第 5 章　身份验证

一个安全的系统需要控制对资源的访问，这是因为大多数网络本身就是不安全的，又因为众多的用户具有不同的访问权限以及具有可配置权限的资源。在 Windows 2000 安全模型中，对资源可用性的控制是一个分为两阶段的过程：第一阶段，系统必须对请求访问特定资源的个体或客户的身份进行验证，从而防止未知的用户访问网络资源；第二阶段，系统根据授予用户和资源的权限执行访问控制检查。这种授权检查就让管理员能够为不同的用户分配不同的访问权限。

本章将先主要介绍上述第一阶段的安全功能，即对用户的身份进行验证，这是 Windows 系统安全的一个重要方面。

5.1　身份验证概述

这里的身份验证指的是一个用户或客户为了访问服务或资源而向服务器验证自己的身份。由于网络上的大多数数据传输都是不安全的，所以有必要使得系统只将访问权限授予那些能够成功证明其身份的用户。

Windows 2000 的身份验证包括两个部分：交互式登录过程和网络身份验证过程，而用户身份验证的成功与否同时取决于这两个过程。交互式登录要求用户登录到域账户或者本地计算机账户，而网络身份验证则是向特定的网络服务提供对身份的证明。

对于登录到本地计算机账户的用户而言，网络身份验证是每次请求网络服务时都要重复进行的一个手工完成的过程；而登录到域账户的用户则由于 Windows 2000 中的单一登录特性（Single Sigh-on, SSO），只要登录到域账户，那么每次请求网络服务的时候都会透明地完成网络身份验证，无须任何手工操作。

过去简单的身份验证机制使用口令来控制对计算机和用户账户的访问。虽然在 Windows 2000 系统中，共享密钥仍然是身份验证的基础，但是用来保护这些密钥的机制和协议却已经发生了变化。由于使用了有效的验证协议，中间攻击人将很难截获登录证书、假冒用户。Windows 2000 系统支持大量的验证协议：其中 Kerberos v5 是主要的用于交互式登录和网络身份验证的协议，它也是 Windows 2000 系统默认的验证协议（Windows NT 默认的身份验证协议是 NTLM）；向下兼容 Windows NT 4.0 中 NTLM（NT LAN Manager）所提供的验证协议；为了保护 Web 服务器而进行双向的身份验证，提供了基于公私钥技术的安全套接字层（SSL）和传输层安全（TLS）协议。此外，Windows 2000 还支持把硬件令牌用于身份验证。如使用智能卡将密钥存储在硬件设备中，并用个人身份号码（PIN）或口令进行保护，从而降低了密钥的脆弱性。这样在进行身份验证的时候，除了必须提供正确的 PIN 之外，还必须实际持有硬件令牌，更有效地抵抗了网络假冒攻击。

5.2　交互式登录

如前所述，用户可以交互式登录到本地计算机或域账户。到本地计算机的成功登录可以向用户提供对该计算机上资源和服务的访问权限；而到域账户的成功登录，则可以同时向用户提供对本地计算机和域上身份验证服务的访问权限，在对基于服务器资源的访问请求进行网络身份验证期间就会用到此验证服务。

5.2.1 交互式登录组件

Windows 2000 系统的交互式登录需要下面三个系统组件：Winlogon.exe、GINA（Graphical Identification and Authentication, 图形化标识与验证）的动态链接库和网络提供程序的动态链接库。

- Winlogon：与 Windows NT 4.0 相同，Windows 2000 使用 Winlogon.exe 来提供对交互式登录的支持。Winlogon 负责管理登录相关的安全性工作，处理用户的登录与注销、启动用户 shell、输入口令、更改口令、锁定与解锁工作站等。Winlogon 还要向 GINA 发送事件通知消息，并提供可供 GINA 调用的各种函数。此外，Winlogon 还必须保证其与安全相关操作对其他进程不可见，以免其他进程获取登录密码。
- GINA 的动态链接库：登录进程的验证和身份验证都是在 GINA 所提供的动态链接库（DLL 文件）中实现的，它在系统引导的时候被 Winlogon 进程所加载。微软的 GINA 是 MSGINA.dll，实现了默认的 Windows 登录界面，提供了 Winlogon 用于标识和验证用户的输出函数。这个动态链接库是允许被替换的，这样任何人都可以自行定制系统的用户识别和身份验证。
- 网络提供程序的动态链接库：Winlogon 还可以加载一个或多个网络提供程序的动态链接库，以提供通过标准协议到其他类型网络（如 Novell）的辅助身份验证功能。

在启动用户程序之前的系统初始化阶段，Winlogon 将会注册一个安全注意序列（SAS, Secure Attention Sequence）的热键。任何时候按下 SAS 热键（默认为 Ctrl+Alt+Del），将调用 Winlogon 切换到安全桌面，从而使密码截获程序不能试图捕获登录密码或者更改密码等安全活动。

