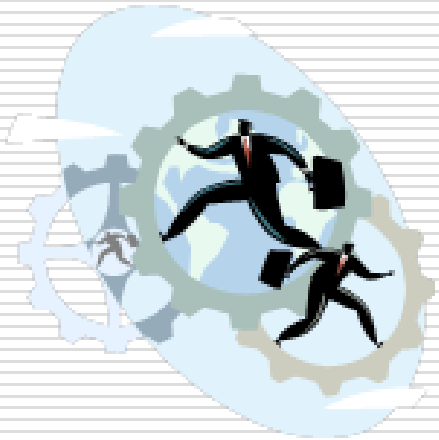


操作系统安全

二、windows系统安全概述

- 上期回顾
  - 重点：计算机系统的纵深防御体系
    - 具体安全服务
    - 安全管理

windows系统安全概述

1. Windows安全需求&评估标准
2. Windows 基础与安全
3. Windows 20/03新增安全特性

1.1 Windows系统的安全需求

- 安全威胁的来源
  - 系统主机层面
  - 应用服务层面
  - 网络通讯层面
  - 安全管理层面
- 用户规模不同，其相应的安全需求也不一样
  - 单个用户
  - 小，中规模组织或单位
  - 大规模组织或单位

Windows 9X 内核系列的发展	Windows NT内核系列的发展
1983年11月：Windows宣布诞生	
1985年11月：Windows1.0	
1987年4月：Windows 2.0	
1990年5月：Windows 3.0	
	1993年5月：Windows NT 3.11
1994年2月：Windows 3.11	1994年9月：Windows NT 3.5
1995年8月：Windows 95	1995年6月：Windows NT 3.51
	1996年8月：Windows NT 4.0
	1997年9月：Windows NT 5.0 Beta 1
1998年6月：Windows 98	1998年8月： Windows NT 5.0 Beta 2
1999年5月：Windows 98 SE	1999年4月：Windows 2000 Beta 3
1999年11月：Windows Mill. Beta 2	
2000年9月：Windows me	2000年2月：Windows 2000
	2001年10月：Windows XP
2001年1月：Windows 9X内核正式终止	2003年5月：Windows Server 2003
	2006年5月：Windows visa
	2008：Windows Server 2008
	2009：Windows 7
	2012：Windows8 windows server2012
	2016：Windows10 windows server2016

	2018: windows server2019

1.2信息安全评估标准

- TCSEC（Trusted Computer System Evaluation Criteria）
- ITSEC（Information Technology Security Evaluation Criteria）
- BS 7799:2000标准体系,后升级为ISO 17799标准
- CC(Common Critical)标准

过程：

- 1983年，美国国防部出版了历史上第一个计算机安全评价标准——《可信计算机系统评价准则（TCSEC）》，1985年，美国国防部对TCSEC进行了修订。
- 1991年，在欧洲共同体的赞助下，英、德、法、荷4国制定了拟为欧共体成员国使用的共同标准——信息技术安全评定标准（ITSEC）。
- 随着各种标准的推出和安全技术产品的发展，美国和加拿大及欧共体国家一起制定了通用安全评价准则（Common Criteria for IT Security Evaluation，CC）

TCSEC定义的内容

A 级	校验级保护，提供低级别手段
B3 级	安全域，数据隐藏与分层、屏蔽
B2 级	结构化内容保护，支持硬件保护
B1 级	标记安全保护，如System V等
C2 级	有自主的访问安全性，区分用户
C1 级	不区分用户，基本的访问控制
D 级	没有安全性可言，例如MS DOS

- 根据TCSEC标准，通常称B1级以上的操作系统为安全操作系统。
- 目前主流商用操作系统包括Windows都是C2级

- **基于标记安全的保护Labelled Security Protection Profile:LSPP**

一个高可信的安全操作系统本身也是一个难题，其核心是实现LSPP，LSPP被认为是B1级安全操作系统的基本要求。也就是实现强制访问控制MAC（MAC是基于标记安全的）。

- **可控的访问安全保护Controlled Access Protection Profile：CAPP**

如果只实现了CAPP,只能满足C2级的要求。

- 尽管有些的Unix操作系统实现了LSPP，但最有价值的却是在Windows上实现LSPP，因为超过90%以上的操作系统是Windows，无论是那个国家，无论是军方还是政府，都不例外。

1.2信息安全评估标准

□ Windows 的C2级别的安全性策略

- **强制的用户标识和认证**

  所有用户都必须以唯一的登录标识和密码来鉴别自身。

- **自主访问控制（Discretionary Access Control，DAC）**

  自由的访问控制 资源的所有者必须能够控制对资源的访问。

- **可记账性和审核**

  能够审计所有安全相关事件和个人活动

  只有管理员才有权限访问

- **对象的重用**

  必须能够保护对象在完成其使命后，不再被其他对象所利用。

- 如果在CC标准下，Windows属于EAL4 级别

windows系统安全概述

1. Windows安全需求&评估标准
2. Windows 安全体系及特性
3. Windows 20/03新增安全特性

2.1 Windows的安全体系结构

基本安全术语的出现：

1969年B.W.Lampson通过形式化表示方法运用主体（subject）、客体（object）和访问矩阵（access matrix）的思想第一次对访问控制问题进行了抽象。

