[toc]

芯片操作系统与嵌入式软件安全

- 软件定义硬件

  > 软件开发者通常不在意底层的硬件实现，一般只调用硬件提供的上层api

嵌入式系统的生命周期

1. 嵌入式系统的定义

   > 来自用户的需求

2. IC开发
3. IC制造和测试
4. IC封装和测试
5. 产品化流程

   > 集成测试

6. 嵌入式软件系统个人化

   > 和应用直接相关

7. 嵌入式软件系统最终应用

安全的嵌入式软件

- 评价标准
  - Common Criteria

操作系统安全

- TCSEC
- 传统操作系统的安全关注点

  > 账户管理和访问控制
  >
  > 网络安全
  >
  > 病毒和防火墙
  >
  > 漏洞扫描与升级
  >
  > 流量监控

- 嵌入式操作系统的安全关注点

  > 安全审计

> 数据空间暴力破解
>
> 密钥功能
>
> 数据传输保护
>
> 数据访问控制
>
> 环境压力
>
> 文件结构控制
>
> 启动序列
>
> - 启动是最脆弱的过程
>
> ……

- 与传统操作系统应用场景不同

  > 需要考虑物理防护、侧信道攻击、IP隔离

COS的基本概念

- 不包括硬件可分为4层，由下到上为

> HAL：硬件抽象层
>
> Kernel：核心层
>
> - 消息处理和事件处理
> - 存储器管理
>   - 存储器类型
>   - 暂态存储器
>   - 持久化存储器
>   - 分配方式
>   - 静态分配
>   - 动态分配
>
>   > 内存分配和垃圾回收
> - 资源调度和互斥
>
> installer + GP环境
>
> - 对应用进行检查和二次编译
>
> API

- 系统

    - 文件系统
    - 安全系统
    - 命令系统
    - 接口系统

- 认证
    - 认证方法

      > 密码
      >
      > 口令
      >
      > 生物识别
      >
      > 多因子认证

    - 认证协议

      > SCP
      >
      > 7816

    - 认证存储安全

      > PUF
      >
      > MCB
      >
      > Memory

GlobalPlatform

guide

- 当设计协议时先学习**标准**
    - 弄懂之后再尝试自己设计
- 做安全不能只学安全本身
    - 必须要有计算机基础