5.2.2 身份验证程序包

身份验证程序包位于一个动态链接库文件之中，它可以接受输入的登录证书，并且通过验证程序来决定是否允许用户登录。根据这个程序包，登录证书中可以包括口令、加密数据甚至生物统计学数据。

由于本地安全授权机构（Local Security Authority, LSA）在系统启动期间加载这个身份验证程序包，因此 LSA 在任何时候都可以对用户进行验证。这个验证的过程在 Windows 2000 身份验证的交互式登录阶段和网络验证阶段都会发生。

身份验证程序包除了验证用户之外，还要为用户新建一个 LSA 登录会话并返回一组绑定到用户安全令牌中的安全标识符（SID）。

Windows 2000 默认安装了两个验证程序包，它们分别是 MSV1_0 和 Kerberos v5。另外，Windows 2000 是可扩展的，即允许自行开发验证程序包来实现不同类型的用户验证过程。

5.2.3 本地安全授权机构

GINA 收集用户的登录数据，然后集中传递到本地安全授权机构（LSA）。作为 Windows 2000 系统的核心安全组件，LSA 负责在本地登录和远程登录中验证用户的身份，并维护本地安全策略。如图 5-1 所示，LSA 通过调用特定的身份验证程序来完成这些任务。

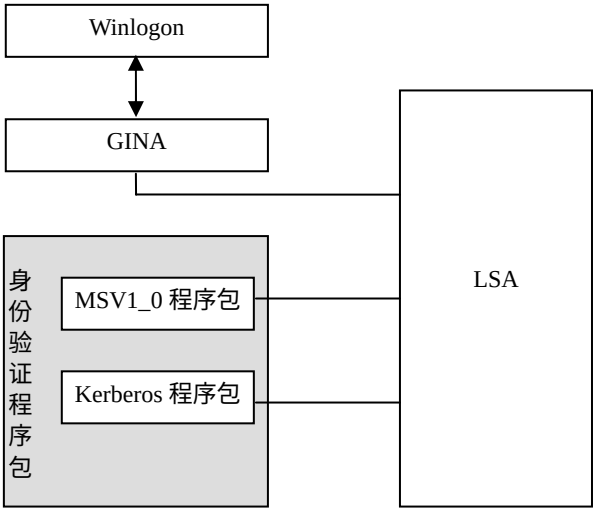

图 5-1　交互式登录组件

当身份验证程序包在用户验证时无论接受还是拒绝登录数据后，其结果都会通过 LSA 返回给 GINA，由 GINA 向用户显示验证是否成功，GINA 再将结果返回给 Winlogon。如果身份验证程序包成功的验证了用户身份，那么 Winlogon 就会为用户创建一个 Windows Workstation 和桌面，并启动用户与计算机进行交互的 Shell 进程。

5.2.4　交互式登录到本地计算机

为了登录到本地计算机，每个 Windows 2000 用户都必须在系统安全账户管理器（Security Account Manager, SAM）中具有一个账户。SAM 是一个受到保护的子系统，它通过存储在本地计算机注册表（位于 HKEY_LOCAL_MACHINE\SAM\SAM 下）中的安全账户来管理用户和组信息。当用户请求登录到本地计算机时，系统将登录信息与 SAM 数据库中的条目进行比较来判断用户提交的信息是否正确。虽然 Kerberos 是 Windows 2000 的默认身份验证协议，但它并不处理本地登录请求。

用户通过按下 SAS 热键（默认为 Ctrl+Alt+Del）来启动登录过程。Winlogon 一旦接收到此 SAS 热键就会切换到 Winlogon 桌面，并且调用 GINA 来显示标准的登录对话框，提示用户输入用户名和口令。一旦用户输入了这些信息，GINA 就将它传送给 LSA 进行验证。LSA 则调用适当的验证程序包（如 MSV1_0），并且将口令使用单向散列函数转换成非可逆的密钥形式，然后在 SAM 数据库中找寻匹配的密钥。如果 SAM 找到了账户信息，就向身份验证程序包返回用户的 SID 和用户所在组的 SID。验证程序包再向 LSA 返回这些 SID，LSA 使用这些 SID 创建安全访问令牌，并把令牌句柄和登录确认信息返回给 Winlogon。经历了这样的一个过程，用户就可以进入 Windows 桌面了。

5.2.5　交互式登录到域账户

域用户账户的信息存储在域的活动目录服务中。这样，当用户从一台 Windows 2000 计算机登录到域账户时，用户实质上是在请求允许使用那台计算上的本地系统服务。请求使用任何域服务的所有用户都必须在获得访问权限之前首先向域验证自己的身份。同样的，用户在允许使用 Windows 2000 计算机的本地系统服务之前也必须证明自己的身份。

默认情况下，域环境的登录和身份验证使用 Kerberos v5 协议，这里面包含有多个步骤。Kerberos 是一个基于票据（Ticket）的协议，为客户与服务器之间提供了双向的身份验证。为了访问和使用网络资源和服务需要进行票据申请和票据授予。本章稍后将会详细介绍 Kerberos v5 协议。

