



计算机安全与维护

第一章 Windows 系统基本概念



关于课程你需要了解...

中国传媒大学



教学团队

- 主讲教师
 - 黄玮
 - 信息安全博士，讲师
- 助教
 - 李美聪 信息安全硕士
 - 李建方 信息安全硕士



课程概况

- 上课地点
 - 讲授&实验：48教 A101
 - 上课时间
 - 1-16 周二 第9、10、11节
- 答疑地点/时间
 - A101E 周一到周五白天
 - 新浪微博 @中传黄玮 / 随时
 - 邮箱： i@huangwei.me



课程概况

- 先修课程
— 无
- 参考教材
— 无
- 硬件和软件环境
— PC + VirtualBox
- 开卷考试（60%）+ 平时成绩（40%）
— 平时成绩：出勤 + 课堂表现 + 实验报告



在线资源

- <http://cs.cuc.edu.cn/huangwei/wiki>



关于课程的教、学方法和原则

- 教

- 授人以渔
 - 重思路、方向讲解，轻傻瓜式重复

- 学

- 兴趣第一
- 尽信师，不如无师：质疑、思考、实践
- 会用、用好互联网
 - 每人建立一个课程专用blog，微博@我 或发邮件告诉我地址、姓名、学号



安全卫士与电脑管家时代的计算机安全与维护



医生：请脱衣接受检查

病人：不行，这是我的隐私！

医生：。。。你想治病吗？

病人：算了，我自助！



安全卫士与电脑管家时代的计算机安全与维护

- 作为一名计算机及信息安全相关专业的学生，你是否经常遇到以下求助：
 - 电脑运行很慢，求加速
 - 数据丢失，求恢复
 - 电脑无法开机，求解决
 - 杀软提示有病毒，但杀不干净，求清理



关于《计算机安全与维护》课程的内容

- 计算机硬件基础知识与实践
- 以Windows系统的安全使用与维护为主
 - 基本概念、进阶操作
 - 以实践为基础的知识体系构建
 - 体验操作系统攻防，培养信息安全意识
- 兼顾移动终端安全科普
 - Android + iOS



考核方式

- 平时成绩
 - 占总评成绩的百分比为**40%**
 - 主要包括以下形式：
 - 上课考勤，作业、测验，实验上机
- 期末考试
 - 开卷
 - 占学期总成绩**60%**，着重进行能力考察



计算机硬件拆解

中国传媒大学



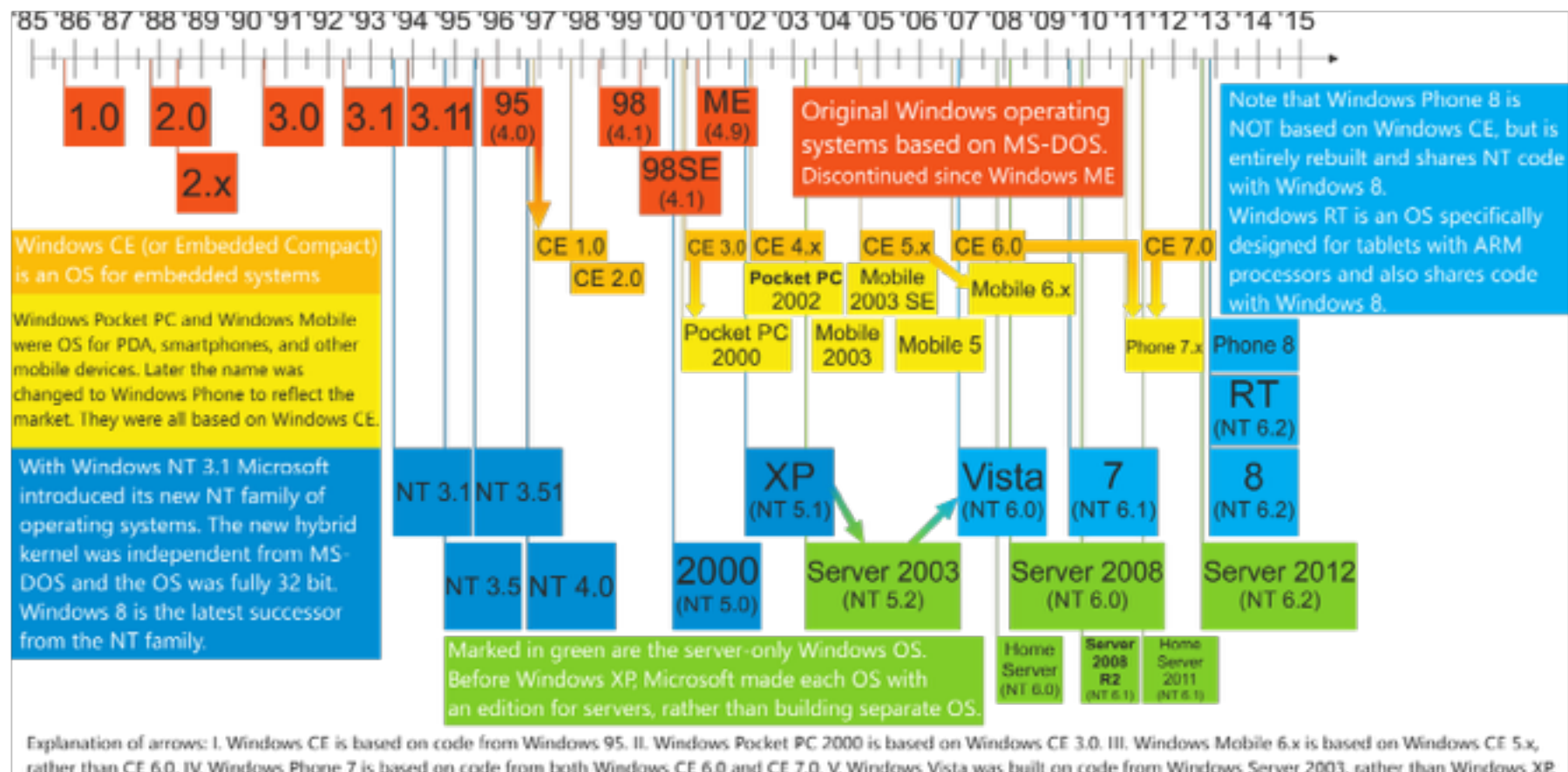
动手时间!



关于WINDOWS家族



Windows 家族编年史





人民群众眼中的Windows





关于Windows XP

Windows XP SP3 和 Office 2003
将于 2014 年 4 月 8 日结束支持



原因？

为什么 Microsoft 要结束对 Windows XP SP3 和 Office 2003 的支持？



什么？

结束支持对于客户意味着什么？



如何？

如何开始迁移？

升级至 Windows 7？

[单击此处开始](#)

升级至 Windows 8.1？

[单击此处开始](#)

通过 Microsoft 服务即刻开始
Windows XP 迁移



关于Windows操作系统产品的版本与命名

- 按家族里程碑/产品内核版本分类
- 按支持的CPU类型分类
 - x86 32bit/x86 64bit/ARM
- 按销售渠道类型分类
- 按产品功能类型分类
- 按产品语言支持分类
 - 简体中文、英文、法文。。。。



按家族里程碑/产品内核版本分类

开发代号	版本	版本号	发布日期
Interface Manager	Windows 1.0	1.0	1985-11-20
无	Windows 2.0	2.0	1987-11-1
无	Windows 3.0	3.0	1990-5-22
Janus	Windows 3.1	3.1	1992-3-18
NTOS/2	Windows NT 3.1	NT 3.1	1993-7-27
Janus	Windows 3.2	3.2	1994-4-14
Chicago	Windows 95	4.0	1995-8-24
Daytona	Windows NT 3.5	NT 3.5	1995-11-20
Cairo	Windows NT 4.0	NT 4.0	1996-7-29
Detroit	Windows 95OSR2	4.00.950B	1996-8-24
Memphis	Windows 98	4.1	1998-6-25
Memphis	Windows 98 Second Edition	4.10.2222A	1999-5-5
Windows NT 5.0	Windows 2000	NT 5.0	2000-2-17
Millennium	Windows ME	4.9	2000-9-14
Whistler	Windows XP	NT 5.1	2001-10-25
Whistler Server	Windows Server 2003	NT 5.2	2003-4-24
Longhorn	Windows Vista	NT 6.0	2007-1-30
Longhorn Server	Windows Server 2008	NT 6.0	2008-2-27
Windows 7	Windows 7	NT 6.1	2009-10-22
Windows Server 7	Windows Server 2008 R2	NT 6.1	2009-10-22
无	Windows Thin PC	NT 6.1	2011-07-11
Windows 8	Windows 8	NT 6.2	2012-10-25
Windows Server 8	Windows Server 2012	NT 6.2	2012-9-4
Windows Blue	Windows 8.1	NT 6.3	2013-10-18
无	Windows Server 2012 R2	NT 6.3	2013-10-18

开发代号：Windows 7
版本：Windows 7
版本号：NT 6.1



按销售渠道类型分类

- MSDN (Microsoft Developer Network) 版
 - 面向开发者
- OEM (original equipment manufacturer) 版
 - 面向设备制造商定制
- RTM (release.to.manufacturing) 版
 - 面向零售渠道



按产品功能分类——以Windows 7标准版为例

- Windows 7 入门版 (Starter)
- Windows 7 家庭普通版 (Home Basic)
- Windows 7 家庭高级版 (Home Premium)
- Windows 7 专业版 (Professional)
- Windows 7 企业版 (Enterprise)
- Windows 7 旗舰版 (Ultimate)
- Windows 7 家用服务器版 (Home Server)

