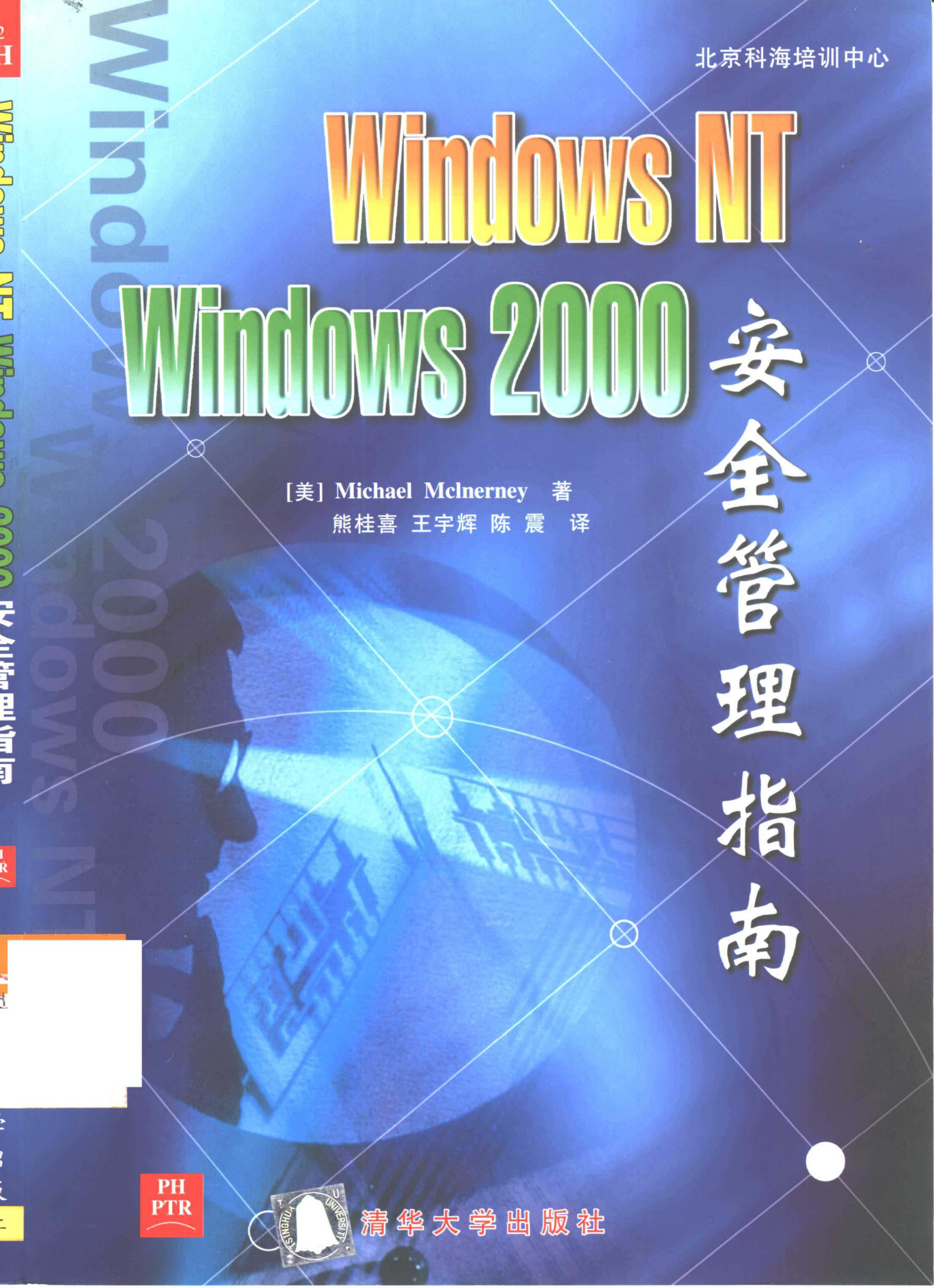
北京科海培训中心

Windows NT Windows 2000 安全管理指南

[美] Michael Mclnerney 著
熊桂喜 王宇辉 陈 震 译



PH PTR
清华大学出版社

PTR 北京科海培训中心

Windows NT Windows 2000 安全管理指南

[美] Michael McInerney 著

熊桂喜 王宇辉 陈 震 译

清华大学出版社

(京)新登字 158 号

北京市版权局著作权合同登记号:01-1999-3355

内 容 提 要

本书是介绍 Windows NT 及 Windows 2000 安全管理策略和方法的专著,适用于在网络环境下拥有 Windows NT 及 Windows 2000,或准备将 NT 升级至 2000 的用户和读者。