用户通过按下 SAS 热键（默认为 Ctrl+Alt+Del）来启动登录过程。Winlogon 一旦接收到此 SAS 热键就会切换到 Winlogon 桌面，并调用 GINA 来显示标准的登录对话框，提示用户输入用户名、口令和域名称。对域账户而言，用户登录名与用户主体名（UPN）格式一致。用户主体名由包含在账户中的用户账户名和账户所在域的域名组成，并由“@”字符隔开，例如 eric@SjtuInfosec.net。一旦用户输入了 UPN 和口令并选择了正确的域名，GINA 就会将这些信息传到 LSA 进行验证。

当 LSA 接收到用户的登录信息后，将口令使用单向散列函数转换成非可逆的密钥形式，然后将其存储在以后还可以检索到的证书缓存区中。LSA 通过 Kerberos 验证程序包与域控制器的密钥分发中心（Key Distribution Center, KDC）进行通信。Kerberos 验证程序包向 KDC 发送一个含有用户身份信息和验证预处理数据的验证服务请求。KDC 一旦收到这个验证服务请求之后，就用自己的密钥对其解密来验证用户是否确实知道口令。

一旦 KDC 证实了用户的身份，就会为客户返回一个登录会话密钥（用客户密钥加密），并且向 Kerberos 验证程序包返回一个 TGT（Ticket Granting Ticket，票据授予票据）。该 TGT（用 KDC 自己的密钥加密）允许用户为获得包括目录计算机上的系统服务在内的域服务而申请票据。Kerberos 验证程序包会将会话密钥解密并将它同 TGT 一起存储到证书缓存区中以备后用。

Kerberos 验证程序包为本地计算机向 KDC 发送一个票据请求，KDC 则会用会话票据响应。用户就可以用这个会话票据来请求访问计算机上的系统服务了。然后，LSA 确定用户是否为任何本地安全组的一部分，以及用户在这台计算机上是否拥有任何特权。据此而得到的 SID 与来自会话票据的 SID 一起被 LSA 用来创建会话令牌。该令牌句柄和登录确认信息返回到 Winlogon。至此，用户就可以进入 Windows 桌面了。交互式域账户登录的过程如图 5-2 所示。

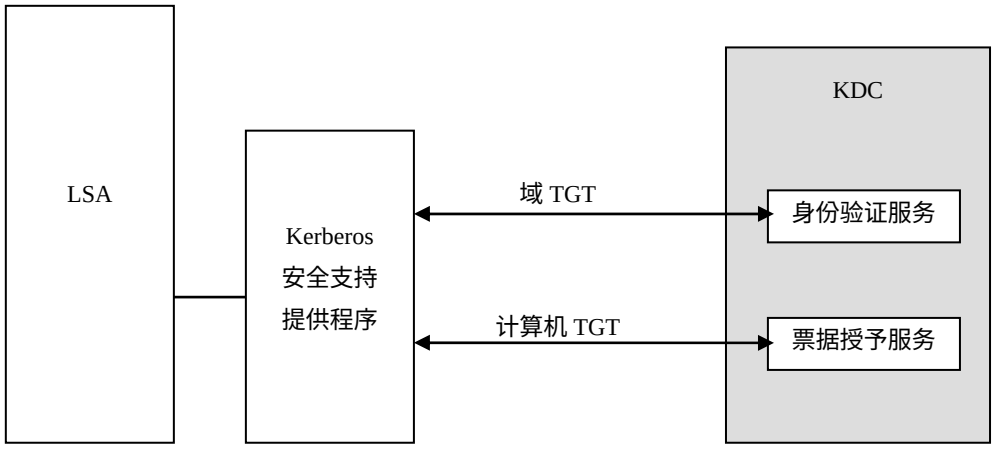

图 5-2　交互式域账户登录

默认情况下，每个域控制器都向域提供了一个 Kerberos v5 的 KDC。当 Windows 2000 计算机上的 Kerberos 客户想要向域验证自己的身份时，系统就会从 DNS 中找出最近可用的域控制器来进行密钥分配，即变成首选的 KDC。在用户登录会话期间，如果首选的 KDC 失效，那么客户就会从 DNS 中另外寻找一个 KDC 来继续进行验证。如果客户找不到任何可用于身份验证的域控制器，那么 Windows 2000 就会尝试使用 MSV1_0 来对用户进行身份验证。

5.3 网络身份验证

在 Windows 2000 单一登录特性这种架构中，网络身份验证依赖于成功的交互式域账户登录。单次登录（Single Sigh-on, SSO）是指用户只须向网络验证一次身份，之后无须另外验证身份就可访问所有被授权的网络资源。

网络身份验证的过程如图 5-3 所示。通过 Kerberos 验证程序包，用户会话将预先建立的 TGT 提交给 KDC 上的 TGS（Ticket Granting Service, 票据授予服务），TGS 向用户发行一个用于该项服务或资源的会话票据。然后，用户把这个服务票据（Service Ticket）提交给所请求的资源，就可以被授予相应的访问权限（由访问控制模型决定）。

