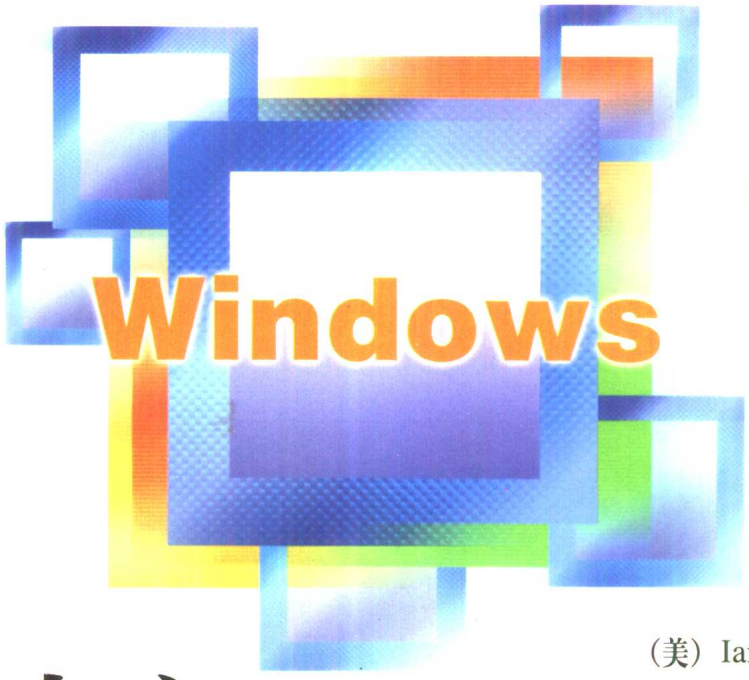
Windows 2000 Security Little Black Book

HZ BOOKS

Windows 技术丛书



Windows 2000

(美) Ian Mclean 著 吴世忠 祝世雄 等译

中文 Windows 2000 安全技术

机械工业出版社 China Machine Press

CORIOLIS

Windows技术丛书

中文Windows 2000 安全技术

（美） Ian McLean 著
吴世忠 祝世雄 等译
[redacted] 审校

机械工业出版社
China Machine Press

本书全面介绍Windows 2000最新安全技术，内容包括账户管理、Kerberos5鉴别协议、基于公钥证书的鉴别、基于安全套接层（SSL 3）的安全通道、密码应用程序接口、虚拟专用网等。本书图文并茂，条理清晰，包括大量实用的快速解决方案。无论是Windows 2000的新用户还是老用户，都能从本书受益。

Ian McLean: Windows 2000 Security Little Black Book.

Original English language edition published by The Coriolis Group LLC, 14455 N. Hayden Drive, Suite 220, Scottsdale, Arizona 85260 USA, telephone (602) 483-0192, fax (602) 483-0193.

本书版权登记号：图字：01-2000-1719

图书在版编目（CIP）数据

中文Windows 2000安全技术 /（美）米克林（McLean, I.）著；吴世忠等译. -北京：机械工业出版社，2001.6

（Windows技术丛书）

书名原文：Windows 2000 Security Little Black Book

ISBN 7-111-08882-4

Ⅰ.中… Ⅱ.①米…②吴… Ⅲ.①计算机网络-安全技术②服务器-操作系统（软件），Windows 2000 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2000）第19374号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：程代伟 张鸿斌

北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行

2001年6月第1版第1次印刷

787mm × 1092mm 1/16 · 16.25印张

印数：0 001-5 000册

定价：35.00元

译 者 序

操作系统是信息系统中最基本的软件系统，它直接管理硬件资源的使用，同时向其他的程序、软件提供服务，信息系统的安全依赖于运行的操作系统平台，操作系统安全在信息系统安全中处于最基础、最核心的地位，因此操作系统是否安全关系到整个系统的安全。

Windows操作系统是微软公司的拳头产品，由于其操作简单，易于使用，具有友好的用户界面，因而在全球得到了广泛的应用。微软很重视Windows操作系统及其应用软件的开发和应用，投入了大量的人力和物力进行Windows系统产品的开发，相继发布了Windows NT、Windows 95、Windows 98等系列产品。最近又推出了声称具有完整的安全解决方案的操作系统，即Windows 2000。

