

第5章 访问控制

许海燕



主要内容

5.1 概述

5.2 访问控制模型

5.2.1 自主访问控制

5.2.2 强制访问控制

5.2.3 基于角色的访问控制

5.3 Windows系统的安全管理

5.3.1 Windows系统结构

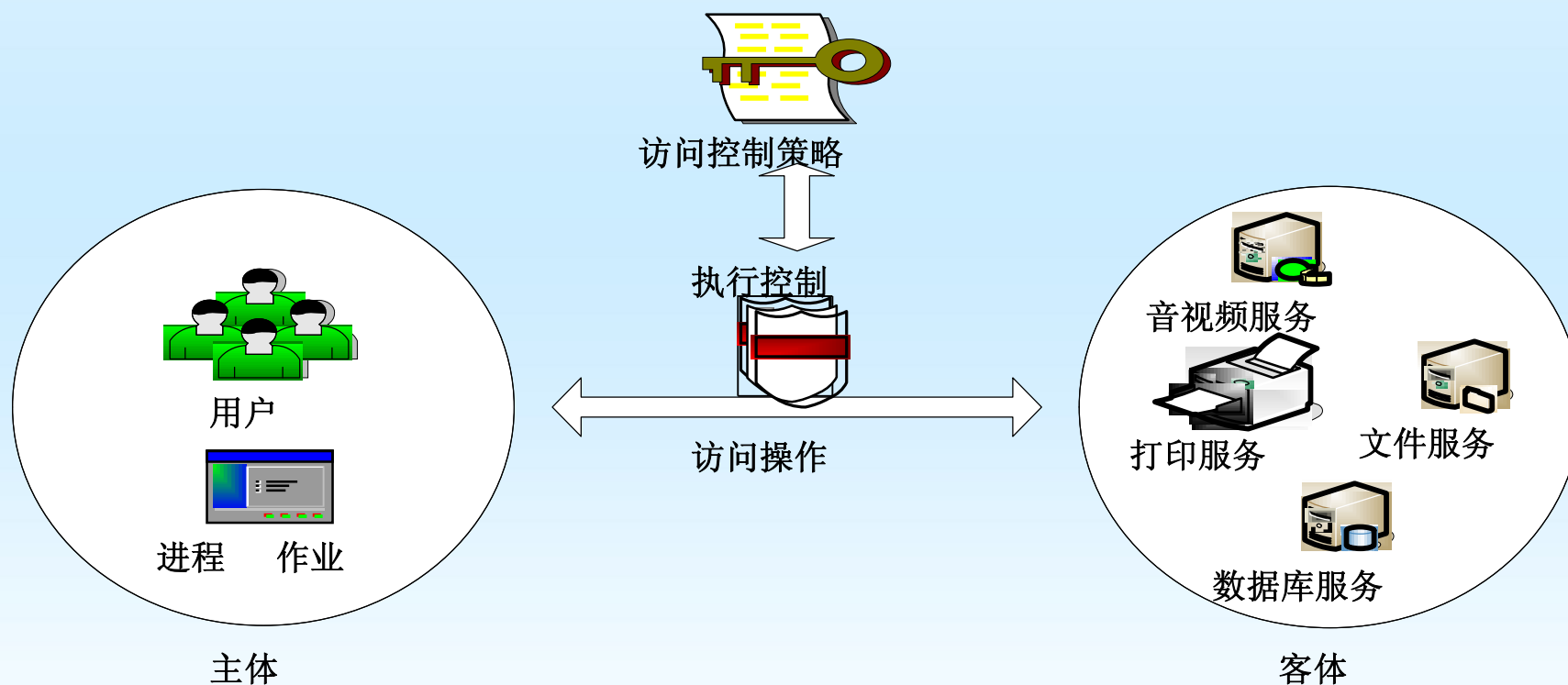
5.3.2 Windows安全体系结构

5.3.3 Windows系统的访问控制

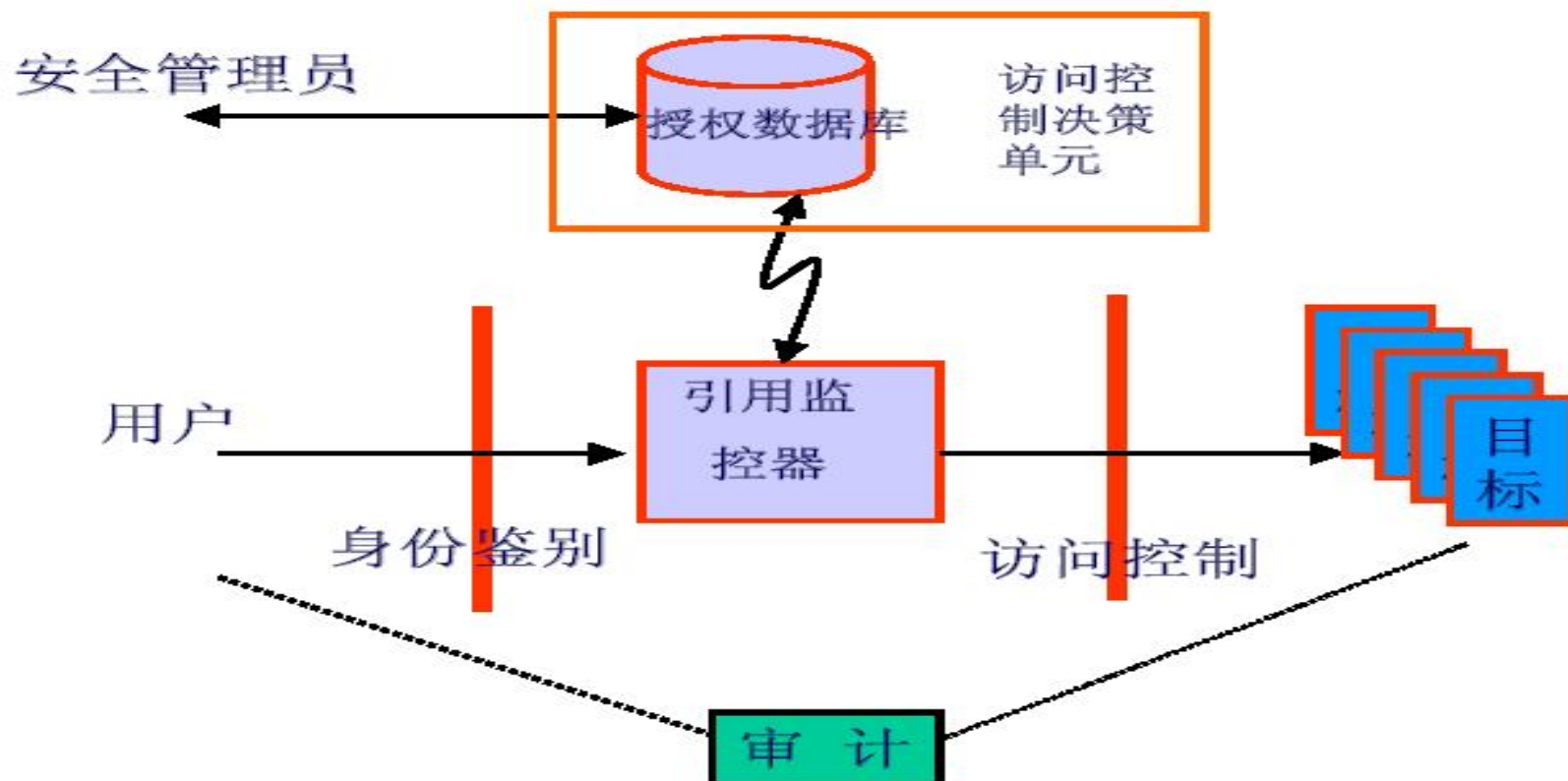
5.3.4 活动目录与组策略

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



访问控制与其他安全措施的关系



•访问控制包括三方面的内容:

- ✓ 认证: 考虑对合法用户进行验证
- ✓ 控制策略实现: 对控制策略的选用与管理, 对非法用户或是越权操作进行管理
- ✓ 审计: 对非法用户或是越权操作进行追踪



访问控制的基本组成元素

- ◆ **主体(Subject)**：是指**提出访问请求的实体**，是动作的发起者，但不一定是动作的执行者。主体可以是用户或其它代理用户行为的实体（如进程、作业和程序等）。
- ◆ **客体(Object)**：是指可以接受主体访问的被动实体。客体的内涵很广泛，凡是可以被操作的**信息、资源、对象**都可以认为是客体。
- ◆ **访问控制策略（Access Control Policy）**：是指主体对客体的**操作行为和约束条件**的关联集合。
 - 访问控制策略是主体对客体的**访问规则集合**，这个规则集合可以直接决定主体是否可以对客体实施的特定的操作。

访问控制应用类型

- ◆ 根据应用环境，访问控制应用类型可分为
 1. 物理网络，如防火墙
 2. 操作系统，如操作系统的访问控制列表
 3. 应用，如大型数据库的数据表的访问控制策略



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

5.2.1 自主访问控制

◆ 自主访问控制DAC模型

- 根据自主访问控制策略建立的一种模型
- 允许合法用户以用户或用户组的身份来访问系统控制策略许可的客体，同时阻止非授权用户访问客体，
- 某些用户还可以自主地把自己所拥有的客体的访问权限授予其它用户。

