EISS-2019企业信息安全峰会

北京站/3.29

IoT安全

白嘎力 Rokid公司

Who Am I

白嘎力　　信息安全工程师

领域：Android安全，IoT，逆向工程，漏洞挖掘

PKAV，360信息安全，360企业安全，Rokid公司

今天的IoT

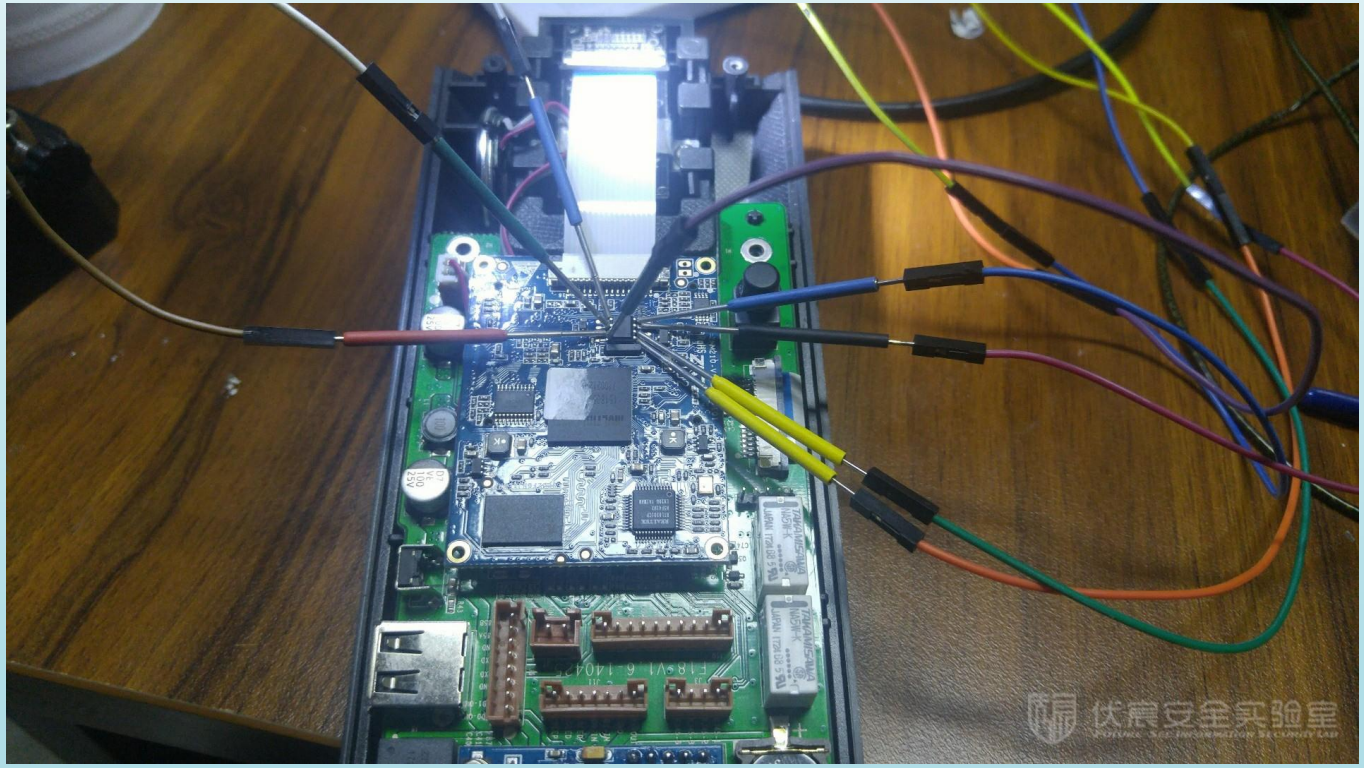
10亿设备接入：2020年

4 个维度威胁：硬件，软件，云安全，设备互联

4 个严重态势：车联网，智慧医疗，智慧城市，智能家居

硬件安全

硬件分析：芯片，电路
固件分析：提取，逆向
协议分析：网络，USB
硬件调试：串口，jtag
硬件修改：硬改，软改



软件安全

软件漏洞，协议漏洞，OTA升级，

DNS劫持，硬编码口令，WIFI，

蓝牙，ZigBee，第三方库，开源软件，

硬编码的秘钥，系统漏洞，监测监控，

云服务

APP接口，服务端安全，指令下发，

升级服务器，各类传统安全，

MQTT服务，链路加解密，

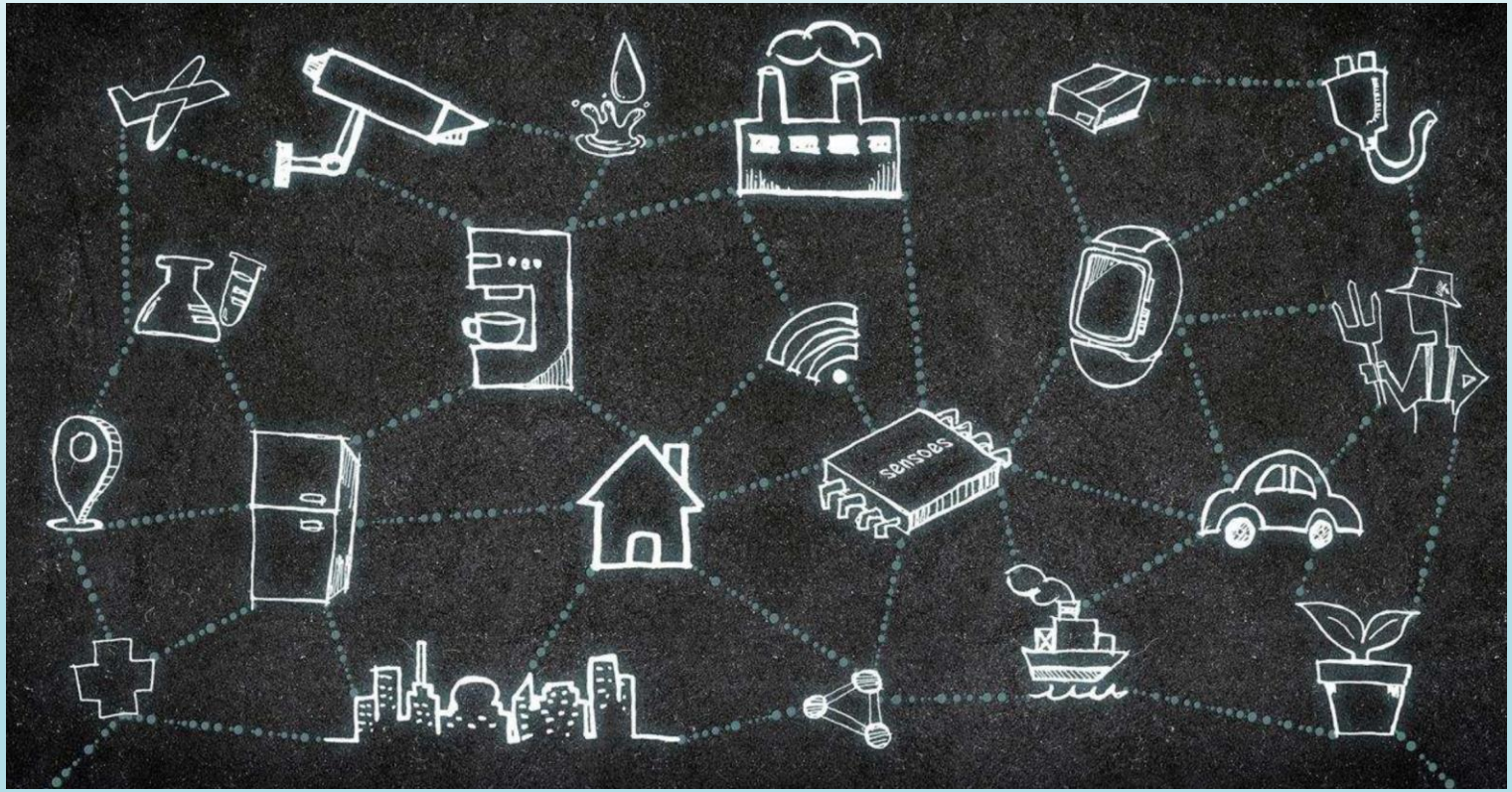
敏感信息存储，秘钥传输使用

设备互联

设备之间互联存在开放协议

标准不统一，缺乏共识

协议加解密，秘钥交换



IoT 安全

硬件安全

芯片

- 硬件调试
- 硬件破解
- 硬件修改
- 软件修改

固件

- 固件提取
- 固件逆向