参考自: http://zh.wikipedia.org/wiki/Windows_7%E7%89%88%E6%9C%AC%E5%88%97%E8%A1%A8



关于本课程的讲授内容和实验环境

- Windows XP SP3 32bit 简体中文版
- Windows 7 Ultimate SP1 32bit 简体中文版
- Windows 7 Ultimate SP1 64bit 简体中文版



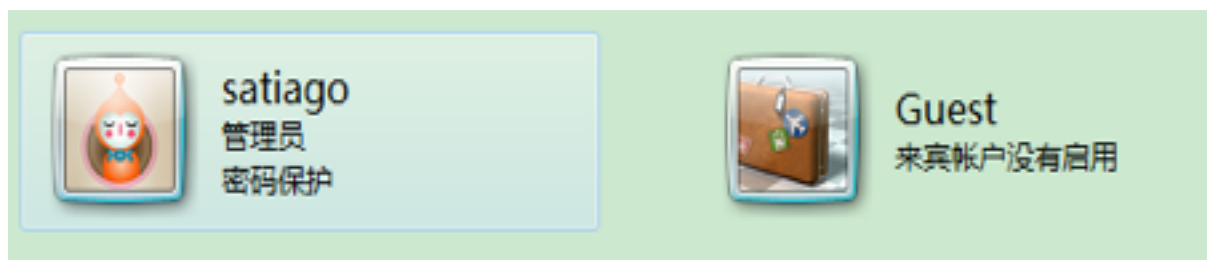
本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



什么是windows用户帐号

- 为了Windows系统环境的安全性和个人信息的私密性，在windows NT/2000/XP及以后的系统中，用户帐号成为了系统安全的重要组件。
- 通过不同类型的用户帐号来对用户角色进行定位，并提供相应的服务和操作权限。





为什么使用windows用户帐号

- 系统的安全性
- 用户的角色定位
- 操作权限的设置
- 个人信息的私密性
- 系统管理的方便有序
- 提供相应系统及网络共享服务



Windows 用户帐号类型

- Windows 内置用户帐号
- Administrator 用户
- 该帐号为系统默认的管理员帐号，该帐户具有 Windows 的最高管理权限，用来完成软件安装、系统设置等任务。
- Guest 用户
- 提供给没有用户帐户，但是需要访问本地计算机内资源的用户使用，该类型的用户无法永久地改变其桌面的工作环境。



Windows 用户帐号类型

- 用户自定义帐号
- 除内置的系统帐户外，用户可以自己为登陆系统而创建新帐户，用户类型分为“标准用户”和“管理员”两种。

命名帐户并选择帐户类型

该名称将显示在欢迎屏幕和「开始」菜单上。

新帐户名

☒ 标准用户(S)

标准帐户用户可以使用大多数软件以及更改不影响其他用户或计算机安全的系统设置。

☐ 管理员(A)

管理员有计算机的完全访问权，可以做任何需要的更改。根据通知设置，可能会要求管理员在做出会影响其他用户的更改前提供密码或确认。

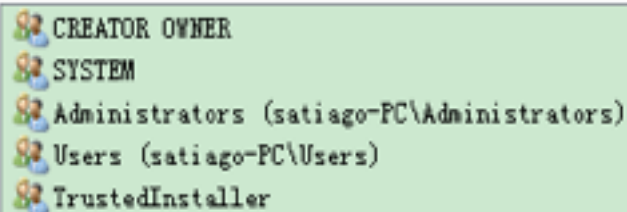
我们建议使用强密码保护每个帐户。



什么是用户组

- 用户组即把类型相同的一些用户帐号放置在一个组群中，方便对其进行全局的权限和服务的设置管理。

组或用户名 (G):



```
CREATOR OWNER
SYSTEM
Administrators (satiago-PC\Administrators)
Users (satiago-PC\Users)
TrustedInstaller
```



Administrators

管理员组，默认情况下，Administrators中的用户对计算机/域有不受限制的完全访问权。分配给该组的默认权限允许对整个系统进行完全控制。一般来说，应该把系统管理员或者与其有着同样权限的用户设置为该组的成员。



Users

普通用户组，这个组的用户无法进行有意或无意的改动。因此，用户可以运行经过验证的应用程序，但不可以运行大多数旧版应用程序。Users 组是最安全的组，因为分配给该组的默认权限不允许成员修改操作系统的设置或用户资料。Users 组提供了一个最安全的程序运行环境。在经过 NTFS 格式化的卷上，默认安全设置旨在禁止该组的成员危及操作系统和已安装程序的完整性。用户不能修改系统注册表设置、操作系统文件或程序文件。Users 可以创建本地组，但只能修改自己创建的本地组。Users 可以关闭工作站，但不能关闭服务器。



Power Users

高级用户组，Power Users 可以执行除了为 Administrators 组保留的任务外的其他任何操作系统任务。分配给 Power Users 组的默认权限允许 Power Users 组的成员修改整个计算机的设置。但Power Users 不具有将自己添加到 Administrators 组的权限。在权限设置中，这个组的权限是仅次于Administrators的。



用户组的类型

Guests

来宾组，来宾组跟普通组Users的成员有同等访问权，但来宾帐户的限制更多。

Everyone

所有的用户，这个计算机上的所有用户都属于这个组。



SYSTEM

这个组拥有和Administrators一样甚至更高的权限，在察看用户组的时候它不会被显示出来，也不允许任何用户的加入。这个组主要是保证了系统服务的正常运行，赋予系统及系统服务的权限。

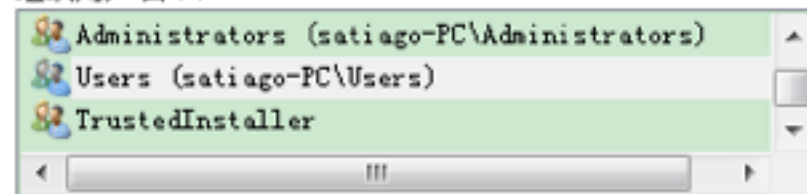


Windows的权限

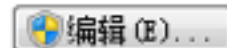
- 权限定义了授予用户或组对某个对象或对象属性的访问类型。
- Windows系统对权限的分类定义来确保不同类型的用户对系统的控制能力。

对象名称: C:\Program Files

组或用户名 (G):



要更改权限，请单击“编辑”。



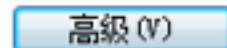
Users 的权限 (F)

允许

拒绝

修改		
读取和执行	✓	
列出文件夹内容	✓	
读取	✓	
写入		
特殊权限		

有关特殊权限或高级设置，请单击“高级”。



[了解访问控制和权限](#)



Windows权限分类

- 遍历文件夹/执行文件
- 列出文件夹/读取数据
- 读取属性
- 读取扩展属性
- 创建文件/写入数据
- 创建文件夹/附加数据
- 写入属性



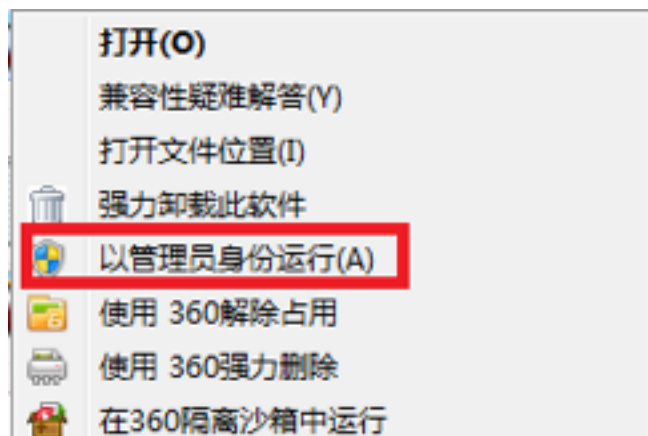
Windows权限分类

- 写入扩展属性
- 删除子文件夹及文件
- 删除
- 读取权限
- 更改权限
- 取得所有权
- 同步



Windows的权限管理

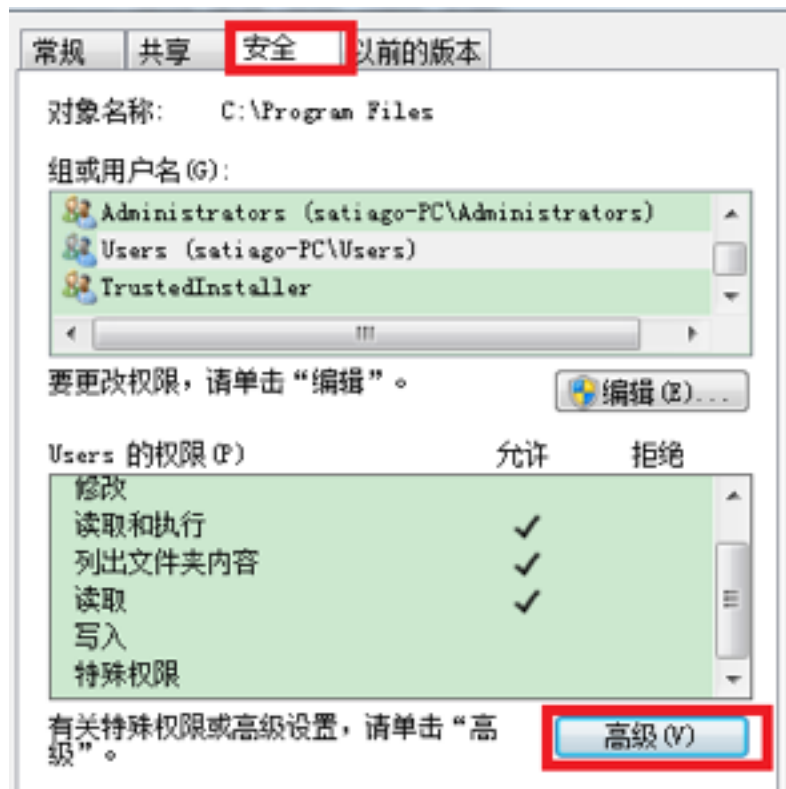
- Windows 7中对可执行程序的执行可以**按需**使用管理员权限
—最小化授权策略





