北京大学网络攻防技术与实践课程

4. Windows操作系统及其安全机制

诸葛建伟

zhugejianwei@icst.pku.edu.cn

北京大学计算机研究所信安中心

内容

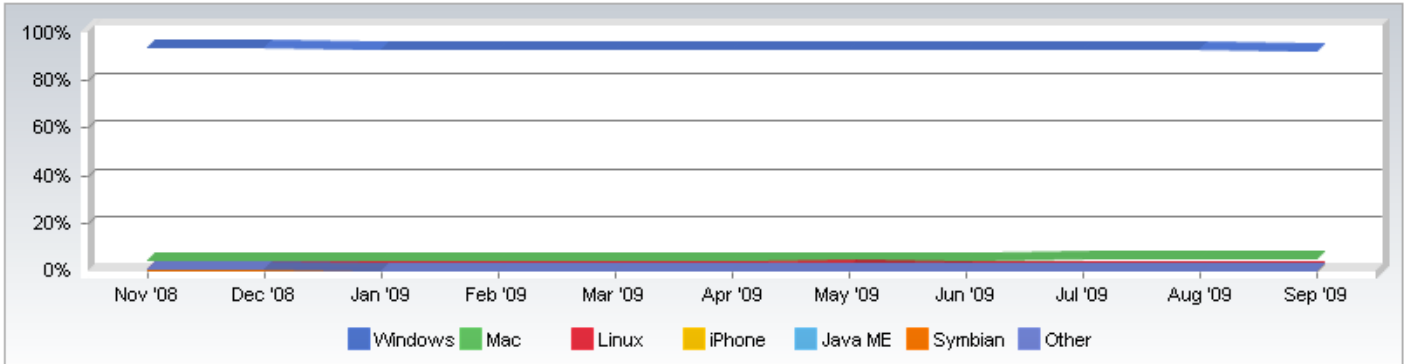
1. Windows操作系统简介
2. Windows NT 5.x的系统结构
3. Windows NT 5.x的网络结构
4. Windows NT 5.x的安全结构

桌面操作系统市场份额

Top Operating System Share Trend

SHARE RSS Click here to get our market share updates on Twitter November, 2008 to September, 2009

Timeframe Export To Options Help



Month	Windows	Mac	Linux	iPhone	Java ME	Symbian	Other
November, 2008	94.41%	4.12%	0.91%	0.15%	0.00%	0.00%	0.40%
December, 2008	93.90%	4.45%	0.98%	0.18%	0.00%	0.01%	0.48%
January, 2009	93.66%	4.71%	0.90%	0.20%	0.22%	0.07%	0.24%
February, 2009	93.74%	4.55%	0.98%	0.19%	0.23%	0.08%	0.23%
March, 2009	93.51%	4.69%	1.01%	0.20%	0.23%	0.11%	0.25%
April, 2009	93.45%	4.64%	1.06%	0.22%	0.25%	0.11%	0.28%
May, 2009	93.18%	4.73%	1.17%	0.25%	0.25%	0.12%	0.30%
June, 2009	93.39%	4.70%	1.00%	0.27%	0.25%	0.12%	0.27%
July, 2009	93.04%	4.86%	1.05%	0.30%	0.29%	0.14%	0.31%
August, 2009	93.06%	4.87%	0.94%	0.33%	0.31%	0.14%	0.36%
September, 2009	92.77%	5.12%	0.95%	0.35%	0.30%	0.15%	0.36%

- **http://marketshare.hitslink.com 数据.**

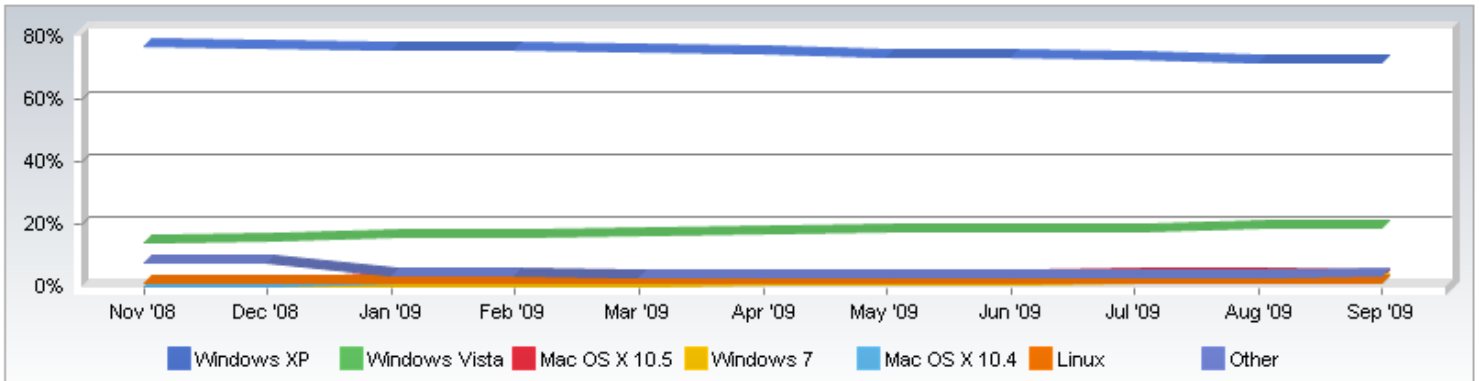
桌面操作系统市场份额(2)

Top Operating System Share Trend

SHARE RSS Click here to get our market share updates on Twitter

November, 2008 to September, 2009

Timeframe Export To Options Help



Month	Windows XP	Windows Vista	Mac OS X 10.5	Windows 7	Mac OS X 10.4	Linux	Other
November, 2008	77.18%	14.28%	0.00%	0.00%	0.00%	0.91%	7.63%
December, 2008	76.60%	14.90%	0.00%	0.02%	0.00%	0.98%	7.50%
January, 2009	75.86%	15.72%	2.57%	0.13%	1.19%	0.90%	3.64%
February, 2009	75.68%	15.94%	2.74%	0.22%	1.19%	0.98%	3.25%
March, 2009	75.02%	16.44%	2.96%	0.26%	1.17%	1.01%	3.14%
April, 2009	74.47%	17.00%	3.03%	0.31%	1.11%	1.06%	3.03%
May, 2009	73.72%	17.36%	3.17%	0.56%	1.08%	1.17%	2.93%
June, 2009	73.62%	17.58%	3.22%	0.75%	1.04%	1.00%	2.80%
July, 2009	72.93%	17.90%	3.42%	0.89%	1.03%	1.05%	2.77%
August, 2009	71.79%	18.80%	3.45%	1.18%	0.99%	0.94%	2.84%
September, 2009	71.51%	18.62%	3.03%	1.52%	0.96%	0.95%	3.42%

服务器操作系统市场份额

- IDC市场报告
  - 2005年：Windows 在2005年首次超过Unix，成为服务器上的第一号操作系统，增长迅速的Linux 首次攀升到第三的位置
- 市场调研机构Gartner提供数据－2007年在全球发货的服务器中：
  - Windows服务器的份额已经增长到66.8%
  - Linux服务器的份额下滑到23.2%
  - Unix服务器的份额从2006年的8.1%下滑到6.8%

Windows操作系统发展轨迹

- 桌面(客户端)操作系统
  - **1990: Windows 3.x**
  - **1995-1999: Windows 95, 98, ME(4.x)**
  - **2000: Windows 2000 Pro(5.0.x)**
  - **2001: Windows XP(5.1.x)**
  - **2007: Windows Vista(6.0.x)**
  - **2009: Windows 7(6.1.x)**
- 服务器操作系统
  - **1993: Windows NT (3.x, 4.x)**
  - **2000: Windows 2000 Server(5.0.x)**
  - **2003: Windows Server 2003 (5.2.x)**
  - **2008: Windows Server 2008 (6.x)**
- **Windows NT 5.x系列操作系统**
  - **Windows 2000 Pro/Windows XP**
  - **Windows 2000 Server/Windows Server 2003**

Windows 7

- **Windows7零售版正式发布时间：10月22日**
- **Win 7比XP更安全吗？**
  - **Win7内部机制分析**
  - 安全机制优化机制研究
- 盗版已经盛行
  - 盗版机理研究
  - 盗版与正版的差异性对比分析
- 针对**Win7**的安全漏洞挖掘研究
- 推荐实践选题
  - 提供**MSDN AA Win7**正版资源
  - 盗版？

盗版名称
JUJUMAO Windows7_32位官方简体中文集成安装光盘V09.10
JUJUMAO Windows7_32位官方简体中文旗舰纯净版V09.09
JUJUMAO Windows_7_32位官方简体中文正式旗舰VHD光盘版 V09.09
JUJUMAO Windows 7 32位官方简体中文正式旗舰克隆版V09.08
JUJUMAO Windows 7 32位官方简体中文联想OEM旗舰版集成安装光盘 V09.08
电脑公司Ghost_windows 7_7600简体中文特别版
win7-MSDN-x86/X64简体中文免激活安装版
Windows7 RTM 32位小锋中文正式版
Windows7_7600微软(32位DVD)旗舰中文版
Windows 7 RTM Build 7600.16385 x86(简体中文)
Windows7_Professional_X86简体中文0929精简版
金狐Windows7_ghost适度精简优化版
远景系统Windows 7_Build7260_X86简体中文旗舰版
远景系统Windows 7_Build7231_X86简体中文旗舰版
远景系统Win7_7100 4in1DVD版
Windows7 Ultimate-x86 build-7106-小兵作品
龙行天下windows7Ultimate 7000简体中文ghost版
windows7小锋精简优化中文版

微软首度针对Windows 7修补安全漏洞

搜狐 - 2009年10月9日

【搜狐IT消息】（文/刘瑞刚）据中国台湾媒体报道，微软将在美国时间下周二发布13个安全性更新，并首次针对尚未上市的操作系统Windows 7发布安全修补程序。 ...

微软即将修复Win7第一个严重安全漏洞 腾讯网

微软将修复Windows 7高危漏洞 网易

微软下周二发布13个补丁 修复34个安全漏洞 中新网

内容

1. Windows操作系统简介
2. Windows NT 5.x的系统结构
3. Windows NT 5.x的网络结构
4. Windows NT 5.x的安全结构

推荐书籍

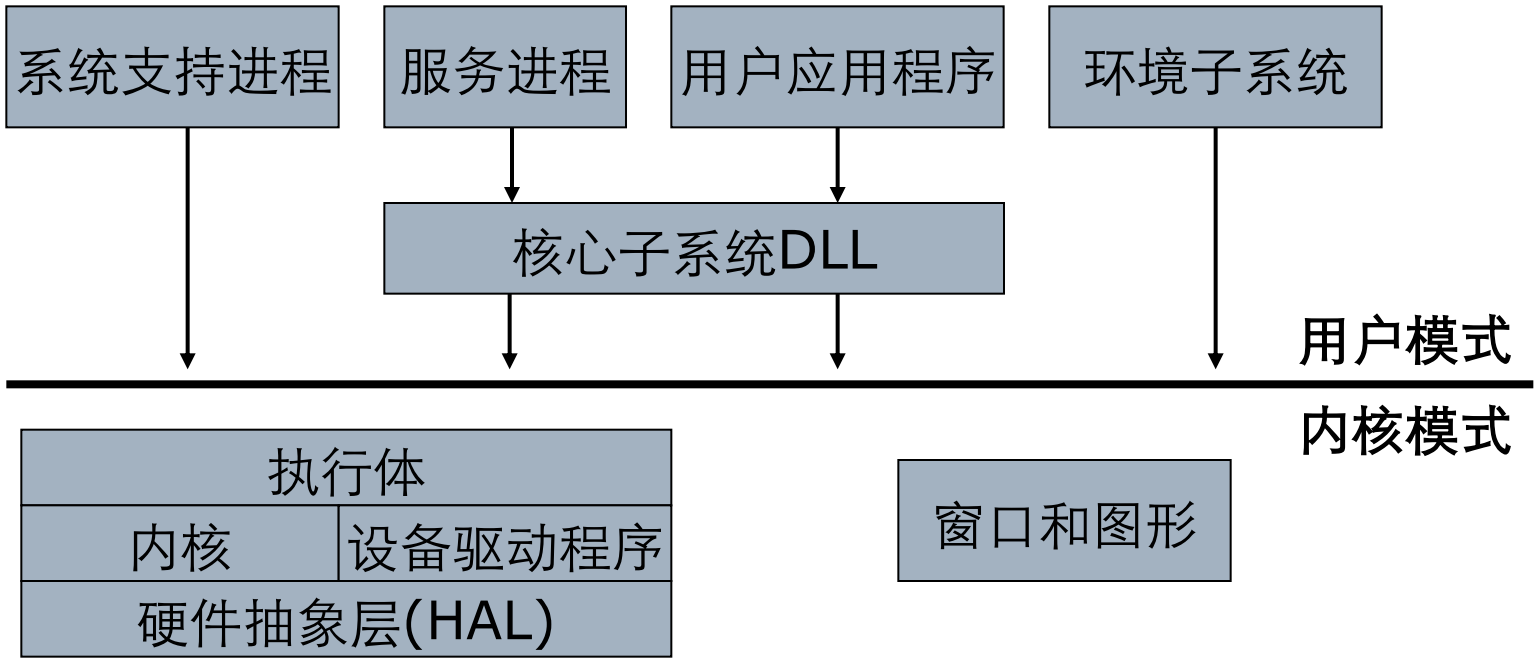
- 深入解析Windows操作系统(第四版)
  - **Windows Server 2003/Windows XP/Windows 2000技术内幕**
- 作者
  - **Mark E. Russinovich**
    - **sysinternals**
  - **David A. Solomon**
- 译者
  - 潘爱民研究员@MSRA
- 英文版电子书

Windows Kernel和软件资源

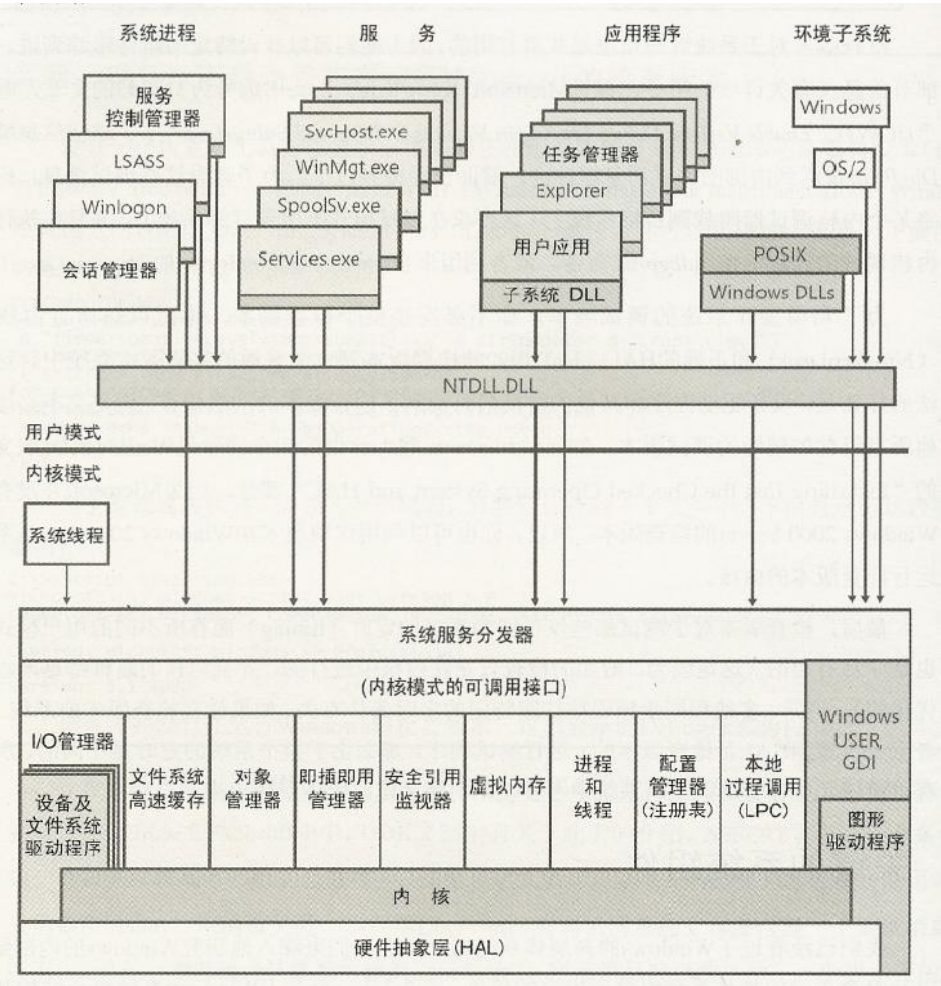
- Windows Research Kernel (WRK)
  - Subset of Windows kernel source code
  - For more information, see http://www.microsoft.com/resources/sharedsource/Licensing/WindowsAcademic.mspx
- Windows Operating System Internals Curriculum Resource Kit (CRK)