软件安全

漏洞

- 软件漏洞
- OTA升级
- 开源软件
- 第三方库
- 系统漏洞
- 硬编码

协议

- 秘钥交换
- 加解密
- WIFI
- 蓝牙
- DNS
- ZigBee

云服务，APP

本地应用

- 接口
- 秘钥
- 加固
- 逆向

云服务

- MQTT
- 云服务器
- 指令下发
- 应急响应

设备互联

协议不统一

- 碎片化
- 标准不统一
- 自定义
- 厂商多
- 适配难
- 协议漏洞
- 秘钥交换
- 类型不一样

AIoT

语音

语音识别，语音合成，智能唤醒，自然语音处理，声纹识别、支付、身份验证

图像

人脸识别，活体、文字识别，场景、物识别，图片内容检索，图像搜索

智慧

智慧医疗，智慧城市，智慧交通，智能家居，车载应用，智能音箱，智慧应用

近期的案例

事件	案例	出处	类型
2018年	AI模型逆向	360 HITB （Likang）	逆向
2018年	Amazon Echo cracked（Tencent）	Tencent BH 2018	Dos
2018年	How to Hack a Bluetooth Lock	CVE-2016-10115	bof
2017年	Netgear Arlo Webcam	-	bof
2017年	Dyn DDoS	-	DDOS
2017年	Mirai病毒	DVR摄像头	口令
2017年	某汽车重放攻击	钥匙信号重放	重放

