Chapter 7: 安全策略

- Reading
  - Introduction to Computer Security chapter4-chapter7

主要内容

- **7.1 策略**
- 7.2 信任
- 7.3 安全机制的属性
- 7.4 策略示例

7.1 安全策略略

- 什么是安全策略略?
  - 安全策略略定义了系统的“secure ”
  - 安全策略略可以是非形式化的、也可以是数学描述
  - 精确定义安全策略略后, 我们“信任”安全策略略, 在安全策略略基础上讨论几类策略略模型

7.1 安全策略

- 把计算机系统想象成有限状态的自动机 **(finite-state automation)**

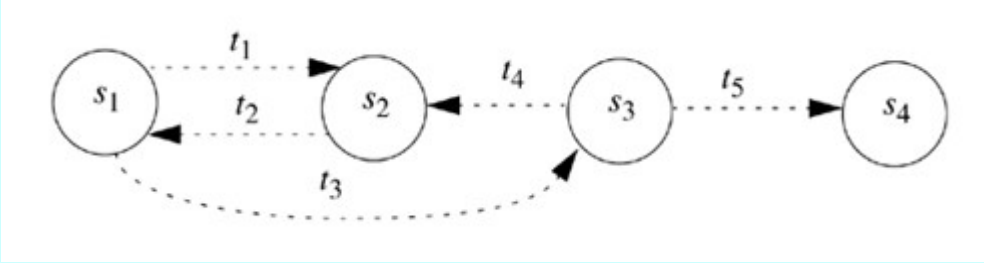
- 一系列转换函数:改变状态

7.1 安全策略

- 策略将系统状态划分为:
  - 被授权状态 (安全)
    - 系统可进入的状态
  - 未授权状态 (不安全)
    - 系统进入这些状态, 违背了安全性

- 安全的系统
  - 初始于授权状态
  - 永不进入未授权状态

7.1 安全策略



- 授权状态 A = { s_1, s_2 } ， 未授权状态 UA = { s_3, s_4 }.

- 系统安全么？
  - 不安全

  - 系统初始于授权状态,可以进入未授权状态

7.1 机密性

- X 实体集　　I 信息
- I 具有机密性属性：如果无 $x \in X$ 可以从 I *获得信息*
- Example:
  - X 学生集合　　I 期末考试答案
  - I 对 X 来说有机密性：如果学生不能得到期末考试答案

7.1 机密性

- 机密性：防止信息泄露给未授权用户，识别泄露信息的状态
- 包括权限的泄露、信息的非法转移
- 例：一个公司的承包人，当合约到期，承包人不能再访问信息

7.1 完整性

- X 实体集, I 信息
- I 相对 X 来说有完整性，当所有的 $x \in X$，信任 I *中的信息*

- 信任的类型:
  - 信任 I, 包括传递和保护 (数据完整性)
  - I 的起源和身份(初始完整性, 鉴别)
  - 信任其能按预定的功能工作 (保障)

7.1 完整性

- 完整性策略定义授权方式
  - 信息如何被修改，实体如何被授权可修改
- 所授权限由多个关系进行定义,外部关联关系对权限进行限制
- 例:
  - 在多个交易中, 责任分离原则禁止一个实体单独完成一个交易

7.1 可用性

- X 实体集　　I 资源
  - I 相对 X 来说有可用性：当所有的 $x \in X$ 可以访问 I

- 可用性类型:
  - 传统: x 可访问或不可访问
  - 服务质量: 访问效率 (如, 带宽)，能访问不意味着达到预定的质量
  - 例: 书店，买1本书要花1小时

    医师申请麻药请求，花了1小时

7.1 可用性

- Availability 描述提供什么样的服务
- 可访问的服务的参数
- Example:
  - 浏览器可以下载 web pages，而不是java applets.
  - 服务器在请求后1分钟内提供鉴别数据

主要内容

- 7.1 策略
- **7.2** 信任
- 7.3 安全机制的属性
- 7.4 策略示例

7.2 策略模型

- 策略或策略集：是抽象描述
- 策略中的重点关注点
  - 多级安全模型中的安全级
  - 责任分离
  - 中国墙模型的利益冲突问题

7.2 安全策略的类型

- 1、军队 (政府)的安全策略
  - 策略主要保护什么？

    机密性

  - 军队的需求：保护信息
    - 军舰的出海时间：秘密. 机密性遭泄露后会引发灾难
    - 隐私法Privacy Act.
    - 限制信息被个人获取，非授权的泄漏会判刑、罚金

7.2 安全策略的类型

- 2、 商业的安全性
  - 策略保护什么？

    完整性
  - 商业公司要防止数据被篡改
  - 如果银行的计算机被攻击，账户的存款状况被泄漏，破坏了机密性
  - 账户余额被篡改，破坏财务收支平衡

7.2 安全策略的类型

- 机密性策略
  - 策略仅保护机密性
- 完整性策略
  - 策略仅保护完整性

7.2 完整性和事务

- 初始于完整性状态
  - 完整性“Consistent”是比较抽象的
- 执行一系列动作 (*事务*)
  - 动作可以被中断
  - 完成一个动作，系统处于一致性状态
  - 动作未完成, 系统回退到初始的一致性状态