在Windows 2000推出之际，我们翻译了这本专门介绍其安全特性的书籍，本书介绍了Windows操作系统的许多新的安全特点，如更加灵活安全的账户管理、Kerberos 5鉴别协议、基于公钥证书的鉴别、基于安全套接层（SSL 3）的安全通道、密码应用程序接口（CryptoAPI）、虚拟专用网（VPN）等安全技术。增强了Windows操作系统的安全性。

必须声明的是，我们翻译本书是希望国内用户对Windows 2000的安全特征有所了解，并不表明Windows 2000本身就已经很安全，实际上，从它面市的那一天起，就不断有关于Windows 2000安全漏洞的新闻流传，在Windows 2000中使用的DES加密算法，是美国政府用于非保密数据保护的算法，其使用的安全性和实际强度的隐患是学术界和使用界长期存在的话题。今年欧盟又专门披露了美国国家安全局（NSA）在出口到美国以外的安全产品（包括操作系统）中使用“密码功能降低字段”（WRF）的真相，更大大降低了美国出口产品的安全性。同时，在微软的Windows系统中，还有关于USA密钥，NSA密钥的风波，更使Windows系统的安全性扑朔迷离。好在本书对Windows 2000的安全性能有详细的介绍和分析，相信读者能从中受益。

在本书的翻译过程中，得到了国防保密通信重点实验室和国家信息安全测评认证中心的大力支持，在文字校对上得到北京启明星辰公司的热情帮助，很多同志付出了艰辛的努力，除封面署名外，参加翻译校对的还有钟博、童登高、武怀玉、邱敏、陈维彬、宋立军、黄橙、王辉、韦文玉、杨鹏等。由于译者水平有限，疏漏之处在所难免，敬请读者指正。

2000年10月

前　言

要达到正确的网络安全级别简直就像走钢丝，显得像漫步在有十二个车道的高速公路中一样地困难。作为一名系统管理员，除非确信绝对必要，否则是不会指定权限和许可的。虽然用户需要访问足够的资源来完成他们的工作，但他们想要的资源总是比实际需要的更多。高级管理人员往往要求提供不恰当的高安全级别，当然，这不花费什么，但他们根本就不会用到这么多。而且你不得不改进，并且不停地改进。昨天是安全的，今天就不一定安全，对明天的技术来说，永远没有安全可言。

虽然许多好的安全准则是独立于产品的，但本书要讨论的是有关微软Windows 2000的网络安全问题。这是一本技术手册，着眼于技术问题——但请牢记，安全性不仅是技术问题，更是人的问题。不管你的安全设计得多么高明，也仍会遇到用户不经意离开处于登录状态的机器、写下他们的口令并贴在VDU（视频显示装置）上，或者他们不慎丢失了皮夹或钱包，而其中有信用卡和个人识别号（PIN）。你要做的工作是平衡安全性和可用性，建立一个大家能接受的、可用的、切合实际的安全准则。安全需求越严格、越麻烦，使用者越不喜欢。

Windows 2000的安全特性

Windows 2000的安全特性是建立在Windows NT 4提供的安全特性之上的。在NT 4中，Windows域中的单点登录允许用户在公司网络的任何地方访问资源。它为安全策略和账户管理提供了易于使用的工具。灵活的域模式（从局部的单域到覆盖全球的多主域）支持广泛的网络配置。

Windows 2000也为应用服务的BackOffice系列产品提供了一体化的安全基础，包括Microsoft Exchange、SQL Server、SNA Server和Microsoft Systems Management Server。Windows 2000的安全模式使各组织可以与合作伙伴、供应商、以及在信任关系之上使用基于Internet技术的消费者安全地交互。Windows 2000重新定义了信任关系，使得它们比NT 4模型更易于使用。

安全技术发展很快。公钥证书和动态口令满足了企业环境的安全性需求。通过公开网络的远程访问和用于商业对商业（B to B）通信的Internet访问正在推动安全技术的发展。智能卡正在代替已证明有问题的口令字安全。生物统计学为账户安全和易用的结合提供了合理的基础，它使用独一无二的物理特性（如指纹和视网膜扫描）代替PIN。注意，我说的是“合理的”，而不是“完全可靠的”。没有任何东西是完全可靠的。

