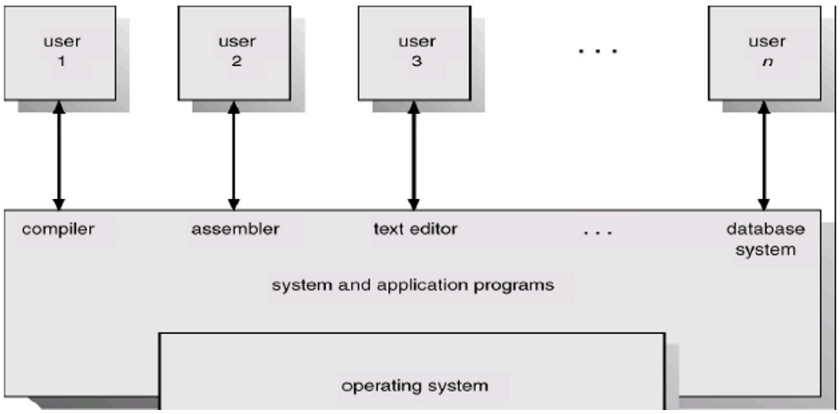
5-1 win系统安全

2019年4月10日 23:36

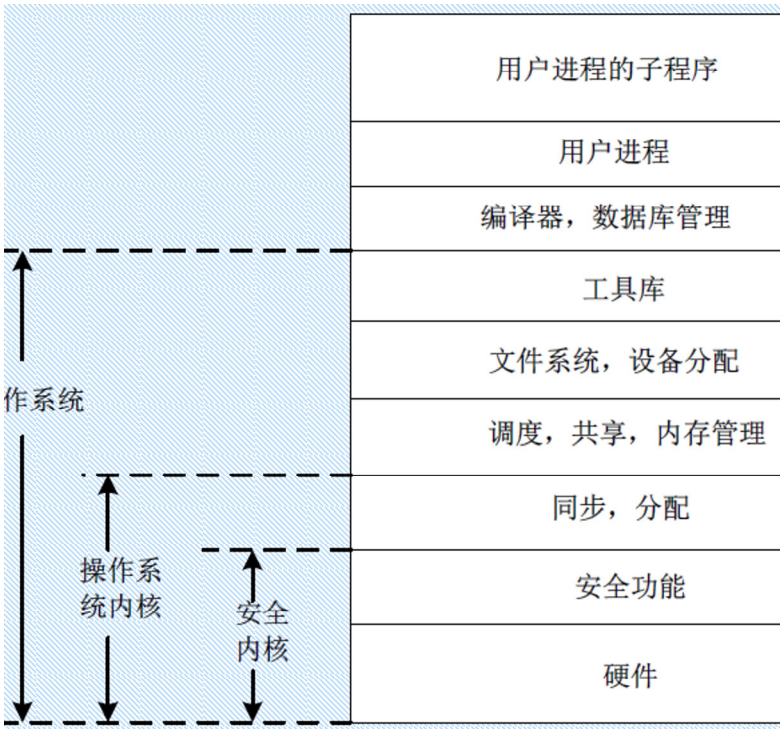
1 操作系统安全基础

1.1 计算机系统组成的层次形式

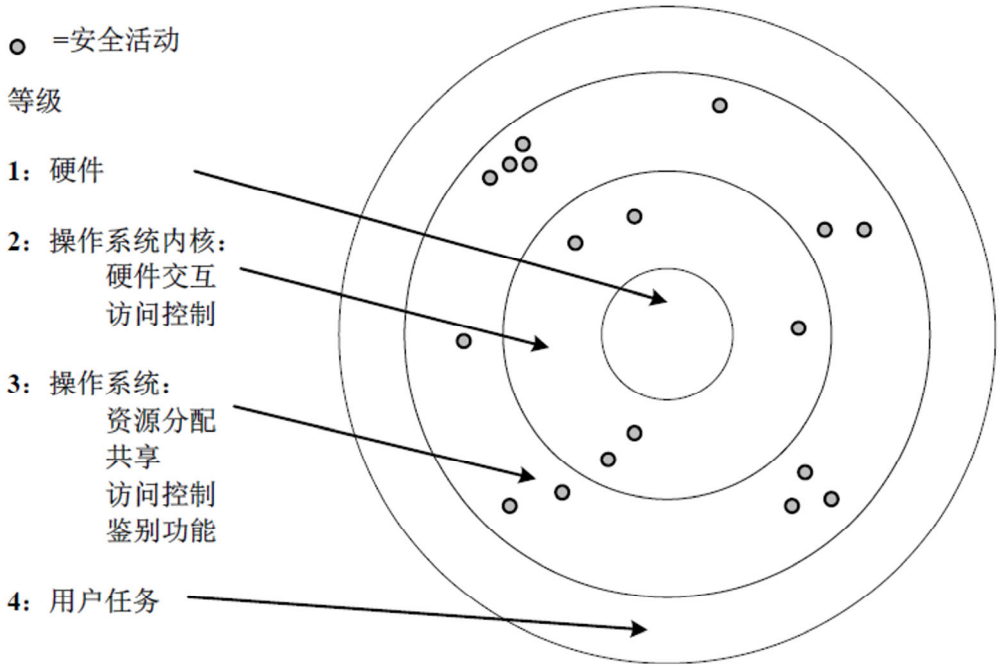
- 

- 操作系统是信息系统资源的基本控制器——这使其成为主要的攻击目标

