信安必考点

信息三要素

- Confidentially：私密性：保持数据和资源被隐藏
- Integrity：完整性：数据或资源的可信度：数据可以被非法更改吗？->数据或资源的可信度
- Availability：可用性：使访问数据和资源成为可能

策略与机制

- 策略定义什么可以做，什么不可以做。它定义了安全
- 机制执行策略，强化安全（技术层面？程序层面？）
    - secure，precise，partial

安全保障

- Assurance：测量多大程度上可以信任系统会做其应做的事情。
- 规范（specification）
    - 系统的目的被规范定义
    - 对预期功能的声明，并非对规范本身
- 设计（design）
    - 系统如何满足规范
- 实现（impomentation）
    - 创建符合该设计的系统

常见攻击类型

- passive attack：监听
- Active attack：修改，延迟，重放，拒绝

凯撒密码（右移三位）

维吉尼亚方阵

- 单秘钥
- 双秘钥
- 破译：通过检测多个（组）重复元素寻找可能长度（约数），然后通过设长度，频率分析解答（每一个都是凯撒偏移量密码）

攻击类型

- cipertxt only
- known plaintext
    - some plain--ciper pair
- chosen plaintxt
    - attackers can generate ciphertext for any plaintext he selected

ECB对称加密

- 针对ecb的问题
  - ciper-only attack 利用现有密文
  - build a codebook of <Ck, guessed Pk> pairs (chosen plaintext attacks). Replay Attacks?
  - codebook的解决方案： identical input plaintext Pi = Pk won't result in same output code due to memory-based chaining. IV = Initialization Vector use only once

RSA

- 安全原因？
  - 破解策略：偷到私钥
  - 知道原理后暴搜（时间长）
  - 通过原理计算d problem: Given two numbers (r,s), the algorithm outputsa number x such that r * x = 1 (mod s).
  - 时间开销主要在n = p * q 分解上，但是乘起来容易分解难！
  - longer than 155 decimal digits 更安全
  - 更为好的方法：伪造一个自己的钥匙对，发消息欺骗alice换公钥了！
    - 使用数字签名防止

好的单向哈希算法

- 哈希无论多长出来都一样长（同一个算法的话）
- 易于分析（计算）（amy document很快出结果）
- 难以逆运算（单向）
- 难以发现冲突（两个不同的数据几乎不可能有相同哈希值）
- 抽屉原理（N>哈希码可表示数量）
  - 可能存在冲突但很难追溯原文

数字签名

- 不可伪造；（unforgeble）
- 签字人不可否认
- 可被广泛验证
- doc之间不同
- 易于实现
- 用私钥加密，用公钥解密
  - 很长文本签名先用哈希再给哈希签名

基于生物识别的

- 优点
  - 不会泄露丢失遗忘
- 缺点
  - 花销较大，安装困难，保持问题
  - 对算法的要求较高
    - fraud rate欺诈率 insult rate 侮辱率
    - 反比关系

    - 隐私问题
    - 被伪造后影响不可逆
    - 可以通过重放攻击攻破

用户，主体，对象

- ub和用户
    - 注意 user 可能对应多个principal
    - user有很多principal，但一个prin只有一个user 确保了责任制（accountability）
    - 一个主体是一个代表着某一特定principal的程序/应用
    - 一个principal可以是闲置的，也可以被多个主体代表
- principal和subject
    - 一般情况下（不总是！）每个主体只有一个principal
    - 一个prin的所有主体有相同的权限
- 对象（Object）
    - 种类
        - 文件，路径（文件夹），内存片区
    - sub也可以成为ob！kill subject（之类的）时候
- ACL vs.capability
    - 如何实现？
    - ACL（访问控制列表）
    - 存储矩阵的列（user123……） 和资源一起，文件拥有用户
    - capa
        - 用户为每个资源持有不可伪造的票证
        - capa提供对subject的更细粒度的最小权限控制，尤其是针对特定任务创建动态的的即时subject
    - 常用ACL

RWX（基于ACL）

DAC MAC

- 前者允许访问权限在sub之间传递；主体对某一访问权限的拥有足以允许（其授权其他sub）访问该对象了。 换句话说，我有了这个权限，我就能给别人 后者将主体对对象的访问限制在安全标签的规定之内。有严格的等级

BLP model

- 向下读，向上写
- 包含类别

隐通道

- 资源耗尽通道
- 负载敏感通道
- 解决：关闭通道或减慢速度

病毒

```
beginvirus:
    if spread-condition then begin
        for some set of target files do begin
            if target is not infected then begin
                determine where to place virus instructions
                copy instructions from beginvirus to endvirus into target
                alter target to execute added instructions
            end;
        end;
    end;
 perform some action(s)
 goto beginning of infected program
 endvirus:
```

木马

- 可复制木马

蠕虫

- 选择攻击目标
- 放钩子
- 拉入蠕虫代码
- 获取编译器命令
- 生成感染者列表
- 开始主动感染

缓冲区溢出攻击（argu溢出影响ret）

跨栈脚本攻击

僵尸网络实现

- 感染过程
    - 插入shellcode
    - sehllcode下载安装actuall bot
    - bot关闭防火墙和杀毒软件
    - 定位IRC Server， 连接加入通道
    - 重设认证模式防止被其他机器再度利用；
- 繁殖
    - 每个肉鸡）扫描新受害者的ip，这一过程是自动的
    - 主动botnet管理
        - Detect non-responding bots, identify “superbots”
    - Evidence of botnet-on-botnet warfare
- DDoS时的树形结构

防火墙区别

- 无状态包筛选器
- 有状态防火墙
    - flows
- 应用级防火墙
- 区别