◆ UNIX、Linux以及Windows NT等操作系统都提供自主访问控制的功能。

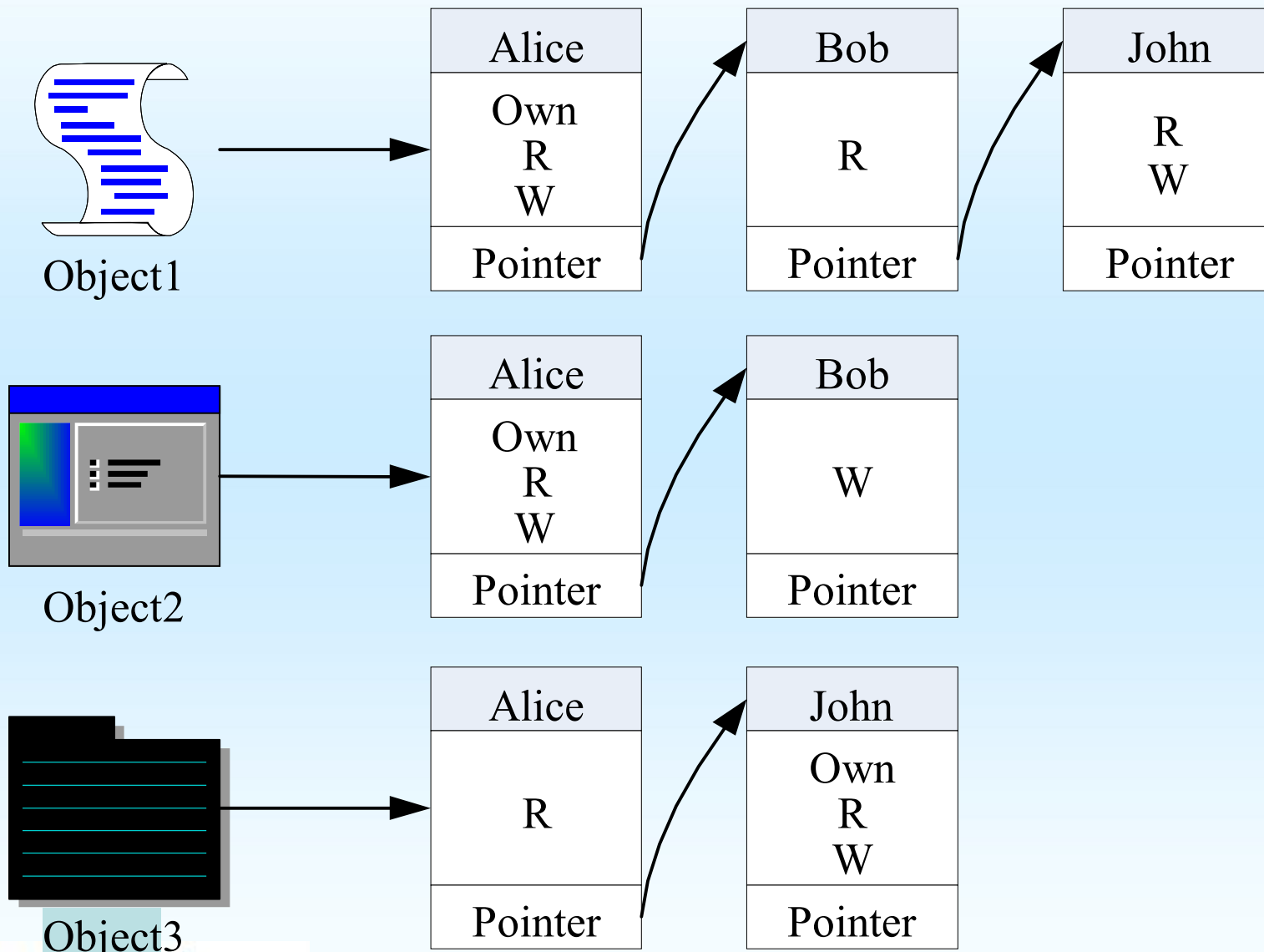


访问控制的实现方法

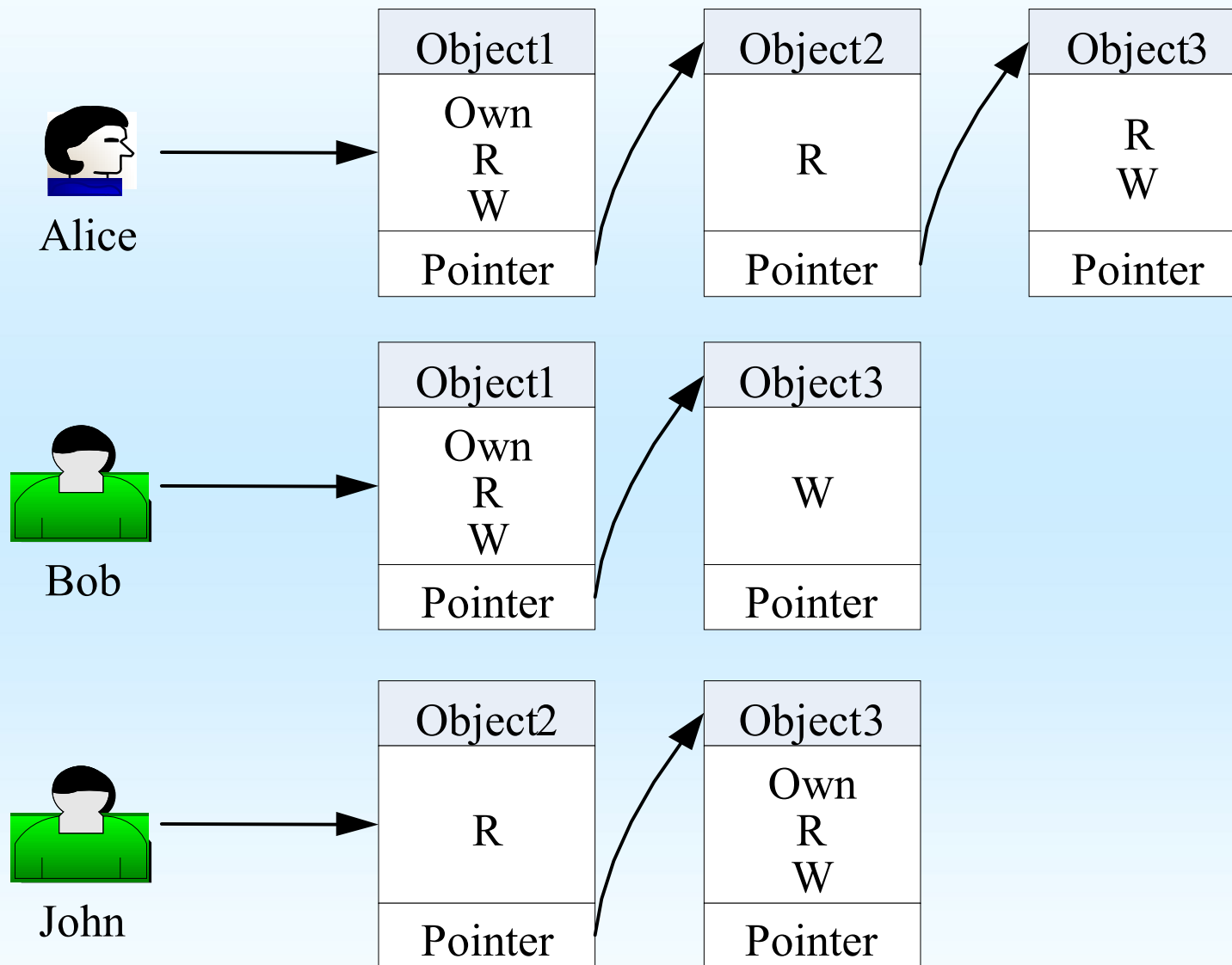
- 访问控制表ACL (Access Control Lists)
- 访问控制能力表ACCL (Access Control Capability Lists)
- 访问控制矩阵ACM (Access Control Matrix)



访问控制表ACL



访问控制能力表ACCL



访问控制矩阵ACM

主体 \ 客体	Object1	Object2	Object3
Alice	Own , R , W	R	R , W
Bob	R	Own , R , W	
John	R , W		Own , R , W



5.2.2 强制访问控制

◆ 强制访问控制MAC是一种多级访问控制策略

- 系统事先给访问主体和受控客体分配不同的安全级别属性，
- 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受控客体。

◆ MAC模型形式化描述

- 主体集S和客体集O
- 安全类 $SC(x) = \langle L, C \rangle$
 - ✓ L为有层次的安全级别Level
 - ✓ C为无层次的安全范畴Category

访问的四种形式

◆ 向下读 (RD , Read Down) :

- 主体安全级别高于客体信息资源的安全级别时 , 即 $SC(s) \geq SC(o)$, 允许读操作 ; Bell-LaPadula

◆ 向上写 (WU , Write Up) :

- $SC(s) \leq SC(o)$ 时 , 允许写操作。 Bell-LaPadula

◆ 向上读 (RU , Read Up) :

- 主体安全级别低于客体信息资源的安全级别时 , 即 $SC(s) \leq SC(o)$, 允许读操作 ; Biba

◆ 向下写 (WD , Write Down) :

- $SC(s) \geq SC(o)$ 时 , 允许写操作 ; Biba



5.2.3 基于角色的访问控制

- ◆ Group的概念，一般认为Group是具有某些相同特质的用户集合。
- ◆ 在UNIX操作系统中Group可以被看成是拥有相同访问权限的用户集合，
 - 定义用户组时会为该组赋予相应的访问权限。
 - 如果一个用户加入了该组，则该用户即具有了该用户组的访问权限
 - 角色Role的概念，可以这样理解一个角色是一个与特定工作活动相关联的行为与责任的集合