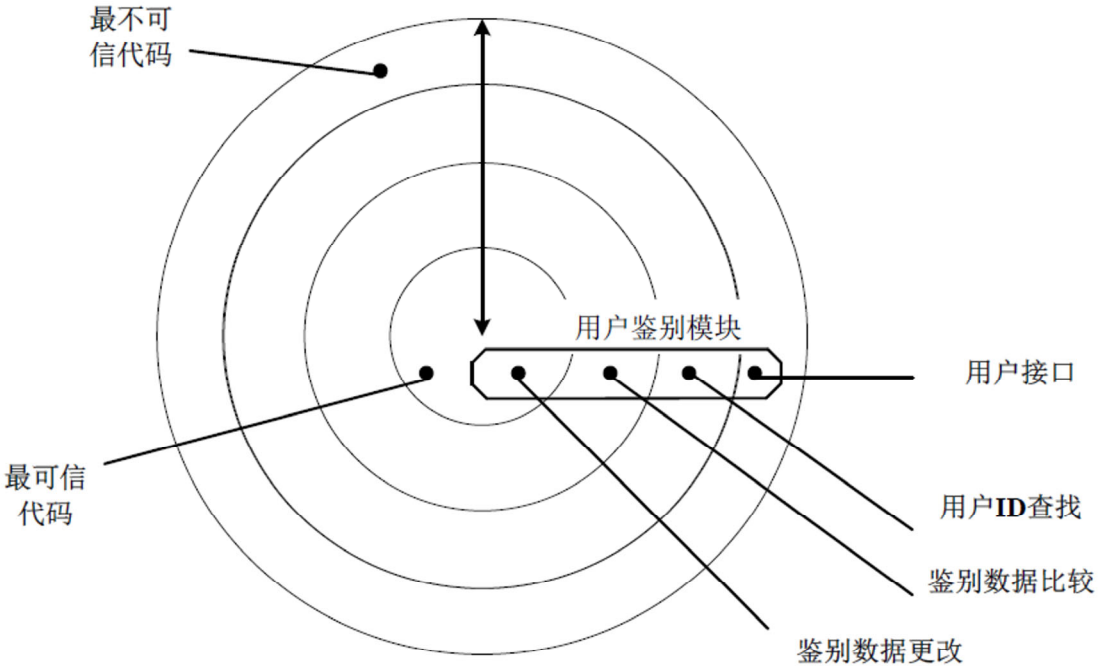
分层的操作系统



组合的安全内核/操作系统



操作系统各层的身份验证功能

- 

1.2 操作系统的安全性方法

操作系统的安全目标

- 目标1:允许多用户安全的共享单机
  - 进程、内存、文件、设备等的分离与共享
- 目标2:确保网络环境下的安全操作-安全需求
  - 鉴别
  - 访问控制
  - 安全通信
  - 记录日志&审计
  - 入侵检测
  - 恢复