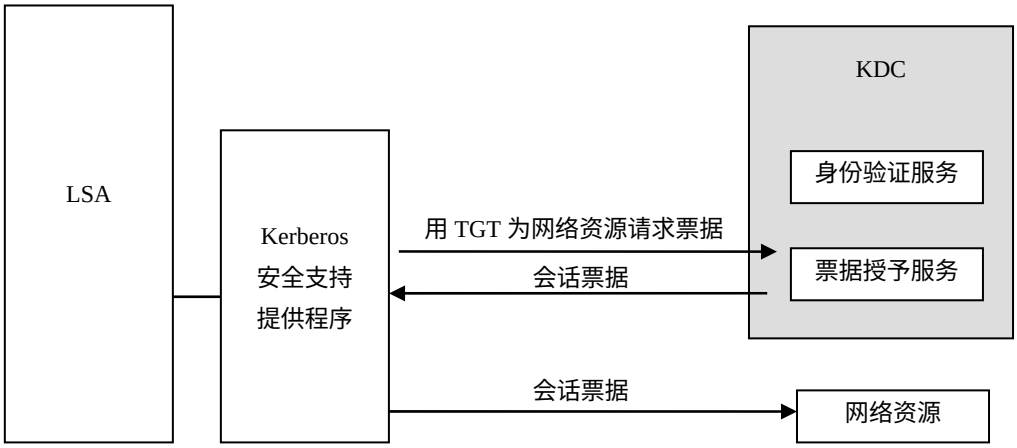

图 5-3 网络身份验证

5.4 NTLM 身份验证协议

NTLM（NT 局域网管理器）被用于验证不能使用 Kerberos 进行身份验证的客户，包括装有 Windows 95、Windows 98 和 Windows NT 的计算机。NTLM 协议是 Windows NT 4.0 系统中身份验证的默认协议，它在 Windows 2000 中仍然为了低版本客户和服务器的兼容性而保留。

NTLM 安全协议确实提供了许多的安全功能和相当严谨的用户认证机制，可是由于它存在着以下几种问题，造成了它的缺陷：

- NTLM 是微软开发的专用协议，而不是开放式的工业标准，所以对它的支持只有微软和它的支持厂商。
- NTLM 不提供双向的认证，只有服务器认证客户端，而客户端却没有一个相反的认证去支持服务器。例如 Linux 下的 Samba 服务器，就可以提供虚拟的 Windows NT 4.0 域控制器的作用，使用户网络中的 Windows NT 客户端认为它是一个标准的域控制器。这同时也使得 NT 的网络易于被黑客攻击，使用伪装的服务器认证，从而获得系统的访问权限。

在 Windows 2000 中，NTLM 被用作域中两台计算机之间事务的身份验证协议，其中一台或两台计算机运行 Windows NT 4.0 或更早的版本。

Windows 2000 在默认情况下以混合模式的网络配置安装。混合模式的网络配置使用 Windows NT 4.0 和 Windows 2000 的任意组合系统。如果没有混合模式网络，可以在域控制器中转换为本地模式来禁用 NTLM 身份验证。例

如，以下配置将使用 NTLM 作为身份验证机制。

- Windows 2000 Professional 客户端向 Windows NT 4.0 的域控制器验证身份
- Windows NT 4.0 Workstation 客户端向 Windows 2000 域控制器验证身份

- Windows NT 4.0 Workstation 客户端向 Windows NT 4.0 域控制器验证身份
- Windows NT 4.0 域中的用户向 Windows 2000 域验证身份

此外，NTLM 还是为没有加入到域中的计算机（如单机服务器和工作站）提供的身份验证协议。

5.5 Kerberos 身份验证协议

Windows 2000 系统采用 Kerberos 作为默认的身份验证协议。Kerberos 协议是美国麻省理工学院为 Athena 工程而设计的，它为分布式计算环境提供一种对用户双方进行验证的认证方法。Kerberos 是一种新的标准，它提供了协同工作的基础，同时增强了企业范围网络身份验证的安全。Kerberos 协议的最新版本 Kerberos v5，用来在分布式网络中提供一个单一的验证服务，已经被 IETF（Internet 工程任务组）在 RFC 1510 中所采纳。

Windows 2000 使用公钥验证的扩展来实现 Kerberos v5。Kerberos 客户是作为安全提供者通过安全支持提供者接口实现的。Kerberos 密钥分发中心（KDC）与运行在域控制器的其他 Windows 2000 安全服务相结合，并且使用域活动目录服务作为它的安全账户数据库（SAM）。

5.5.1 Kerberos 身份验证概述

Kerberos 身份验证的根据是票据。换句话说，Kerberos 协议是一个基于票据的系统。客户向网络验证，并从 KDC 请求票据用以访问网络资源。

Kerberos 协议所依靠的身份验证技术叫做共享机密身份验证。这个方法的前提很简单：若仅有两个人知道秘密，那么两人中的任何一个人都可以通过确认另一个人是否知道这个秘密来确认对方的身份。