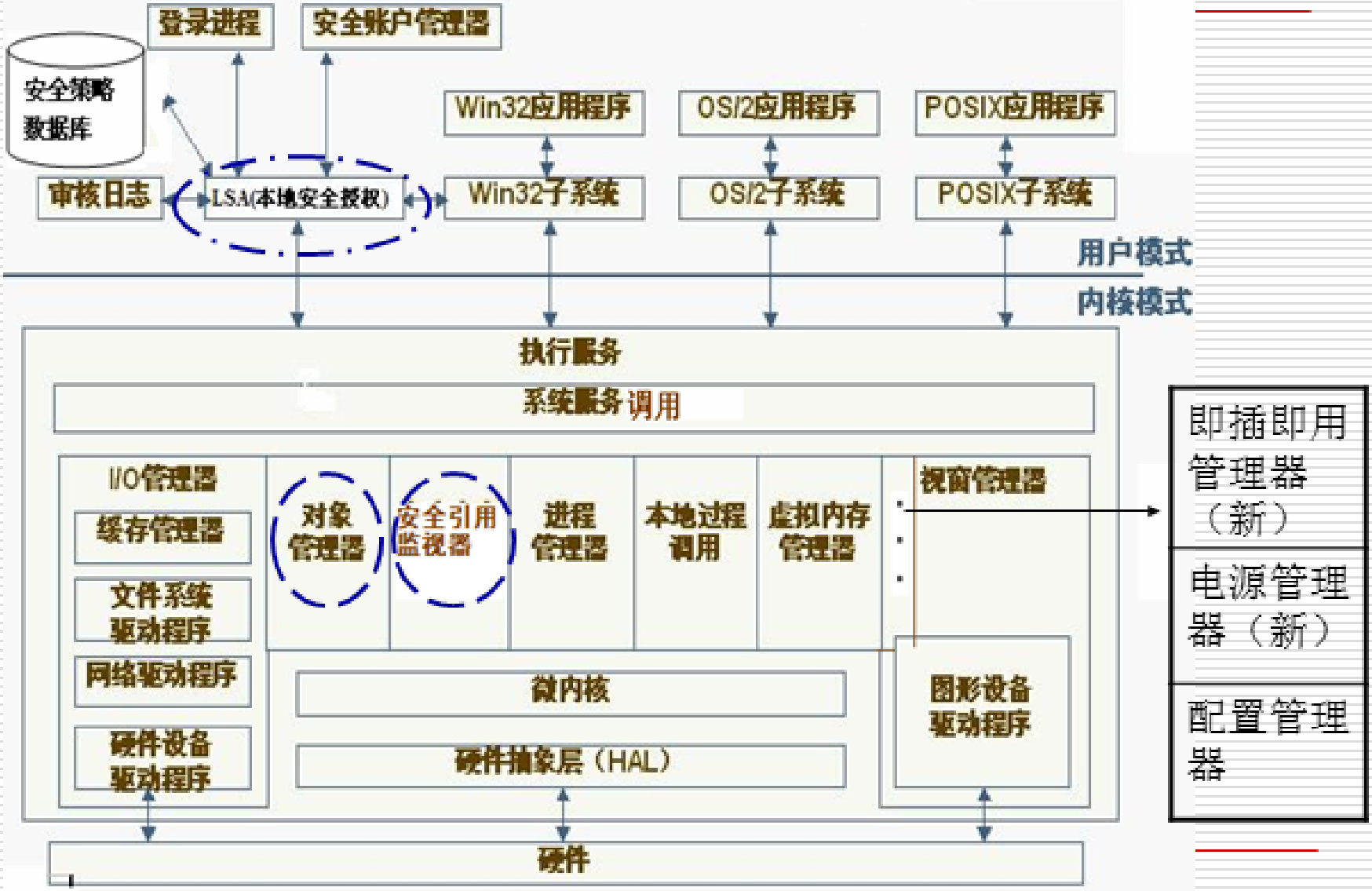
1972年，J.P.Anderson在一份研究报告中提出了引用监视器（reference monitor）、访问验证机制（reference validation mechanism）、安全内核（security kernel）和安全建模（modeling）等重要思想。

1973年，B.W.Lampson提出了隐蔽通道的概念，他发现两个被限制通信的实体之间如果共享某种资源，那么它们可以利用隐蔽通道传递信息。

2.1 Windows的安全体系结构

- Windows NT体系结构分为内核模式（Kernel Mode）和用户模式（User Mode）
  - Intel的CPU将特权级别分为4个级别：ring0,ring1,ring2,ring3。Windows只使用其中的两个级别ring0和ring3
  - 内核模式中的代码具有极高的特权，可以直接对硬件进行操作和直接访问所有的内存空间 ring0级
  - 用户模式中的代码拥有较低的特权，不能对硬件直接进行访问，内存访问受限。 ring3级

2.1Windows NT 安全体系结构



2.1Windows NT 安全体系结构

- 用户模式下
  - 本地安全子系统:支持Windows的身份验证，审核
    - 核心为 LSA (local security authentication)
    - 需和win32子系统通信
- 内核模式下
  - 组成内核模式的整套服务被称为执行服务
    - 对象管理器（OM:Object Manager）
    - 安全引用监控器（SRM: security reference monitor）

2.1Windows NT 安全体系结构

本地安全授权（LSA）

- LSA负责使所有本地和远程的用户登录生效，生成安全访问令牌；访问令牌：访问令牌是一个二进制的数据包，它描述了用户的访问权限以及用户所属的组。
  - 令牌在每个进程中都存在。
- 管理本地安全策略
- LSA负责记录安全引用监视器(SRM)的任何审核消息所产生的事件日志.