保护对象

- 内存
- 可共享的I/O设备，如磁盘
- 可连续复用的I/O设备，如打印机
- 可共享的程序或者子程序
- 网络
- 可共享数据

保护方法

- 基本原理
  - 访问控制

    对操作系统各种资源的存取控制，既包括对设备（如内存、虚拟存储器或磁盘等外存储器）的存取控制，也包括对文件、数据的存取控制。

    - 隔离控制
        - 物理隔离。不同的进程使用不同的物理对象。例如把不同的打印机分配给不同安全级别的用户。
        - 时间隔离。不同安全需求的进程，在不同的时间执行。
        - 逻辑隔离。限制程序的访问，使其不能访问许可域之外的对象，用户感觉好像是在没有其他进程的情况下执行自己的进程。
        - 加密隔离。进程加密其数据和计算，使其他进程无法理解。
    - 认证
    - 安全通信
    - 安全审计
    - 入侵检测
    - 恢复

保护模式

- 内存保护模式
- cpu运行模式
- 系统调用

内存保护

- 操作系统进程、用户进程：具有不同的权限
    - 界地址
    - 界地址寄存器
- 保证一个用户的进程不能访问其他人的内存空间
    - 栅栏
        - 分段
        - 分页
    - 基址/范围寄存器
    - 重分配

CPU模式(又称处理器模式)

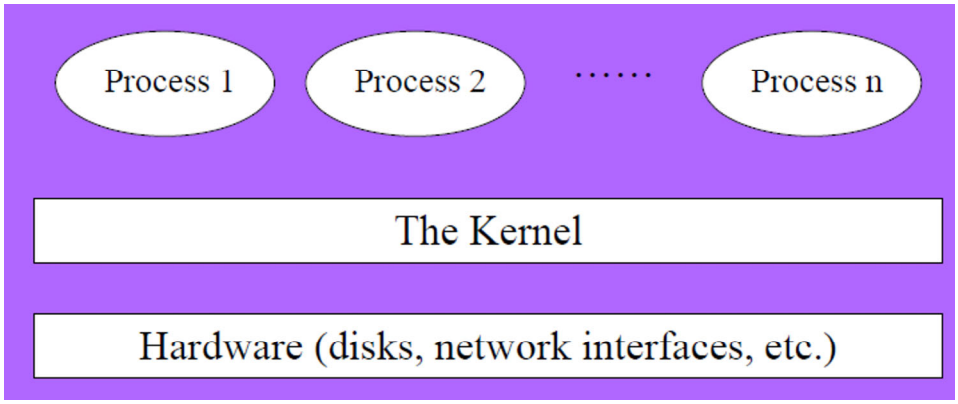
- 系统模式(特权模式，主模式，超模式，内核模式)
    - 可以执行任意指令、访问任意内存地址、硬件设备、中断操作、改变处理器特权状态、访问内存管理单元、修改寄存器。
- 用户模式
    - 受限的内存访问，有些指令不能执行
    - 不能：停止中断，改变任意进程状态，访问内存管理单元等。
- 从用户模式转到系统模式的切换必须通过系统调用(Systemcalls)

(不考)内核空间vs用户空间

- 操作系统的一部分运行在内核模式--故称为OS kernel

- 操作系统的其他部分运行在用户模式，包括服务程序(daemon programs)，用户的应用等
  - 作为进程运行
  - 形成用户空间
- Root(orSuperuser,Administrator)运行的进程可能在内核模式或用户模式

