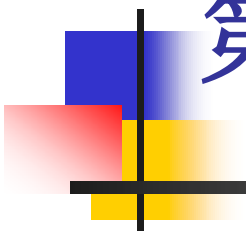
第4章网络操作系统安全与访问控制



4.1 网络操作系统的概念

4.2 操作系统安全级别

4.3 系统访问控制

4.4 常见操作系统的安全配置

4.1 网络操作系统的概念

- 操作系统（**Operating System**，简称**OS**）是计算机系统中用来管理各种软硬件资源，提供人机交互使用的软件。操作系统提供进程管理、存储管理、设备管理、文件管理和人机接口五大基本功能。
- 早期计算机的操作系统，如**DOS**、**Windows3.1**和**OS/2**等，只能使用本地计算机的软硬件资源，如中央处理器，主存储器，磁盘存储器，打印机，磁带存储器，显示器，键盘输入设备和鼠标等，存放于计算机内的各种数据，如文件，程序库，知识库，系统软件和应用软件等。
- 网络操作系统（**Network Operating System**，简称**NOS**）除了实现单机操作系统的全部功能外，还具备管理网络中的共享资源，实现用户通信以及方便用户使用网络等功能，是网络用户与计算机网络之间的接口。

网络操作系统特点

- 网络操作系统作为网络用户和计算机之间的接口，通常具有复杂性、并行性、高效性和安全性等特点。
- 网络操作系统一般具有如下功能：

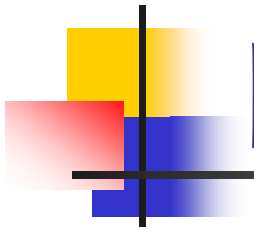
（1）支持多任务：要求操作系统在同一时间能够处理多个应用程序，每个应用程序在不同的内存空间运行。

（2）支持大内存：要求操作系统支持较大的物理内存，以便应用程序能够更好的运行。

（3）支持对称多处理：要求操作系统支持多个CPU减少事务处理时间，提高操作系统性能。

（4）支持网络负载平衡：要求操作系统能够与其它计算机构成一个虚拟系统，满足多用户访问时的需要。

（5）支持远程管理：要求操作系统能够支持用户通过Internet远程管理和维护，比如Windows Server 2003操作系统支持的终端服务。



网络操作系统结构

NOS工作模式通常有对等网络和客户机/服务器网络两种。

- 客户机/服务器网络 Client/Server (C/S)

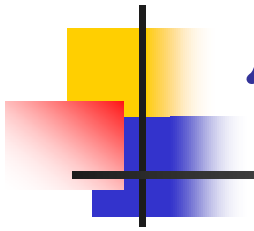
  Novell NetWare是典型的客户机/服务器网络操作系统，主要用在局域网。

  客户机操作系统的功能是让用户能够使用本地资源和处理本地的命令和应用程序，另一方面实现客户机与服务器的通信，可以搜索所需的服务器资源，并能接收服务器所传递的数据。

  服务器操作系统其主要功能是管理服务器和网络中的各种资源，实现服务器与客户机的通信，提供网络服务和提供网络安全管理。

- 网络操作系统对等模式 Peer to Peer (P2P)

  采用这种模式的站点都是对等的，既可以作为客户访问其它站点，又可以作为服务器向其他站点提供服务。这种模式具有分布处理和分布控制的功能。

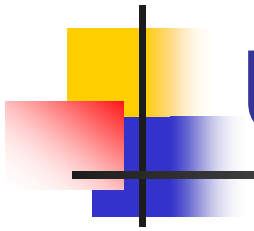


常见网络操作系统

目前服务器常用的操作系统有三类：

- **Unix**
- **Linux**
- **Windows NT系列**

这些操作系统都是符合**C2**级安全级别



UNIX系统

- UNIX操作系统是由美国贝尔实验室开发的一种多用户、多任务的通用操作系统。它从一个实验室的产品发展成为当前使用普遍、影响深远的主流操作系统。

- UNIX诞生于20世纪60年代末期，贝尔实验室的研究人员于1969年开始在GE645计算机上实现一种分时操作系统的雏形，后来该系统被移植到了DEC的PDP-7小型机上。

- 1970年给系统正式取名为Unix操作系统。到1973年，Unix系统的绝大部分源代码都用C语言重新编写过，大大提高了Unix系统的可移植性，也为提高系统软件的开发效率创造了条件。

主要特色

- UNIX操作系统经过20多年的发展后，已经成为一种成熟的主流操作系统，并在发展过程中逐步形成了一些新的特色，其中主要特色包括5个方面。

  （1）可靠性高

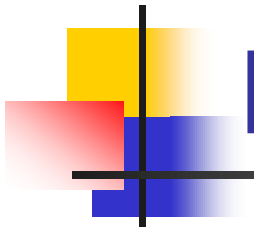
  （2）极强的伸缩性

  （3）网络功能强

  （4）强大的数据库支持功能

  （5）开放性好

- IBM AIX，Sun Solaris，HP-UX，Apple MacOS，FreeBSD，NetBSD

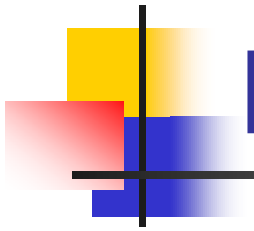


Linux系统

- Linux是一套可以免费使用和自由传播的类Unix操作系统，主要用于基于Intel x86系列CPU的计算机上。这个系统是由全世界各地的成千上万的程序员设计和实现的。其目的是建立不受任何商品化软件的版权制约的、全世界都能自由使用的Unix兼容产品。

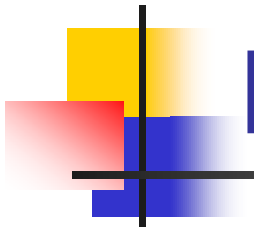
- Linux最早开始于一位名叫Linus Torvalds的计算机业余爱好者，当时他是芬兰赫尔辛基大学的学生。

- 目的是想设计一个代替Minix（是由一位名叫Andrew Tannebaum的计算机教授编写的一个操作系统示教程序）的操作系统。这个操作系统可用于386、486或奔腾处理器的个人计算机上，并且具有Unix操作系统的全部功能。



Linux系统

- Linux是一个免费的操作系统，用户可以免费获得其源代码，并能够随意修改。
- 它是在共用许可证GPL(General Public License)保护下的自由软件，也有好几种版本，如Red Hat Linux、Slackware，以及国内的Xteam Linux、红旗Linux等等。Linux的流行是因为它具有许多优点，典型的优点有7个。



Linux的优点

（1）完全免费
（2）完全兼容POSIX 1.0标准
（3）多用户、多任务
（4）良好的界面
（5）丰富的网络功能
（6）安全可靠、性能稳定
（7）支持多种平台 x86，ARM，SPARC，Alpha，MIPS，龙芯等，可运行在手机、平板电脑、路由器、视频游戏控制台、个人计算机、大型机和超级计算机。

Windows系统

- Windows NT（New Technology）是微软公司第一个真正意义上的网络操作系统，发展经过3.0、4.0、5.0（Windows 2000）、5.1（Windows XP）5.2（Windows Server 2003）、6.0（Vista/2008）6.1（Windows7/2008R2）6.2（Windows 8/2012）、6.3（Windows 8.1/2012R2）10（Windows 10）等众多版本，并逐步占据了广大的中小网络操作系统的市场。
- Windows NT与Windows 9X的用户界面和操作方法基本相同。与Windows 9X相比，Windows NT的网络功能更加强大并且安全。

Windows NT系列操作系统

- Windows NT系列操作系统具有以下三方面的优点。

（1）支持多种网络协议

- 由于在网络中可能存在多种客户机，如Windows 95/98、Apple Macintosh、Unix、OS/2等等，而这些客户机可能使用了不同的网络协议，如TCP/IP协议、IPX/SPX等。Windows NT系列操作支持几乎所有常见的网络协议。