Windows操作系统基本结构

- **Windows操作系统基本模型**
  - 内核模式：内核代码运行在处理器特权模式(ring 0)
  - 用户模式：应用程序代码运行在处理器非特权模式(ring 3)



Windows系统核心结构和组件



- 系统进程
  - **Idle/System/smss/winlogon/lsass/services**
- **Windows**环境子系统
  - 内核:**win32k.sys**
  - 用户:**csrss.exe**
  - 子系统**DLL: Kernel32/Advapi32/User32/Gdi32**
- **Ntdll.dll**
  - 用户模式/内核模式**GW**
- **Windows**执行体
  - **Ntoskrnl.exe**上层
- 内核
  - **Ntoskrnl.exe**中函数和硬件体系结构支持
- 硬件抽象层**hal.dll**
- 设备驱动程序

Windows系统的启动机制

- **Boot Loader Phase**
  - **NTLDR**
  - 休眠模式恢复: 系统盘***hiberfil.sys***
  - **boot.ini**
    - **multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft Windows XP Professional" /fastdetect**
- **Kernel Loading Phase**
  - **装载Kernel: ntoskrnl.exe/hal.dll/kdcom.dll/bootvid.dll**
  - 装载系统盘

Windows系统的启动机制(2)

- Session Manager
  - 内核进程启动Session Manager Subsystem(smss.exe)
  - 创建环境变量
  - 启动Win32子系统(win32k.sys)
  - 启动Win32子系统用户模式组件(csrss.exe)
  - 创建虚拟内存映射
  - 启动Winlogon登录界面(winlogon.exe)

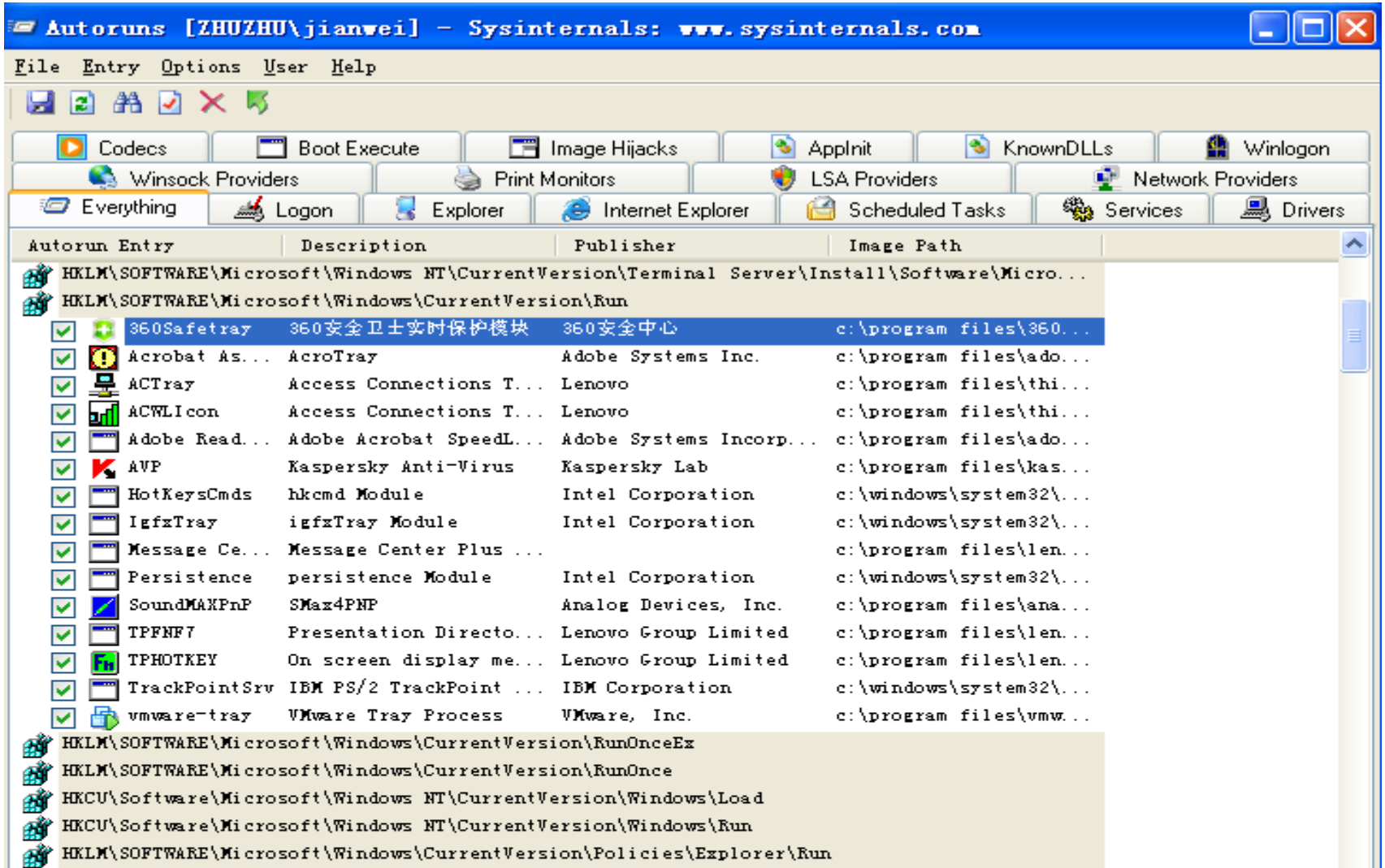
Windows系统的启动机制(3)

- **Winlogon**
  - **调用GINA－登录界面处理，获得用户credentials**
  - **Winlogon将credentials传递给LSA(Local Security Authority)**
  - **LSA确定登录帐号对应的帐号数据库(Local SAM, Domain SAM, Active Directory)，并credentials是否可登录**
- **Logon phase**
  - **启动Service Control Manager(SCM, service.exe)，启动设置为“自动启动”的服务**
  - **启动LSASS(Local Security Authority Subsystem Service, lsass.exe)，执行本地安全策略和组策略**
  - **启动设置为“开机自动启动”的应用程序**

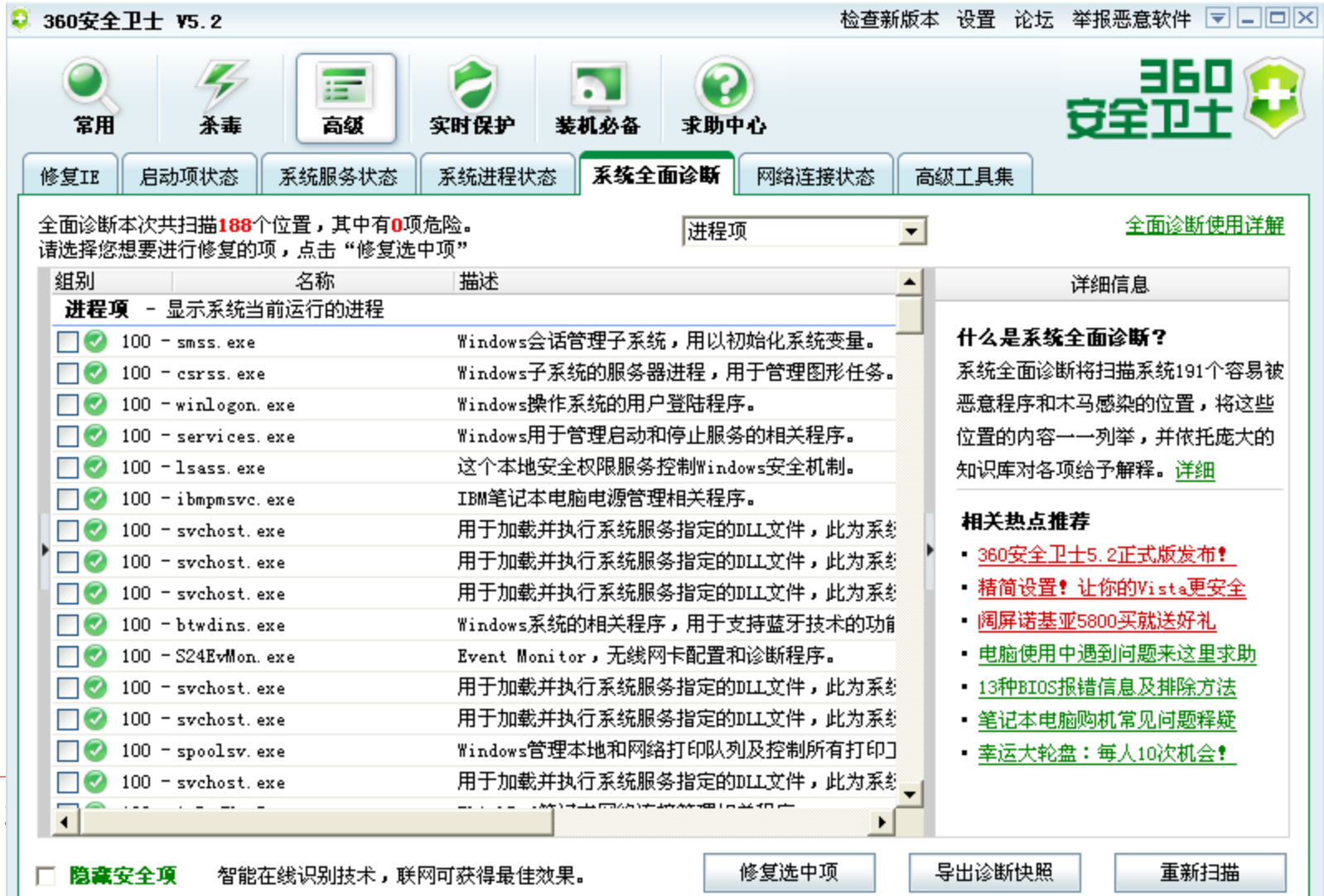
“开机自启”应用程序位置

- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run**
- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
- **HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run**
- **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**
- **HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce**
- ***All Users ProfilePath*\Start Menu\Programs\Startup\ (please note that this path is localized on non-English versions of Windows)**
- ***Current User ProfilePath*\Start Menu\Programs\Startup\ (please note that this path is localized on non-English versions of Windows)**
- “开机自启”是恶意程序期望的目标!
- 太多了？！找工具帮你的忙
  - **Autoruns**
  - **SReng**
  - **360安全卫士***

AutoRuns

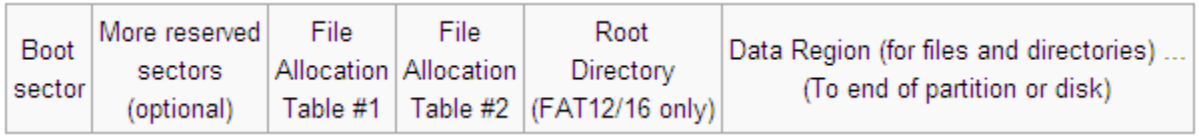

Autoruns [ZHUZHU\jianwei] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Codecs
Boot Execute
Image Hijacks
AppInit
KnownDLLs
Winlogon
Winsock Providers
Print Monitors
LSA Providers
Network Providers
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Autorun Entry
Description
Publisher
Image Path
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Micro...
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
360Safetray 360安全卫士实时保护模块 360安全中心 c:\program files\360...
Acrobat As... AcroTray Adobe Systems Inc. c:\program files\ado...
ACTray Access Connections T... Lenovo c:\program files\thi...
ACWLIcon Access Connections T... Lenovo c:\program files\thi...
Adobe Read... Adobe Acrobat SpeedL... Adobe Systems Incorp... c:\program files\ado...
AVP Kaspersky Anti-Virus Kaspersky Lab c:\program files\kas...
HotKeysCmds hkcmd Module Intel Corporation c:\windows\system32\...
IgfxTray igfxTray Module Intel Corporation c:\windows\system32\...
Message Ce... Message Center Plus ... c:\program files\len...
Persistence persistence Module Intel Corporation c:\windows\system32\...
SoundMAXPnP SMax4PNP Analog Devices, Inc. c:\program files\ana...
TPFNF7 Presentation Directo... Lenovo Group Limited c:\program files\len...
TPHOTKEY On screen display me... Lenovo Group Limited c:\program files\len...
TrackPointSrv IBM PS/2 TrackPoint ... IBM Corporation c:\windows\system32\...
vmware-tray VMware Tray Process VMware, Inc. c:\program files\vmw...
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

360安全卫士-系统诊断功能

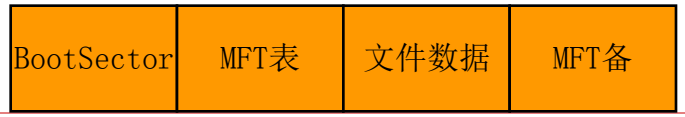


Windows文件系统

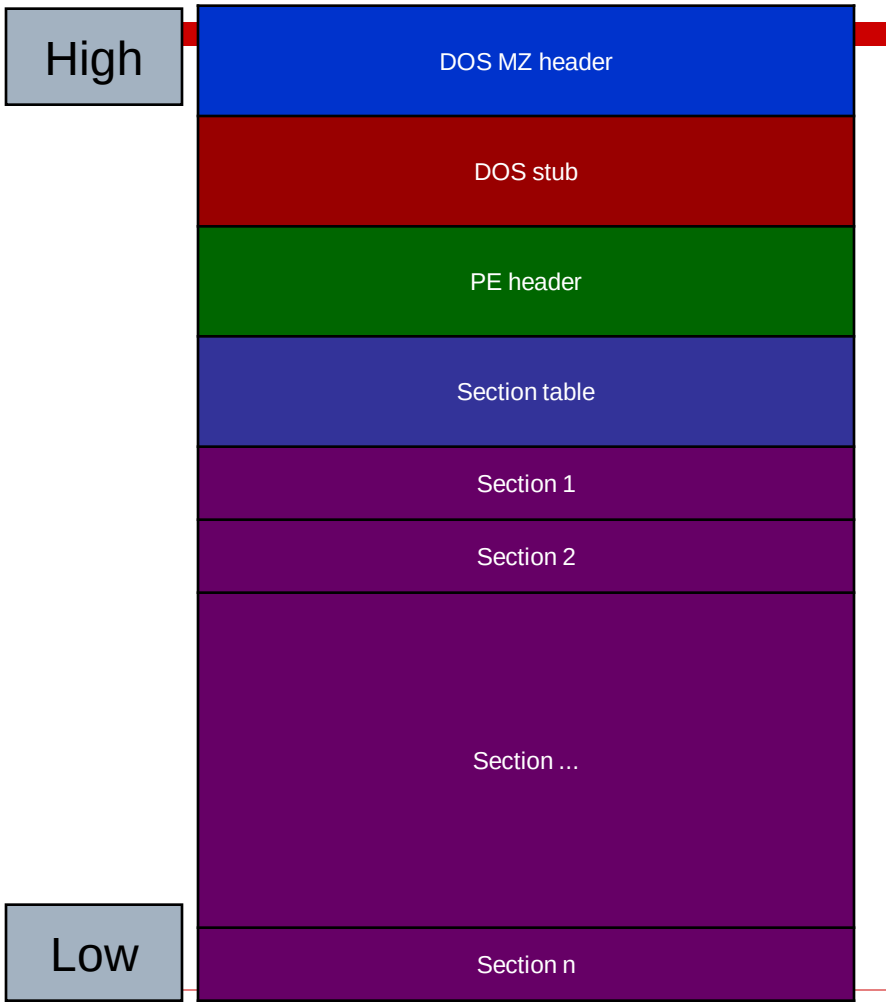
- **FAT (File Allocation Table文件分配表)**
  - **1980: FAT12 → 1987: FAT16 → 1995: FAT32**
  - 文件目录表：**Table;** 文件分配表：**Linked List**
  - 安全性弱，正在被**NTFS**取代

