第 3 章 Windows 2000 安全基础

3.1 Windows 2000 系统结构

Windows 2000 系统的体系结构与 Windows NT 系统基本相同。应用程序通常运行于用户模式，而操作系统函数则运行于内核模式，从而保证应用程序不能直接访问硬件和系统代码。

（1） 用户模式。用户模式下的软件在没有特权的状态下运行，对系统资源只有有限的访问权限。例如，软件不能直接访问硬件。Windows 2000 基础的应用程序和被保护的子系统运行在用户模式下。被保护的子系统运行在自己的空间内，不会互相干涉。

（2） 内核模式。在内核模式中，软件可以访问所有的系统资源，例如计算机硬件和敏感的系统数据。内核模式中的软件构成了操作系统的核心，它们可以分为如下几组。

- 执行体（Executive）：包含为环境子系统和其他执行体组件提供系统服务的系统组件。它们执行的系统任务包括输入/输出、文件管理、虚拟内存管理、资源管理以及进程内部通信等。
- 设备驱动程序（Device drivers）：将组件的调用（例如打印机请求）翻译为硬件操作。
- 硬件抽象层（Hardware abstraction layer, HAL）：将 Windows 2000 执行体的其他部分与特定的硬件分离开来，使操作系统与多处理器平台相兼容。
- 微内核（Microkernel）：管理微处理器。它执行一些重要的功能，例如调度、中断以及多处理器同步等。

Windows 2000 的用户模式和内核模式分离的体系结构保证了失控的用户进程不会破坏处于内核模式下的低层次的系统驱动程序。所有对内核模式的访问都是受保护的。当一个用户程序对位于内核模式下的系统服务提出要求时，这个要求必须通过一个应用程序接口（API），该 API 将在内核模式下把请求的服务转移到相应的服务上去。

3.2 Windows 2000 安全模型

Windows 2000 安全性是相当复杂的。但总的来说，Windows 2000 安全性试图达到以下几个目标：

- 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

为了实现这些安全性目标，Windows 2000 使用了安全模型这一概念。这个模型定义了 Windows 2000 操作系统的不同部分配合工作的方式。这种结构中的一些底层原理包括：

- 服务器提供对象访问

- 客户只能通过服务器（服务）访问对象
- 对象管理器和安全引用监视器（Security Reference Monitor, SRM）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可以是全局的，也可以是本地的

Windows 2000 的安全性在用户模式和内核模式下是分离的。在用户模式下，安全子系统是运行活动目录（Active Directory）服务的真正子系统。在内核模式下，安全引用监视器（Security Reference Monitor, SRM）执行安全子系统规则。因此，安全性能得到了真正的加强，在这里不会发生用户干涉。

在安全子系统下的 Active Directory 的集成保证了在 Windows 2000 下可以存在分布式的安全服务。因为 Active Directory 位于安全子系统下，所以可以由下列三个部分来联合保护所有的访问：

- 身份验证
- 提供身份验证和授权的安全主体
- 安全主体对执行任务的必要许可的合法性

安全子系统通过在内核模式下将请求转给安全引用监视器，以比较该请求和正在连接的对象的任意访问控制列表（Discretional Access Control List，DACL）是否相符，并根据它来执行此授权。DACL 包括访问控制项（Access Control Entries，ACE），它定义了该对象的安全主体和该安全主体对于此对象享有哪些权限。

3.2.1 安全引用监视器

安全引用监视器（SRM）位于 Windows 2000 的执行体中，它的职责是监视对象访问，并在必要的时候生成安全性审核。SRM 确保所有的对象访问都连接到对象的安全性描述符（SD, security descriptor）一致。为此，SRM 需要和 Windows 2000 执行体的另一个组件对象管理器（Object Manager）紧密合作。

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，这仅仅是因为性能上的考虑。可以想象，如果每次访问一个文件（对象的一种）的时候都对安全性进行解析，那么将会导致多大的性能瓶颈。SRM 假定在句柄处于打开状态时安全性不会发生改变，因此，如果在句柄创建时允许访问，则该访问将一直有效，直到句柄被关闭。在考虑安全性时记住这一点很重要，这解释了为什么对某个对象安全性方面的修改不会立刻生效，因为用户可能打开了该对象的句柄。