（2）内置Internet功能

- 随着Internet的流行和TCP/IP协议组的标准化，Windows NT内置了IIS（Internet Information Server），可以使网络管理员轻松的配置WWW和FTP等服务。

（3）支持NTFS文件系统

- Windows 9X所使用的文件系统是FAT，在NT中内置同时支持FAT和NTFS的磁盘分区格式。使用NTFS的好处主要是可以提高文件管理的安全性，用户可以对NTFS系统中的任何文件、目录设置权限，这样当多用户同时访问系统的时候，可以增加文件的安全性。

4.2 操作系统安全级别

- 为了对一个计算机系统进行安全评估，美国国防部按处理信息的等级和应采用的相应措施，将计算机安全分为：A、B、C、D 4等8个级别，共27条评估准则，可信任计算机系统评价标准（TCSEC）。从最低等级D等开始，到A等。随着安全等级的提高，系统的可信度随之增加，风险逐渐减少。
- 国内的安全操作系统评估标准

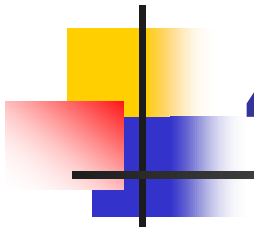
  《信息技术安全性评估准则》GB/T 18336 2001。该准则将操作系统安全分为五个级别，分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。

4.2 操作系统安全级别

- D等非保护级，不能在多用户环境下处理敏感信息。
- C等为自主保护级，具有一定的保护功能，采用的措施是自主访问控制和审计跟踪。它一般只适用于具有一定等级的多用户环境，并具有对主体责任和对他们的初始动作审计的能力。
- B等为强制保护级，这一等级比C等级的安全功能有很大增强。它要求对客体实施强制访问控制，并要求客体必须带有敏感标志，可信计算机利用它去施加强制访问控制。
- A等是验证保护级。它的显著特征是从形式设计规范说明和验证技术导出分析，并高度地保证正确地实现可信计算

表3-1 可信计算机系统评估准则

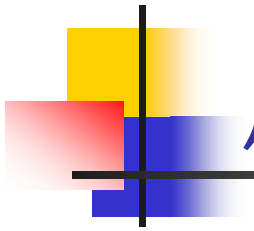
类别	名称	主 要 特 征
A	可验证的安全设计	形式化的最高级描述和验证，形式化的隐秘通道分析，非形式化的代码一致性证明
B3	安全域机制	安全内核，高抗渗透能力
B2	结构化安全保护	设计系统时必须有一个合理的总体设计方案，面向安全的体系结构，遵循最小授权原则，较好的抗渗透能力，访问控制应对所有的主体和客体提供保护，对系统进行隐蔽通道分析
B1	标号安全保护	除了C2级别的安全需求外，增加安全策略模型、数据标号(安全和属性)、托管访问控制
C2	受控的访问环境	存取控制以用户为单位广泛地审计 UNIX、LINUX和WindowsNT
C1	选择的安全保护	有选择的存取控制，用户与数据分离，数据的保护以用户组为单位 早期的Unix
D	最小保护	保护措施很少，安全功能太弱 DOS，WINDOWS98



4.3 系统访问控制

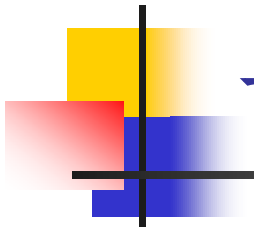
用户帐户管理

- 帐户：用于管理访问计算机系统的实体
  - 人
  - 软件实体
  - 其它计算机
  - ……
- 用户登录系统时，确定每个用户访问系统资源的权限
  - 登录计算机
  - 访问文件系统
  - 执行系统命令
  - 系统管理
  - ……



用户登录

- 用户只有登录才能访问系统
- 用户身份识别
  - 用户名/口令
  - 智能卡
  - 身份认证协议：**PAP、CHAP、Kerberos、…**
    - **Password Authentication Protocol, Challenge-Handshake Authentication Protocol**
  - ……
- 对用户的访问授权
  - 根据用户帐户数据库中的信息对登录用户授权
  - 存在多种访问控制方法，相应的授权和管理方法也不同

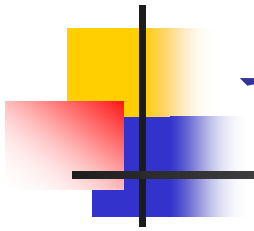


访问控制

- 访问控制
  - 为了安全目的，依据策略或权限机制，控制对资源进行的不同授权访问
  - 保障授权用户能获取所需资源
  - 拒绝非授权用户的资源访问请求
- 身份认证是访问控制的前提条件
- 访问控制是应用系统不可缺少的重要部分
- 访问控制包含3个要素：主体、客体和控制策略。

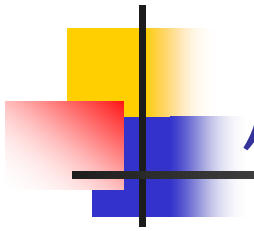
访问控制的相关概念

- 主体（**Subject**）
  - 是指一个提出请求或要求的实体，是动作的发起者，但不一定是动作的执行者。通常指用户或代表用户执行的程序
- 客体（**Object**）
  - 是指接受其它实体访问的被动实体，是规定需要保护的资源，又称作目标。既可以是信息、文件、记录，也可以是硬件设备
- 控制策略
  - 是主体对客体的操作行为集和约束条件集。简单讲，控制策略是主体对客体的访问规则集，体现了一种授权行为，也就是客体对主体的权限允许，这种允许不得超过规则集



访问控制的目的

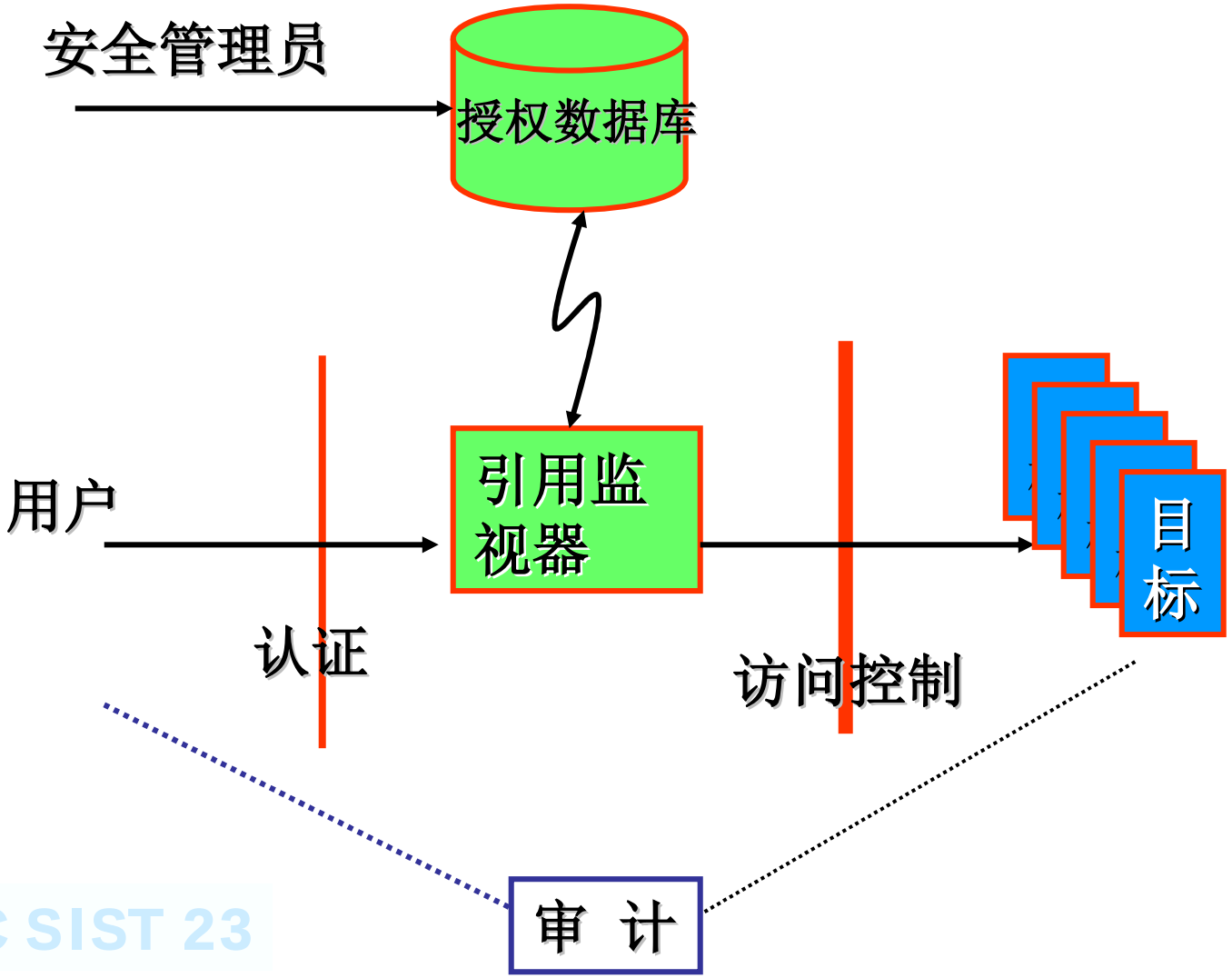
- 通过访问控制策略显式地准许或限制主体的访问能力及范围
- 限制和管理合法用户对关键资源的访问，使得资源的使用在合法范围内进行
- 防止和追踪非法用户的侵入，以及合法用户的不慎操作等行为对权威机构造成的破坏



