操作系统安全简论

——Windows NT 操作系统安全(一)

卿斯汉 (中科院信息安全技术工程研究中心 100080)

1 Windows NT 操作系统简介

Windows NT是Microsoft公司于1992年开发的一个完全32位的操作系统，它支持进程、多线程、均衡处理和分布式计算。Windows NT是一个支持并发的单用户系统,可以运行在不同的硬件平台上，例如：Intel系列、MIPS和Alpha AXP等。Windows NT的结构是层次结构和客户机/服务器结构的混合体，除了与硬件直接相关的部分由汇编语言实现外，其余主要部分是用C语言编写的。Windows NT用对象模型管理它的资源，因此，在Windows NT中使用对象而不是资源。Microsoft宣称Windows NT是一个安全的操作系统，它的设计目标是橘皮书的C2级。一个C2级别的操作系统必须在用户级实现自主访问控制，必须提供审计访问对象的机制。此外，必须实现客体重用。

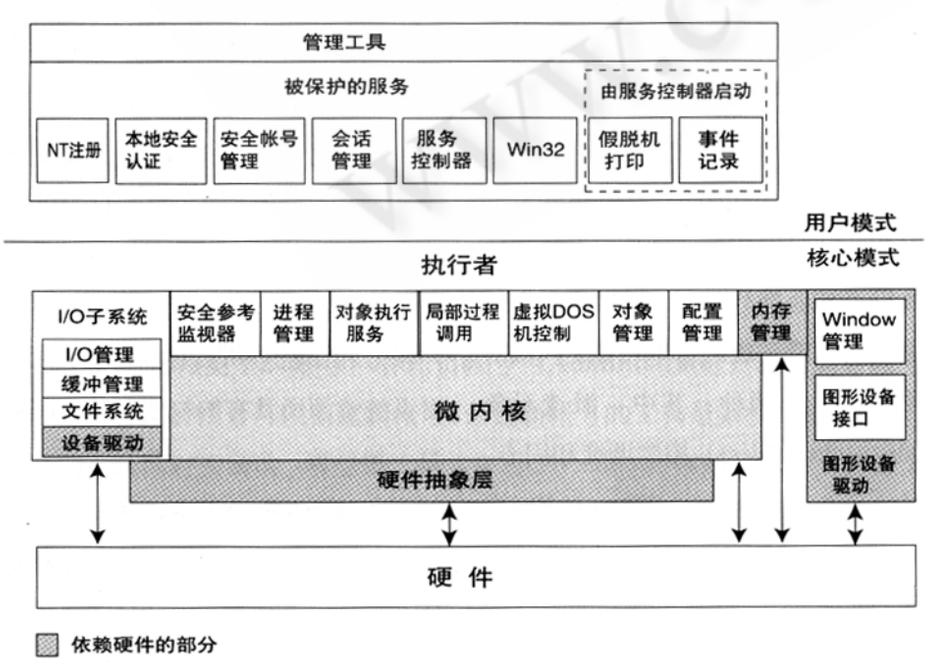

图 1 Windows NT 系统结构

一个操作系统可以用以下几种方法设计。第一种方法，一般是小系统比如MS-DOS，系统由可以相互调用的一系列过程组成。这种结构有许多缺点，例如，修改一个过程可能导致系统其他部分发生错误。另一种方法把系统划分为模块和层，这种系统称为层次系统。每个模块为其他模块（在更高层）提供一系列函数以供调用。这种设计方法比较容易修改和测试，此外，可以方便地替换掉一层；第三种方法是客户机/服务器结构，在这种方法中操作系统被划分为一个或多个进程。每个进程被称为服务器，它提供服务，例如内存管理。可执行的应用被称为客户机，一个客户机通过向指定的服务器发消息请求服务。系统中所有的消息都是通过微内核发送的，如果有多个服务器存在，则它们共享一个微内核。另一方面，客户机和服务器均在用户模式执行。这种方法的优点是，一个服务器发生错误或重起时，不影响系统的其他部分。MACH操作系统就是用这种方法设计的。

Windows NT的结构是层次结构

和客户机/服务器结构的混合体，其系统结构如图1所示。

执行者是唯一运行在核心模式中的部分。它划分为三层：最底层是硬件抽象层，它为上面的一层提供硬件结构的接口，有了这一层就可以使系统方便地移植。在硬件抽象层之上是微内核，它为低层提供执行、中断、异常处理和同步的支持。最高层由一系列实现基本系统服务的模块组成，例如：虚拟内存管理、对象管理、进程和线程管理、I/O管理、进程间通信和安全参考监视器。这些模块之间的通信是通过定义在每个模块中的函数实现的。

被保护的子系统提供了应用程序接口（API）。被保护的子系统有时被称为服务器或是被保护服务，它以具有一定特权的进程形式在用户模式下执行。当一个应用调用API时，则消息通过局部过程调用（LPC）发送给对应的服务器，然后服务器通过发送消息应答调用者。可信计算基（TCB）服务是被保护的服务，它在与系统安全相关的环境下以进程方式执行，这就意味着进程占有一个系统访问令牌。