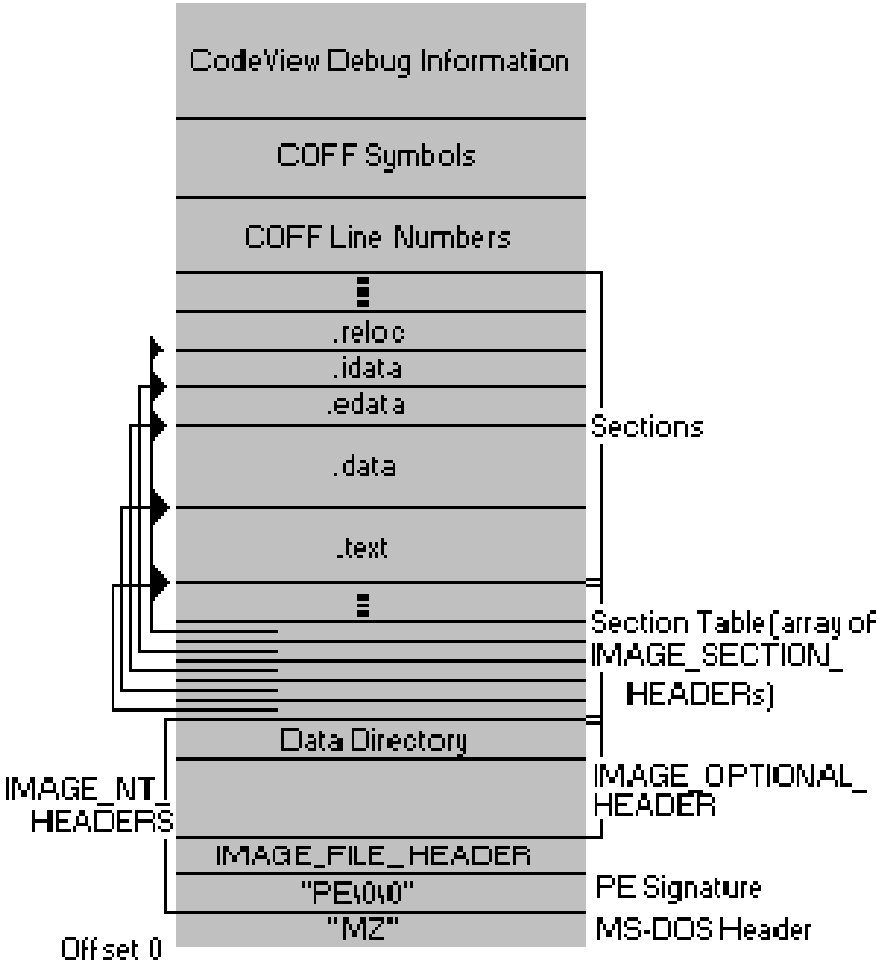


- **NTFS (NT File System)**
  - **1990s: M$/IBM joint project,** 从**OS/2**文件系统**HPFS**继承
  - **NTFS v3.x for Windows NT 5.x,** 较**FAT**更具安全性**(ACL)**，更好的性能、可靠性和磁盘利用效率
  - 基于访问控制列表机制保证文件读写安全性
  - 支持任意**UTF-16**命名，使用**B+**树进行索引，...
  - **Metadata**保存文件相关各种数据，保存在**Meta File Table(MFT)**



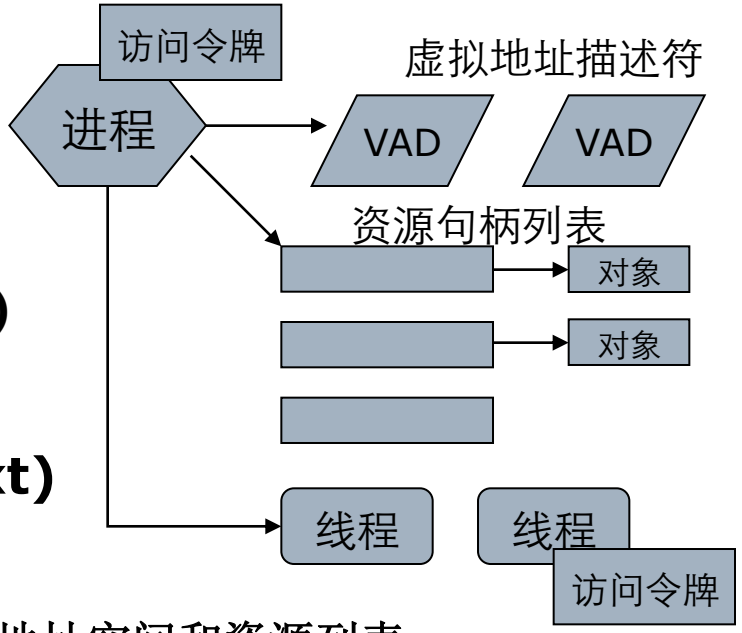
PE文件格式





Windows的进程和线程管理

- **Windows下的进程和线程**
  - 可执行程序: 静态指令序列
  - 进程：一个容器，包含至少一个执行线程
  - 线程：进程内部的指令执行实体
- **Windows进程构成元素**
  - 私有虚拟内存地址空间
  - 映射至进程内存空间的可执行程序
  - 资源句柄列表
  - 访问令牌(Security Access Token)
  - 进程ID，父进程ID
  - 至少一个执行线程
- **Windows线程包含基本部件(context)**
  - 处理器状态 CPU寄存器内容
  - 两个栈(内核模式、用户模式)
  - 线程局部存储区(TLS)，共享进程虚拟地址空间和资源列表
  - 线程ID



执行体进程块(EPROCESS/KPROCESS/PEB)

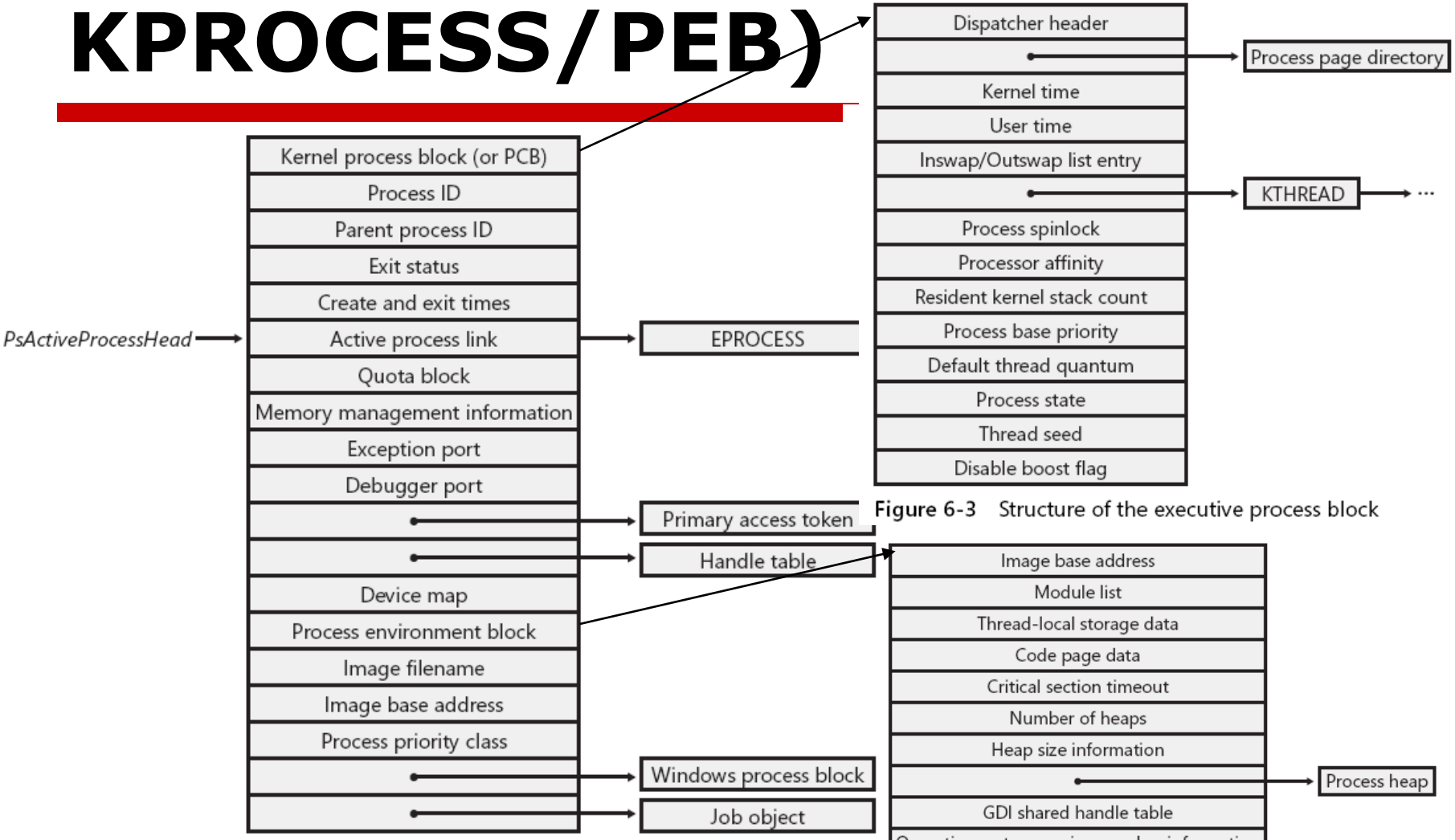


Figure 6-2 Structure of an executive process block

Figure 6-3 Structure of the executive process block

Figure 6-4 Fields of the process environment block

执行体线程块(ETHREAD/KTHREAD/TEB)

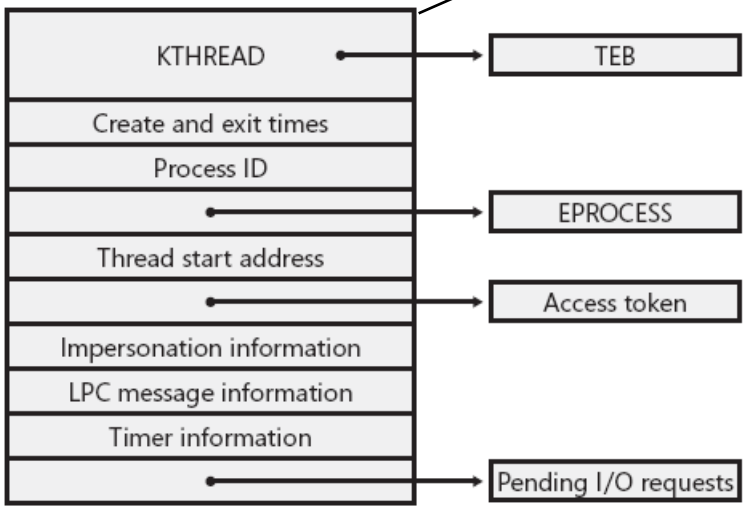


Figure 6-7 Structure of the executive thread block

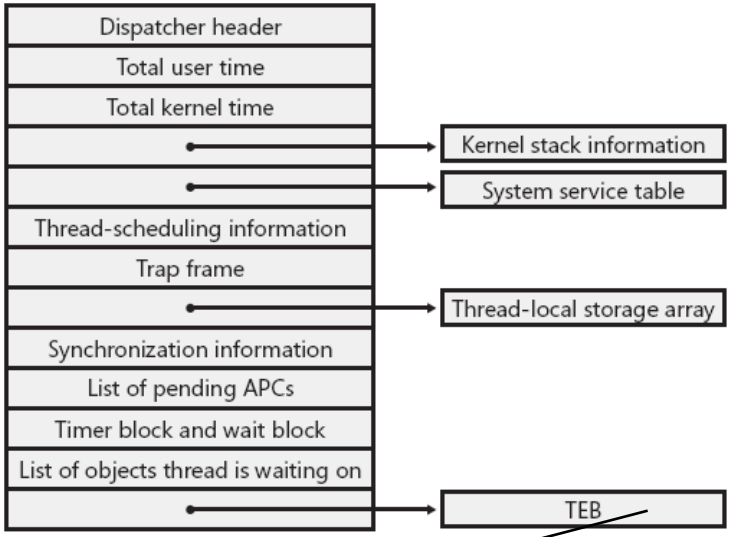


Figure 6-8 Structure of the kernel thread block

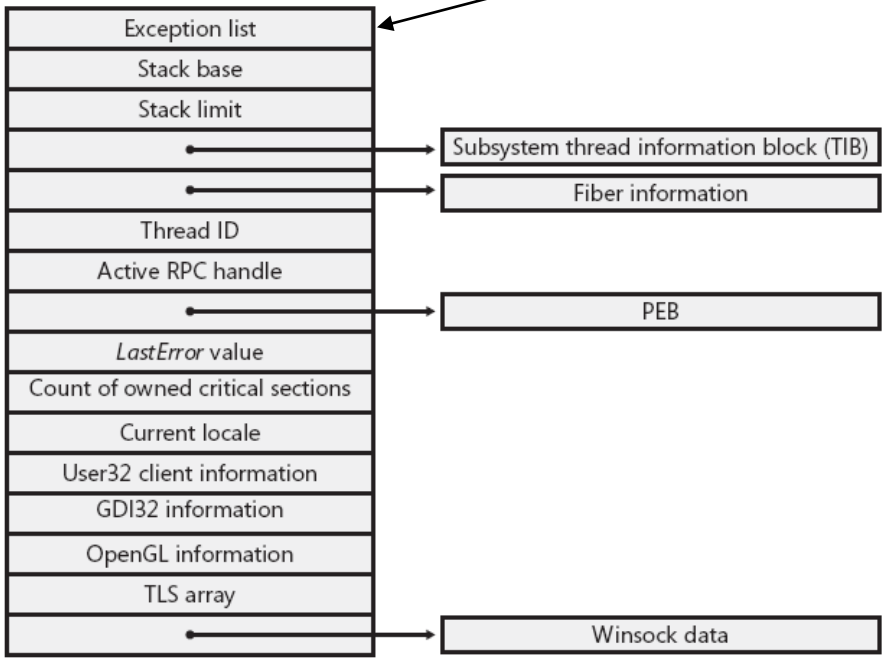
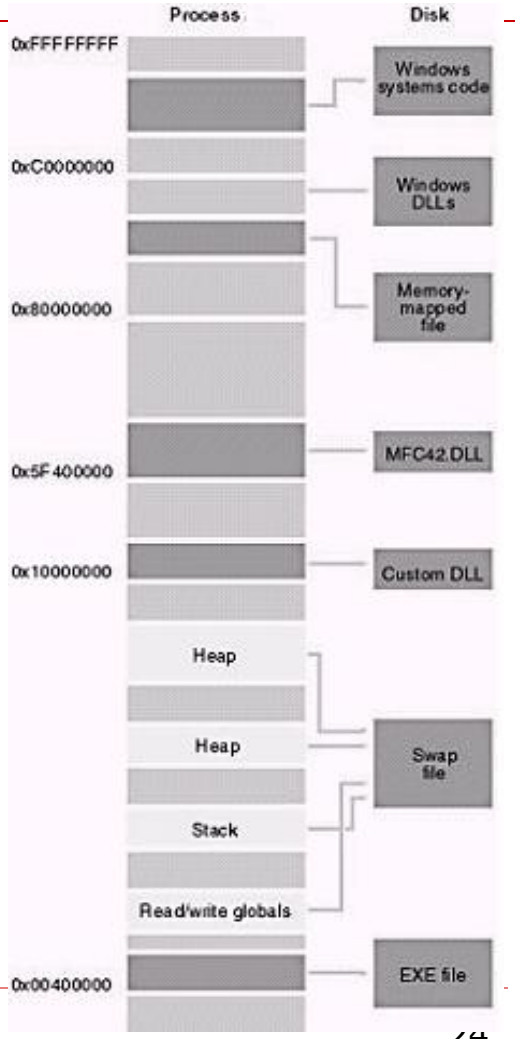


