信息安全概论

访问控制

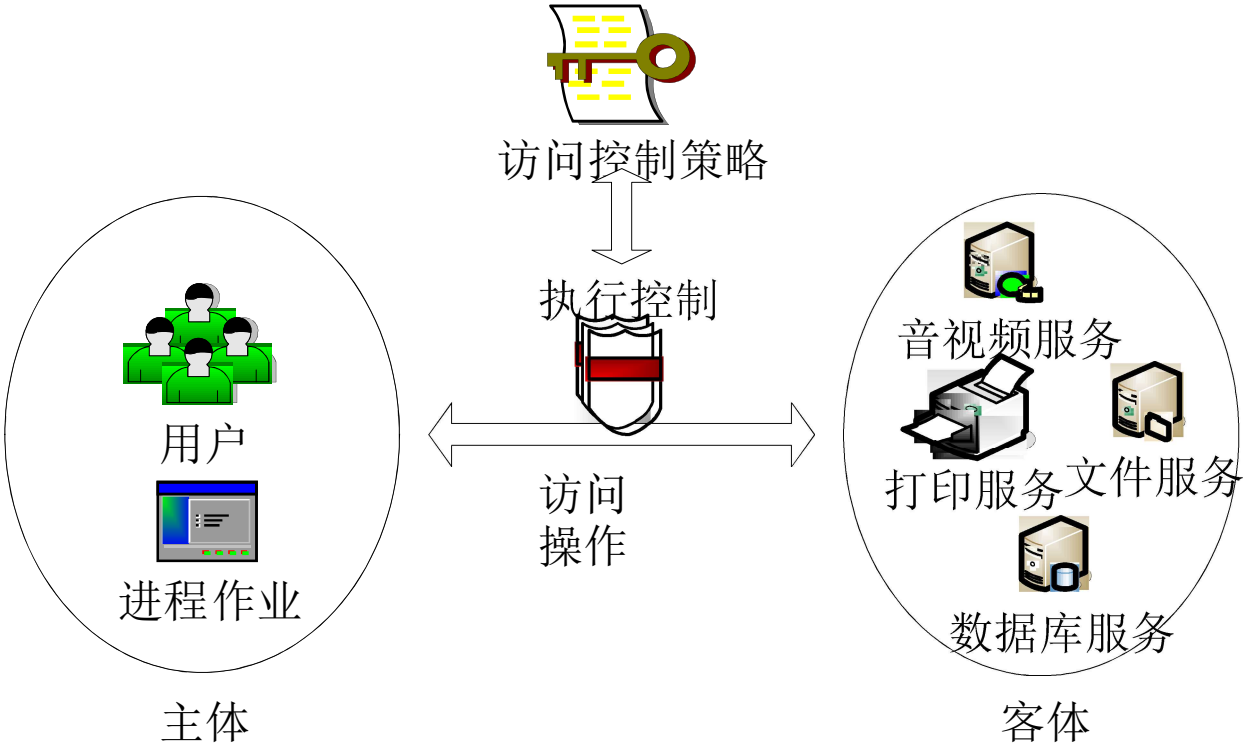
刘亚维

主要内容

- 访问控制的有关概念
- 访问控制的策略和机制
- 授权的管理、网络访问控制组件的分布
- Windows系统的安全管理

5.1 概述

- 身份认证：识别“用户是谁”的问题
- 访问控制：管理用户对资源的访问



访问控制

- 安全服务(Security Services)
  - 计算机系统中，主要的安全保护措施被称作安全服务。
- 根据ISO7498-2，安全服务包括：
  - 数据机密性(Data Confidentiality)
  - 数据完整性(Data Integrity)
  - 抗抵赖(Non-repudiation)
  - 鉴别(Authentication)
  - 访问控制(Access Control)

基本概念

- 一般定义
  - 是针对越权使用资源的防御措施
- 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，或代表用户操作的程序能做什么
  - 未授权的访问包括：
    - 非法用户进入系统
    - 合法用户对系统资源的非法使用，如未经授权的使用、泄露、修改、销毁信息以及执行指令等

基本概念

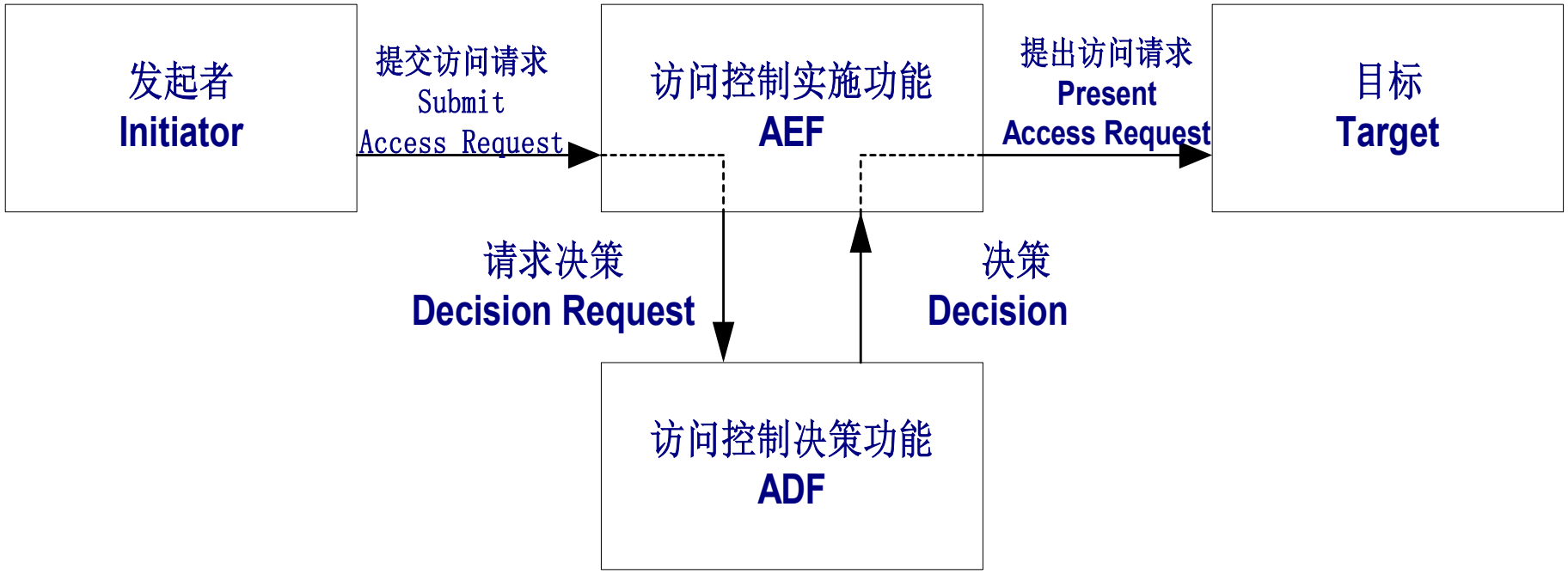
- 主要作用
  - 访问控制直接影响信息的机密性和完整性
  - 对于可用性，访问控制通过对以下信息的有效控制来实现
    - 谁可以颁发影响网络可用性的网络管理指令
    - 谁能够滥用资源以达到占用资源的目的
    - 谁能够获得可以用于拒绝服务攻击的信息