使用 Kerberos 协议，客户机和服务器都会向 Kerberos 身份验证服务器注册。使用 Kerberos 身份验证的客户端将由用户密码派生的加密信息发送到 Kerberos 服务器，该服务器使用它来验证用户的身份。同样地，服务器将信息发送到客户端的 Kerberos 软件，该软件就可验证服务器的身份。该相互身份验证过程可同时避免客户机和服务器被怀有恶意的用户冒充。

5.5.2 Kerberos 的身份验证过程

KDC 提供了下面两项服务：

- 身份验证服务（AS）。AS 对客户进行验证，并发行供客户用来请求会话票据的 TGT（票据授予票据）。
- 票据授予服务（TGS）。TGS 在发行给客户 TGT 的基础上，为网络服务发行 ST（会话票据）。

在客户可以为网络服务请求会话票据之前，这些客户必须向网络验证自己的身份。AS 通过把所提交的登录证书与活动目录中的用户账户进行比较来确认客户的身份。一经确认，AS 就会发行一个供客户用来请求会话票据的 TGT。

默认情况下，TGT 的生存期为 10 小时。每次客户想要访问一个不同的网络服务时都会使用到 TGT。客户把 TGT 与他想要获得其票据的服务名一同提交给 TGS。一经批准，TGS 就会发行一个会话票据。客户收到该会话票据后就可将它存储在自己的票据缓存区中。

会话票据内部的字段内限定了该票据的有效期限。客户每次请求使用网络服务时，都要从它的票据缓存区中检索票据，并将它提交给所要访问的服务。上述过程可参见图 1-3。

从上述过程中可以看出，使用 TGT 的最主要好处就是减少了 KDC 必须查阅客户端信息的次数。虽然这个过程较为复杂，但用户惟一要做的就是输入自己的密码用来登录。

图 5-4 显示了客户机、KDC、活动目录和使用 Kerberos 身份验证协议的网络服务器三者之间的关系。

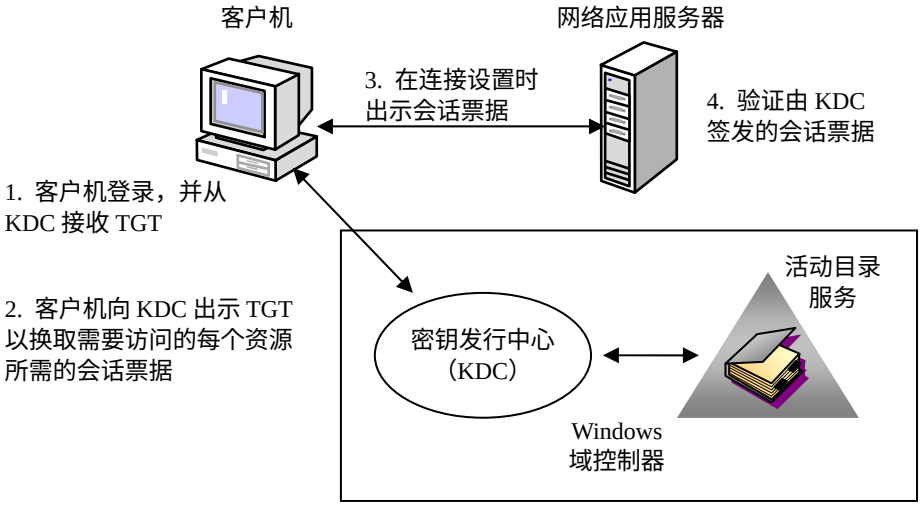

图 5-4　Kerberos 身份验证过程

5.5.3　Kerberos 的票据

出于保密性考虑，服务票据中的大部分数据都用服务器的密钥进行了加密。当然，为了客户能够管理自己的票据，每个票据都需要一个非敏感性的头信息，以供任何程序都不用对票据进行解密就可以访问到这个头信息。

以下的票据信息都是非加密的。

- 票据格式的版本号。在 Windows 2000 Kerberos v5 协议中，该版本号为 5。
- 发布票据的域的名称。
- 密钥发行中心的服务器名称。

而以下的票据信息则被服务器的密钥进行了保护。

- 客户和服务之间为安全传输而共享的会话密钥。
- 客户所在域的名称。
- 客户名称。
- 票据起始时间。
- 票据生存时间（有效时间）。

票据（包括 TGT 和 ST）是有生存时间的，那么当票据过期后会发生什么情况呢？Kerberos 协议改进网络和服务器性能的一种方式就是：当某个票据过期时，客户将不会得到任何通知。这是因为如果 Kerberos 对所有发布了票证的客户进行通知，那么用户的 KDC 和网络性能将会受到很大的影响。