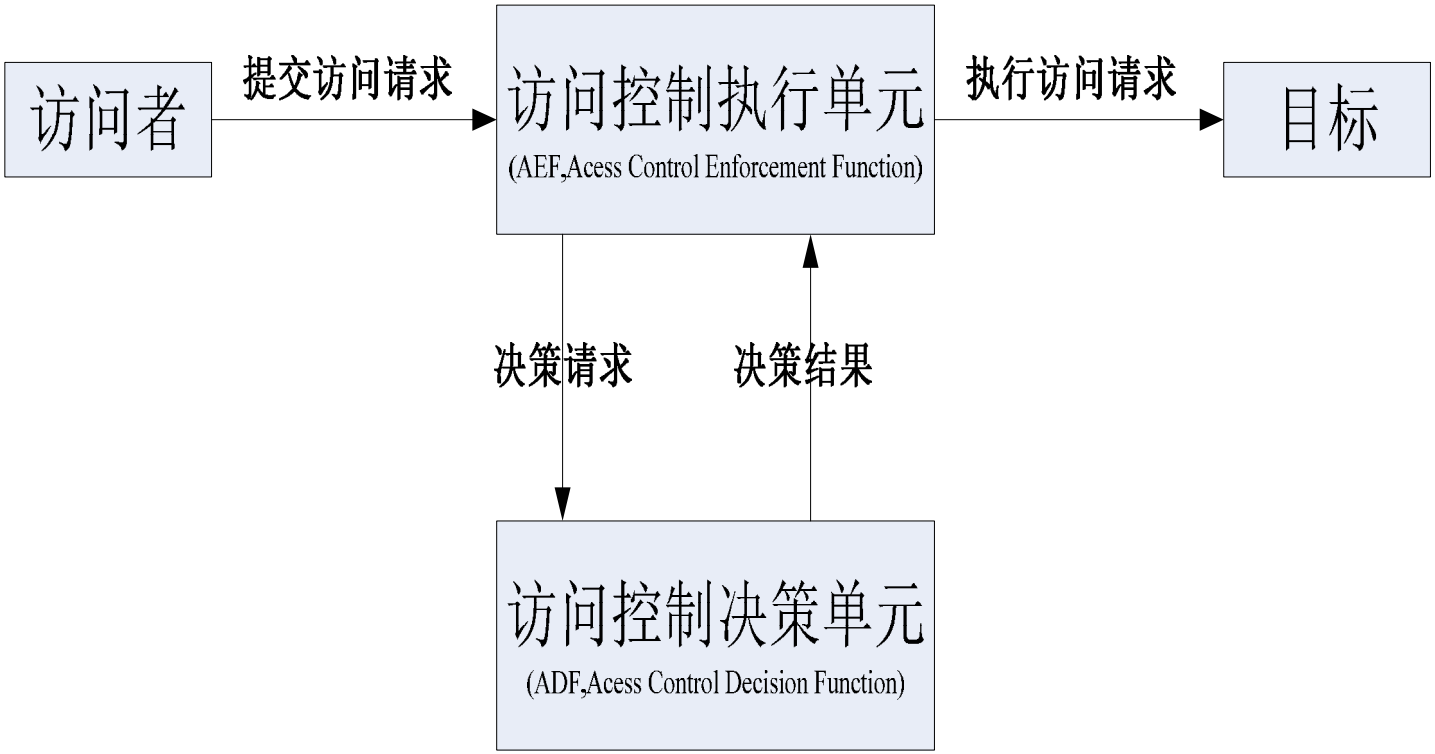
用户认证、授权和访问控制

- 计算机系统中，用户对数据的访问必须在系统的控制之下进行，以保证计算机系统的安全性
- 访问控制一般通过设置访问权限而实现
- 访问控制功能一般集成在操作系统中
- 访问控制建立在用户身份认证基础之上
- 访问控制是审计和计费的前提