以下介绍一些标准的服务：会话管理（Session Manager）、NT注册（WinLogon）、Win32、本地安全认证（LSA）和安全帐号管理（SAM）。

会话管理是Windows NT启动的第一个服务。它负责启动DOS设备驱动，将子系统在注册表中注册，并且初始化动态链接库（DLLs），然后启动NT注册（WinLogon）服务。

NT注册是一个注册进程。它负责为交互式注册和注销提供接口。此外，它还管理Windows NT的桌面。NT注册服务本身在系统初始化时，以logon进程通过Win32注册。

Win32为应用程序提供有效的微软32API。另外，它提供图形的用户接口并且控制所有用户的输入和输出。此服务只输出两种对象：WindowStation（例如，用户的输入/输出设备：鼠标、键盘和显示器）和桌面对象。

本地安全认证主要是进行安全服务的。它在用户注册进程、安全事件日志进程等本地系统安全策略中起到重要的作用。安全策略是由本地安全策略库实现的，库中主要保存着可信域、用户和用户组的特权和访问权限、安全事件。这个数据库是由本地安全认证来管理的，并且只有通过本地安全认证才能访问它。

安全帐号管理主要是管理用户和用户组的帐号，根据它的权限决定它的作用是在本地内还是在域的范围。此外，它还为认证服务提供支持。安全帐号作为子对象存储在注册表中的数据库中，这个数据库只有通过安全帐号管理才能访问和管理。

在Windows NT中，所有的软件、硬件资源都是用对象表示的。例如：文件、信号量、计时器、线程、进程和内存。实际上，它们可分为以下两种：

（1）微内核对象，有时称为内核对象。它是由微内核产生的最基本的对象，对用户是不可见的。它输出给执行者其他部分应用，提供只有内核最低层才能完成的基本功能。内核对象也可分为两种：其中，派遣对象（dispatcher object）控制调度和同步。Mutant,、Event、Event Pair、Semaphore、Timer、Thread、Process和Queue都是NT中的派遣对象。派遣对象有一个信号状态，它可以允许线程挂起对象的执行，直到信号状态发生改变。控制对象（Control objects）是由执行者和设备驱动控制的。它们不可等待，因此，没有信号状态。控制对象包括：中断、设备队列、Profiles、异步过程调用（APCs）、延迟过程调用（DPCs）。

（2）执行者对象，它在用户模式下可见。大多数执行者对象封装一个或多个微内核对象。执行者为诸如Win32的服务提供一系列的对象。这些对象与通过Win32 API、POSIX API或是OS/2 API提供给应用程序的对象不同。通常情况下，服务直接为客户机程序提供执行者对象。另外，服务可以为客户机应用基于一个或多个简单对象构造一个新的对象。

2 Windows NT 安全模型

Windows NT的安全模型影响整个Windows NT操作系统。由于对对象的访问必须经过一个核心区域的验证，因此没有得到正确授权的用户是不能访问对象的。

首先，必须在Windows NT中拥有一个帐号；其次，规定该帐号在系统中的特权和权限。在Windows NT系统中，特权专指用户对整个系统能够做的事情，如关闭系统、添加设备和更改系统时间等。权限专指用户对系统资源所能做的事情，如对某文件的读、写和操作，对打印机队列的管理等。Windows NT系统中有一个安全帐号数据库，其中存放的内容有用户帐号和该帐号所具有的特权，用户对系统资源所具有的权限和特定的资源一起存放。

在Windows NT中，安全模型由本地安全认证、安全帐号管理器和安全参考监视器构成。除此之外，还包括注册、访问控制和对象安全服务等，它们之间的相互作用和集成构成了安全模型的主要部分。Windows