Windows的权限管理

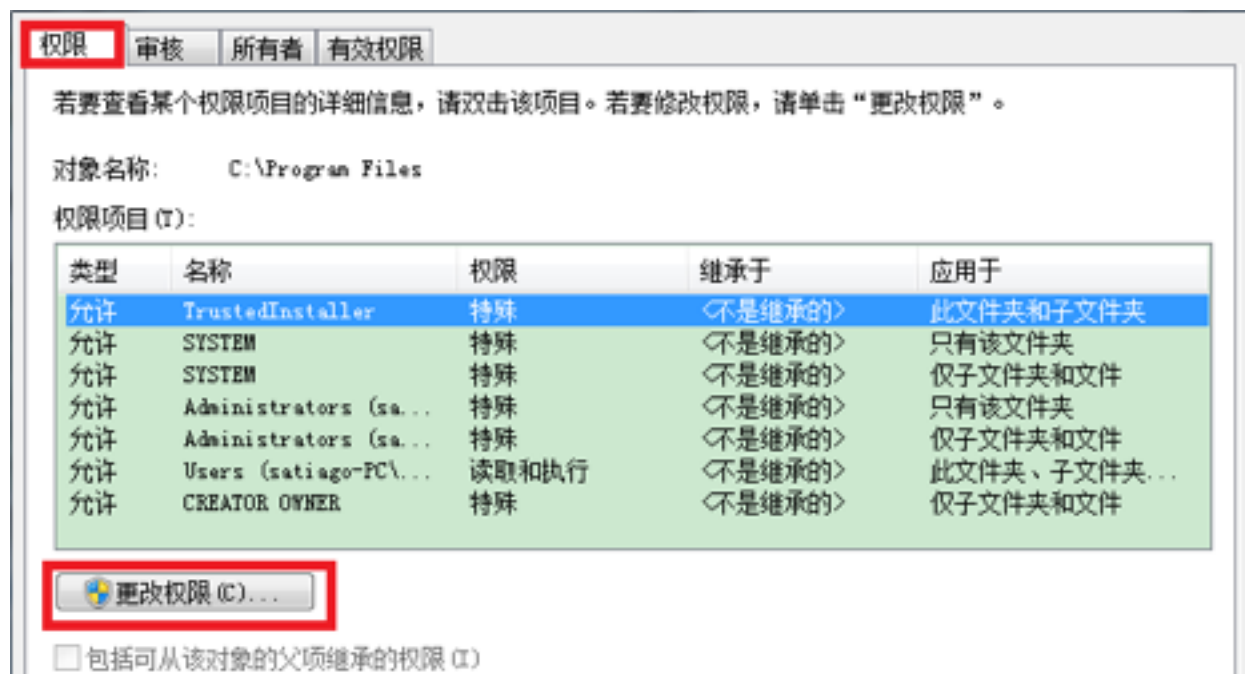
- 对文件或者文件夹的权限操作
- 在属性对话框的安全页选择高级选项





Windows的权限管理

- 更改当前文件或者文件夹的权限，并且需要管理员的用户权限。





本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



内核态 vs. 用户态

- 操作系统为了防止用户应用程序访问或破坏系统关键数据而建立的一种指令运行模式
 - 操作系统级别的服务
 - 设备驱动程序
- 可以访问到所有系统物理内存空间和CPU指令
 - 高权限
- ring 0级别
- 无法直接访问操作系统级别服务和硬件设备
- 有限的内存空间访问和CPU指令访问
- ring 3级别



本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



容易混淆的一些概念

- Windows API Functions
 - 有文档记录，Windows编程接口中可被调用的子例程。例如：CreateProcess, CreateFile, GetMessage
- 原生系统服务（系统调用）
 - 没有文档记录，可在用户态调用的Windows编程接口。例如：NtCreateUserProcess
- 内核支持函数（例程，routines）
 - 仅能在内核态调用的Windows编程接口。例如：ExAllocatePoolWithTag



什么是windows的服务

- Windows中的一些进程会在系统启动后**时刻保持运行**，提供一些不依赖于任何交互式用户的服务，通过系统的API与系统进行交互，称为windows服务(windows service)。
- Windows服务是由**三个组件**构成：
- 服务应用
- 服务控制程序 (SCP,service control program)
- 服务控制管理器 (SCM,service control manager)



- 服务应用也是简单的windows可执行程序（GUI风格或者控制台风格），加上一些代码来接收SCM的命令，并且把状态反馈给SCM。
- 安装服务应用程序时，系统调用CreateService来注册服务，SCM为该服务在注册表HKLM\SYSTEM\CurrentControlSet\Service下创建一个注册表键。



- 启动该服务应用通过调用StartService函数实现,
- 服务启动的注册表键值有以下四种:
- SERVICE_BOOT_START(0)(内核驱动初始化)
- SERVICE_SYSTEM_START(1)(内核初始化后加载)
- SERVICE_AUTO_START(2)(SCM启动之后加载运行)
- SERVICE_DEMAND_START(3)(根据需求加载运行)



服务控制程序

- 服务控制程序是标准的Windows应用程序，用到了XSCM服务管理函数，这些函数包括：
- CreateService()
- OpenService()
- StartService()
- ControlService()
- QueryServiceStatus()
- DeleteService()



- 使用之前列举的函数必须首先调用 OpenSCManager 函数，打开一个 SCM 的通信通道。
- 当 SCP 利用 CreateService 函数来创建一个服务时，会指定一个安全描述符，SCM 将此安全描述符与服务相关联，保证访问的安全性。
- SCP 可以请求的访问方式有：
 - 查询服务的状态
 - 配置服务，停止服务及启动服务



- 服务控制管理器的可执行文件是
\\windows\\system32\\Service.exe,该程序也是作为一个控制台程序来运行的。
- 服务控制管理器的启动函数SvcCtrlMain由Winlogon进程引导启动。并创建同步事件SvcCtrlEvent_A3752DX初始化为无信号状态。
- 服务控制程序与服务控制管理器之间建立对话使用OpenSCManager函数。

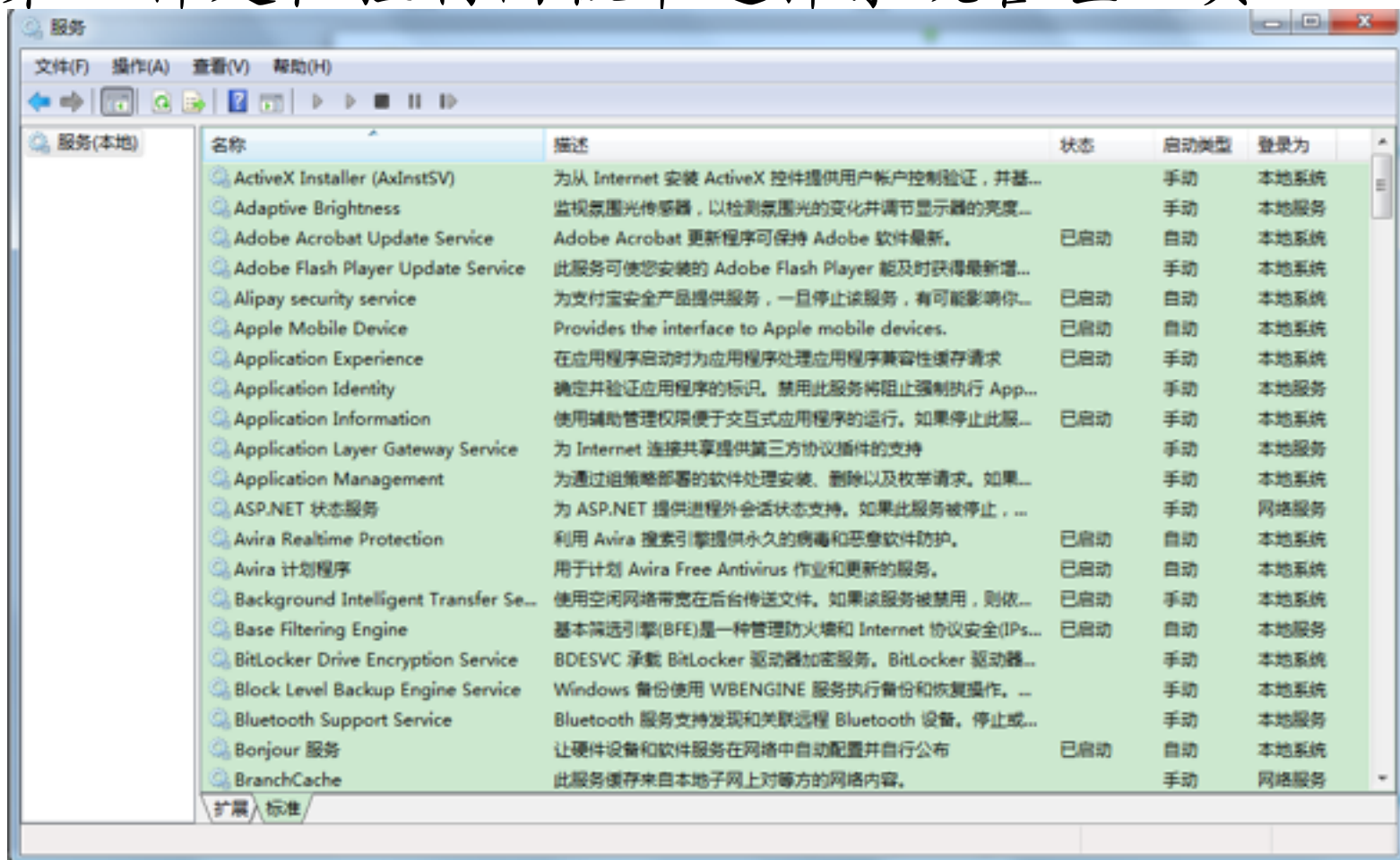


- SvcCtrlMain的工作流程
- 调用ScCreateServiceDB函数，建立SCM内部的服务数据库，并扫描注册表获取服务信息。
- 调用ScAutoStartService函数来启动被指定为“自动启动”的服务。
- 调用ScStartService函数来启动其他指定的服务