本书首先介绍了网络安全的一般概念(第 1,2 章),然后介绍了在 NT 下配置和管理各类安全策略的组件和方法(第 3,4,5 章)。在介绍了密码学的基本知识(第 6 章)后,介绍了 Proxy Server 的配置方法(第 7 章)。然后,介绍了注册表(Registry)及 NT 审计策略的实现(第 8,9 章)。从第 10 章开始,介绍 Windows 2000 下主要安全工具的特点及配置方法(第 11～16 章)。其中,有些工具在 NT 下初步实现了,但不完整。

网络安全是一个有一定难度的主题,但本书内容安排条理清晰,通俗易懂,适合于具有一定使用和管理 Windows 网络经验的中级读者。

图书在版编目(CIP)数据

Windows NT、Windows 2000 安全管理指南/(美)麦克勒尼(McInerney,M.)著;熊桂喜译.—北京:清华大学出版社,2001

ISBN 7-302-04240-3

I. W… II. ①麦…②熊… III. 服务器—操作系统(软件),Windows NT、Windows 2000 IV. TP316.96

中国版本图书馆 CIP 数据核字(2000)第 88466 号

出版者:清华大学出版社(北京清华大学校内,邮编 100084)

网 址:http://www.tup.tsinghua.edu.cn

印刷者:北京门头沟胶印厂

发 行:新华书店总店北京科技发行所

开 本:787×1092 1/16 印张:19.375 字数:471 千字

版 次:2001 年 1 月第 1 版 2001 年 2 月第 2 次印刷

印 数:5001～10000

书 号:ISBN 7-302-04240-3/TP.2493

定 价:30.00 元

致　谢

编写一本这样的安全专题书是一件十分困难的工作，写完本书所付出的艰辛是我过去未曾碰到的。我想编写任何其他专题书籍的作者也会有类似的经历。如果没有很多人向我提供不同形式的帮助，这项工程是很难完成的。

首先也是最重要的，我要感谢我的妻子 Linda，她的热情支持和鼓励，以及在需要时的正确引导，一直是我工作的动力来源。在我写作和出版期间，她花了大量的时间来帮助我录入和编辑，我写的内容在她的努力下变得更有条理。如果没有她的帮助和支持，本书将很难完成。

Vincent Daly 和 Thomas Niestroj 是我在 IBM 的同事，也是我应该重点感谢的朋友。我非常感激他们在审定技术内容上所花的精力。我还要多谢 Curt Aubley——《Tuning and Sizing NT Server》的作者（该书已由 Prentice Hall 出版），它为本书的内容和结构安排提供了极有价值的建议。

接下来我要感谢 Jane Heffernan。Jane 总是毫无保留地发表她的意见，而且总是充满新意。有这样的好朋友是我的荣幸。

我要感谢 Prentice Hall 的各位工作人员。首先感谢 Mary Franz，她给了我写这本书的机会，并提供了我所要求的全部支持。对其他为本书付出了劳动的工作人员，我同样深表谢意。有了这些专业人员的帮助，我的工作变得轻松一些，也少走了不少弯路。

最后，我对这里未曾提到的其他人员表示歉意，我非常感谢你们对我的帮助和支持。

作者简介

写作对于我来说并不是第一次。尽管这是我出版的第一本书，但我估计已写过成千上万页的资料。本书不过是各种技术手册和杂志论文的综合结果汇集。

作为 Insight Business Solutions 公司的创始人和技术指导，我的主要业务和擅长之处在于计算机安全、网络设计和技术培训。我公司的主要商业目标是提供高水平的、有特色的专业支持，而我的客户是来自欧洲和美国的公司。在我的客户中，有很多是来自不同国家的银行、基金会和工厂。

