第十四章 控制和监控访问

14.1 对比访问控制模型

- 授权主体访问客体根据不同IT系统的访问控制方法不同而不同
- 明确提到的四种方法：自主访问控制（DAC），强制访问控制（MAC），基于角色的访问控制（role-BAC），基于规则的访问控制（rule-BAC）

14.1.1 对比许可、权限和特权

- 许可：许可是指授予对象的访问权以及对具体的访问权内容的确定
- 权限：指一个对象采取行动的能力
- 特权：特权是许可和权限的结合

14.1.2 理解授权机制

- 隐私拒绝：访问控制的基本原则是隐私拒绝，并且为大多数授权机制所使用
- 访问控制矩阵：一个包含主体、客体和分配权限的表格，当主体想要执行某个动作时，系统检查访问控制矩阵来确定主体是否有适当的权限执行该动作
- 功能表：分配给主体特权的另一种方式，关注主体（如用户、用户组）(DAC自主访问控制)
- 限制接口：根据用户的特权限制用户可以做什么可以看什么
- 内容有关的控制：基于客体中的内容来限制对数据的访问，数据库视图使一个基于内容的控制
- 上下文相关的控制： 需要在授予用户访问权之前进行特定的活动
- 知其所需：确定主体只在他们的工作任务和工作职能有要求时被授予访问权
- 最小特权：确保主体只能被授予他们执行工作任务和工作职能所需的特权
- 职责分离：确保敏感功能被分成由两个或两个以上员工执行

14.1.3 用安全策略定义需求

- 安全策略：一个定义组织安全需求的问题，它识别需要保护的资产，以及安全解决方案应该保护他们的程度

14.1.4 部署纵深防御

- 组织使用深度防护 策略实现访问控制，使得多层访问控制提供多层安全
- 深度防御的概念重点：

    - 组织的安全策略，这是惯例访问控制之一，通过定义安全需求为资产提供了一层防御
    - 人员是防御的重要组成部分
    - 行政管理性、技术性和物理性访问控制的结合提供更为强大的防御

14.1.5 自主访问控制

- 自主访问控制：系统允许客体的所有者、创建者或数据保管者控制和定义主体对客体的访问
- 基于身份的访问控制是DAC的一个子集
- 常常针对客体的访问控制列表来实现DAC模型

14.1.5 非自主访问控制

- 可自由支配和不可任意支配的访问控制之间的主要区别在于他们如何对他们进行控制和管理
- 非DAC访问不关注用户的身份，集中控制易于管理，主要为基于规则的、基于角色和基于格子的访问控制
- 基于角色的访问控制：采用基于角色或基于任务的访问控制系统基于主体的角色或分配任务定义主体访问对象的能力，基于角色的访问控制经常使用组来管理，类似银行机构，基于角色的访问控制在有频繁认识变动的动态环境是有用的
    - DAC和role-BAC的区别：DAC中，所有者确定谁有权利访问；role-BAC中，管理员确定主体特权，并将特权分配给角色和组
    - TBAC与role-BAC相似：区别为TBAC通过分配任务而不是通过用户身份来控制访问
- 基于规则的访问控制：使用一套规则、限制或过滤器来确定能以及不能出现在系统上的东西，它的独特特征是适用于所有主体的全局规则，常见例子防火墙
- 基于属性的访问控制：用使用多个属性的规则策略，许多软件定义的网络应用使用ABAC模型
- 强制访问控制模型：**依赖标签（通过分级和分类识别）**，每个分类标签代表一个安全域或安全领域，安全域是共享安全策略的主客体集合，客体由标签来表明他们的分类水平和敏感度，通常被称为**基于格子的模型（基于格子访问控制模型，包含一对元素即主体与客体，主体具有上限或高于上限的被访问对象）**
- MAC模型中的分类使用一下三种类型的环境之一
    - 分层环境：将有序结构中的各个分类标签与低安全等级、中安全等级、高安全等级相互联系
    - 隔离区环境：一个安全域和另一个安全域之间没有关系