2.1Windows NT 安全体系结构

安全引用监控器SRM

- SRM和对象管理器（Object Manager）联合起来，实施访问控制策略和审核策略。

（由本地安全策略和域中的组策略设定）

2.1Windows NT 安全体系结构

- 对象管理器（Object Manager）
  - 作用：负责对象的命名、保护、分配和处理
  - 管理的对象包括：
    - 目录、文件、注册表项、设备、符号链接
    - 进程、线程
    - 网络共享资源
    - 端口
    - 窗口
    - 事件对象
    - 管道、内存、通讯等
  - 每一个资源对象都与一个安全描述符相关联。

NT 所引入的其他安全项

- 用户账户（User Account）
- 权限（Right）
- 共享权限
- 安全审核（Security Audit）
- NTFS (Windows NT File System)
- 域(Domain)
- 工作组（Workgroup）

Windows 的用户和用户组

- 用户账户
  - 使用用户名和密码进行标识
  - SID(Security Identifiers,SID安全标识符)：账户的关键标识符,所有内部进程 都使用SID识别用户账号。
- 用户组账户
  - 具有相似工作或资源要求的用户可组成一个用户组。
  - 对资源的存取权限许可分配给一用户组，就是同时分配给该组中的所有成员。

Windows NT内置的用户和组帐号

- 内置用户账号
  - Administrator 和 Guest

    提示：
    - Adminstrator账号是最高级别的账号，应重命名该账号并设置密码以隐藏它，以免受到攻击。
    - 保持Guest账号的禁用状态。
  - System/LocalSystem:技术角度最高权限，自动运行程序所使用的运行环境

- 内置用户组帐号
  - Administrators ：管理员组
  - Users ： 普通用户组
  - Guests ： 来宾用户组
  - Backup Operators 备份操作组，做系统的备份操作
  - Replicator ： 复制操作组
  - *Operators（Print ,Account, Server）
  - Domain*(Administrators, Users, Guests) ： 只在域服务器上的组
  - 特殊组(Network, Interative, Everyone, ….)

2.1.2 NT 所引入的安全特性

- 用户账户（User Account）
- 权限（Right）
- 共享权限

访问控制

- 安全审核（Security Audit）
- NTFS (Windows NT File System)
- 域(Domain)
- 工作组（Workgroup）

2.1.2 NT 所引入的安全特性

- 用户账户（User Account）
- 权限（Right）
- 共享权限
- 安全审核（Security Audit）
- NTFS (Windows NT File System)
- 域(Domain)
- 工作组（Workgroup）

NTFS

操作系统中管理文件目录的机制

- FAT(File Allocation Table标准文件分配表)
  - 适合于较小的卷
  - 没有安全性
- NTFS
  - 支持用户的访问控制和文件（夹）所有权的设置。
  - 支持对共享文件夹的权限指定。
  - 使用事务日志自动记录文件和文件夹的更新
  - 支持文件和文件夹的压缩
  - 支持透明加解密

2.1.2 NT 所引入的安全特性

- 权限（Right）
- 许可（Permission）
- 共享权限
- 用户账户（User Account）
- 安全审核（Security Audit）
- NTFS (Windows NT File System)
- 域(Domain)
- 工作组（Workgroup）

} 组织管理方式

工作组，域 和信任关系

- 工作组（Workgroup）
  - 为小型办公系统提供了资源共享功能，使用户可共享其他计算机上的本地资源。
  - 不共享任何用户账户信息和组账户信息，每个系统使用自身的SAM (security account manager)数据库独立验证
    - **被系统进程以独占的方式使用，用户不能读取**
  - 适用于小型的环境，不进行集中控制，用户数量增多时，难以管理。

工作组，域 和信任关系

- 域（Domain）

域是一批具有集中安全授权机构和若干台工作站和成员服务器的计算机集合。

- 特点
  - 域为用户，组和计算机账户定义了管理边界范围
  - 一个域中的所有用户共享域用户账户数据库和普通的安全策略。
  - 每台计算机不需要提供自己的验证服务。
  - 一旦用户用域验证服务通过验证，就可以在域内访问权限内资源了，如Exchange Server，SharePoint Server，File Server，SQL Server，打印机共享。

工作组，域 和信任关系

信任关系

当网络更大时，可以用信任关系来创建并链接多个域。

- 信任关系是域之间的关系
  - 当域之间建立信任关系后，一个域就可以信任另一个域中的用户访问自己的资源，而又不必在本域拥有这个用户的账户和口令。
- 信任关系的好处
  - 实现跨域的集中安全验证
  - 支持用户的单一登录

域（Domain）

信任关系的种类：

- 1 单向信任关系： 信任域--->受信任域
  - 信任域信任受信任域的用户
  - 受信任域中的用户允许访问信任域中的资源
- 2 双向信任关系：信任域<---->受信任域
  - 两个域之间彼此信任对方
  - 每个域中的用户账户都可以授权访问另一个域中的资源

- 提示：
  - Windows NT的信任关系是单向且不具传递性
    - A-->B & B-->C ‡ A-->C
  - 但2000以后默认信任关系是双向且可传递

域与工作组对比

- 域可定义安全管理边界，工作组无集中管理，相互独立。
  - 域中所有用户共享普通的用户账户数据库和安全策略。
  - 工作组中计算机使用本地账户和本地策略
- 验证：
  - 安全账户数据库

    工作组中计算机上的用户账户(SAM)数据库，是用在登录本机的时候用的。当登录到域时用的是域上的用户账户(SAM)数据库
  - 验证服务：

    ---域验证时，每台计算机不需要提供自己的验证服务

    ---工作组中登录验证用的是本机的验证服务。
- 登录成功访问范围：
  - 域在整个受信任域中访问许可的资源，工作组为本机资源。

2.1.2 NT 所引入的安全特性

- 用户账户（User Account）
- 权限（Right）
- 许可（Permission）
- 共享权限
- 安全审核（Security Audit）
- NTFS (Windows NT File System)
- 域(Domain)
- 工作组（Workgroup）