主要内容

- 7.1 策略
- 7.2 信任
- **7.3 安全机制的属性**
- 7.4 策略示例

7.3 信任的作用

- 不同策略，信任的含义不同
  - 机密性策略不信任客体, 说明客体是否被泄漏, 并未说明客体是否应被信任
  - 完整性策略, 说明客体被信任的程度
    - 给定信任级别, 策略说明主体可对客体做什么
    - 如何指定信任级别？
    - 例: 一个网站得到一个新版本的程序, 高完整性级别(信任新版本), 低级别(经过完全测试)

7.3 信任的作用

- 信任含义：对理解计算机安全是非常关键的
- 机制：实施安全策略的某些部分的实体或规程
- 策略和机制是建立在特定的前提下
- 安全策略、安全机制、安全过程，都建立在一定的前提基础上，可更好地理解这些策略的效果

7.3 信任的作用

例: 管理员安装补丁

信任:

--补丁来自软件供应商, 在传输过程未被篡改

--供应商对补丁做了充分的测试

--供应商的测试关键和你的环境一样

--补丁被正确安装

7.3 形式化验证信任

- 形式化的数学证明：输入 i, 程序 P 产生预定义的输出 o
- 假定一个安全相关的程序 S 形式化证明了可在操作系统下工作
- 我们假定了哪些前提?

7.3 信任的形式化方法

信任：

1. 证明没有错误
2. 预设条件和*S*使用的条件一致
3. *S* 转移到可执行态*S′*，*S′*的行为用代码完成
   - 编译器有 bugs, linker/loader/library 有问题
1. 硬件按预想的执行 *S′*
   - 硬件 bugs (Pentium f00f bug, for example)

安全策略示例

- 学生提交作业：策略要求不允许欺骗
  - 他人授权或非授权情况下，不允许拷贝作业
  - CS 专业学生可以在计算机上做作业
  - Anne 忘记对作业文件添加写保护
  - Bill 拷贝了作业
- 谁违背策略?

  Anne, Bill, or both?

Answer Part 2

- 如果策略要求：学生必须给作业文件加上读保护
  - Anne违背安全策略？

  - 违背

安全机制

- 实施安全策略的部分实体或过程
  - 访问控制 (如，防止作业被读)
  - 不允许人们拿CD或磁盘进入计算机系统，防止对计算机进行攻击

主要内容

- 7.1 策略
- 7.2 信任
- 7.3 安全机制的属性
- **7.4 策略示例**

7.4 示例：学校的安全策略

- 大学的计算机安全策略
  - 大学有多个园区, 有校级管理员
  - 每个校园有自己的管理员, 有自己的特殊需求

- 包括
  - 通用大学策略
  - 电子邮件策略

通用大学策略

- 可接受使用策略
  - 可在园区内使用
  - 重点强调
- 加强机制
  - 警告
  - 拒绝访问计算机
  - 行政措施：开除
- 非形式化的文档，使得用户可用

电子邮件策略

- 系统级, 非一个园区

- 三部分
  - 电子邮件策略总则
  - 完全策略
  - 各园区的解释

电子邮件策略总则

- 警告：电子邮件不是专用的
  - 在正常系统管理情况下，可能被阅读
  - 可能被伪造、篡改、发出
- 告诉用户：该做什么，不该做什么
- 警告用户会面临威胁
  - 通常,策略说明禁止哪些问题,但不具体定义威胁

完全策略

- 对策略进行详细描述，定义更清晰
- 用户可以做什么，不可以做什么
  - 发送前自己考虑清楚
  - 礼貌、尊重他人
  - 不要干扰他人使用邮件
- 个人可以使用, 但不要对系统造成太大影响
- 施行对象
  - UC校园是准政府部门, 应有自己的特殊策略
  - 系统维护、升级会影响应用

完全策略

- 特殊说明
  - 不适用于Dept. of Energy的实验室
  - 不适用于打印的邮件
  - E-mail, 大学的基础设施
    - 学术自由,言论自由
    - 研究垃圾邮件等学术性活动：用户未授权使用，得到副校长的许可依旧可以使用用户数据

电子邮件的使用

- 允许匿名使用
  - 例外: 违背法律和其它政策
- 不能干扰他人使用电子邮件
  - No spam, letter bombs, e-mailed worms, *etc*.
- 个人使用e-mail有一定的限制条件
  - 不能干扰学校的事务
  - 不能泄露信息

E-mail的安全

- 学校能够阅读e-mail
  - 不能超出其权限范围
  - 在合法的前提下可以阅读
  - 保证e-mail系统健壮性, 可靠性
- 允许归档、备份

重点

- 策略：描述了允许什么
- 机制：控制实施策略
- Trust是基础