Windows安全原理与技术

— 第六章：访问控制

王轶骏， Eric Ericwyj@sjtu.edu.cn

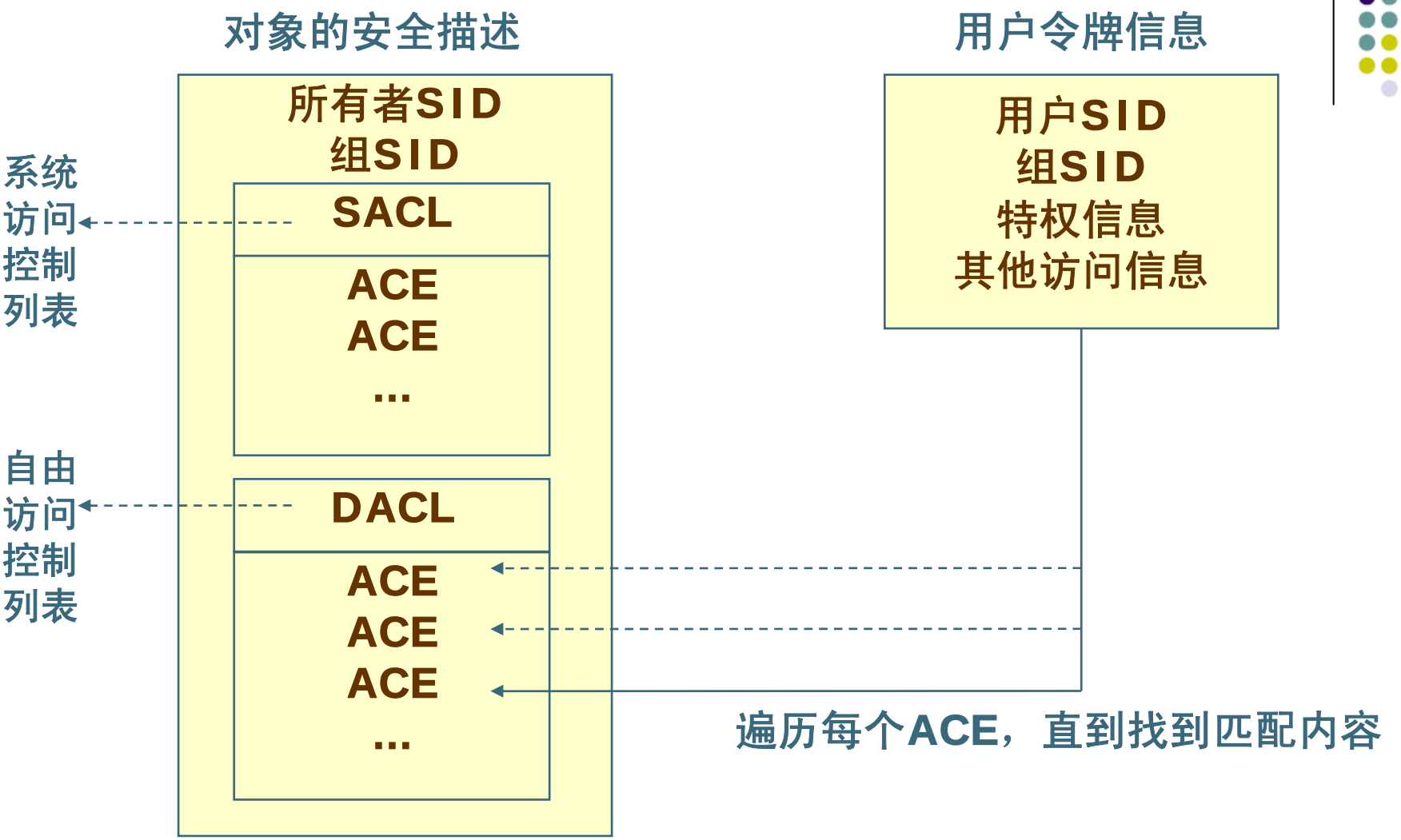
SJTU.INFOSEC.A.D.T, 2008

访问控制的目的

- 限制访问主体（用户、进程、服务等）对访问客体（文件、系统等）的访问权限，从而使计算机系统在合法范围内使用。

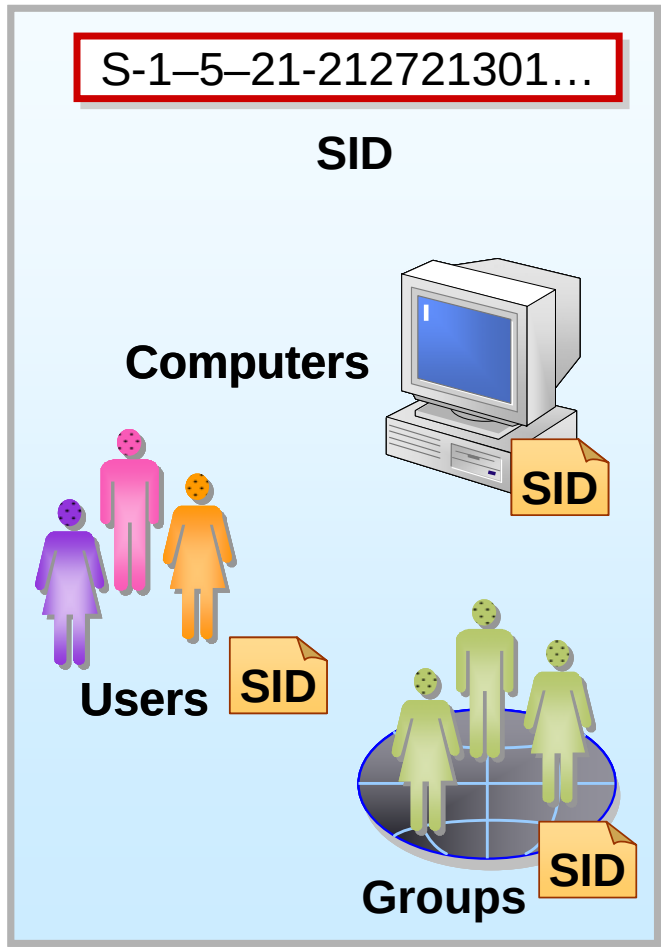
访问控制概述

- 安全主体的访问令牌 ←→ 客体的安全描述
  - 用户登录时，系统为其创建访问令牌。
  - 用户启动程序时，线程获取令牌的拷贝。
  - 程序请求访问客体时，提交令牌。
  - 系统使用该令牌与客体的安全描述进行比较来执行访问检查和控制。


对象的安全描述
用户令牌信息
所有者SID
组SID
SACL
ACE
ACE
...
DACL
ACE
ACE
ACE
...
用户SID
组SID
特权信息
其他访问信息
系统访问控制列表
自由访问控制列表
遍历每个ACE，直到找到匹配内容

安全标识符

- Windows 2000使用安全标识符（SID）来唯一表示安全主体和安全组。
- SID在主体账户和安全组创建时生成。
- SID的创建者和作用范围依赖于账户类型。
  - 本地用户账户
  - 域用户账户



SID的一般格式

$$S\text{-}R\text{-}X\text{-}Y^{1}\text{-}Y^{2}\ldots Y^{n-1}\text{-}Y^{n}$$

- S：表示该字符串为一个SID。
- R：表示SID结构的版本号。（Windows 2000中为1）
- X：表示标示符颁发机构。
  - 对于Administrators组等Windows 2000特定的帐户和组，该值为5（NT Authority）。
  - 对于Everyone等一般用户和组，该值为1（World Authority）。
- Y^{1}-Y^{n-1}：表示子级颁发机构，标识了各级不同的域。
  - Administrators组的域标识符是32（Builtin）。
  - Everyone组没有域标识符。
- Y^{n}：表示域内特定的帐户和组，也叫相对标识符。
  - Administrators组的相对标识符是544。
  - Administrator的相对标识符是500，Guest是501。
  - Everyone组的相对标识符为空。

安全访问令牌的内容

- 用户账号的SID
- 所属组的SID
- 针对计算机的特权（Privileges）列表
- 所有者的SID
- 持有用户主安全组的SID
- 默认任意访问控制表
- 源，即导致访问令牌被创建的进程
- 类型，主令牌还是模拟令牌
- 模拟级别
- 统计信息
- 限制SID
- 会话ID

