KCon

纵横

服务器可信与硬件安全实践

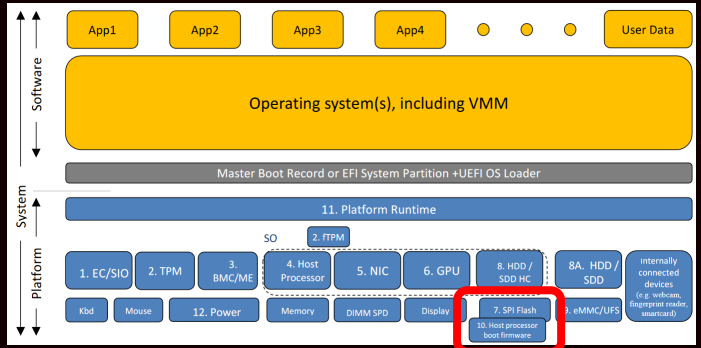
演讲者：杨韬

目录

- **启动安全威胁**
- 政策与行业
- 腾讯实践探索

启动安全威胁

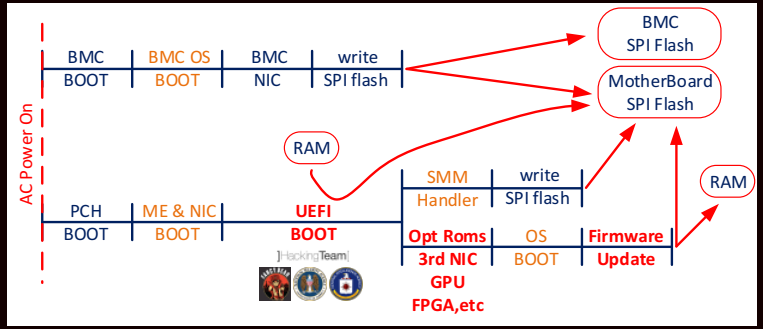
服务器系统构成



启动安全威胁

启动链威胁

红色：已知在野案例
橙色：实验案例



启动安全威胁

案例
- Apt28-Lojax，首个针对UEFI BIOS的持久化攻击
- NSA，针对戴尔、惠普服务器的BIOS后门泄密
- CIA，针对苹果计算机的BIOS间谍工具泄密

威胁来源
- 安全漏洞
- 物理接触（邪恶女仆）
- 供应链

更隐蔽、更顽固

目录

- 启动安全威胁
- **政策与行业**
- 腾讯实践探索

等保2.0要求

第一级安全要求

分类要求	可信验证要求内容
安全（通信网络|边界区域|计算环境）	可基于可信根对（通信|边界|计算）设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

等保2.0要求

二、三、四级要求

分类要求	可信验证要求内容
第二级	• 可信验证对象增加重要配置参数和应用程序 • 验证结果形成审计记录送至安全中心
第三级	在应用程序的关键执行环节进行动态可信验证
第四级	• 在应用程序的**所有执行环节**进行动态可信验证 • 进行动态关联感知

业界回顾

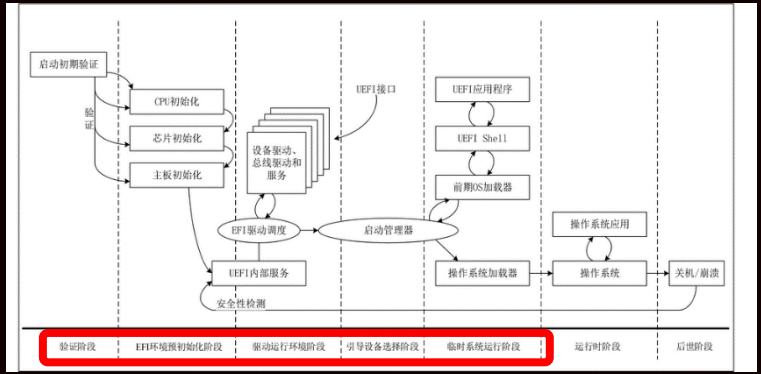
- 谷歌，专用芯片titan，固件校验与通信网关
- 亚马逊云，智能网卡nitro，固件校验与更新，主机对固件只读
- 微软，层级化可信根Cerberus，类似谷歌
- 华为，自研BMC
- 浪潮，自研BMC + 国产可信模块
- EDR行业，增加PC端查杀能力