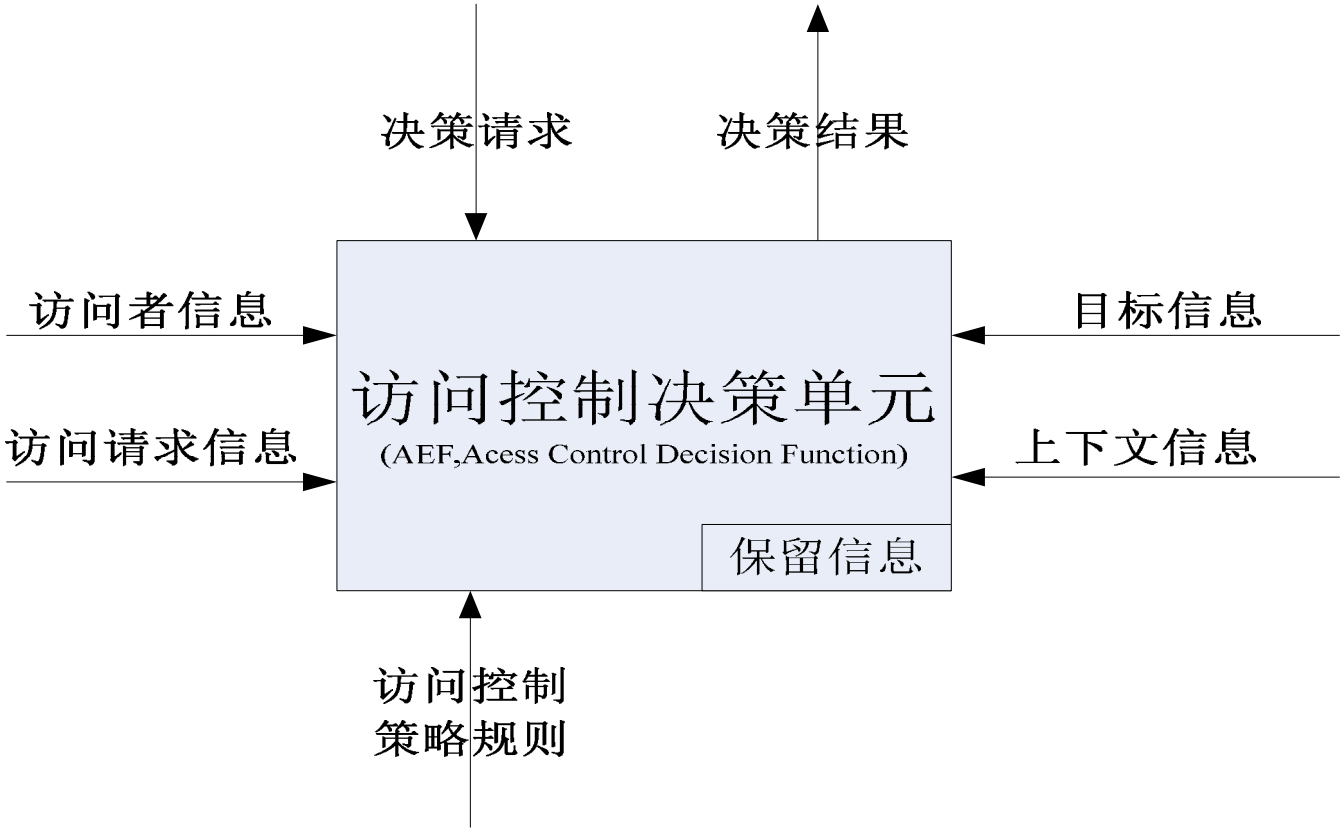
访问控制的一般模型

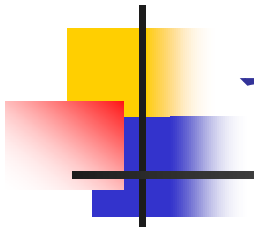


访问控制模型基本组成


访问者
提交访问请求
访问控制执行单元
(AEF,Acess Control Enforcement Function)
执行访问请求
目标
决策请求
决策结果
访问控制决策单元
(ADF,Acess Control Decision Function)

访问控制决策单元

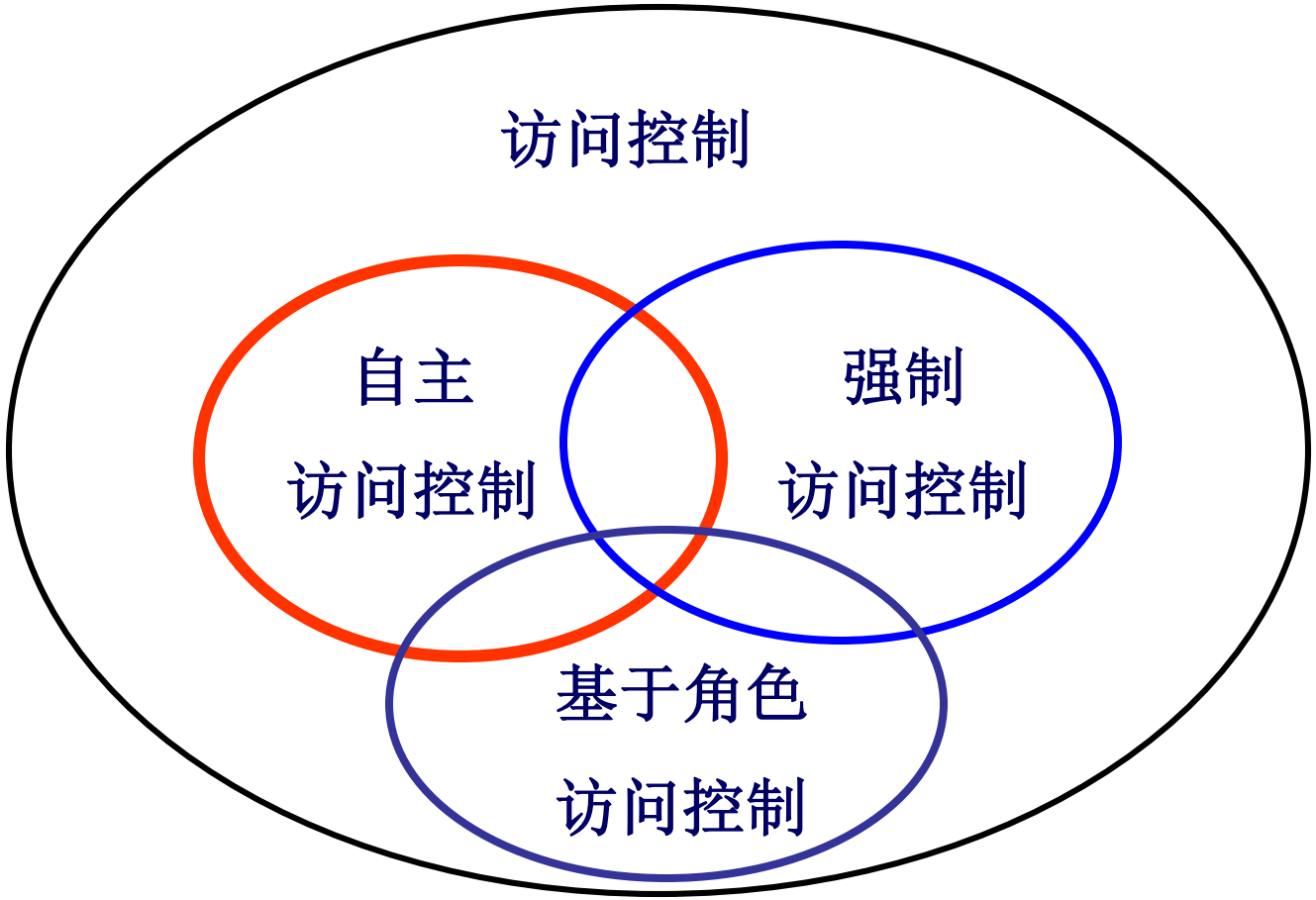

决策请求
决策结果
访问者信息
目标信息
访问控制决策单元
(AEF,Acess Control Decision Function)
访问请求信息
上下文信息
保留信息
访问控制
策略规则

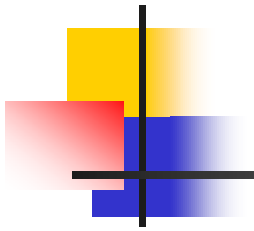


访问控制策略的分类

- 自主访问控制（Discretionary Access Control)简称DAC
- 强制访问控制(Mandatory Access Control）简称MAC
- 基于角色的访问控制(Role Based Access Control)简称RBAC

访问控制策略





自主访问控制

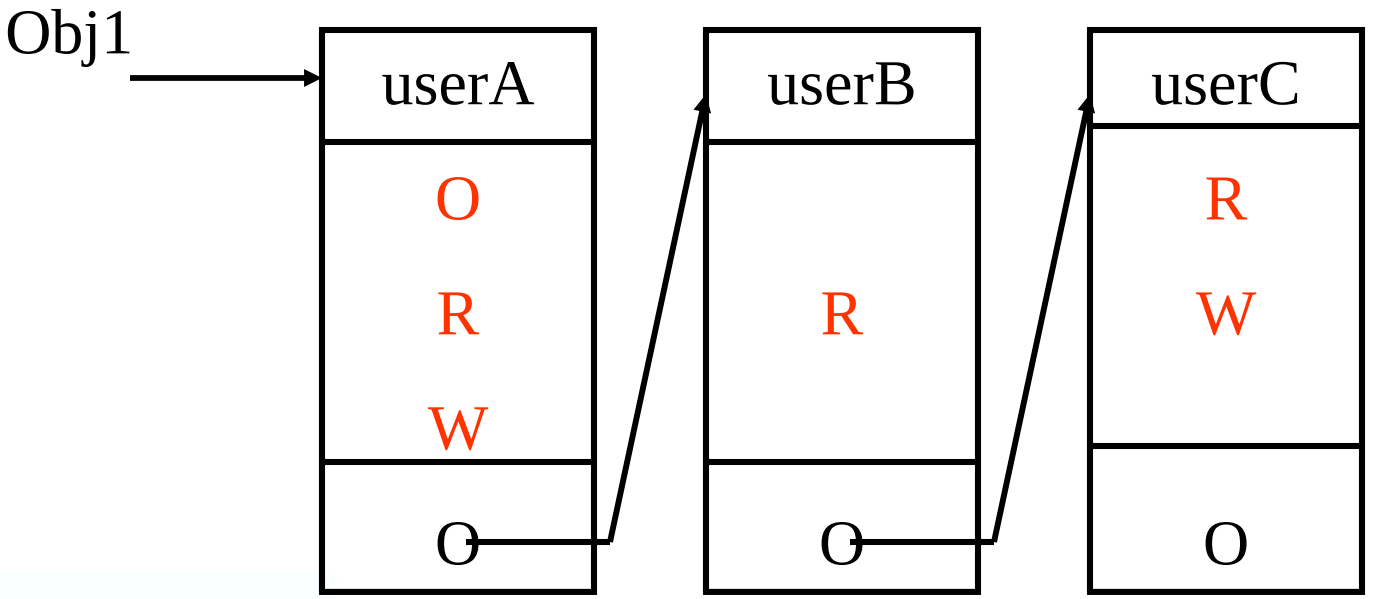
- 根据用户的身份或组成员身份，允许合法用户访问策略规定的客体，同时阻止非授权用户访问客体
- 用户还可以把自己所拥有的客体的访问权限授予其它用户。
- 自主是指
  - 用户有权对自身所创建的访问对象(文件、数据库表等)进行访问，
  - 有权将对这些对象的访问权授予其他用户和从授予权限的用户收回其访问权限。

