信息安全导论

第六讲 访问控制

1 访问控制基本概念

2 常见访问控制模型

什么是访问控制

管理用户对资源的访问，是针对越权使用资源的防御措施。

记忆

教师登录学校个人门户

学生登录学校个人门户

相同的系统，不同的用户拥有不同的访问权限！

理解

访问控制的基本目标

防止对任何资源（如计算资源、通信资源或信息资源）进行未授权的访问。从而使计算机系统在合法范围内使用；决定用户能做什么，也决定代表一定用户的程序能做什么。

未授权的访问包括：未经授权的使用、泄露、修改、销毁信息以及颁发指令等

访问控制的三要素

主体、客体、访问控制策略

访问控制对机密性和完整性起直接作用，并对可用性产生影响。

理解

访问控制的相关概念

客体（Object）	规定需要保护的资源，又称作目标（target)
主体（Subject）	或称为发起者(Initiator)，是一个主动的实体，规定可以访问该资源的实体（用户或代表用户执行的程序）
授权（Authorization)	规定可对该资源执行的动作（例如读、写、执行或拒绝访问）。
访问控制策略（policy）	是主体对客体的相关访问规则集合，即属性集合。访问策略体现了一种授权行为，也是客体对主体某些操作行为的默认。

理解：

◆一个主体为了完成任务，可以创建另外的主体，这些子主体可以在网络上不同的计算机上运行，并由父主体控制它们。

◆主客体的关系是相对的

如何确定访问权限

用户分类（主体）、资源（客体）、访问规则（策略）

用户分类举例

（1）特殊的用户：系统管理员，具有最高级别的特权，可以访问任何资源，并具有任何类型的访问操作能力
（2）一般的用户：最大的一类用户，他们的访问操作受到一定限制，由系统管理员分配
（3）作审计的用户：负责整个安全系统范围内的安全控制与资源使用情况的审计
（4）作废的用户：被系统拒绝的用户。

认证：主体对客体的识别认证；客体对主体检验认证。
控制策略的实现：设定规则集合确保用户对资源合法使用，防止非法用户，防止敏感资源泄露。
审计：对客体资源管理者进行监督，防止权力滥用。

资源举例

- 磁盘与磁带卷标
- 远程终端
- 信息管理系统的事务处理及其应用
- 数据库中的数据
- 应用资源
- ……

访问规则

- 规定若干条件下，可准许访问的资源。
- 规则使用户与资源配对，指定该用户可在该资源上执行哪些操作，如只读、不许执行或不许访问。
- 由系统管理人员来应用这些规则，由硬件或软件的安全内核部分负责实施。