模拟（Impersonation）

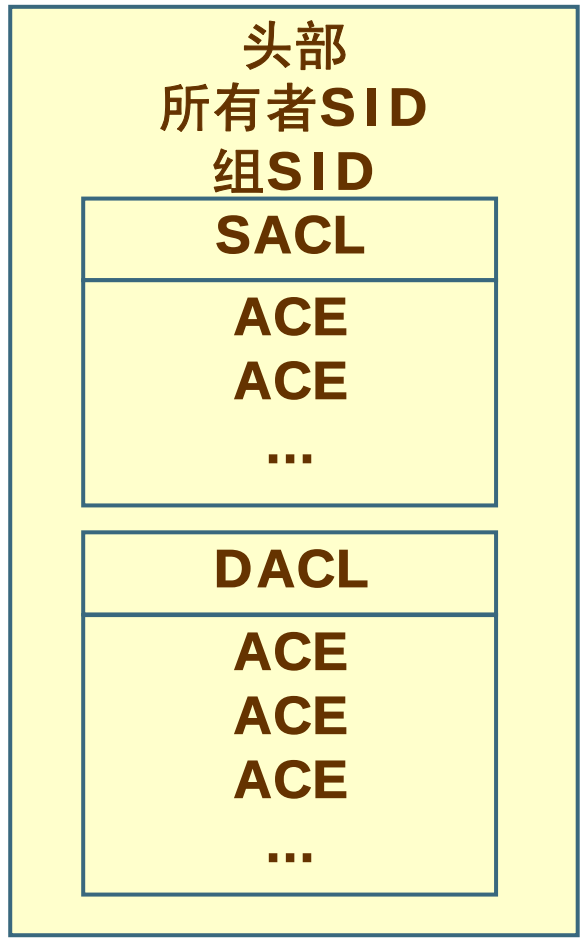
- 模拟能力是为了适应客户/服务器应用的安全需求而设计的。
  - 正常情况下，服务进程在自己的安全上下文内运行，其中的线程使用服务自己安全环境相关联的主访问令牌。
  - 客户请求服务时，服务进程创建执行线程来完成任务。该线程使用客户安全环境相关联的模拟令牌。
  - 任务完成之后，线程丢弃模拟令牌并重新使用服务的主访问令牌。

安全描述

- 当在授权用户安全环境中执行的线程创建对象时，安全描述中就会被填入访问控制信息。
- 访问控制信息的来源：
  - 执行线程（主体线程）直接把访问控制信息分配给对象。
  - 系统从父对象中检查可继承的访问控制信息，并将其分配给对象。
  - 系统使用对象管理器所提供的默认访问控制信息，并将其分配给对象。

安全描述的内容

- 头部
  - 版本号、控制标志、自动传播信息
- 所有者的SID
- 所有者主要组的SID
- DACL
  - 控制特定用户和组对对象的访问
- SACL
  - 审核特定用户和组对对象的访问



默认安全描述

- 所有者的默认设置
- 所有者所在组的默认设置
- DACL的默认设置
  - 直接DACL
  - 继承下来的DACL
  - 活动目录架构提供的默认DACL
- SACL的默认设置
  - 与DACL类似

安全描述的更改

- 对象所有者、拥有所有者权限的用户以及在其安全环境中进行操作的执行线程，都可以改变对象的访问控制信息。
- 对象所属容器的变化也会导致对象的安全描述被修改。

访问控制列表

- 访问控制列表（ACL）是访问控制项（ACE）的有序列表。

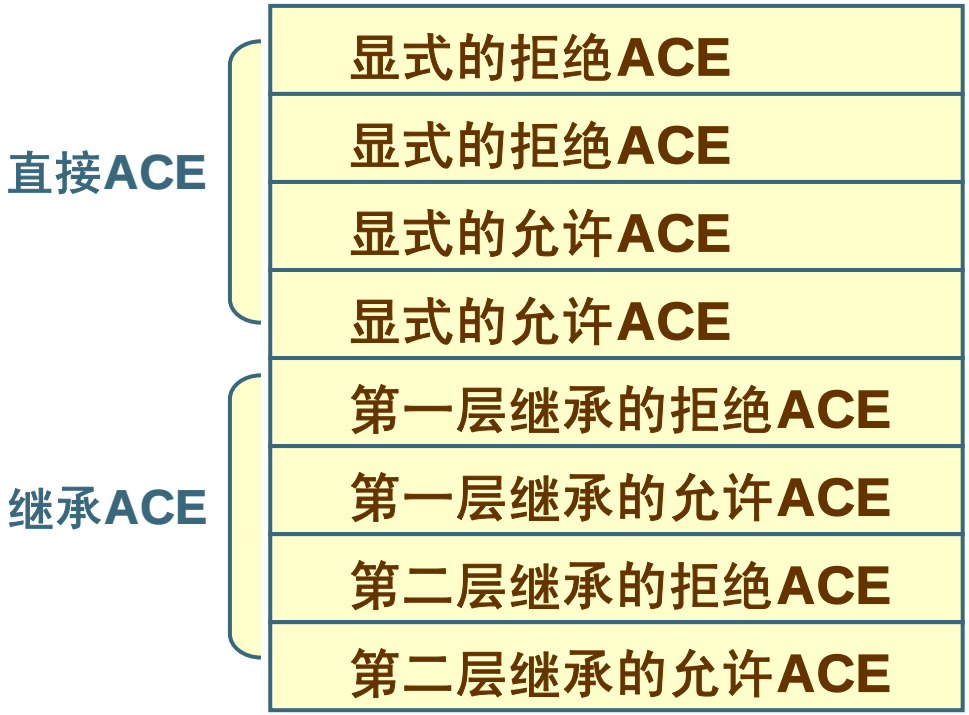
ACL大小	ACL修改版本
ACE数目	
[ACE 1]	
[ACE …]	
[ACE n]	