角色Role的理解

◆ 一个角色是一个与特定工作活动相关联的行为与责任的集合。

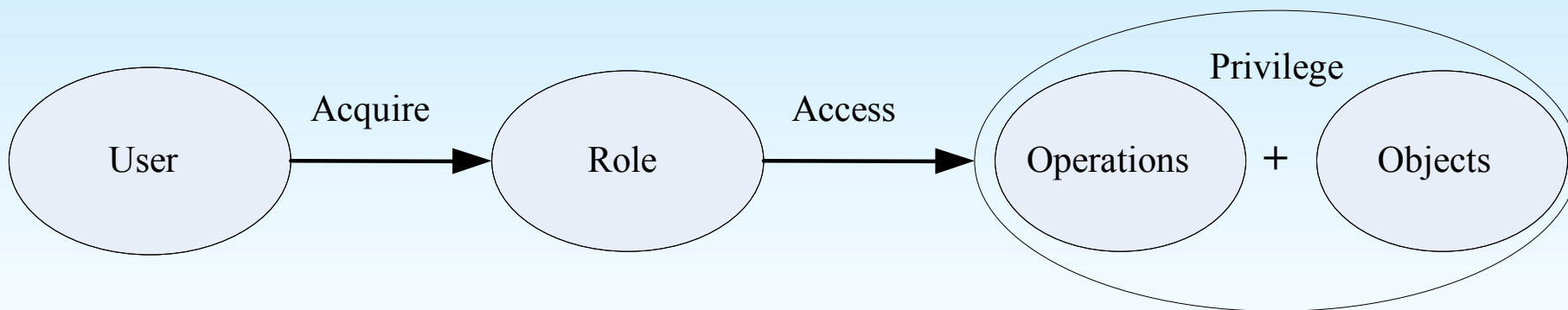
- Role不是用户的集合，也就与组Group不同。
- 当将一个角色与一个组绑定，则这个组就拥有了该角色拥有的特定工作的行为能力和责任。
- 组Group和用户User都可以看成是角色分配的单位和载体。
- 而一个角色Role可以看成具有某种能力或某些属性的主体的一个抽象。



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。



例子

- ◆ 在一个公司里，用户角色可以定义为经理、会计、出纳员和审计员，具体的权限如下：
 - 经理：允许查询公司的经营状况和财务信息，但不允许修改具体财务信息，必要时可以根据财务凭证支付或收取现金，并编制银行账和现金帐；
 - 会计：允许根据实际情况编制各种财务凭证及账簿，但不包括银行账和现金帐；
 - 出纳员：允许根据财务凭证支付或收取现金，并编制银行账和现金帐；
 - 审计员：允许查询审查公司的经营状况和财务信息，但不允许修改任何账目。



- ◆ RBAC的策略陈述易于被非技术的组织策略者理解，既具有基于身份策略的特征，也具有基于规则策略的特征。
- ◆ 在基于组或角色的访问控制中，一个用户可能不只是一个组或角色的成员，有时又可能有所限制。
- ◆ 例如经理可以充当出纳员的角色，但不能负责会计工作，即各角色之间存在相容和相斥的关系。

制定访问控制策略的三个基本原则

◆ 最小特权原则

- 指主体执行操作时，按照主体所需权利的最小化原则分配主体权力。
- 最小特权原则的优点是最大限度地限制了主体实施授权行为，可以避免来自突发事件和错误操作带来的危险。

◆ 最小泄漏原则：

- 是指主体执行任务时，按照主体所需要知道信息的最小化原则分配给主体访问权限。

◆ 多级安全策略：

- 是指主体和客体间的数据流方向必须受到安全等级的约束。多级安全策略的优点是避免敏感信息的扩散。
- 对于具有安全级别的信息资源，只有安全级别比它高的主体才能够对其访问。

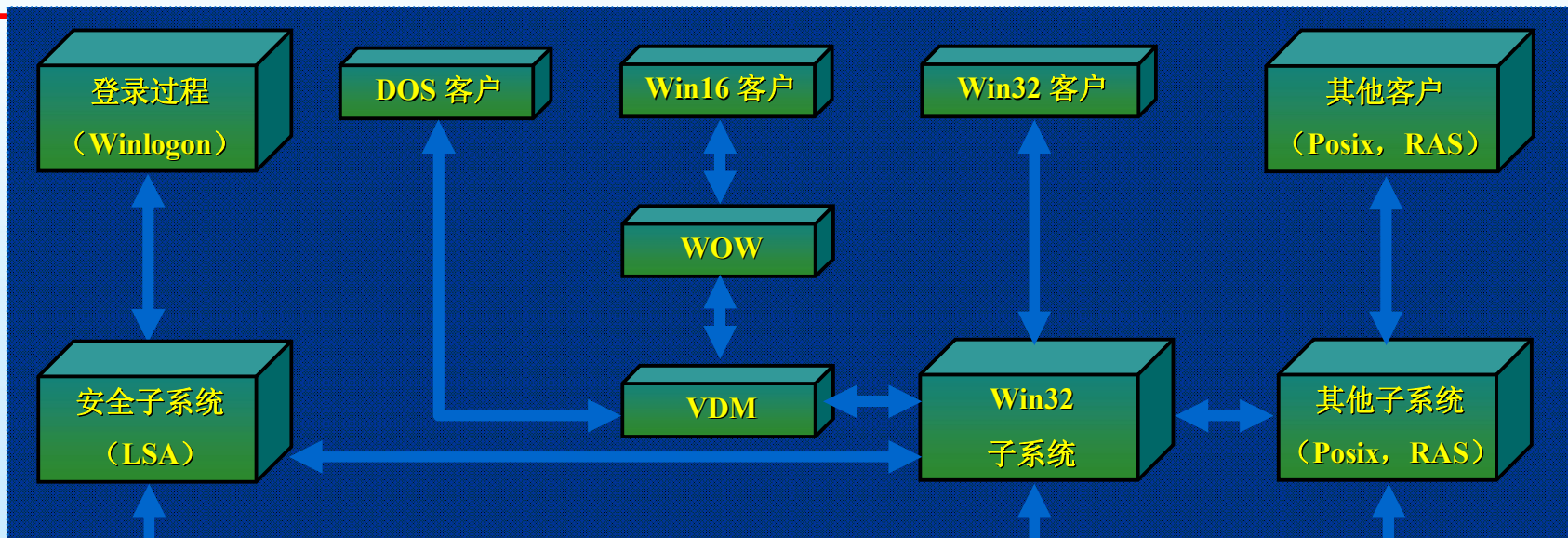


5.3 Windows系统的安全管理

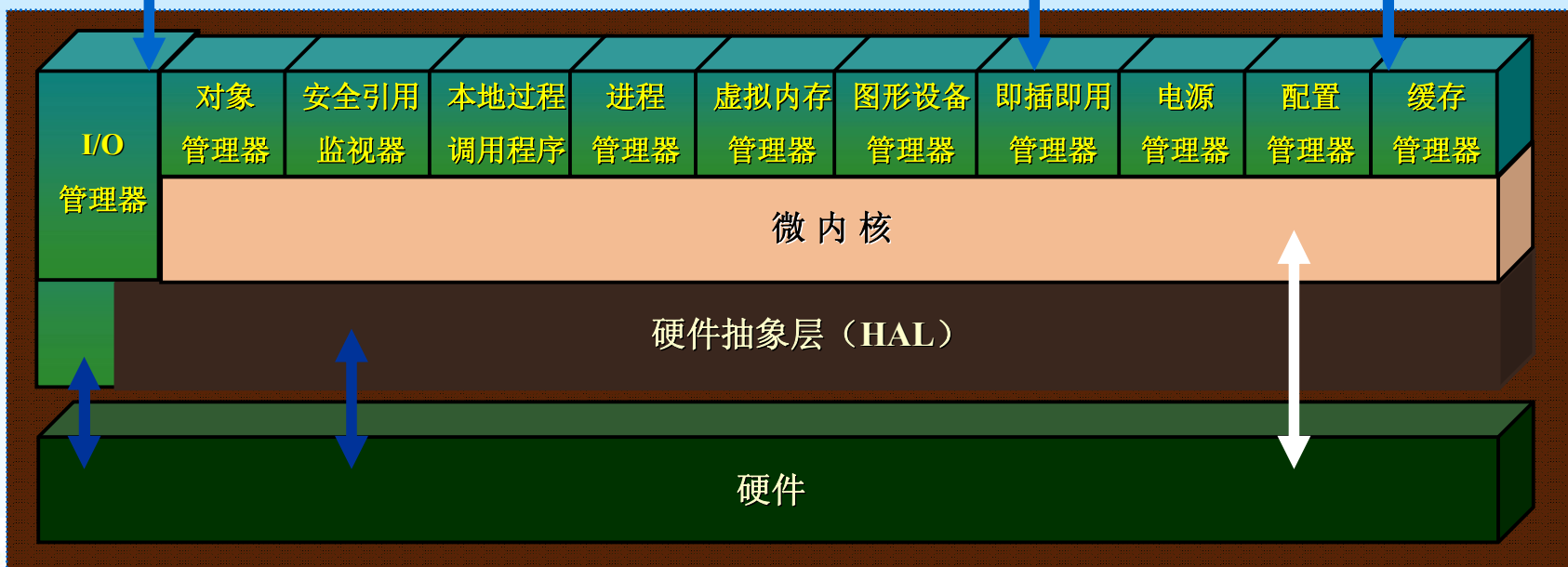


5.3.1 windows 系统结构

用户模式 (2GB | 4GB)



内核模式 (0GB | 2GB)