本书适合读者

本书适合于有Windows NT 4、NetWare或UNIX背景的网络专业人员，以及那些正在管理或打算管理Windows 2000网络——特别是想设置Windows 2000安全性的人员。它也适合于技术支

持人员、顾问、负责网络安全开发和设置的设计人员。本书的结构使得读者能很快解决实际问题。

关于Windows NT 4和基本网络理论已有许多好书。我不想重复它们的内容。本书假定读者知道NT 4的信任机制，并且曾是域用户管理员、服务器管理员、系统策略编辑员和事件检查员，而且有TCP/IP方面的知识，知道10BaseT的限制。

Windows 2000安全性的新特点

Windows 2000安全性（微软称之为“分布式安全性”），采用了许多新的特性以简化域管理，提高性能，并且集成基于公钥密码的Internet安全技术。本书详细地描述了这些新特点，限于篇幅不能在此一一列出。但有许多特点是特别重要的，例如：

- 集成了Windows 2000活动目录，为具有精细访问控制和管理授权的大型域提供了可伸缩的、灵活的账户管理。
- Kerberos 5鉴别协议是Internet安全的工业标准，Windows 2000用它作为网络鉴别的默认协议，为鉴别的互操作性提供了基础。
- 使用公钥证书的鉴别、基于安全套接层（SSL）3的安全通道，数据工业标准协议实现的在公共网络上保证数据完整性和保密性的加密接口（CryptoAPI）。

这些特点和其他特点都将在本书中详述。

本书的结构

第1章概要地介绍了后面将要详细描述的主题，以及在实现Windows 2000的安全性时经常会遇到的术语和缩写词。这一章的目的是提供本书的综述，使读者熟悉概念，知道哪些章节是读者特别感兴趣的。本书是用来解决问题的。第1章指出了问题从哪儿开始，该找些什么、以及在哪儿能找到。

第2章描述活动目录，活动目录定义了Windows 2000的网络结构，提供了实现结构化的手段，多级安全区域比微软以前实现的Windows提供了更好的粒度控制。这一章介绍了如何定制活动目录，如何配置存取控制设置，介绍了微软管理控制台（MMC）插件，它用于配置和管理Windows 2000，包括安全策略。第3章描述了组策略，以及将包含于组策略对象（GPO）中的设置方法应用于活动目录对象，如网站、域和组织单元（OU）等。这一章讨论了策略的继承性，域级策略如何在活动目录结构中的更低级执行和阻止，安全组过滤如何在不放弃全域策略控制的情况下，委托特定OU进行管理。

第4章介绍各种Windows 2000安全协议及其使用方法。这一章特别强调了Kerberos 5协议，它是Windows 2000的默认鉴别协议。这章描述了怎样通过使用共享秘密协议来完成相互鉴别，讨论了共享密钥、会话密钥、密钥分发中心、Kerberos票据、票据授权服务和跨域鉴别。这一章描述的原理和实际操作是整个Windows 2000安全概念的中心。第5章描述了对敏感数据id的非法访问问题和Windows 2000的解决方案，描述了加密文件系统（EFS）。通常情况下，对访问和编辑自己文件的用户来说，EFS是不可见的，而这些文件是其他任何用户都不可访问的。这有它自己的问题。如何使用恢复代理恢复加密文件也在讨论之列。

第6章和第7章是互相关联的。使用公钥、私钥和安全证书为敏感数据通过危险环境（如Internet）传输提供了强大的安全性。第6章讨论了Windows 2000公钥结构，利用SSL3协议建立安全的站点，使用数字签名和加密来保护敏感的电子邮件传输。第7章讨论了证书颁发机构（CA），包括微软证书服务和第三方CA如VeriSign和Thawte。这一章描述了如何建立CA，如何获得证书和如何建立证书吊销列表（CRL）。

第8和第9章着眼于解决在口令字保护不是最佳方案时的用户认证问题。第8章讨论了证书映射，该方法实现经由危险环境（如Internet）的基于证书的安全登录，它为在域中没有个人账户的合作方雇员或子公司提供了登录的鉴别方法。在第9章中讨论了智能卡，智能卡正变成一种可供选择的鉴别手段，特别对大的组织来说，他们已发现基于口令字的安全难于满足需要。

