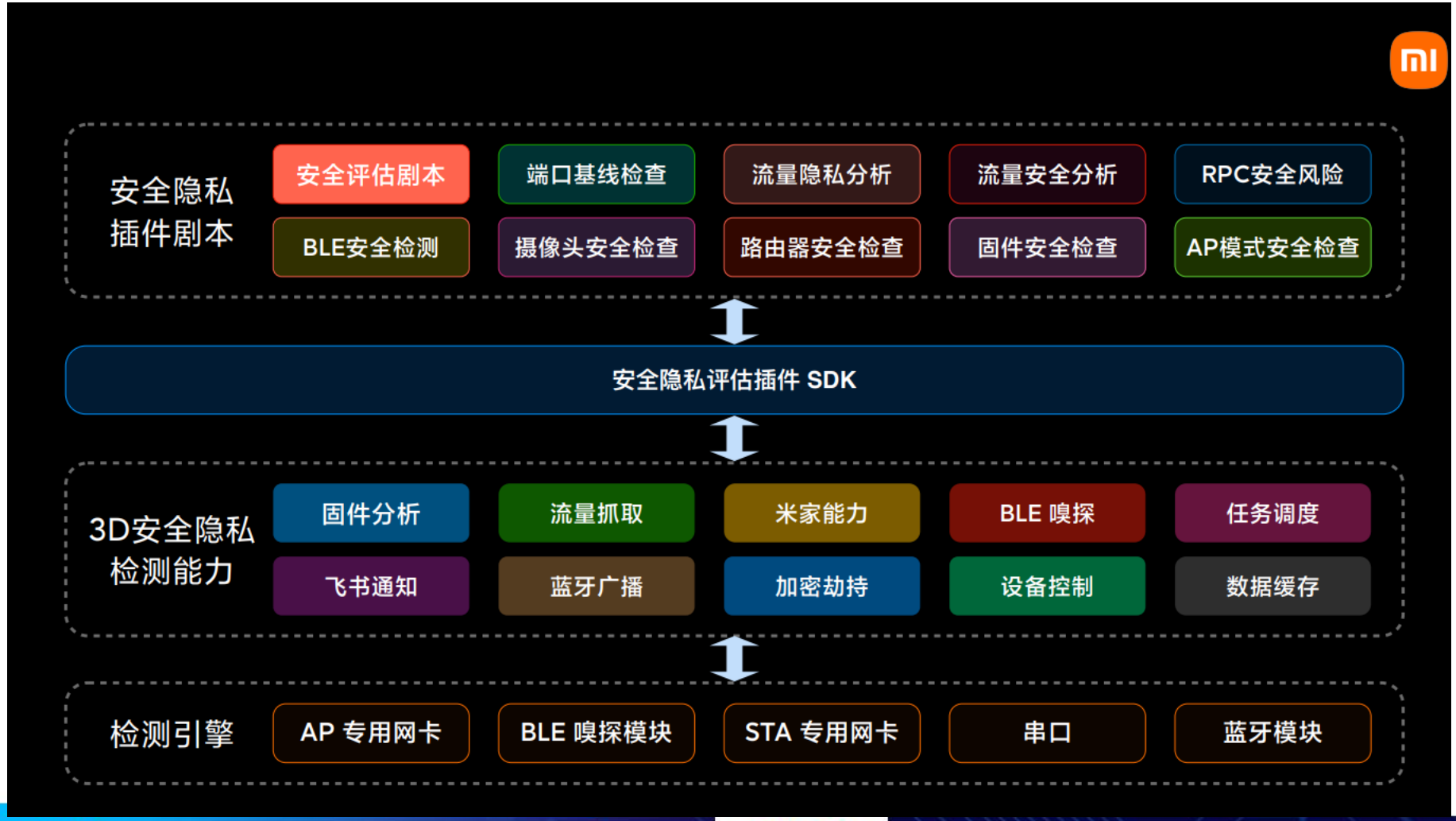
安全能力一键调用

硬件层	通讯层	协议层	固件层	系统层	应用层	云端层	提测信息
SPI I2C JTAG UART 固件读写 ...	IP 蓝牙 射频 ZigBee ...	HTTP TLS劫持 流量监测 BLE广播 BLE ATT BLE GATT MIOT私有协议 ...	格式识别 固件解包 文件分析 漏洞扫描 ...	端口信息 处理器架构 iptables信息 安全基线检测 轻量级Hook框架 ...	URL分析 APP安全分析 Frida Hook框架 ...	设备信息 当前版本 固件信息 RPC通道 插件信息 ...	通讯方式 软件功能 硬件安全 通讯安全 系统安全 编码安全 业务逻辑安全 隐私合规 ...