就我个人而言，我是一个获得了 Microsoft Certified Systems Engineer（MCSE，微软认证系统工程师）和 Master Certified Novell Engineer（MCNE，Novell 认证高级工程师）证书的专业工程师。我在计算机及网络行业中工作了 12 年。在过去几年中，我曾做过许多技术讲授工作，也做过 Microsoft 和 Novell 的技术咨询。我最近几年的培训活动主要集中于各种研讨会，我的注意力集中于系统安全。

前　言

系统安全是一个很难写好的主题。准确地说明什么是安全的，什么是不安全的，是一个非常主观的过程，并且与很多因素相关。衡量安全的因素包括：你的单位今天的某些需求、假设、未来环境应关心的内容，还有你所处系统的重要程度等。

当然，对我来说，根据我的考虑来教你如何使你的系统更安全是很容易的。但是，如果不结合你所处的具体环境和具体需求，这样的安全措施是无用的。

在本书中，我以两种方式来介绍安全主题。首先，我尝试说明，为什么你要考虑实现某一特定的安全特性或过程。其中我还给出了你和同事们在设计安全模型时必须要考虑和讨论的一些内容。接着，我会给出一步步的指导，说明如何真正地实现安全性。你可按照这些操作步骤来实现所需的安全特性，判断哪些特性正好适用于你的单位，并按照需要采纳我所给出的例子。

本书的读者对象

本书的读者对象为系统管理员和网络管理员、安全专家、系统审计专业人员、系统协调员、开发人员，以及任何希望了解 Windows NT 和 Windows 2000 安全特性的技术人员。

如今人们都十分关心他们数据的安全性，这意味着进行各种管理工作时应更加注重于数据和系统的安全特性。不幸的是，如果只是将这些关注和努力转变为加大投资来购买额外的工具，花钱聘请咨询专家来设计你的安全模型，并帮助你实现系统安全，则是远远不够的。设计、实现并维护安全模型的责任责无旁贷地落在了系统管理员以及那些过去曾关心过，而现在则必须面对挑战的专业人员肩上。

本书所介绍的内容要求读者具备很好的 Windows NT 系统管理知识，如果你准备部署 Windows 2000，则还应具备 Windows 2000 知识。我在书中讨论的许多功能和特性都将集中于系统注册表上，而注册表(Registry)既是各种信息的来源地，也是你应努力改善系统安全性的目标。基于这一原因，我将本书的读者水平定位为中高级。读者在尝试进行各种练习之前，必须习惯于使用注册表编辑工具来查看和修改注册表的设置值。

本书的内容安排

全书共分 3 个部分。

第 1 部分“系统安全概述”，介绍了安全概念以及这些概念在 Windows NT 安全结构中是如何体现的。本部分内容对所有读者来说，都应该是一个好的开端，因为它给出了了解安全这一主题的背景知识。具备了安全知识的专业人员，也可以将本部分内容与自己的思考作一个比较。

第 2 部分“Windows NT 4.0 安全性组件”，讨论了与 Windows NT 4.0 安全性有关的组

件。本书的这一部分讨论了 Windows NT 所有内置的安全特性，以及如何让它们更好地满足你的站点的安全需求。这一部分还介绍了适用于商业环境的各种灵活特性。

第 3 部分“Windows 2000 安全特性介绍”，介绍了 Windows 2000 的特性，以及 Windows NT 4.0 和 Windows 2000 在安全模型方面的差别。这一部分首先介绍了 Active Directory（活动目录），然后转入新的操作系统中所包含的与安全有关的内容。加密文件系统、分布式文件系统以及围绕着 Active Directory 技术的安全性，安全性配置工具及组策略，都在这一部分中进行了讨论。

每一章都各自独立为一个单元，每一章都可单独阅读。由于采取了这种编写方式，所以熟练的 NT 专业人员可以将本书作为一本参考手册来翻阅，并可直接跳至你所关心的主题。但是，本书的主旨仍然是帮助读者构造你自己单位的安全模型。读者读完全书后，就可以利用本书所介绍的概念和讨论的方法来定义自己的安全模型。我认为以这种方式来组织内容，能为读者提供更方便的阅读途径。

目　录

第 1 部分　系统安全概述

第 2 部分 Windows NT 4.0 安全性组件

第 3 部分　Windows 2000 安全特性介绍