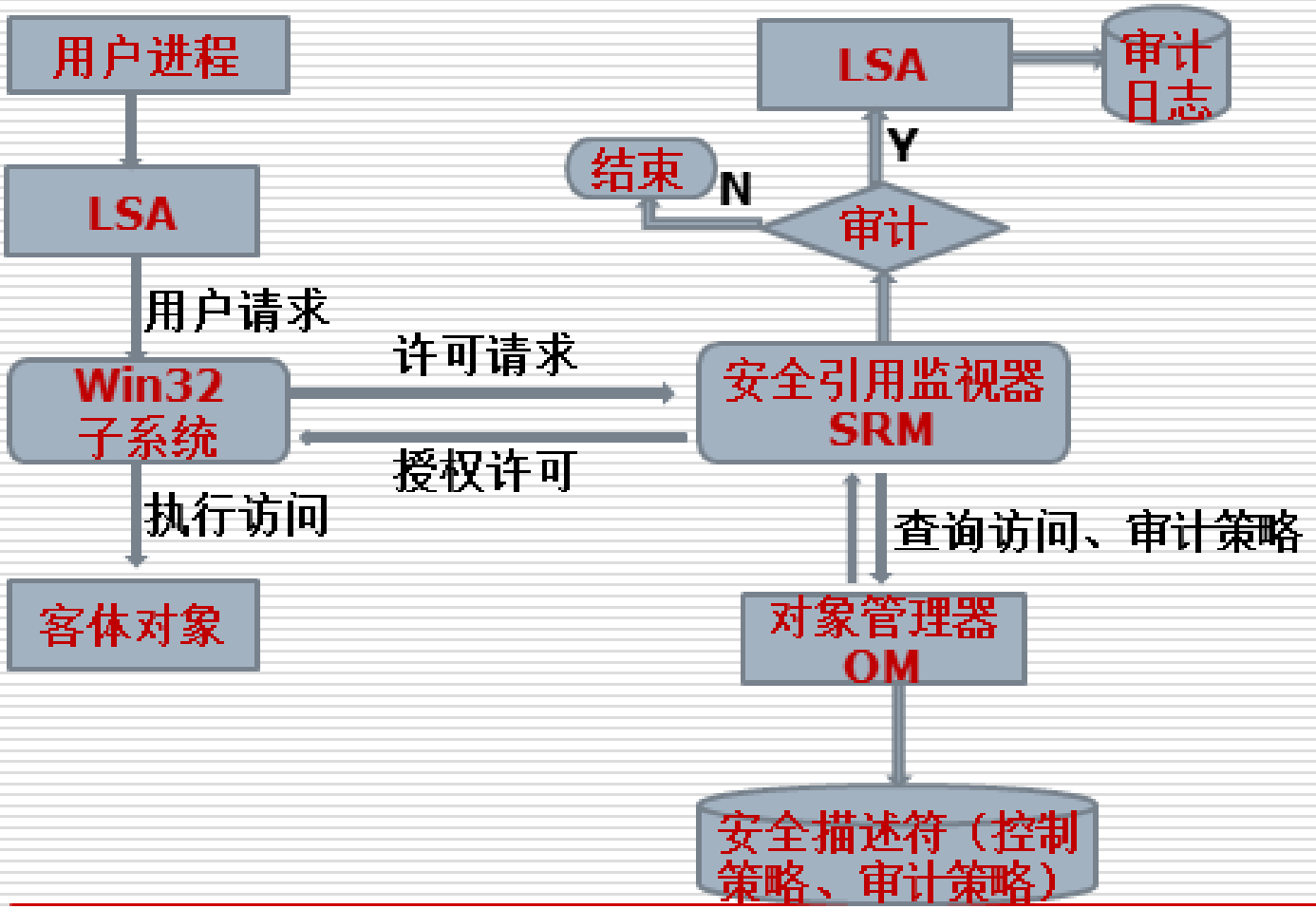
Windows NT的安全审核

- 安全审核的内容
  - 登录和注销
  - 文件或对象访问
  - 用户权限使用
  - 用户和组管理
  - 安全策略改变
  - 重启动、关闭和系统安全性
  - 过程跟踪

安全审核数据的存储

日志类型	存储内容	备注
系统	关于硬件和操作系统事件的信息	任何人都可以查看
应用程序	应用软件记录不同的信息，内容因应用而异	任何人都可以查看
安全	系统管理员选择审核的安全相关操作	只能由审计管理员才能查看和管理

系统资源访问及审计过程



- 2.1 Windows NT安全
  - 2.1.1安全体系结构
  - 2.1.2安全特性
- 2.2 Windows 20/03安全
  - 2.2.1安全模型与组件
  - 2.2.2新增安全特性

2.2 Windows 20/03的安全

- Windows 20/03系统
  - 保留了部分NT系统的内核
  - 增加了大量的内容，大部分集中在安全方面
    - 以活动目录为核心
    - 存在着安全功能的诸多新方面