敏感数据在通过网络传输时是非常危险的。当浏览器使用SSL3加密时，它要求网络应用也支持SSL3。第10章讨论的Internet协议安全性（IPSec）提供了对用户透明的，能防止外部或内部恶意人员攻击的网络安全传输手段。第11章讨论了通过国外网络的通信（如Internet）、虚拟专用网的隧道技术，它为安全业务提供了合算的解决方案。第12章着眼于提供各种工具，这些工具用安全模板来配置本地安全、编辑安全参数、创建新模板和分析安全设置。

最后列出了一个术语表，解释了书中用到的技术术语。

怎样使用本书

从头到尾地阅读本书可以为读者打下有关Windows 2000安全性的极好基础。但是，读者也可以跳读，为完成当前的任务或碰到的问题找到例子和程序。本书是一个参考资料。读者可以根据自己的需要使用本书。

欢迎任何意见和建设性的批评。我的email地址是ianm@cableinet.co.uk。请在邮件中注明书名。

目　录

第1章 Windows 2000的安全特征

本章快速解决方案内容如下：

- 了解活动目录结构
- 集中式安全账户管理
- 使用可传递的双向信任
- 委托管理
- 运用访问控制表实现细粒度访问权限
- 使用安全性协议
- 使用安全支持提供者接口
- 使用Kerberos5鉴别协议
- 为Internet安全使用公钥证书
- 实现企业与企业之间的访问
- 提供企业解决方案
- 使用NTLM凭证
- 使用Kerberos凭证
- 使用私/公钥对和证书
- 使用Internet协议安全性
- 使用虚拟专用网络
- 使用安全配置工具
- 从NT4移植到Windows 2000

1.1 简介

Windows 2000的安全性很灵活并且可升级——从小的公司到跨国集团公司，通过广域网（WAN）（包括Internet）时，首先要考虑的问题是严格的安全性。然而，在Windows 2000中大多数新开发的应用主要是支持基于Internet的企业。在大型组织当中，其安全是通过使用分级的Windows 2000 活动目录（Active Directory）来实现的。其他改变是利用Windows安全结构的灵活性来统一使用Internet公钥证书的鉴别和智能卡（Smart Cards）的交互式登录。Windows 2000将易于使用、良好的管理工具和支持企业与Internet的一体化安全基础设施等优势集于一身。

1.1.1 Windows 2000的活动目录

Windows 2000的活动目录存储了所有的域安全策略和账户信息，为多域控制器（Domain Controller, DC）提供复制和可用的账户信息，以方便远程管理。Windows 2000支持对用户、组及计算机账户信息的分层命名空间。账户根据组织单元（Organizational Unit，OU）分组，而不

是根据Windows NT 4所提供的平面域账户名字空间来分组。

注意 在Windows NT4中，域名空间是由用户、全局组、本地组及计算机账户所组成。在Windows NT4的域名空间中不存在分层——所有的一切都是同一级别。然而，尽管全局组可以放入本地组中，但全局组和本地组不能嵌套。由于不存在更高的级别，所以一个全局组不能从另一高级别的全局组那里继承权限或许可。这被称为平面名字空间。相反，在Windows 2000中，名字空间是分层的。OU可以从更高级别的OU处继承安全策略，继承性可以被中止或执行。Windows 2000的分层名字空间将在本章后面讨论。第3章将详细讨论OU及组策略对象（GPO）。

创建及管理用户账户或组账户的权限可以委托给OU这一级。访问权限能够赋予用户对象的单独属性。例如，允许指定的个体或组拥有复位口令的权限，但却不能修改其他账户信息。活动目录复制允许更新任一DC上的账户信息，而在Windows NT4中，仅允许在主域控制器（Primary Domain Controller, PDC）中更新。在其他的DC中，活动目录的多主复制（Multiple master replication）是自动更新和同步的。

注意 Windows 2000的域中没有PDC——尽管在域中的某一DC承担起PDC仿真器的角色，但是所有的Windows 2000 DC都是平等的。在有Windows NT4 PDC的混合域中，Windows 2000的DC能起到一个相当于备份域控制器（Backup Domain Controller, BDC）的作用。这样就提供了从Windows NT4到Windows 2000的平稳过渡。