访问控制的基本过程

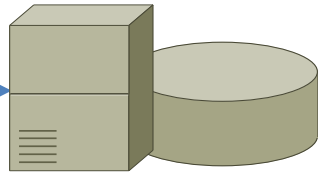
认证、鉴权、审计

授权（authorization）

授权信息

身份认证

访问控制

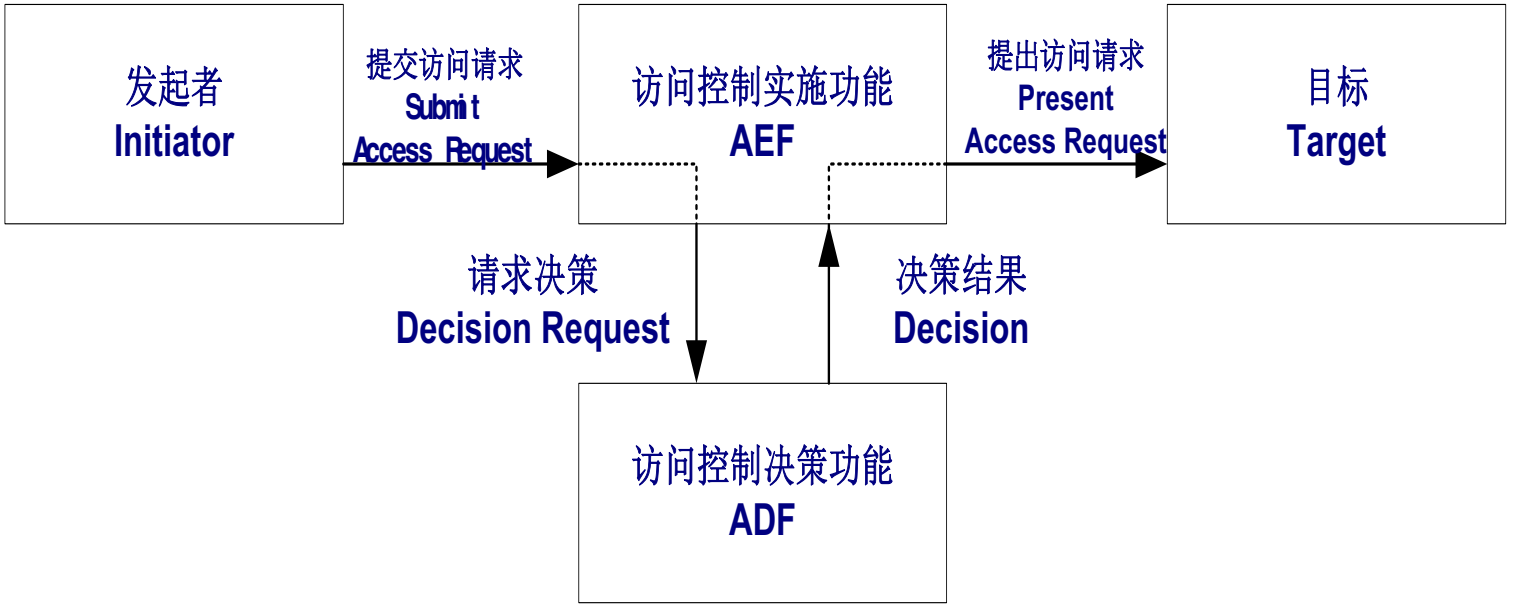


主体

客体

审计

Log



访问控制模型的组成

主要有八类：

1）入网访问控制
2）网络权限控制
3）目录级安全控制
4）属性安全控制
5）网络服务器安全控制
6）网络监测和锁定控制
7）网络端口和节点的安全控制　　8）防火墙控制

理解

一、自主访问控制

（Discretionary Access Control）根据访问者和它所属组的身份来控制对客体目标的授权访问。

- 自主访问控制规定客体的创建者为其所有者，可以完全控制该客体；客体所有者有权将该客体的访问权授予别人。
- 自主访问控制的特点是授权的实施主体自主负责赋予和回收其他主体对客体资源的访问权限。
- 自主是指具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体。

自主访问控制的特点

- 优点：灵活性高，被大量采用（尤其在商业和工业环境的应用上）。
  - 例如：用户可以自由传递权限，使得没有访问某个文件权限的用户U1可以从有该文件访问权限的用户Un那里得到访问权限或是直接拷贝该文件。
- 缺点：不易控制权限传递，容易被非法用户绕过而获得访问。
  - 例如：用户A可将其对目标O的访问权限传递给用户B，从而使不具备对O访问权限的B可访问O。