到windowsNT，发现管理域缺少一个目录结构，这是win2000以后的活动目录（Active Directory）所要解决的问题。

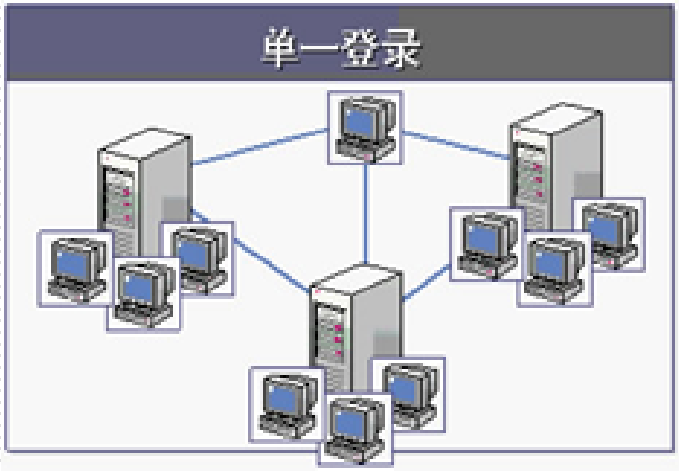
2.2 Windows 20/03安全

Windows 20/03提供大多数功能的能力是以组策略和Active Directory（AD活动目录）为基础的

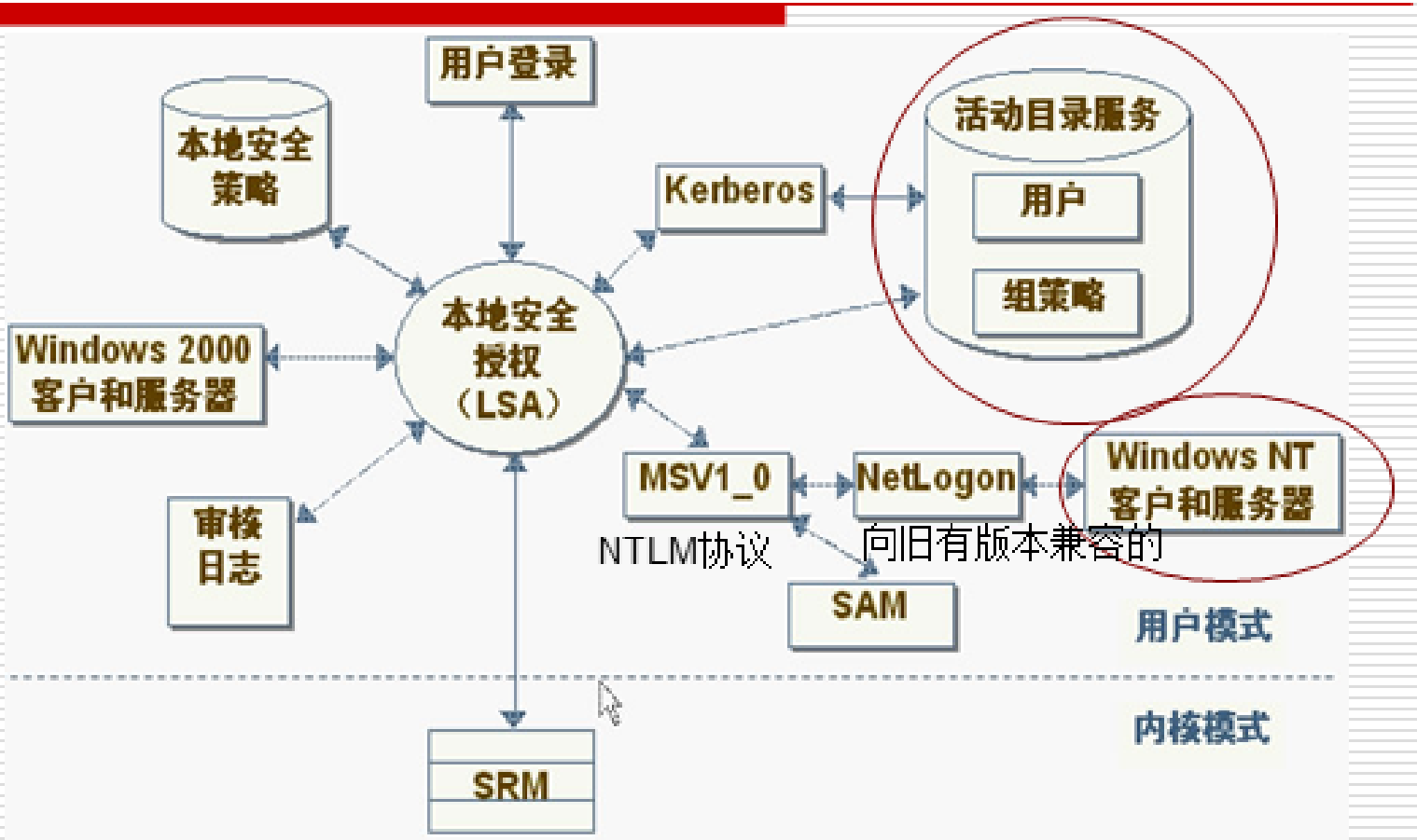
- 策略将组安全特性（应用于一组计算机、用户）组合在一起。
- Windows 在安全子系统下集成的活动目录提供了分布式的安全服务
- 没有AD的windows2000网络就与Windows NT4.0网络无太大区别了。

2.2.1 Windows 20/03 安全模型

- Windows 20/03安全性目标
  - 强大的身份验证，企业中的单一登录
  - 集成的安全服务，实现管理的委派和可扩展性
  - 实现互操作能力的标准协议
  - 审核服务