Windows 2000采用一种新的域模型，它使用活动目录支持多级分层域树。在整个域树中，通过使用双向传递信任（Kerberos信任）简化了域间信任关系的管理。Windows 2000的域树及Kerberos信任确保了Windows 2000的升级性。这将在第2章中讨论。

相关信息 1.2.3节“使用可传递的双向”信任，2.2.5节“灵活性”

1.1.2 分布式安全和安全协议

Windows安全性包括基于Internet标准安全协议的鉴别。为了保证向后兼容，虽然也支持Windows NT LAN Manger（NTLM），但Windows 2000的默认鉴别协议是Kerberos 5（在第4章中讨论）。基于安全套接层版本3（SSL3/TLS）的传输层安全（Transport Layer Security, TLS）协议通过将公钥证书形式存在的用户凭据映射到现存的Windows NT账户来支持客户鉴别，并提供增强的特征支持Windows 2000中的公钥协议。公钥的安全性和SSL3/TLS将在第6章中讨论。无论是使用共享秘密鉴别还是使用公钥安全性，用于账户信息及访问控制管理的仍是通用的管理工具。

除了口令字之外，Windows 2000还支持将可选的智能卡（Smart Cards）用于交互式登录。智能卡看起来像用于自动取款机（ATM）的银行磁卡，但它却比磁卡多存储数千倍的信息，它亦支持加密和对私钥和证书的安全存储，确保了可靠的分布式安全鉴别。

提示 有关智能卡的类型、外观及相关信息可在下面的地址中找到：www.gemplus.com/basics/what.htm和www.gemplus.com/basics/terms.htm。

在网络级，Windows 2000使用Internet 安全协议（IPSec），IPSec将在第10章中讨论。在第11章中将讨论在广域网（包括Internet）上用于远程访问的虚拟专用网（VPN）。那些用于在VPN上实现隧道的协议，如点到点协议（PPP）、点到点隧道协议（PPTP）及第二层隧道协议（L2TP）等将在第10章中讨论。

在全书中到处都将讨论协议，而在本章的介绍中，仅列出了最为重要的部分。在RFC文档中包含了协议规范。例如，如果想找到更多有关域名系统安全扩充（RFC 2535）或安全关联和密钥管理协议（RFC 2408）的详细信息，可分别在以下地址中找到：ftp://ftp.isi.edu/innotes/rfc2535.txt和ftp://ftp.isi.edu/in-notes/rfc2408.txt。

提示 以数字为序的RFC列表可在地址http://ercole.di.unito.it/CIE/RFC/rfc-ind.htm找到。

相关信息 4.2.1节“建立共享秘密协议”，“应用Windows 2000公钥的安全性”，9.2.2节“安装智能卡注册站”

1.1.3 配置智能卡

Microsoft的证书服务器允许组织机构向他们的雇员及商务伙伴发布X.509版本3的证书。这包括为证书管理引入密码应用编程接口（CAPI）。组织机构可使用由商业证书颁发机构（CA）、第三方CA或是Microsoft证书服务器发布的公钥证书。系统管理员可以定义在他们的环境中哪些CA是可以信赖的，从而决定在客户鉴别和资源访问时哪些证书是可以接受的。

使用公钥证书并映射到现存的Windows账户能够对那些没有Windows 2000账户的外部用户进行鉴别。由Windows账户所定义的访问权限决定了外部用户能够在该系统中使用的资源。使用公钥证书的客户鉴别允许Windows 2000根据可信CA所发布的证书对外部用户进行鉴别。

Windows 2000用户有适当的工具和共用接口会话框，以便管理私／公钥对和证书，用户使用证书访问基于Internet的资源。存储的个人安全凭据（使用安全的、基于磁盘的存储方式）易于用工业标准协议Personal Information Exchange（PIE）传输。Windows 2000已集成了支持智能卡的设备。

相关信息 7.2.1节“建立证书颁发机构”，7.2.3节“安装CA证书”