基本概念

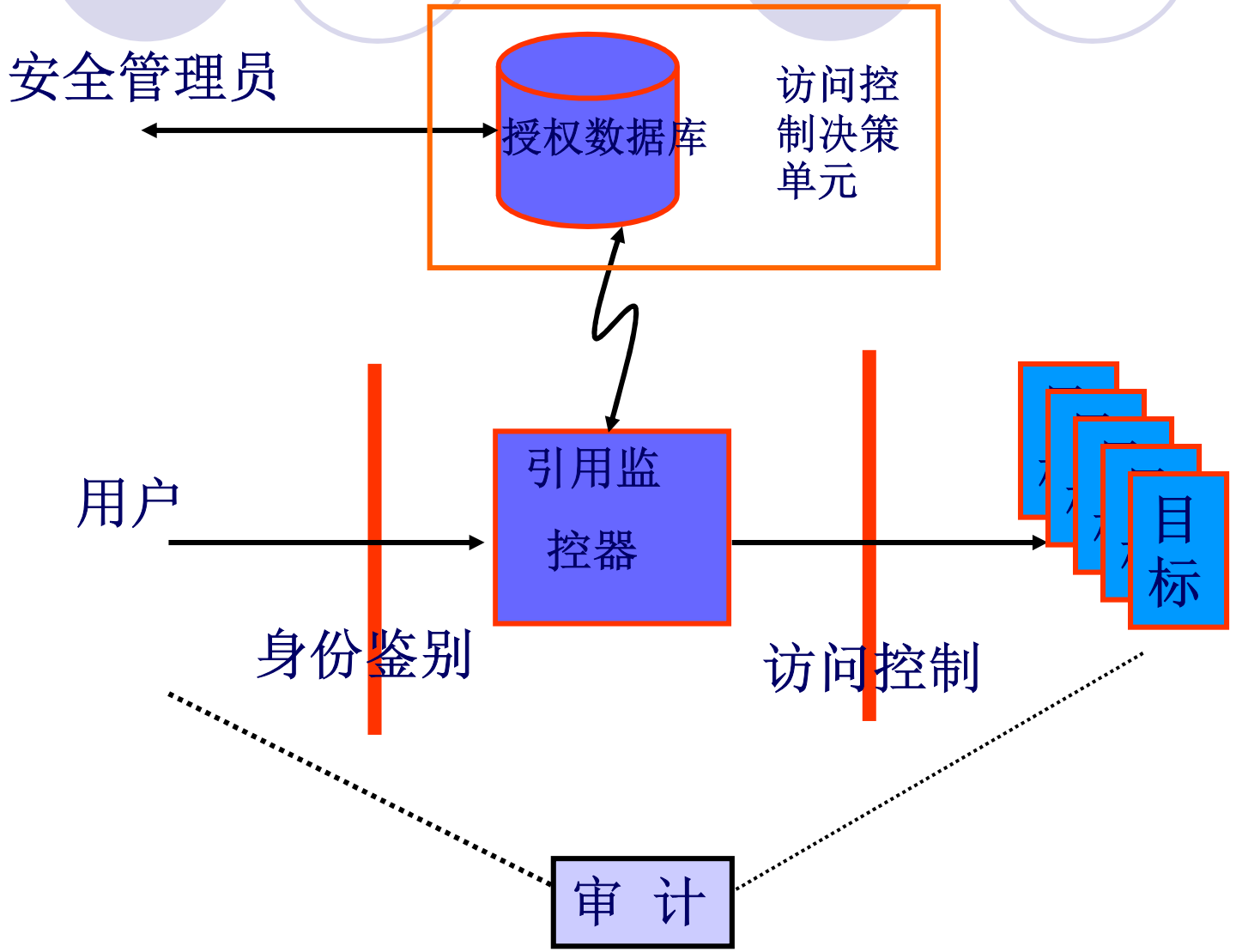
- 有关术语
  - 主体(Subject)
    - 或称为发起者(Initiator)，是一个主动的实体，根据规定可以访问某些资源(通常指用户或代表用户执行的程序)
  - 客体(Object)
    - 规定需要保护的资源，又称作目标(Target)。
  - 授权(Authorization)
    - 规定可对某资源执行的动作(如读、写、执行或拒绝访问)
  - 主客体的关系是相对的。

访问控制系统的组成

实现访问控制策略的模型



访问控制与其他安全服务的关系模型



访问控制相关概念

- 有关术语
  - 安全策略
    - 是为了描述系统的安全需求而制定的对用户行为进行约束的一整套严谨的规则。
    - 安全策略主要说明如何控制对信息的访问，说明什么样的信息流是不允许的。
  - 安全模型
    - 是对安全策略所表达的安全需求简单、抽象、无二义的描述，用来为安全系统的设计开发提供指导方针

访问控制相关概念

- 有关术语
  - 访问控制策略(Access Control Policy)：
    - 访问控制策略在系统安全策略级上表示授权。是对访问如何控制，如何作出访问决定的高层指南
  - 访问控制机制(Access Control Mechanisms)：
    - 是访问控制策略的软硬件低层实现。

如何决定访问权限

- 应该从主体和客体的标识方式以及主体对客体的访问方式等多个方面制定访问规则
  - 用户分类
  - 资源
  - 资源及使用
  - 访问规则

主体的标识

- 用户的分类
  - 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
  - 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(如UNIX系统中的root用户)
    - 还可以细分不同职责的管理员
  - 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
  - 作废的用户
    - 被系统拒绝的用户

客体的标识

- 资源的分类
  - 磁盘与磁带文件
  - 数据库中的数据
  - 系统工具和应用程序
  - 远程终端，外部设备
  - 信息管理系统的事务处理及其应用

控制资源的使用

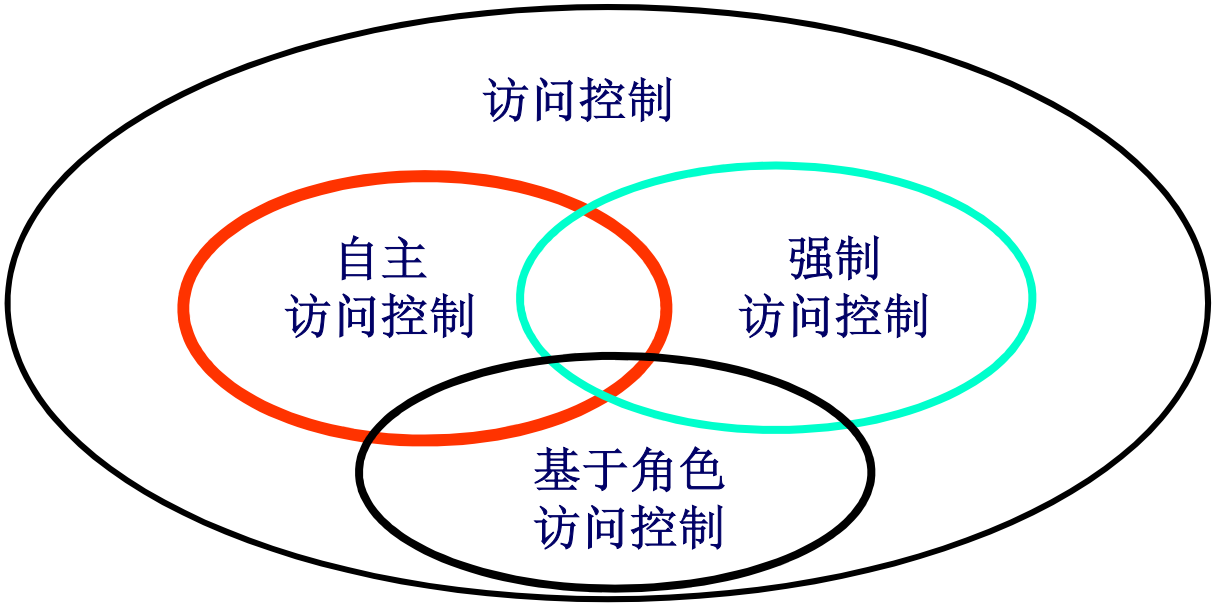
- 对需要保护的资源定义一个访问控制包(Access Control Packet)，内容包括
  - 资源名及拥有者的标识符
  - 缺省访问权
  - 用户、用户组的特权明细表
  - 允许资源的拥有者对其添加新的可用数据的操作
  - 审计数据

访问规则

- 规定了若干条件，在这些条件下，可准许访问一个资源。
- 规则使用户与资源配对，指定该用户可在该文件上执行哪些操作，如只读、不许执行或不许访问。
- 由系统管理人员或资源所有者来定义这些规则，由硬件或软件的安全内核部分负责实施。

常用的访问控制策略

- 即实施授权的指导方案
  - 自主访问控制(Discretionary Policies)
  - 强制访问控制(Mandatory Policies)
  - 基于角色的访问控制(Role-based Policies)
  - 可根据实际情况结合使用



5.2 访问控制模型

- 1985年美国军方提出可信计算机系统评估准则TCSEC，其中描述了两种著名的访问控制模型：
  - 自主访问控制DAC(Discretionary Access Control)
  - 强制访问控制MAC(Mandatory Access Control)
- 1992年美国国家标准与技术研究所(NIST)的David Ferraiolo和Rick Kuhn提出一个模型
  - 基于角色的访问控制RBAC（Role Based Access Control）模型

自主访问控制(DAC)

- 基于身份的访问控制IBAC(Identity Based Access Control)，
- 由客体的所有者自主定义访问规则，确定可以访问的主体
- 灵活宽松，被广泛使用

自主访问控制

- 记录访问规则的方式
  - 访问控制矩阵
  - 访问控制表(Access Control List)
  - 访问能力表(Access Capabilities List)