查询服务状态的方法

- 第一种是在控制面板中选择系统管理工具





查询服务状态的方法

- 第二种是在控制台输入指令tasklist /svc

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\docsatiago>tasklist /svc

映像名称                                PID  服务
=====
System Idle Process                    0    暂缺
System                                4    暂缺
smss.exe                               380   暂缺
csrss.exe                              552   暂缺
wininit.exe                            612   暂缺
csrss.exe                              620   暂缺
services.exe                          660   暂缺
lsass.exe                              680   KeyIso, SamSs, VaultSvc
lsm.exe                                688   暂缺
winlogon.exe                           808   暂缺
svchost.exe                            844   DcomLaunch, PlugPlay, Power
TrueSuiteService.exe                  916   FPLService
ibmpmsvc.exe                           964   IBMPMSVC
svchost.exe                            1020  RpcEptMapper, RpcSs
svchost.exe                            1100  Audiosrv, Dhcp, eventlog,
                                          HomeGroupProvider, lnhosts, wscsvc
svchost.exe                            1152  AudioEndpointBuilder, CscService, Netman,
                                          半:
```



本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



进程 (process)

- 可执行程序 \neq 进程
 - 可执行程序：静态，文件级别
 - 由一系列计算机指令构成
 - 进程：动态
 - 进程唯一标识 (PID)
 - 私有虚拟地址空间
 - 访问令牌
 - 主体：用户、用户组
 - 访问控制策略 (DACL)



线程 (thread)

- 线程包含于进程中
 - Windows操作系统的指令执行最小调度单位
 - 线程唯一标识 (TID)
 - 同一进程内的多个线程可以实现数据共享
- 多线程间执行切换需要系统内核调度
 - 资源消耗较大
 - Windows实现了2种线程
 - 纤程 (fiber)
 - 用户态调度 (user-mode scheduling, UMS)



作业 (jobs)

- Windows平台特有的一种进程模型
 - 基本设计思想：实现相似功能进程的分组管理和调度
 - 类似UNIX系统上的进程树模型



本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



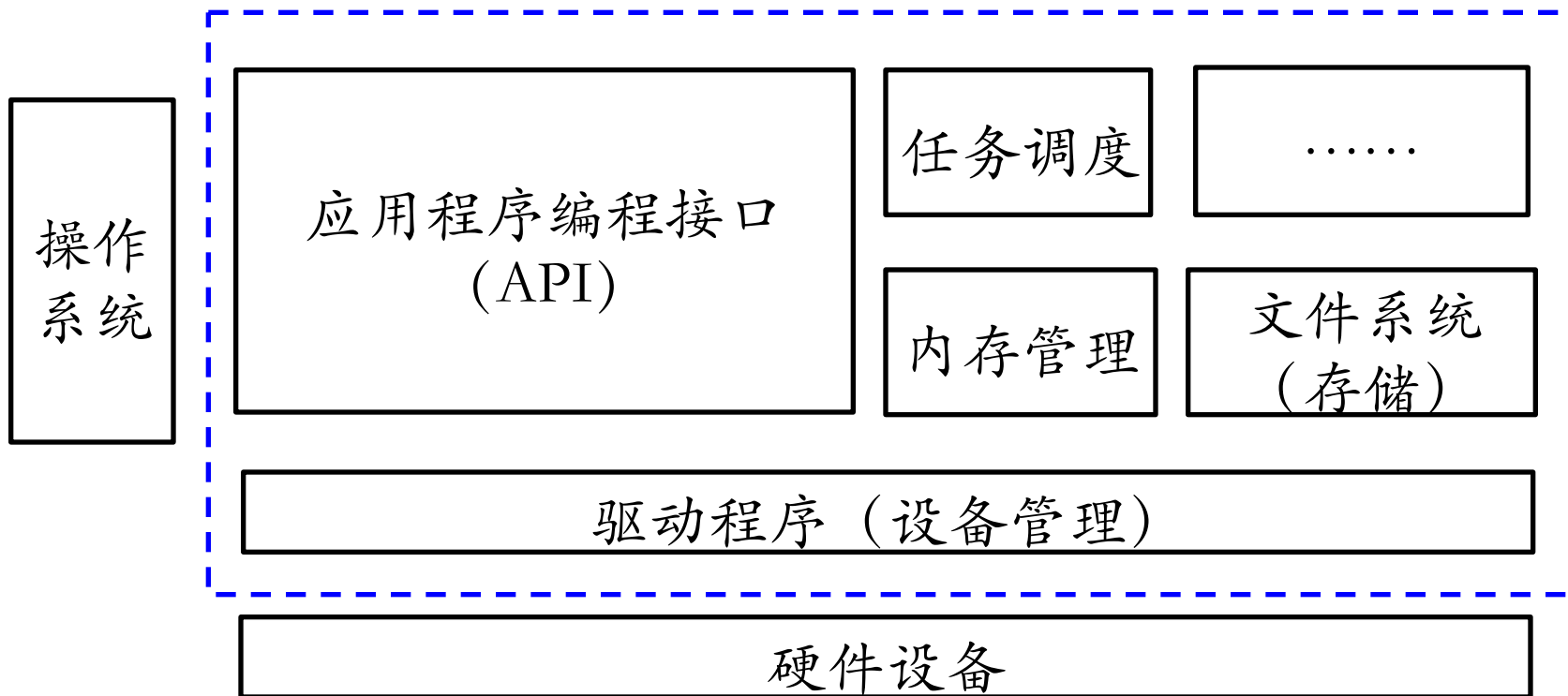
系统的硬件设备

- 一般来讲，电脑的硬件设备分为以下几种：

- 主板
- CPU
- 内存
- 界面卡（显卡，声卡）
- 输入设备（键盘，鼠标）
- 输出设备（显示器，扬声器）
- 内置存储器（硬盘）
- 外置存储器（U盘，CD-ROM）
- 网卡（有线、无线）
- 散热器
- 电源
- 机箱



硬件设备与操作系统的交互





硬件抽象层 (HAL)

- HAL是一个可加载的，内核模式的模块，它提供了针对Windows运行的硬件平台的底层接口同时隐藏硬件的相关细节，使得Windows系统的可移植性成为可能。
- X86平台的HAL有两种：
 - Halacpi.dll支持高级配置和电源接口(ACPI)PC
 - Halmacpi.dll支持多处理器ACPI PC



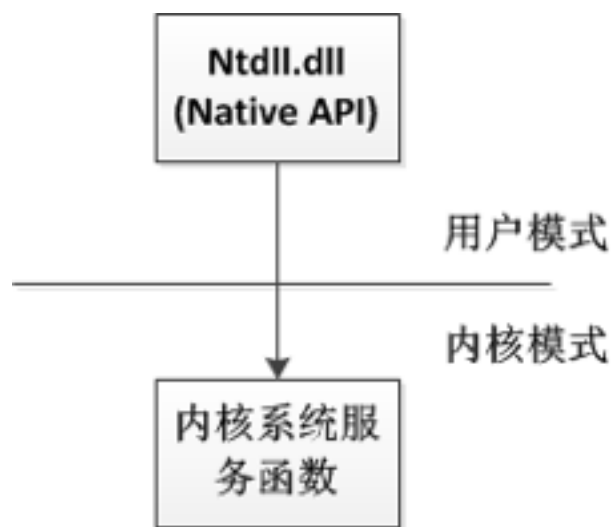
驱动程序

- 设备硬件与系统进行交互需要通过设备驱动程序，该程序文件以sys的文件类型存在于系统中，并且运行于内核中。
- 设备驱动程序有以下几种类型：
 - 硬件设备驱动程序
 - 文件系统驱动程序
 - 文件系统过滤驱动程序
 - 网络重定向和服务
 - 协议驱动程序
 - 内核流式过滤器驱动程序



Ntdll.dll

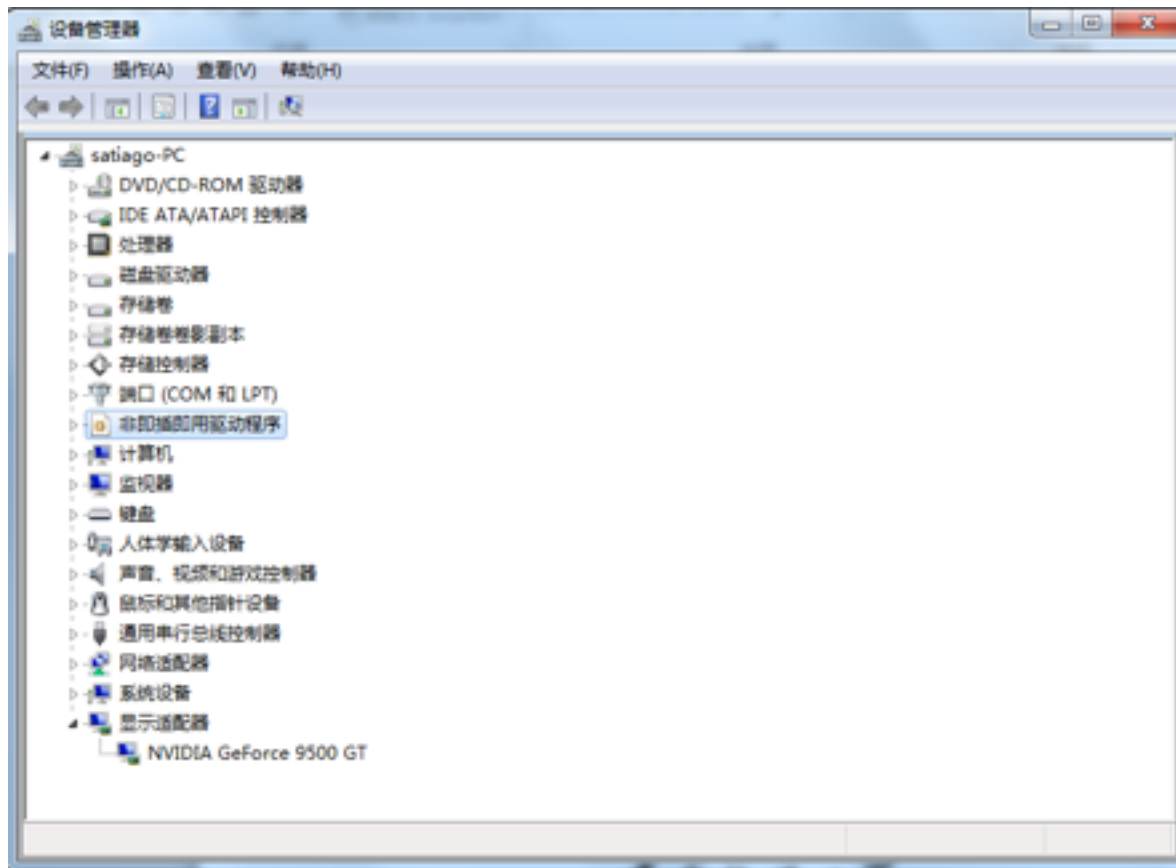
- Ntdll.dll是一个特殊的系统支持库，不仅可以在用户模式下调用接口函数执行系统服务，而且可以切换到内核模式下，调用系统服务分发器（system service dispatcher）执行内核系统服务。





Windows的设备管理器

在“我的电脑”右键属性即可找到。





本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