智能设备主要安全隐患

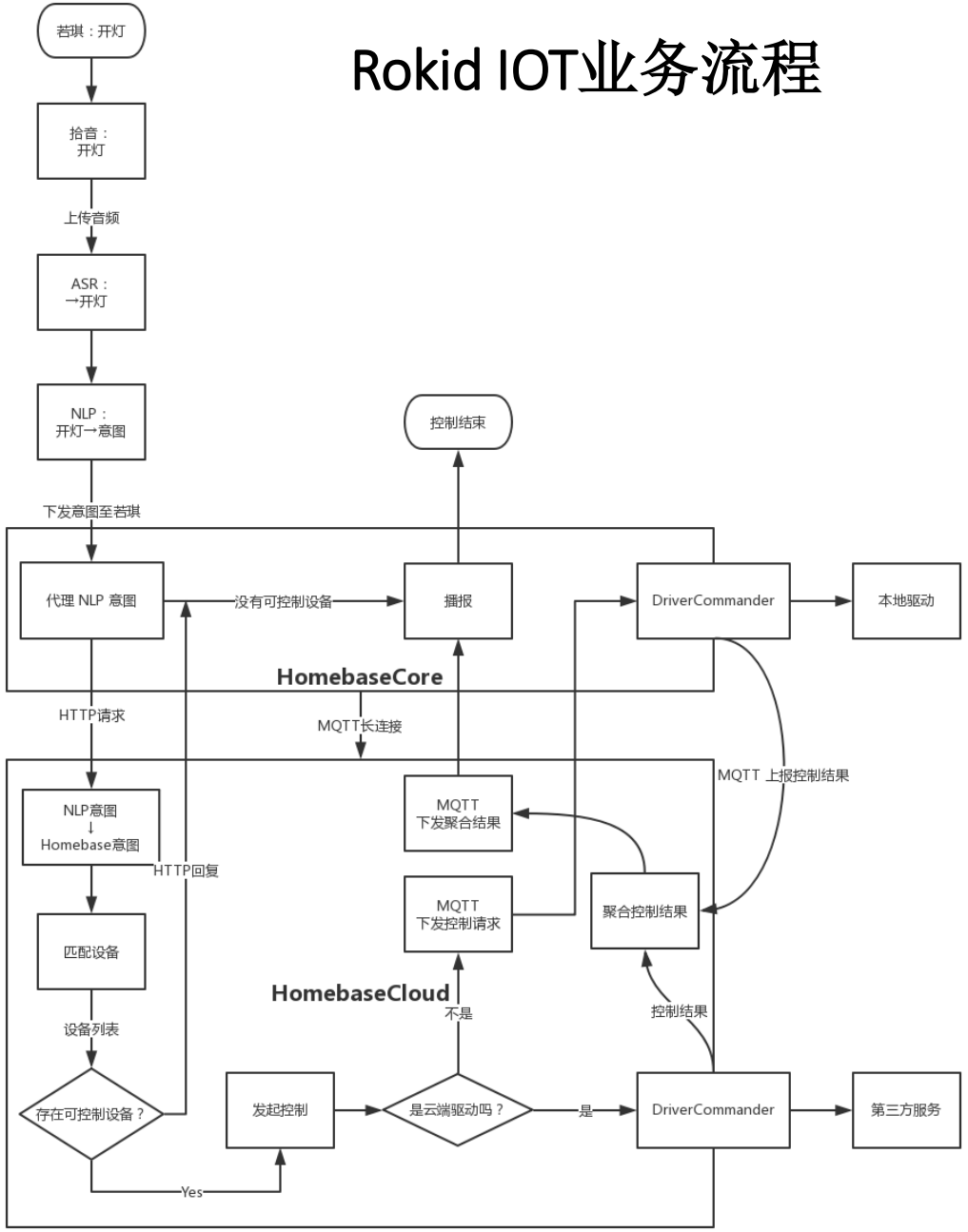
开放调试接口

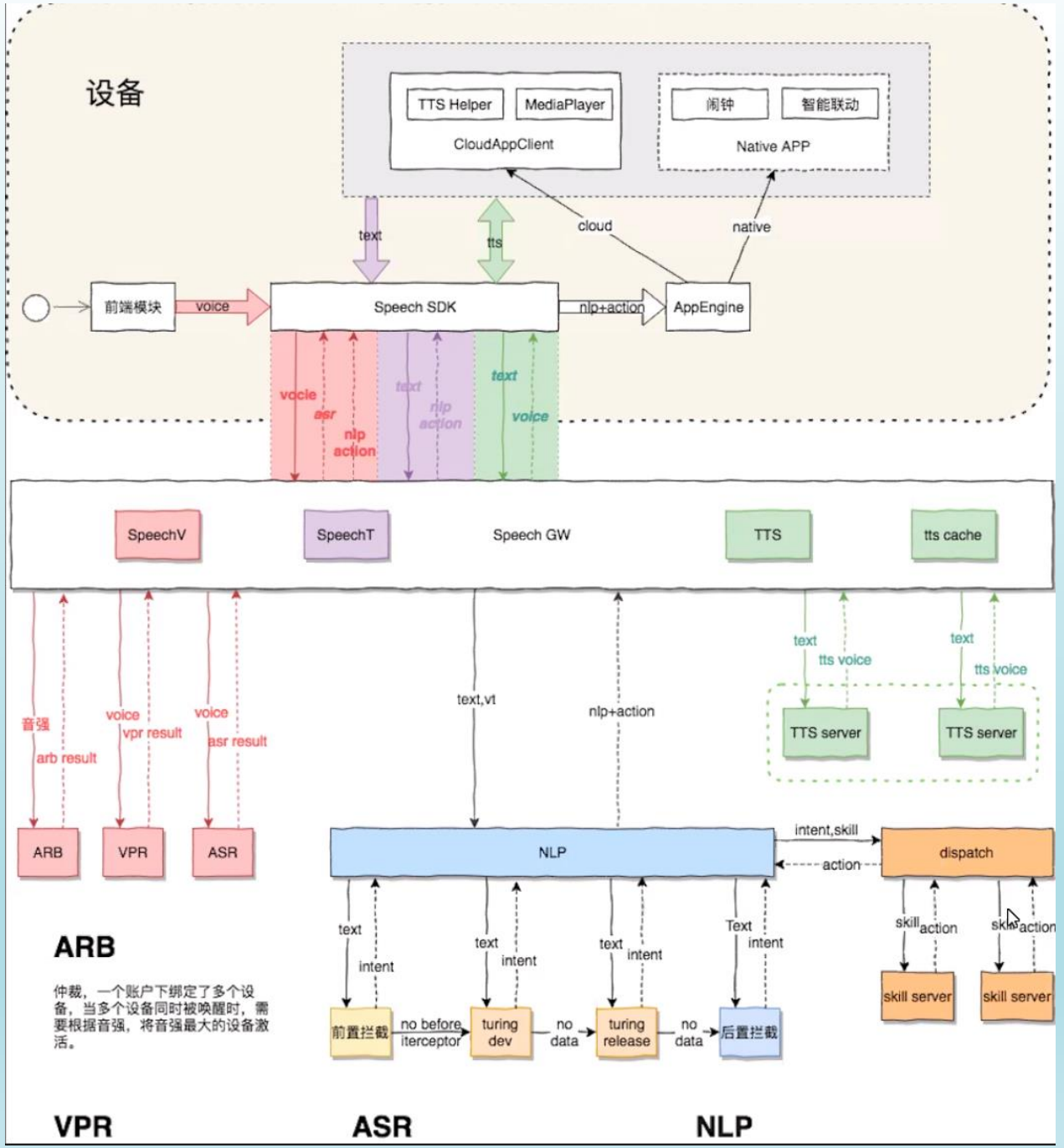
弱口令，默认口令

语音控制模块具备设备操作功能

版本更新机制，OTA劫持，链路劫持等

Rokid IOT业务流程

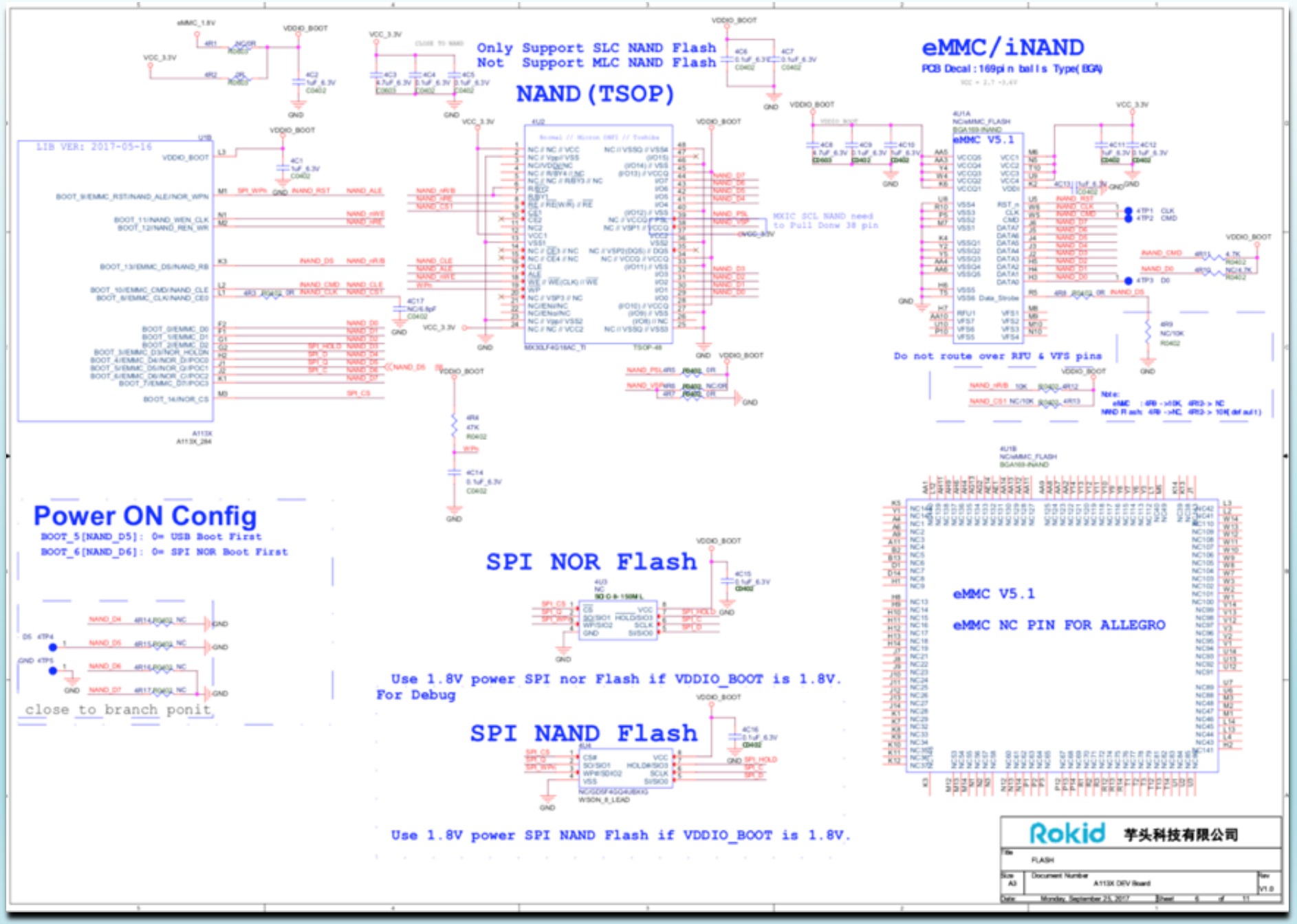




IOT底层架构

Armlogic 架构

存储以及处理器架构



软件的攻防

防护