架构：AIoT智能安全评估



架构：AIoT智能安全评估



流程设计

AIoT安全隐私评估系统

标准化提测产品提测信息

统一通过SOC平台进行提测

产品安全测试流程

填写测试信息
提供测试应用或样机

提交测试申请

材料初审

自动化评估和测试

提供初测结论
提交漏洞

修复漏洞

复测验证

测试通过
完成评估

业务部门　信息安全与隐私部

IoT产品新产品、新版本上线前均强制测试

自动化测试 + 输出报告

飞书+邮件通知结果

安全测试与响应

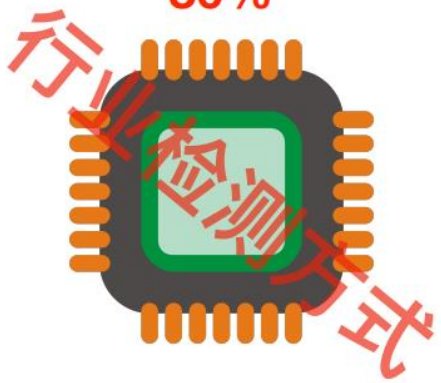
- 自动化固件安全扫描
- 自定义测试用例
- 与日常工作通知系统相结合
- 自动化漏洞告警，与办公IM联动
- 数据跨境检测
- 自动化评估报告
- 7*24小时安全监控