自主访问控制

- 访问控制矩阵
  - 以矩阵形式记录规则：行对应于主体，列对应于目标，每个矩阵元素规定了主体对相应的目标被准予的访问行为。
  - 实现不方便，效率低

目标 / 用户	目标X	目标Y	目标Z
用户A	R、W、Own	R、W	R
用户B		R、W、Own	
用户C	R	R、W	
用户D	R、W	R	

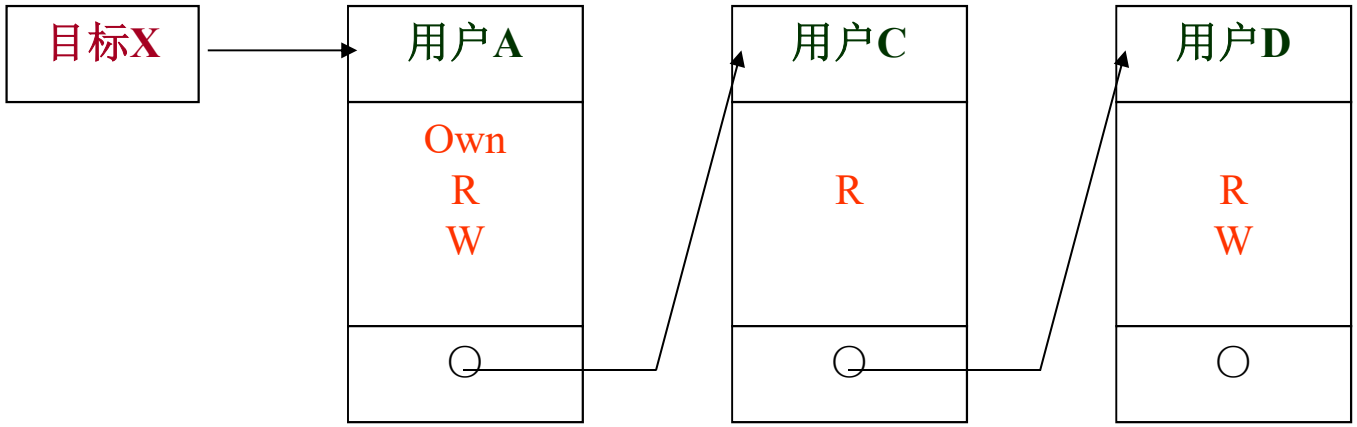
自主访问控制

- 访问控制矩阵
  - 按列看是访问控制表内容
  - 按行看是访问能力表内容

	Objects		
Subjects	O_1	O_2	O_3
S_1	Read/write		
S_2		Write	
S_3	Execute		Read

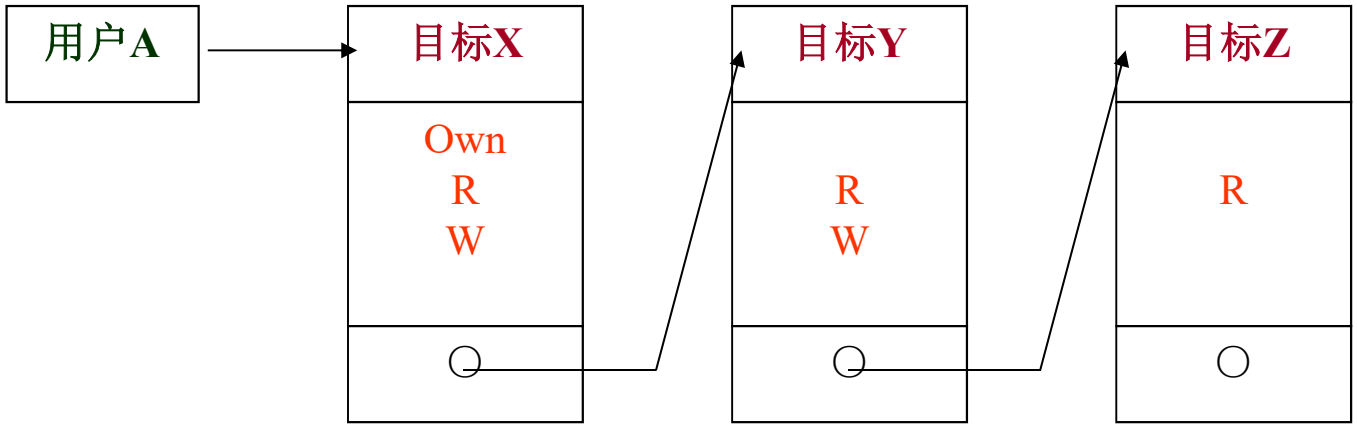
自主访问控制

- 访问控制表
  - 每个客体附加一个可以访问它的主体的链表
  - 访问控制矩阵按列看即为访问控制表
  - 可以快速根据客体查找可以访问它的主体



自主访问控制

- 访问能力表
  - 每个主体附加一个可以被他访问的客体的链表
  - 访问控制矩阵按行看即为访问能力表
  - 可以快速根据主体查找其能访问的客体



自主访问控制

- 基于组的策略
  - 当多个主体对同一个客体具有相同的访问权限时，可以采用组的策略压缩访问控制矩阵
  - 如系统公告能被所有用户读，临时目录能被所有用户写
  - 被大多数系统所采用，如Windows、Unix

自主访问控制

- 自主访问控制的缺陷
  - 过于灵活、限制较弱、可能存在安全隐患
    - 如用户A把目标X的访问权赋予了用户B，用户B可能会把X访问权转赋予用户C，而A可能并不愿意让C访问X
    - 用户A把目标X的访问权赋予了用户B，而根据系统基本安全规则，B并不能访问X

强制访问控制(MAC)

- 基于规则的访问控制，主体和客体分别定义安全等级标记，在自主访问控制的基础上还必须受到安全标记的约束。
- 安全标记是限制在目标上的一组安全属性信息项。在访问控制中，一个安全标记隶属于一个用户、一个目标、一个访问请求。

强制访问控制

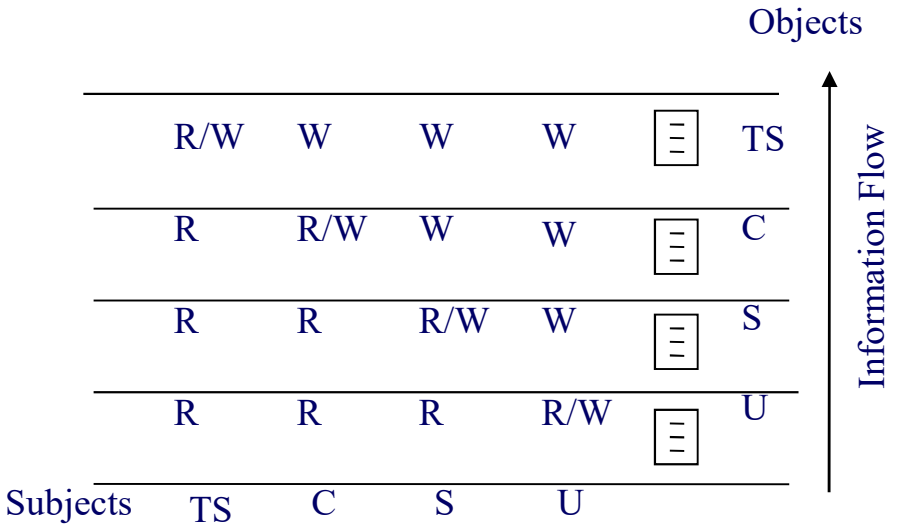
- 实现策略
  - 将主体和客体分级，根据主体和客体的级别标记来决定访问模式。
    - 绝密级，机密级，秘密级，无密级（内平）
  - 根据安全保障的重点制定控制策略
    - 保障完整性：上读/下写
    - 保障机密性：下读/上写
  - 通过安全标签实现单向信息流通

强制访问控制

- 精确描述——BLP模型
  - Bell-Lapadula模型：70年代初提出，是对多级安全策略形式化的第一个数学模型，已为许多操作系统所使用。
  - BLP模型是一个状态机模型，用状态变量来表示系统的安全状态，用状态转换规则来描述系统的变化过程。

强制访问控制

- BLP模型下保障信息机密性的控制策略



密级	英文
绝密TS	Top Secret
机密C	Confidential
秘密S	Secret
无密级U	Unclassified

基于角色的访问控制(RBAC)