2.2.1 Win20/03 安全组件



- 在用户模式下，安全子系统是运行活动目录服务的真正子系统
- 在内核模式下，安全引用监视器执行安全子系统规则

WIN03中本地安全授权（LSA）功能

- 用户身份和权限管理
  - 交互式身份验证
  - 生成安全访问令牌
  - 确定用户权限
- 安全策略管理
- 对象管理
  - 建立可信任域列表
  - 确定对象的安全审核策略

2.2.2 win20/03新增安全特性

- 活动目录（**Active Directory ,AD**）
- **Kerberos**协议
- 组策略对象**(Group Policy Object , GPO)**
- **IP**安全协议**(IPSec)**
- 加密文件系统**(EFS)**
- 公钥基础结构**(Public Key Infrastructure, PKI)**
- 安全配置工具集
- 智能卡支持

活动目录

- 活动目录提供了完全集成在Windows中的一个安全、分布式、可扩展以及重复的分层目录服务，安装在域控制器上。
  - Windows 安全模型灵活性和可扩展性的核心
  - 提供了关于网络中所有对象的信息
  - 简化了一般的管理任务

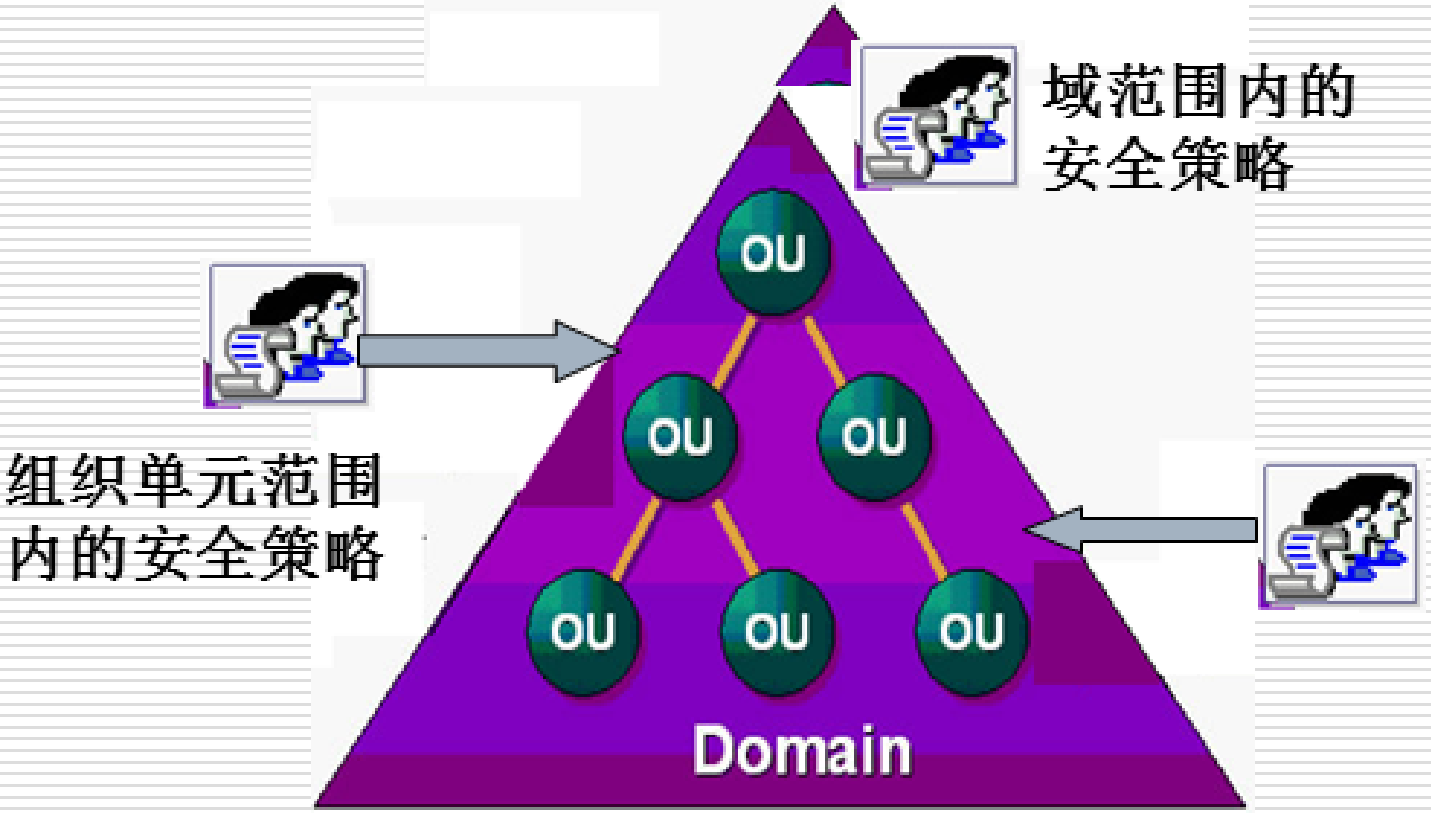
- 活动目录包含的内容
  - 目录本身：指目录中所存储的内容
  - 目录服务：使得管理员能轻松的操作目录中内容(操作指：访问，搜索，配置等)。

2.2.2 win20/03新增安全特性

- 活动目录（**Active Directory ,AD**）
- 组策略对象**(Group Policy Object , GPO)**
- **Kerberos**协议
- **IP**安全协议**(IPSec)**
- 加密文件系统**(EFS)**
- 公钥基础结构**(Public Key Infrastructure, PKI)**
- 安全配置工具集
- 智能卡支持