微内核

1. 基本功能

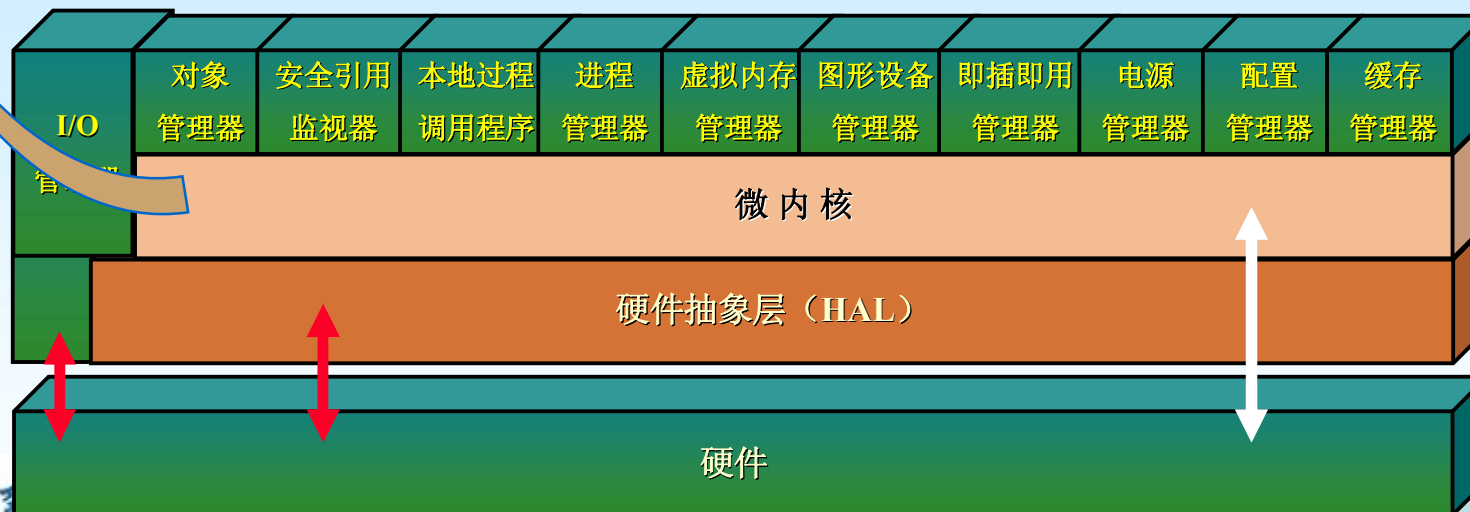
- 调度线程执行
- 在线程之间切换设备环境
- 捕获并处理中断和异常
- 对内核对象的管理
- 在处理器之间负责同步（在多处理器系统中）

2. 内核进程的特性

- 内核的执行除了中断服务例程(ISR)外，不会被其他线程所抢先
- 内核的大部分代码和数据不会被调页到物理RAM之外

3. 内核和执行体（对象管理器、内存管理等统称为执行体）的关系：

- 两者都在文件C:\WINNT\SYSTEM32\NTOSKRNL.EXE中实现
- 执行体具有相对较高的级别
- 内核不能从用户模式调用，其功能是通过执行体来从用户模式下访问的

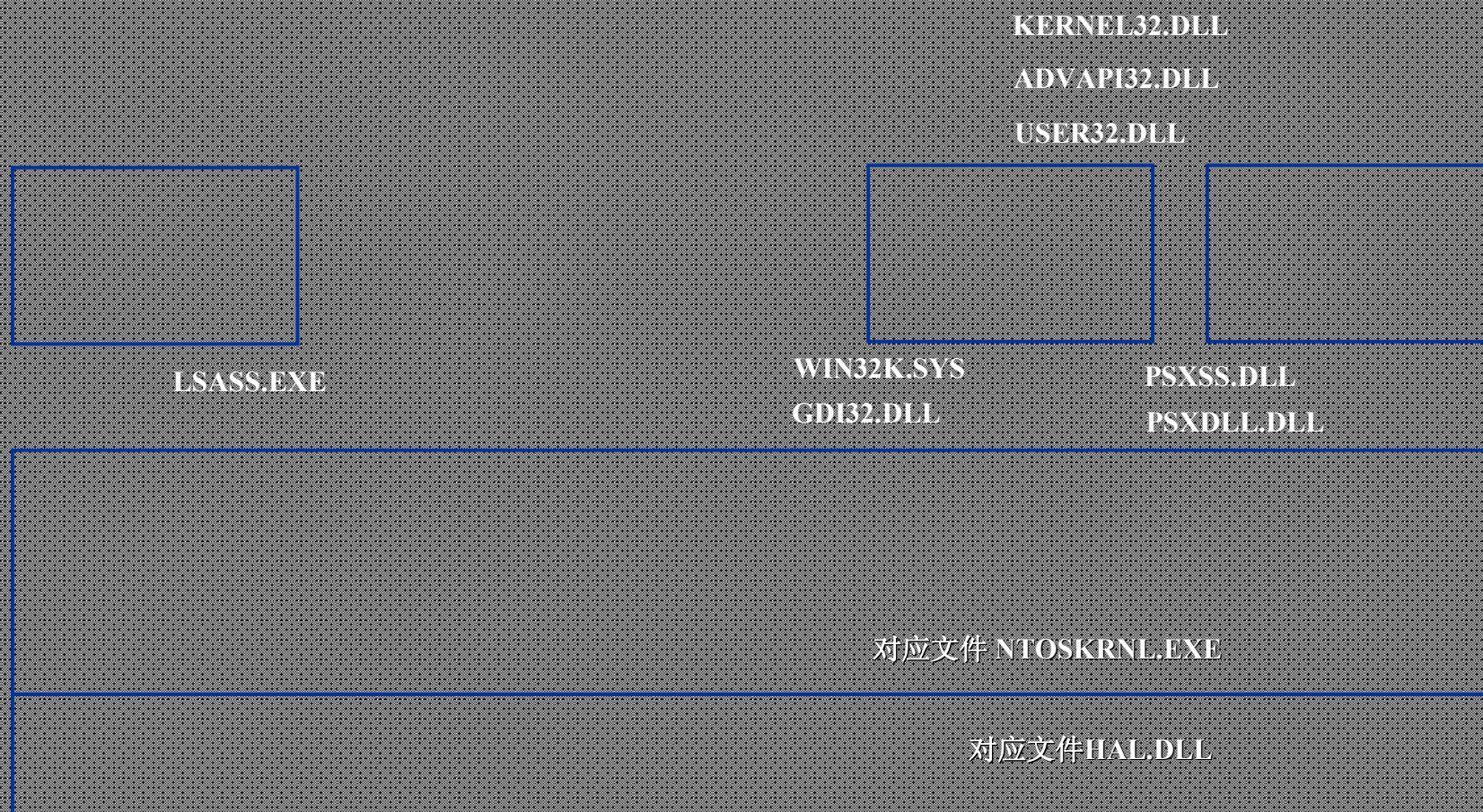


Windows重要的系统文件

名称	模块所实现的位置	模式	何时被启动/被加载	由谁启动
HAL.DLL	硬件抽象层	N/A	系统启动时	SYSTEM
NTOSKRNL.EXE	内核和执行体	内核	系统启动时	SYSTEM
KERNEL32.DLL	WIN32子系统.DLL	N/A	系统启动时	SYSTEM
GDI32.DLL	WIN32子系统.DLL	N/A	系统启动时	SYSTEM
USER32.DLL	WIN32子系统.DLL	N/A	系统启动时	SYSTEM
ADVAPI32.DLL	WIN32子系统.DLL	N/A	系统启动时	SYSTEM
SMSS.EXE	会话管理器	用户	系统启动时	SYSTEM
WIN32K.SYS	WIN32的内核模式部分	内核	系统启动时	SMSS.EXE
CSRSS.EXE	用户模式进程	用户	系统启动时	SMSS.EXE
WINLOGON.EXE	Windows登录进程	用户	系统启动时	SMSS.EXE
LSASS.EXE	本地安全性鉴别子系统	用户	系统启动时	WINLOGON.EXE
MSGINA.DLL	缺省GINA	N/A	系统启动时	WINLOGON.EXE
SERVICES.EXE	服务控制器	用户	系统启动时	WINLOGON.EXE
NTDLL.DLL	支持函数和到执行体的接口	N/A	系统启动时	SMSS.EXE
OS2SS.EXE	OS/2子系统进程	用户	根据需要	SMSS.EXE
PSXDLL.DLL	POSIX子系统.DLL	N/A	根据需要	SMSS.EXE
PSXSS.DLL	POSIX子系统进程	用户	根据需要	SMSS.EXE



Windows 子系统与文件的对应关系



WINDOWS 2000 的运行模式

- ◆ Intel x86处理器支持4种运行模式，或称计算环(ring)
 - Ring 0：最高优先级
 - Ring 1：
 - Ring 2:
 - Ring 3：最低优先级
- ◆ Win2K仅使用两种运行模式
 - Ring 0：内核模式
 - ✓ 所有内核模式进程共享一个地址空间
 - Ring 3：用户模式
 - ✓ 每个用户模式进程拥有自己私有的虚拟内存空间

Windows 的系统服务介绍

单击“开始” ----- 指向“设置” ----- 然后单击“控制面板” ----- 双击“管理工具” ----- 然后双击“服务”：在列表框中显示的是系统可以使用的服务。

Windows下可以在命令行中输入**services.msc**打开服务列表。

文件(F) 操作(A) 查看(V) 帮助(H)

← →

服务(本地)