1.1.4 加密

Windows 2000操作系统采用了好几种加密方法，其目的是通过使用数字签名提供鉴别过的数据流。除了签名过的ActiveX控件和用于Internet Explorer的Java类以外，Windows 2000使用数字签名保证各种程序组件的图形完整性。内部开发人员亦能为发布和防范病毒创建签名的软件。

第三方供应商可以在Windows 2000服务器上使用动态口令鉴别服务并把动态口令与Windows 2000域鉴别结合起来。应用程序接口（API）和支持第三方产品的文档可在Microsoft软件开发平台工具包（SDK）中得到。

相关信息 5.2.2节“文件或文件夹加密”6.2.4节“在IE中使用基于公钥的验证”

1.1.5 IP安全

商业领域广泛使用Internet、Intranet、分支机构及远程访问。网络不断传递敏感信息。管理人员和其他网络专业人员的任务是必须确保数据的完整性、保密性和可鉴别性。数据必须免受以下破坏：

- 在传输过程中被修改。
- 被截取、阅读或复制。
- 被未经授权的人访问。

为满足这些要求，Windows 2000服务器操作系统使用了IP安全协议（IPSec），它是由Internet工程任务组（IETF）制定的。IPSec位于传输层之下，因此它的安全服务对应用是透明的。Microsoft Windows IP安全采用工业标准加密算法及综合安全管理方式，为一个组织的防火墙两端的所有TCP/IP通信提供安全，从而实现了Windows 2000服务器端到端的安全策略，以抵御外部和内部的攻击。IPSec将在第10章中详细讨论。

1.1.6 虚拟专用网

虚拟专用网（VPN）允许用户以隧道方式通过Internet或其他的公共网络，同时保持与专用网相同的安全级别。从用户的角度来说，VPN好像是公司服务器间的点到点连接。VPN必须允许漫游或远程客户能连接到资源，并安全地进行鉴别。用户的个人地址、名字及口令必须保密，数据必须加密。必须产生和更新客户与服务器双方的加密密钥，且必须支持公共网络所用的公共协议。

警告 世界上没有什么是永久安全的，加密密钥亦不例外。因此，它们都有一个有效期，需要定期地更新。如同备用的数据通路，在密钥更新期应当谨慎从事。如果未经授权用户截取了更新的密钥，那么，安全性就不复存在。

Windows 2000目前支持基于PPTP的VPN解决方案，并支持最近开发的L2TP。IPSec也支持VPN，但通常并不能满足所有的要求。VPN将在第11章讨论。

1.1.7 安全配置和分析工具

Windows 2000提供了安全模板、安全配置与分析插件，以及secedit命令行实用程序，利用它们可以配置和分析基于一系列标准模板的安全设置，可以加载、组合、编辑这些标准模板来配置本地的安全。运用这些工具，可将安全设置与默认值比较以分析安全设置，并可输出定制的安全模板，该模板是为在网络中使用的其他计算机而创建的。也允许在本地机器上配置安全，或者修改特定的机器类型模板，使它适用于网络中同类型的机器（如工作站、成员服务器等）。

尽管Windows NT4提供了许多图形化的工具，它们都能单独用于对系统安全的各个方面进行配置，但这些工具不是集中化的，管理者可能需要打开三个甚至四个应用程序才能为一台计算机配置安全。安全配置可能十分复杂，由于在Windows 2000中增加了分布式的安全特征，更增加了配置的复杂性。

安全性配置工具的设计就是为了满足集中式安全配置的需要，并提供企业级的安全性分析。

1.2 快速解决方案

1.2.1 了解活动目录结构

Windows 2000的安全性将活动目录作为账户信息的存储库。在性能及灵活性方面，活动目录比NT基于注册的实现有了显著的改进，并且提供了富有特色的管理环境。

在Windows NT4中，域账户保持在没有内部组织的同级别的名字空间中。然而，在Windows 2000中，用户、组及机器的账户被组织到叫做组织单元（OU）的目录容器中。域可以具有以树形结构名字空间组织的任意多个OU。企业可以按名字空间来组织其账户信息，以代表该公司的各部门及机构。像OU一样，用户账户也是目录对象，当组织改变时，目录对象能轻易地在该域树内重新命名。