Figure 6-9 Fields of the thread environment block

Windows的内存管理

- 系统核心内存区间
  - **0xFFFFFFFF~0x80000000 (4G~2G)**
  - 映射内核、**HAL**、**Win32k.sys**子系统等
  - 内核态可操纵**(DKOM)**
- 用户内存区间
  - **0x00000000~0x80000000 (2G~0G)**
  - 堆**:** 动态分配变量**(malloc),** 向高地址增长
  - 静态内存区间**:** 全局变量、静态变量
  - 代码区间**:** 从**0x00400000**开始
  - 栈**:** 向低地址增长
    - 单线程进程：**(**栈底地址**: 0x0012FFXXXX)**
  - 每个线程对应一个用户态的栈和堆
- **Windows Memory layout**



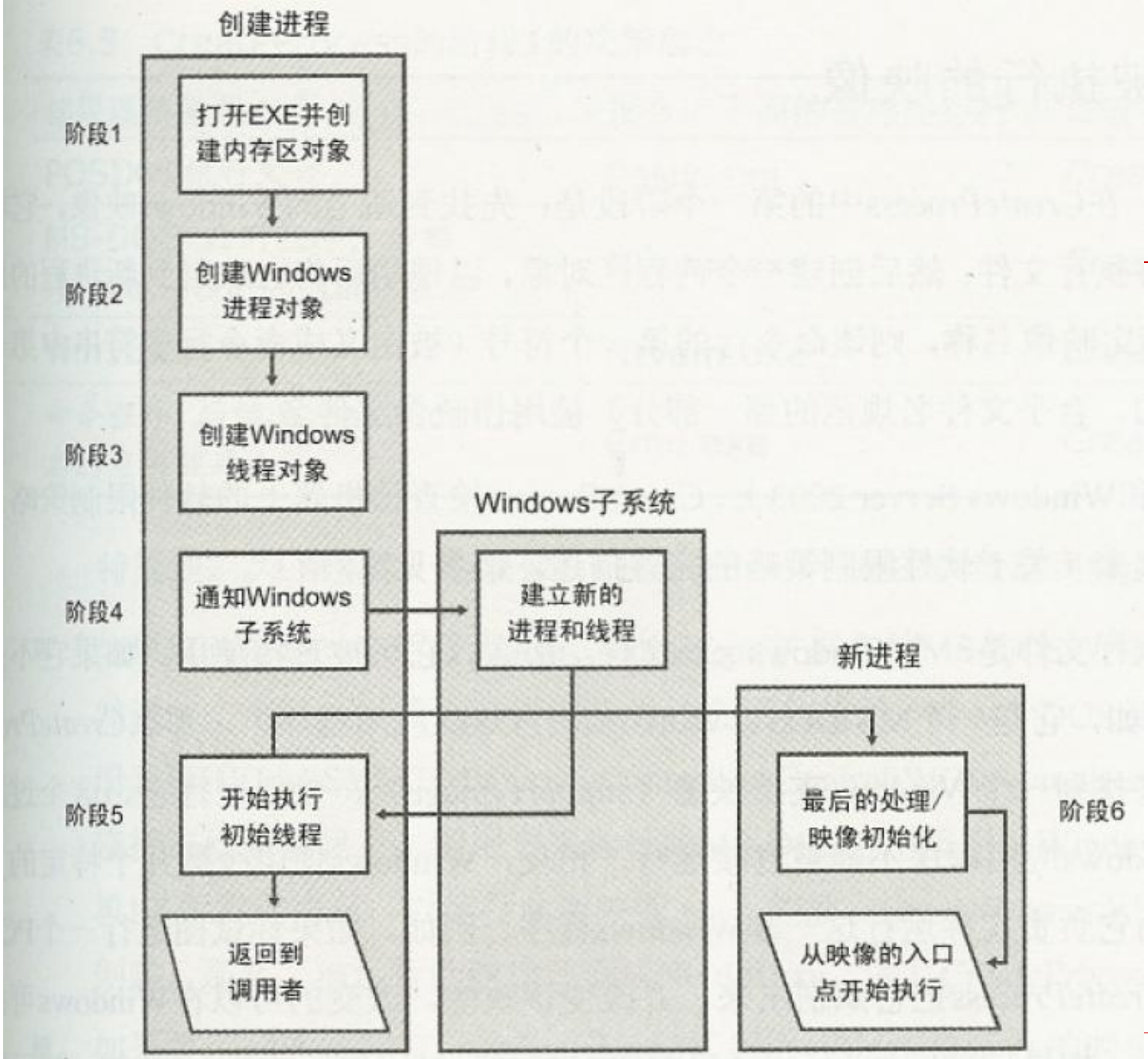
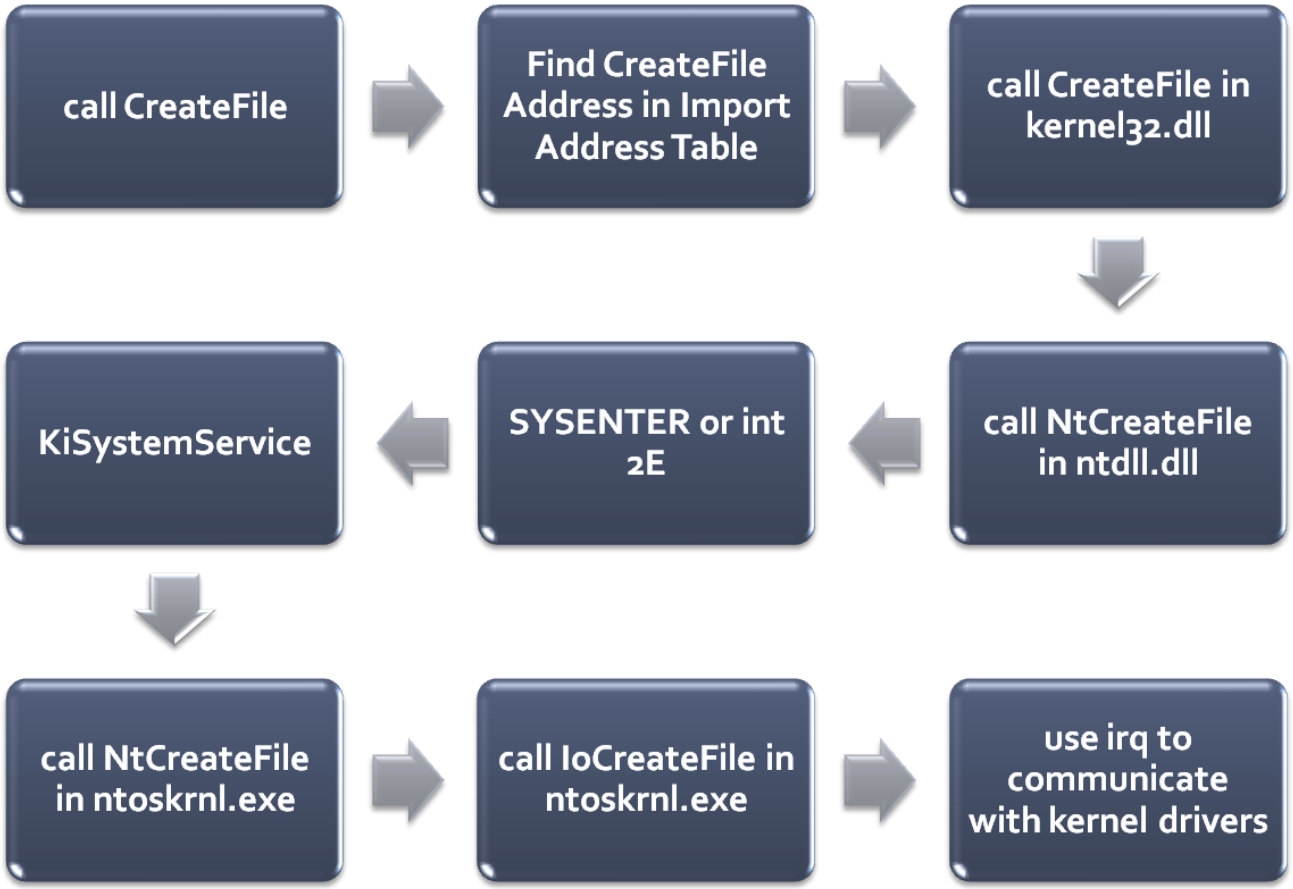


图6.5 进程创建过程的主要阶段

程序装载和运行

Windows系统API调用过程



API Hooking机制

- **API Hooing:** 对**API**调用过程进行**Hook(**挂钩**),** 改变**API**调用流程以达到某种目的的技术方法。
- **API Hooking**目的
  - 隐藏自身存在**:** 恶意代码**, Rootkit**
  - 安全监控和加强**:** 防病毒软件**, …**
  - 安全监控和分析**: Sandbox, …**
- **API Hooking**技术手段
  - 用户层**API Hooking: Proxy DLL, IAT Patching, Code overwriting, Debugger**
  - 内核层**API Hooking: SSDT hook, IDT Hook, Sysenter hook, IRP hook**
  - 混合模式**API Hooking:** 结合两者，有些内核**API**没有很好的文档支持

Windows系统的注册表

- Windows系统注册表
  - Windows配置和控制方面关键角色
  - 系统全局配置的存储仓库
  - 每个用户配置信息的存储仓库
- 注册表查找编辑工具
  - Regedit.exe
- 注册表的读写
  - 读取: 系统引导过程, 系统登录过程, 应用程序启动过程
  - 修改: 缺省安装, 应用程序安装, 设备驱动安装, 修改应用程序配置
- 注册表在文件系统上的存储(Hive)
  - HKLM\SYSTEM\CurrentControlSet\Control\hivelist
- 注册表监视工具
  - RegMon
- 注册表ASEP点-autorun
  - 经常被恶意代码/攻击者利用

注册表储巢—Hive

- 注册表储巢

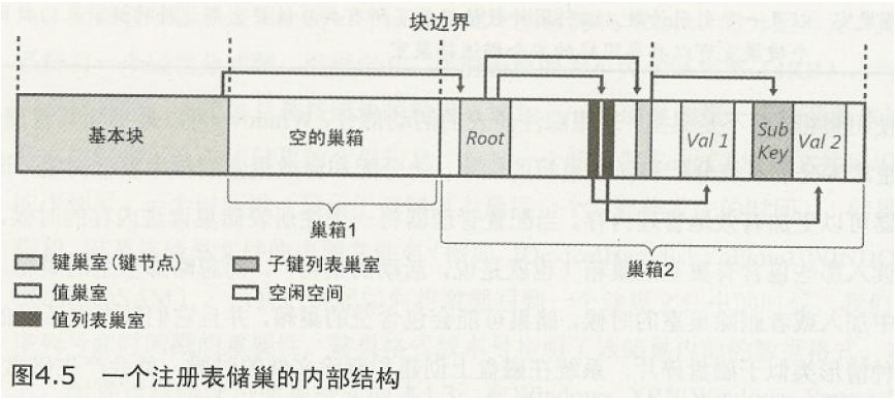


图4.5 一个注册表储巢的内部结构

- 由配置管理器读入内存(内核地址空间换页池)—巢室索引结构

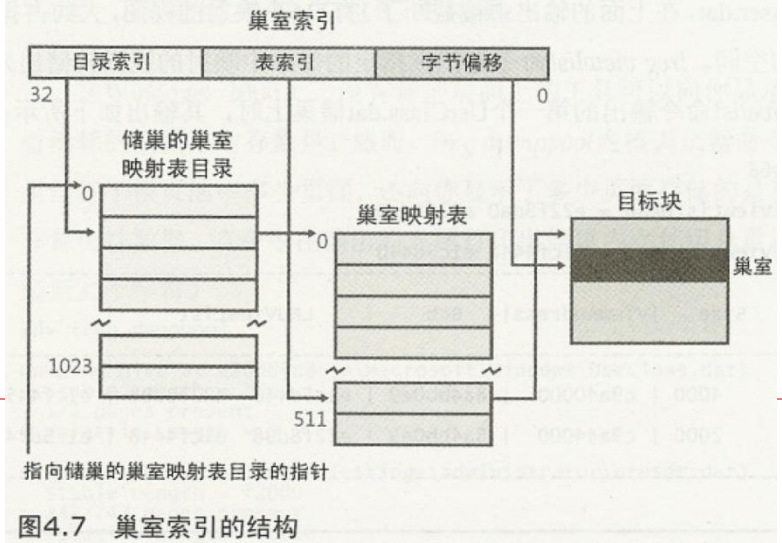
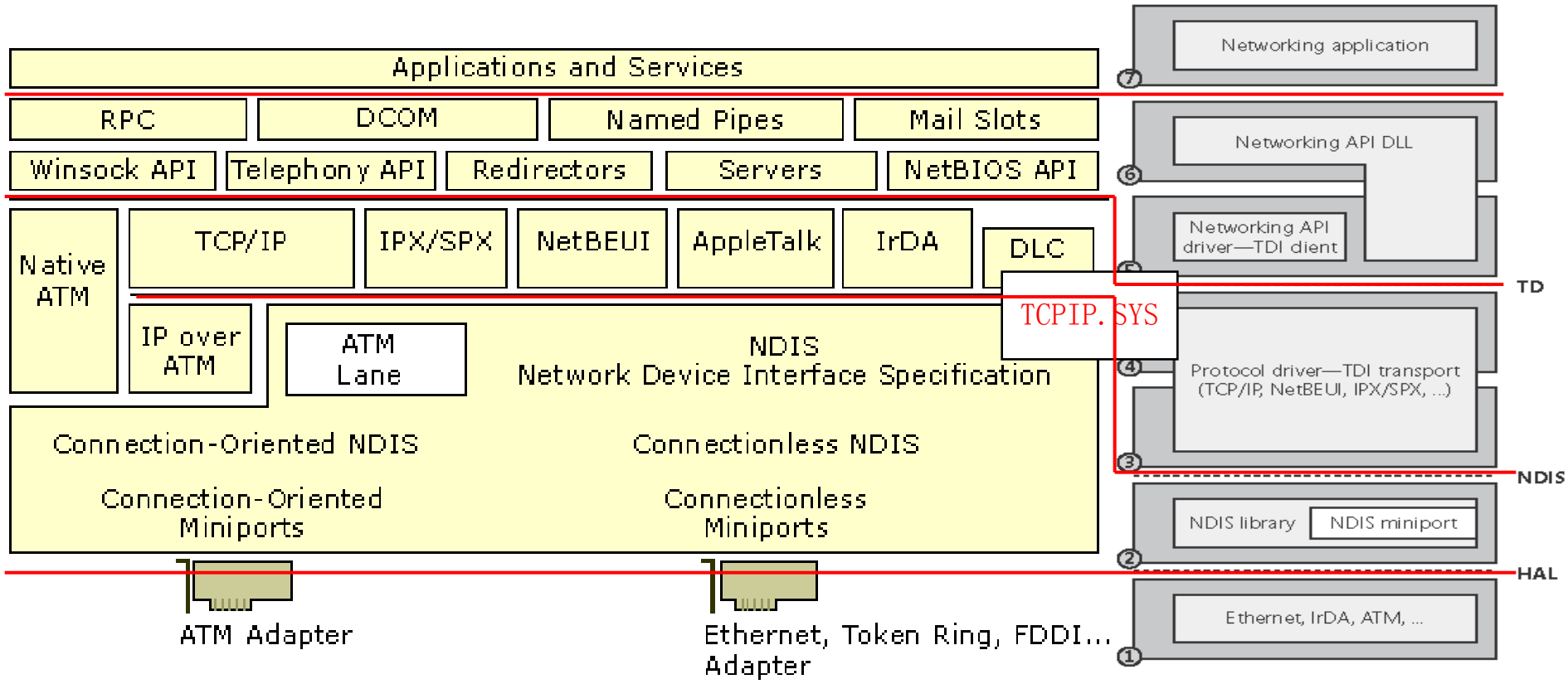