现在的加固以混淆为目的，运行环境中自身解密，虚拟主机保护的防护手段

攻击

操作系统底层绕过防护限制，寻找加固代码逻辑漏洞，内存还原技术

反逆向

反调试

代码混淆

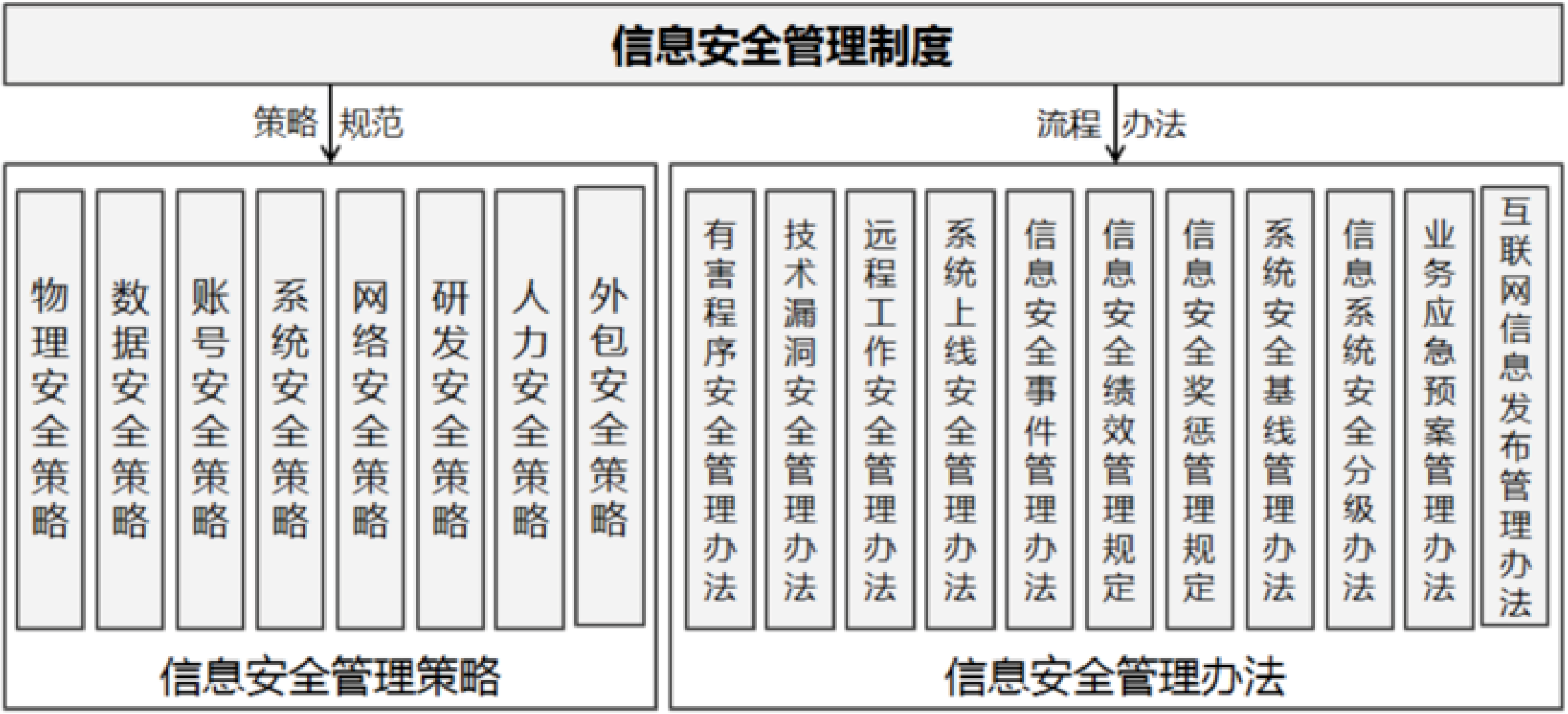
逆向工程

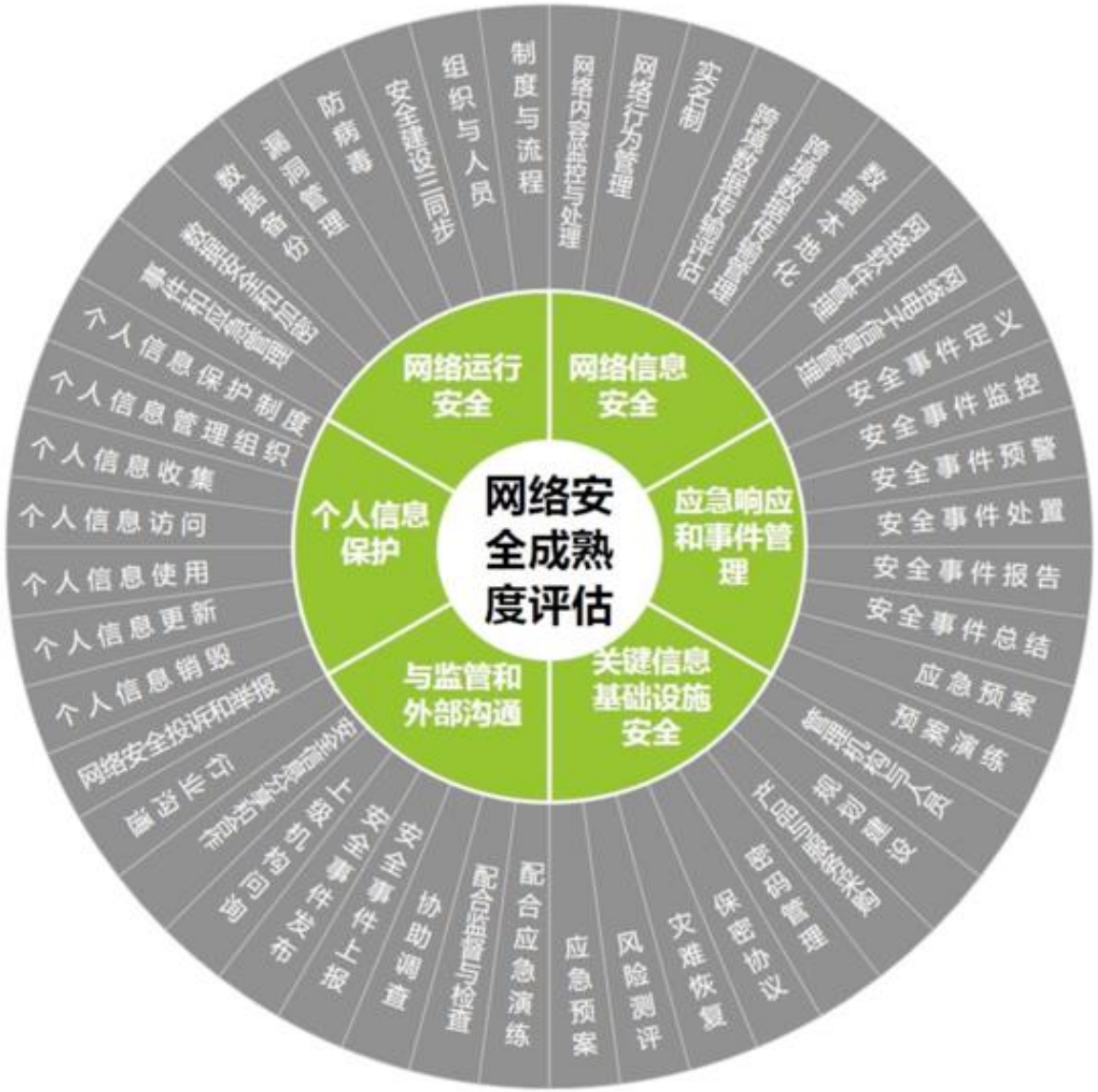
反反调试

代码逻辑漏洞

One	Two	Three	Four
国内App加固技术没有本质上的改变，依然使用20年前的技术	没有破解不了的"壳"，只是破解成本上提升，防止自动化破解	