- 文件系统格式 (File system format) 定义了文件数据在存储介质上的存储方式，文件格式也体现了文件的安全性和对文件存储的大小限制。
- 当前windows支持以下几种文件格式：
 - CDFS
 - UDF
 - FAT12,FAT16,FAT32
 - exFAT
 - NTFS



- CDFS是指CD-ROM文件系统，是一个只读文件系统驱动程序，驱动文件路径为
\\windows\\system32\\Drivers\\Cdfs.sys。它支持ISO-9660格式以及Joliet磁盘格式的超集。当两种格式同时存在时，采用Joliet格式
- CDFS有以下限制：
 - 单个文件大小最大为4GB
 - 最多65535个目录
- 目前业界已经采用UDF(通用磁盘格式) 作为只读介质的标准。



- UDF(通用磁盘格式)是与OSTA UDF兼容的，该格式对于像CD-R和DVD-R/RW之类的格式进行了扩展。
- UDF是ISO-13346格式的一个子集，比CDFS更加灵活。
- UDF支持最新的2.60版本，当使用2.50版本时，UDF的驱动程序(Udfs.sys)支持DVD,CD等的可读写操作，而2.60版本仅仅支持只读操作。



- UDF文件格式具有以下特点
- 目录和文件名可以达到254 ASCII字符或者127 UNICODE字符长。
 - 文件可以是稀疏的
 - 文件的大小用64位来指定
 - 支持ACLs(访问控制列表)
 - 支持交换数据流



FAT12,FAT16,FAT32

- Windows对于FAT文件系统给的支持主要是为了能够从其他版本升级过来，也保证在多引导系统中与其他的操作系统保持兼容。作为一种软盘格式，文件驱动程序位于
`\windows\system32\drivers\Fastfat.sys`。

引导扇区	文件分配表1	文件分配表2 (复本)	根目录	其他的目录 和所有文件
------	--------	----------------	-----	----------------

FAT格式的组织



FAT12,FAT16,FAT32

- 每一种FAT格式的名称都包含一个数值，指明该格式用于标示磁盘上的簇所需要的位数。Windows使用的簇大小是从512字节到8KB。
- FAT12的12位簇限定了一个分区最多只能存储4096簇，这就限定了一个FAT12卷的大小最多为32MB。Windows使用FAT12作为所有5英寸软盘和3.5英寸软盘的格式。



FAT12,FAT16,FAT32

- FAT16使用16位的簇标识符，它可以处理65536个簇。Windows上，FAT16的簇大小从512字节到64KB,这限定了FAT16卷的大小最多只能是4GB。

Volume Size	Default Cluster Size
<8 MB	Not supported
8 MB–32 MB	512 bytes
32 MB–64 MB	1 KB
64 MB–128 MB	2 KB
128 MB–256 MB	4 KB
256 MB–512 MB	8 KB
512 MB–1,024 MB	16 KB
1 GB–2 GB	32 KB
2 GB–4 GB	64 KB
>16 GB	Not supported



FAT12,FAT16,FAT32

- FAT32是最新定义的基于FAT的文件系统格式，FAT32使用32位簇标识符，但是保留了高四位，所以只有28为簇标识符。FAT簇大小可以到32KB。Windows限制新的FAT32卷最大只能为32GB。

Partition Size	Default Cluster Size
<32 MB	Not supported
32 MB–64 MB	512 bytes
64 MB–128 MB	1 KB
128 MB–256 MB	2 KB
256 MB–8 GB	4 KB
8 GB–16 GB	8 KB
16 GB–32 GB	16 KB
>32 GB	Not supported



- exFAT (Extended File Allocation Table file system) 扩展FAT,又叫做FAT64,该文件格式是特别为U盘等闪存定制的。簇最大可到32MB。

Volume Size	Default Cluster Size
<7 MB	Not supported
7 MB–256 MB	4 KB
256 MB–32 GB	32 KB
32 GB–256 TB	128 KB
>256 TB	Not supported



- NTFS文件系统是windows的原生文件系统格式。NTFS使用64位簇编号。然而，windows限制NTFS卷的大小为“可用32位簇来寻址”，这稍小于256TB。NTFS限制文件的最大尺寸为16TB。

Volume Size	Default Cluster Size
<7 MB	Not supported
7 MB–16 TB	4 KB
16 TB–32 TB	8 KB
32 TB–64 TB	16 KB
64 TB–128 TB	32 KB
128 TB–256 TB	64 KB



- NTFS 包含了许多高级特性
 - 文件和目录的安全性
 - 磁盘配额
 - 文件压缩
 - 基于目录的符号链接
 - 加密
 - 可恢复性



本章内容提要

- 用户、用户组和权限管理
- 内核态 vs. 用户态
- 服务、函数和例程
- 进程、线程和作业
- 设备管理
- 文件系统基础与分类
- 注册表



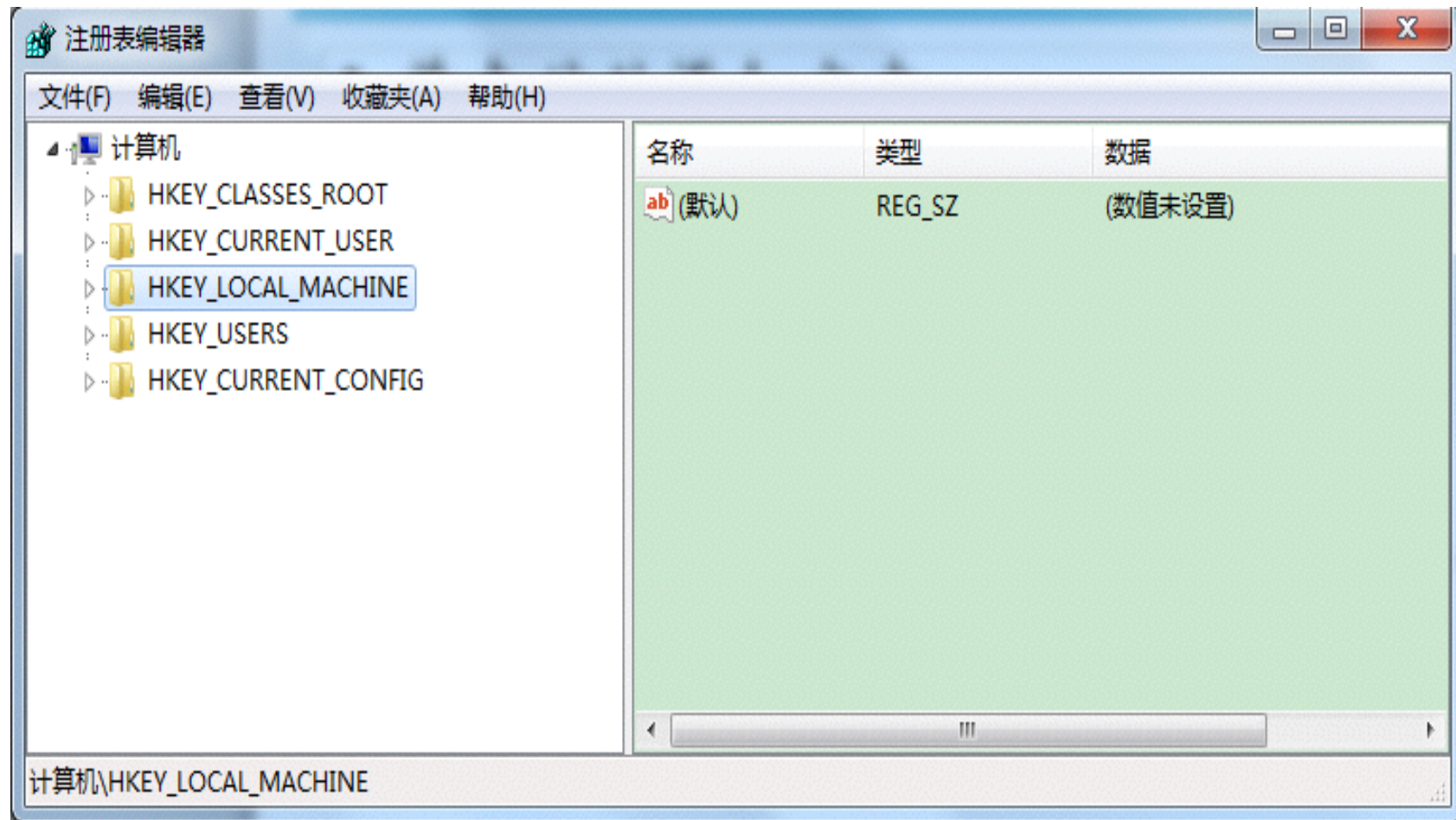
什么是注册表

- 注册表在windows系统的配置和控制方面扮演了一个非常关键的角色，它既是系统全局设置的存储仓库，也是每个用户的设置信息的存储仓库。
- 可编辑注册表的工具：Regedit.exe,该工具支持注册表的搜索，导入和导出和一些安全属性编辑功能。打开regedit需要在开始菜单中搜索或者在控制台输入指令。

