Windows安全原理与技术

— 第三章：Windows 2000安全基础

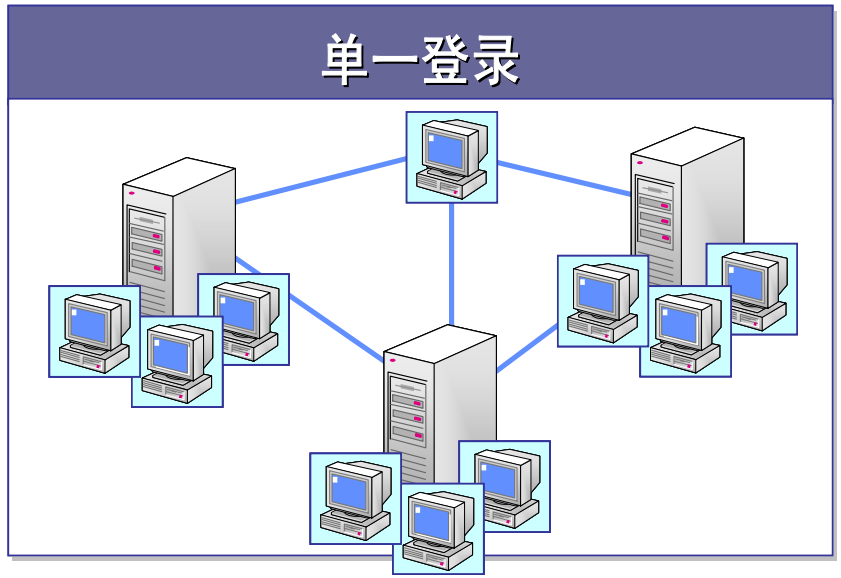
王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