理解

自主访问控制的实现机制

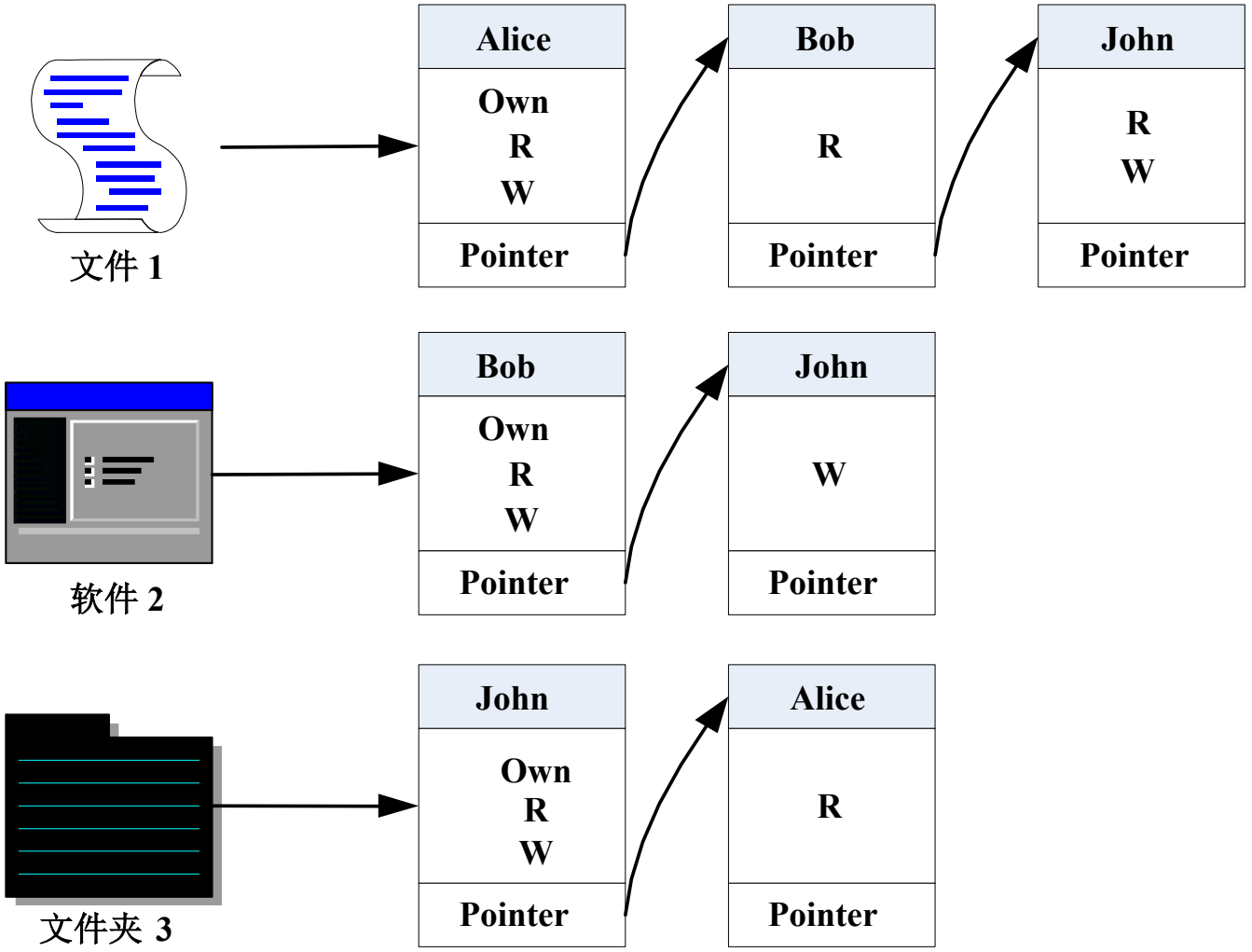
DAC一般采用以下三种机制来存放不同主体的访问控制权限，从而完成对主体访问权限的限制：

- **访问控制列表**
- **访问控制能力列表**
- **访问控制矩阵**

假定有三个用户：Alice，Bob，John，三个资源：文件1，软件2，文件夹3，Alice创建了文件1，并允许Bob读取，允许John读，写；Bob创建了软件2，并允许John写；John创建了文件夹3，并允许Alice读。