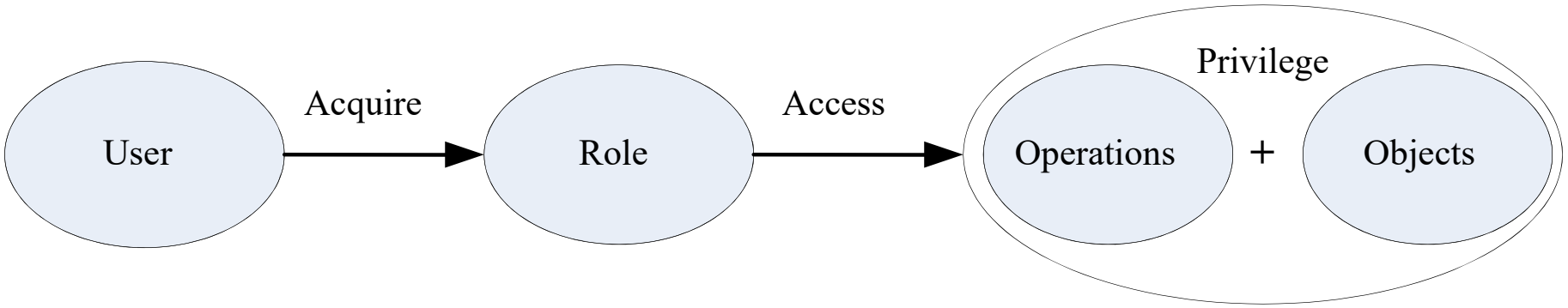
- 问题的提出
  - 自主访问控制
    - 配置的粒度小
    - 配置的工作量大，效率低
  - 强制访问控制
    - 配置的粒度大
    - 缺乏灵活性

基于角色的访问控制

- 并不直接将原子权限赋予用户，而是根据实际情况将权限组合成角色，然后指定用户的角色
- 起源于UNIX系统或别的操作系统中组的概念，是与现代的商业环境相结合的产物
  - 角色与组的区别
    - 组：一组用户的集合，通常对应于部门
    - 角色：一组用户的集合 + 一组操作权限的集合，通常对应于职务

引入角色Role的目的

- Role的目的：
  - 为了隔离User与Privilege。
  - Role作为一个用户与权限的代理层，所有的授权应该给予Role而不是直接给User或Group。
  - RBAC模型的基本思想是将访问权限分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。



基于角色的访问控制

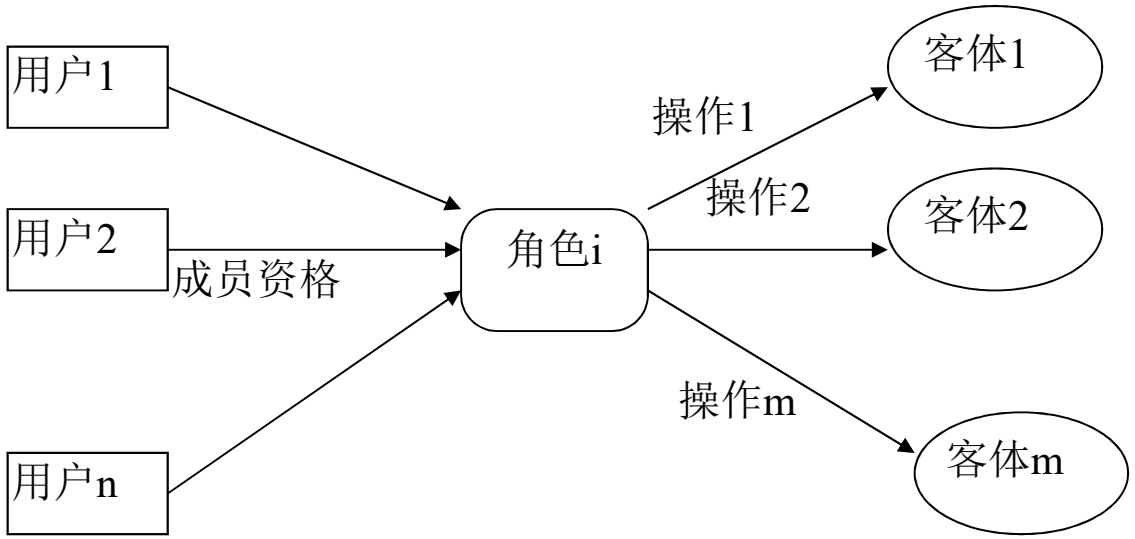
- 基于角色的访问控制的实例1
  - 在银行环境中，用户角色可以定义为出纳员、分行管理者、顾客、系统管理者和审计员
    - 出纳员可以操作顾客的帐号（如存款和取款、转帐等），并允许查询所有帐号记录
    - 分行管理者可以查询所有帐号，也允许查询分行资金报表
    - 顾客只能查询和操作他自己的帐号（如修改密码等）
    - 系统的管理者容查询系统状态（如终端连接数、ATM现金数等）和开关系统，但不允许读或操作用户的帐号
    - 审计员读系统中的审计数据，但不允许修改任何数据

基于角色的访问控制

- 基于角色的访问控制的实例2
  - 在学校环境中，用户角色可分为教师、教务员、实验员、学生等
    - 教师：制定教学计划，授课，批改作业，编写试卷，批改试卷，修改学生成绩
    - 教务员：安排课程，安排考试，登记学生成绩，查询成绩，发送成绩单
    - 实验员：安排上机，安装试验环境
    - 学生：查询成绩

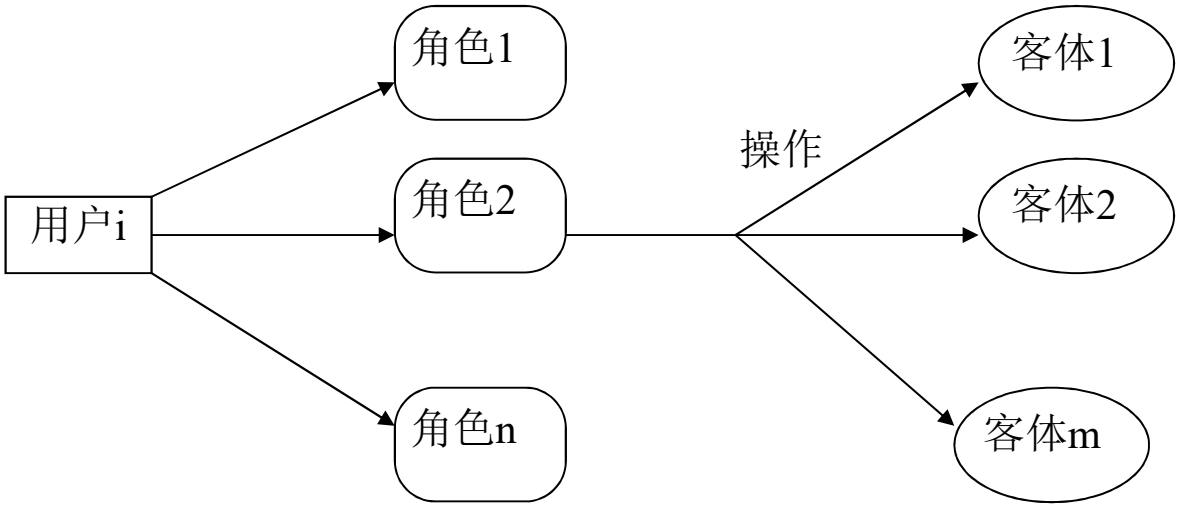
基于角色的访问控制

- 用户、角色、权限之间的关系
  - 一个角色可以拥有多个用户成员
    - 与现实相应的是在一个组织中可以有多个用户担任同一个职务，如银行有多个出纳员，学校有多位教师



基于角色的访问控制

- 用户、角色、权限之间的关系
  - 一个用户又可以是多个角色的成员
    - 与现实相应的是，在一个组织中，有些人可以身兼多职。如院长又是教授



基于角色的访问控制

- 用户、角色、权限之间的关系
  - 一个角色可以包含多种操作权限
  - 一种操作权限可以授予多个角色
  - 通过角色，用户与权限也形成多对多的关系
    - 一个用户可以具有多种操作权限
    - 一种权限可以分配给多个用户

基于角色的访问控制

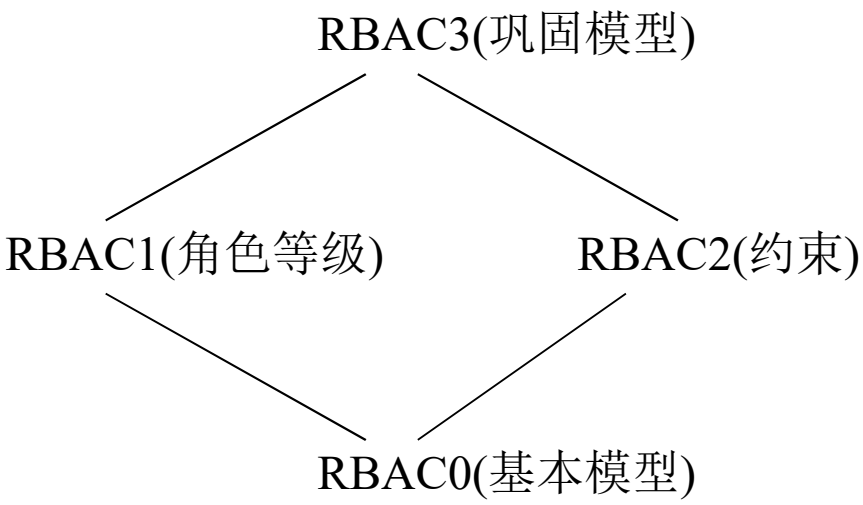
- 基于角色的访问控制的特点
  - 易于被非技术的组织策略者理解；同时也易于映射到访问控制矩阵或基于组的策略描述。
  - 同时具有基于身份策略的特征，也具有基于规则的策略的特征
  - 便于实现，容易理解