```
Microsoft Windows [版本 6.1.7600]  
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。  
C:\Users\santiago>regedit
```



注册表的配置工具





- 在引导过程中，系统读取有关的设置信息，指定应该加载的设备驱动程序，以及子系统的配置和调整系统的行为。
- 在登陆过程中，windows组件从注册表中读取到每个用户的参数选择。
- 应用程序启动过程中读取系统全局范围的设置，可选安装的组件列表和许可数据，还读取每个用户的设置信息。



注册表的数据类型

- REG_NONE
—没有值的类型
- REG_SZ
—固定长度的UNICODE字符串
- REG_EXPAND_SZ
—可变长度的UNICODE字符串，可以有内嵌的环境变量
- REG_BINARY
—任意长度的二进制数据



注册表的数据类型

- REG_DWORD
—32位整数
- REG_DWORD_BIG_ENDIAN
—32位整数，高字节在前
- REG_LINK
—UNICODE符号链接



注册表的数据类型

- REG_MULTI_SZ
—以NULL结尾的UNICODE字符串的数组
- REG_RESOURCE_LIST
—硬件资源描述
- REG_FULL_RESOURCE_DESCRIPTOR
—硬件资源描述
- REG_RESOURCE_REQUIREMENTS_LIST
—资源需求



注册表的数据类型

- REG_QWORD
—64位整数
- REG_QWORD_BIG_ENDIAN
—64位整数，高字节在前



注册表的逻辑结构

- HKEY_CURRENT_USER
 - 存储一些与当前登录用户有关联的数据
- HKEY_USER
 - 存储有关该机器上所有帐户的信息
- HKEY_CLASSES_ROOT
