Windows安全原理与技术

— 第二章：Windows NT安全

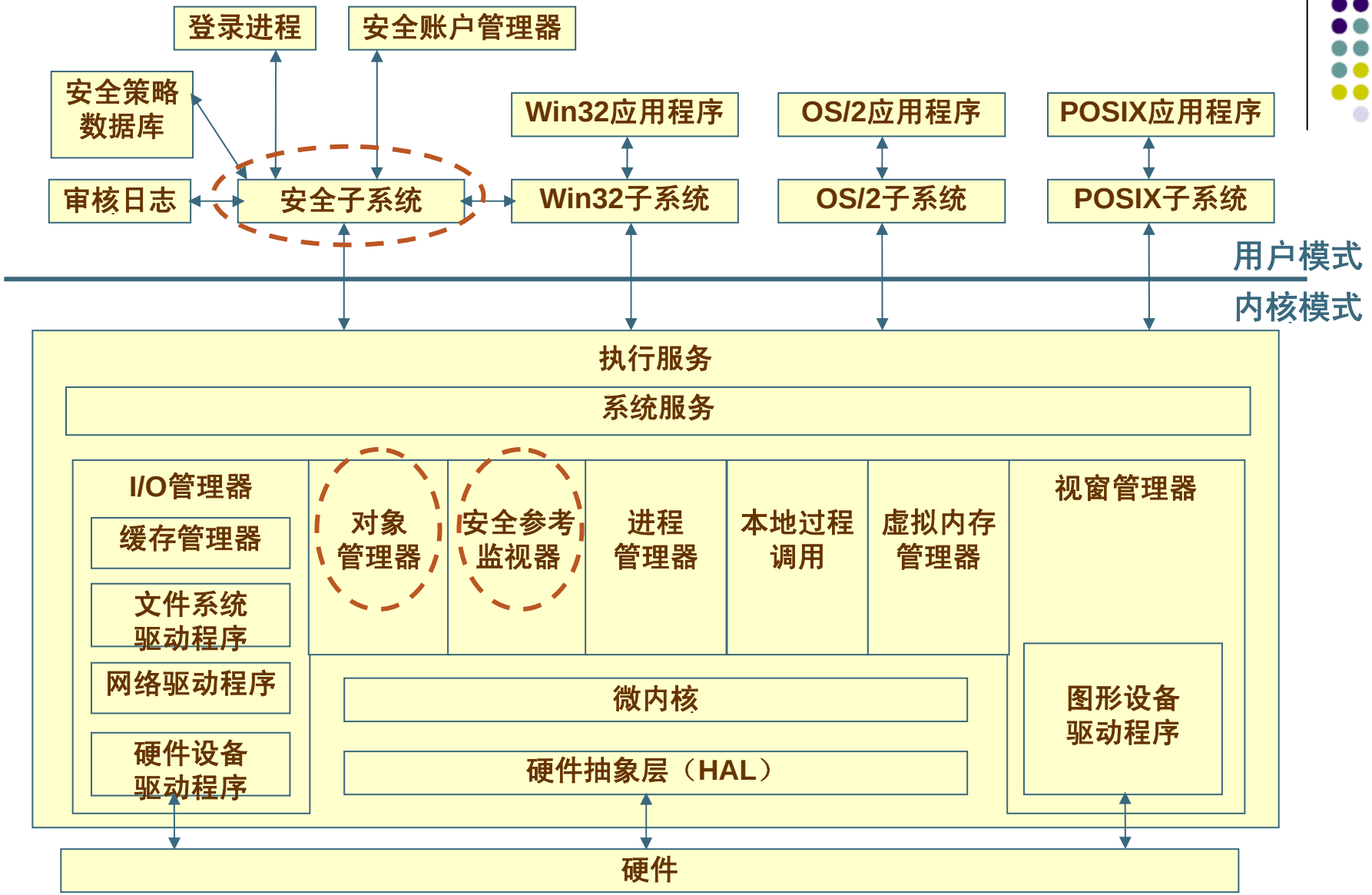
王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

