2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

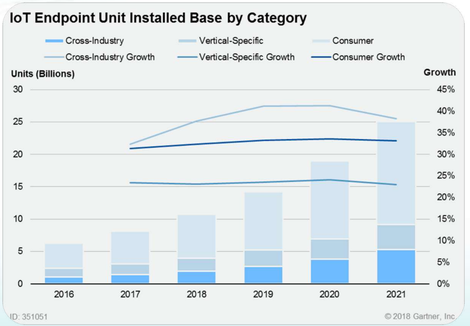
构建IoT终端自适应安全体系

主讲人：陈彪

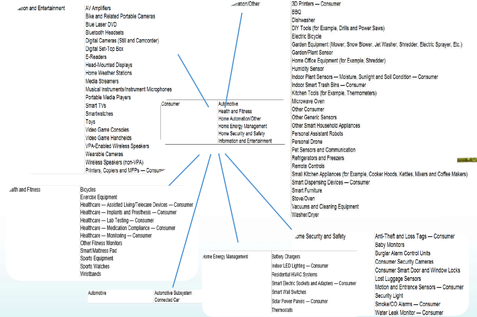
CONTENTS

目 录

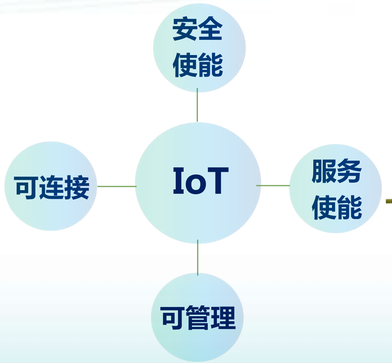
IoT终端的结构



海量的终端



碎片化的终端



归一化的功能

归一化的结构

IoT终端的攻击面

攻击COST

1 通信安全

- 通信认证、加密和完整性漏洞

2 软件安全

- 固件安全/OS安全/应用安全/配置安全服务安全脆弱性

3 硬件安全

- 主板、总线物理接口调试/侧信道和注入式攻击

防御COST

IoT终端的安全需求

信任根（RoT）的实现

安全启动

安全的初始化和认证

安全的加密服务集

应用安全保证

终端生命周期安全

IoT终端自适应安全体系

从预测、防护、检测和响应四个维度建设IoT终端安全体系

IoT终端应用保护

应用保护对象的基本分类

RICH环境

- 功能强、具备完善的计算机结构、支持嵌入式OS或通用OS
- 如智能盒子、车机、POS机等

RTE环境

- 仅具有基本功能和有限计算能力，如MCU、SoC等、支持嵌入式软件
- 如水表、气表、停车锁、传感器等

编译全生命周期保护

源码 → IR层 → 二进制

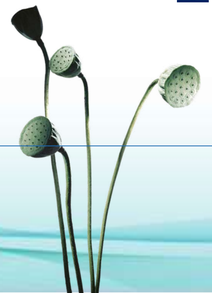
源码	IR层	二进制
字符串加密	基本块切割	ELF加壳
反调试	指令替换	SO加壳
控制流混淆	字符串加密	虚假控制流
反HOOK	控制流混淆	虚拟化保护（IRVMP）
不透明谓词	密钥白盒	
密钥白盒		
完整性保护		