图4.7 巢室索引的结构

内容

1. Windows操作系统简介
2. Windows NT 5.x的系统结构
3. Windows NT 5.x的网络结构
4. Windows NT 5.x的安全结构

Windows NT5.x中的网络结构



Windows Networking API

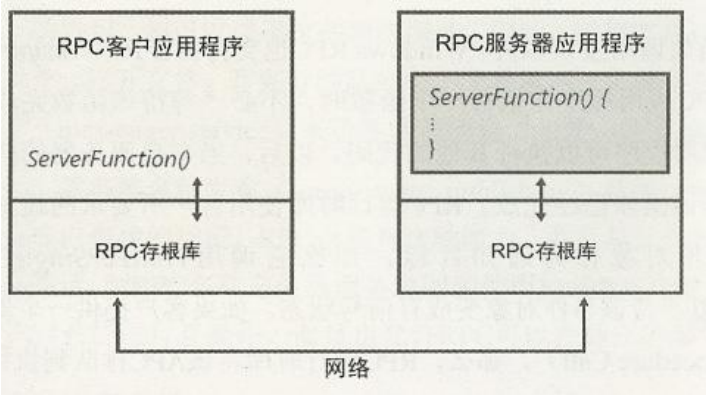
- NetBIOS－网络基本输入/输出系统
  - Windows独有的局域网组网协议
- RPC – 远过程调用
  - PRC/DCOM
- WinSock API
- 命名管道(Named Pipes)和邮件槽(Mail Slots)
  - 命名管道：提供可靠双向通信，协议无关的标识Windows网络资源的方法
  - 邮件槽：提供不可靠的单向数据传输，支持广播
- Web访问API
  - WinInet/WinHTTP/HTTP API

NetBIOS

- NetBIOS(网络基本输入/输出系统)：最初由IBM开发，MS利用NetBIOS作为构建局域网的上层协议
- NetBIOS使得程序和网络之间有了标准的接口，方便应用程序的开发。并且可以移植到其他的网络中
- NetBIOS位于OSI模型会话层，TCP/IP之上
- NetBIOS有两种通讯模式
  - 会话模式。一对一进行通讯，LAN中的机器之间建立会话，可以传输较多的信息，并且可以检查传输错误
  - 数据报模式。可以进行广播或者一对多的通讯，传输数据大小受限制，没有错误检查机制，也不必建立通讯会话
- NetBIOS over TCP/IP，支持三种服务
  - 名字服务 UDP 137
  - 会话服务 TCP 139/445
  - 数据报服务 UDP 138

MSRPC远程进程调用/DCOM

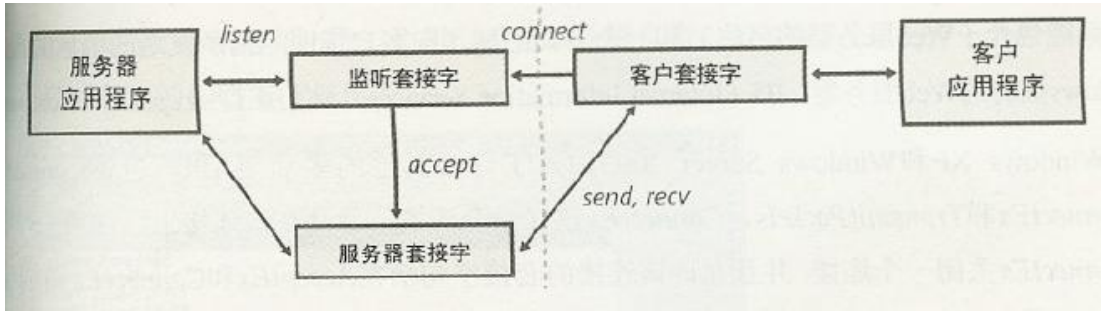
- **RPC (Remote Procedure Call)**
  - 网络编程标准
  - 目的: 提供“能在某种程度上像应用程序开发人员隐藏有关网络编程细节”的编程模型
- **RPC调用**
  - 允许程序员编写的客户应用程序跨网络调用远程计算机上服务器应用程序中的过程



- **COM/DCOM**
  - **COM对象:** 使应用程序由不同组件构成，导出面向对象接口，提高软件模块化、可扩展性和可交互性。
  - **DCOM:** 提供**COM**组件的位置透明性，依赖于**RPC**
  - **Know More:** 潘爱民著《**COM**组件技术》，《组件技术讲义》

WinSock API

- WinSock: Windows套接字
  - Winsock 1.0: Microsoft的BSD套接字实现
  - Winsock 2.2: 支持面向连接/无连接通信，异步I/O，更好性能和伸缩性
- 面向连接的Winsock操作



- WinSock编程
  - 《Microsoft Windows网络编程》

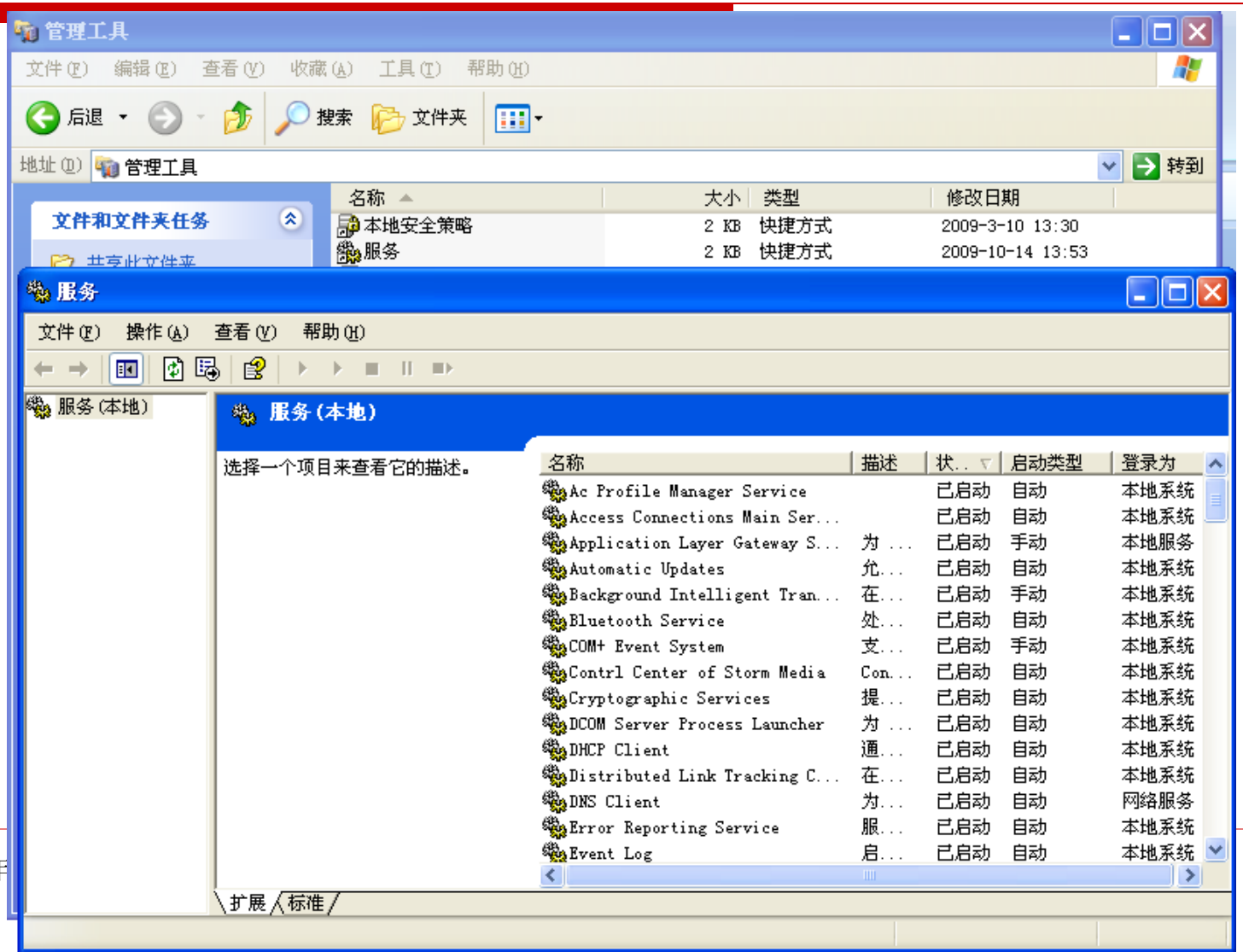
常用的Windows应用层网络服务

- Network Applications
- IIS (Internet Information Services)
  - HTTP/FTP/…
- Email
  - Exchange Server
- Database
  - MS SQL Server
- RDP
  - Remote Desktop Protocol
- 通常以Windows服务方式后台运行

Windows服务

- **Windows服务－系统启动时刻启动进程的机制，提供不依赖于任何交互式的服务。**
- **Windows服务**
  - 服务应用程序
    - 注册服务**Advapi32.dll, CreateService/StartServices**
    - 注册表: **HKLM\SYSTEM\CurrentControlSet\Services**
    - 共享服务进程: 服务宿主**svchost.exe**
  - 服务控制管理器**(SCM, service control manager, services.exe)**
    - **Winlogon**进程在加载**GINA**之前执行**SCM**启动函数
    - **SCM**中的**ScCreateServiceDB**根据注册表分别启动服务
    - **SCM**中的**ScAutoStartServices**启动“自动启动”的服务
  - 服务控制程序**(SCP, service control program)**
    - 控制面板，服务插件...

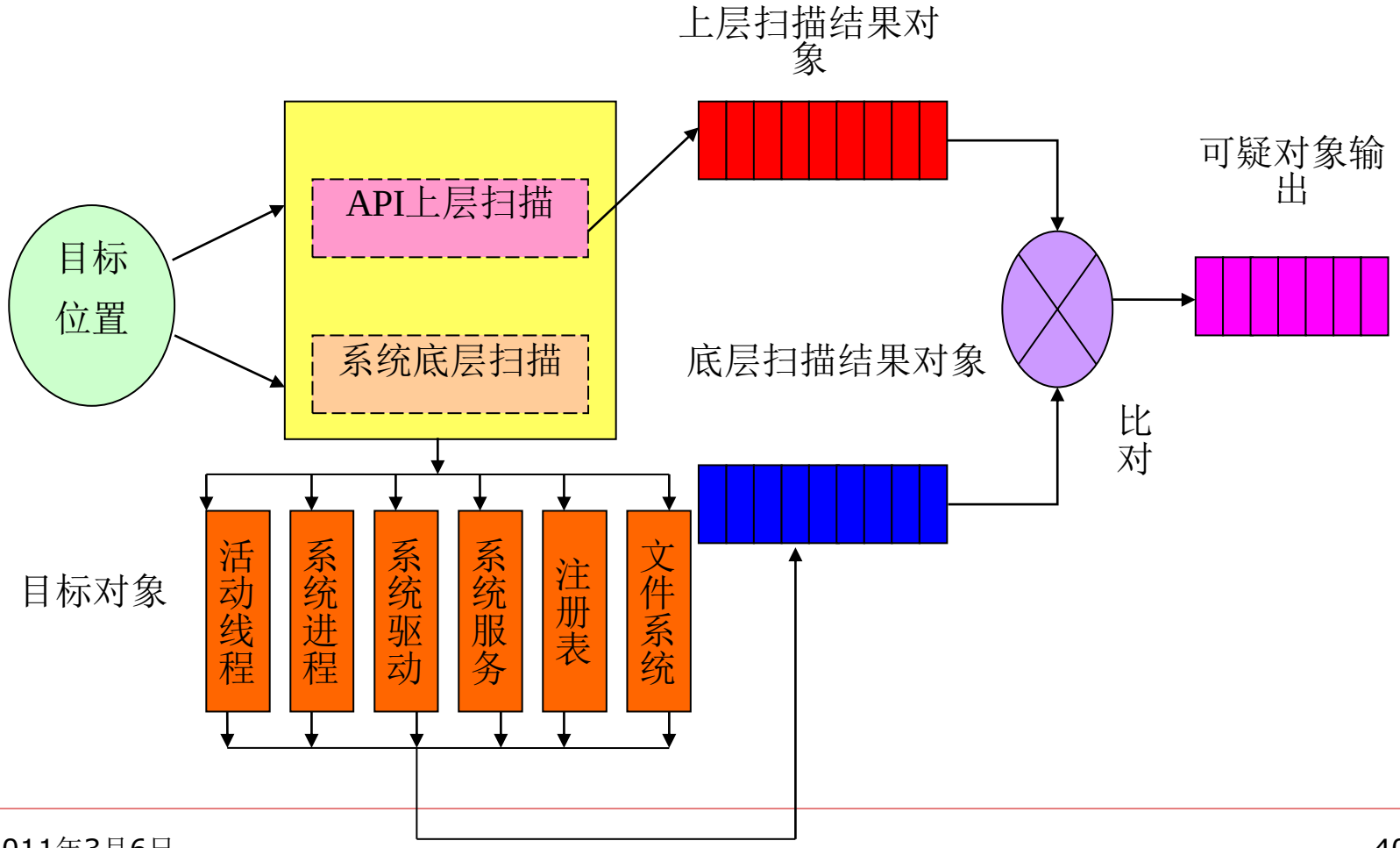
Windows服务控制面板



什么时候需要了解Windows内部机制？

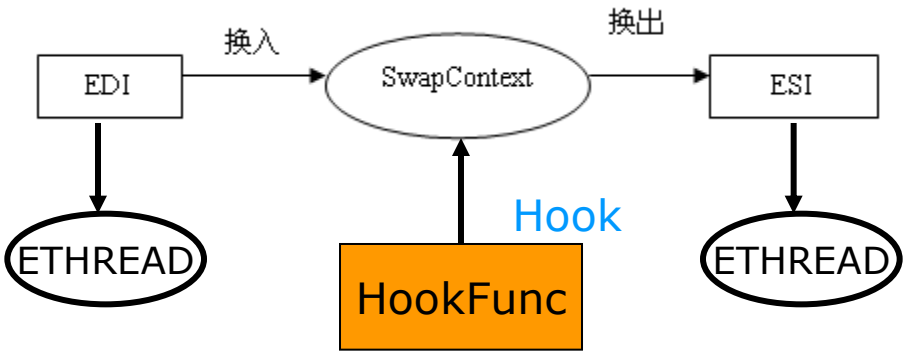
- Windows应用编程开发
  - 熟悉掌握Windows操作系统向上层应用提供的API
  - 基本了解所涉及的Windows组件的内部实现原理
- Windows内核编程开发
  - 深入了解涉及的Windows组件内部实现机制
  - 掌握在内核中直接操纵Windows对象的技术方法
- 针对Windows平台的攻击
- 针对Windows恶意代码、攻击的监控与防护

Rootkit检测技术总体流程图



检测技术分析—活动线程检测

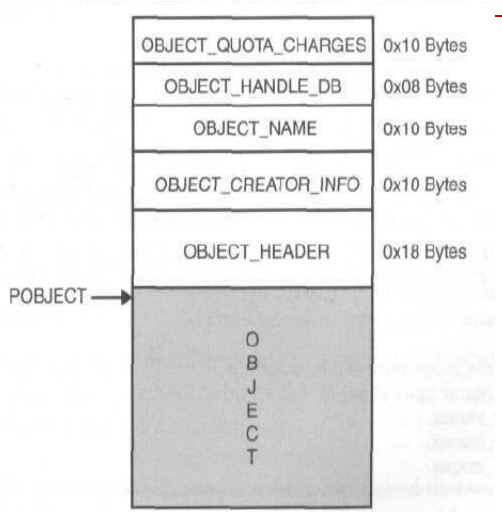
- 隐藏机制：钩子，**DKOM**
- 内核线程调度机制：**SwapContext()**函数