Windows NT的安全体系结构

- **Windows NT的体系结构分为内核模式（Kernel Mode）和用户模式（User Mode）**
  - **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。**
  - **用户模式中的代码拥有较低特权，不能对硬件直接进行访问，内存访问受限。**

Windows NT的安全体系结构



用户模式

- Win32子系统
  - 所有的32位Windows应用程序
- 本地安全子系统
  - 支持Windows的登录过程，包括身份验证和审核工作。
  - 需要和Win32子系统通信。
- OS/2子系统，POSIX子系统

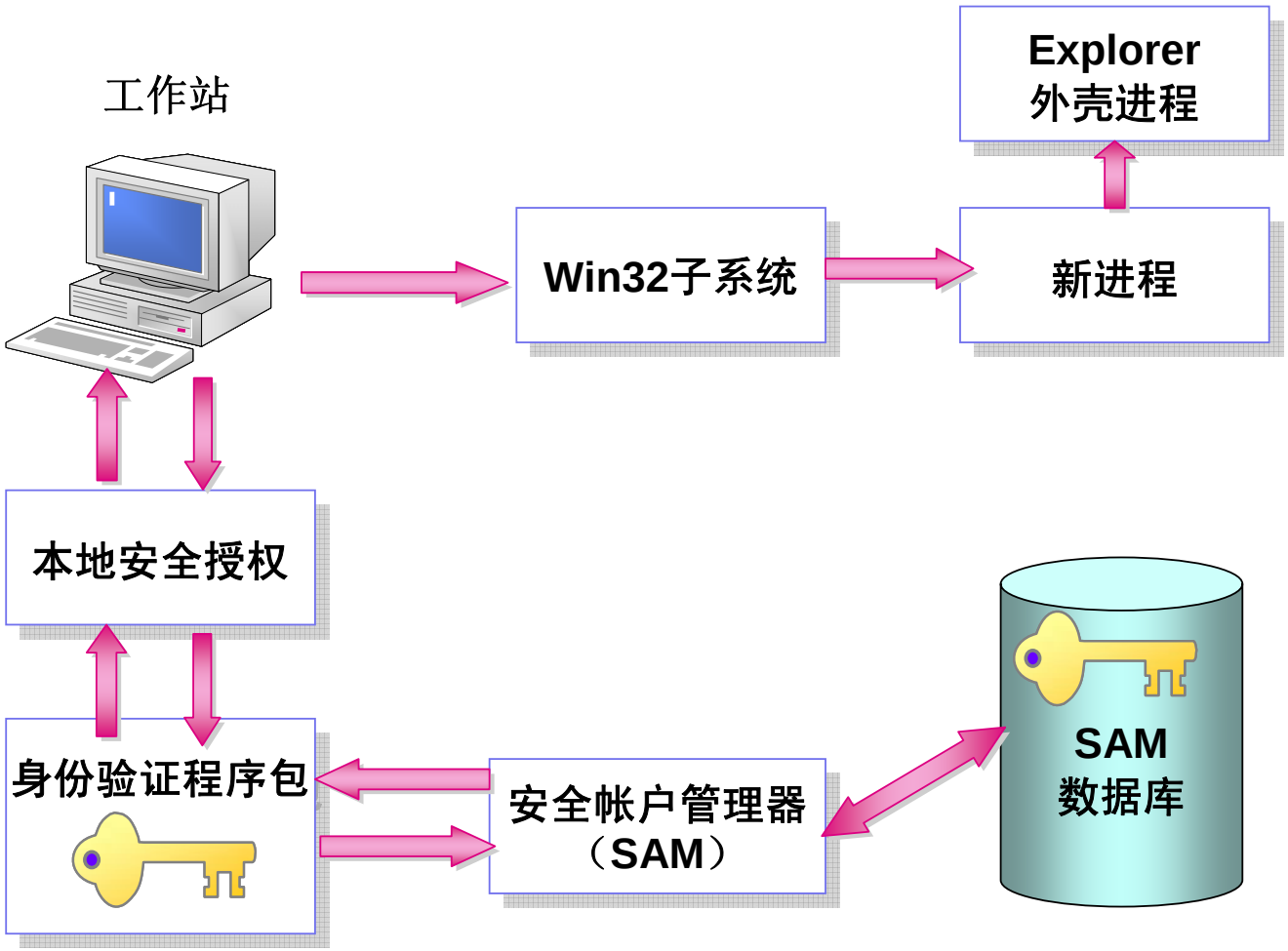
内核模式

- 组成内核模式的整套服务被称为执行服务（Windows NT Executive）
  - 通过响应用户模式下应用程序发出的请求来提供内核模式服务。
- I/O管理器
- 对象管理器（Object Manager）
- 安全参考管理器（SRM）
- 本地过程调用（LPC）
- 虚拟内存管理器
- 视窗管理器