下面让我们来看一下过期的 TGT 和 ST 的情况。

第一种情况是当某个客户的 TGT 过期，并且客户正在请求一个用于某个网络资源的 ST 时。此时当客户请求新的 ST 时，KDC 将响应一个错误消息，客户必须从 KDC 请求一个新的 TGT。

第二种情况是当客户试图使用一个过期的 ST 访问一个网络资源时。此时如果客户通过一个 ST 访问位于服务器上的某个资源，那么该服务器将响应一个错误信息，客户必须从 KDC 请求一个新的 ST。当客户被认证通过之后，他便可以访问服务器上的资源了。如果 ST 是在客户已连接到资源的期间过期的，那么客户不会立即断开连接；但是，当客户下一次请求访问该资源时，就需要上述过程来进行访问。

5.5.4 Kerberos 和 Active Directory

每个基于 Windows 2000 的域控制器将 Active Directory 实现为其目录并集成 KDC。这允许所有用户账户信息存储在单个目录中。若一个组织是中型或大型的，就可能有多个域控制器来给组织提供可用性和容量。这不会影响使用 Kerberos 身份验证的能力，因为只要有 Active Directory 的副本，就会有 Kerberos 身份验证服务的副本。

5.5.5 Kerberos 的身份验证委派

前面已经说明了客户端访问单个服务器的情况。然而，对于应用程序而言，使用几个服务器来执行任务是很平常的。例如，基于 Web 的应用程序可能既使用 Web 服务器，又使用一个数据库服务器，以此为基于浏览器的客户端提供信息。不用让客户端通过其所使用的每个服务器的个别身份验证过程，Windows 2000 提供跨多层应用程序（通常称为三层应用程序）的安全措施。

如前所述，基于 Windows 2000 的域间的传递信任关系极大地扩展了运行 Windows 2000 或 Windows NT 工作站的客户端在登录到基于 Windows 2000 的域后可访问的资源范围，无须使用许多不同密码来访问不同服务器和资源。访问范围（称为单一登录）是通过结合 Windows 2000 信任机制和 Kerberos 协议使用 Active Directory 来处理客户端身份验证的方法而达成的。

操作系统提供单一安全模型及基本结构以定义用户账户及管理访问权限。这表示可以在 Active Directory 中一次性定义设置，然后将其用于组织中的所有应用程序服务器。这种用来支持三层模型的方法就叫做身份验证委派，如图 5-5 所示。

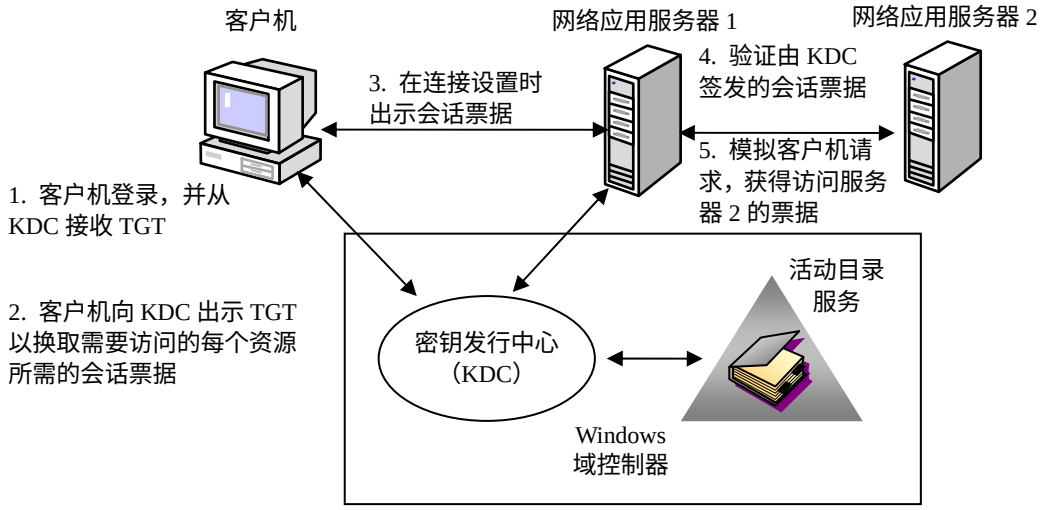

图 5-5 Kerberos 的身份验证委派

这种模型允许客户端身份验证交给应用程序涉及的服务器。此服务器会模拟客户端，并代表客户端来执行访问请求。这表示所有身份验证凭据和票据的传递并不需要用户输入。虽然服务器会模拟客户端，但对原始客户端的审核记录会被保存。当服务器处理一个由另一个服务器转送过来的请求时，其记录会显示客户机的名称，而非中介服务器的名称。

该模型是 Windows 2000 的一个重要元素，因为它支持单一登录并简化（不影响）安全性。现在的许多应用程序需要为安全性准备单独的账户数据库。但是使用 Active Directory 集中存储安全信息的应用程序有助于创建更易于管理和伸缩的网络。