自主访问控制模型的应用

- 自主访问控制又称为任意访问控制，是一种常用的访问控制方式。
  - UNIX、Windows SERVER版本的操作系统都提供自主访问控制的功能。
- 在实现上，首先要对用户的身份进行鉴别，然后按照访问控制列表所赋予用户的权限，允许和限制用户使用客体的资源。
- 主体控制权限的修改通常由特权用户（管理员）或是特权用户组实现。

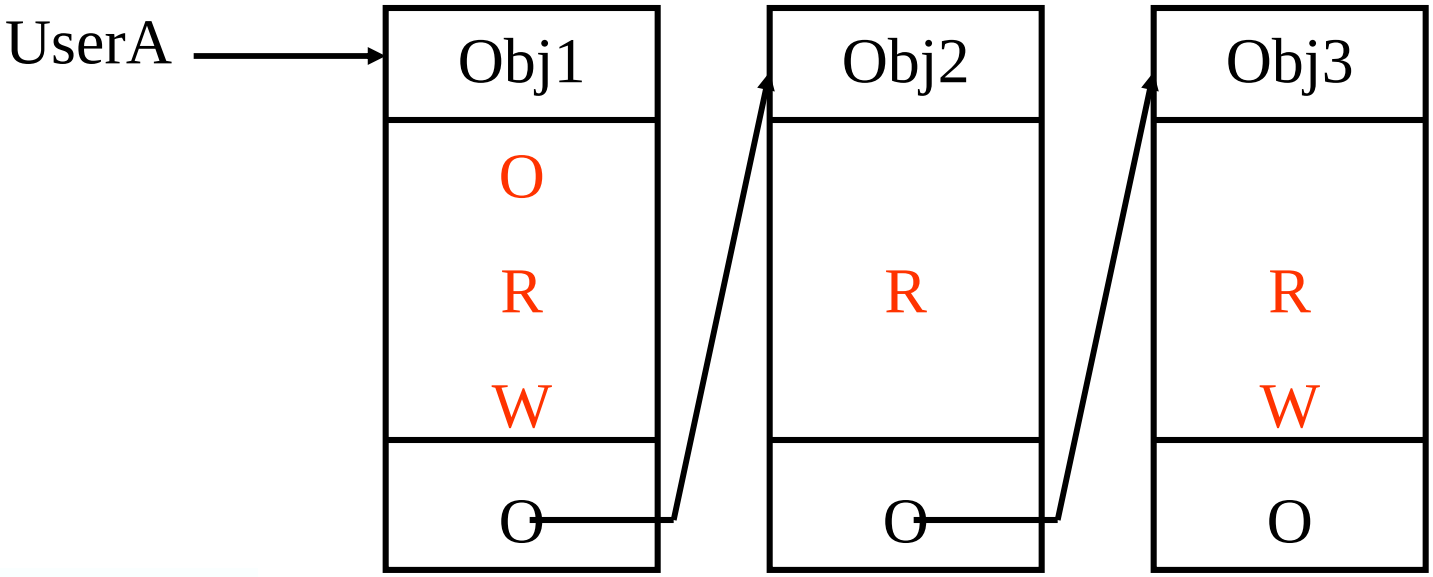
访问控制表（Acess Control List）

- 以客体为中心建立的访问权限表。
- 根据访问者（主体）的请求（客体信息），结合访问者身份在访问控制表中查找访问者的权限，判断访问者是否具有操作客体的能力。



访问能力表（Acess Capabilities List）

- 以主体为中心建立访问权限表
- 根据访问者（主体）的身份，结合请求（客体信息）信息在访问能力表中查找访问者的权限，判断访问者是否具有操作客体的能力。

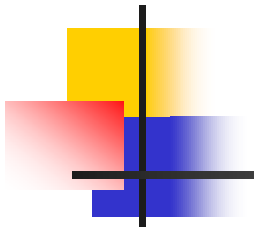


实现举例

- 通过矩阵形式表示访问控制规则和授权用户权限的方法。
  - 对每个主体而言，都拥有对哪些客体的哪些访问权限；而对客体而言，又有哪些主体对他可以实施访问；将这种关连关系加以阐述，就形成了控制矩阵。
- 如果主体和客体很多，控制矩阵将会成几何级数增长，会有大量的空余空间。

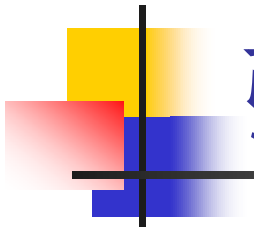
- 按列看是访问控制表内容
- 按行看是访问能力表内容

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



自主访问控制的特点

- 特点
  - 根据主体的身份和授权来决定访问模式
- 缺点
  - 信息在移动过程中其访问权限关系会被改变
  - 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**



强制访问控制

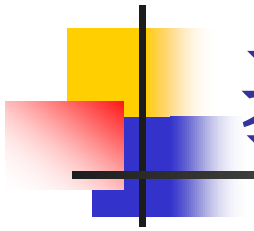
- 主体和客体都被赋予一定的安全级别，如，绝密级，机密级，秘密级，无密级
  - 用户不能改变自身和客体的安全级别，只有管理员才能够确定用户和组的访问权限
- 根据主体和客体的级别标记来决定访问模式
  - 在实施访问控制时，系统先对访问主体和受控客体的安全级别属性进行比较，再决定访问主体能否访问该客体
- 强制访问控制是指
  - 系统对用户所创建的对象进行统一的强制性控制，按照确定的规则决定哪些用户可以对哪些对象进行哪些操作类型的访问
  - 即使是创建者用户，在创建一个对象后．也可能无权访问该对象

强制访问控制模型的应用

- 下读/上写策略
  - 低级用户和进程不能访问安全级别比他们高的信息资源 -无上读
  - 安全级别高的用户和进程也不能向比他安全级别低的用户和进程写入数据 -无下写
  - 保障信息机密性
- 上读/下写策略
  - 用户只能向比自己安全级别低的客体写入信息，从而防止非法用户创建安全级别高的客体信息，避免越权、篡改等行为的产生
  - 完整性级别高的文件是一定由完整性高的进程所产生的，从而保证了完整性级别高的文件不会被完整性低的文件或完整性低的进程中的信息所覆盖
  - 保障信息完整性