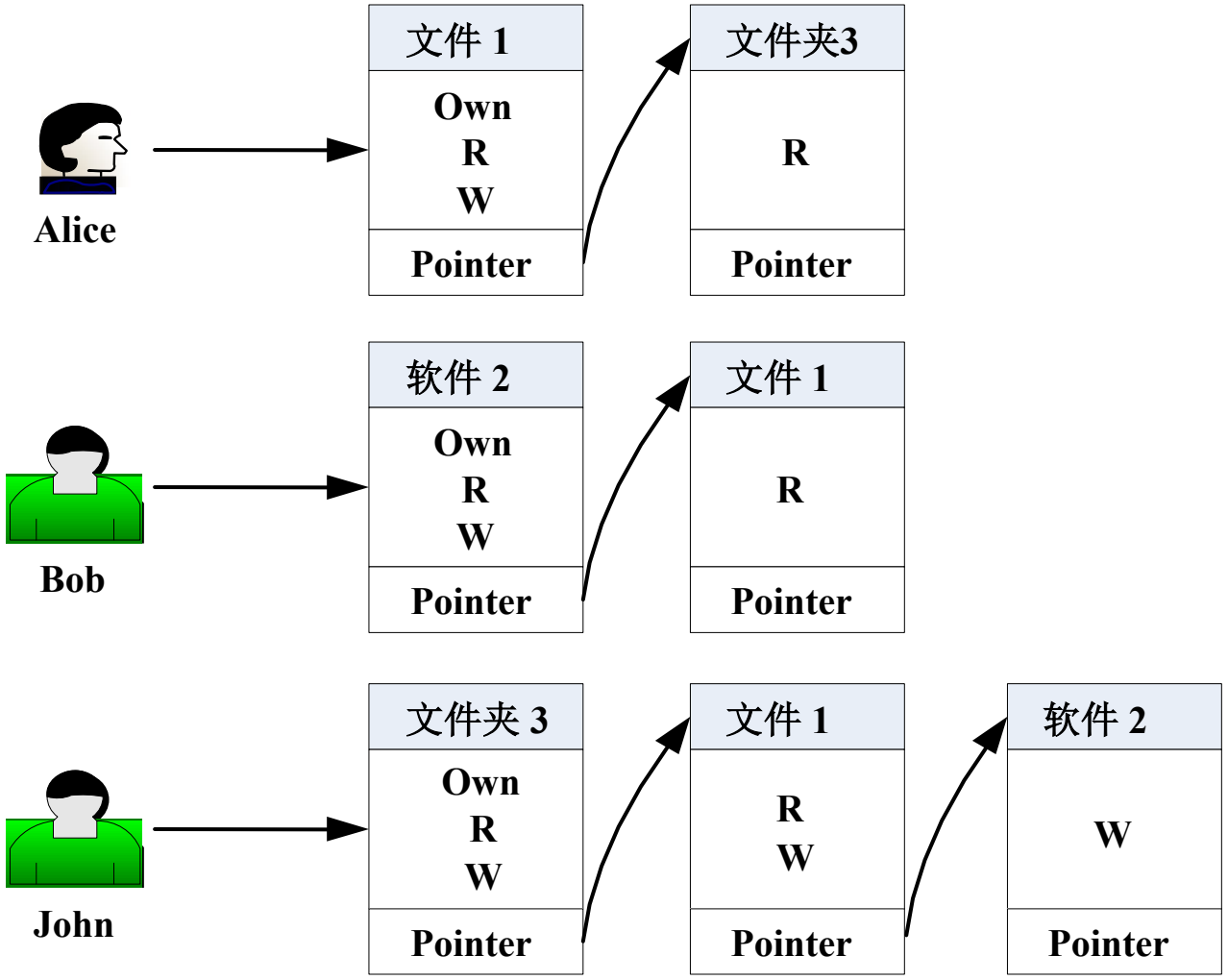
访问控制列表（ACL）

以资源（客体）为中心建立访问权限表



访问控制能力列表（ACCL）

以用户（主体）为中心建立访问权限表



访问控制矩阵（ACM）

是通过二维矩阵形式表示访问控制规则和授权用户权限的方法。重点掌握表8-4

主体 \ 客体	文件1	软件2	文件夹3
Alice	Own，R，W		R
Bob	R	Own，R，W	
John	R,W	W	Own，R，W

理解

ACL、ACCL、ACM对比

ACL

◆ 优点：权限回收容易；
◆ 缺点：权限传递困难，如访问控制列表太大或经常改变，那么维护访问控制列表就成为一个问题；
◆ 使用情况：系统需要区分的用户相对较少，并且这些用户大都比较稳定；