(不考)内核空间vs用户空间的层次性视图

- 

(不考)内核实现方法：

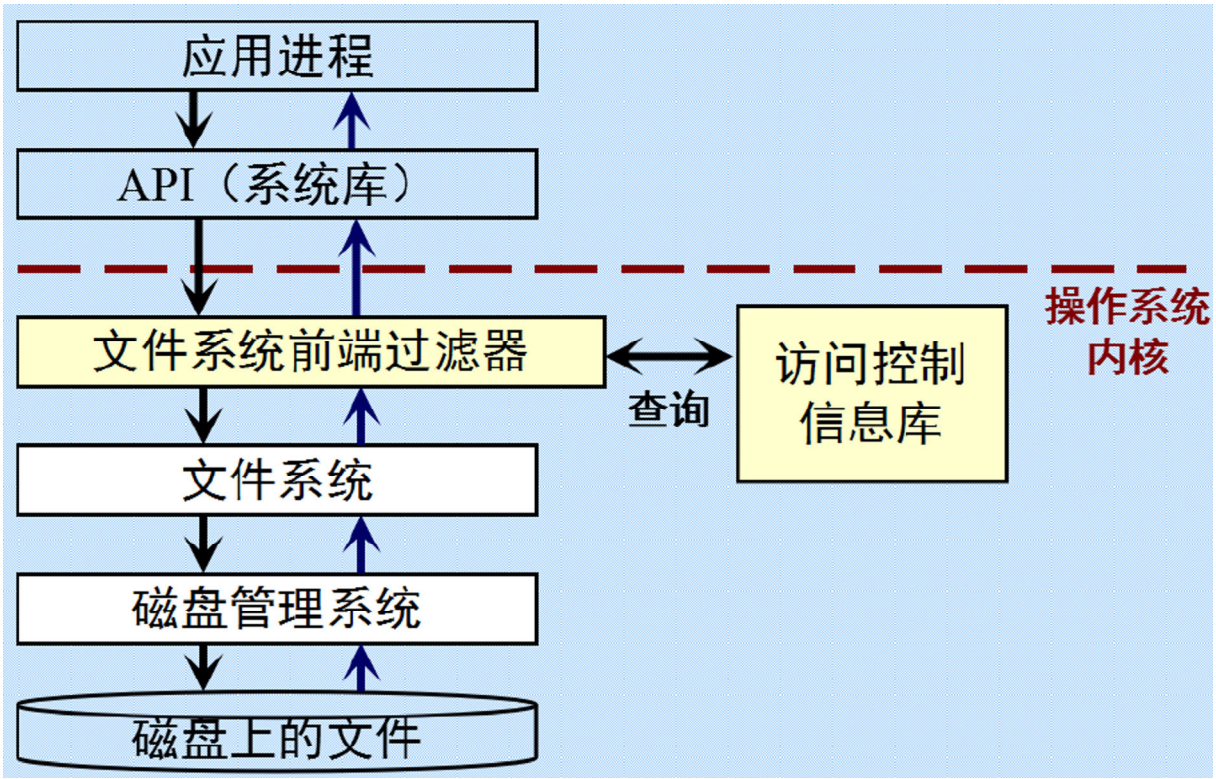
- 单核:一个大内核提供所有的服务，包括文件系统、网络服务、设备驱动等。
  - 所有内核代码运行在单地址空间，互相之间会产生影响。例如Linux26内核有6百万条代码
  - 优点:高效
  - 缺点:复杂，某部分的bug会影响整个系统
- 微内核:内核较小，仅提供执行系统服务必须的机制。
  - 内核提供：低地址空间的管理，线程管理，进程间通信（IPC）
  - 操作系统的服务可在用户模式下工作：包括设备驱动、协议栈、文件系统、用户的接口代码
  - 优点:可实现最小特权，容忍设备驱动的失败/错误等
  - 缺点:性能差，系统的关键服务出错会使得系统停机