自主/强制访问的问题

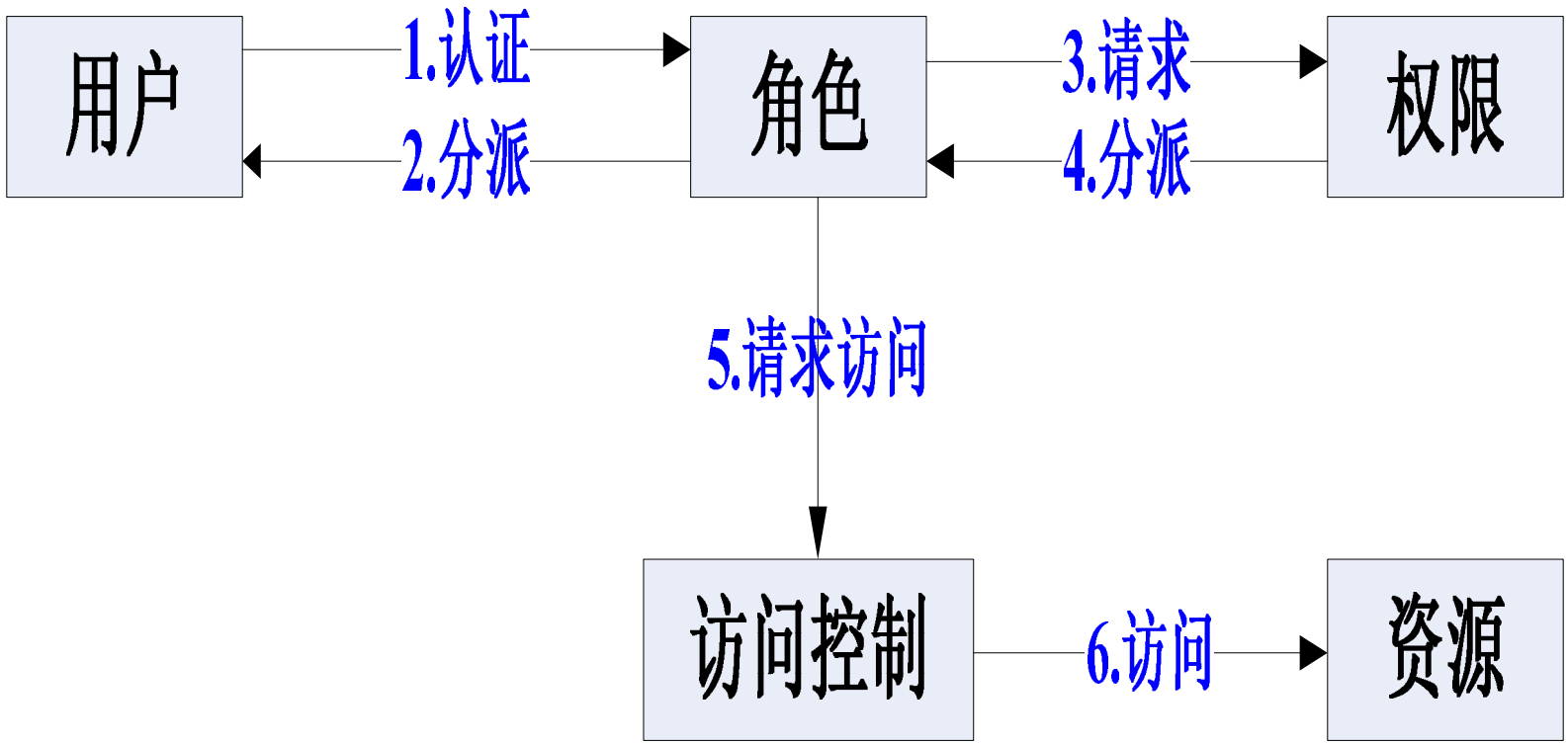
- 自主访问控制
  - 配置的粒度小
  - 配置的工作量大，效率低
- 强制访问控制
  - 配置的粒度大
  - 缺乏灵活性
- 例：1000主体访问10000客体须1000万次配置，如每次配置需1秒，每天工作8小时，就需10,000,000/ 3600*8 =347.2天。



基于角色的访问控制（RBAC）

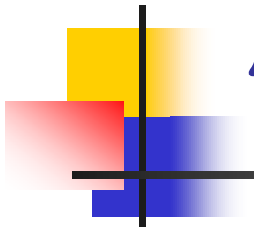
- 根据分配给主体的角色来管理访问和权限的处理过程。
  - 角色是与一个特定活动相关联的一组动作和责任。
  - 系统中主体担任角色，完成角色规定的责任，具有角色拥有的权利。
  - 一个主体可以同时担任多个角色，它的权限就是多个角色权限的总和。
  - 基于角色的访问控制就是通过各种角色的不同搭配授权来尽可能实现主体的最小权限。
  - 系统的访问控制机制只看到角色，而看不到用户。

RBAC实现过程



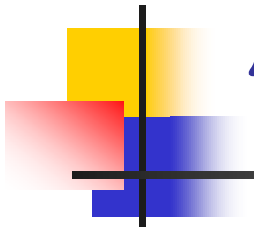
基于角色访问控制的特点

- 提供灵活的授权管理途径。
  - 改变客体的访问权限
  - 改变角色的访问权限
  - 改变主体所担任的角色
- 灵活、高效的授权管理。
  - 企业的组织结构或系统的安全需求有变化，系统管理员只变更角色权限即可。
- 角色的关系可以实现层次化，便于管理。
- 主体与客体无直接联系
  - 角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，主体只有通过角色才享有的权限，从而访问相应的客体。



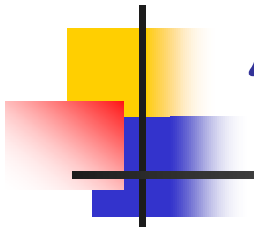
审计

- 审计：根据一定的策略，通过记录、分析历史操作事件发现和改进系统性能和安全
- 审计的需求
  - 几乎所有的安全事件的查处和追踪依赖系统历史事件记录
  - 系统资源的改善需要历史经验数据
- 审计是对访问控制的必要补充，是访问控制的一个重要内容，审计是实现系统安全的防线之一



审计的作用

- 对潜在的攻击者起到震摄或警告。
- 对于已经发生的系统破坏行为提供有效的追究证据。
- 为系统管理员提供有价值的系统使用日志从而及时发现系统入侵行为或潜在的系统漏洞。
- 提供信息有助于数据恢复。

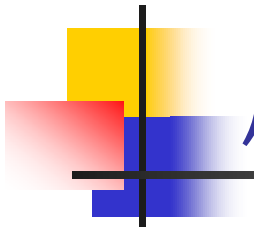


审计过程

- 审计的基础在于事件记录：
  - 系统活动记录；
  - 用户活动记录；
- 收集审计事件，产生审计记录；
- 根据记录进行安全事件的分析；
- 采取处理措施；

应用举例（1）

- 确定记录事件类型：
  - 登录及注销；
  - 文件及对象访问；
  - 用户权力的使用，用户及组管理；
  - 安全性规则更改；
  - 重新启动关机及系统；
  - 进程追踪等



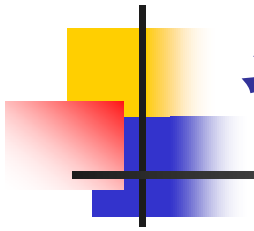
应用举例（2）

- 确定记录事件内容：
  - 时间；
  - 来源；
  - 状态（成功、失败）；
  - 类型；
  - 用户；
  - 对象等

应用举例（3）

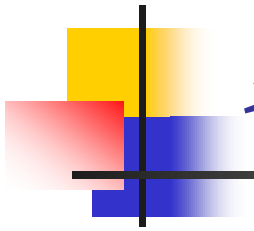
- Windows日志文件
  （ %SystemRoot%\System32\config\ ）：
  - AppEvent.evt（应用程序）
  - SecEvent.evt（安全性）
  - SysEvent.evt（系统）

  %SystemRoot%\System32\winevt\Logs\
  - *.evtx
- 控制面板/管理工具/计算机管理/事件查看器



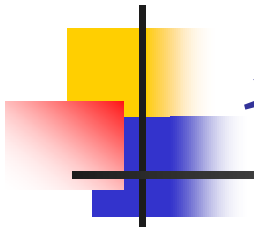
备份

- 备份的原因
  - 灾难事故，如火灾、地震、洪水等重大意外事故；
  - 系统故障，包括软硬件故障；
  - 误操作或病毒等引起的故障；
  - 人为的破坏，例如，黑客、恶意员工等的破坏。
  - 勒索 **TeslaCrypt**