ACCL

◆ 优点：权限传递简单；
◆ 缺点：权限回收困难，用户生成一个新的客体并对其授权、或删除一个客体时都比较复杂。
◆ 使用情况：适用于分布式系统，用户量大且不稳定；

ACM

◆ 优点：清晰地实现认证与访问控制的相互分离；
◆ 缺点：在较大系统中，如果用户和资源都非常多，那么访问控制矩阵非常巨大；而且每个用户可能访问的资源有限，矩阵中许多格可能都为空，浪费存储空间；
◆ 使用情况：较少使用

理解

二、强制访问控制

（Mandatory Access Control）访问控制策略给出资源受到的限制和实体的安全级别，对资源的访问取决于实体的安全级别而非实体的身份。

- 强制访问控制（Mandatory Access Control）是比DAC更为严格的访问控制策略。
- 具体实现时，每个用户及实体都被赋予一定的安全级别，用户不能改变自身或任何客体的安全级别，只有系统管理员可以确定用户和组的访问权限。系统通过比较用户和访问的实体的安全级别来决定用户是否可以访问该文件。
- 安全级别一般有五级：绝密级（Top Secret，T）、秘密级（Secret，S）、机密级（Confidential，C）、限制级（Restricted，R）和无密级（Unclassified，U），其中T > S > C > R > U。

强制访问控制的实现机制

访问控制安全标签列表ACSSL

- 强制访问控制通常借助访问控制安全标签列表来实现。
- 安全标签是限制和附属在主体或客体上的一组安全属性信息。
- 访问控制标签列表是限定一个用户对一个客体目标访问的安全属性集合。

理解

访问控制安全标签列表实例

用户	安全级别
用户A	S
用户B	C
…	…
用户X	T

文件	安全级别
File 1	R
File 2	T
…	…
File n	S

- 左侧为用户对应的安全级别，右侧为文件系统对应的安全级别。
- 如果需要保护机密性，用户A的安全级别为S，那么他请求访问文件File 2 时，由于T > S，访问会被拒绝；当他访问File1 时，由于S > R，所以允许访问。

理解

三、基于角色的访问控制

Role-based Access Control将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。

- 与MAC和DAC将权限直接授予用户的方式不同，RBAC从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系；通过给用户分配合适的角色，让用户与访问权限相联系。
- 角色成为访问控制中访问主体和受控对象之间的一座桥梁。

基于角色的访问控制实例

- 假设Tch1，Tch2，Tch3，… Tchi是对应的教师，Stu1，Stu2，Stu3，… Stuj是相应的学生，Mng1， Mng2， Mng3，… Mngk是教务处管理人员。
- 角色定义：老师的权限为TchAC={查询成绩、上传所教课程的成绩}；学生的权限为StudAC={查询成绩、反映意见}；教务处管理人员的权限为MngAC={查询、修改成绩、打印成绩清单}。老师、学生及教务处管理人员分别对应一个角色。
- 授权：如果学校新进一名教师Tchx，那么系统管理员只需将Tchx添加到教师这一角色的成员中即可，而无须对访问控制列表做改动。
- 用户与角色的多对多关系：同一个用户可以是扮演多个角色，比如一个用户可以是老师，同时也可以作为进修的学生；同样，一个角色可以拥有多个用户成员，比如老师、学生以及教务处管理人员都可以有多个。

理解

基于角色的访问控制特点

- RBAC是实施面向企业的安全策略的一种有效的访问控制方式，具有灵活性、方便性和安全性的特点，目前在大型数据库系统的权限管理中得到普遍应用。
- 与DAC的根本区别：用户不能自主地将访问权限授给别的用户。
- 与MAC的区别在于：MAC基于多级安全需求，而RBAC则不是。

