- Security
  - Authentication & Password
    - Threat Model
    - Guard Model
      - 存在的问题
        - 软件bug导致有些数据可以绕开complete mediation
        - 有些内存可以绕开OS防御
        - User会犯错
        - 安全等级
      - 解决方案
        - 微内核，代码越少，潜在bug越少
        - 永远不要使用root权限登录
        - 使用一个很长的正则表达式将危险的单双引号过滤，预防SQL注入
      - Authentic&Authorize
        - 攻击
          - timing attack
            - 加盐 hash(pwd|salt)
            - 避免一直输密码：使用cookie&Session
          - 钓鱼攻击(Phishing)
            - Challenge-Response Scheme
            - 使用密码验证服务器的安全性
            - 把离线攻击转变为在线攻击，让攻击留下痕迹
            - 每个网站使用不同的密码
            - 一次性密码
            - 每个请求都加上authority信息
            - FIDO 物理层面/Trust Zone
  - 安全数据流
    - 攻击者偷走我们数据的方式
      - KeyLogger/TouchLogger
      - MemScan
      - Screen Capture
      - Cold-boot
      - Side-Channel(利用陀螺仪)
    - Strategy
      - Taint Checking
      - SDO
      - TinMan
    - Secure Channel
      - 普通加密 — reply attacks & reflection attacks — 使用seq和不同的key解决
      - 交换密钥 — DH密钥交换算法 — 无法抵御中间人攻击
      - RSA 非对称加密算法
      - TPM
  - ROP
    - ASLR
    - Canary
    - CFI
  - Data private
    - ZKP
    - PIR
    - OT
    - DP
    - Secret Sharing
    - Secure MPC
    - 同态加密
      - SWHE
      - FHE
    - Hardware Enclave