名称	描述	状态	启动类型	登录为
Alerter	通知所选用户和计算机有关系统管理级警报。如果服务停止，使用管理警报的程序将不会...		手动	本地服务
Application Lay...	为 Internet 连接共享和 Internet 连接防火墙提供第三方协议插件的支持	已启动	手动	本地服务
Application Man...	提供软件安装服务，诸如分派，发行以及删除。		手动	本地系统
Automatic Updates	从 Windows Update 启用重要的 Windows 更新的下载和安装。如果禁用该服务，操作系...	已启动	自动	本地系统
Background Inte...	使用空闲的网络带宽传输数据。		手动	本地系统
ClipBook	启用“剪贴簿查看器”储存信息并与远程计算机共享。如果此服务终止，“剪贴簿查看器...		手动	本地系统
COM+ Event System	支持系统事件通知服务 (SENS)，此服务为订阅组件对象模型 (COM) 组件事件提供自动分布...	已启动	手动	本地系统
COM+ System App...	管理 基于COM+ 组件的配置和跟踪。如果服务停止，大多数基于 COM+ 组件将不能正常工...		手动	本地系统
Computer Browser	维护网络上计算机的更新列表，并将列表提供给计算机指定浏览。如果服务停止，列表不...	已启动	自动	本地系统
Cryptographic S...	提供三种管理服务：编录数据库服务，它确定 Windows 文件的签字；受保护的根服务，...	已启动	自动	本地系统
DHCP Client	通过注册和更改 IP 地址以及 DNS 名称来管理网络配置。	已启动	自动	本地系统
Distributed Lin...	在计算机内 NTFS 文件之间保持链接或在网络域中的计算机之间保持链接。	已启动	自动	本地系统
Distributed Tra...	协调跨多个数据库、消息队列、文件系统等资源管理器的事务。如果停止此服务，则不会...		手动	网络服务
DNS Client	为此计算机解析和缓冲域名系统 (DNS) 名称。如果此服务被停止，计算机将不能解析 DN...	已启动	自动	网络服务
Error Reporting...	服务和应用程序在非标准环境下运行时允许错误报告。	已启动	自动	本地系统
Event Log	启用在事件查看器查看基于 Windows 的程序和组件颁发的事件日志消息。无法终止此服务。	已启动	自动	本地系统
Fast User Switc...	为在多用户下需要协助的应用程序提供管理。	已启动	手动	本地系统
Help and Support	启用在此计算机上运行帮助和支持中心。如果停止服务，帮助和支持中心将不可用。如果...	已启动	自动	本地系统
Human Interface...	启用对智能界面设备 (HID) 的通用输入访问，它激活并保存键盘、远程控制和其它多媒体...		已禁用	本地系统
IMAPI CD-Burnin...	用 Image Mastering Applications Programming Interface (IMAPI) 管理 CD 录制。如...		手动	本地系统
Indexing Service	本地和远程计算机上文件的索引内容和属性；通过灵活查询语言提供文件快速访问。		手动	本地系统
Internet Connec...	为家庭或小型办公网络提供网络地址转换，定址以及名称解析和/或防止入侵服务。	已启动	自动	本地系统
IPSEC Services	管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序。	已启动	自动	本地系统

Windows 基本的系统进程

➤基本的系统进程:

1. smss.exe Session Manager
2. csrss.exe 子系统服务器进程
3. winlogon.exe 管理用户登录
4. services.exe 包含很多系统服务
5. lsass.exe 管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序。(系统服务)
6. svchost.exe 包含很多系统服务
7. spoolsv.exe 将文件加载到内存中以便迟后打印。(系统服务)
8. explorer.exe 资源管理器
9. internat.exe 输入法



Windows主要系统进程详细介绍

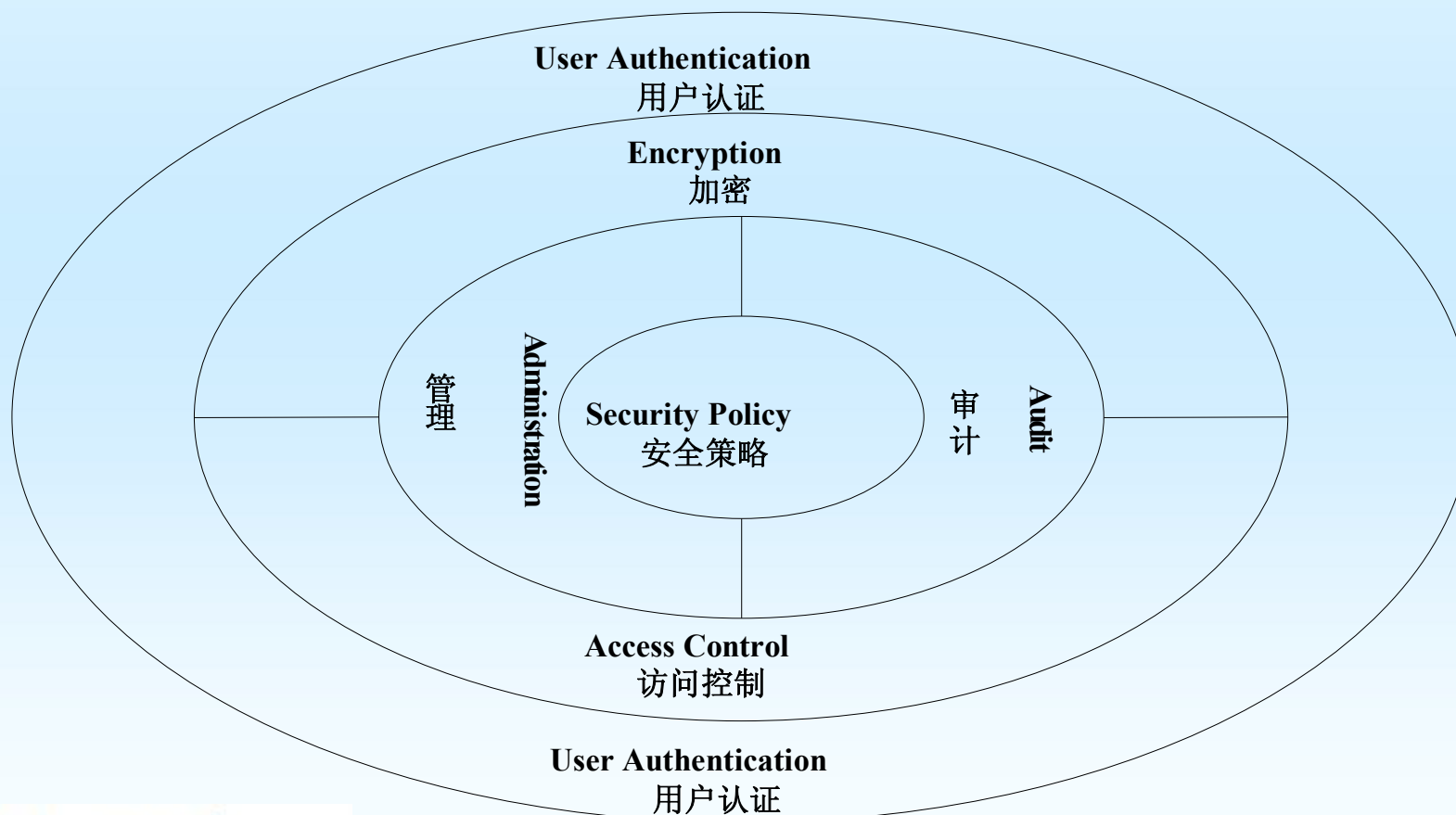
1. 会话管理器(SMSS.EXE):
 - a. Win2K在启动过程中第一个启动的用户模式进程
 - b. 优先的用户模式进程
 - c. 进程实现的主要功能
 - a. 关闭系统
 - b. 改变系统时间
 - c. 绕过文件访问权限/审核来执行备份
 - d. 加载/卸载设备驱动程序
 - e. 调整页面文件
 - f. 连接调试器到某个进程
2. WINLOGON (.EXE)
3. 本地安全性鉴别子系统(LSASS.EXE)
4. 图形化标识和鉴别(Graphical Identification and Authentication—GINA)模块处理用户登录凭证



5.3 Windows系统的安全管理

5.3.2 Windows安全体系结构

Windows的层次性的安全架构:

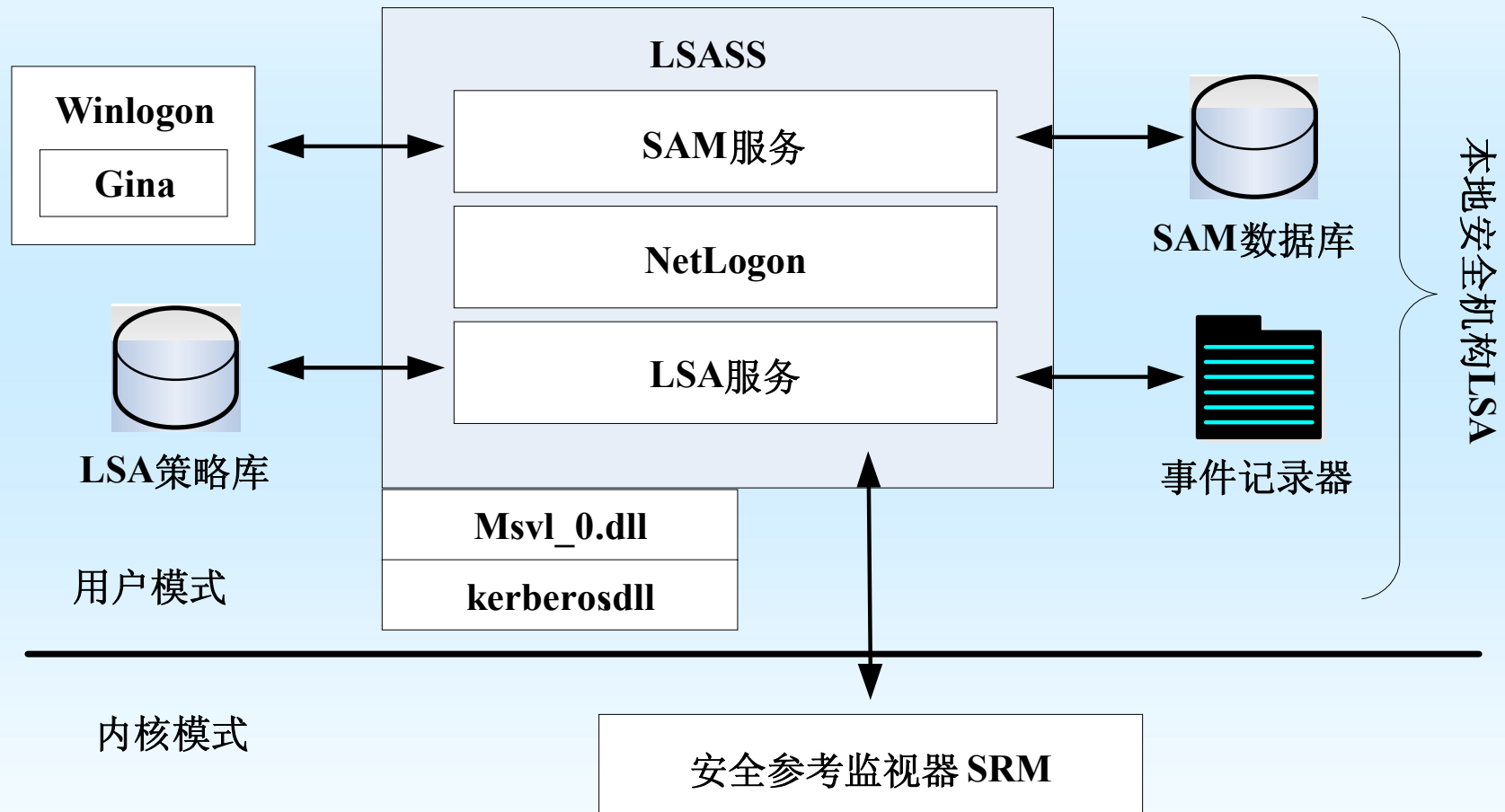


安全主体

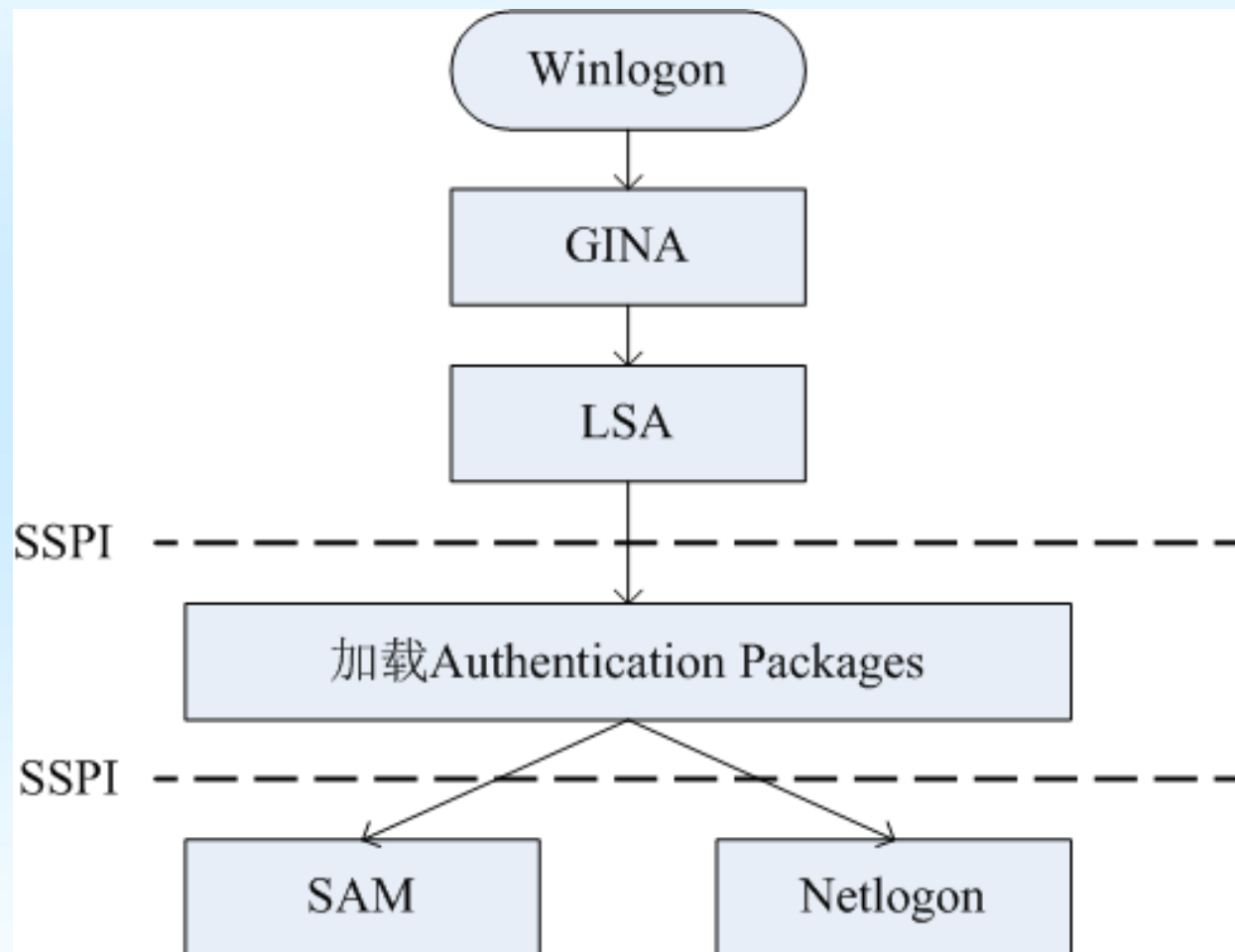
- ◆ Windows的安全性主要围绕安全主体展开，保护其安全性。
- ◆ 安全主体主要包括用户、组、计算机以及域等。
 - 用户：Windows系统中操作计算机资源的主体，每个用户必须先加入Windows系统，并被指定唯一的账户
 - 组：用户账户集合的一种容器，同时组也被赋予了一定的访问权限，放到一个组中的所有账户都会继承这些权限；
 - 计算机：一台独立计算机的全部主体和客体资源的集合，也是Windows系统管理的独立单元；
 - 域：使用域控制器(DC, Domain Controller)进行集中管理的网络，域控制器是共享的域信息的安全存储仓库，同时也作为域用户认证的中央控制机构。

安全子系统

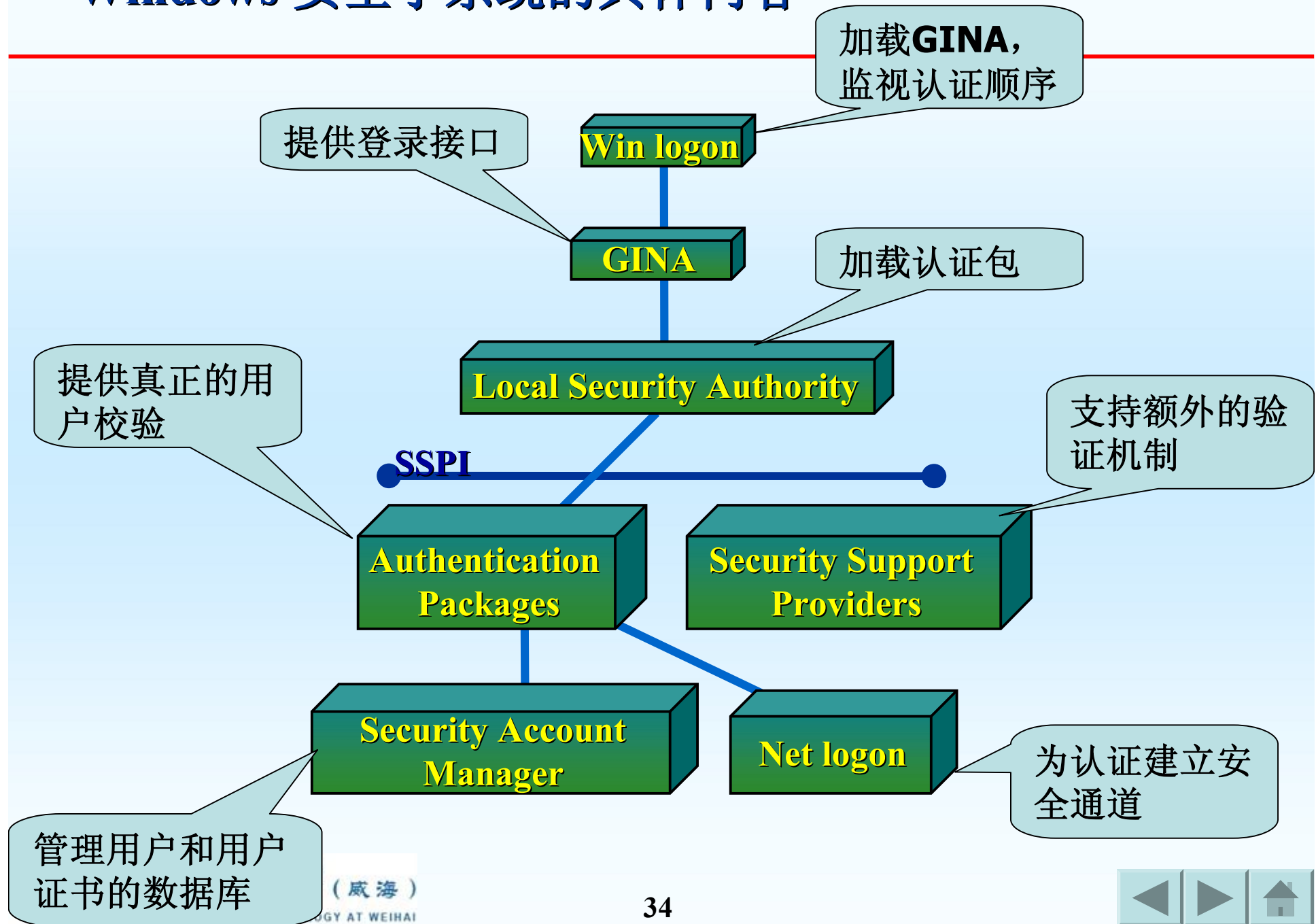
◆安全子系统提供的服务主要包括：身份认证、访问控制、审计。



Windows登录认证流程



Windows 安全子系统的具体内容



Windows 安全子系统2 -----LSA

本地安全认证（**Local Security Authority**）：是一个被保护的子系统，它负责以下任务：

1. 调用所有的认证包，检查在注册表

\HKLM\SYSTEM\CurrentControlSet\Control\LSA下

AuthenticationPackages下的值，并调用该DLL进行认证。

- **msv1_0.dll**是在进行**Windows**身份验证的**LSASS**进程的描述表中运行。这个**DLL**负责检查给定的用户名和密码是否和**SAM**数据库中指定的相匹配，如果匹配，返回该用户的信息。