3.2.2 安全子系统组件

Windows 2000 安全子系统影响整个 Windows 2000 操作系统。它提供了单一的系统，通过它检查对对象（包括磁盘上的文件、内存中的进程或者到外部设备的端口）的所有访问，以便确保应用程序或用户不会在未经适当授权的情况下获得访问权限。图 3-1 显示了安全子系统组件。

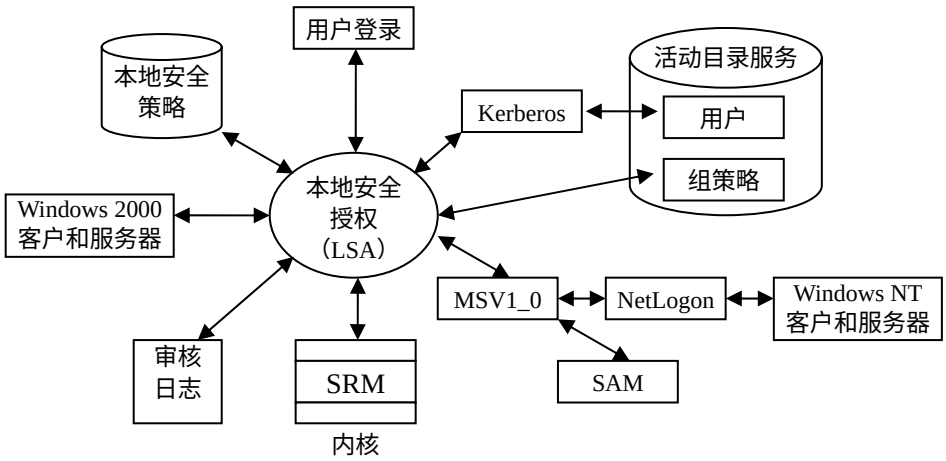

图 3-1 Windows 2000 安全子系统组件

安全子系统运行于本地安全授权机构（Local Security Authority, LSA）进程的安全环境中。这个进程在用户模式和内核模式下是分开的。在本地安全授权机构进程中有：

- Netlogon 服务（Netlogon.dll） Netlogon 服务维护计算机到其所在域内的域控制器的安全信道。Netlogon 服务通过一个安全信道将证书交给域控制器，再为安全主体返回一个带有安全标识符和用户权力的访问权标。
- NTLM 身份验证协议（MSV1_0.dll） NTLM 被用于验证不能使用 Kerberos 身份验证的客户，包括装有 Windows 9x 和 Windows NT 的计算机。
- 安全套接字层（Schannel.dll） 安全套接字层(Secure Sockets Layers, SLL）在应用层提供传输数据的加密服务。所有经过加密信道的数据在网络上都受到保护。为了使用 SSL，必须将应用程序编码以识别和执行 SSL。
- Kerberos v5 身份验证协议（Kerberos.dll） Kerberos v5 是 Windows 2000 使用的默认验证协议。Kerberos 身份验证以票据授予票据(Ticket-granting tickets, TGT）和票据授予服务（Ticket-granting service, TGS）为基础。
- Kerberos 密钥分发中心（Kdcsvc.dll） 在客户端接受网络身份验证的初期，Kerberos 密钥分发中心（Kerberos Distribution Center, KDC）服务负责向它颁发 TGT，然后该 TGT 被用于后续的对服务票据的一系列请求，获得的票据最后被用于对发出请求的客户端进行身份验证。
- 本地安全授权（lsasrv.dll） 本地安全授权（Local Security Authority, LSA）是安全子系统的核心组件，在 Active Directory 下执行所有定义的安全策略。
- 安全账户管理（Samsrv.dll） 安全账户管理（Security Accounts Manager, SAM）程序被用于在一个非域控制器上存储本地安全账户。SAM 同时也执行所有本地的存储策略。
- 目录服务模块（ntdsa.dll）：目录服务模块支持 Windows 2000 域控制器之间的复制，以及所有基于轻量级目录访问协议的、对 Active Directory 和保存在 Active Directory 下的命名上下文管理的访问。命名上下文包括域命名上下文、配置命名上下文和框架命名上下文。
- 多重身份验证提供程序（Secur32.dll）：多重身份验证提供程序（Multiple Authentication Provider, MAP）支持所有系统当中可用的安全包。安全包包括 Kerberos、Windows NT 局域网管理程序（NT LAN Manager, NTLM）、Secure 信道和分布式密码身份验证（Distributed Password Authentication, DPA）包。