备份的理解

- 备份是系统不可缺少的部分；
- 备份需要代价的，有时影响系统正常运行；
- 备份贵在坚持，尤其系统一直稳定运行时，一旦出现故障，备份能使损失降到最少；
- 备份是为恢复做准备；
- 备份要有专人负责；
- 备份计划依赖备份策略，备份策略依赖系统的功能；

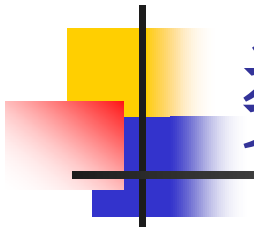


备份策略（1）

- 备份的范围是多少？
  - 数据、应用程序、操作系统、硬件设备（双机热备份）等
- 备份执行的频率是多少？
  - 自动还是手工，一般选择系统最闲时
- 执行备份的过程是怎样的？
- 谁将负责生成正确的备份？
  - 由专人或小组负责、检查、管理。

备份策略（2）

- 备份储存在哪里？
  - 切忌存放在同一物理设备上，同时要求防窃、防磁、防火、防泄密，异地。
- 备份需要维护多长时间？
  - 考虑介质老化和兼容问题。
- 需要维护多少份副本？
  - 多种方式存储，提高备份数据的安全性。

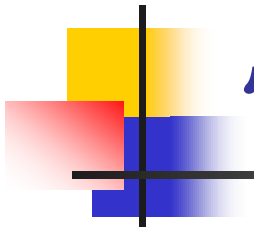


数据备份类型

- 完全备份
  - 所有数据被复制到存储介质中。
- 差量备份
  - 只有从上一次完全备份之后改变的数据才需要完整地存储。
- 增量备份
  - 仅仅复制那些在最后一次完全备份或增量备份之后改变的数据。

不同数据备份类型对比

	完全备份	差量备份	增量备份
存储空间	大	中等	小
消耗时间	长	中等	短
执行频率	长	中等	短
恢复过程	简单	简单	复杂



恢复

- 称为重载或重入，是指当磁盘损坏或系统崩溃时，通过转储或卸载的备份重新安装数据或系统的过程。
- 恢复技术依赖于备份技术；

4.4 常见操作系统的安全配置

Windows NT系统的安全基础概念

- **Windows NT**的安全机制是建立在对象的基础之上，因而对象的概念在整个与安全相关的主题中，都占有相当重要的地位。
- 对象是构成**Windows NT**操作系统的基本元素，对象可以是文件、目录、存储器、驱动器、系统程序或**Windows**桌面等。
- 对象为**Windows NT**操作系统提供了较高的安全级。对外来者，它们的数据封装在对象中，并只按对象的功能所定义的方式提供数据。对所有对象的操作都必须事先得到授权并由操作系统来执行。这就建立起一个保护层，可以有效地防止外部程序直接访问网络数据。**Windows NT**正是通过阻止程序直接访问对象来获得高安全级。

Windows NT

- 在Windows NT中，对象的属性可以用安全描述器和存储标识来设定和保护。设定的属性包括以下几个方面：

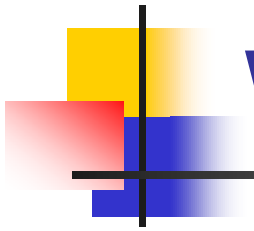
(1) 指明谁是对象的所有者和使用者的安全身份号(SID)。

(2) 只能被可移植操作系统界面(POSIX)子系统使用的组安全身份号(SID)。

(3) 包含用户和组访问许可权限的可自由决定的访问控制列表，此列表由对象所有者控制。

(4) 控制审核信息生成的系统访问控制列表(ACL)。

共有两种形式的对象，即集装箱式的对象和非集装箱式的对象。集装箱式的对象可以容纳别的对象，而非集装箱式的对象则不能容纳别的对象。例如，目录是集装箱式的对象，而文件则是非集装箱式的对象。在父集装箱式对象中所生成的子对象，可以拥有父集装箱式对象所有的许可权限。



Windows NT

- 域

  域是指共享公共账号数据库和数据安全策略的计算机的逻辑组合，提供登录验证，并只有惟一的域名。

- 用户账户与组

  任何一个用户想要登录到**Windows NT**服务器上，就必须要拥有一个属于自己的用户账户。

  将做相同工作或需要同一资源的用户分为全局组和本地组，分组使得授予权限和资源许可权更为方便，只需将权限和资源许可权授予一个组，就等于将权限或许可权授予了现在和未来的组成员

Windows NT

组分为全局组和本地组。

① 全局组： 一个全局组是能在自己的域以及其他信任这个域的域中被赋予权限和许可权的用户的集合。全局组只能包含用户账户，不能包含其他的全局组或本地组。当全局组创建后，它就全局有效。一个全局组是由来自一个域的一些用户账户组织在一起并给一个组名。全局组只能包含来自创建全局组的域的用户账户。当全局组创建以后，它就全局有效。它能在自己的域中被授予权限和许可权。

② 本地组： 本地组是一些组织在一个组名下的来自一个或多个域的用户和全局组的集合。因为一个域的本地组可以包括该域或信任该域的域的用户和全局组，所以可以授予本地组对其所在域的资源的

Windows NT

- 权限和许可权。该组的使用只限于所在的域。本地组可以包括用户和全局组，但不能包含其他本地组。作为成员服务器或工作站的本地组成员具有在这台计算机上执行各种任务的权力和能力。
- 域的全局组只能包含域的用户，而域的本地组可以包含域的用户和全局组。
- 本地组有**Administrators**组、**Power User**组、**User**组、**Guests**组、**Everyone**组、**Backup Operators**组等。见计算机管理

Windows NT

- **Administrators组：** 在域或计算机上的**Administrators**本地组中的账户有能力做域或计算机上可做的任何事情，包括创建、修改、删除和管理用户账户、全局组、本地组、设置文件所有权、备份文件目录、共享和停止共享目录、共享和停止共享打印机等。
- **Power User组：** 属于本组的成员可以从本地登录、从网络访问计算机、关闭系统、创建和管理用户账户(只能修改和删除他自己所创建的账户)和本地组(但不能修改**Administrators**组和**Backup Operators**组)、共享和停止共享目录、共享和停止共享打印机等。
- **User组：** 属于本组的成员可以在工作站上登录并用它访问网络资源、锁定和关闭工作站、拥有一个在工作站上的用户配置文件、修改他所创建的本地组的成员(但不能修改内嵌的或其他人创建的本地组)。

Windows NT

- **Guests组：** 在运行**Windows NT Server**的域控制器上，**Guests**组的成员拥有和**User**组成员一样的权限，两个组都只能通过网络访问域控制器，而不能在域控制器上本地登录。在运行**Windows NT Workstation**的计算机上工作时，**Guests**的权限比**User**的要小，**Guests**不能保持本地的用户配置文件、锁定工作站以及创建、删除和修改工作站上的本地组。
- **Everyone组：** 包含所有用户的组。**(XP**以后已取消**)**
- **Backup Operators组：** 属于本组的成员能备份文件、恢复文件、本地登录以及关闭计算机。

Windows NT

内嵌账户

当NT安装后，默认的用户和组账户已输入到计算机的账户数据库中。两个默认的用户账户初始化在每个NT计算机上：Administrator和Guest。

- Administrator： 在用户创建其他用户账户之前，Administrator是最先能使用的管理新服务器和工作站的账户，不能删除或使之失效，这保证用户永远不能通过删除或使管理账户无效而锁定自己，可以改名。
- Guest： 是用作Guest登录的账户，它可被那些在计算机或域中没有账户的人用来登录的。在NT安装时，Guest账户被默认的置为无效，但若要允许Guest登录，可使之有效。但Guest在域中的权限非常小，几乎不能完成某项具体的工作。

Windows NT

内嵌全局组

- 在域的主域和备份域控制中，有3个内嵌的全局组：**Domain Admins**、**Domain Users**和**Domain Guests**，它们都不能被删除。