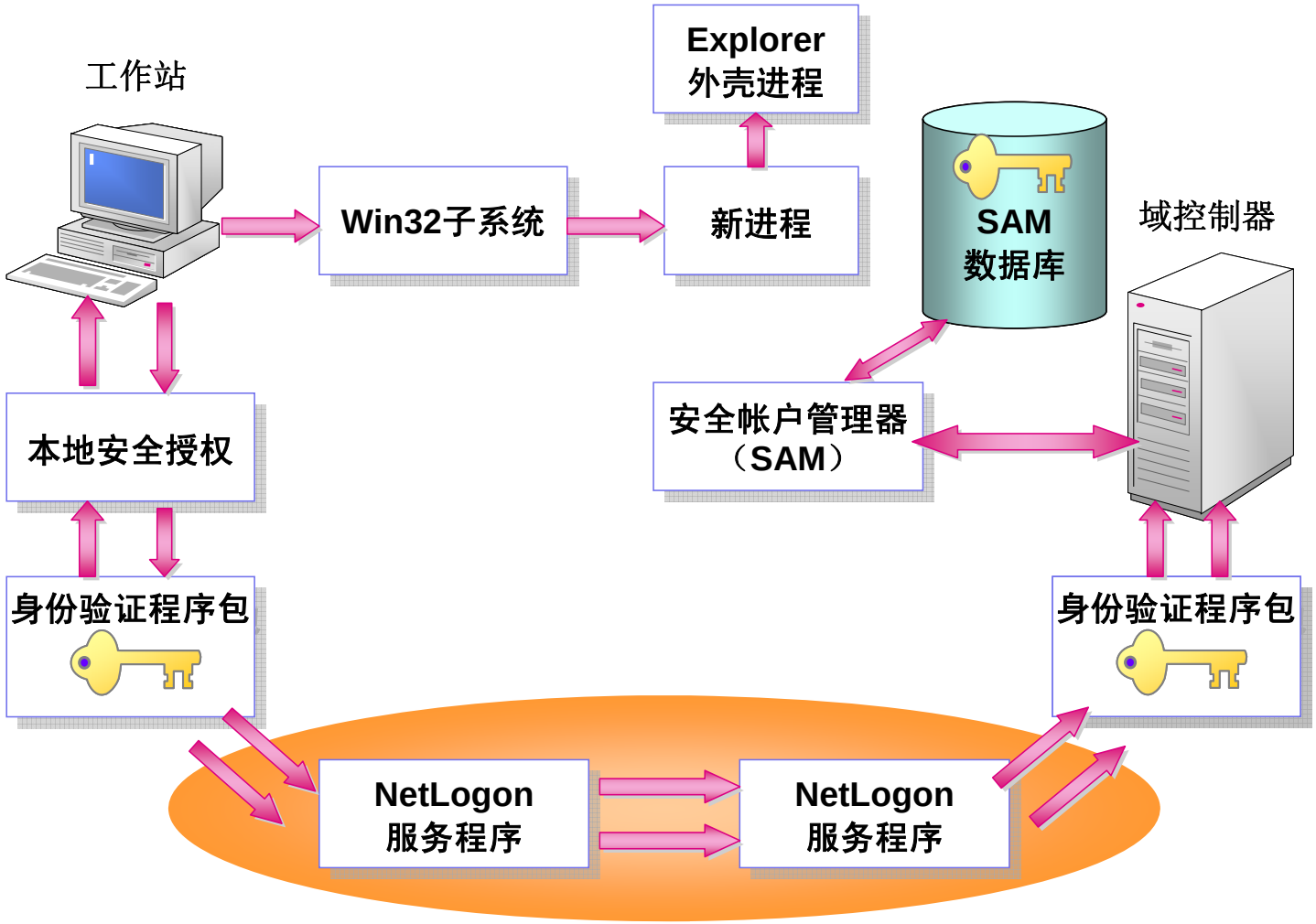
安全登录过程

- Winlogon
- GINA（图形化识别与验证）动态链接库
- 大量的网络提供程序

本地交互式登录


工作站
Explorer
外壳进程
Win32子系统
新进程
本地安全授权
身份验证程序包
安全帐户管理器
（SAM）
SAM
数据库

域账户交互登录


工作站
Explorer
外壳进程
Win32子系统
新进程
SAM
数据库
域控制器
本地安全授权
安全帐户管理器
（SAM）
身份验证程序包
身份验证程序包
NetLogon
服务程序
NetLogon
服务程序

本地安全授权（LSA）

- LSA是安全子系统的一个核心组件。
- 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，管理本地安全策略。
- LSA负责记录安全参考监视器的任何审核消息所产生的事件日志。

安全参考监视器（SRM）

- SRM负责所有对对象的访问控制和审核策略（本地安全策略范围之内）。
- SRM和Object Manager联合起来，保证用户和进程访问对象的有效性，生成任何所需的审核消息。

对象管理器

- Object Manager的作用负责对象的命名、保护、分配和处置。
- 管理的对象包括：
  - 目录、文件、设备
  - 进程、线程
  - 网络共享资源
  - 端口
  - 打印机
  - 符号链接
  - 窗口

安全账户管理器（SAM）

- Security Account Manager负责SAM数据库的控制与维护。
- SAM数据库位于受到保护的注册表中，只允许系统程序和管理员访问。
- SAM数据库包含了所有的用户账户、组账户信息以及每个用户口令的加密散列值。
  - LAN Manager口令
  - Windows NT口令

LAN Manager验证

- LAN Manager口令基于标准的原始设备制造商字符集，对大小写不敏感，最大长度不超过14个字符。
- LAN Manager口令算法的致命缺陷。
  - 算法
  - 可用字符=36
  - 口令空间=2 * 36^7
  - 没有引入Salt机制

Window NT和C2级安全

- 《可信计算机系统评估准则》（TCSEC，橘皮书）
  - 将操作系统的安全等级分为4大类：

    A、B、C、D