目录

- 启动安全威胁
- 政策与行业
- **腾讯实践探索**

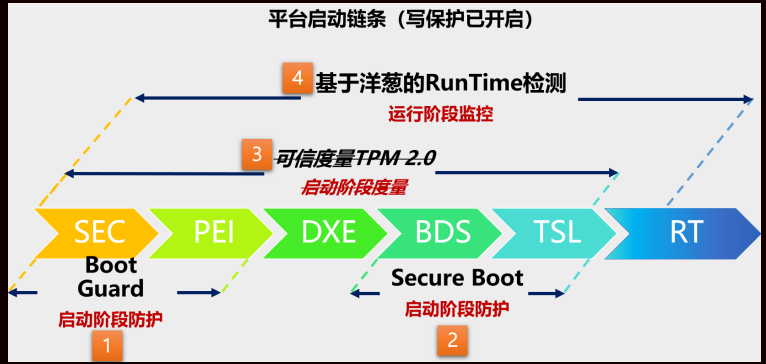
腾讯探索实践

UEFI启动过程



腾讯探索实践

防护链展示



腾讯探索实践

洋葱运行时监控

BIOS镜像校验

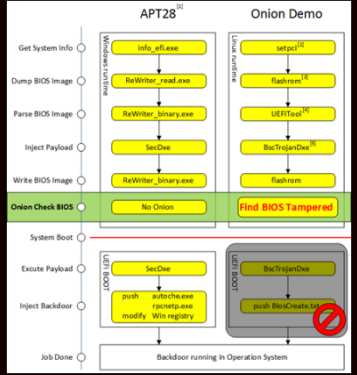
- 周期导出BIOS镜像
- 拆分UEFI文件系统
- 对比厂商原始BIOS镜像

硬件配置基线校验

- 主板BIOS写保护状态
- BootGuard
- Secure Boot

腾讯探索实践

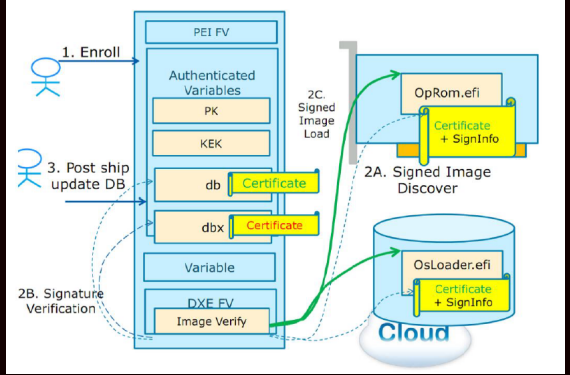
APT28 攻击仿真



腾讯探索实践

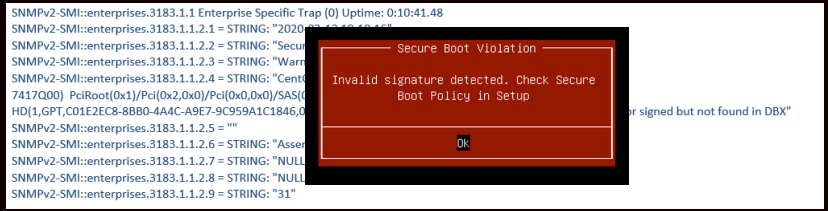
UEFI原生能力 Secure Boot

- 支持证书/HASH黑白名单
- 验证板卡驱动与BootLoader
- 通过OEM侧注入腾讯自主证书链
- 定制告警能力



腾讯探索实践

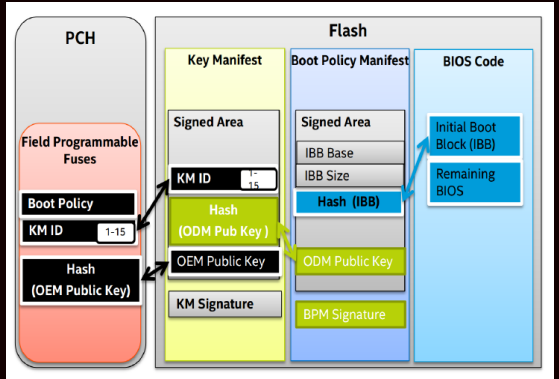
Secure Boot 改造效果



腾讯探索实践

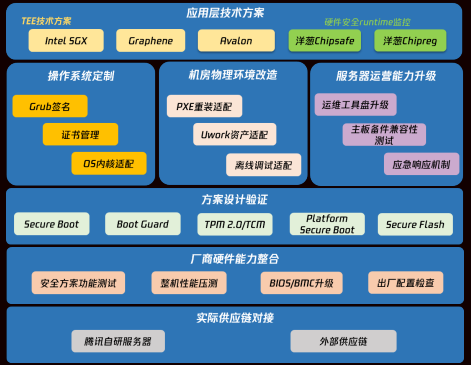
UEFI启动前验证-BootGuard

- 基于证书 + 验证签名合法性
- 验证范围是UEFI镜像中的SEC卷与PEI卷
- DXE卷由供应商自由发挥
- 黑屏阻断，需定制告警能力



腾讯探索实践

落地部署


应用层技术方案
TEE技术方案
Intel SGX
Graphene
Avalon
硬件安全runtime监控
洋葱Chipsafe
洋葱Chipreg
操作系统定制
Grub签名
证书管理
OS内核适配
机房物理环境改造
PXE重装适配
Uwork资产适配
离线调试适配
服务器运营能力升级
运维工具盘升级
主板备件兼容性测试
应急响应机制
方案设计验证
Secure Boot
Boot Guard
TPM 2.0/TCM
Platform Secure Boot
Secure Flash
厂商硬件能力整合
安全方案功能测试
整机性能压测
BIOS/BMC升级
出厂配置检查
实际供应链对接
腾讯自研服务器
外部供应链

腾讯探索实践

遇到的坑

- 上游供应商成熟度
- 软硬结合兼容性
- 主板BIOS BUG
- 内核内存调度 BUG
- 供应链-维保体系改造

感谢观看！

KCon 汇聚黑客的智慧

知道创宇 | KCon