挑战与突破

挑战与突破:3D立体安全隐私检测

静态安全检测

30%



方式：固件安全检测。
优点：检测速度快，普通服务器即可实现。
缺点：误报率、漏报率高，检测维度有限，蓝牙、流量、硬件相关问题均无法检测。

动态安全检测

70%

方式：3D立体检测（硬件、蓝牙、网络等）
优点：覆盖面全、准确率高，维度广。
缺点：没有行业先例，IoT 通讯协议不统一，找不到能够支撑的硬件设备。

挑战与突破:3D立体检测引擎

难点：由于需要进行3D立体安全隐私扫描，行业内 没有一款引擎可以支持。

解决：

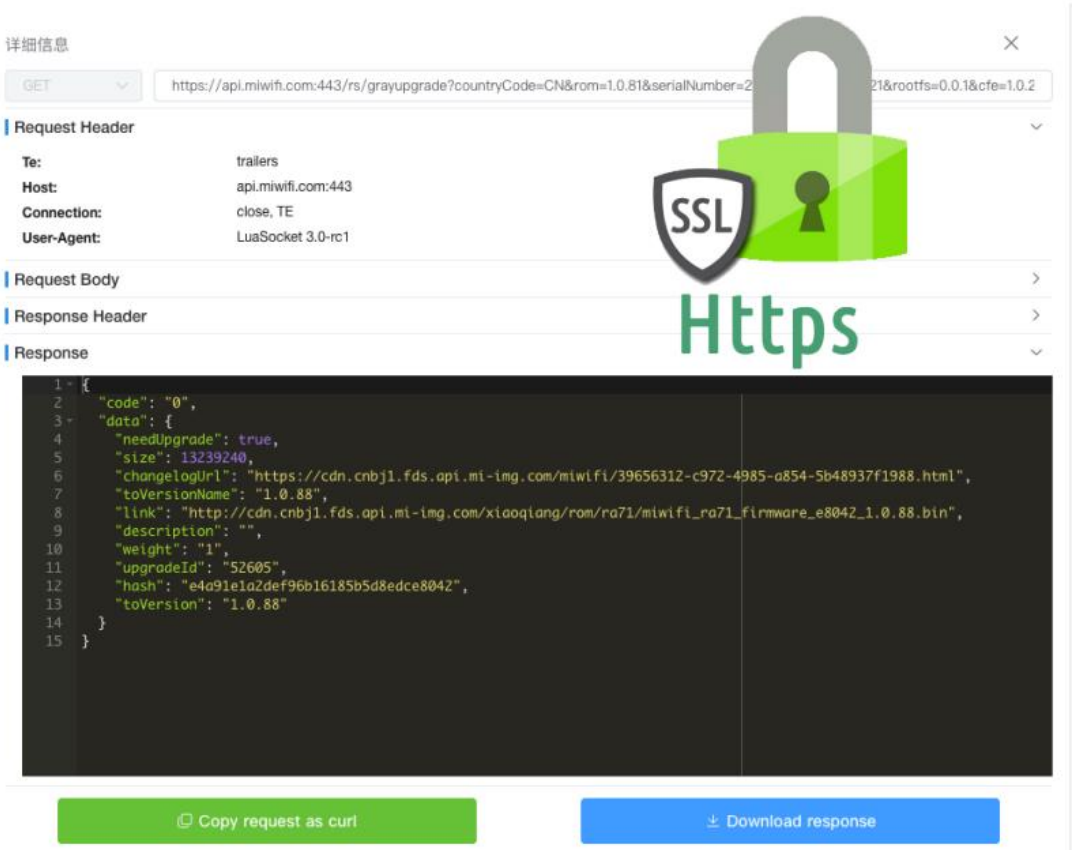
【平台】调研行业内20余款开发板，综合考虑软件兼 容性、硬件扩展性、易用性等因素，最终选择UP2作 为硬件平台。