  - 安全等级从高到低为：

    A、B3、B2、B1、C2、C1、D

C2级别的安全性策略

—自由控制的访问权限

（Discretionary Access Control, DAC）

- 自由的访问控制
- 对象的重用
- 强制的用户标识和认证
- 可记账性和审核

Windows NT的文件系统

- **FAT（标准文件分配表）**
  - 适合于较小的卷。
  - 最大支持4GB的卷。
  - 没有安全性。
- **NTFS**
  - 支持用户的访问控制和所有权设置。
  - 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。

Windows NT的用户和用户组

- 用户账户
  - 使用用户名和密码进行标识。
  - 用户名：账户的文本标签。
  - 密码：账户的身份验证字符串。
  - SID（安全标识符）：账户的关键标识符。
- 用户组账户

Windows NT内置的用户和组帐号

- 内置用户帐号
  - Administrator和Guest
  - 可以改名，不能删除
- 内置用户组帐号
  - Administrators
  - Users
  - Guests
  - Backup Operators
  - Replicator
  - * Operators（Print, Account, Server）
  - Domain * （Administrators, Users, Guests）
  - 特殊组 （Network, Interative, Everyone, …）

账户作用域 — 全局和本地

工具	账户类型	作用域	使用
用户管理器（Windows NT Workstation）	用户	本地	单台计算机
	组	本地	单台计算机
域用户管理器（Windows NT Server）	用户	全局（默认）	多台计算机
	本地组	本地	单台计算机
	全局组	全局	多台计算机

单台计算机：用于未加入 Windows NT域的工作组或计算机。
多台计算机：用于当前选定的整个域。

Windows NT的工作组和域

- 工作组（Workgroup）
  - 不共享任何用户账户信息和组账户信息的小型Windows NT系统集合。
  - 每个系统使用自身的SAM数据库独立验证。
  - 适用于最小型的环境，不进行集中控制，难以管理。