5.5.6 Kerberos 协议的优缺点

Kerberos 协议比 NTLM 协议更加灵活和有效率，并且更加安全。使用 Kerberos 验证有以下好处。

- 服务器更加高效的验证。使用 NTLM 验证，应用程序服务器为了验证每一个用户必须连接到域控制器。而使用 Kerberos 验证，服务器就不再需要连接到域控制器了，它能够通过检查当前用户的信用证书验证客户。客户能够一次获得特定服务器的信用证书，并且在网络登录对话中再次使用它们。
- 相互验证。NTLM 允许服务器检验它们客户的身份。它不允许客户检验服务器身份，或者一个服务器检验另一个服务器的身份。NTLM 验证是为服务器假定为纯粹的网络环境中而设计的，而 Kerberos 协议不需要任何假设，网络连接两端的团体都能够知道另一端的团体所声称的是什么。
- 授权验证。Windows 服务在自己访问需要资源时模拟客户。许多情况下，服务能够通过访问本地计算机中的资源为客户完成工作。NTLM 和 Kerberos 都提供服务需要模拟其本地客户的信息。然而，一些分布式应用程序设计用来使得前端服务在连接到其他计算机上的后端服务时必须模拟客户。Kerberos 协议有代理机制，它允许服务在连接到其他服务时模拟其客户，而不需要存在 NTLM。
- 简化信任管理。Kerberos 协议的好处之一是 Windows 2000 域之间的信任验证是通过默认的双向和传递。多域网络不再需要明确的、点到点信任关系的复杂网络。相反，能够组织大型网络中的许多域到传递的、相互的信任树中。如果网络包含超过一个的树时，整个森林将接受任何树中的域发出的信任证书。
- 协同工作能力。Microsoft 对于 Kerberos 协议的实现是基于 Internet 工程任务组（IETF）推荐的标准途径规范的。因此，当 Kerberos v5 用作验证时，Windows 2000 中此协议的实现是位于同其他网络协同工作能力基础之上的。

Kerberos 协议有其优点，同时也有其固有的缺点，主要如下所述。

- Kerberos 服务器与用户共享的秘密是用户的口令字，服务器在回应时不验证用户的真实性，假设只有合法用户拥有口令字。如攻击者记录申请回答报文，就易形成代码本攻击。
- AS 和 TGS 是集中式管理，容易形成瓶颈，系统的性能和安全也严重依赖于 AS 和 TGS 的性能和安全。
- 随着用户数的增加，密钥管理较为复杂。Kerberos 拥有每个用户的口令字的散列值，AS 与 TGS 负责户间通信密钥的分配。当 N 个用户想同时通信时，仍需要 N*(N-1)/2 个密钥 。

5.5.7 启用 Kerberos 协议

若想使用 Kerberos v5 协议在运行网络服务的服务器与需要访问这些服务的客户机之间进行身份验证，那么客户机与服务器都必须运行 Windows 2000。

在安装 Windows 2000 时，就自动启用了 Kerberos 协议来进行身份验证。与 KDC 和 TGS 一样，位于域控制器上的 Kerberos v5 服务也是用“活动目录安装向导”来安装的。一旦安装了这些服务，安装程序就会启动 TGS 并启用 Kerberos 身份验证。

5.5.8 Kerberos 协议的其他应用

在 Windows 2000 系统中，除了将 Kerberos v5 应用于身份验证之外，还在许多其他的系统服务中应用了 Kerberos 协议。例如，在后续章节中介绍的 IPSec 就是默认使用 Kerberos v5 作为身份验证协议的。

5.6 智能卡

Windows 2000 系统引入了智能卡验证（通过 Kerberos v5 协议的一个扩展），以取代口令来实现可靠的网络身份验证。在 Windows 2000 系统中，Microsoft 通过将公钥证书技术和智能卡集成在一起，帮助客户增强了他们的安全等级。

5.6.1 何为智能卡

“智能卡”这一名词被用来描述一类信用卡大小的卡片。它具有多种性能，如保值卡、触摸卡和 IC 卡（ICC）等，所有这些卡的功能各不相同。IC 卡对于 Windows 2000 系统来说是最适用的，因为它能够执行许多复杂的操作，例如数字签名和密钥交换。一块智能卡从本质上来说是一个微型的计算机，以信用卡的形式嵌在塑料内，具有有限的存储和处理能力。将智能卡插入智能卡阅读机中，其中的电路就可以获取能量。智能卡同运行于计算机上的应用程序之间的数据通信通过一个双向的串口进行，并由智能卡阅读机和相关的设备驱动程序进行控制。智能卡阅读机有多种形状，并且能够通过 RS－232、PCMCIA 或者 USB 等接口同计算机相连。