2. 重新找回本地组的SIDs和用户的权限
3. 创建用户的访问令牌
4. 管理本地安装的服务所使用的服务账号
5. 储存和映射用户权限
6. 管理审核的策略和设置
7. 管理信任关系。



Windows 安全子系统3 -----SSPI 和AP

1. 安全支持提供者的接口（**Security Support Provide Interface**）：
 - 微软的**Security Support Provide Interface**，提供一些安全服务的**API**，为应用程序和服务提供请求安全的认证连接的方法。
2. 认证包（**Authentication Package**）：


认证包可以为真实用户提供认证。通过**GINA DLL**的可信认证后，认证包返回用户的**SIDs**给**LSA**，然后将其放在用户的访问令牌中。

Windows 安全子系统4 -----SSP

- 安全支持提供者（**Security Support Provider**）：
 - 安全支持提供者是以驱动的形式安装的，能够实现一些附加的安全机制。
 - **NTLM**（**NT LAN Manager**）
 - **Kerberos**

Windows 安全子系统1 -----Winlogon Gina

Winlogon and Gina:

1. Winlogon调用GINA DLL，并监视安全认证序列。
2. GINA DLL提供一个交互式的界面为用户登陆提供认证请求。
 GINA DLL被设计成一个独立的模块，当然我们也可以用更加强有力的认证方式（指纹、视网膜）替换内置的GINA DLL。
3. Winlogon在注册表中查找\HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon，如果存在GinaDLL键，Winlogon将使用这个DLL，如果不存在该键，Winlogon将使用默认值MSGINA.DLL



5.3.3 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)

- ✓ 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

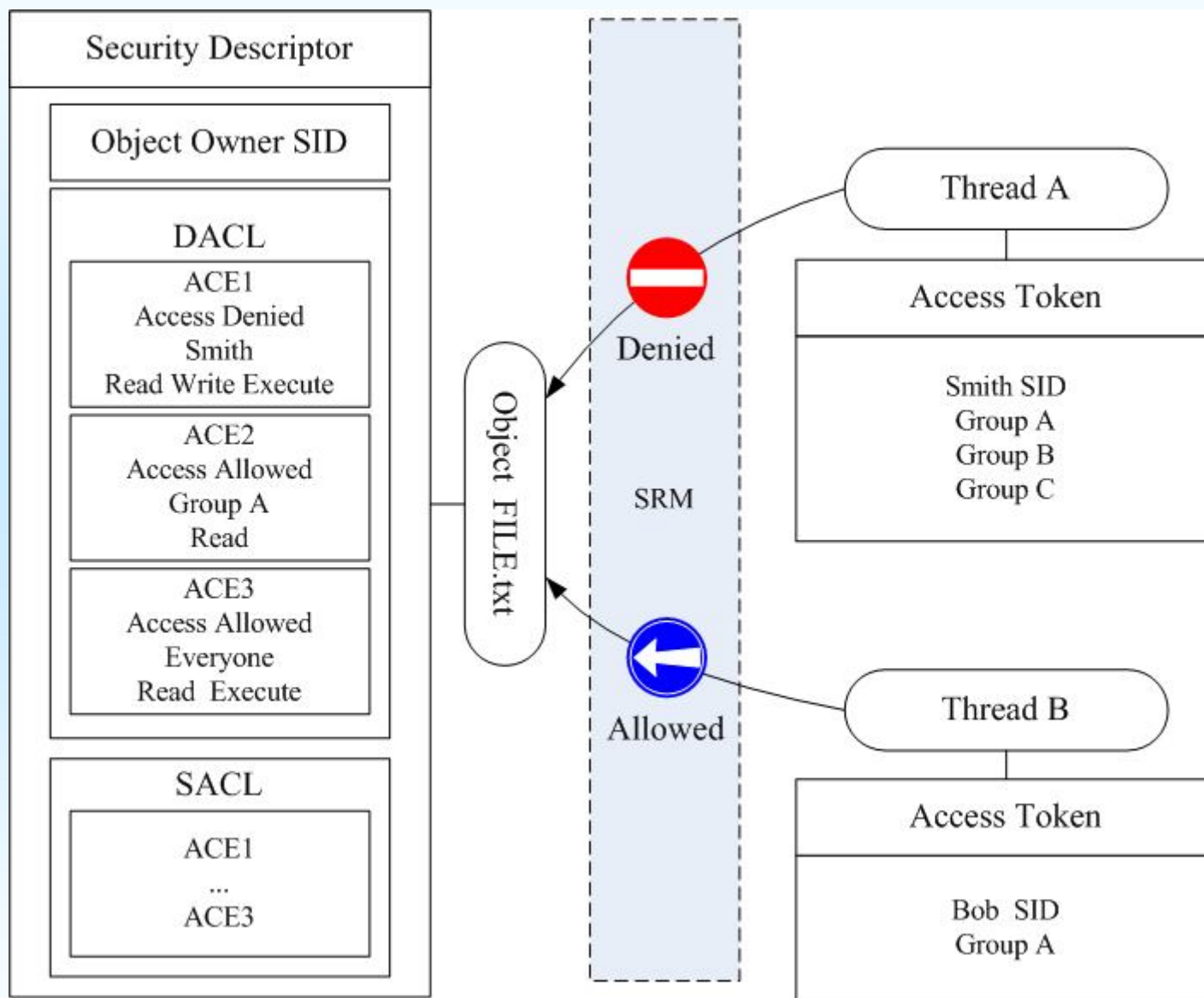
[Group 5] = "BUILTIN\Users" S-1-5-32-545

[Group 6] = "NT AUTHORITY\INTERACTIVE" S-1-5-4

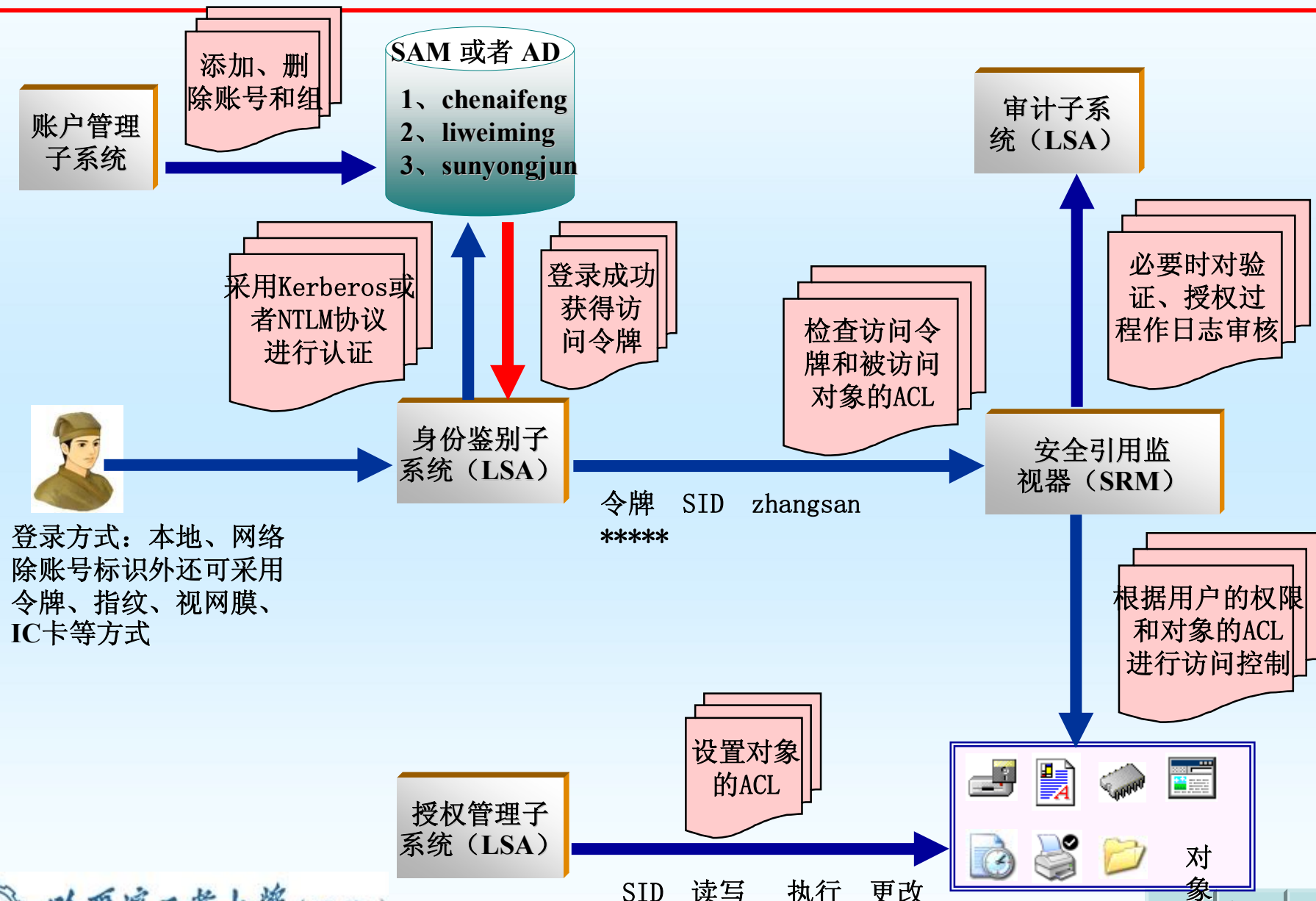
[Group 7] = "NT AUTHORITY\Authenticated Users" S-1-5-11