“空DACL”和“无DACL”

- 空DACL
  - 在列表中没有任何ACE的存在，因此也就不允许任何用户进行访问 。
- 无DACL
  - 指的是对于该对象没有任何保护，发出请求的任何用户都被允许访问该对象 。

访问控制项在列表中的顺序

- 直接ACE在继承ACE之前。
- 从第一层（父对象）继承下来的ACE在ACL的最前面。
- 拒绝ACE在允许ACE之前。



访问控制项的类型

- 一般访问控制项
  - 存在于所有的安全对象中。
  - 包括拒绝访问、允许访问和系统审核。
- 与对象有关的访问控制项
  - 只存在于活动目录对象中。
  - 对可以继承自己的子对象类型提供了更大的控制粒度。
  - 包括特殊对象的拒绝访问、特殊对象的允许访问和特殊对象的系统审核。

一般访问控制项的结构

- ACE大小
  - 分配的内存字节数。
- ACE类型
  - 允许、禁止或监视访问。
- 继承和审计标志
- 访问屏蔽码
  - 32位，每一位对应着该对象的访问权限，可设置为打开或关闭。
- SID标识

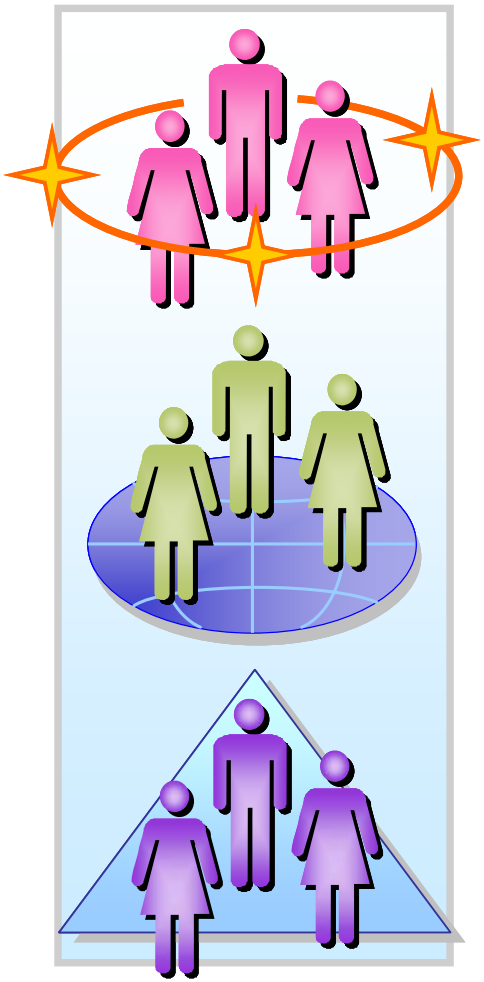
用户和组

- 用户
  - 本地用户账户
  - 域用户账户
- 组
  - 用户账户的集合，方便权限分配。
  - 计算机帐户的集合，方便资源访问。

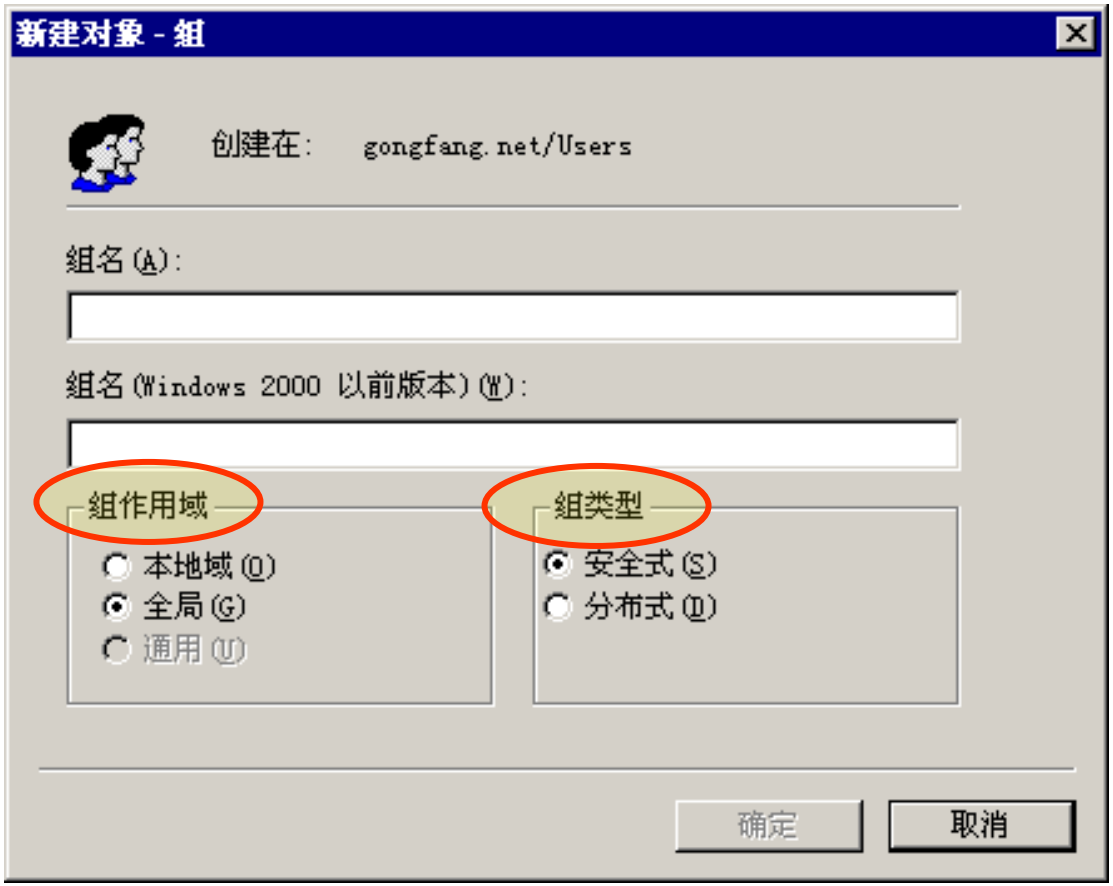
组类型

- 安全组
  - Windows 2000自身只使用安全组。
  - 安全组可被分配访问资源的权限和执行任务的权利。
  - 安全组可拥有分布组的所有功能。
- 分布组
  - 当组的惟一功能与安全性（如同时向一组用户发送电子邮件）不相关时，就可以使用分布组。
  - 分布组不能用来分配权限。

组作用域



- 通用组（ Universal Group）
  - 成员可来自森林中的任何域。
  - 可访问任何域中的资源。
- 全局组（ Global Group）
  - 成员仅可来自本地域。
  - 可访问任何域中的资源。
- 域本地组（ Domain Local Group）
  - 成员可来自森林中的任何域。
  - 仅可访问本地域内的资源


新建对象 - 组
创建在: gongfang.net/Users
组名(A):
组名(Windows 2000 以前版本)(W):
组作用域
本地域(O)
全局(G)
通用(U)
组类型
安全式(S)
分布式(D)
确定
取消

指定组作用域和组类型

本地组

- 本地组是本地计算机上的用户账户集合
  - 本地组不同于具有域本地作用域的活动目录组。
  - 本地组权限只提供对本地组所在计算机上资源的访问。
  - 可在运行Windows 2000的非域控制器的计算机上使用本地组，不能在域控制器上创建本地组。