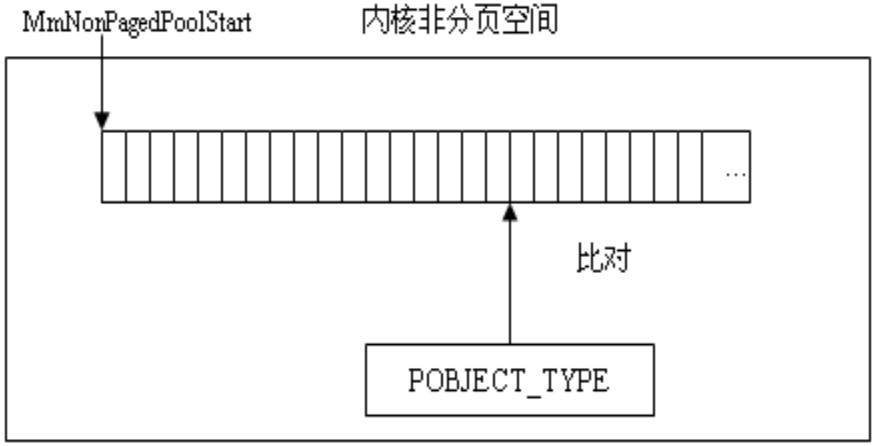
- 活动线程检测：线程结构

检测技术分析—进程、驱动检测

- 隐藏机制：钩子，**DKOM**
- 内核对象概念
- 内核对象结构

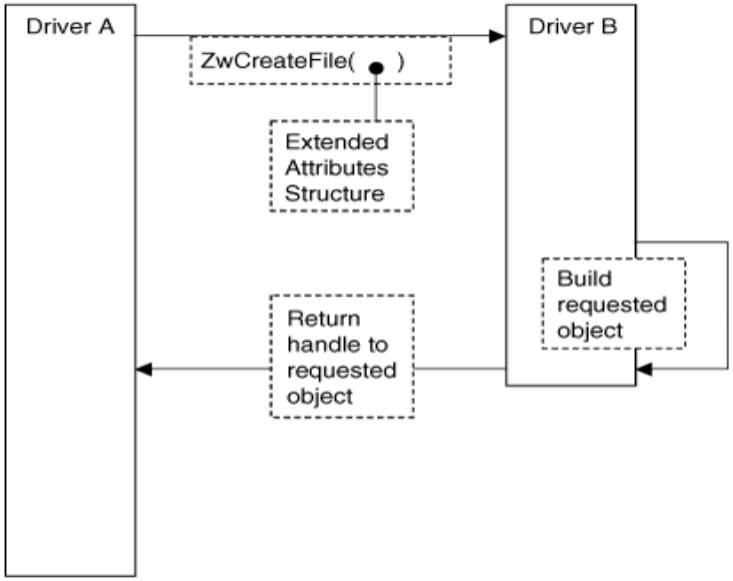


- 进程、驱动检测：
  基于内核对象特征
  的虚拟内存搜索方法

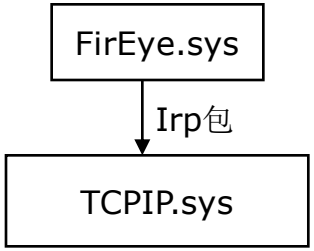


检测技术分析—网络端口检测

- 隐藏机制：钩子
- 驱动会话机制

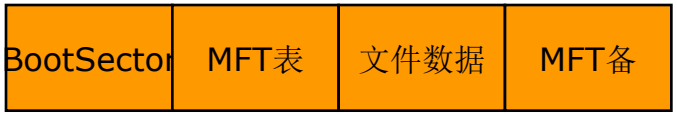


- 基于驱动会话的隐藏端口检测方法



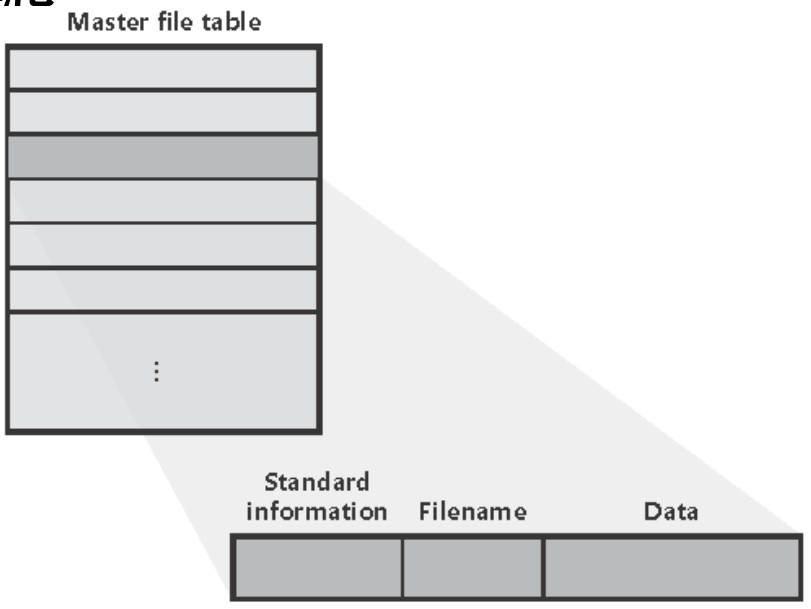
检测技术分析—文件系统隐藏检测

- 隐藏机制：钩子或文件系统过滤
- **NTFS与MFT表**



- **FAT32与FAT表**

- 文件系统隐藏检测：
  基于磁盘扇区直接读写
  的隐藏文件搜索方法



检测技术分析—注册表、系统服务、启动项

- 隐藏机制：钩子（**Hook)**
- **Hive结构：struct hive;**
- **Dump注册表文件**
- 基于**Hive**结构的二进制文件分析方法

  获得底层视图

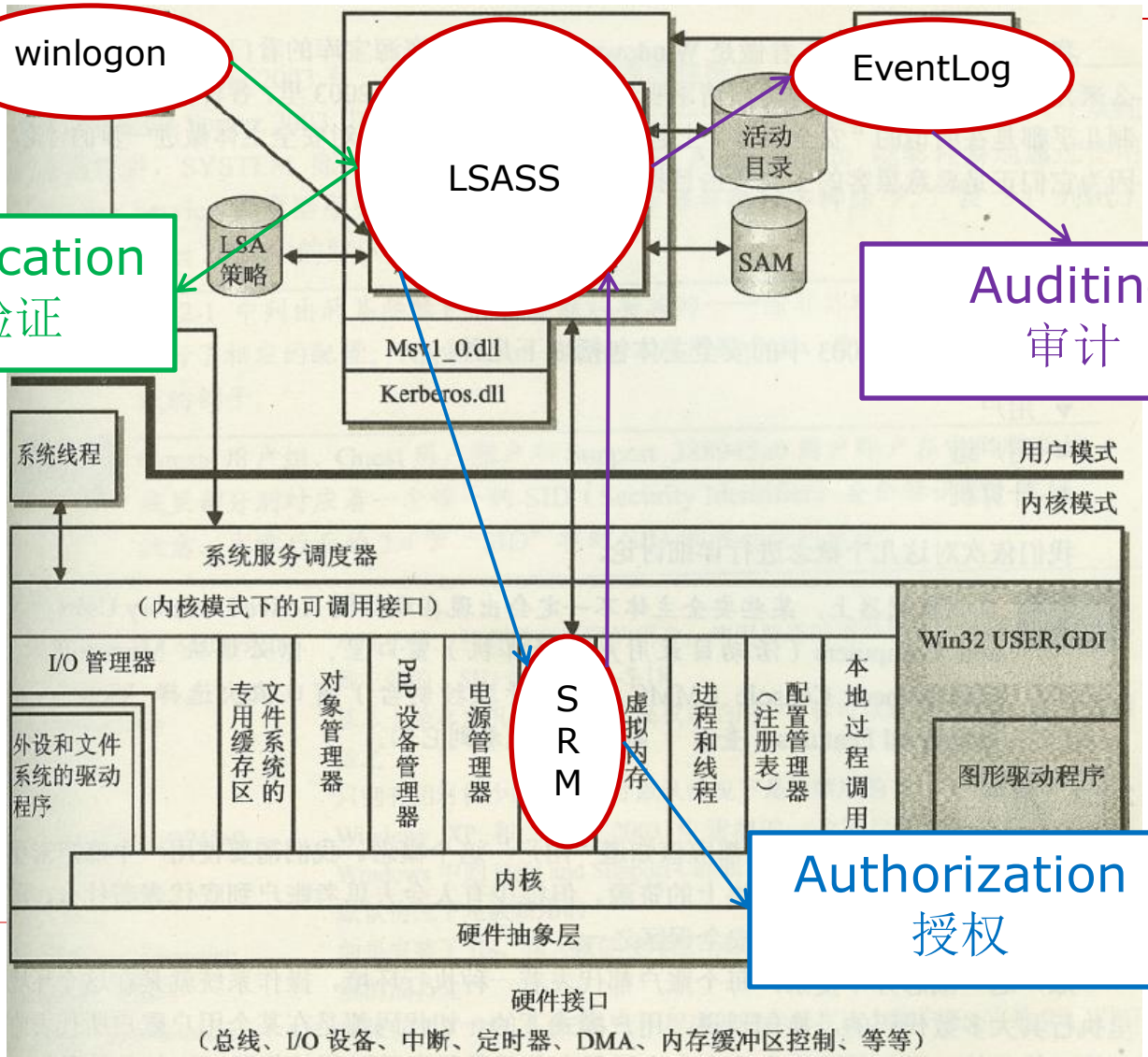
内容

1. Windows操作系统简介
2. Windows NT 5.x的系统结构
3. Windows NT 5.x的网络结构
4. Windows NT 5.x的安全结构

Windows安全性

- 设计目标
  - 一致的、健壮的、基于对象的安全模型
  - 满足商业用户的安全需求, 达到CC评估标准EAL4
    - **AAA:** 身份验证、授权、审计
  - 一台机器上多个用户之间安全地共享资源
    - 进程，内存，设备，文件，网络
- 安全模型
  - 服务器管理和保护各种对象
  - 客户通过服务器访问对象
    - 服务器扮演客户，访问对象
    - 访问的结果返回给服务器
- 攻击者目标
  - 在拥有最高权限的用户帐户环境中执行命令。

Windows NT 5.x安全体系结构



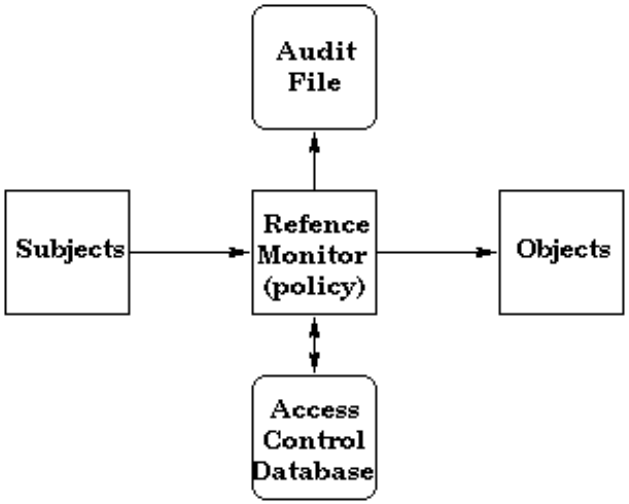
Authentication
身份验证

Auditing
审计

Authorization
授权

SRM-安全引用监控器

- **SRM (Security Reference Monitor)**
  - 安全引用监控器
  - **Windows资源宝库的看门人**
  - 位置: **Windows执行体Ntoskrnl.exe上层**
  - 内核模式，负责对运行在用户模式代码的各种资源存取请求进行检查



S. Ames, M. Gasser, and R.Schell, John S. *Security Kernel Design and Implementation: An Introduction*, IEEE Computer, Vol. 16, No. 7, 1983.

Subject – 安全主体

- Windows NT 5.x的安全主体
  - 用户(users) 和 用户帐户(accounts)
  - 用户组(groups)
  - 计算机(computers)
- Account Identifier: Security identifier(SID)安全标识符
  - 时间和空间唯一的安全主体帐户标识
  - 48位数值: S-1-N-Y1-Y2-Y3-Y4
  - Some well-known SIDs: Administrator Y4(RID)=500

用户帐户

- 用户帐户
  - 操作系统运行程序代码的执行环境
- 帐户权限
  - 限制该用户帐户内运行程序对系统资源对象的访问
- **Windows内建帐户**
  - 本地**Administrator帐户: 最高权限**
  - **SYSTEM/LocalSystem: 技术角度最高权限，自动运行程序所使用的运行环境**
  - **Guest帐户: 相对极少的权限**
  - **IUSR_*machinename*: IIS匿名网络访问帐户, Guest组**
  - **IWAM_*machinename*: IIS应用程序运行帐户**
- 黑客眼里的**Windows帐户**
  - 本地**Administrator和SYSTEM帐户拥有最高权限，是终极目标**

用户组

- 用户组
  - 简化用户管理引入的用户帐户容器
  - 将用户帐户添加入特定用户组，该用户即拥有用户组配置的全部权限
- **Windows内建用户组**
  - **Administrators:** 本地最高权限用户组
  - **Account/Backup/Server/Print Operators:** 略低于**Administrators**
  - **Network/Local Service:** 用于容纳服务帐户，替代原先用于启动服务的**SYSTEM**帐户
  - **Users:** 所有用户帐户
- **Windows域中的内建用户组**
  - **Domain Admins:** 域中最高权限
  - **Enterprise Admins:** 森林中最高权限组

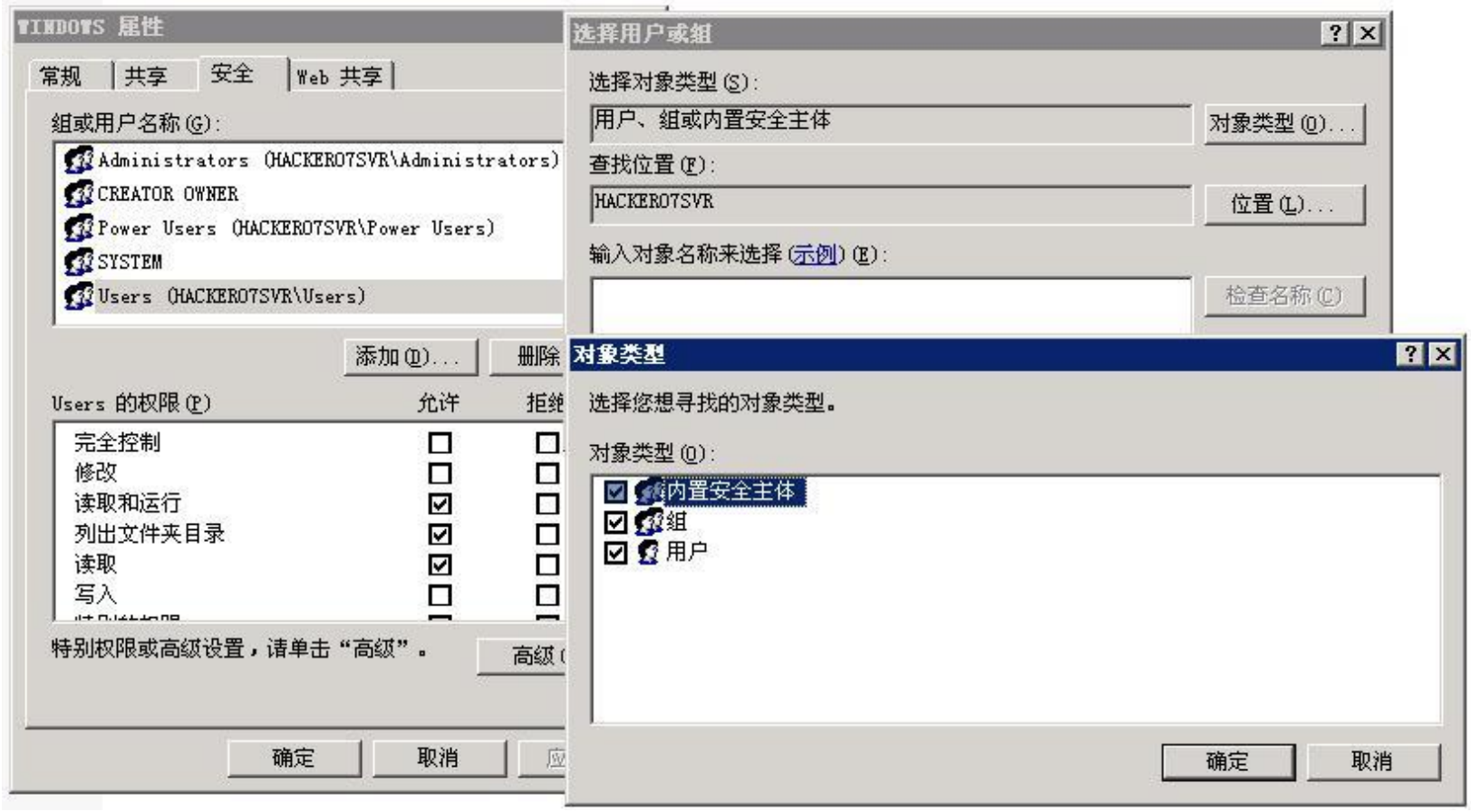
帐户口令管理-SAM和活动目录

- 本地帐户和口令信息-保存在SAM中
  - **SAM: Security Accounts Manager**
  - 加密口令字存储: 不可逆Hash后存储
  - **SAM位置:** 运行时刻不能直接读取
    - 文件系统: **%systemroot%\system32\config\sam**
    - 注册表: **HKEY_LOCAL_MACHINE\SAM**
- 域帐户和口令信息-保存在域控制器的活动目录AD中
  - **AD: Active Directory**
  - **AD位置: %systemroot%\ntds\ntds.dit**
  - 加密格式与单机平台一致，但访问方法不同
- **SYSKEY机制- 128位随机密钥加密保护机制**