基于角色的访问控制

- 精确描述——RBAC模型
  - 虽然RBAC有很多优点，但系统的研究直到90年代后期才开始
  - 其中最权威的是由George Mason大学著名学者Ravi Sandhu领导的LIST实验室(Lab for Information Security Technology)相关的研究成果——RBAC96和RBAC97模型

基于角色的访问控制

- RBAC模型基本结构
  - RBAC0：基本模型，规定了任何RBAC系统所必须的最小要求
  - RBAC1：在RBAC0的基础上增加了角色等级的概念
  - RBAC2：在RBAC0的基础上增加了限制概念
  - RBAC3：包含了RBAC1和RBAC2，由于传递性也包含了RBAC0



基于角色的访问控制

- RBAC0（基本模型）
  - 对RBAC0模型的定义如下：
    - U：表示用户集合；R：表示角色集合；P：表示权限集合；S：表示会话（用户的一次访问请求，到操作完成）集合
    - $PA \subseteq P \times R$：表示（权限，角色）的多对多关系
    - $UA \subseteq U \times R$：表示（用户，角色）的多对多关系
    - User：$S \rightarrow U$，每一会话S_i所对应单一用户的映射
    - Roles：$S \rightarrow R$，每一会话S_i到角色集合的映射

      即$Roles(S_i) \subseteq \{r \mid (User(S_i), r) \in UA\}$

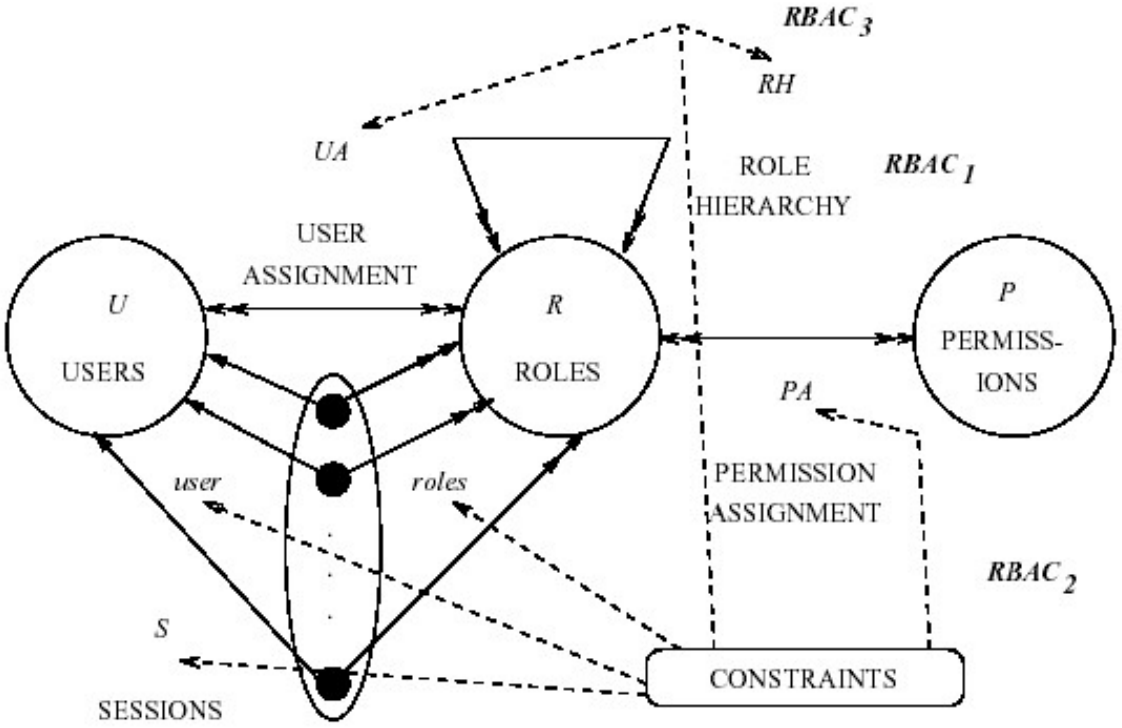
  会话S_i成功的条件：
    - 会话请求的操作$\times Roles(S_i) \in PA$

基于角色的访问控制

- RBAC0应用建模示例
  - 设U={张三，李四，王五}；R={教师，学生，教务员}；P={查成绩，改成绩，登记成绩}
  - PA={(查成绩，教师)，(查成绩，学生)，(查成绩，教务员)，(改成绩，教师)，(登记成绩，教务员)}
  - UA={(张三，教务员)，(李四，教师)，(王五，学生)}
  - 判断下列会话能否执行成功：
  - S={张三查成绩，李四改成绩，王五改成绩}
  - S_1=张三查成绩，则S_1请求的操作是{查成绩}，角色是Roles(S_1)={教务员}
  - (查成绩，教务员)∈PA，所以操作成功。