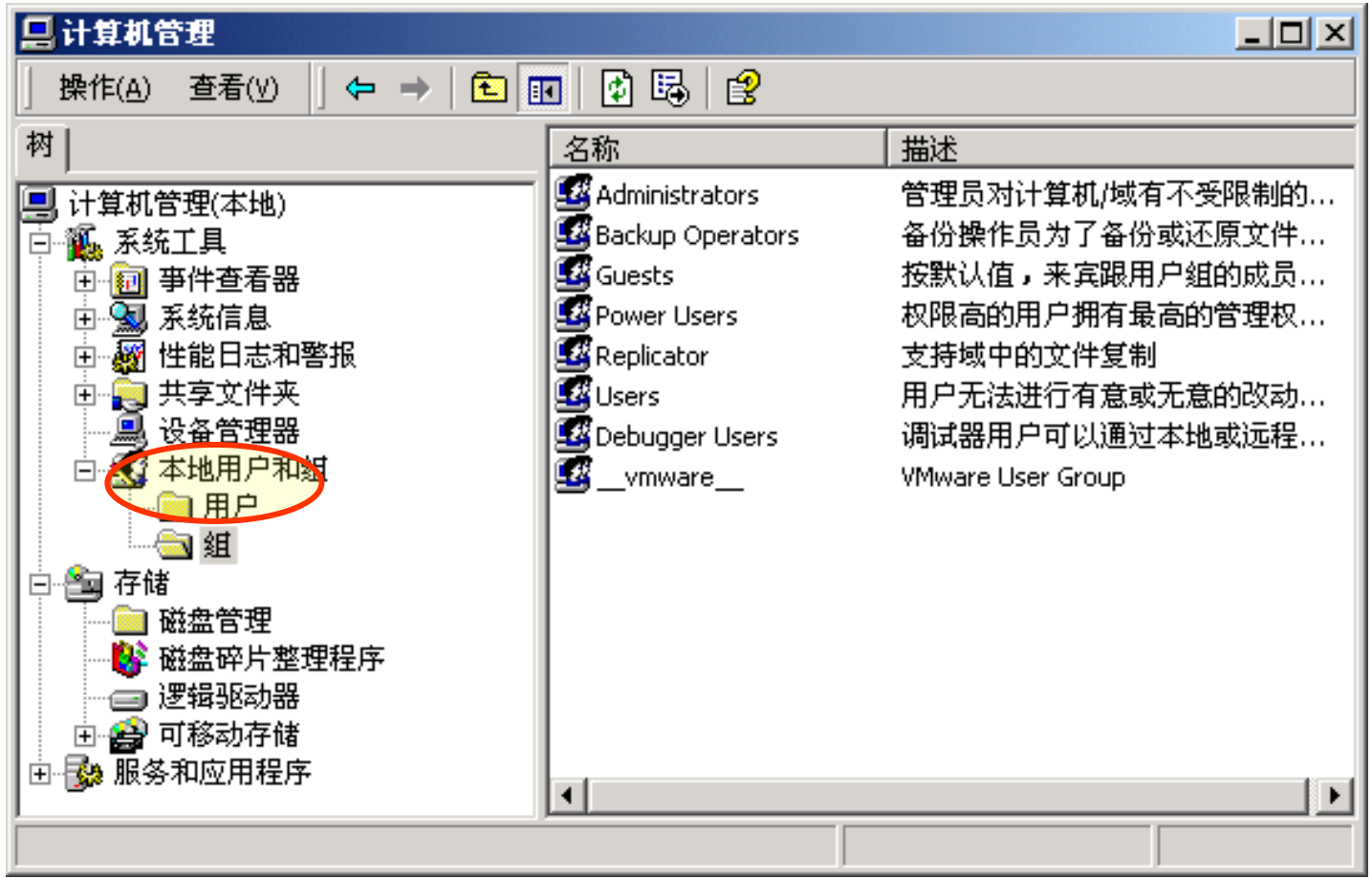
内置本地组

成员服务器

Administrators	管理员对计算机 / 域有不受限制的完全访问权。
Backup Operators	备份操作员为了备份或还原文件可以替代安全限制。
Guests	按默认值，来宾跟用户组的成员有同等访问权，但来宾帐户的限制更多。
Power Users	权限高的用户拥有最高的管理权限，但有限制。因此，权限高的用户可以运行经过证明的文件，也可以运行继承应用程序。
Replicator	支持域中的文件复制。
Users	用户无法进行有意或无意的改动。因此，用户可以运行经过证明的文件，但不能运行大多数继承应用程序。

域控制器

Account Operators	成员可以管理域用户和组帐户。
Print Operators	成员可以管理域打印机。
Server Operators	成员可以管理域服务器。


计算机管理
操作(A)
查看(V)
树
计算机管理(本地)
系统工具
事件查看器
系统信息
性能日志和警报
共享文件夹
设备管理器
本地用户和组
用户
组
存储
磁盘管理
磁盘碎片整理程序
逻辑驱动器
可移动存储
服务和应用程序
名称
描述
Administrators
管理员对计算机/域有不受限制的...
Backup Operators
备份操作员为了备份或还原文件...
Guests
按默认值，来宾跟用户组的成员...
Power Users
权限高的用户拥有最高的管理权...
Replicator
支持域中的文件复制
Users
用户无法进行有意或无意的改动...
Debugger Users
调试器用户可以通过本地或远程...
__vmware__
VMware User Group

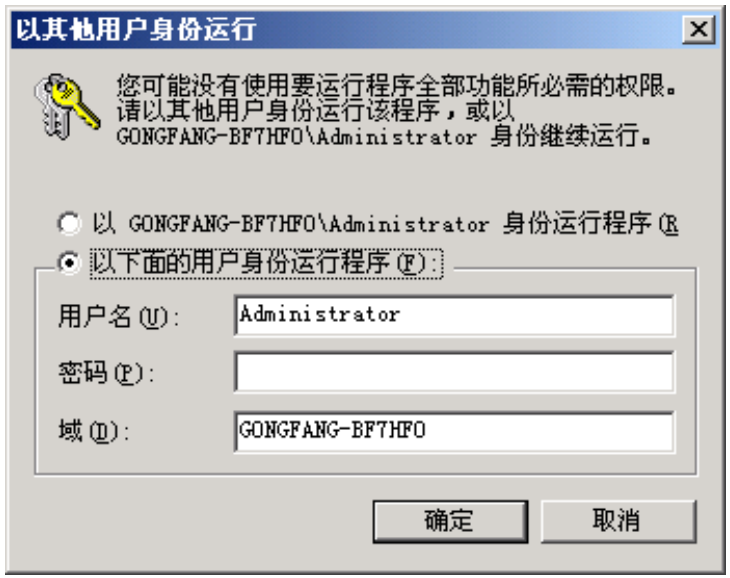
本地组管理工具

Administrators组

- 安装操作系统和组件。
  （包括硬件驱动程序，系统服务及其他）
- 安装 Service Pack 和Hotfix修补程序。
- 安装 Windows Update。
- 升级和修复操作系统 。
- 配置机器范围内的重要的操作系统参数。
  （如密码策略、访问控制、审核策略、内核模式驱动程序配置等）
- 获取已经不能访问的文件的所有权。
- 管理安全措施和审核日志。
- 备份和还原系统。