系统调用

涵义：从用户模式进入内核模式的系统程序

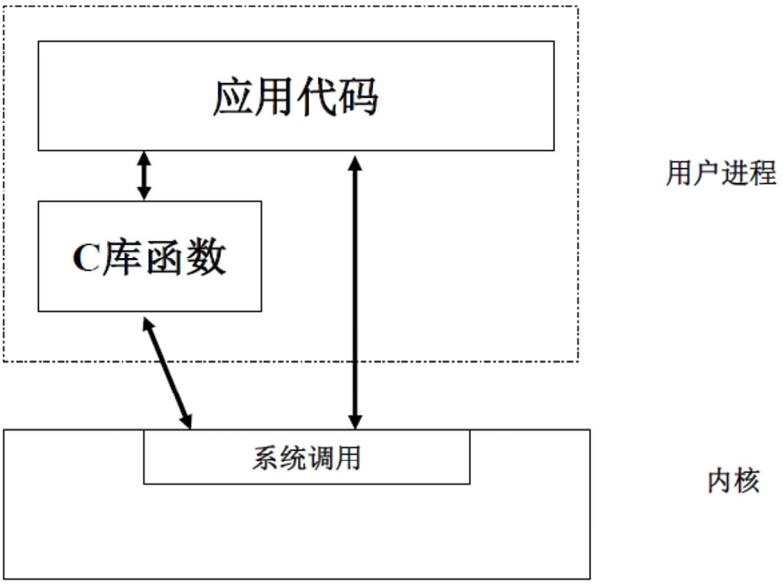
- 系统调用是用户程序和内核交互的接口
- 所有的操作系统都提供多种服务的入口点，由调用程序向内核请求服务；系统调用不能更改
- 系统调用把应用程序的请求传递给内核，调用相应的内核函数完成所需的处理，将处理结果返回给应用程序；如果没有系统调用和内核函数，用户编写大型应用程序非常困难。

访问控制在操作系统中的实现

- 

函数库与系统调用的关系

- UNIX为每个系统调用在标准C库中设置一个同样名字的函数。用户进程用标准C调用序列来调用这些函数，启动函数调用对应的内核服务。
  - 从执行者角度，系统调用和库函数有重大区别
  - 从用户角度，区别不重要

- 

系统调用分类

- 进程控制
- 文件管理
- 设备管理
- 信息维护
- 通信

1.3 用户空间的安全机制

- 用户认证
- 访问控制
- 记录日志和审计
- 入侵检测
- 备份/恢复

备份策略：

- 实时备份：持续跟踪目标数据的改变，并将其备份。
- 整体备份：一个备份周期内的数据完全备份。
- 增量备份：只备份上次备份以后有变化的数据。

可信计算机系统评估准则TCSEC

- TCSEC，(TrustedComputerSystemEvaluationCriteria)，简称橙皮书；
- 1983年由美国NCSC(NationalComputerSecurityCenter)发表；
- 2005年为CC(CommonCriteria)替代，ISO15408；
- TCSEC对计算机的安全级别进行了分类，由低到高，分为D、C、B、A级。