组策略

- 使用组策略进行不同层次策略管理
  - 设置对象：可以是OU,也可以是domain



2.2.2 win20/03新增安全特性

- 活动目录（Active Directory ,AD）
- 组策略对象**(Group Policy Object , GPO)**
- **Kerberos**协议
- **IP**安全协议**(IPSec)**
- 加密文件系统**(EFS)**
- 公钥基础结构**(Public Key Infrastructure, PKI)**
- 安全配置工具集
- 智能卡支持

2.2.2 win20/03新增安全特性

- 活动目录（Active Directory ,AD）
- 组策略对象**(Group Policy Object , GPO)**
- **Kerberos**协议
- **IP**安全协议**(IPSec)**
- 加密文件系统**(EFS:encryption File System)**
- 公钥基础结构**(PKI:Public Key Infrastructure)**
- 安全配置工具集
- 智能卡支持

知识回顾

- 加密需求
  - 保密性(C:confidential)
  - 完整性(I:integrity)
  - 不可抵赖性
- 加密技术
  - 对称加密
  - 公钥加密
  - 数字签名
- 加密应用
  - 加密存储在磁盘上的数据
  - 加密在网络上传输的数据

2.2.2 win20/03新增安全特性

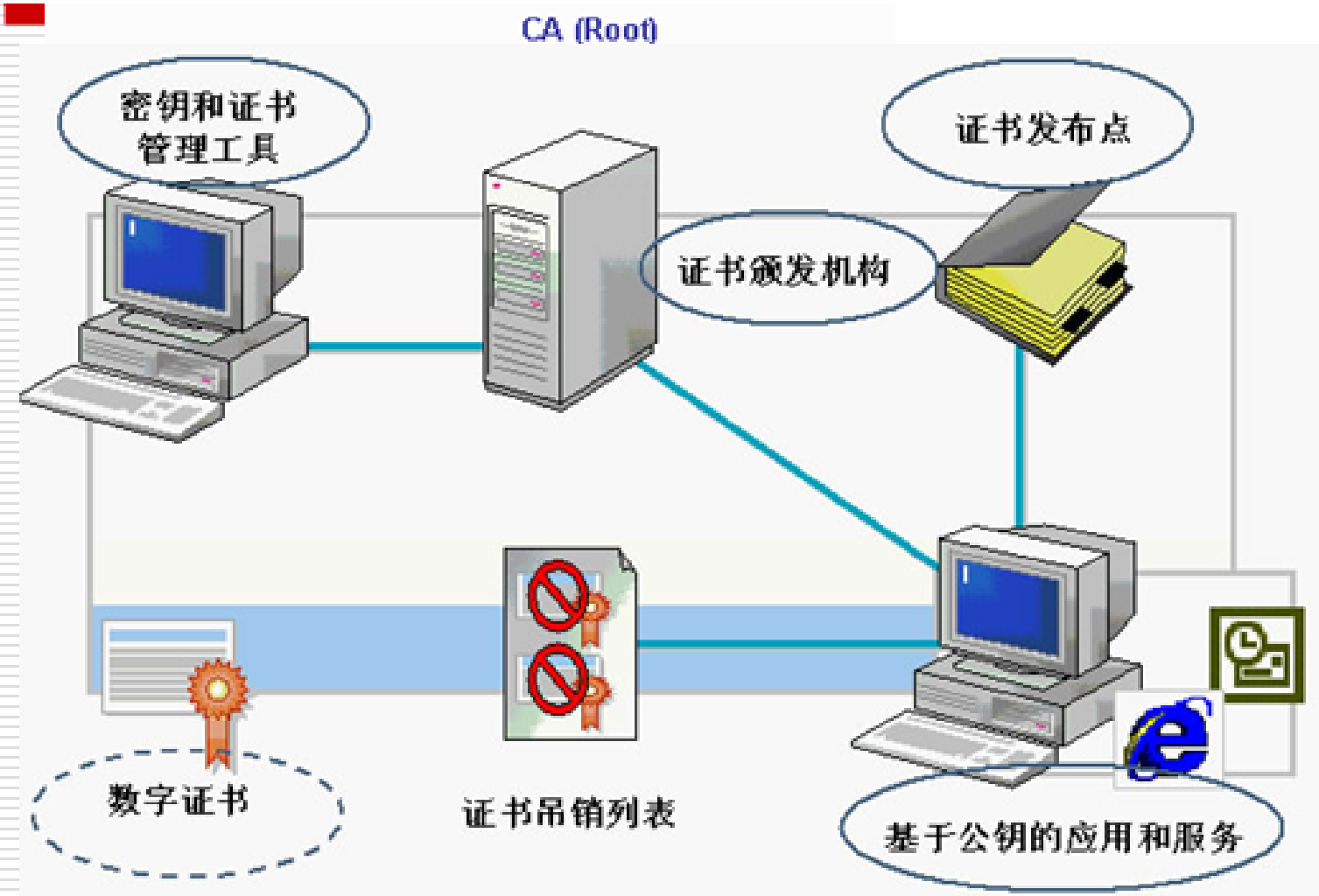
- 活动目录（Active Directory ,AD）
- 组策略对象**(Group Policy Object , GPO)**
- **Kerberos**协议
- IP安全协议(IPSec)
- 加密文件系统(EFS)
- 公钥基础结构**(Public Key Infrastructure, PKI)**
- 安全配置工具集
- 智能卡支持

PKI(public key infrastructure)组件

- PKI体系结构采用证书来管理公钥和身份信息，
- 通过第三方的可信机构CA(certificate authority),把用户的公钥和用户的其他标识信息捆绑在一起.
- 负责在Internet验证数字证书持有者身份的，保证网上数据的机密性、完整性。