NT的安全模型如图2所示：

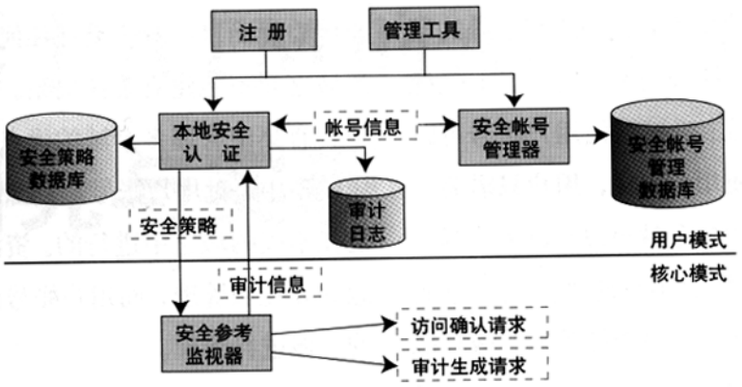

图 2 Windows NT 的安全模型

2.1 用户和工作组

在Windows NT中，每个用户必须有一个帐号，以便登录和访问计算机的资源和网络资源。用户帐号包含的内容如表1所示：

表 1 用户帐号中所含的部分数据

项 目	说 明
用户名（Username）	用户登录名
用户全称（Full Name）	用户全称，例如用户名为TAI，而用户全称为“David TAI”
用户密码（Password）	用户用来登录的密码
隶属的工作组（group）	用户属于哪一个工作组
用户环境配置文件（Profile）	设置与记录用户登录时的工作配置文件。例如，包含哪些程序组、屏幕的颜色、网络的连接状况等设置
可在哪些时间登录（Logon Hours）	设置用户只有在允许的时间内，才可登录
可从哪些工作站登录	限制用户只能够在某些工作站上登录
帐号有效日期（Expiration Date）	有效日期过后，用户无法进行登录
登录脚本文件（Logon Script）	设置用户在登录时自动运行的文件
主目录（Home Directory）	设置用户登录后的起始工作目录
拨入（Dialin）	设置用户是否可以通过拨号的方式连接Windows NT网络

一般有两种类型的帐号：管理员帐号（Administrator）和访问者帐号(Guest)。管理员帐号可以创建新帐号，创建新帐号的工具是系统的标准配置，它是随系统同时安装的。从范围的角度来看，Windows NT还可以分为两种类型的帐号：全局帐号和本地帐号。全局帐号可以在整个域内应用，而本地帐号只能在生成它的本机上应用。

类似UNIX组的概念，Windows NT支持工作组。通过工作组，可以方便地给一组相关的用户授予特权和权限。此外，一个用户可以同时属于一个或多个工作组。进一步，Windows NT提供了许多内置的工作组：管理员(Administrator)、备份操作员(Backup Operators)、打印操作员（Printer Operators)、特权用户(Power Users)、用户(Users)和访问用户(Guest)。例如，一个备份操作员工作组的用户具有备分系统的特权。总之，在Windows NT中，不同的系统管理员有不同的特权。除了内置的工作组，系统管理员可以通过User Manager定义新的工作组。

在Windows NT中，有两种类型的工作组：全局工作组和本地工作组。本地工作组只能在本地的系统或域内使用。在本地系统的级别上，本地工作组可以用于管理它们所处系统的特权和权限；在域的级别上，本地工作组可以用于管理它们所处的域服务器中的特权和权限。总之，只有在创建它的本地系统或域中才能利用本地工作组实现对特权和权限的管理。全局工作组可以在系统中相互信任的域中使用。利用全局工作组，系统管理员能够有效地将用户按他们的需要进行排序。

2.2 域和委托

域模型是Windows NT网络系统的核心，所有Windows NT的相关内容都是围绕着域来组织的，而且大部分Windows NT的网络都是基于域模型。同工作组相比，域模型在安全方面有非常突出的优越性。

域是一些服务器的集合，这些服务器被归为一组并共享同一个安全策略和用户帐号数据库。域的集中化用户帐号数据库和安全策略使得系统管理员可以用一个简单而有效的方法维护整个网络的安全。域由一个主域控制器、备份域控制器、服务器和工作站组成。建立域可以把机构中不同的部门区分开来。虽然设定正确的域配

置并不能保证人们获得一个安全的网络系统，但使管理员能控制网络用户的访问。

在域中，维护域的安全和安全帐号管理数据库的服务器称为主域控制器，而其他存有域的安全数据和用户帐号信息的服务器则称为备份域控制器。主域控制器和备份域控制器都能验证用户登录上网的要求。备份域控制器的作用在于，如果主域控制器崩溃，它能为网络提供一个备份并防止重要数据因此而丢失。每个域只允许有一台主域控制器。安全帐号管理数据库的原件就存放在主域控制器中，并且只能在主域控制器中对数据进行维护。在备份域控制器中，不允许对数据进行任何改动。

委托是一种管理方法，它将两个域连接在一起，并允许域中的用户互相访问。委托关系可使用户帐号和工作组能够在建立它们的域之外的域中使用。委托分为两个部分，即受托域和委托域。受托域使用户帐号可以被委托域使用。这样，用户只需要一个用户名和口令就可以访问多个域。

委托关系只能被定义为单向的。为了获得双向委托关系，域与域之间必须相互委托。受托域就是帐号所在的域，也称为帐号域；委托域含有可用的资源，也称为资源域。在Windows NT中有三种委托关系：单一域模型、主域模型和多主域模型。

在单一域模型中，由于只有一个域，因此没有管理委托关系的负担。用户帐号是集中管理的，资源可以被整个工作组的成员访问。

在主域模型中有多个域，其中一个被设定为主域。主域被所有的资源域委托而自己却不委托任何域。资源域之间不能建立委托关系。这种模型具有集中管理多个域的优点。在主域模型中，对用户帐号和资源的管理是在不同的域之中进行的。资源由本地的委托域管理，而用户帐号由受托的主域进行管理。

在多主域模型中，除了拥有一个以上的主域外，多主域模型和主域模型基本上是一样的。所有的主域彼此都建立了双向委托关系。所有的资源都委托所有的主域，而资源域之间彼此都不建立任何委托关系。由于主域彼此委托，因此只需要一份用户帐号数据库的拷贝。■

（未完待续）