(了解)TCSEC对计算机安全级别的分类

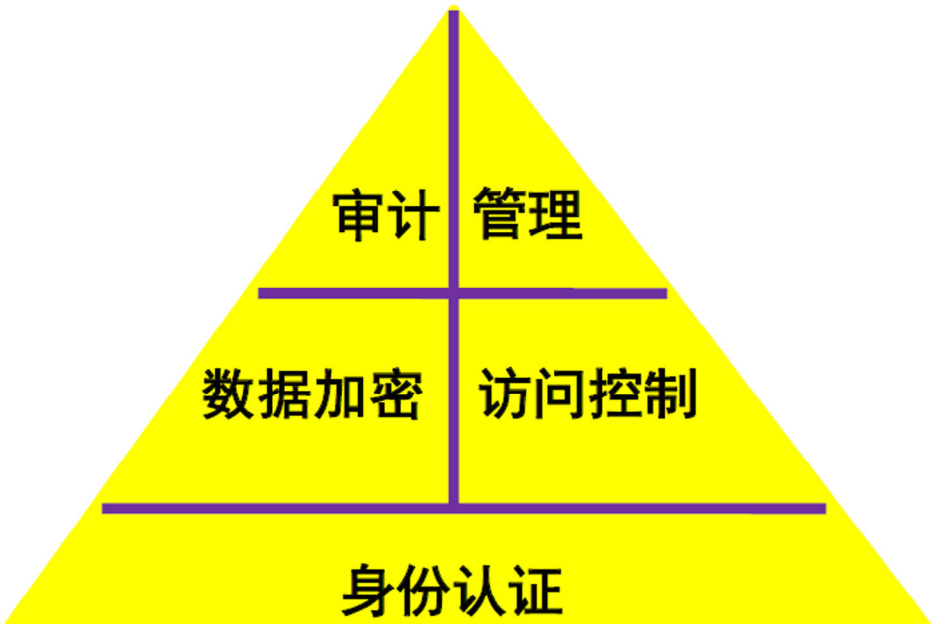
- D类安全等级
  - D类安全等级只包括D1一个级别，D1的安全等级最低；
  - 系统只为文件和用户提供安全保护；
  - D1系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。
- C类安全等级
  - C类安全等级能够提供审记的保护，并为用户的行动和责任提供审计能力。
  - C1级：自主安全保护系统。系统的可信任运算基础体制（TrustedComputingBase，TCB）通过将用户和数据分开来达到安全的目的。C1系统中，用户认为系统中的所有文档都具有相同的机密性。
  - C2级：受控存取控制系统。系统比C1系统加强了可调的审慎控制，通过登陆过程、安全事件和资源隔离来增强这种控制。
- B类安全等级
  - B类系统：强制保护类
  - 具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。
  - B1安全级别
    - 标记安全保护级。
    - 系统对每个对象都进行灵敏度标记；系统使用灵敏度标记作为所有强迫访问控制的基础；
    - 系统必须通过审计来记录未授权访问的企图。

    - B2安全级别
        - 结构保护级
        - B2系统必须满足B1系统的所有要求。
        - B2系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。
    - B3安全级别
        - 安全域级。
        - B3系统必须符合B2系统的所有安全需求。
        - B3系统具有很强的监视委托管理访问能力和抗干扰能力。
        - B3系统必须设有安全管理员。
- A类安全等级
    - 验证保护级
    - A类系统的安全级别最高。目前，A类安全等级只包含A1一个安全类别。
    - A1系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统，设计者必须运用核对技术来确保系统符合设计规范。

2 Windows安全概述

2.1 Windows操作系统安全功能概览

- C2级安全功能
    - 安全登录
    - 自主访问控制
    - 安全审计
    - 客体重用object reuse
        - 在对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的全部授权，当主体获得对一个已被释放客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。
- B级安全功能
    - 可信通路
- 其他安全功能
    - 加密文件系统（Windows2000之后）
    - IPSec（Windows2000之后）
    - Kerberos（Windows2000之后）
    - PKI（Windows2000之后）
    - 防火墙（WindowsXP之后）

- 

Windows体系结构

- Windows操作系统采用用户模式和核心模式分离的体系结构；
- 用户模式下的软件在无特权的状态下运行，系统资源访问权限有限；
- 所有对核心模式的访问都是受保护的，避免失控的用户进程破坏处于核心模式下的低层次的系统驱动程序。