Windows 2000的体系结构

- Windows 2K的体系结构和Windows NT基本相同
  - 用户模式
  - 内核模式

Windows 2000安全性目标



- 企业中的单一登录
- 集成的安全服务
- 管理的委派和可扩展性
- 强大的身份验证
- 用于实现互操作能力的基于标准的协议
- 审核服务

Windows 2000安全模型

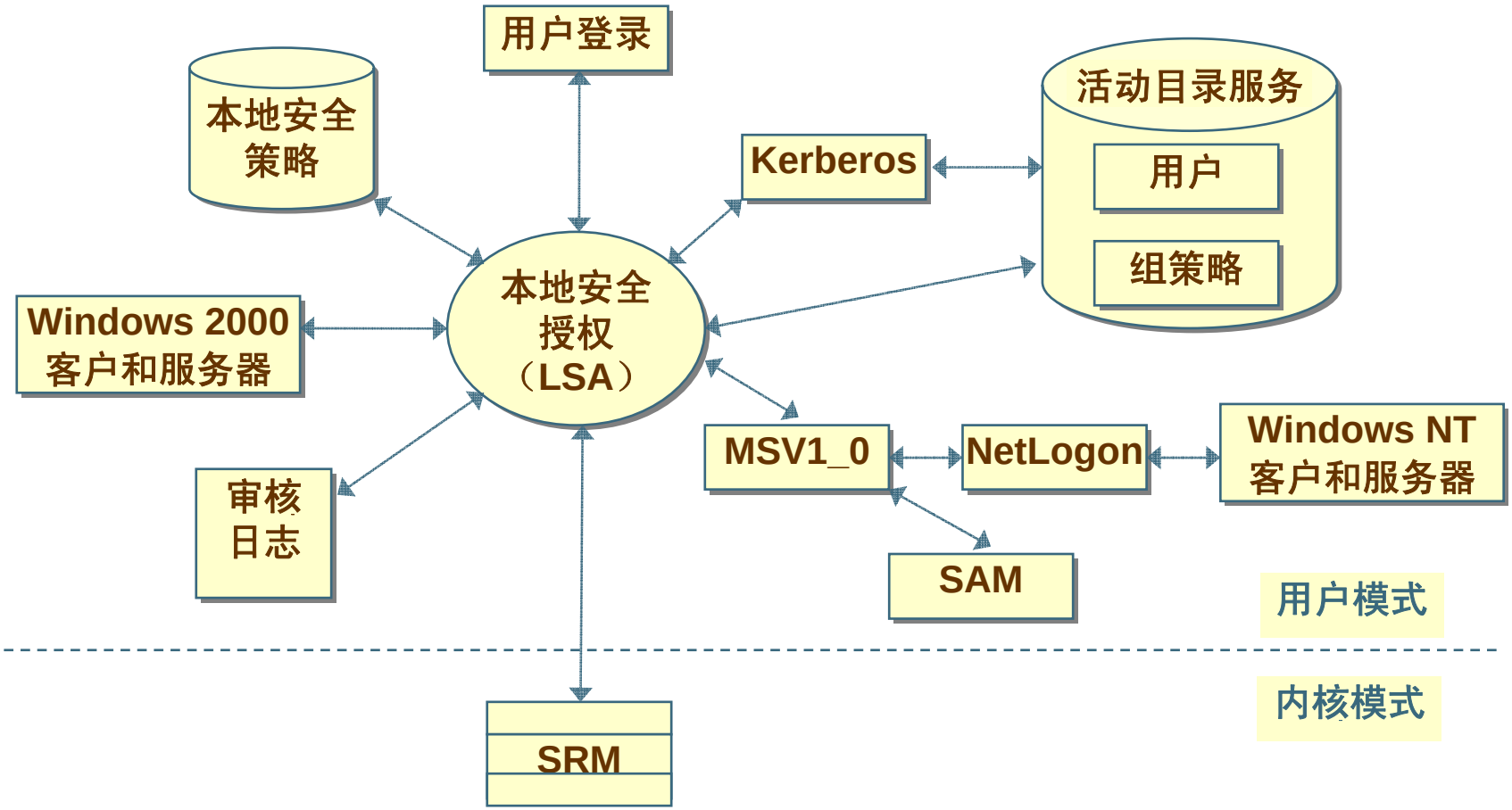
- Windows 2000的安全模型对基于组成员关系的所有域资源实现一致的访问控制。
- 模型的底层原理包括：
  - 服务器提供对象访问。
  - 客户只能通过服务器访问对象。
  - 对象管理器和安全引用监视器决定谁对对象拥有哪些权限。
  - 可以使用多个协议验证用户。
  - 管理安全策略的方式既可以是全局的，也可以是本地的。

活动目录与Windows 2000安全模型的集成

- 活动目录的目录服务与Windows 2000安全模型之间存在着一种基本的关系。
- Windows 2000在安全子系统下的活动目录的集成提供了分布式的安全服务。

- 活动目录
  - 存储了所有域的安全策略信息
  - 存储了域总体管理的安全策略信息
- Windows 2000安全模型
  - 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，安全参考监视器执行安全子系统规则。

安全子系统组件


用户登录
本地安全策略
活动目录服务
用户
组策略
Kerberos
本地安全授权（LSA）
Windows 2000客户和服务器
审核日志
MSV1_0
NetLogon
Windows NT客户和服务器
SAM
用户模式
内核模式
SRM

- 本地安全授权（Local Security Authority, LSA）
- 多重身份验证提供程序

  （Multiple Authentication Provider, MAP）
- Kerberos v5身份验证协议
- NTLM身份验证协议
- Netlogon服务
- 安全账户管理
- 安全套接字层（Secure Socket Layer, SSL）