 - 存储文件关联和对象模型的对象注册信息



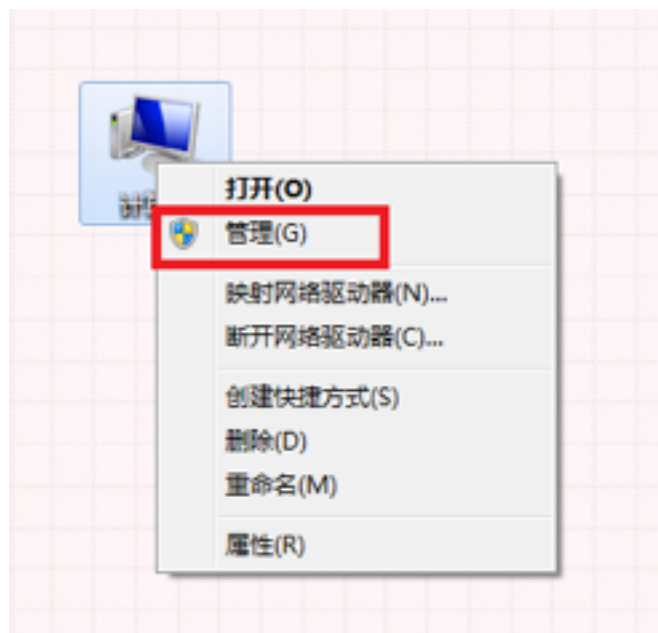
注册表的逻辑结构

- HKEY_LOCAL_MACHINE
—存储与系统有关的信息
- HKEY_PERFORMANCE_DATA
—存储与性能有关的信息
- HKEY_CURRENT_CONFIG
—存储关于当前硬件配置的一些信息



- 实验一 通过windows界面对用户进行添加，删除等操作

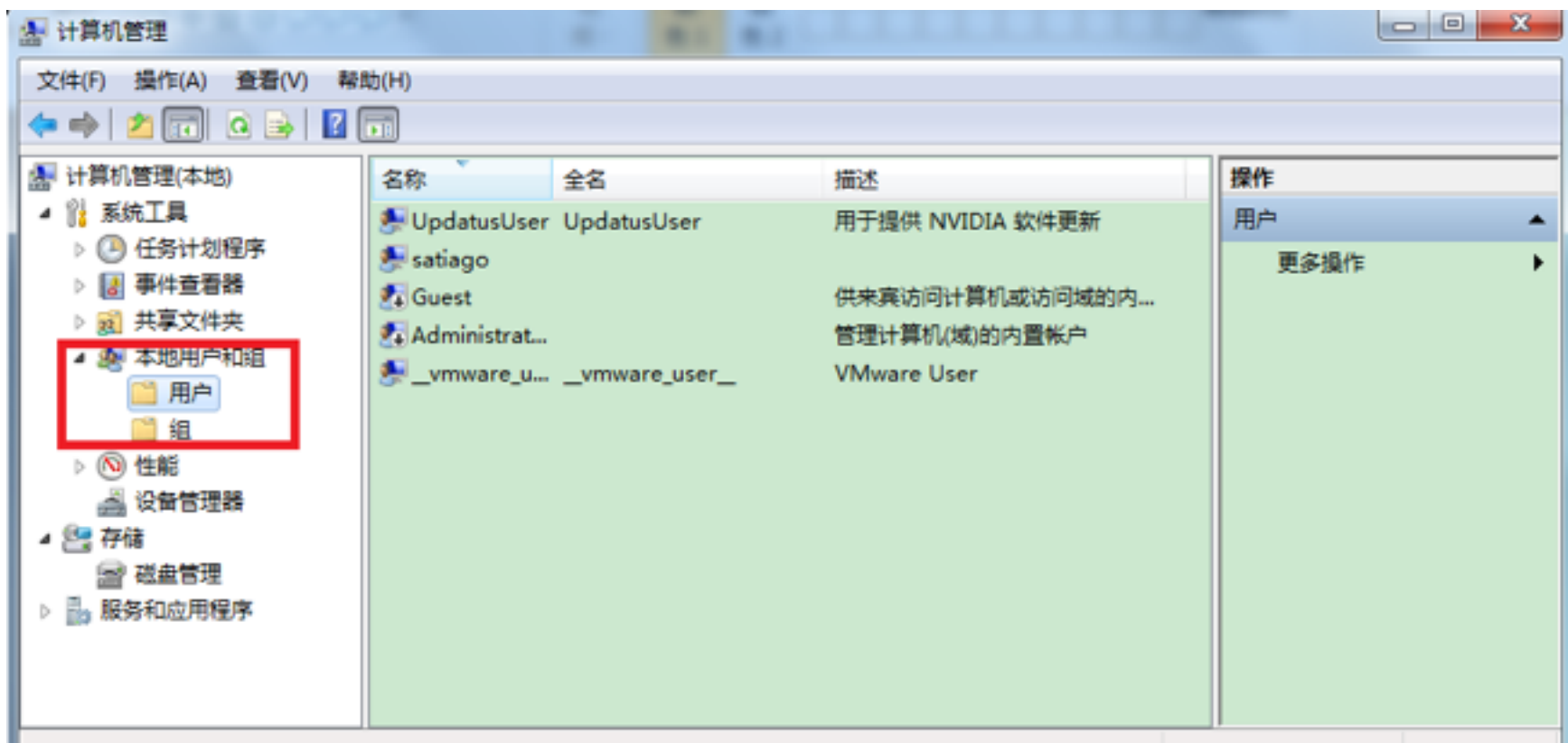
—右键“我的电脑”，打开计算机管理界面





课内实验

—如图所示，之后在“用户”文件夹点击右键，选择“新用户”





课内实验

—如图，填写用户名和密码后点击创建就可以添加新用户

新用户

用户名 (U):

全名 (F):

描述 (D):

密码 (P):

确认密码 (C):

☒ 用户下次登录时须更改密码 (M)

☐ 用户不能更改密码 (S)

☐ 密码永不过期 (W)

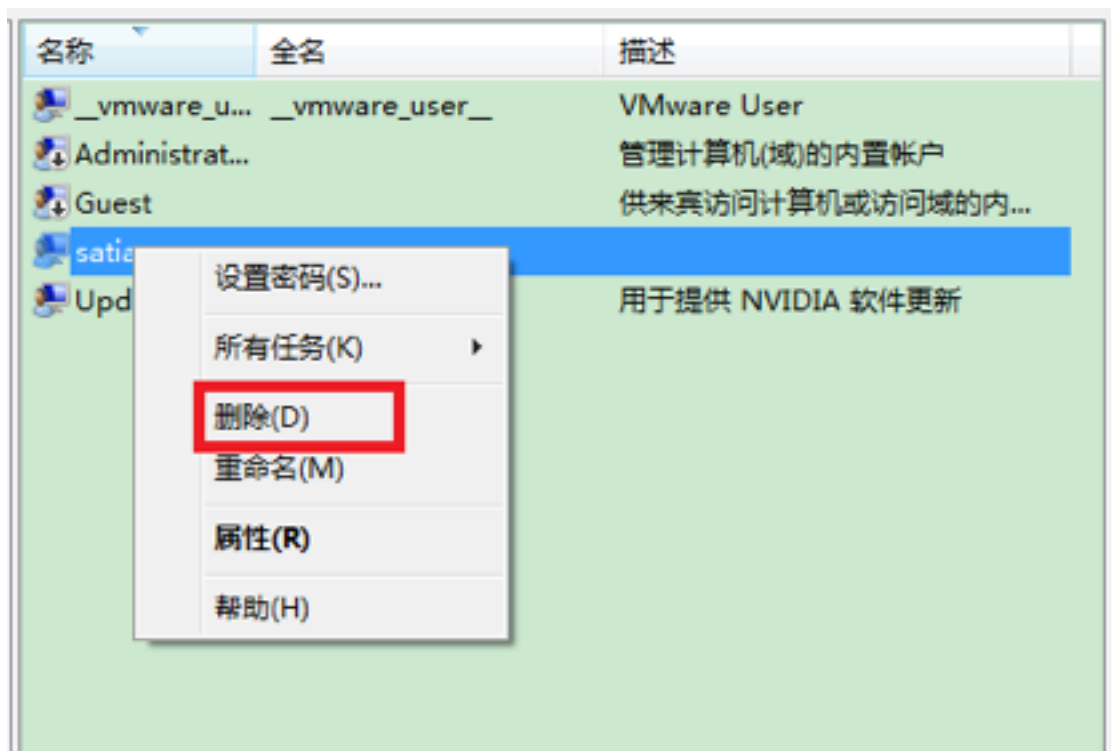
☐ 帐户已禁用 (D)

帮助 (H) 创建 (E) 关闭 (O)



课内实验

—删除用户时同理，在选择的用户点击右键选择删除即可。

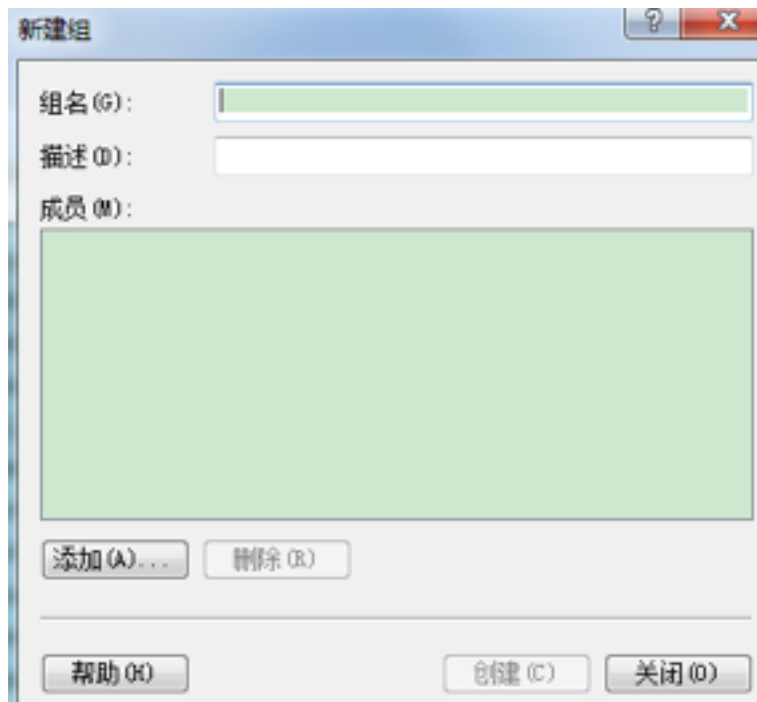




课内实验

- 实验二 通过windows界面对用户组进行添加，删除等操作

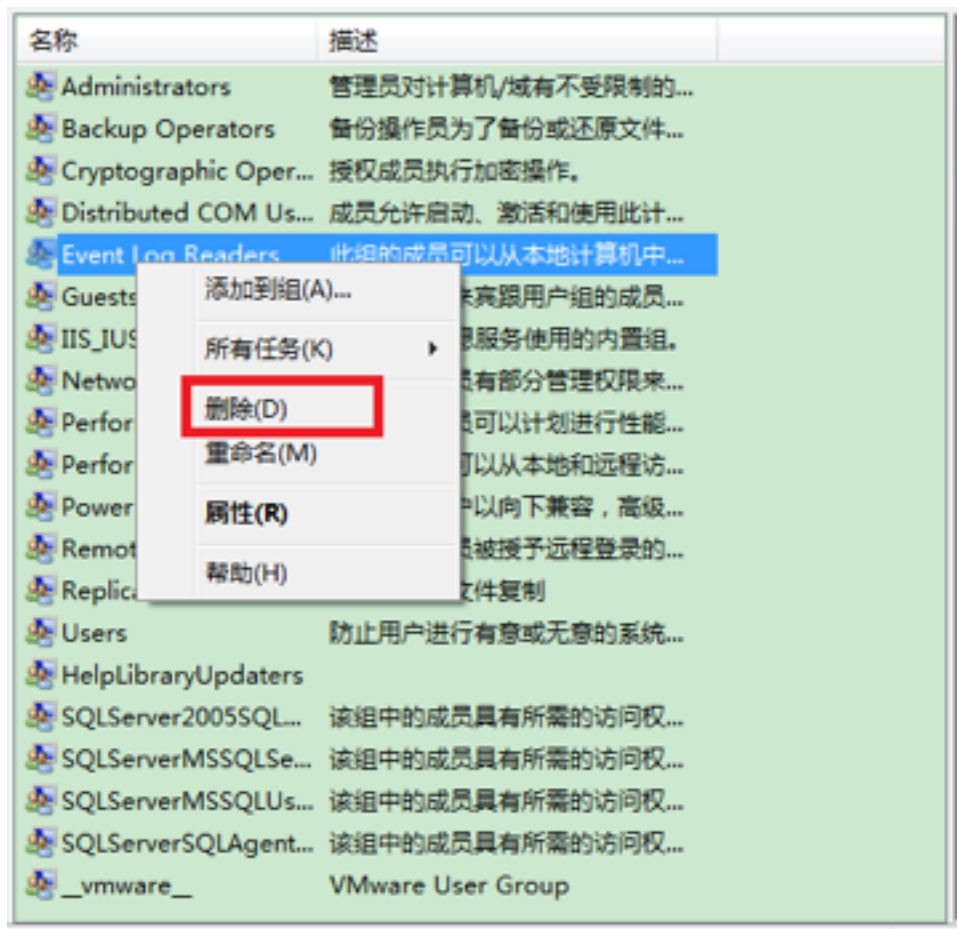
—填写组名和成员，点击创建





课内实验

—删除用户组时同理，在选择的用户组点击右键选择删除即可。





- 实验三 通过命令行对用户进行添加，删除操作

—添加用户的命令是net user

—如图为命令的语法说明