【嗅探】行业内没有成品扩展卡能够支持BLE嗅探， 我们自己设计了硬件扩展板，实现了硬件能力。

【蓝牙】安全测试有修改蓝牙MAC地址的特殊需求， 一般网卡无法满足，我们选择了BCM板卡进行开发， 实现了硬件能力。

【网络】设备需要支持50+设备的WiFi接入，一般网 卡无法满足，我们选择了QCA芯片的工业级网卡， 并进行信号调优

挑战与突破:加密流量



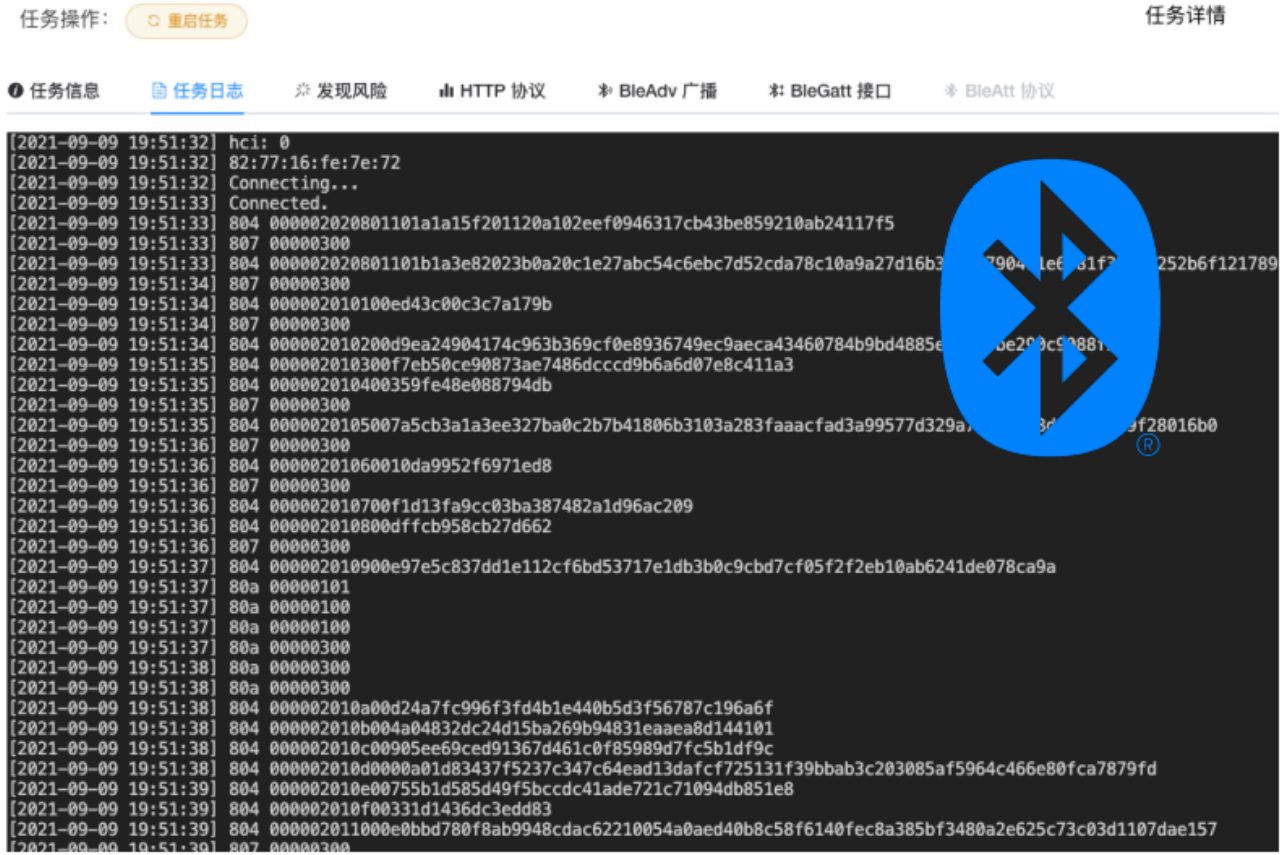
难点：越来越多设备使用 HTTPS 加密流量。我们需 要检查HTTPS加密的可靠性，需要能解密流量，检查 是否存在隐私问题。在满足需求的同时，不能影响设 备正常使用。行业内没有能够满足需求的产品。

解决：

【解密】在IoT设备中植入自签名根证书，引擎在设 备发起HTTPS请求的握手阶段，替换服务器证书，解 密加密流量。 【劫持】在握手阶段，根据服务器证书中的常用名称 等信息，伪造对应域名的二级证书，利用新生成的证书替换连接证书，判断设备是否接受。

