[toc]

安全威胁类型

物理威胁

- 偷窃、间谍、废物搜寻等

线缆连接

- 拨号进入、冒名顶替、窃听等

身份鉴别

- 算法考虑不周、随意**口令**、口令破解、口令圈套等
- **口令(password) $\ne$ 密码(cipher)**
- 身份认证方式
  - 口令、生物特征、证书、PUF等

编程

- 病毒、代码炸弹、特洛伊木马、更新或下载等

系统漏洞

- 不安全服务、配置、初始化、乘虚而入等
- 最小权限原则

安全的目标

- 基本目标
  - 安全保护能力
    > 采取积极的防御措施
  - 隐患发现能力
    > 及时、准确发现并消除安全隐患
  - 应急反应能力
    > 遭受到攻击时，以最小的代价、最短的时间恢复系统，使信息资产得到保护
  - 信息对抗能力
    > 不仅是科技水平，更是综合国力的体现。信息对抗将在一定程度上决定战争的胜负

安全体系

- 物理安全

    - 环境安全
    - 媒体安全
    - 设备安全

- 网络安全
    - 反病毒
    - 备份恢复
    - 审计监控
    - **访问控制**
        - 控制表技术

        > 出入控制
        >
        > 存取控制

    - **安全检测**
        - 攻击技术

        > 安全扫描
        >
        > 入侵检测
        >
        > - 异常检测
        > - 误用检测

- 信息安全
    - **用户鉴权**
        - 口令技术

        > 主体特征
        >
        > 口令机制

        - 加密技术安全协议

        > 口令特征
        >
        > 智能卡
        >
        > 数字证书

    - **传输安全**
        - 加密技术安全协议

        > 口令机制
        >
        > 智能卡

> 数字证书
>
> 传输数据加密
>
> 数据完整鉴别

- 存储安全
- 内容审计

> 图像识别、语义识别

安全体系结构

- P2DR