运行时漏洞缓解

- 防动态调试
- 密钥白盒
- 反HOOK
- 控制流CFI
- 完整性保护

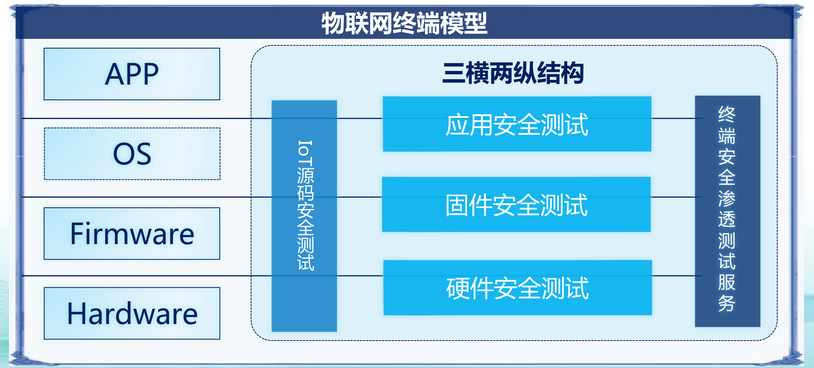
IoT终端应用保护

基于SIM、SE、vSE提供IoT终端信任根服务



IoT终端安全测试体系

IoT安全测试体系



提供**三横两纵**结构的IoT终端安全测试体系覆盖；通过工具和服务方式、覆盖白盒、黑盒、灰盒测试

硬件安全测试

- 侧信道测试
- 故障注入测试
- SE安全测试、TEE安全测试

源码测试

- 基于编译器技术的源码分析

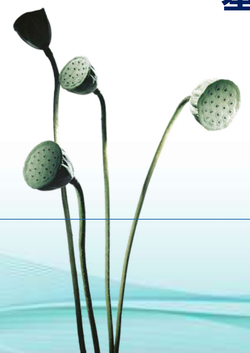
固件&应用安全测试

- 逆向解包、软件成分分析、漏洞分析
- 基于符号执行的二进制扫描
- 嵌入式软件安全测试

IoT渗透测试服务

- 覆盖终端安全、管安全和云安全
- 执行完整的业务安全测试

下一代源码安全测试



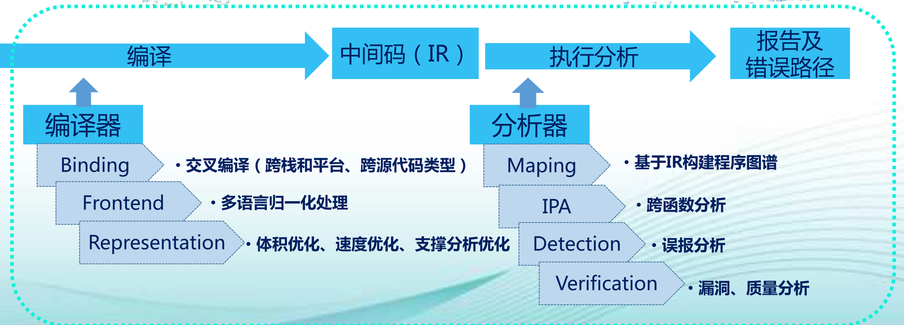
基于编译器的下一代源码分析工具

- Enable碎片化平台上下文的漏洞扫描
- Testing到Verification
- 以垂直行业法规模板要素去索引有价值的漏洞问题

传统静态分析工具分析原理

源代码
- C/C++
- Python
- Java
- JavaScript
- Kotlin
- GO
- ...

梆梆安全下一代源码测试分析原理



IoT终端安全响应体系

构建运营漏洞治理体系

1 建立完整的“资产”视角

2 建设漏洞库

- 漏洞
- 恶意代码

资产上下文

3 建设漏洞评级机制

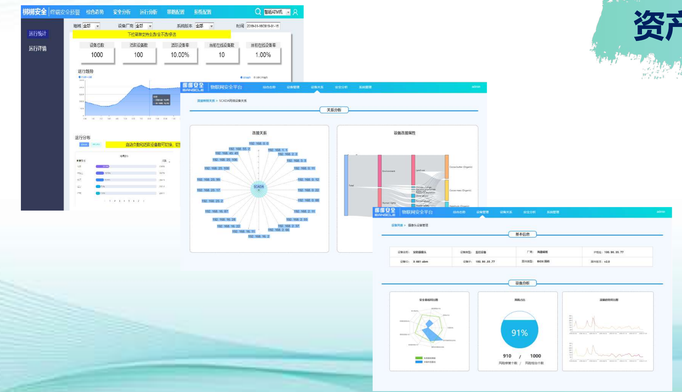
- 危害等级
- 解决方案

业务上下文

4 实现漏洞修复

- OTA
- 厂商补丁工具
- 其他处置方案

IoT终端安全预测体系



资产可视化、管理赋能

- 面向IoT环境、OT环境
- 多个维度呈现资产系统整体运行态势
- 设备全生命周期管理
- 设备关系图谱可视化

资产感知

威胁感知

威胁管理

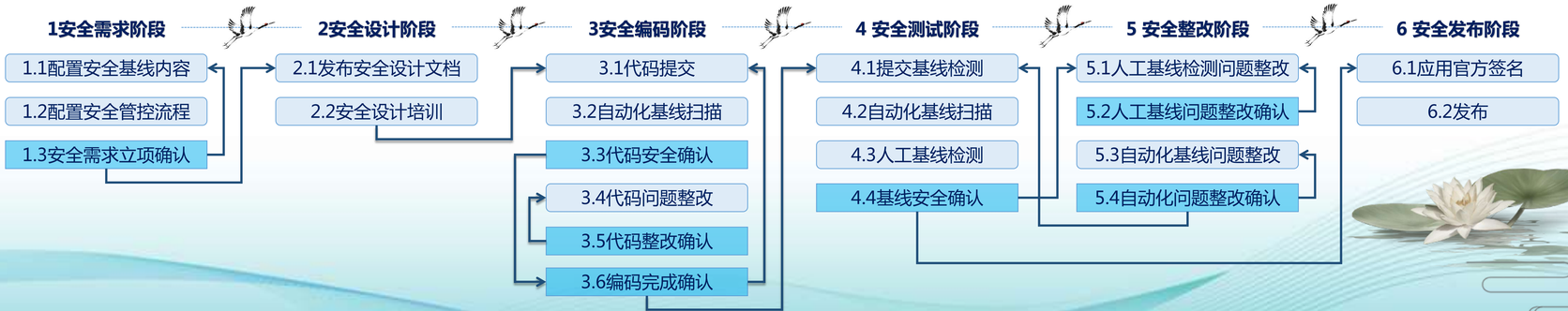
- 从多个维度全面监测设备安全风险和安全态势
- 执行高级威胁分析、如攻击链条回溯

非法root	非法网络访问	非法应用安装
外设异常	终端风险进程	终端位置异常
终端文件异常	终端流量异常	终端运行异常

IoT终端安全质控体系

作为IoT场景下全供应链基线管控的重要实践，应用安全开发管控平台基于IoT应用的用户场景、通过威胁场景分析和威胁建模、结合对具体合规政策的落地。打造行业专属的基线标准和响应流程，匹配自动化和半自动化的检测管理，从技术、管理等维度整体提高IoT应用安全质量水平

- 基于IoT具体业务Usercase形成基线
- 适配全体系供应链的管控流程，打造一致的质量体系标准
- 开放对接各类IT工具、OT工具及安全检测工具、全面提升检测的自动化水平、提升效率
- 针对基线和流程要求，提供可落地的方案和套件、赋能开发体系和供应链体系



THANK YOU

谢　　谢　　观　　看