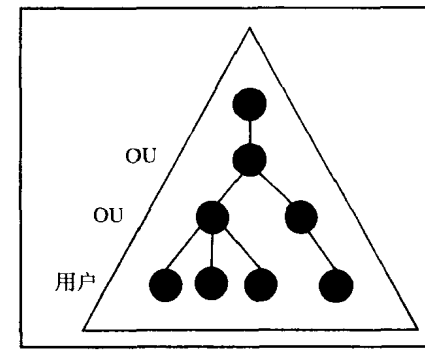


图1-1 Windows 2000分层的域名空间

由于活动目录是一种分层的结构，Windows 2000的域名空间通常以三角形的形式来说明，如图1-1所示。

Windows 2000的多域模型也是分层结构，而Windows NT的主控域模型仅有两级的层次结构。由于在Windows 2000中使用可传递双向Kerberos信任（将在1.2.3节描述），在Windows 2000中实现安全信任模型更容易。图1-2显示了典型的Windows 2000多域结构。

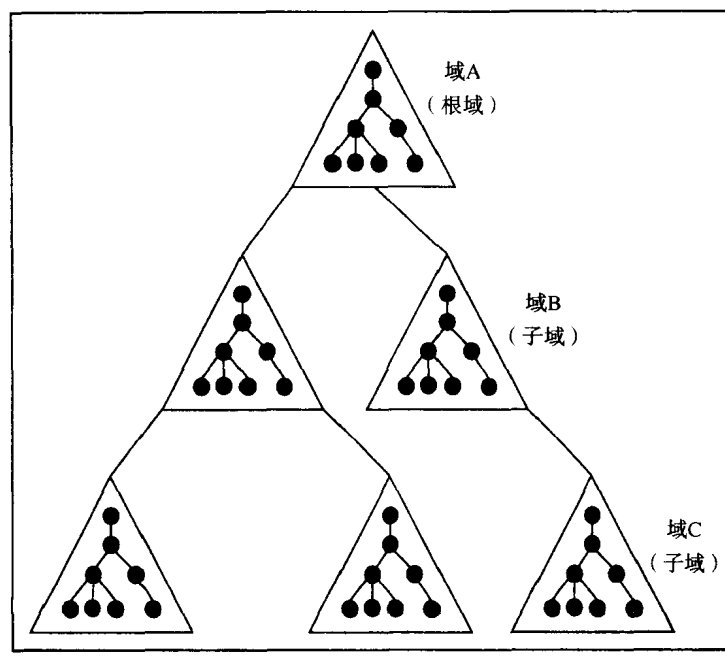


图1-2 多域模型

1.2.2 集中式安全账户管理

Windows 2000的安全模型提供了基于组成员资格的、对所有域资源实行统一的、一致性的访问控制。Windows 2000的安全组件能够信任存储于目录中的与安全相关的信息。例如，Windows 2000鉴别服务将经加密的口令信息存储在用户对象目录中的安全部分，操作系统保证安全策略信息已得到安全存储，且任何未经授权访问的人不能改变对账户的限制或组成员间的关系。此外，对全域管理的安全策略信息也保存在活动目录中。

在活动目录中存储安全账户信息意味着把用户和组当作目录中的对象。对目录中对象的读写访问可作为一个整体，或是作为单独的属性授与对象。管理员能够更好地控制谁可以更新用户或组信息。具体访问权限的界定将在本章的后面详细描述（关于怎样使用组策略 MMC去创建和编辑GPO，在第3章中给出了一个分步的指南）。

活动目录存储了域安全策略信息，诸如域范围口令限制和系统访问特权。Windows 2000对所有位于活动目录中的对象实现了基于对象的安全模型和访问控制。在活动目录中的每一个对象有一个唯一的安全描述符，该描述符定义了读或更新对象属性时所要求的访问权限。活动目录使用模仿和Windows 2000访问验证来决定活动目录客户是否能够读或更新预定的对象。这就意味着轻量目录访问协议（LDAP）的客户对目录的请求要求操作系统实施访问控制，而不是让活动目录本身作出访问控制的决定。