【正常使用】在一次劫持失败后，将DST IP加入白名 单中，设备再次发起连接时直接放行

蓝牙



难点：BLE安全测试中，需要验证设备通讯协议的安 全性，重放攻击往往是最有效便捷的方式。但是，行 业内没有一款产品支持BLE重放测试。

解决：

【抓包】通过自研的BLE嗅探硬件板卡，对设备的 BLE通讯进行嗅探，通过解析BLE数据包，记录下 Handle、Data、Time等信息。

【重放】通过第一步记录的数据，使用BCM无线网 卡，通过BLE连接设备，按照时序发送数据，实现重 放安全测试。

落地实践和成果

漏洞挖掘应用

#	RSSI	MAC	Name	Company ID	Raw Data	Connect	Type	Time
1		3F:BF:69:AE:01:04		Apple, Inc.	02011a0bff4c000906030c0abd6209			2022-10-11 19:35:11
2		52:0F:8E:CD:9E:CD		Apple, Inc.	02011a020a0c0bff4c0010060c1da24b3a38			2022-10-11 19:35:11
3		60:A9:B1:59:7F:0C		Apple, Inc.	02011a020a0c0bff4c001006131eec2de7ed			2022-10-11 19:35:12
4		2C:9E:FD:15:4E:28		Apple, Inc.	02011a0bff4c00090603230abd5d1e			2022-10-11 19:35:12
5		3B:11:18:FB:08:3E		Xiaomi Inc.	17ff8f0313110011027342656636b20577524726038c00e04			2022-10-11 19:35:12
6		71:3C:5F:B9:0C:35		Apple, Inc.	02011a020a0c0aff4c0010054b1c654315			2022-10-11 19:35:12
7		38:53:D0:17:DA:29		Microsoft	1eff060001092002023 87cfd5f2b7bcc42323390e7fe758907eb3e0db42069			2022-10-11 19:35:12
8		5A:D5:6E:06:0E:03		Xiaomi Inc.	02010217ff8f032d1110184122343665341526080857010304830b0303aafd			2022-10-11 19:35:13
9		19:EA:EF:CD:CF:A9		Microsoft	1eff060001092002e094c9995fd2c19728412e974a032a4e947a2dbceec0d3			2022-10-11 19:35:13
10		4A:FA:55:34:76:95		Apple, Inc.	1eff4c000719010f2000f38f00000459cfc6911412d075ab28728593759047			2022-10-11 19:35:13
11		8C:5A:F8:37:E5:6A		Xiaomi Inc.	02010217ff8f030a10ffffff655551433968de2011080810172534030 3aafd			2022-10-11 19:35:13
12		4D:D1:7A:48:E9:23		Apple, Inc.	0201060aff4c0010050118d7a2a1			2022-10-11 19:35:13
13		8C:85:90:6E:27:D0		Apple, Inc.	0201060aff4c0010054b1c41d577			2022-10-11 19:35:16
14		8C:5A:F8:EE:DB:E8		Xiaomi Inc.	0fff8f030a10ffffff4caa31d41b0de0303aafd			2022-10-11 19:35:16
15		5E:92:B5:92:45:D7		Apple, Inc.	02011a020a180aff4c0010050018276a3d			2022-10-11 19:35:17
16		20:4C:03:8E:E2:A4	dAEA00000AEe@r156;...	Apple, Inc.	0201041aff4c0002154152554ef99b4a3b86d0947070693a7800000000c81e0964414541303030303041456540723135363b7e333b2b4f43462d4...			2022-10-11 19:35:17
17		68:E1:EB:31:8E:D1		Apple, Inc.	02011a020a080cff4c001007251f999d5d5958			2022-10-11 19:35:17
18		16:FB:DF:0E:7E:0C			03036ffd17166ffd354161e8f09ed47bfe5d4d04a9d2453c6737ca26			2022-10-11 19:35:17
19		1E:54:0C:DC:75:F9		Microsoft	1eff0600010920024e2add7f7b8b6794b32c6cad20715e19124fc7d23ba94e			2022-10-11 19:35:17
20		DF:82:6D:4E:87:58		Apple, Inc.	07ff4c0012020001			2022-10-11 19:35:17
21		4F:A5:59:84:F6:BE		Apple, Inc.	02011a1bff4c000c0e00859c665918869c8487ce2d4f711006451dd1de5b68			2022-10-11 19:35:17
22		20:4C:03:8E:E2:78		Apple, Inc.	0201041aff4c0002154152554ef99b4a3b86d0947070693a7800000000c8			2022-10-11 19:35:17
23		51:1B:D1:83:84:B6		Xiaomi Inc.	02010217ff8f032d1110184122343133331526080857010304830b0303aafd			2022-10-11 19:35:18
24		74:93:B8:19:95:57		Apple, Inc.	02011a020a080cff4c001007331fedfcb8b018			2022-10-11 19:35:18
25		7C:B5:AF:89:8A:C4		Microsoft	1eff060001092002059b442178a23a3ae470591879bf439c8d09385478f7c3			2022-10-11 19:35:18