- 域（Domain）
  - 具有集中安全授权机构（如PDC）的一批计算机。
  - 至少包括一台主域服务器（PDC）和若干台工作站和成员服务器。
  - 一般还存在备份服务器（BDC）。
- 域为用户、组和计算机账户定义了安全边界的管理范围。
  - 一个域中的所有用户共享普通的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PDC或BDC的验证服务通过域验证，该用户就可以在具有必要权限的域和主体内的任何地方访问资源了。
  - BDC提供了分布式验证和一定的负载平衡。

信任关系

- 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。
- 信任关系是域之间的关系
  - 一个域允许另一个域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与口令。

信任关系的种类

- 单向信任关系：信任域 → 受信任域
  - 信任域信任受信任域中的用户。
  - 受信任域中的用户允许访问信任域中的资源。
- 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。

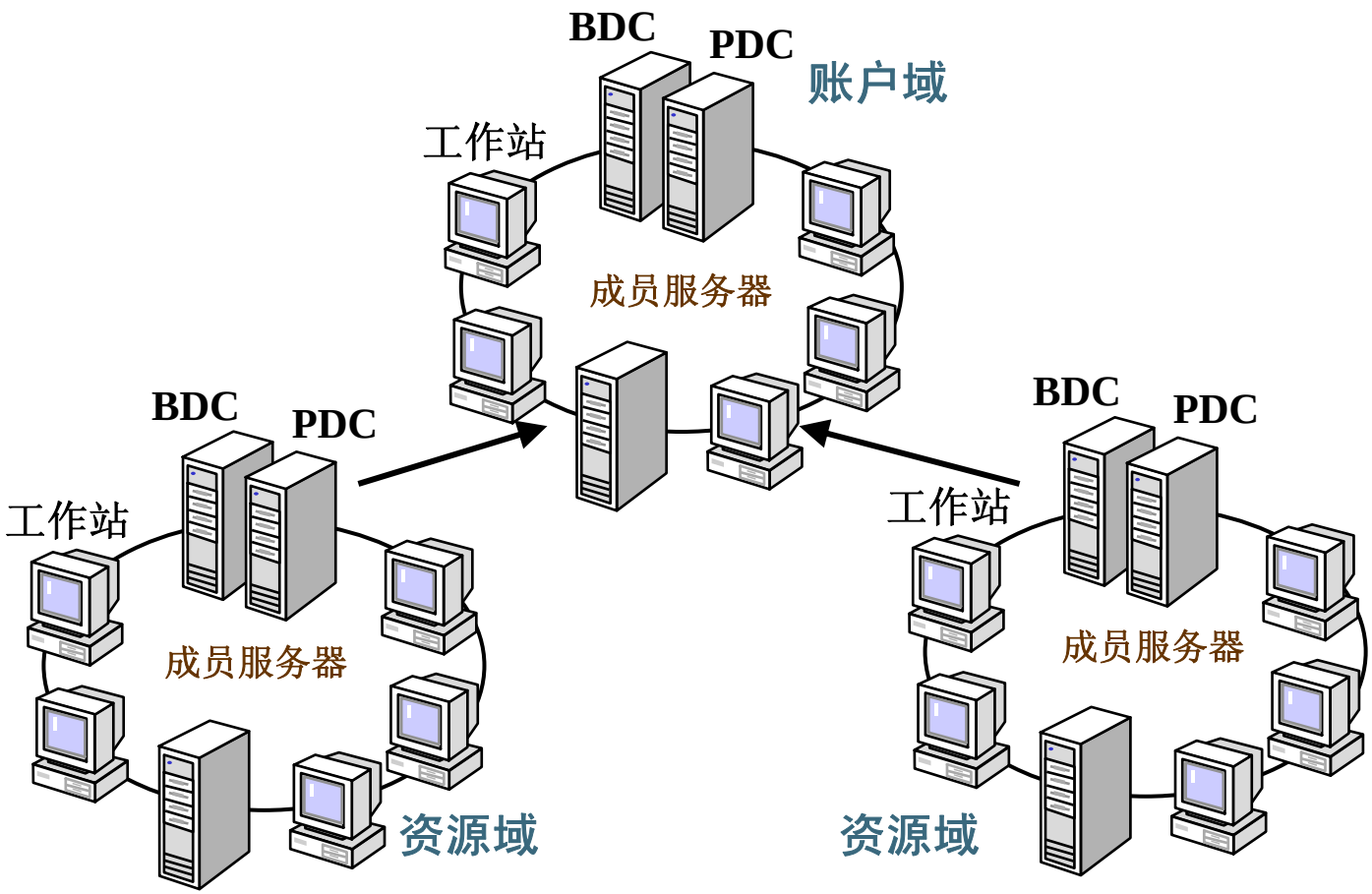
Windows NT的信任关系

- 信任关系只限于域和域之间，不能存在于域和工作组之间。
- 信任关系之间不具有传递性。
  - A→B & B→C ≠> A→C

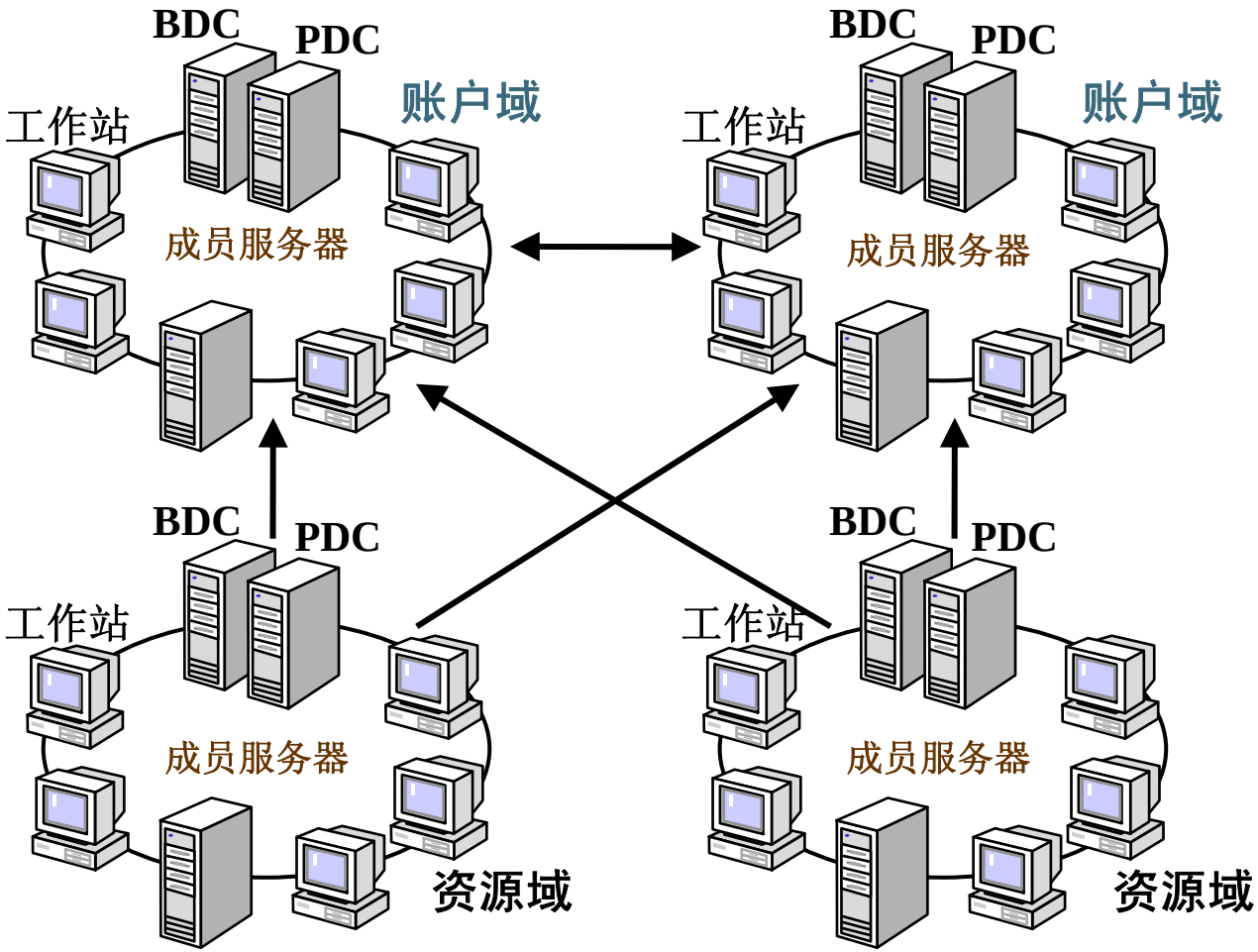
信任关系模型

- 单域模型