安全参考监视器（SRM）

- SRM的职责：
  - 监视对象访问
  - 必要的时候生成安全审核
- SRM在对象句柄创建时进行安全性检查，而并不是在每次访问时进行检查。

解释：

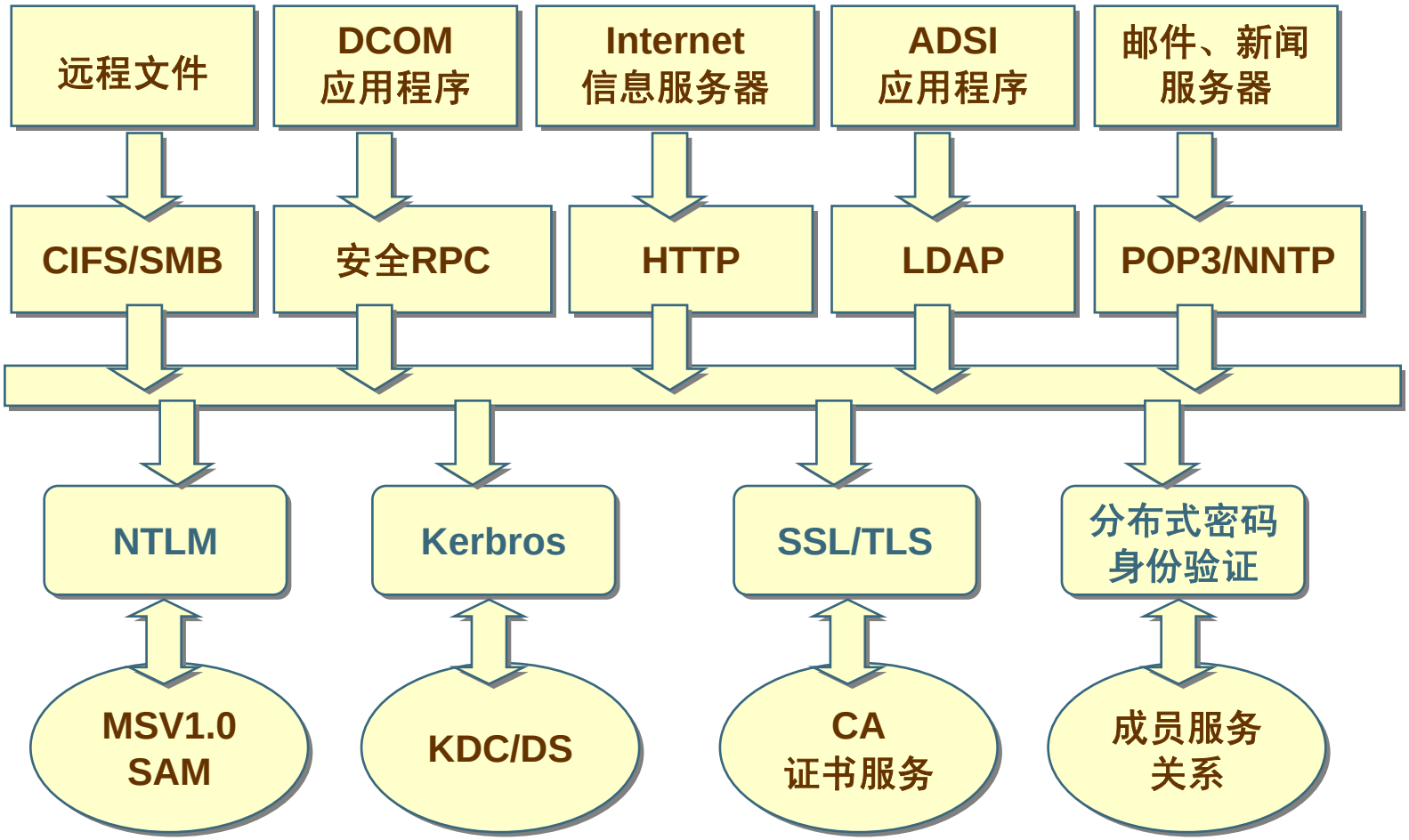
为什么有的时候对某个对象安全性方面的修改不会立刻生效？

本地安全授权（LSA）

- 用户身份和权限管理
  - 交互式身份验证
  - 生成安全访问令牌
  - 分配用户特权
  - 确定用户权限
- 安全策略管理
  - 管理本地安全策略
  - 管理审核策略
- 对象管理
  - 建立可信任域列表
  - 确定对象的安全审核策略
  - 内存的配额管理