① **Domain Admins**： 初始化时包含**Administrator**账户。当为域管理员创建账户时，创建者应该将这些管理员账户放入**Domain Admins** 全局组，而不是放在**Administrator**本地组中。

② **Domain Users** ： 初始化时包含**Administrator**账户，每个域管理员后来加入到该域的账户均被自动放到**Domain Users**全局组中。

③ **Domain Guests** ： 初始化时包含**Guest**账户。

用户帐户控制

- 用户帐户控制 (UAC) 是一种新的安全组件，使用户可以用非管理员身份（在此版本的 Windows 中称为“标准用户”）以及管理员身份执行常见任务，而无需切换用户、注销或使用“以管理员身份运行”命令。
- 当管理员登录到运行Vista以后的Windows 的计算机时，将为该用户分配两个单独的访问令牌（标准用户和管理员）。Windows 使用访问令牌（包含用户的组成员身份、授权数据和访问控制数据）控制用户可以访问的资源和任务。
- 在一些先前版本的 Windows（如 Windows XP）中，管理员帐户只有一个访问令牌，其中包含的数据可授予该用户访问所有 Windows 资源的权限。此访问控制模型不包含任何故障保险检查，恶意软件可以将其自身安装在计算机上，而不会通知用户。此过程通常称为“无提示”安装。因为用户是管理员，所以恶意软件可以使用管理员的访问控制数据感染核心操作系统文件。在某些情况下，恶意软件可能会变得几乎不可能被删除，而且可能会造成更多破坏。
- Vista以后的Windows版本中，标准用户和管理员之间的主要区别在于他们对计算机有多少控制权。管理员可以更改系统状态、关闭防火墙、关闭策略、安装影响计算机上每个用户的服务或驱动程序等等。管理员可以为整台计算机安装软件。标准用户无法以这种方式更改系统状态。

IE 保护模式（protected mode）

- UIPI（User Interface Privilege Isolation）（用户界面特权隔离）只允许高级进程给平级或者低级的进程发送消息。IE缺省运行级别比较低，若IE加载项需要给外部进程发送Windows消息，就会被阻止，从而导致部分程序无法正常工作。无法输入文字或窗口无法滚动，拖放失效等。
- 解决方法：

  依次点击开始-->>>搜索框里输入regedit 打开注册表，并找到以下路径：

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableUIPI

  将该值设置为0以禁用UIPI

  将该值设置为1或删除以启用UIPI

- 在IE9中，微软进一步提高了浏览器的安全级别，可以管理员身份运行IE突破用户界面特权隔离，或禁用UAC

注册表与组策略编辑器

- 注册表（Registry）是Microsoft Windows中的一个重要的数据库，包括了应用程序、系统设置、硬件设备、设备驱动程序配置、网络协议设置等各种信息。具有容错功能，一般不会崩溃。如果系统出现错误，Windows NT可使用日志文件恢复和修改数据库，以保证系统正常运行。
- 早在Windows 3.0推出OLE技术的时候，注册表就已经出现。随后推出的Windows NT是第一个从系统级别广泛使用注册表的操作系统。Windows 95推出后，注册表成为Windows用户经常接触的内容，并在其后的操作系统中沿用至今。
- 注册表替代了微软早期操作系统中config.sys，autoexec.bat，system.ini，win.ini，protocol.ini，lanman.ini，control.ini等文件的作用，目前通过控制面板进行的设置，相应值基本都保存在注册表中。
- 虽然多个 Windows 操作系统都有注册表，但这些操作系统的注册表存在一些差异。

注册表

- 注册表配置单元是注册表中的一组项、子项和值，它有一组包含其数据备份的支持文件。所有Windows NT架构的配置单元（HKEY_CURRENT_USER 除外）的支持文件都位于 %SystemRoot%\System32\Config 文件夹中。HKEY_CURRENT_USER 的支持文件位于 %SystemRoot%\Profiles\Username 文件夹中。

注册表文件：

- Sam -（Security Account Manager安全账户管理器）注册表文件，主要存放账户密码信息。
- Default - 默认的注册表文件
- Security - 安全性注册表文件
- System - 系统注册表文件
- Software - 应用软件注册表文件
- Components - 系统组件注册表文件
- 注册表文件都是没有扩展名的，而其他扩展名为.log、.log1、.log2的，都是注册表的日志文件，在“RegBack”目录下的是备份的注册表文件。和XP相比，Windows 7注册表增加了Components文件。

注册表

- 注册表的数据结构由以下5个子树构成：

① **HKEY_LOCAL_MACHINE**：包含特定于计算机的配置信息（用于任何用户）。此项有时缩写为“**HKLM**”。这些信息包括硬件设置、操作系统设置、启动控制数据和驱动器的驱动程序。

② **HKEY_CLASS_ROOT**：是 **HKEY_LOCAL_MACHINE\Software** 的子项。存储在这里的信息可确保使用 **Windows** 资源管理器打开文件时能打开正确的程序。此项有时缩写为“**HKCR**”。从 **Windows 2000** 开始，这些信息同时存储在 **HKEY_LOCAL_MACHINE** 和 **HKEY_CURRENT_USER** 项下。**HKEY_LOCAL_MACHINE\Software\Classes** 项包含可应用于本地计算机上的所有用户的默认设置。**HKEY_CURRENT_USER\Software\Classes** 项包含覆盖默认设置并且只应用于交互用户的设置。**HKEY_CLASSES_ROOT** 项提供合并上述两个来源的信息的注册表视图。

③ **HKEY_CURRENT_USER**：包含当前登录的用户的配置信息的根目录。该用户的文件夹、屏幕颜色和“控制面板”设置都存储在这里。这些信息与用户的配置文件相关联。此项有时缩写为“**HKCU**”。

④ **HKEY_USER**：包含计算机上的所有以活动方式加载的用户配置文件。**HKEY_CURRENT_USER** 是 **HKEY_USERS** 的子项。**HKEY_USERS** 有时缩写为“**HKU**”。

⑤ **HKEY_CURRENT_CONFIG**：包含有关本地计算机在系统启动时使用的硬件配置文件的信息。

编辑注册表

- 注册表编辑器（Regedit.exe 或 Regedt32.exe），命令行reg.exe,，第三方Registry Workshop
- 组策略gpedit.msc、系统策略（NT4 98 Me）poledit.exe
- 注册表 (.reg) 文件
- 编程或通过运行脚本（例如，VisualBasic 脚本文件）

操作：

- 查找子树、项、子项或值
- 添加子项或值
- 更改值
- 删除子项或值
- 重命名子项或值

https://support.microsoft.com/zh-cn/kb/256986

Linux安全策略配置

一、磁盘分区

1、如果是新安装系统，对磁盘分区应考虑安全性：

1）根目录（/）、用户目录（/home）、临时目录（/tmp）和/var目录应分开到不同的磁盘分区；

2）以上各目录所在分区的磁盘空间大小应充分考虑，避免因某些原因造成分区空间用完而导致系统崩溃；

2、对于/tmp和/var目录所在分区，大多数情况下不需要有suid属性的程序，所以应为这些分区添加nosuid属性；

方法一：修改/etc/fstab文件，添加nosuid属性字。例如：

/dev/hda2 /tmp ext2 exec,dev,nosuid,rw 0 0

方法二：通过linuxconf等程序来修改。

二、软件包安装

1、对于非测试主机，不应安装过多的软件包。这样可以降低因软件包而导致出现安全漏洞的可能性。

2、对于非测试主机，在选择主机启动服务时不应选择非必需的服务。例如routed、ftpd等。

Linux安全策略配置

三、安全配置与增强 （选择支持良好的发行版）

- 内核升级，在线更新。
- 关闭危险的网络服务。**echo、chargen、shell、login、finger、NFS、RPC**等
- 关闭非必需的网络服务。**talk、ntalk、pop-2**等
- 确保网络服务所使用版本为当前最新和最安全的版本。
- 取消匿名**FTP**访问
- 去除非必需的**suid**程序
- 使用**tcpwrapper**
- 使用**ipchains、iptables**等防火墙
- 日志系统**syslogd**
- 开启**SELinux**