- 主域模型
- 多主域模型
- 完全信任模型

主域模型


BDC
PDC
账户域
工作站
成员服务器
BDC
PDC
工作站
成员服务器
资源域
BDC
PDC
工作站
成员服务器
资源域

多主域模型


BDC
PDC
账户域
工作站
成员服务器
BDC
PDC
工作站
成员服务器
BDC
PDC
工作站
成员服务器
资源域
BDC
PDC
工作站
成员服务器
资源域

Windows NT的访问控制

- 访问控制模型
  - 主体的安全访问令牌（Security Access Token）
  - 客体的访问控制列表（ACL）
- 安全访问令牌
  - 当用户通过登录验证后，安全访问令牌由登录进程分配。
  - 安全访问令牌伴随用户启动的每一个进程。
  - 安全访问令牌是用户访问系统资源的凭证。
  - 安全访问令牌的内容。

- 访问控制列表
  - ACL（Access Control List）是包含有访问控制项的一个列表。
- 访问控制项
  - ACE（Access Control Entry）包含了某用户或组的SID以及该用户或组针对该客体的访问权限。

标准的文件访问权限

访问类型	无	读取	修改	完全控制
显示文件数据		√	√	√
显示文件属性		√	√	√
运行程序文件		√	√	√
显示文件所有者与权限		√	√	√
修改文件属性			√	√
修改文件中的数据			√	√
删除文件			√	√
修改文件所有者和权限				√

特殊的文件访问权限

访问类型	无	读取	写入	执行	删除	修改权限	获取所有权	完全控制
显示文件数据		√						√
显示文件属性		√		√				√