- 混合环境： 结合分层和隔离区间的概念，包含更多细分等级，与安全域的剩余部分相隔离

14.2 理解访问控制攻击方式

- 访问控制的目标就是组织针对客体的未授权访问，包括访问任何系统信息，IT安全方法试图防止机密性破坏、完整性破坏和可用性破坏

14.2.1 风险元素

- 风险指的是某种潜在的威胁利用某种漏洞造成某种损失的可能性
- 威胁指的是某个时间发生的趋势，可能会产生某种不良后果
- 漏洞指的是任何类型的脆弱性

风险管理，即通过执行控制和应对措施视图减少或消除漏洞或减少潜在威胁的影响

1. 识别资产
   - 资产评估值得是确定各种资产的实际价值并对他们进行目标优选
   - 风险管理就是将重点放在价值高的资产上，并执行控制来减少风险对这些资产的影响
2. 识别威胁
   - 识别资产并确定优先级后，组织试图是被对有价值系统的任何可能威胁
   - 试图减少漏洞，以及减少任何易燃存在的漏洞的影响，总体是减少风险
3. 威胁建模方法
   - 专注资产： 使用资产估值结果，并试图是被对有价值资产的威胁
   - 专注攻击者： 是被潜在的攻击者，并基于攻击者的目标是被他们代表的威胁
   - 专注软件： 组织开发软件，考虑针对软件的潜在威胁
4. 高级持续性威胁
   - APT 一群熟练者持续高强度的攻击
5. 识别脆弱性
   - 试图发现这些系统在潜在威胁前面的弱点
   - 脆弱性分析是一个持续的过程，包括技术和管理措施
   - 风险分析通常包括脆弱性分析，评价系统和环境的已知威胁和漏洞，然后利用漏洞的渗透测试

14.2.2 常见的访问控制攻击

- 访问控制攻击试图绕过访问控制方法
  - 访问聚合攻击：收集多个非敏感信息，然后将他们结合起来获得敏感信息，侦查攻击就是访问聚合攻击

    - 密码攻击：密码是最弱的形式认证，攻击者成功发动密码攻击，就可以访问账户和授权给账户的所有资源了
    - 字典攻击：通过预定义数据库或常见预定义密码列表中所有可能的密码来发现密码
    - 暴力攻击：试图通过系统尝试所有可能的字母、数字和符号组合来发现用户账户的密码
    - 生日攻击：关注寻找碰撞，可以通过带有足够位数的散列算法和盐来降低生日攻击的成功性
    - 彩虹表攻击：通过大型预先计算的散列数据库来减少时间，许多系统通过撒盐来减少彩虹表攻击的有效性
    - 嗅探攻击：通过网络发送的数据包，以便对数据包进行分析
    - 电子欺骗攻击：伪装成某物或某人
    - 邮件欺骗：伪装邮件地址，行程邮件来自其他来源的假象，如钓鱼攻击
    - 电话欺骗：更改电话号码
    - 社会工程学攻击：攻击者通过欺骗尝试获取他们信任的行为，诱骗人们透露敏感信息
    - 网络钓鱼：一种社交工程陷阱，诱骗用户，打开附件或链接
    - 鱼叉式钓鱼：一种针对特定用户组的钓鱼方式
    - 捕鲸：目标欧式高层人员或高管
    - 语音钓鱼：通过及时通信和网络电话欺骗用户
    - 智能卡攻击：旁路是一种被动的、非侵入性的攻击
    - 拒绝服务攻击： 最值系统记性处理或组织和发流量或资源请求的响应
- 防护方法汇总
    - 对系统的物理访问控制：“如果攻击者无限制地对计算机进行物理访问，攻击者就会拥有它”
    - 对文件的电子访问控制：严格控制和监控对密码文件的电子访问
    - 加密密码文件： 对可用操作系统的密码文件进行强加密有助于保护他们免受未经授权的访问
    - 创建强密码策略： 通过编程的密码策略可用强制使用强密码策略
    - 使用密码掩码：确保应用程序在任何屏幕上都没有以明文方式显示过密码
    - 配置多因素身份认证：比如使用生物识别技术或令牌设备
    - 使用账户锁定控制：有助于防止在线密码攻击
    - 使用最后一次登录通知：记录最后一次成功登陆的时间、日期和地点，用户可以注意到是否有其他人登陆自己账户
    - 对用户进行安全教育