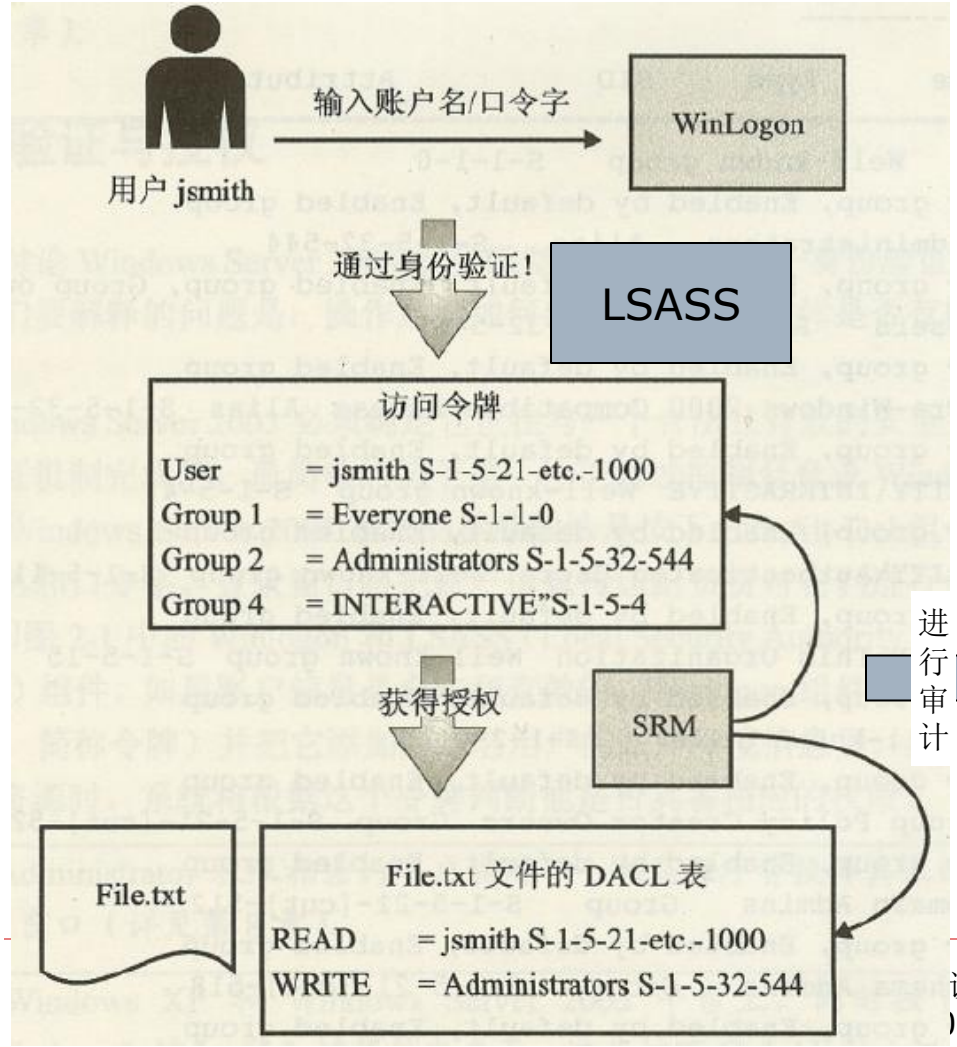
对象 - Object

- 对象-系统中所有需保护的资源
  - 文件、目录、注册表键
  - 内核对象
  - 同步对象
  - 私有对象(如打印机等)
  - 管道、内存、通讯，等
- 对象的安全描述符**SD(Security Descriptor)**
  - **Owner SID**
  - **Group SIDs**
  - **Discretionary ACL (授权)**
  - **Audit: System ACL (审计)**

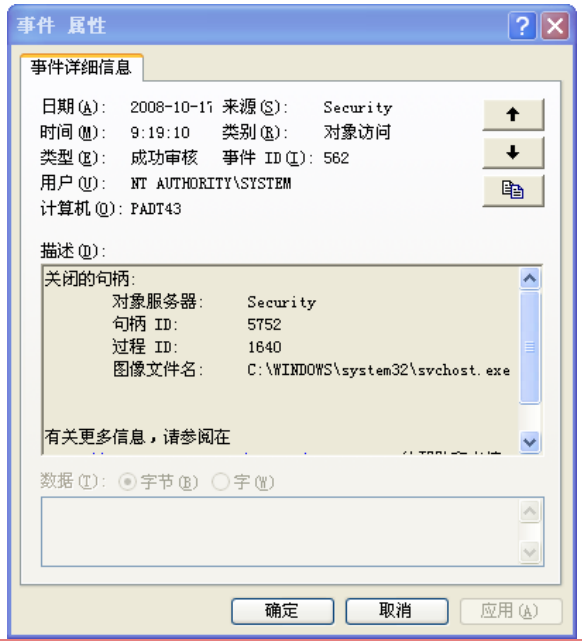
DACL



AAA


输入账户名/口令字
WinLogon
用户 jsmith
通过身份验证!
LSASS
访问令牌
User = jsmith S-1-5-21-etc.-1000
Group 1 = Everyone S-1-1-0
Group 2 = Administrators S-1-5-32-544
Group 4 = INTERACTIVE"S-1-5-4
获得授权
SRM
File.txt
File.txt 文件的 DACL 表
READ = jsmith S-1-5-21-etc.-1000
WRITE = Administrators S-1-5-32-544

进行审计


事件 属性
事件详细信息
日期(A): 2008-10-17 来源(S): Security
时间(M): 9:19:10 类别(R): 对象访问
类型(E): 成功审核 事件 ID(I): 562
用户(U): NT AUTHORITY\SYSTEM
计算机(O): PADT43
描述(D):
关闭的句柄:
对象服务器: Security
句柄 ID: 5752
过程 ID: 1640
图像文件名: C:\WINDOWS\system32\svchost.exe
有关更多信息，请参阅在
数据(T): 字节(B) 字(W)
确定
取消
应用(A)

Authentication-身份验证

- 身份验证
  - 操作系统通过一些秘密信息认证安全主体真实合法的身份
  - 秘密信息: 口令、指纹...
- 身份验证方式
  - 本地身份验证: 本地系统登录Ctrl-Alt-Del
  - 网络身份验证: 远程访问

令牌

- 令牌
  - 保存一份与登录帐户有关的安全主体**SID**列表
  - 帐户本身**SID**、所属用户组的**SID**等
- 进程的访问令牌**(Security Access Token)**
  - 继承启动进程的用户帐户所拥有的令牌
  - 是对一个进程安全环境的完整描述
- 包括以下主要信息
  - 用户帐户的**SID**
  - 所有包含该用户的安全组的**SIDs**
  - 特权：该用户和用户组所拥有的权利
  - **Owner**
  - **Default Discretionary Access Control List (DACL)**

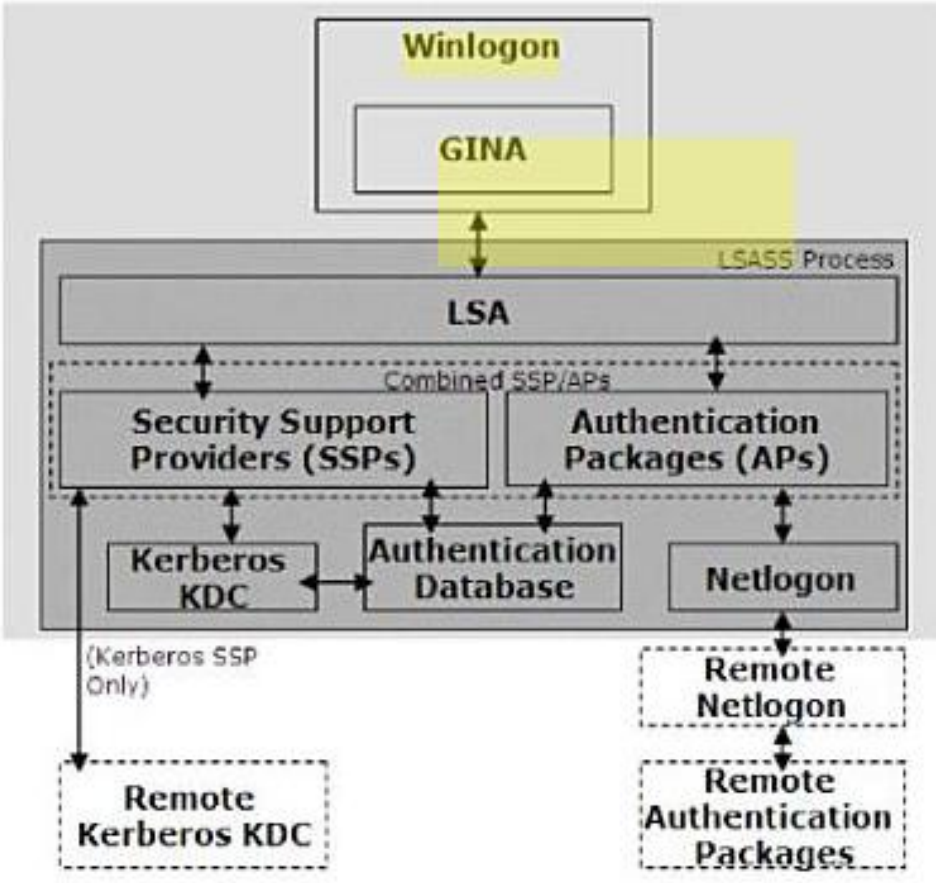
Whoami

```
C:\Documents and Settings\Administrator>whoami /all
用户信息
----------------
用户名                    SID
========================= ============================================
hacker07svr\administrator S-1-5-21-3597023897-2545237904-3072378509-500
组信息
-----------------
组名                                   类型   SID
          属性
====================================== ====== ====================================
Everyone                               已知组 S-1-1-0          必需的组，启用于默认，启用的组
HACKER07SVR\ORA_DBA                    别名   S-1-5-21-3597023897-2545237904-3072378509-1007 必需的组，启
用于默认，启用的组
BUILTIN\Administrators                 别名   S-1-5-32-544     必需的组，启用于默认，启用的组，组的所有者
BUILTIN\Remote Desktop Users           别名   S-1-5-32-555     必需的组，启用于默认，启用的组
BUILTIN\Users                          别名   S-1-5-32-545     必需的组，启用于默认，启用的组
NT AUTHORITY\REMOTE INTERACTIVE LOGON  已知组 S-1-5-14          必需的组，启用于默认，启用的组
NT AUTHORITY\INTERACTIVE               已知组 S-1-5-4           必需的组，启用于默认，启用的组
NT AUTHORITY\Authenticated Users       已知组 S-1-5-11          必需的组，启用于默认，启用的组
NT AUTHORITY\This Organization         已知组 S-1-5-15          必需的组，启用于默认，启用的组
LOCAL                                  已知组 S-1-2-0           必需的组，启用于默认，启用的组
NT AUTHORITY\NTLM Authentication       已知组 S-1-5-64-10       必需的组，启用于默认，启用的组

特权信息
----------------------
特权名                         描述                         状态
============================== ============================ ======
SeChangeNotifyPrivilege        跳过遍历检查                 已启用
SeSecurityPrivilege            管理审核和安全日志           已禁用
...
```

身份验证-winlogon/GINA/LSASS

- **Winlogon(winlogon.exe)**
  - 响应**Ctrl-Alt-Del (SAS: Secure Attention Sequence)**
  - 处理交互式登录和身份验证
- **GINA (gina.dll)**
  - **Graphical Identification and Authentication**
  - 显示登录窗口，提取用户秘密信息，移送给**LSA**
- **LSASS (lsass.exe)**
  - 保存并执行本地安全策略
  - 提供身份验证服务
  - 支持可扩展的**SSP**和**APs**



网络身份验证-netlogon

- 质询/应答方式
- 网络身份验证方式
  - **LANMan (win9x)**
  - **MSV1_0**
    - **NTLM (NT4SP3, NT5.x)**
    - **NTLMv2 (NT4SP4, NT5.x)**
  - **Kerberos (NT5.x Server)**

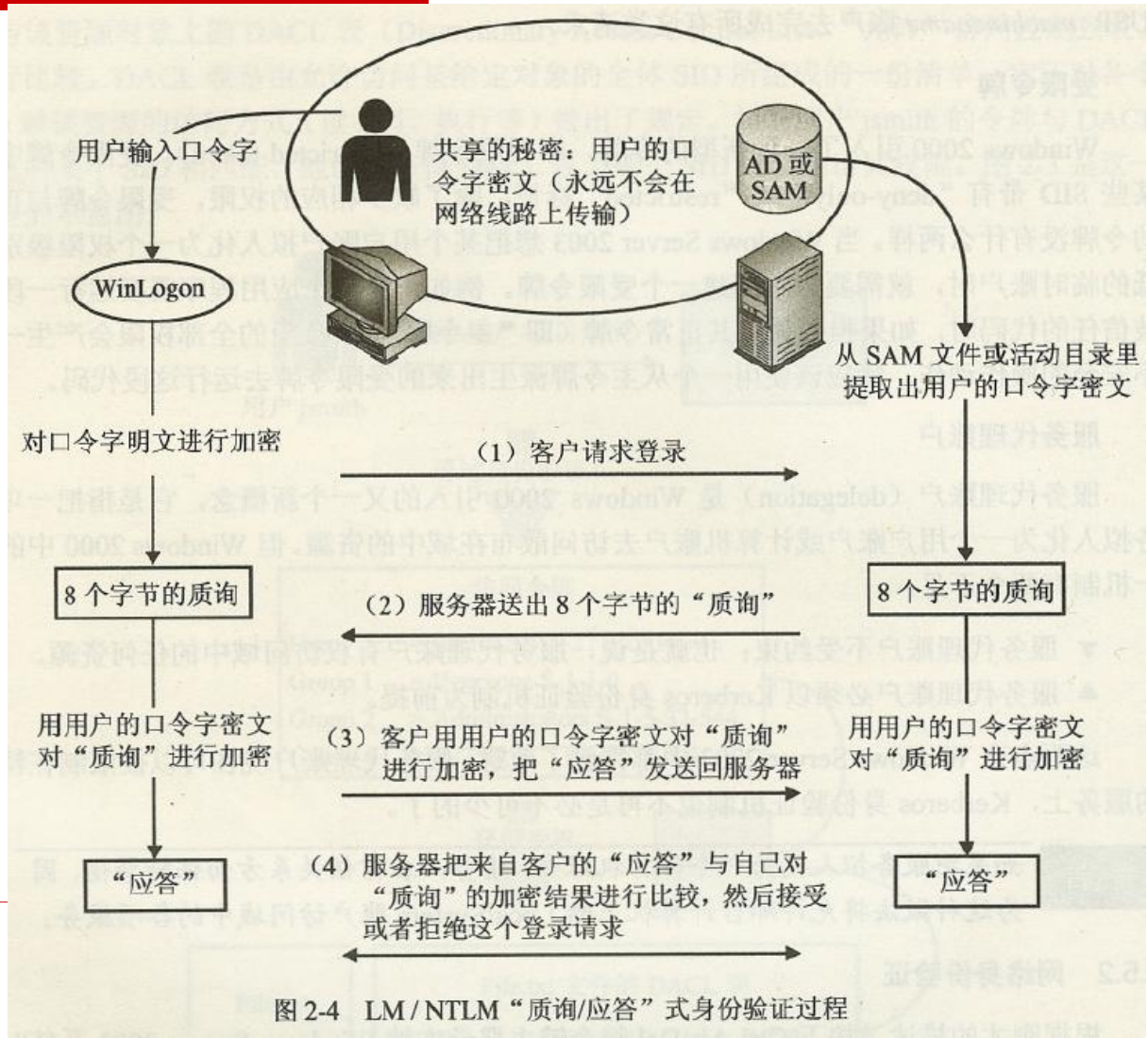
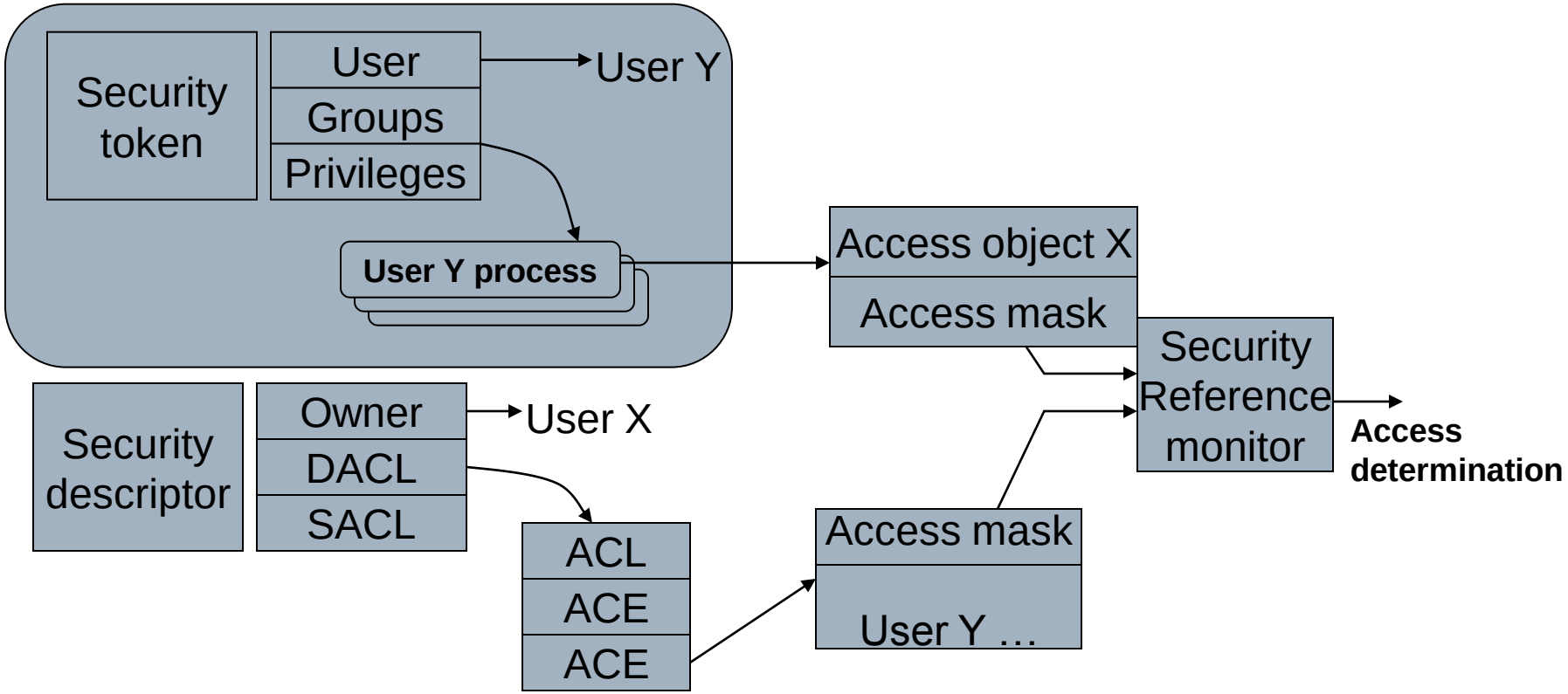


