安卓安全机制

2020/04/22
最初版
v1.0

- 系统
  - 应用
    - framework应用沙箱
      - 强制应用隔离
      - 数据目录加密：/data/data/等
    - 签名 – V1/V2/V3
    - 进程隔离扩展
      - gid uid 扩展给app进程（userid（app_xxx），groupid）
      - 系统权限规则存放在/system/etc/permission/
      - app使用Androidmanifest. xml 注册申请额外的系统权限
  - 只读系统分区和安全模式
  - 文件系统权限
    - 用户/组/rwx
  - 启动时验证(AVB)
    - 设备状态 – lock/unlock
    - 信任根
      - 硬件可信根
      - 用户配置可信根 – 公钥
        - 设置 – avbtool/fastboot
        - 擦除 – fastboot
    - 可信链传递
      - 启动加载验证：fastboot - 内核 - 设备树 - system分区 - vendor分区 - system_other分区（A/B设备）等
    - 回滚保护
      - 基于防篡改的存储空间记录版本
  - 加密
    - 标准和常用
      - AES
      - RSA
      - DSA
      - SHA
      - 国密 – 国内使用较多
    - 协议
      - SSL
        - HTTPS等
    - KeyChain 类–存储私钥和证书链
    - 用户安全功能
      - 全文件系统加密
      - 全盘加密
      - 文件级加密
    - 密钥库
  - 获取设备的 Root 权限
  - 设备管理
    - Android Device Administration API
  - Trustly TEE
    - 硬件/软件隔离–与主系统并行的系统
    - 敏感数据传到这里处理，把计算的结果返回出去
    - 实例
      - 数字版权管理框架
      - 移动支付、安全银行、多重身份验证、设备重置保护、抗重放攻击的持久存储、安全 PIN 和指纹处理，甚至还能用于恶意软件检测
- 内核
  - Linux 安全
    - namespace/cgroup
      - 基于用户的权限模式（DAC）
      - 进程隔离
      - 伪文件系统
    - seccomp
    - ASLR
    - 用于实现安全 IPC 的可扩展机制
    - 能够移除内核中不必要的和可能不安全的部分
    - audit 审计
    - syslog 日志
    - 其他
      - 内存地址隔离
      - 内核结构体地址随机化
      - CFI – 基于LLVM
      - 模块版本校验
      - 内核签名
      - kallsyms符号隐藏等等
  - 安全增强型 Linux（MAC）– 属于内核LSM类
    - 涉及node节点等
      内核功能调用机制，用户态实现策略
    - 可信计算 – we work here
      - 硬件芯片算法/软算法
        - 可信根
        - 可信链的传递
        - 加密
        - 完整性校验
          - 运行控制
      - 防篡改
      - 三权分立
        - 安全用户/普通用户/审计用户
      - 云
        - 授权
        - 签名验签
          - 软件安装控制
        - 远程证明
      - 动态度量
        - 进程/系统调用/内核/模块/网络/文件系统
      - 设备管控
      - xxx
    - Selinux – 默认只开这一个，LSM类安全机制可以叠加
      - 基于角色 – 其中，app可以通过不同的【签名/安装方式】获取不同的uid selinux policy规范
      - 类型增强 – 加强强制访问控制
      - 多级安全 – 削减多级安全机制(只保留了sl,cxx)
      - 另外，不同权限apk的数据文件不能相互访问，但是同权限的app的数据可以相互访问
    - smack–阉割版selinux，适合嵌入式系统
    - 涉及路径类
      - tomoyo – 类型增强
      - apparmor – 应用装甲
      - yama – 主要关注ptrace
    - keys – 密钥管理
    - loadpin – 基于dm-verify
      - 思路是只加载第一个文件系统
    - integrity – TCG开放标准的一部分
      - IMA
      - EVM
        - 主要针对离线攻击，比如拆除修改硬盘
- 安全实践方向
  - 组织和运营安全性
    - 组建安全与隐私权团队
    - 创建验证流程
    - 源代码更改跟踪
    - 验证源代码完整性和起源
    - 事件响应
  - 系统安全性
    - 生物识别身份验证
    - 锁了程序
    - 开发工具
      - 应用内嵌套
      - 征求用户同意
    - 安全更新
      - OTA
      - 软件包在线更新
      - 安全补丁 – 官方公告（google/huawei/lg/moto/NOKIA/samsung/xxx）
    - 密钥管理
    - 系统镜像签名
    - 可解锁的引导加载程序
    - 运行控制/防篡改
      - 内核态LSM
        - SELinux
        - 可信计算
      - 用户态
        - hook技术
      - 路径检测
    - 设备测试
      - LLVM
        - 编译插桩
          - 执行流完整性 CFI
          - 应用内存检查 AddressSanitizer(ASan)
          - 内核地址排错 (KASAN)
        - 编译检查
      - 内存错处检查 AddressSanitizer (HWASan)
        - 适用于Android 10+ && aarch64
      - 整形溢出 IntSan
      - 数组边界检查 BoundsSanitizer
      - 模糊测试 libFuzzer
      - 内存
        - 内核运行时内存 KASAN+KCOV
        - 只读内存
        - 堆内存检测 Scudo
      - CDD/CTS兼容性测试
  - 应用安全性
    - 源代码审核
    - 漏洞扫描
    - 权限/签名
    - 沙箱
    - 自动测试
  - 网络安全性
    - 停用 ADB
    - 保护监听套接字
  - 硬件安全性
    - 设备内存
    - StrongBox Keymaster
    - 设备管控
  - 隐私
    - 记录数据
    - 数据收集
    - 间谍软件

XMind：ZEN | 试用模式