```
C:\Users\santiago>net user /?
```

此命令的语法是:

```
NET USER
```

```
[username [password ! *] [options]] [/DOMAIN]
```

```
username {password ! *} /ADD [options] [/DOMAIN]
```

```
username [/DELETE] [/DOMAIN]
```

```
username [/TIMES:{times ! ALL}]
```



课内实验

- 添加用户，删除用户

```
C:\Windows\system32>net user 111 222 /add
命令成功完成。

C:\Windows\system32>net user

\\SANTIAGO-PC 的用户帐户

-----
__vware_user__      111      Administrator
Guest               satiago   UpdatusUser
命令成功完成。

C:\Windows\system32>net user 111 /delete
命令成功完成。

C:\Windows\system32>net user

\\SANTIAGO-PC 的用户帐户

-----
__vware_user__      Administrator      Guest
satiago             UpdatusUser
命令成功完成。

C:\Windows\system32>
```



- 实验四 通过命令行对用户组进行添加，删除操作
 - 添加用户组的命令是net localgroup
 - 如图为命令的语法说明

```
C:\Windows\system32>net localgroup /?  
此命令的语法是:  
  
NET LOCALGROUP  
[groupname [/COMMENT:"text"]] [/DOMAIN]  
    groupname </ADD [/COMMENT:"text"] : /DELETE> [/DOMAIN]  
    groupname name [...] </ADD : /DELETE> [/DOMAIN]
```



课内实验

```
C:\Windows\system32>net localgroup 111 /add  
命令成功完成。
```

```
C:\Windows\system32>net localgroup  
\\SANTIAGO-PC 的别名
```

```
* _vmware_  
111  
*Administrators  
*Backup Operators  
*Cryptographic Operators  
*Distributed COM Users  
*Event Log Readers  
*Guests  
*HelpLibraryUpdaters  
*IIS_IUSRS  
*Network Configuration Operators  
*Performance Log Users  
*Performance Monitor Users  
*Power Users  
*Remote Desktop Users  
*Replicator  
*SQLServer2005SQLBrowserUser$SANTIAGO-PC  
*SQLServerMSSQLServerADHelperUser$SANTIAGO-PC  
*SQLServerMSSQLUser$santiago-PC$SQLEXPRESS  
*SQLServerSQLAgentUser$SANTIAGO-PC$SQLEXPRESS  
*Users  
命令成功完成。
```

```
C:\Windows\system32>net localgroup 111 /delete  
命令成功完成。
```

```
C:\Windows\system32>net localgroup  
\\SANTIAGO-PC 的别名
```

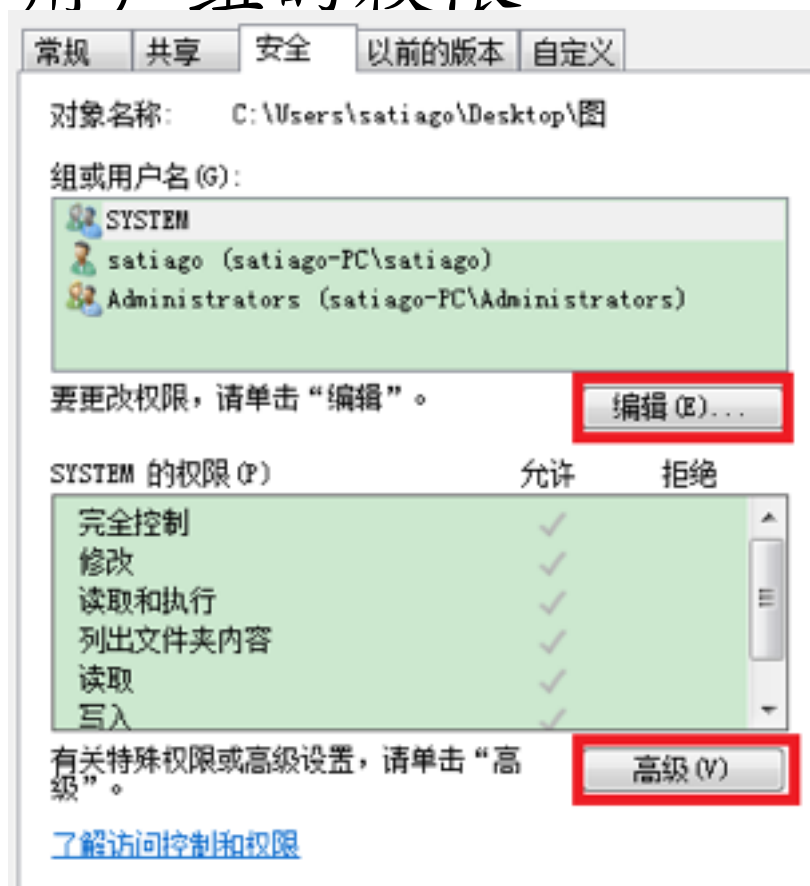
```
* _vmware_  
*Administrators  
*Backup Operators  
*Cryptographic Operators  
*Distributed COM Users  
*Event Log Readers  
*Guests  
*HelpLibraryUpdaters  
*IIS_IUSRS  
*Network Configuration Operators  
*Performance Log Users  
*Performance Monitor Users  
*Power Users  
*Remote Desktop Users  
*Replicator  
*SQLServer2005SQLBrowserUser$SANTIAGO-PC  
*SQLServerMSSQLServerADHelperUser$SANTIAGO-PC  
*SQLServerMSSQLUser$santiago-PC$SQLEXPRESS  
*SQLServerSQLAgentUser$SANTIAGO-PC$SQLEXPRESS  
*Users  
命令成功完成。
```



• 实验五 修改用户或者用户组的权限

—任意选择文件或者文件夹点击右键属性即可得到右图的权限修改界面

—点击图上的“编辑”或者“高级”都可以修改权限





课内实验

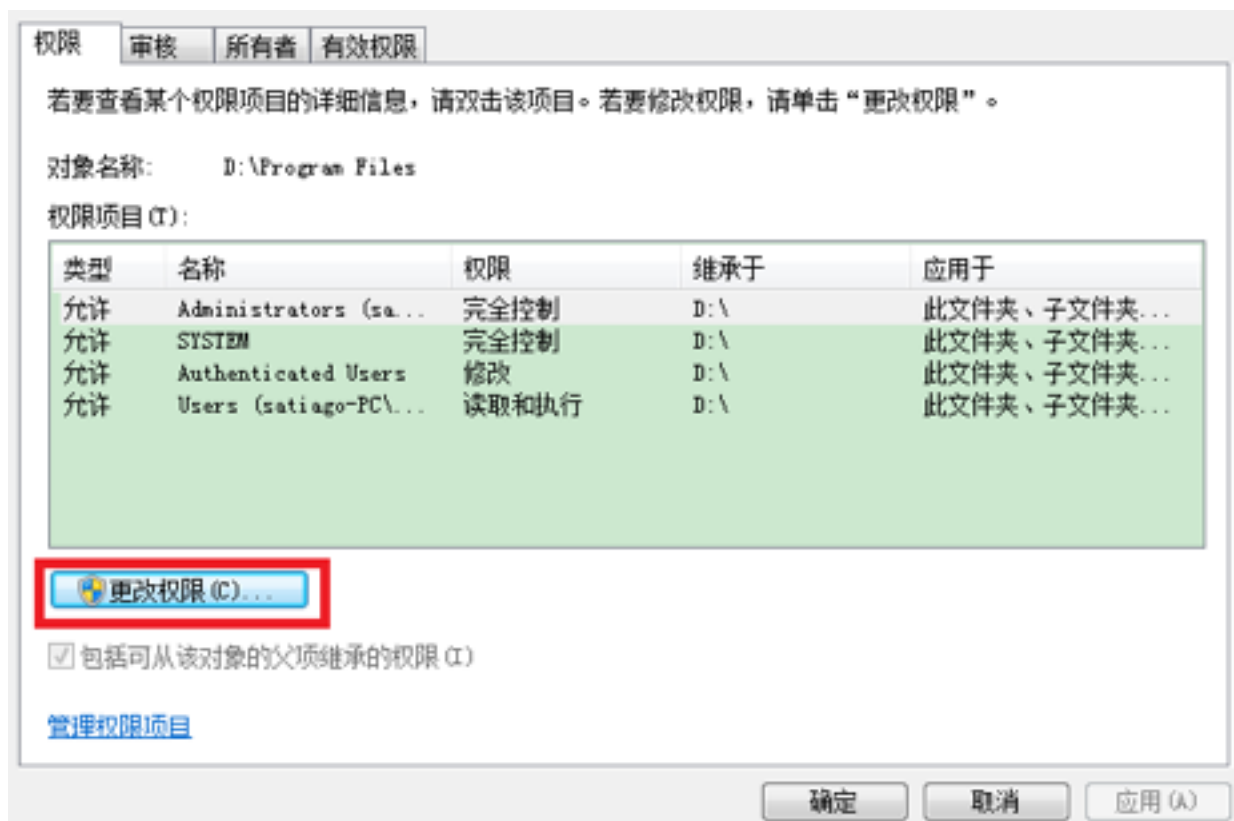
— 点击“编辑”如图可以对权限进行修改





课内实验

—点击“高级”如图可以对权限进行修改





虚拟机软件VirtualBox的使用

- 基础概念
- 功能特性
- 虚拟机的生命周期管理
 - 创建、编辑、导入/导出、删除
- 基于虚拟机的常见实验需求实现
 - 备份与恢复
 - 虚拟网络（拓扑）环境
 - 宿主机与宾客机之间的共享
 - 数据、设备（USB、网卡、声卡、显卡等）



课后实验

- 把你自己的笔记本拆卸再组装还原回去
 - 拆卸成果拍照
 - CPU、内存、硬盘、网卡、显卡



课后实验

- 使用ProcessExplorer查看系统上正在运行的进程列表和进程详情
 - 一找出系统进程和用户进程
 - 一查看一个进程中包含哪些信息
 - 一基于互联网学习这些进程详情的概念



课后实验

- 在Windows 7系统上
 - 对C:\windows\system32\osk.exe重命名
 - 对C:\windows\system32\osk.exe剪切