基于角色的访问控制

- RBAC96模型框架
  - RBAC96模型是一个参考模型，它提出了一个通用的参考结构或框架，为软件开发人员在系统中实现基于角色的访问控制提供了一个准则。

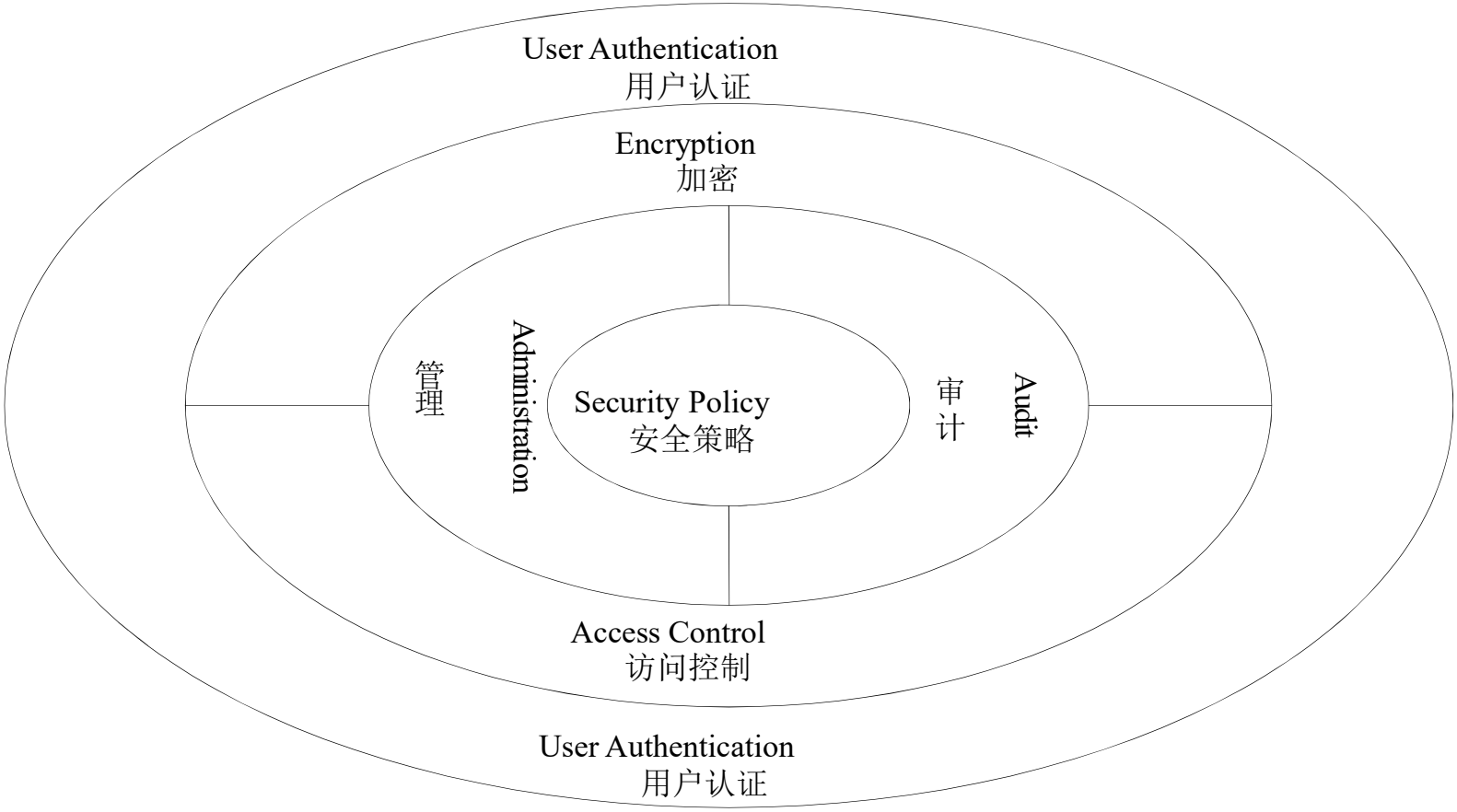


访问控制小结

- 三种最基本的访问控制策略
  - 自主访问控制
  - 强制访问控制
  - 基于角色的访问控制
- 授权基础设施基本概念

5.3 Windows系统的安全管理

5.3.1 Windows系统安全体系结构

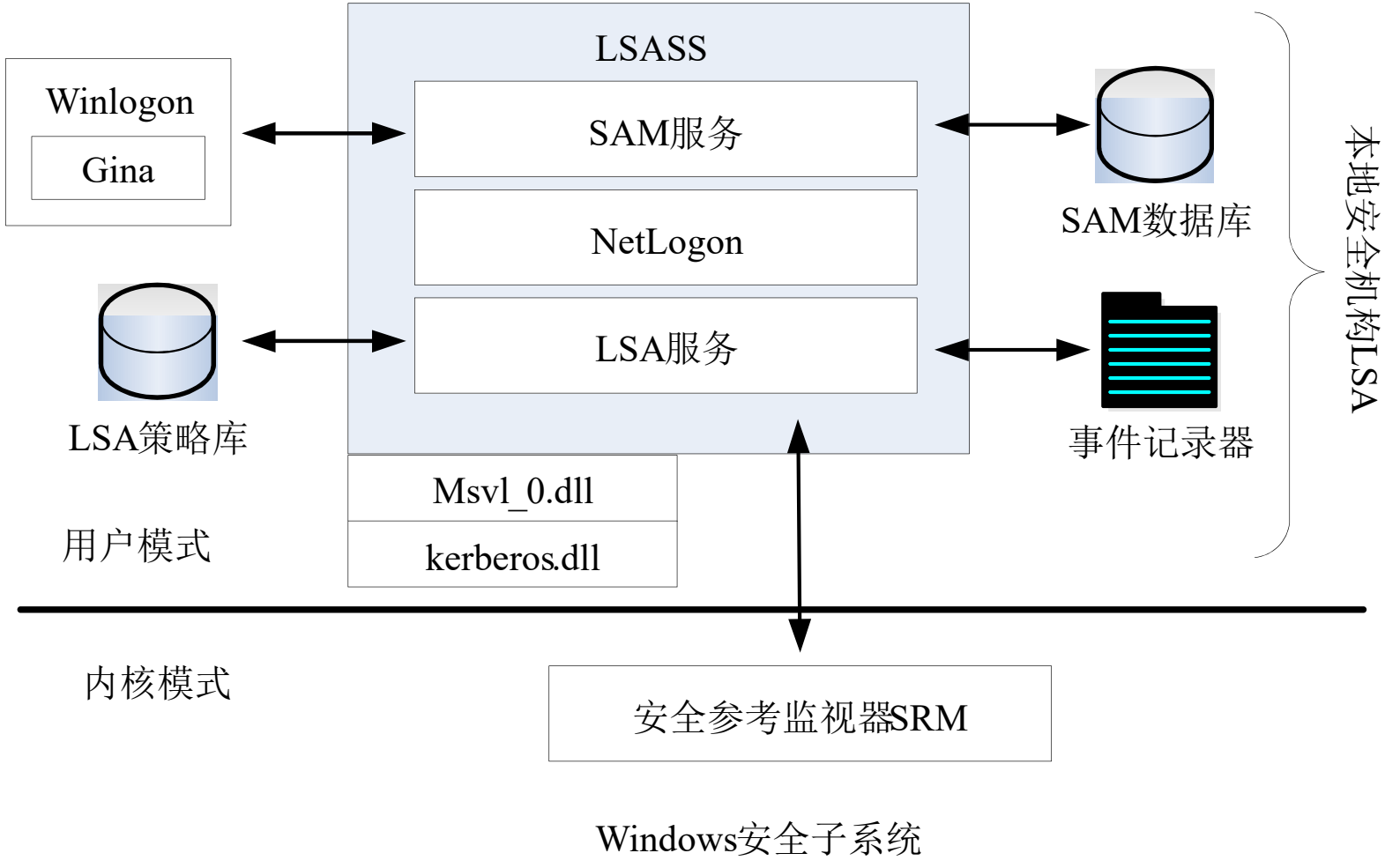


安全主体

- Windows系统的安全性主要围绕安全主体展开，保护其安全性。
- 安全主体主要包括用户、组、计算机以及域等。
  - 用户是Windows系统中操作计算机资源的主体，每个用户必须先行加入Windows系统，并被指定唯一的账户，
  - 组是用户账户集合的一种容器，同时组也被赋予了一定的访问权限，放到一个组中的所有账户都会继承这些权限；
  - 计算机是指一台独立计算机的全部主体和客体资源的集合，也是Windows系统管理的独立单元；
  - 域是使用域控制器(DC, Domain Controller)进行集中管理的网络，域控制器是共享的域信息的安全存储仓库，同时也作为域用户认证的中央控制机构。

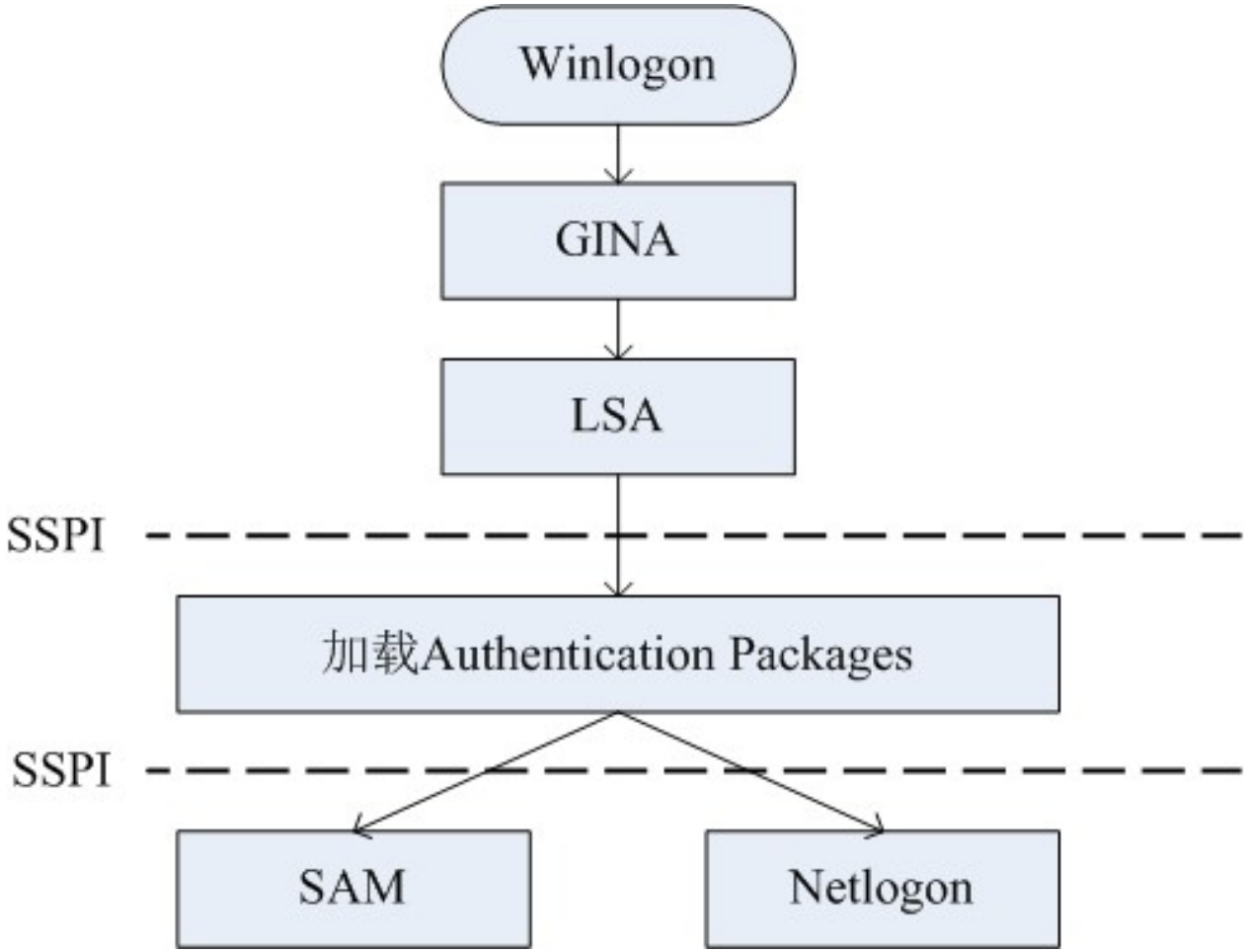
安全子系统

SAM Security Account Manage



Windows安全子系统

Windows登录认证流程



5.3.2 Windows系统的访问控制

- 访问控制模块的组成
  - 访问令牌（Access Token）和安全描述符（Security Descriptor），它们分别被访问者和被访问者持有。通过访问令牌和安全描述符的内容，Windows可以确定持有令牌的访问者能否访问持有安全描述符的对象。
- 访问控制的基本控制单元“账户”。
  - 账户是一种参考上下文(context)，是一个具有特定约束条件的容器，也可以理解为背景环境。
  - 操作系统在这个上下文描述符上运行该账户的大部分代码。
  - 那些在登录之前就运行的代码（例如服务）运行在一个账户（特殊的本地系统账户SYSTEM）的上下文中。