传统加壳软件不修改程序代码，加固引擎效果差	新一代加固方法修改软件代码，在虚拟机环境中自带解密引擎。如(vmprotect)


APP安全防护需求
渠道以及盗版App市场监控
防止逆向，篡改，调试，二次打包
脱壳后的相似App监控
核心算法，核心技术的保护
签名数据对比分析
界面劫持，木马感染，代码注入
APP 运行环境加固
应用源代码加固
防止盗版
应用环境保护
渠道监测监控
加固需求
漏洞扫描
风险控制
存储安全
通信安全
元数据收集分析
秘钥存储，交换
互联网数据传输安全
支付，充值防护
账户，设备绑定
钓鱼诈骗防护
IP地址，身份认证溯源
APP业务安全


信息安全管理制度
策略
规范
流程
办法
物理安全策略
数据安全策略
账号安全策略
系统安全策略
网络安全策略
研发安全策略
人力安全策略
外包安全策略
信息安全管理策略
有害程序安全管理办法
技术漏洞安全管理办法
远程工作安全管理办法
系统上线安全管理办法
信息安全事件管理办法
信息安全绩效管理规定
信息安全奖惩管理规定
系统安全基线管理办法
信息系统安全分级办法
业务应急预案管理办法
互联网信息发布管理办法
信息安全管理办法