蓝牙广播捕获

漏洞挖掘应用

蓝牙广播解析

漏洞挖掘应用

Handles	Service > Characteristics	Properties	Data
1 -> 7	Generic Access Profile (00001800-0000-1000-8000-00805f9b34fb)		
2	Device Name (00002a00-0000-1000-8000-00805f9b34fb)	READ NOTIFY	b'\x12\x03\x00\x00''
4	Appearance (00002a01-0000-1000-8000-00805f9b34fb)	READ	b'\x02\x05\x00\x01''
6	Peripheral Preferred Connection Parameters (00002a04-0000-1000-8000-00805f9b34fb)	READ	b'\x02\x07\x00\x04''
8 -> 11	Generic Attribute Profile (00001801-0000-1000-8000-00805f9b34fb)		
9	Service Changed (00002a05-0000-1000-8000-00805f9b34fb)	INDICATE	
12 -> 21	0000fdab-0000-1000-8000-00805f9b34fb		
13	0000aec9-0000-1000-8000-00805f9b34fb	READ	b'\x02\x0e\x00\xc9\x00'
15	0000aec8-0000-1000-8000-00805f9b34fb	NOTIFY	
18	0000aec7-0000-1000-8000-00805f9b34fb	WRITE NO RESPONSE WRITE	
20	0000aecb-0000-1000-8000-00805f9b34fb	WRITE NO RESPONSE WRITE	
22 -> 53	Xiaomi Inc. (0000fe95-0000-1000-8000-00805f9b34fb)		
23	00000004-0000-1000-8000-00805f9b34fb)	READ	b'\x02'
26	00000010-0000-1000-8000-00805f9b34fb)	WRITE NO RESPONSE NOTIFY	
30	(00000019-0000-1000-8000-00805f9b34fb)	WRITE NO RESPONSE NOTIFY	
34	0000017-0000-1000-8000-00805f9b34fb)	WRITE NOTIFY	
38	00000018-0000-1000-8000-00805f9b34fb)	WRITE NO RESPONSE NOTIFY	
42	0000001a-0000-1000-8000-00805f9b34fb)	WRITE NO RESPONSE NOTIFY	
46	0000001b-0000-1000-8000-00805f9b34fb)	WRITE NO RESPONSE NOTIFY	
50	0000001c-0000-1000-8000-00805f9b34fb	WRITE NO RESPONSE NOTIFY	
54 -> 62	00000100-0065-6c62-2e74-6f696d2e696d)		
55	00000101-0065-6c62-2e74-6f696d2e696d)	WRITE NO RESPONSE	
59	(00000102-0065-6c62-2e74-6f696d2e696d)	NOTIFY	