图 2-4　LM / NTLM “质询/应答”式身份验证过程

Authorization：授权(访问控制)

- 授权(Authorization)
  - 访问控制(Access Control)
  - 通过SRM机制确定某个通过验证的主体对某个对象是否具有访问权限,如是授予访问权.
- Windows授权机制: SRM

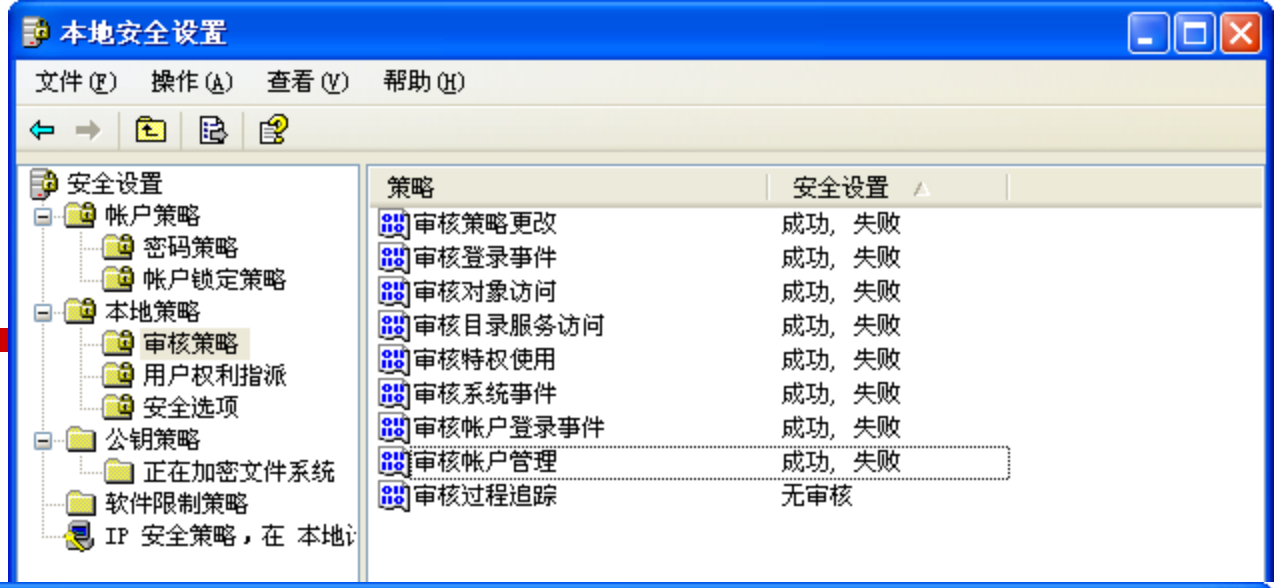
Object Security



审计: Auditing

- 审计策略
  - **Security Policy(本地安全策略)中定义**
  - 定义系统对哪些事件进行记录
- 审计内部机制
  - **LSASS: 保存审计策略, 传递给SRM**
    - 对象启动审计功能后，分配**SACL**表保存
  - **SRM: 生成审计记录，发送回LSASS**
  - **LSASS: 补充审计记录细节信息后，发送给EventLog(事件日志)**
  - **EventLog: 写入日志文件**

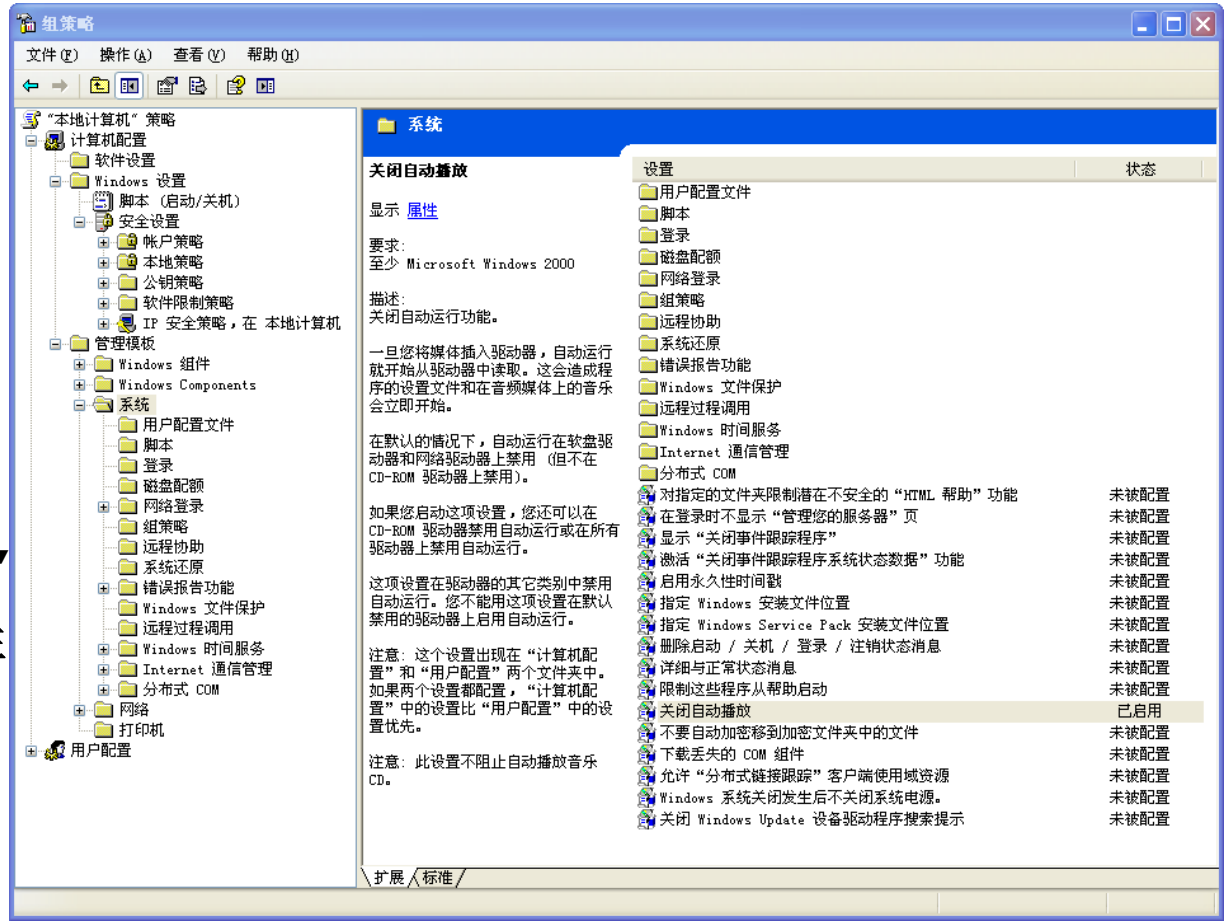
安全审计


本地安全设置
文件(F) 操作(A) 查看(V) 帮助(H)
安全设置
帐户策略
密码策略
帐户锁定策略
本地策略
审核策略
用户权利指派
安全选项
公钥策略
正在加密文件系统
软件限制策略
IP 安全策略，在 本地计
策略
安全设置
审核策略更改 成功，失败
审核登录事件 成功，失败
审核对象访问 成功，失败
审核目录服务访问 成功，失败
审核特权使用 成功，失败
审核系统事件 成功，失败
审核帐户登录事件 成功，失败
审核帐户管理 成功，失败
审核过程追踪 无审核


事件查看器
文件(F) 操作(A) 查看(V) 帮助(H)
事件查看器(本地)
应用程序
安全性
系统
Microsoft Office Diagnosti
Microsoft Office Sessions
安全性 41 个事件
类型 日期 时间 来源 分类 事件 用户 计算机
成功审核 2008-10-16 16:24:30 Security 特权使用 578 zhugejw PADT43
成功审核 2008-10-16 16:24:12 Security 特权使用 578 zhugejw PADT43
成功审核 2008-10-16 16:24:03 Security 特权使用 578 zhugejw PADT43
成功审核 2008-10-16 16:23:34 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:23:34 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:21:34 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:21:34 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:19:32 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:19:32 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:17:28 Security 特权使用 576 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:17:28 Security 登录/注销 528 LOCAL SERVICE PADT43
成功审核 2008-10-16 16:16:07 Security 对象访问 562 zhugejw PADT43
成功审核 2008-10-16 16:16:07 Security 对象访问 562 zhugejw PADT43
成功审核 2008-10-16 16:16:07 Security 策略改动 612 zhugejw PADT43
成功审核 2008-10-16 16:16:07 Security 对象访问 560 zhugejw PADT43

Windows安全配置策略

- 组策略
  - **gpedit.msc**
  - 计算机配置
  - 用户配置
- 最佳安全实践
  - **Google: “windows group policy best practice”**
  - 安全策略: 安全性和易用性的折中
  - 关闭自动播放

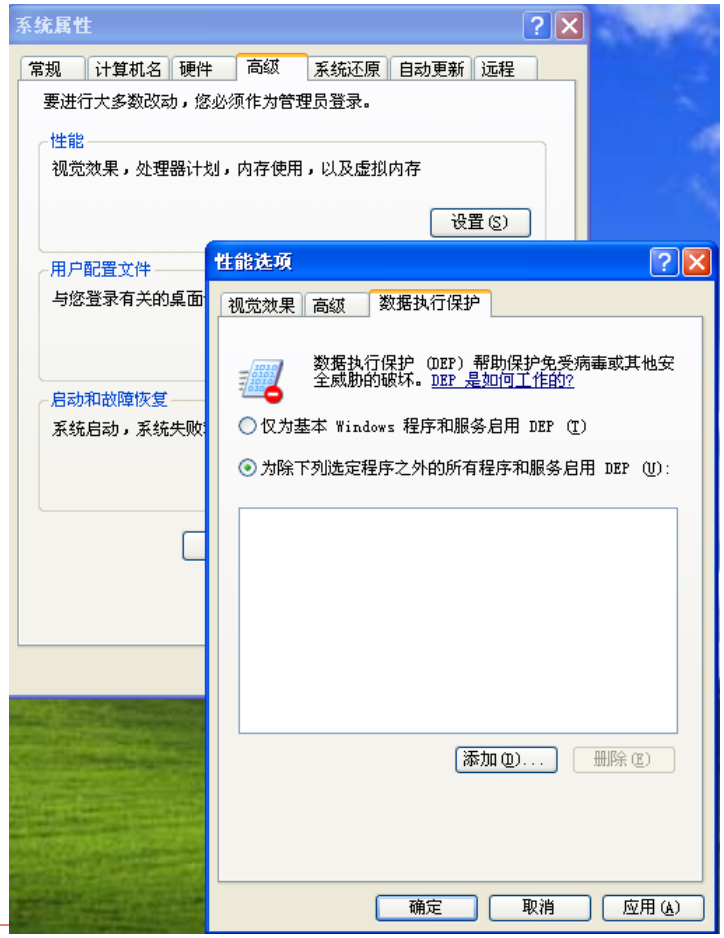


Windows其他安全机制

- **Windows安全中心**
  - 防火墙
  - 自动更新
  - 病毒防护
- **Internet选项**
  - 浏览器安全
  - 隐私保护-cookies
  - 安全证书

Windows其他安全机制(2)

- **DEP: 数据执行保护**
  - 堆栈不可执行
  - 但会造成某些特殊程序无法正常运行
    - 自加密软件
    - **Adobe**部分软件
  - **Windows XP缺省仅为基本Windows程序/服务启用DEP**
  - **Win 7缺省对全部程序启用**
- **ASLR：内存空间随机化**
  - **Vista/Win 7引入实现**



Windows其他安全机制(3)

- IPSec
  - IP加密和验证策略
  - 本地安全配置|IP安全策略
- EFS(加密文件系统)
  - NTFS文件系统被攻陷后抵御物理攻击
  - 性能及易用性问题，很少被使用
- WFP(Windows文件保护机制)
  - 防止Windows操作系统核心文件被恶意替换
  - “驱动程序签名”机制，备份目录dllcache
  - 绕开方法: WinLogon中的SFCDisable设置为0fffff9dh，永久性禁用WFP功能
  - WFP对木马、有经验攻击者很容易被绕过

下堂课预告

- **10月21日10-12节**
  - 作业3.2讲解
  - 课程5-Windows攻击技术及防御方法（部分）
  - 项目实践选题启动
- 建议课前阅读：
  - 基本:《黑客大曝光》第3章“查点”p80-122、第4章“攻击Windows操作系统”
  - 进阶:《Windows Server 2003黑客大曝光》第2部分“侦察”、第3部分“分而治之”、第4部分“攻击脆弱服务和客户端”
- 可从课程共享FTP获取相关资源

Thanks

诸葛建伟

zhugejianwei@icst.pku.edu.cn