Windows 2000 系统的安全模型将智能卡作为加密的外围设备，并用来存储用于网络登录和远程访问验证的验证证书。Microsoft 公钥基础结构（PKI）使用一对密钥来进行需要加密的操作（如身份验证、数据加密和完整性校验等）。实现智能卡功能的加密服务提供程序允许把这一对密钥（包括公钥和私钥）存储在智能卡上。出于对密钥的保护，大多数的智能卡都允许访问公钥，但除了以加密的形式之外都不允许直接对私钥进行读写操作。

5.6.2 智能卡的作用

智能卡可以向诸如客户身份验证、登录到 Windows 2000 域、代码签名和保护电子邮件之类的任务提供安全性解决方案。通过智能卡登录到网络提供了很强的身份验证方式，因为在验证进入域的用户时，这种方式使用了基于加密的身份验证和所有权证据。例如，如果某个攻击者无意或有意得到了用户的密码，就可以使用该密码在网络上假冒该用户的身份。很多人都选择容易记忆的密码，这会使密码具有先天脆弱性，容易遭受到攻击。而在使用智能卡的情况下，那个攻击者将必须获得用户的智能卡和个人识别码（PIN）后才能假冒该用户。显然，该情况下更不容易遭受到攻击。另一个优点是，连续发生几次不成功的 PIN 输入后，智能卡会被锁定，使得对智能卡进行字典式的穷举攻击非常困难。

智能卡是 Microsoft 集成在 Windows 2000 系统中的公钥基础结构（PKI）中的一个关键组件。智能卡增强了诸如交互式登录、客户端验证和远程登录等软件解决方案，它提供了以下一些功能：

- 保护私钥和其他形式个人信息的防篡改存储区。
- 将安全性关键计算隔绝起来，包含从不必“必须知道”的其他组织部门进行的身份验证、数字签名和密钥交换。
- 在单位、家庭或路上的不同计算机之间发凭据及其他私人信息的可携带性。

5.6.3 安装智能卡阅读器

在可以使用智能卡之前，必须在计算机上安装智能卡阅读器。Windows 2000 系统默认安装有一些智能卡阅读器的设备驱动程序。当你需要手动安装智能卡阅读器时，应该按照以下步骤实行。

（1） 关闭计算机，切断电源。

（2） 将阅读器器连接到可用的串行端口，或将 PC 卡阅读器插入到可用的 PCMCIA 类型 II 插槽。

（3） 启动计算机，并且以管理员权限登录。

（4） 执行以下任一项操作：

- 如果 driver.cab（安装 Windows 2000 时安装在硬盘中）文件中提供了智能卡阅读器的设备驱动程序，那么无须用户提示就会进行驱动程序的安装。这可能需要几分钟。当工具栏上出现“拔出或弹出硬件”图标（如果以前没有），以及“拔出或弹出硬件”对话框的硬件设备列表中出现刚刚安装的阅读器时，就可以确认安装成功了。
- 如果智能卡阅读器的设备驱动程序不在 driver.cab 文件中，则会启动“添加/删除硬件向导”。请根据指示来安装设备驱动程序。

如果智能卡阅读器没有自动安装，或“添加/删除硬件向导”没有自动启动，那么这块智能卡阅读器可能不兼容即插即用。这时候应该与智能卡阅读器的制造商联系，以获取设备驱动程序及安装和配置设备的说明。最后，在 Windows 2000 系统平台上不推荐使用非即插即用的智能卡阅读器。

5.6.4 智能卡的使用

只要安装有了智能卡读取器，并且拥有包含登录证书的有效智能卡之后，就可以登录到 Windows 2000 域了。通常情况下，当按下 SAS 热键后，系统便会提示用户名、口令和将要登录的域名称。而对于智能卡身份验证而言，当提示输入 PIN 码时，只要输入正确的 PIN 即可。

使用智能卡进行交互式登录与基于口令的登录过程相似。它们的差别在于：基于口令登录的时候，单一密钥是经过单向散列函数转换生成的；而智能卡是应用公私钥技术的一个产品，并且工作在双密钥系统之上。

Windows 2000 系统实现了 Kerberos v5 的一个公钥扩展，使之能够支持智能卡。当 KDC 验证用户并提供登录会话密钥和 TGT 时，这个扩展修改初始交换信息。KDC 并没有使用基于口令的对称密钥来加密登录会话密钥，而是使用用户的公钥，这样已加密的会话密钥只能通过用户智能卡上的私钥才能解密。

如上所述，当用户将智能卡插入智能卡读取器时就可以启动登录的一系列操作，这会产生一个 SAS，相当于按下了 Ctrl+Alt+Del 组合键。Winlogon 随即切换到 Winlogon 桌面，调出 GINA，显示一个对话框要求用户输入激活的 PIN。当用户输入正确的 PIN 后，GINA 把用户的登录信息传送给 LSA。LSA 用 PIN 获取用户的公钥证书，并把此证书与普通的验证域处理数据一起发送到 KDC。KDC 进行响应时，使用证书中的公钥加密会话密钥。而 LSA 则用智能卡上的私钥解密会话密钥。这样，一旦进行了解密，会话密钥就可以对双方之间的其他传输进行保护了。