运行程序文件				√				√
显示文件所有者与权限		√	√	√				√
修改文件属性			√					√
修改文件中的数据			√					√
删除文件			√		√			√
修改文件所有者							√	√
修改文件权限						√		√

目录访问权限

访问类型	无	读取	写入	列出文件夹	读取和写入	修改	完全控制
显示目录文件名		√		√	√	√	√
显示目录属性		√	√	√	√	√	√
改为子目录		√	√	√	√	√	√
修改目录属性			√		√	√	√
创建子目录与添加文件			√		√	√	√
显示目录所有者与权限		√	√	√	√	√	√
删除目录与子目录						√	√
修改目录权限							√
取消目录所有者身份							√

标准继承权限

目录访问类型	文件继承权限
无	无
读取	读取、执行
写入	未定义
列出文件夹	未定义
读取和写入	读取、执行
修改	读取、写入、执行、删除
完全控制	全部

— Windows NT系统中，继承的权限和直接应用的权限不同的话，就会造成安全问题。

— Windows 2000系统的改进。

共享权限

共享权限级别	允许的用户行为
无（No Access）	禁止对目录和其中的文件及子目录进行访问。
读取（Read）	允许查看文件名和子目录名，改变共享目录的子目录，还允许查看文件的数据和运行应用程序。
修改（Change）	具有“读取”权限中允许的操作，此外还允许往目录中添加文件和子目录，更改文件数据，删除文件和子目录。
完全控制（Full Control）	具有“修改”权限中允许的操作，此外还允许更改权限和获取所有权（这两项只适用于NTFS卷）。