Windows 安全协议

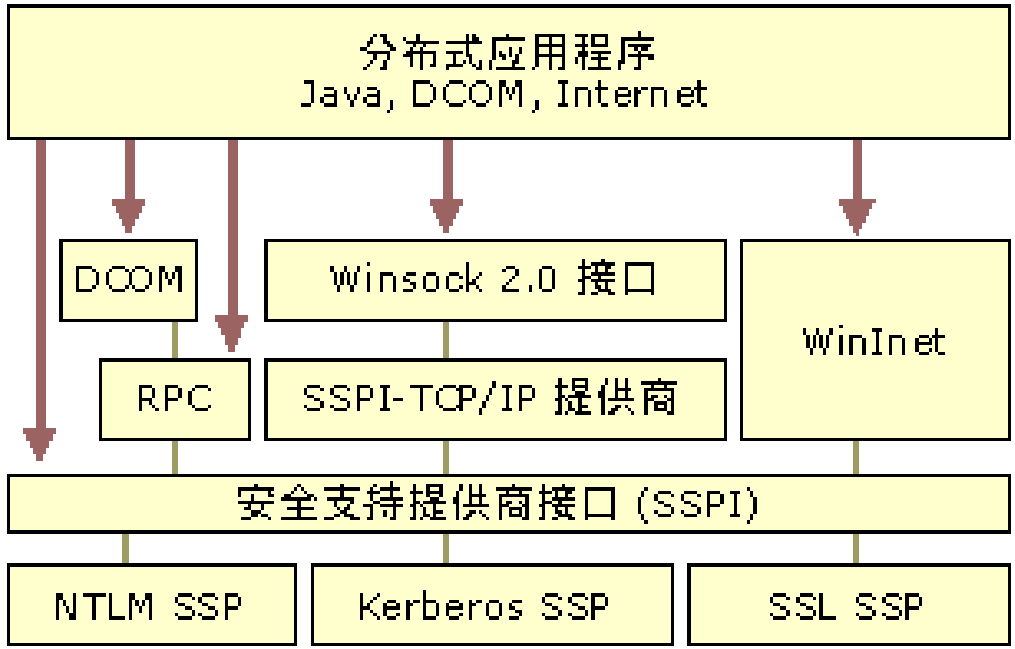
- Windows 2000允许多种网络安全协议来提供身份验证服务。
  - 保证对网络客户端的最大兼容性。
  - 保证了对Windows 2000网络的最大安全访问。


远程文件
DCOM
应用程序
Internet
信息服务器
ADSI
应用程序
邮件、新闻
服务器
CIFS/SMB
安全RPC
HTTP
LDAP
POP3/NNTP
NTLM
Kerbros
SSL/TLS
分布式密码
身份验证
MSV1.0
SAM
KDC/DS
CA
证书服务
成员服务
关系

- **NTLM（Windows NT LAN Manager）**
  - 由Windows NT、Windows 9x客户端使用。
- **Kerberos v5**
  - 基于Windows 2000计算机的默认安全协议。
- **分布式密码身份验证**
  - 由Internet会员组织（如MSN）所使用的共享的秘密身份验证协议。
- **安全信道服务**
  - 提供基于公钥的协议，如SSL和传输层安全（TLS）协议进行身份验证的能力。

Windows 2000安全程序开发体系

- 安全支持提供器接口
  （Security Support Provider Interface, SSPI）
  - 是定义的较全面的公用API。
  - 用来获得验证、信息完整性、信息隐私等集成安全服务。
  - 用于所有分布式应用程序协议的安全方面的服务。



Windows 2000安全程序的开发

- 应用程序开发者可以选择：
  - 直接调用SSPI函数。
  - 使用基于DCOM、经验证的RPC或者Winsock 2.0等更高级的应用程序接口。

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消