RunAs服务（辅助登录服务）

- RunAs服务使得管理员可以使用标准的用户账户登录，并在必要的时候可以调用具有更高权限的管理员控制台来执行管理任务。
  - 在管理工具（Administrative Tool）应用组件上右击，然后从弹出的菜单中选择“运行为…”。
  - 在DoS命令符中输入“runas”，并按回车键 。



Users组

- 不允许破坏操作系统的完整性和所安装的应用程序。
- 不能修改机器级的注册设置、操作系统文件或程序文件。
- 不能安装可以被其他用户运行的应用程序。
- 不能访问其他用户的私有数据。

Power Users组

- 创建本地用户和组 。
- 修改其创建的用户和组 。
- 创建和删除非管理员文件共享。
- 创建、管理、删除和共享本地打印机。
- 修改系统时间。
- 停止或启动非自动启动的服务。
- 允许安装无需修改系统服务的应用程序。

默认访问控制和安全设置

- 针对计算机的默认安全设置
- 针对用户的文件和注册表默认访问控制
- 针对用户的默认用户权利指派

针对用户的文件和注册表默认访问控制

对象	权限
HKEY_CURRENT_USER	完全控制
%USERPROFILE%	完全控制
所有用户\文档	修改
所有用户\应用程序数据	修改
%WINDIR%\TEMP	同步、遍历、添加文件和添加子目录
\（根目录）	安装期间未配置