本地安全授权机构（LSA）为基于 Windows 2000 的计算机维护所有本地的安全信息，它提供了如下一些功能。

- 用户身份和权限管理
  - 它允许用户在基于 Windows2000 的计算机上使用交互式身份验证。
  - 它在验证过程中为安全主体产生一个访问权标。这个访问权标含有用户账号和所有包含该用户账号的组的安全标识符（SID）。
  - 它确定哪些用户已被分配特权。
  - 它确定为某个安全主体的分配了哪些用户权限，并确保安全主体不会执行他没有拥有足够权限的任务。
- 安全策略管理
  - 它管理本地安全策略。这包括所有已为本地计算机定义的安全策略。如果任何一个组策略在站点、域或组织单位一级上被定义，这些设置可以在 Active Directory 中被覆盖。
  - 它管理审核策略和设置。这包括在内核模式下，当由安全引用监视器产生一个审核警报时，为相应的事件记录写一个警告。
- 对象管理
  - 它建立了一个可信任域列表，以在 Windows 2000 身份验证对话框中提供产生“登录到”的下拉列表。
  - 它为每个对象读取系统访问控制列表（System Access Control List, SACL）以确定为对象定义了哪些安全审核。
  - 它能对内存当中分页的和未分页的存储进行配额管理。

3.3 Windows 2000 安全协议概述

Windows 2000 允许多种网络安全协议来提供身份验证服务。这保证了对网络客户端的最大兼容性。这些客户可能包括使用早期操作系统的 Microsoft 客户端和异构的客户端，如 UNIX 客户端。支持多种安全协议保证了对 Windows 2000 网络的最大安全访问，而不必再被限制使用某一特定协议。