Windows中的PKI可以支持企业级的证书服务和独立证书服务。

PKI体系（1）



费

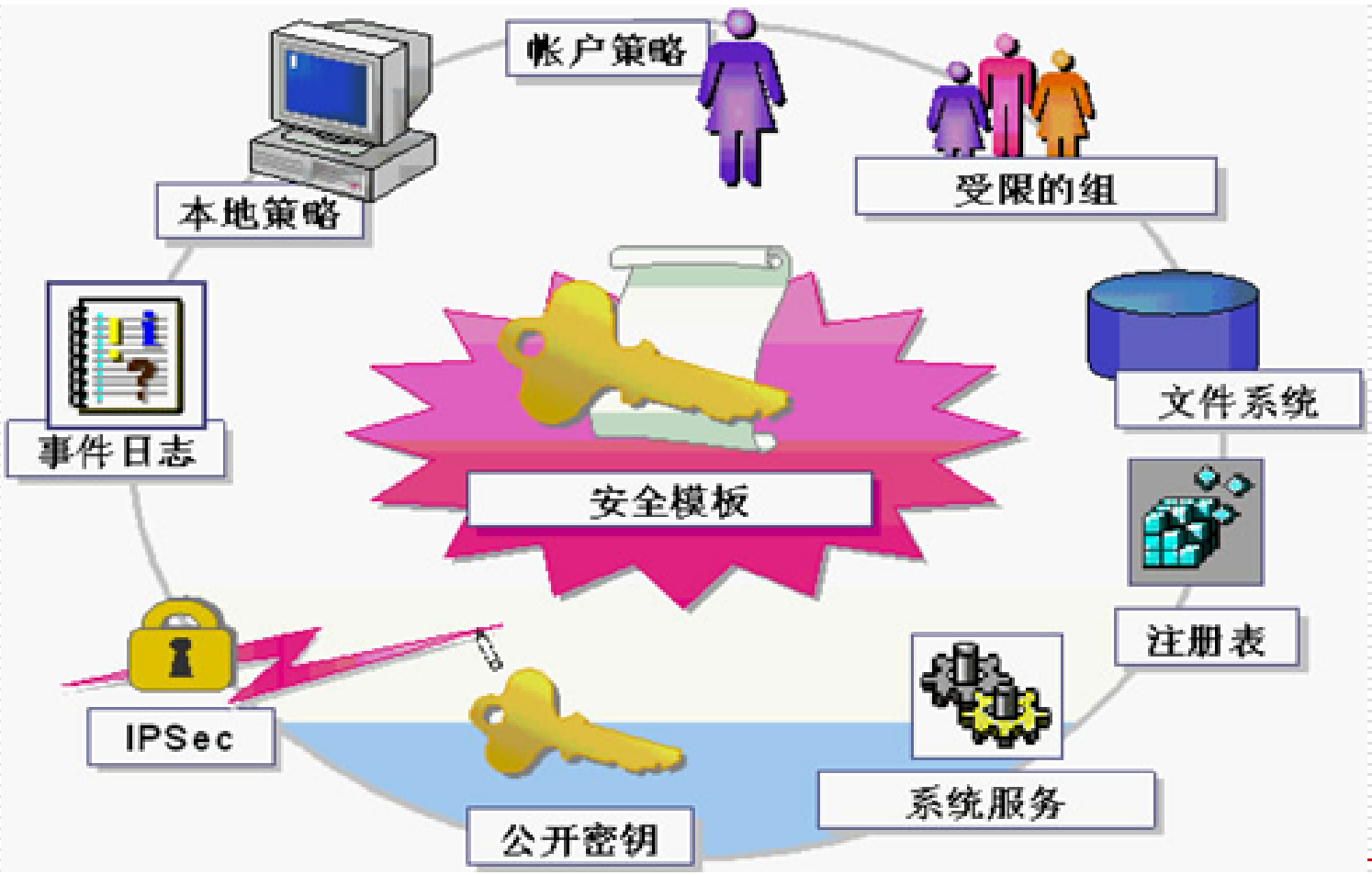
2.2.2 win20/03新增安全特性

- 活动目录（Active Directory ,AD）
- 组策略对象**(Group Policy Object , GPO)**
- **Kerberos**协议
- **IP**安全协议**(IPSec)**
- 加密文件系统**(EFS)**
- 公钥基础结构**(Public Key Infrastructure, PKI)**
- 安全配置工具集
- 智能卡支持

安全配置工具

- 安全模板
- 安全配置与分析工具

安全配置区



Win20/03的其他安全性

- Windows“系统文件”的保护
- 驱动程序签名

二章小结

- WINDOWS的系统安全体系：安全模型及安全组件。
- Windows提供的安全服务
  - NTFS文件系统
  - 加密文件系统(EFS)

  } 静态数据安全
  - 身份认证、访问控制、安全审核
  - Kerberos协议

  } 3A
  - IP安全协议(IPSec) ⟶ 传输数据安全
  - 活动目录（Active Directory ,AD）
  - 组策略对象(Group Policy Object, GPO)
  - 公钥基础结构(Public Key Infrastructure, PKI)
  - 安全配置工具集

  } 安全管理和配置

- 后期版本增加的部分
  - 1 DirectAccess
  - 2 改进的BitLocker(磁盘锁)
  - 3 AppLocker
  - 4 UAC（user account control）
  - 5 Windows Filtering Platform (WFP)
  - 6 Biometric安全特性
  - 7 DNSSEC