安全标识符SID

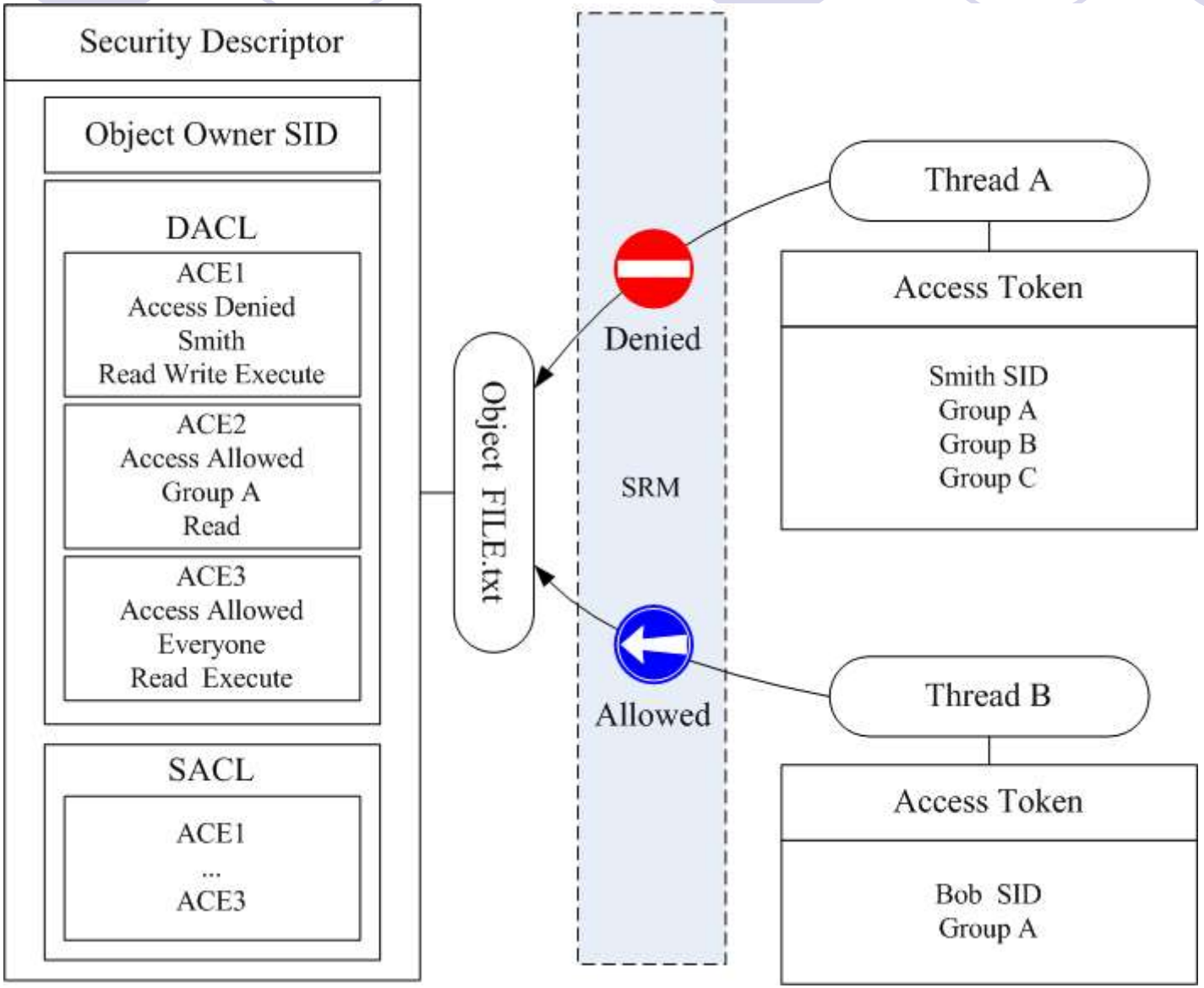
- Windows中的每个账户或账户组都有一个安全标识符SID（Security Identity）
  - Administrator、Users等账户或者账户组在Windows内部均使用SID来标识的。
  - 每个SID在同一个系统中都是唯一的。
    - 例如S-1-5-21-1507001333-1204550764-1011284298-500就是一个完整的SID。
    - 第一个数字（本例中的1）是修订版本编号，
    - 第二个数字是标识符颁发机构代码（Windows 2000为5）
    - 4个子颁发机构代码
    - 相对标识符RID（Relative Identifier） RID 500代表Administrator账户，RID 501是Guest账户。从1000开始的RID代表用户账户