— 共享级访问权限没有很好的控制粒度。

— 联合使用共享级访问权限和目录文件访问权限就可以实现更大程度的控制能力。

注册表访问权限

访问类型	说明
Query value	读取子键某值项的设置。
Set Value	设置子键的值。
Create Subkey	在所选键或子键内创建一个新的键或子键。
Enumerate Subkey	确定某键或子键内的所有子键。
Notify	接收子键产生的审核通知。
Create Link	创建到子键的符号链接。
Delete	删除所选键或子键。
Write DAC	为所选键修改DAC（任意访问控制权限）。
Write Owner	去掉所选键或子键的所有者身份。
Read Control	读取所选子键内的安全信息。

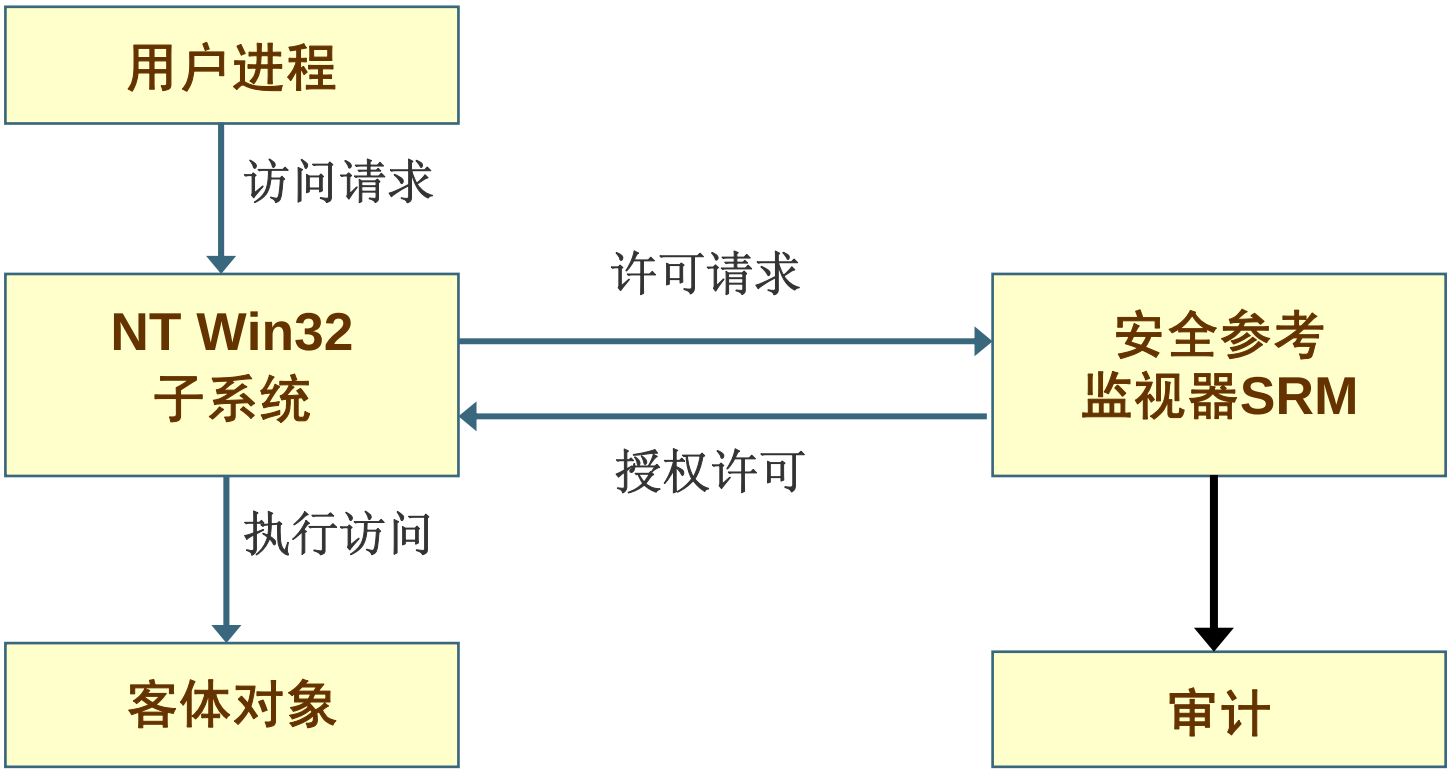
Windows NT的安全审核

- 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。

客体访问的审计过程



SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消