Windows 2000 支持四种不同的安全协议，如图 3-1 所示。

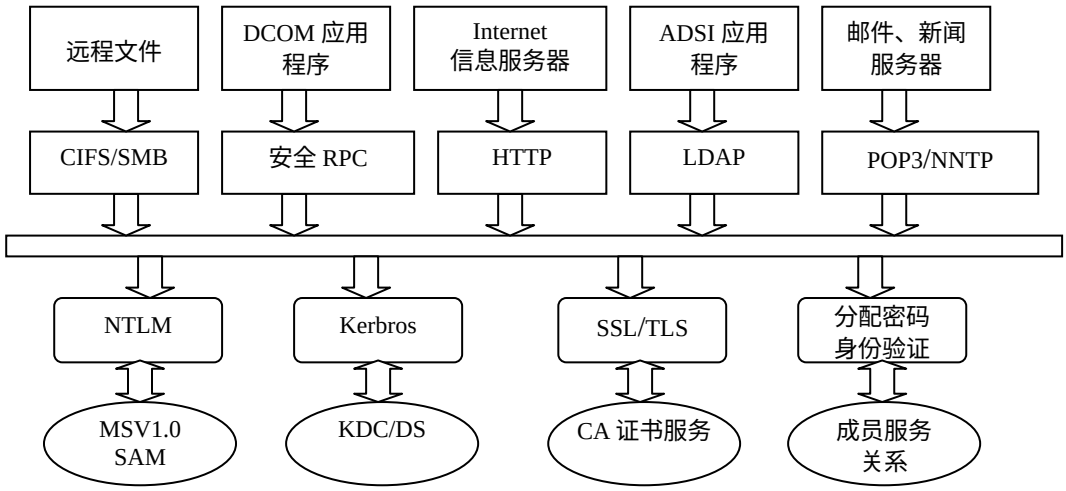

图 3-2 Windows 2000 安全协议

- NTLM（Windows NT LAN Manager）。由 Windows NT、Windows 95 和 Windows 98 客户端使用，这些系统上装有目录服务的客户端程序。NTLM 被用于通过在 Windows 2000 Professional 和 Windows 2000 成员服务器上的网络身份验证和本地账号身份验证以及到 Microsoft 早期操作系统的访问。NTLM 安全服务器使用 MCS1_0 验证服务和 Netlogon 服务来提供客户端身份验证和授权。
- Kerberos v5。基于 Windows 2000 计算机的默认安全协议。Kerberos 提供客户端和服务器的相互认证、更好的性能并提供委派支持。Kerberos 安全提供程序使用域控制器活动目录上的密钥分发中心（KDC）服务来获取 TGT 和服务票据。
- 分布式密码身份验证（Distributed Password Authentication）。由 Internet 会员组织如 MSN 所使用的共享的秘密身份验证协议。DPA 隶属于 Microsoft Commercial System（MCIS），它允许只使用一个账号和密码来连接所有在 Internet 会员组织内的会员站点。DPA 使用 MCIS 安全服务（通常称为“成员资格服务”）来验证会员资格和不同服务器所特有的访问信息。
- 安全信道（Secure Channel）服务。该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。如果使用一个公钥基础机构（PKI），这些协议能在分布式网络上同时提供客户端和服务器的身份验证。在 Windows 2000 中，可以使用证书服务来部署公钥基础机构，以创建证书颁发机构（CA）。这些 CA 负责颁发数字证书以用于身份验证。

3.4 Windows 2000 安全程序开发

Windows 2000 安全程序的开发体系如图 3-3 所示。

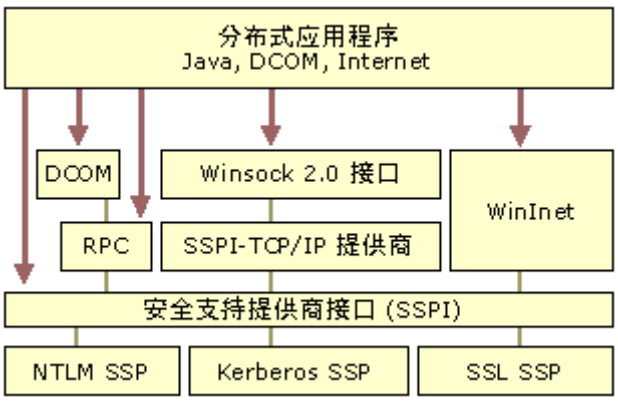

图 3-3 Windows 2000 安全程序开发体系

在该体系中，Microsoft 安全支持提供器接口（Security Support Provider Interface, SSPI）是定义得较全面的公用 API，用来获得验证、信息完整性、信息隐私等集成安全服务，以及用于所有分布式应用程序协议的安全方面的服务。应用程序协议设计者能够利用该接口获得不同的安全性服务而不必修改协议本身。可以将 Windows 2000 验证、信息完整性和个人隐私集成到分布式应用程序中。 应用程序开发者可以使用 DCOM 应用程序框架和被证实的 RPC，从更高级的接口来利用 SSPI 服务的优势。

SSPI 的主要特性是使应用程序拥有了一个公用的 API 来使用不同的安全包，包括 Windows NTLM 验证、SSL/PCT 公用密钥密码技术提供器以及 Windows 2000 中的 Kerberos 安全验证提供器。

应用程序开发者有权选择直接调用 SSPI 函数来集成 Windows NT 安全性，或者使用基于 DCOM、经验证的 RPC 或者 Winsock 2.0 等更高级的应用程序接口。Microsoft 开发了新的基于接口规格的安全包来支持 SSPI，并建议所有的基于 Win32 的应用程序开发者在进行安全分布式应用程序的开发时使用 SSPI 的集成安全特性。