访问令牌

- 每个访问令牌都与特定的Windows账户相关联，访问令牌包含该帐户的SID、所属组的SID以及帐户的特权信息。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\>whoami /all
[User]   = "Smith\Administrator"  S-1-5-21-2000478354-842925246-1202660629-500
[Group 1] = " Smith \None"  S-1-5-21-2000478354-842925246-1202660629-513
[Group 2] = "Everyone"  S-1-1-0
[Group 3] = " Smith \Debugger Users"  S-1-5-21-2000478354-842925246-
1202660629-1004
[Group  4] = "BUILTIN\Administrators"  S-1-5-32-544
[Group  5] = "BUILTIN\Users"  S-1-5-32-545
[Group  6] = "NT AUTHORITY\INTERACTIVE"  S-1-5-4
[Group  7] = "NT AUTHORITY\Authenticated Users"  S-1-5-11
[Group  8] = "LOCAL"  S-1-2-0
```

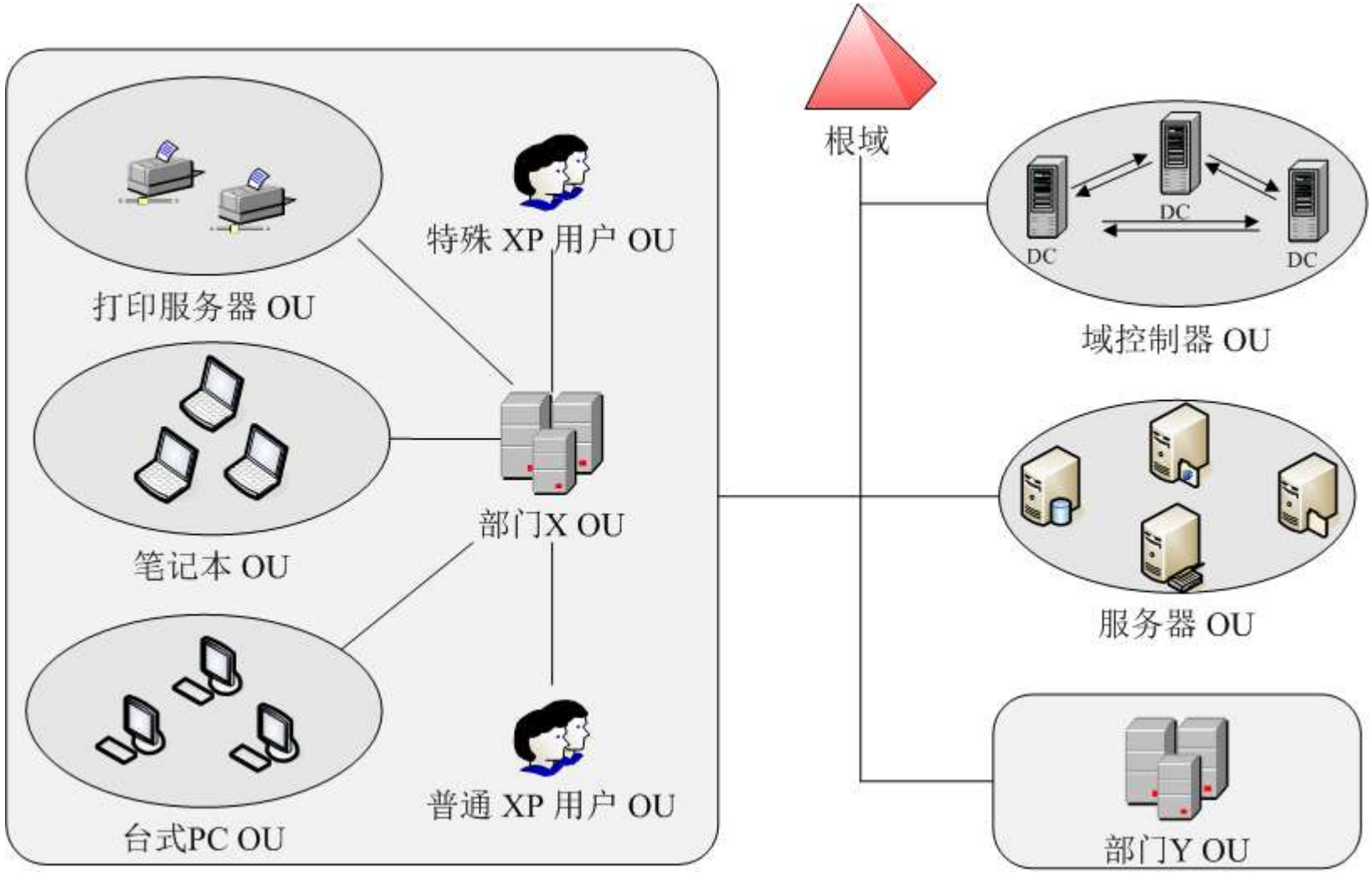
Window 访问控制


Security Descriptor
Object Owner SID
DACL
ACE1
Access Denied
Smith
Read Write Execute
ACE2
Access Allowed
Group A
Read
ACE3
Access Allowed
Everyone
Read Execute
SACL
ACE1
...
ACE3
Object FILE.txt
Denied
SRM
Allowed
Thread A
Access Token
Smith SID
Group A
Group B
Group C
Thread B
Access Token
Bob SID
Group A

5.3.3 活动目录与组策略

- 活动目录AD（Active Directory）是一个面向网络对象管理的综合目录服务，
- 网络对象包括用户、用户组、计算机、打印机、应用服务器、域、组织单元（OU）以及安全策略等。
- AD 提供的是各种网络对象的索引集合，也可以看作是数据存储的视图，
- 将分散的网络对象有效地组织起来，建立网络对象索引目录，并存储在活动目录的数据库内。

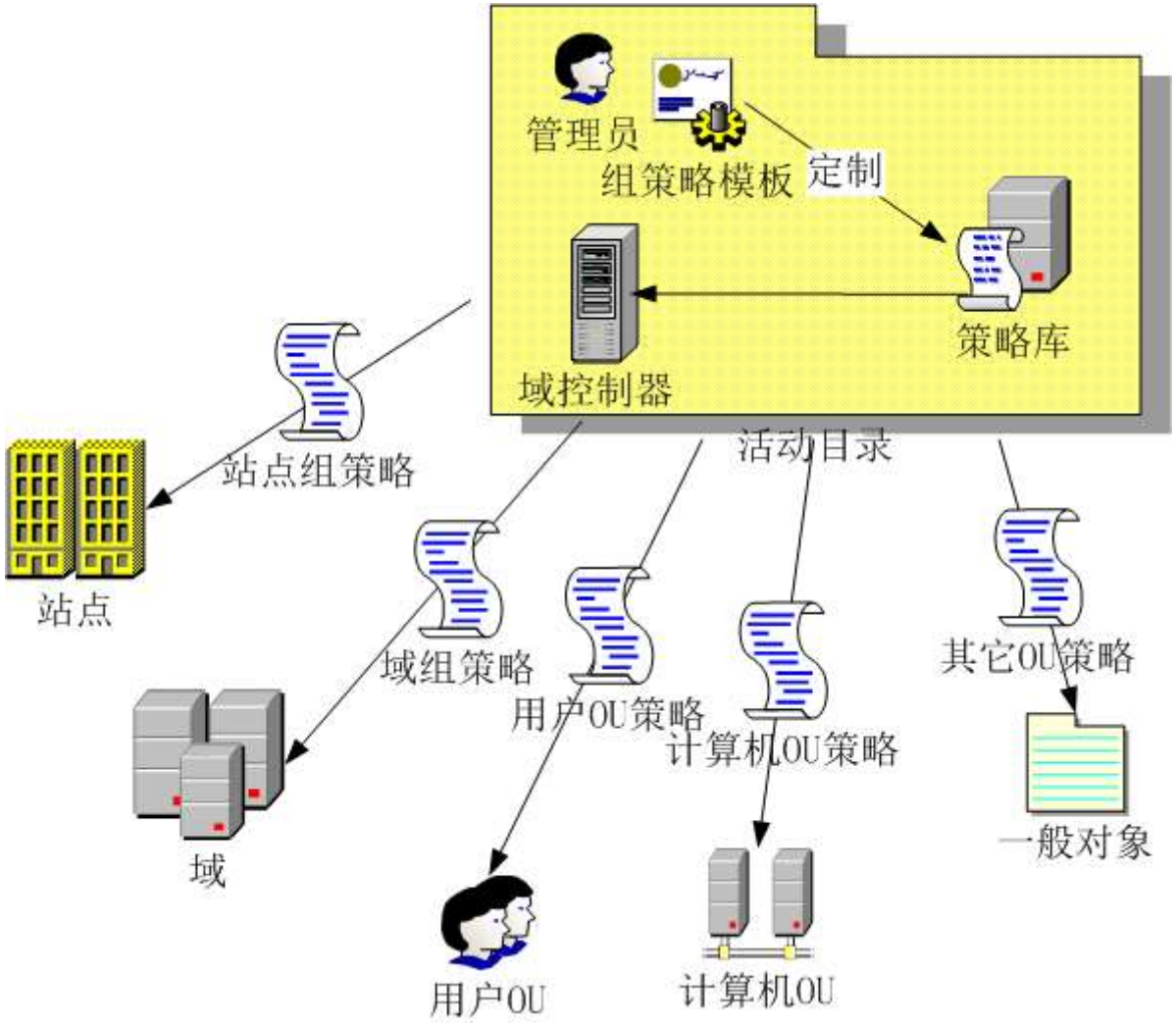
活动目录AD的管理划分



组策略GP

- 活动目录AD是Windows网络中重要的安全管理平台，组策略GP（Group Policy）是其安全性的重要体现。
- 组策略可以理解为依据特定的用户或计算机的安全需求定制的安全配置规则。
- 管理员针对每个组织单元OU定制不同的组策略，并将这些组策略存储在活动目录的相关数据库内，可以强制推送到客户端实施组策略。
- 活动目录AD可以使用组策略命令来通知和改变已经登录的用户的组策略，并执行相关安全配置。

组策略工作流程


管理员
组策略模板
定制
策略库
域控制器
活动目录
站点组策略
站点
域组策略
用户OU策略
计算机OU策略
其它OU策略
域
一般对象
用户OU
计算机OU

组策略的实施

- 注册表是Windows系统中保存系统应用软件配置的数据库。
- 很多配置都是可以自定义设置的，但这些配置发布在注册表的各个角落，如果是手工配置，可想是多么困难和繁琐。
- 组策略可以将系统中重要的配置功能汇集成一个配置集合，管理人员通过配置并实施组策略，达到直接管理计算机的目的。
- 简单点说，实施组策略就是修改注册表中的相关配置。

组策略和活动目录AD配合

- 组策略分为基于活动目录的和基于本地计算机的两种：
  - AD组策略存储在域控制器上活动目录AD的数据库中，它的定制实施由域管理员来执行；而本地组策略存放在本地计算机内，由本地管理员来定制实施。
  - AD组策略实施的对象是整个组织单元OU；本地组策略只负责本地计算机。
- 组策略和活动目录AD配合
  - 组策略部署在OU、站点或域的范围内，也可以部署在本地计算机上。部署在本地计算机时，组策略不能发挥其全部功能，只有和AD配合，组策略才可以发挥出全部潜力。

组策略的主要工作

① 部署软件

② 设置用户权力

③ 软件限制策略

- 管理员可以通过配置组策略，限制某个用户只能运行特定的程序或执行特定的任务。

④ 控制系统设置：

- 允许管理员统一部署网络用户的Windows服务。

⑤ 设置登录、注销、关机、开机脚本。

⑥ 通用桌面控制

⑦ 安全策略

⑧ 重定向文件夹

⑨ 基于注册表的策略设置

Any question?