将安全账户管理与活动目录结合起来有以下优点：

- 活动目录支持的用户对象数量非常大（多于一百万），并且比注册服务有更好的性能。单域的大小不再受安全账户的存储库性能的限制。互连的域树能支持大型的、复杂的组织结构。
- 通过采用对活动目录进行管理的先进图形工具和脚本语言的对象连接及嵌入目录服务（OLE DS）支持，加强了对账户信息的管理。对通常的任务可通过批处理脚本实现自动管理。
- 目录复制服务支持对账户信息的多份复制，并且在任意DC上都可对副本进行更新。LDAP和目录同步（directory synchronization）支持提供了把Windows目录与企业中其他的目录链接在一起的机制。

1.2.3 使用可传递的双向信任

在Windows 2000的分级域树中，域与域之间的信任关系允许在某一个域中定义了账户的用户用另一个域中的资源服务器对它进行鉴别。

在Windows NT4和更早的版本中，域间的信任关系是由域间的单向可信域账户所定义的。在大型网络中，域账户与域资源域之间的信任关系的管理是一项复杂的任务。如果需要，活动目录支持典型的NT4类型的信任，以提供与NT4域的兼容性，并且允许在Windows 2000域之间建立起单向信任关系。

然而，活动目录也支持Windows 2000域树中域与域之间的双向可传递信任关系（Kerberos信任）。在可传递的信任中，如果域A相信域B，而域B又相信域C，那么域A就相信域C。

图1-3所示为Windows 2000中完全信任的域模型，并与Windows NT4中同样的模型进行比较。在Windows NT4模型中要求建立和维护12种信任关系，而在Windows 2000中仅需要3种关系。

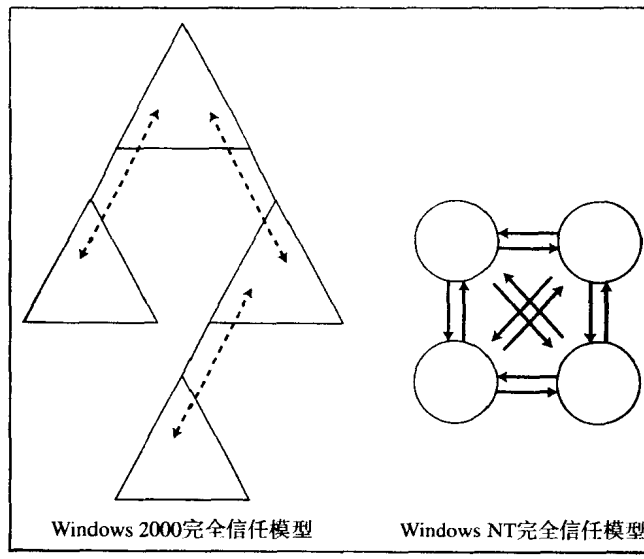


图1-3 两种信任模型的比较

域与域之间的可传递信任关系简化了对域间信任账户的管理。域树中的成员域与它的父域定义了双向信任关系。所有的域都暗含了对域中的其他域的信任。如特定域不想建立双向信任关系，可以定义成明确的单向信任关系。创建的子域将自动地与其父域建立Kerberos信任关系。下面的过程中假定有一个由DC和一个或多个成员服务器支持的域（这个DC将成为根）。

要将一个成员服务器提升为子域的DC，步骤如下：

1) 在成员服务器上选择“开始/运行”，并键入“dcpromo”。

2) 当出现提示时，选择“子域”选项。

3) 指定父域名，以及所在域中管理级账户的账户名和口令。

警告 区分根域与父域是重要的。例如，在图1-2中，域A是根域，同时也是域B的父域。然而，域C的父域是域B，而不是根域。

1.2.4 委托管理

管理权限可以通过委托把安全管理限制到整个组织域的确定子集。委托是授权管理责任范围内的用户或组的小集合，但没有权限管理该组织内其他部分的账户。

创建新用户或新组的责任委托确定在OU级或者在创建该账户的地方。某一OU的组管理员不必为该域内其他OU创建和管理账户。然而，在该目录树中更高级别处所定义的域内策略设定和访问权限通过继承访问权限可应用于整个树。

以下为三种委托管理责任的方式：

- 委托权限以改变该域对象本身的特定容器（如本地策略）的属性。
- 委托权限以创建和删除OU下某特定类型的子对象，如用户、组或打印机等。
- 委托权限以更新OU下某特定类型子对象的特定属性，如用户对象口令设置权。