[Group 8] = "LOCAL" S-1-2-0

Window 访问控制



Windows 安全子系统的工作机理



◆ NTLM工作流程：

- 1、客户端首先在本地加密当前用户的密码成为密码散列
- 2、客户端向服务器发送自己的帐号，这个帐号是没有经过加密的，明文直接传输
- 3、服务器产生一个16位的随机数字发送给客户端，作为一个 challenge（挑战）
- 4、客户端再用加密后的密码散列来加密这个 challenge，然后把这个返回给服务器。作为 response（响应）
- 5、服务器把用户名、给客户端的 challenge、客户端返回的 response 这三个东西，发送域控制器
- 6、域控制器用这个用户名在 SAM 密码管理库中找到这个用户的密码散列，然后使用这个密码散列来加密 challenge。
- 7、域控制器比较两次加密的 challenge，如果相同，那么认证成功。



Kerberos

- ◆ 客户在登录时，将被鉴别。其他客户相信Kerberos鉴别服务器已经正确地对客户进行了验证。
- ◆ 用户必须获得由鉴别服务器发行的许可证，以使用服务器上的可用服务。
- ◆ 所有客户和服务器的会话都是暂时的。如果一个客户需要一个新的会话，就必须获得一个新的鉴别器。

windows本地登录验证过程如下:

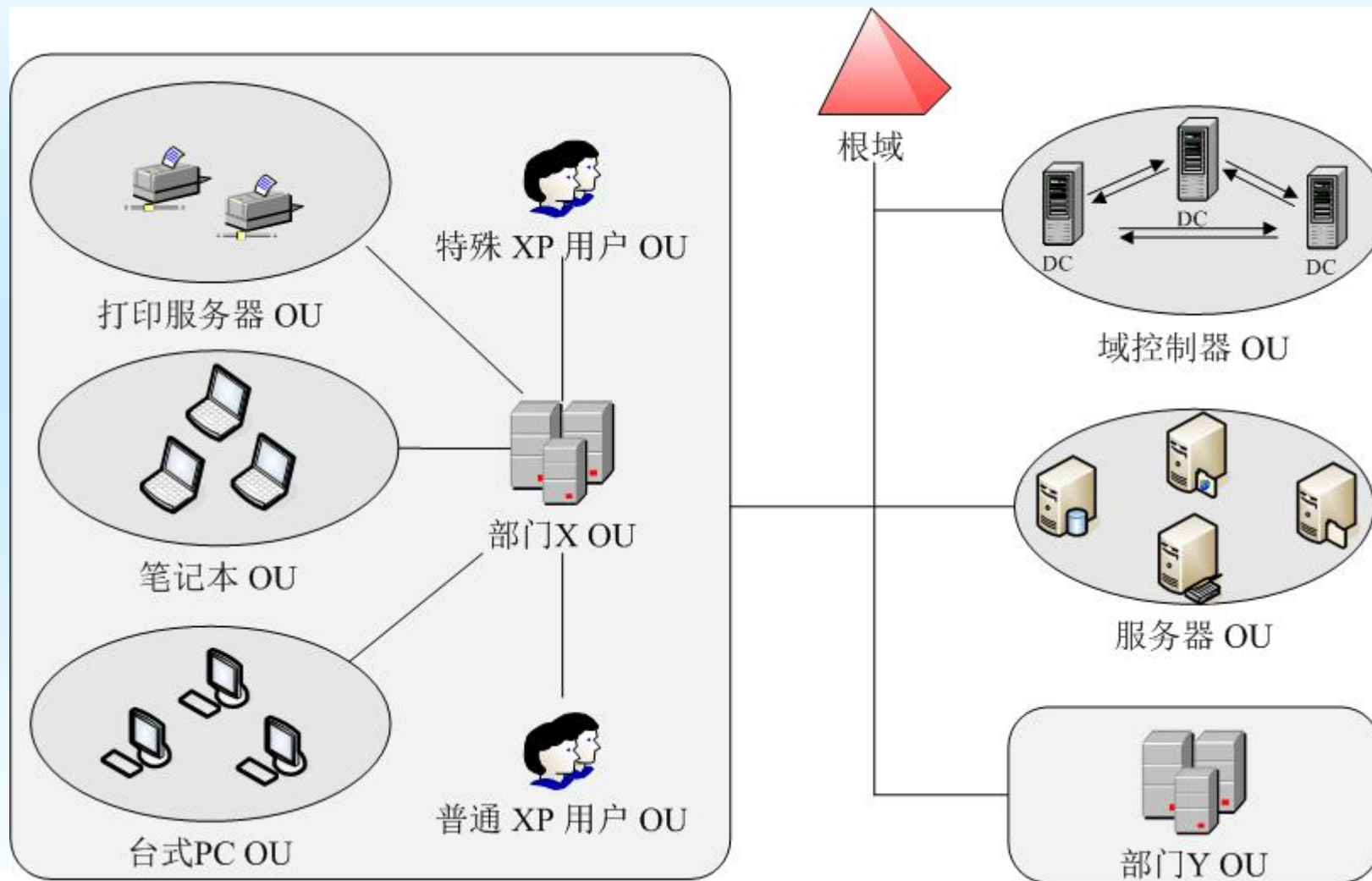
1. 输入用户名及密码然后按回车键. **Graphical Identification and Authentication (GINA)** 会收集这些信息.
2. **GINA** 传送这些安全信息给**Local Security Authority (LSA)** 来进行验证.
3. 在用户登录到本机的情况下, **LSA**会调用**msv1_0.dll**这个验证程序包, 将用户信息处理后生成密钥, 同**SAM**数据库中存储的密钥进行对比.
4. 如果对比后发现用户有效, **SAM**会将用户的**SID(Security Identifier——安全标识)**, 用户所属用户组的**SID**, 和其他一些相关信息发送给**LSA**.
5. **LSA**将收到的**SID**信息创建安全访问令牌, 然后将令牌的句柄和登录信息发送给**winlogon.exe**.

5.3.4 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。
 - 用户和资源管理
 - 网络服务管理：DNS、DHCP、证书服务等
 - 网络应用管理：企业通讯录、用户身份认证、办公自动化等应用



活动目录AD的管理划分

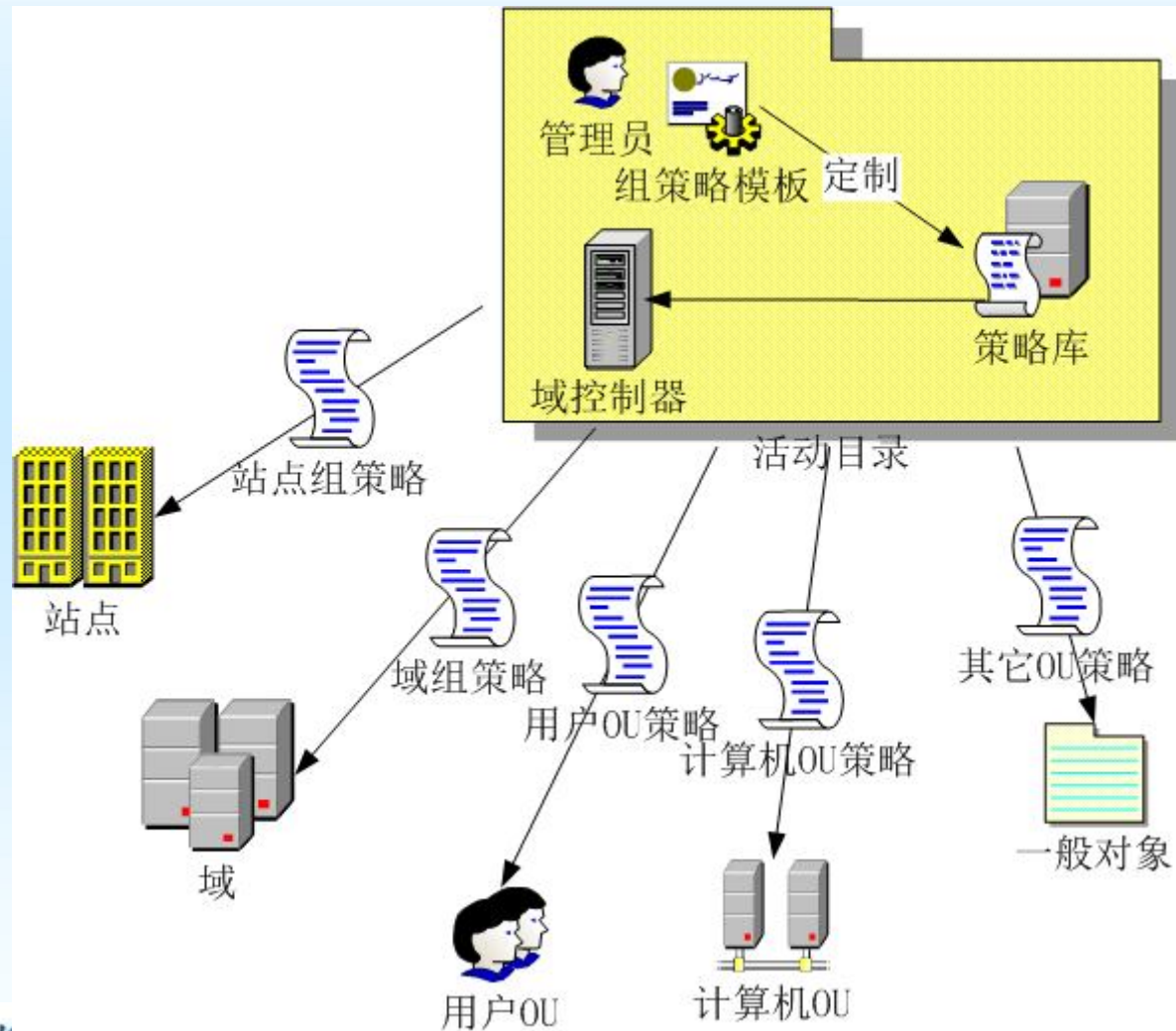


组策略GP

- ◆ 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



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，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?