2.2 Windows安全子系统

- 活动目录
  - 活动目录是一种分布式的目录服务系统。在分布式环境中，要求有各种信息可以被各种应用（用户、程序）很方便地访问读取。
  - 当用户使用域帐户而非本地帐户登录时，Windows客户端会使用活动目录来认证。
  - 活动目录的安全管理单元是域，域中的所有用户和计算机执行相同的域安全策略。
- Winlogon进程
  - 用户登陆程序。
  - 系统启动自动启动的一个程序。
  - 负责管理用户登录和注销过程，加载登录界面并监视安全认证的顺序。
  - 程序
    - System32\Winlogon.exe
  - 功能
    - 负责响应SAS
    - 管理交互式登录会话
- 图形化标识和验证GINA(GraphicalIdentificationandAuthentication)
  - 为用户提供图形化的交互式登录对话框，包括几个动态库文件，被Winlogon进程调用。
  - GINA调用LSA
  - 程序

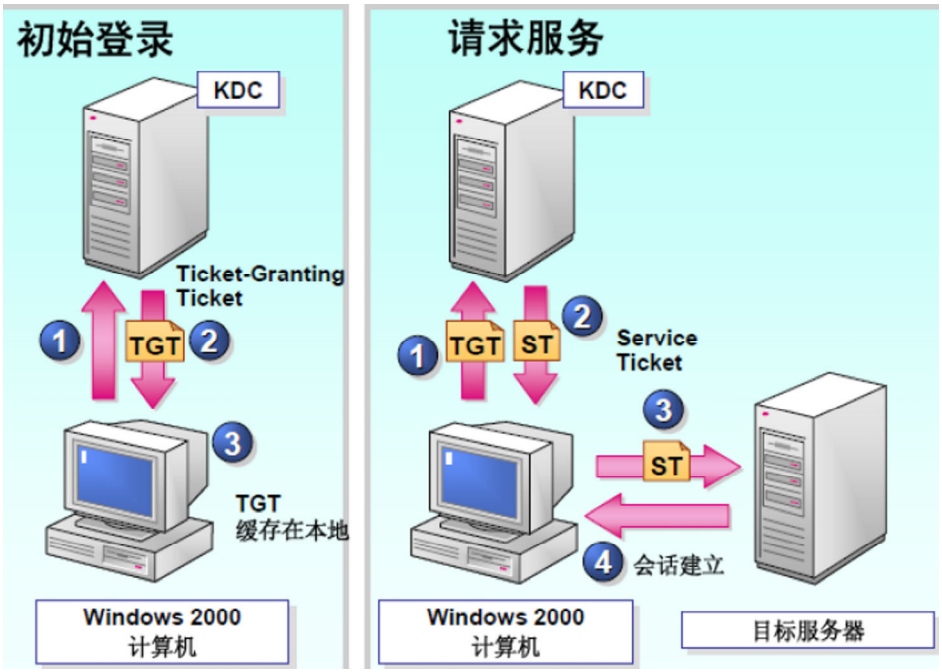
        - System32\Msgina.dll
        - 运行在Winlogon进程中
    - 功能
        - 获得用户的名称
        - 获得用户口令或智能卡的Pin码
- 本地安全认证LSA（LocalSecurityAuthority）
    - 安全子系统的核心组件，负责加载认证包，管理域间的信任关系。
    - 确认SAM中的数据，控制各种类型的用户进行本地和远程登录，提供用户存取许可确认、产生访问令牌。
    - 程序
        - System32\lsass.exe
        - System32\lsasrv.dll（主要由该模块实现）
    - LSA存在于用户模式的进程lsass.exe中，负责管理、执行Windows的本地安全策略，在帐户登陆到系统时发放安全令牌。
    - 安全策略包括口令策略、审计策略和权限设置等。
    - 将SAM产生的审计信息保存在日志文件中。
    - Lsass策略数据库
        - 位置

            HKEY_LOCAL_MACHINE\SECURITY
        - 内容

            哪些域是可信任的

            允许哪些用户以何种方式登录系统

            授予用户哪些权限
- Kerberos身份认证
    - Windows的域身份认证协议。
    - 使用Windows操作系统的计算机之间以及支持Kerberos身份认证的客户之间的身份认证。
    - 运行在Lsass进程环境下的DLL，实现Kerberos认证协议。