GATT 枚举

漏洞挖掘应用

蓝牙嗅探和重放

漏洞挖掘应用

```
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.authenticator()
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.cache()
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.callTimeoutMillis()
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.certificatePinner()
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.connectTimeoutMillis()
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.connectionPool()
[2022-10-11 19:50:41] [TRACE] okhttp3.OkHttpClient.connectionSpecs()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.cookieJar()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.dispatcher()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.dns()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.eventListenerFactory()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.followRedirects()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.followSslRedirects()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.hostnameVerifier()
[2022-10-11 19:50:42] [TRACE] okhttp3.OkHttpClient.interceptors()
[2022-10-11 19:50:43] [TRACE] okhttp3.OkHttpClient.internalCache()
[2022-10-11 19:50:43] [TRACE] okhttp3.OkHttpClient.networkInterceptors()
[2022-10-11 19:50:43] [TRACE] okhttp3.OkHttpClient.newBuilder()
[2022-10-11 19:50:43] [TRACE] okhttp3.OkHttpClient.newCall(okhttp3.Request)
[2022-10-11 19:50:43] [TRACE] okhttp3.OkHttpClient.newWebSocket(okhttp3.Request,okhttp3.WebSocketListener)
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.pingIntervalMillis()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.protocols()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.proxy()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.proxyAuthenticator()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.proxySelector()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.readTimeoutMillis()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.retryOnConnectionFailure()
[2022-10-11 19:50:44] [TRACE] okhttp3.OkHttpClient.socketFactory()
[2022-10-11 19:50:45] [TRACE] okhttp3.OkHttpClient.sslSocketFactory()
[2022-10-11 19:50:45] [TRACE] okhttp3.OkHttpClient.writeTimeoutMillis()
[2022-10-11 19:50:45] [CALL] ------> okhttp3.OkHttpClient.protocols() [SourceFile]
[2022-10-11 19:50:45] RETURN(java.util.Collections$UnmodifiableRandomAccessList): "[object Object]"
[2022-10-11 19:50:45]
[2022-10-11 19:50:45] [CALL] ------> okhttp3.OkHttpClient.connectionPool() [SourceFile]
[2022-10-11 19:50:45] RETURN(okhttp3.ConnectionPool): "okhttp3.ConnectionPool@5b473a9"
[2022-10-11 19:50:45]
[2022-10-11 19:50:45] [CALL] ------> okhttp3.OkHttpClient.eventListenerFactory() [SourceFile]
[2022-10-11 19:50:45] RETURN(_m_j.nej$1): "[object Object]"
[2022-10-11 19:50:45]
[2022-10-11 19:50:45] [CALL] ------> okhttp3.OkHttpClient.callTimeoutMillis() [SourceFile]
[2022-10-11 19:50:45] RETURN(number): "0"
[2022-10-11 19:50:45]
[2022-10-11 19:50:45] [CALL] ------> okhttp3.OkHttpClient.newCall(okhttp3.Request) [SourceFile]
[2022-10-11 19:50:45] ARGS[0](okhttp3.Request): "Request{method=POST, url=https://de.api.io.mi.com/app/mipush/eventsubbatch, tags={class java.lang.Object=vlS3PNl4eVFQRcJgX840hQ==}}"
[2022-10-11 19:50:45] RETURN(okhttp3.RealCall): "[object Object]"
[2022-10-11 19:50:45]
[2022-10-11 19:50:46] [CALL] ------> okhttp3.OkHttpClient.dispatcher() [SourceFile]
[2022-10-11 19:50:46] RETURN(okhttp3.Dispatcher): "okhttp3.Dispatcher@6c8ed2e"
[2022-10-11 19:50:46]
```

自动化Firda hook

发明专利

1. IoT 网络环境模拟方案 202010011507.2

2. IoT 设备漏洞检测实现方法 201911299917.5

3. 中间人智能劫持方案 201911279682.3；111092878B

成果

50+

安全检测能力

500+

检测设备数量

2700+

发现安全漏洞

15分钟

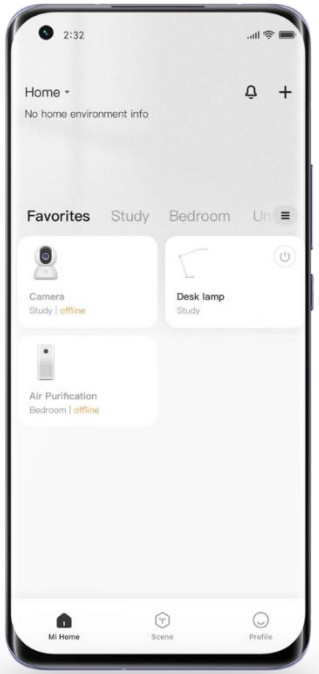
测试时间从一周
缩短到15分钟

认证

2021年8月11日，小米360°家用安全摄像头获得了英国标准学会(BSI)的Kitemark™的家用IoT设备类别 认证。获得Kitemark™认证意味着小米产品符合最佳安全 实践，包括欧洲电信标准协会（ETSI）发布的EN303645标准。这标志着小米在保护消费者信息安 全和隐私方面取得了又一个里程碑。

IoT产品获得的国际安全认证**

根据目前较通用的安全标准EN303645，联合权威机构，对小米多款产品进行了详细测试，并取得认证



密码策略　安全通信　安全更新　漏洞管理

安全存储　输入验证　隐私保护　安全恢复

EN303645消费IoT设备安全基线要求　OWASP ASVS　NIST8259物联网设备安全指南

展望未来

展望

成为 IoT 产品出海的“金钥匙” 为汽车安全保驾护航

THANKS