授权管理

授权管理决定谁能被授权修改允许的访问

1）强制访问控制的授权管理

在强制访问控制中，访问控制完全是根据主体和客体的安全级别决定。其中主体（用户、进程）的安全级别是由系统安全管理员赋予用户，而客体的安全级别则由系统根据创建它们的用户的安全级别决定。因此，强制访问控制的授权管理策略是比较简单的，只有安全管理员能够改变主体和客体的安全级别。

2）自主访问控制的授权管理

集中式管理：单个的管理者或组对用户进行访问控制授权和授权撤消。

分级式管理：一个中心管理者把管理责任分配给其它管理员，这些管理员再对用户进行访问授权和授权撤消。分级式管理可以根据组织结构而实行。

所属权管理：如果一个用户是一个客体的所有者，则该用户可以对其它用户访问该客体进行授权访问和授权撤消。

协作式管理：对于特定系统资源的访问不能有单个用户授权决定，而必须要其它用户的协作授权决定。

分散式管理：在分散管理中，客体所有者可以把管理权限授权给其他用户。

3）角色访问控制的授权管理

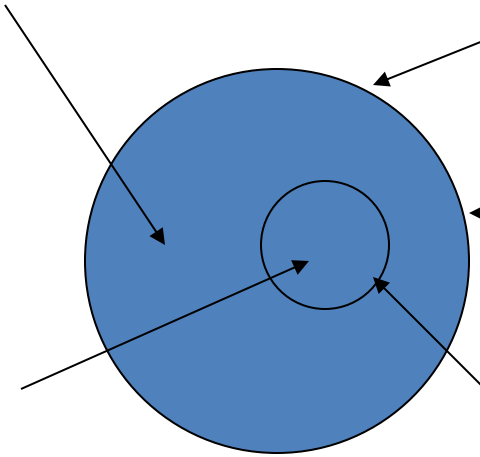
角色访问控制提供了类似自主访问控制的许多管理策略。而且，管理权限的委托代理是角色访问控制管理的重要特点，在以上的两种访问控制的管理策略中都不存在。

目标的粒度和策略的结合

- 对于相同的信息结构，由于粒度不同可能需要逻辑上截然不同的访问控制策略与机制。
  - 比如，有的数据库只能控制对一张表的整体访问或者禁止，而有的可以对一个字段进行控制
- 多种策略的结合
  - 规定策略的优先级
  - 否定策略的优先级

多重策略实例

公司数据



Feng 的数据

主　体	许 可 集
公司外的人	空集
审计员	读全部
Feng	读、修改、管理
组员	读子集
其他人	空集

—缺省策略—
没有允许被认可

—公司策略—
公司外部的人不可能得到任何许可；审计员被允许读

—Feng 的策略—
Feng 被允许读、修改、管理；组员被允许读

1) 审计是系统安全的最后一道防线
2) 审计是系统活动的流水记录
3) 审计跟踪记录系统活动的流水记录

审计内容包括：
1）个人职能：审计跟踪管理人员用来维护个人职能的技术手段
2）事件重建：发生故障后，审计跟踪重建事件和恢复数据
3）入侵检测：可协助入侵检测
4）故障分析：审计跟踪可用于实施审计或监控

- 介绍了访问控制的基本概念
- 介绍了常见访问控制模型

思考题

1、系统中有三个用户Usr1，Usr2和Usr3， Usr1创建了日志文件File1，允许Usr2向文件中写入操作记录，允许Usr3打开文件查看Usr2的操作记录；Usr2创建了一个通信进程，该通信进程允许Usr1收发消息，但只允许USr3接收消息；Usr3创建了一个共享存储区，允许Usr1读存储区内容，Usr2读写存储区内容。根据上述描述，画出对应的ACL和ACM。

2、尝试在Windows操作系统中建立一个文件，并对文件的访问权限进行管理，判断Windows操作系统采用的是否为自主访问控制模型，并说明自己的判断理由。

本讲到此结束，谢谢聆听！

Any question?