网络安全合规

出海业务GDPR

网安等保合规

Iso27000

工信部信息安全合规

电信移动安全合规

移动信息安全合规

联通信息安全合规

AI系统，AI模型安全漏洞

算法样本对抗

AI模型或者算法呗攻击，导致人工智能所驱动识别系统出现混乱，误判或者失效

攻击者可能通过修改现有的训练集生成恶意样本。

比如病毒样本的优化，攻击载荷的逃避监测系统等等案例

AI系统，AI模型安全漏洞

AI系统自身安全漏洞

基于数据流旋盖的任意内存修改，写入等漏洞导致输出结果存在误报，错乱。
也可以通过缓冲区溢出等方法控制数据输入流，任意代码执行，堆栈溢出。

个人隐私保护挑战

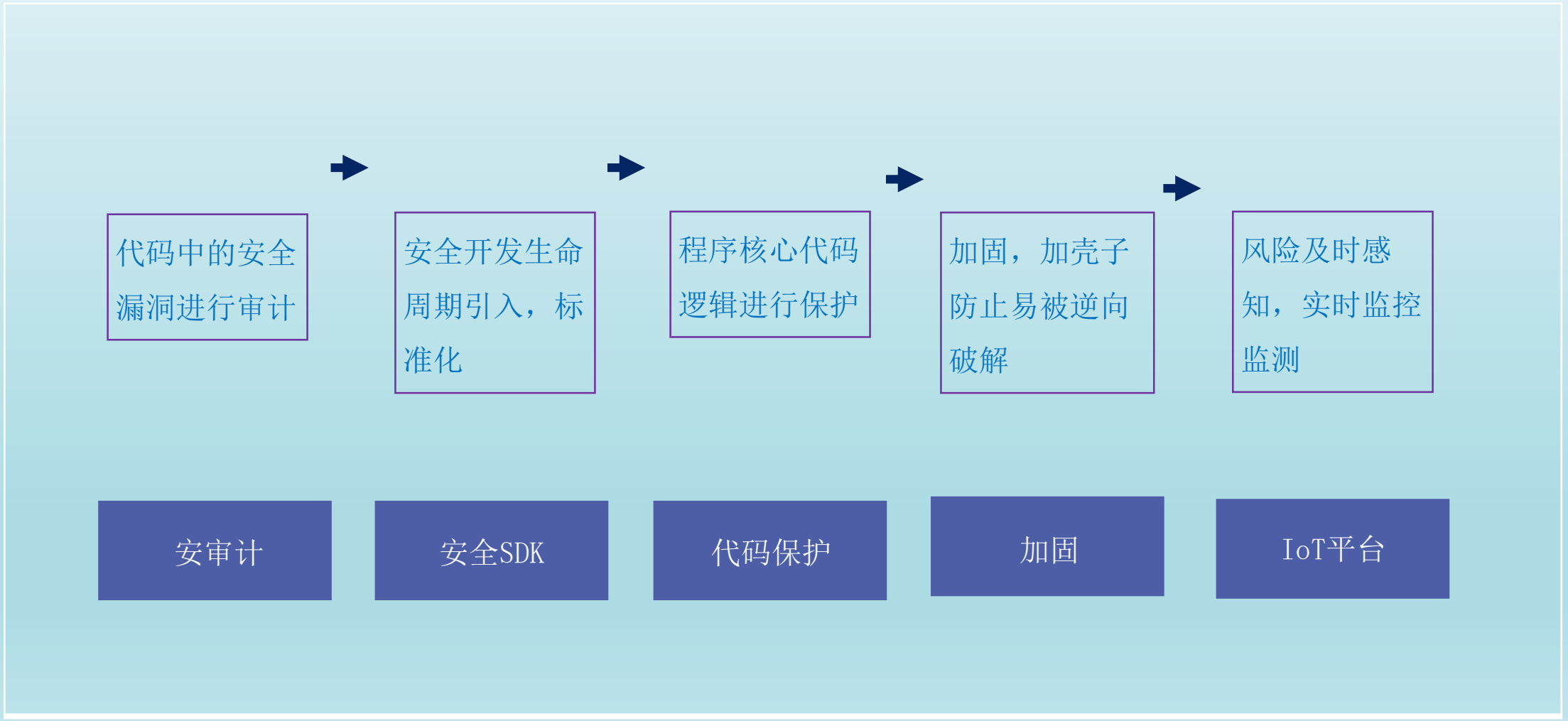
大量的数据进行分析以及训练。
导致用户元数据，生物特征存在泄漏风险加大。

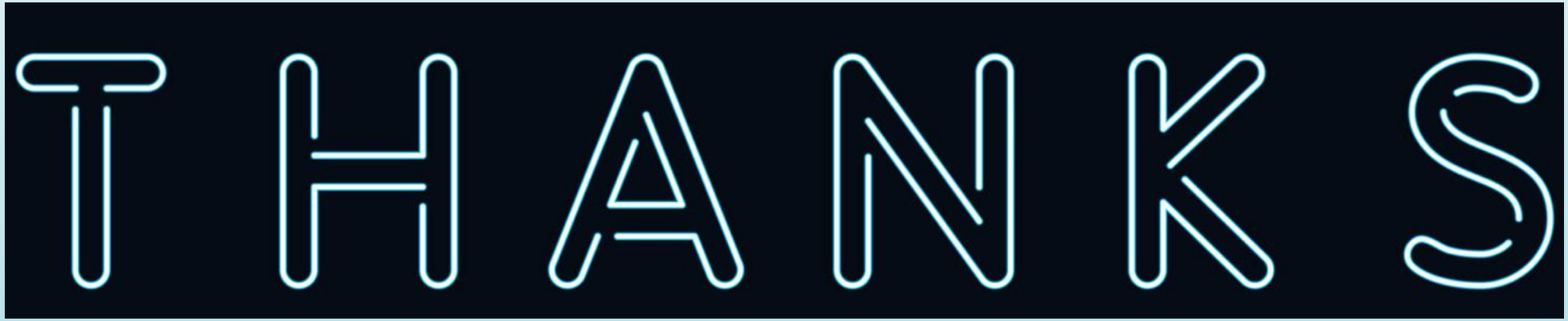
定制化服务，定制化应用需要大量个人信息的基础。

AIoT的个人信息保护意识薄弱，相关的标注不透明导致个人信息将会滥用。
比如征信，行为分析，金融风控。


处理层
AI
认证
授权
管理
...
远程应用程序更新
移动控制终端
网关端
传输层
MQTT
COAP
XAMPP
HTTP
设备ID
DNS防护
.....
4G
NB-IoT
WiFi
ZigBee
安全芯片
内存安全
.....
应用层
远程应用程序更新
基于可信执行环境的应用程序加
抗拒绝服务攻击
对应用程序镜像进行加密签名
第三方代码审计
隐私管理
应用程序架构中执行职责分离
安全用户界面
授权的数据收集
系统固件层
安全的终端身份验证机制
安全启动
使用经过验证的随机数发生器
远程系统更新
执行可信计算基
执行操作系统层级安全增强功能
日志和诊断
异常检测
禁用调试和测试技术
硬件层
使用防篡改产品外壳
执行存储器保护
实施环境锁定阈值
端口防护阻止冷启动
使用内部存储器处理加密信息
设置电量警告阈值
唯一的终端标识
使用安全芯片或TEE
设备停用和废弃

规避风险


代码中的安全漏洞进行审计
安全开发生命周期引入，标准化
程序核心代码逻辑进行保护
加固，加壳子防止易被逆向破解
风险及时感知，实时监控监测
安审计
安全SDK
代码保护
加固
IoT平台


THANKS