- 

- MSV1.0身份认证
  - 为不支持Kerberos身份认证的Windows客户提供基于NTLM的身份认证。
  - Msv1_0dll：运行在Lsass进程环境下的DLL，实现LANManager2协议
- 安全帐户管理器SAM（SecurityAccountManager）
  - 数据库存储本地用户和本地组的帐户以及相关安全信息。
  - 当用户用本地帐户登录到计算机时，SAM进程(samsrv)获得登录信息并查询windowssystem32\config目录下的SAM数据库，如果有匹配的认证，用户就可以登录系统。
  - SAM文件是二进制模式的，而不是文本格式的，口令用MD4散列算法存储。
  - 程序
    - System32\Samsrv.dll
    - 运行于Lsass进程中
  - 功能
    - 提供一组管理本地用户和用户组的子例程
  - SAM数据库
    - 位置

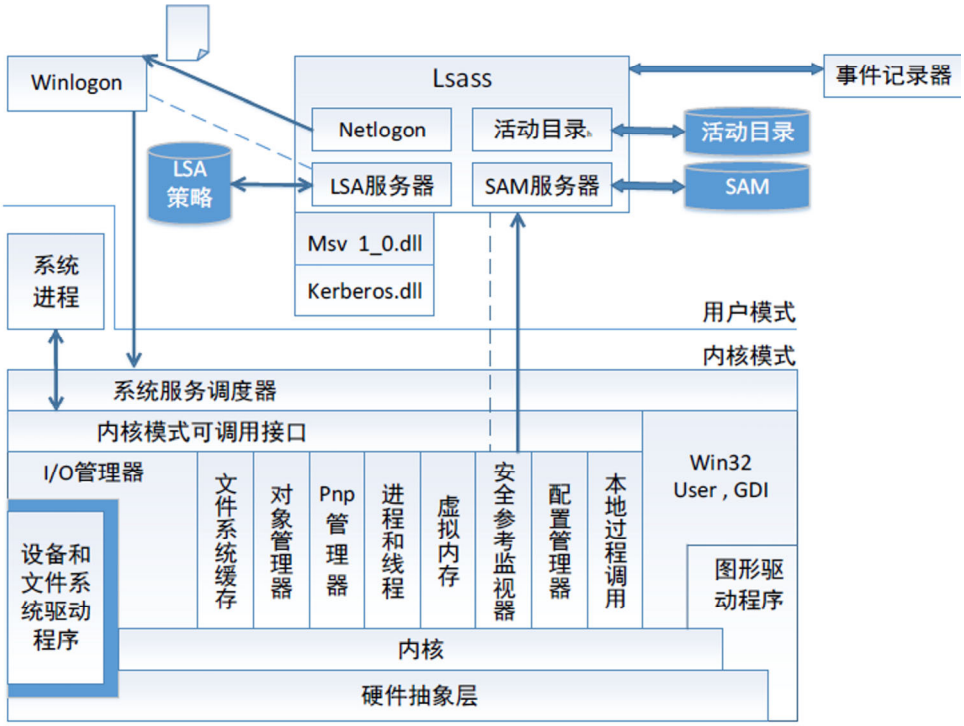
      HKEY_LOCAL_MACHINE\SAM
    - 内容

      本地用户和用户组、以及它们的口令、账户限制等

      系统的管理员恢复账号及口令
- 安全参考监视器SRM(SecurityReferenceMonitor)
  - 内核模式组件，执行对象访问合法性检查、产生审计日志条目、提供用户权限。
- Netlogon进程
  - 网络登录服务。
  - 维护计算机到其所在域内的域控制器的安全信道。
  - 域登录时用到的，建立安全信道，用户名、密码在信道里是加密传输的。
  - Winlogon处理本地键盘登录，而Netlogon处理网络登录。

- 程序

  System32\Netlogon.dll

- 

Windows 安全子系统