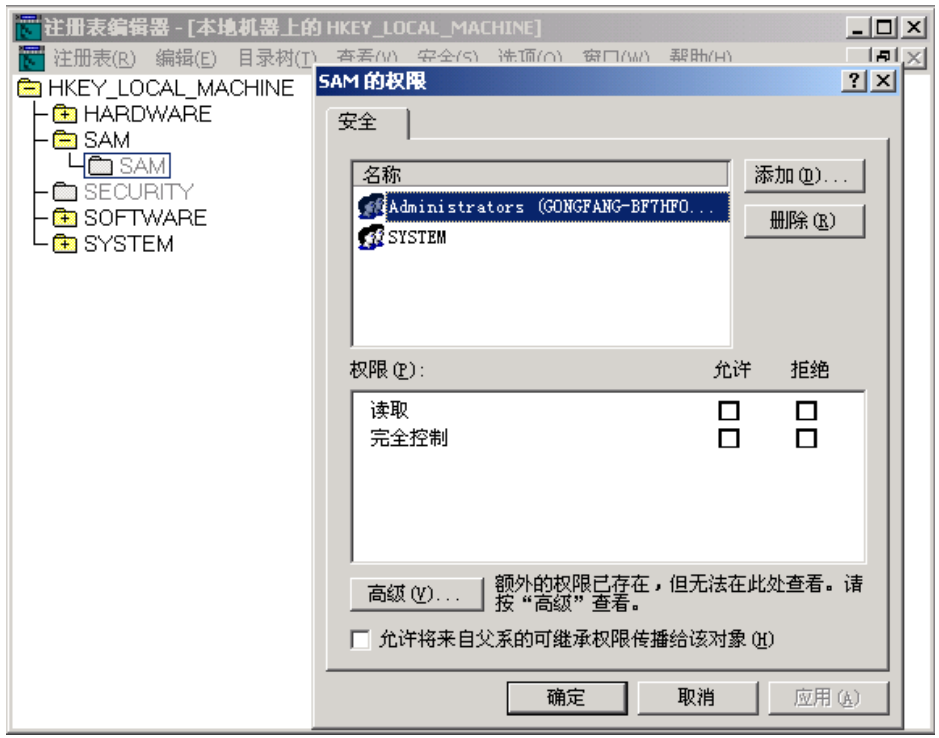
注册表的权限配置

① 选择“开始→运行”命令，运行regedt32.exe命令。

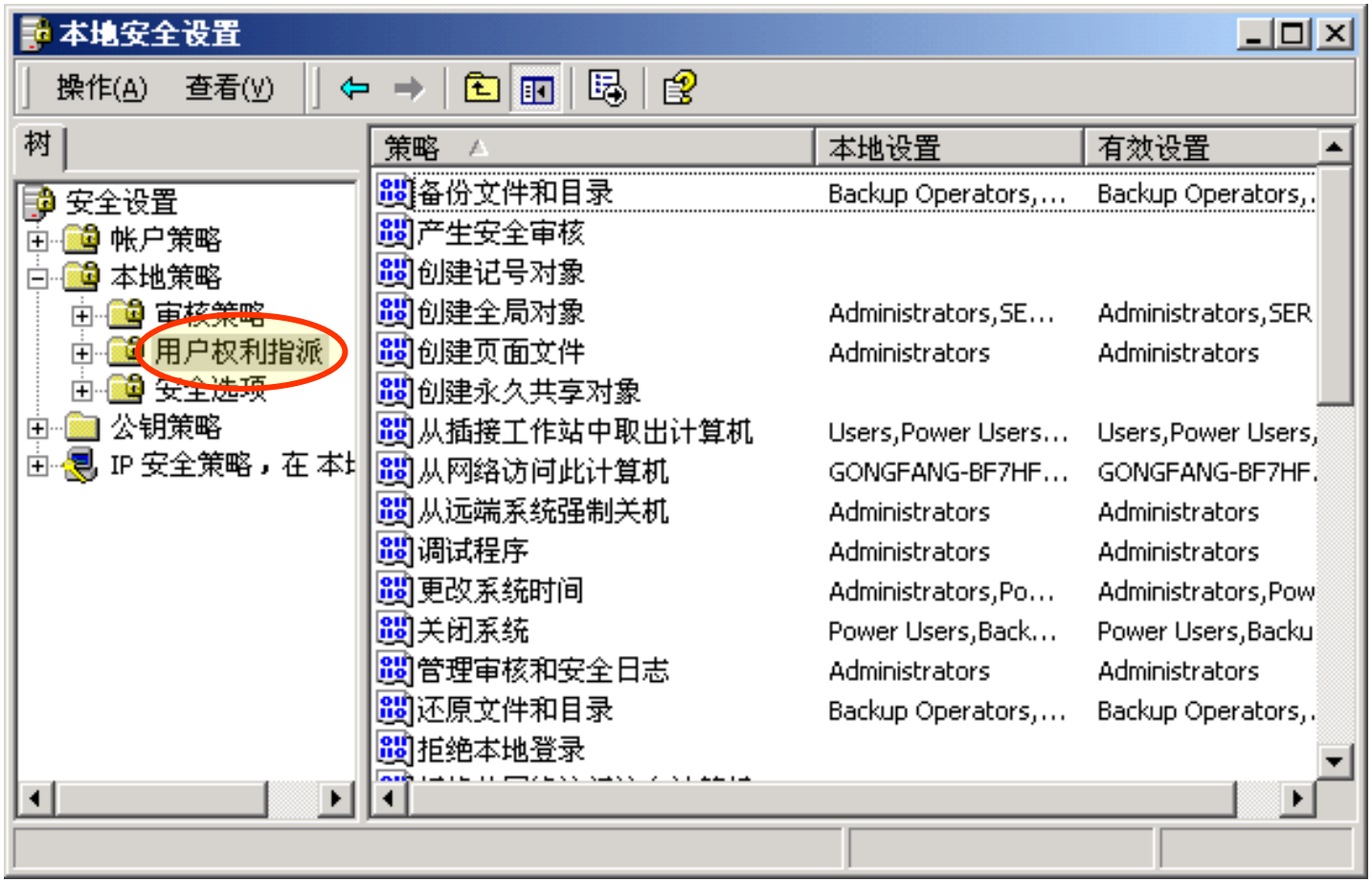
② 选择需要编辑的子键。

③ 选择菜单栏上的“安全”→“权限”命令。

④ 在“安全”选项卡中编辑需要更改的组的权限设置。



用户权利的默认指派


本地安全设置
操作(A)
查看(V)
树
安全设置
帐户策略
本地策略
审核策略
用户权利指派
安全选项
公钥策略
IP 安全策略，在 本
策略
本地设置
有效设置
备份文件和目录
Backup Operators,...
Backup Operators,.
产生安全审核
创建记号对象
创建全局对象
Administrators,SE...
Administrators,SER
创建页面文件
Administrators
Administrators
创建永久共享对象
从插接工作站中取出计算机
Users,Power Users...
Users,Power Users,
从网络访问此计算机
GONGFANG-BF7HF...
GONGFANG-BF7HF.
从远端系统强制关机
Administrators
Administrators
调试程序
Administrators
Administrators
更改系统时间
Administrators,Po...
Administrators,Pow
关闭系统
Power Users,Back...
Power Users,Backu
管理审核和安全日志
Administrators
Administrators
还原文件和目录
Backup Operators,...
Backup Operators,.
拒绝本地登录

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消