NETWORK PROFESSIONAL'S LIBRARY

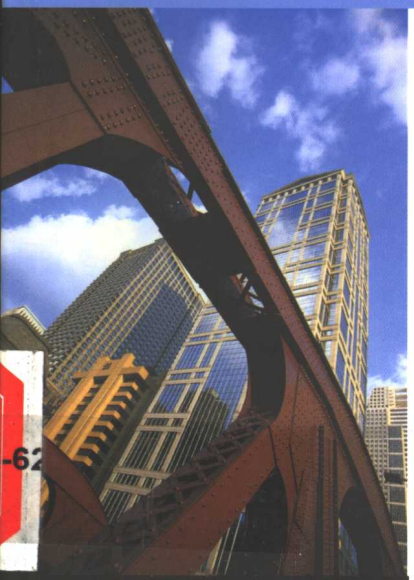
Mc Graw Hill Education

《Windows 2000安全手册》一书提供了关于Windows 2000最新安全特性的综合专业信息。如果正在使用Windows 2000，那么需要阅读这本书。

—— Eric Schultze
Microsoft安全项目经理

WINDOWS 2000 安全手册

[美] Philip Cox
Tom Sheldon 著
天宏工作室 译



- 部署和管理可靠的Windows 2000安全策略
- 使用IPSec保护企业内部网、外部网和Internet事务
- 防御黑客攻击、欺诈攻击、嗅探攻击和DDoS攻击
- 使用防火墙、代理服务器和VPN保护网络

OSBORNE
计算机专业技术丛书

Mc Graw Hill

清华大学出版社

Osborne 计算机专业技术丛书

Windows 2000 安全手册

[美] Philip Cox
Tom Sheldon 著

天宏工作室 译

清华大学出版社
北京

Windows 2000 安全手册
Philip Cox/Tom Sheldon：**Windows 2000 Security Handbook**
EISBN：0-07-212433-4

图书在版编目（CIP）数据

Windows 2000 安全手册/（美）考克斯，（美）谢尔登著；天宏工作室译. —北京：清华大学出版社，2003
（Osborne 计算机专业技术丛书）
书名原文：Windows 2000 Security Handbook
ISBN 7-302-06274-9

Ⅰ. W…　Ⅱ. ①考… ②谢… ③天…　Ⅲ. ①服务器－操作系统（软件），Windows 2000－技术手册 ②计算机网络－安全技术－技术手册　Ⅳ. TP316.86-62

中国版本图书馆 CIP 数据核字（2003）第 005105 号

出 版 者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.tsinghua.edu.cn
责任编辑：付宇光
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　**印张**：44.25　**插页**：4　**字数**：902 千字
版　　次：2003 年 3 月第 1 版　2003 年 3 月第 1 次印刷
书　　号：ISBN 7-302-06274-9/TP・3747
印　　数：0001～4000
定　　价：82.00 元

出版说明

随着计算机技术的深入发展及最新网络操作系统的问世，越来越多的企业和个人逐渐将自己的注意力和兴趣转移到了网络技术上。有关网络的软硬件配置、网络协议、网络安全、网络数据库、网络应用程序开发（特别是Web应用程序开发）等方面的主题备受关注。计算机专业人士和广大计算机爱好者迫切需要一套可以从中汲取网络专业知识的权威书籍。为此，我社选择了美国Osborne/McGraw-Hill出版的Network Professional's Library、Professional Developer's Library和Database Professional's Library等专业性较强的图书，组织成这套Osborne计算机专业技术丛书。我们真诚地希望将这一套丛书作为信息时代的礼物奉献给广大读者。

本套丛书的特点是注重理论方法和实际应用的相互结合。在理论上，讲究技术的新颖和原理的深入；在应用上，讲究方法的直观性和广泛适用性。通过认真学习，读者可以充分地将自己已有的知识融入新技术的学习和掌握中，从更深的层次上理解目前不断出现的新概念、新技术，并且很容易在较短的时间内获得丰硕的学习成果，所有这一切都源于这些图书科学的编排结构、清晰的文字表达和富有代表性的应用示例。目前，计划出版和已出版的一系列图书已经获得广大读者的热切关注和强烈反响，我们坚信我社一贯奉行的打造精品图书的理念会为读者带来巨大的收益。

麦格劳-希尔教育出版集团拥有世界知名的计算机图书出版品牌——Osborne/McGraw-Hill，这是美国出版IT图书的独树一帜的力量。Osborne/McGraw-Hill具有针对普通用户和专业人士的多种图书系列，立足于编程（Programming）、联网（Networking）、数据库（Database）、认证（Certification）以及大众（Consumer）图书五大方向，每年出版图书250余种。由于与Oracle、Cisco、Corel、Global Knowledge和J.D. Edwards等国际著名企业建立了长期战略合作出版关系，Osborne一直拥有最前沿的IT技术图书。相对于其他计算机图书而言，Osborne的系列化图书产品和专业化IT技术参考书目更具特色。这些图书全部由富有技术经验和才华的计算机开发人员编写，将为第一线的专业人士提供最新、最准确和最富于创造性的计算机知识、理论及开发应用的经验。

天宏工作室负责本套丛书的翻译工作，在此感谢他们为此付出的辛勤劳动。

作者简介

Philip Cox

Philip Cox 是 SystemExperts 公司（一家专门处理系统安全和管理的咨询公司）的顾问。他是系统安全（特别是保证 Windows 和 Windows-UNIX 混合环境的安全）领域的知名权威。Philip 的日常职责包括进行全面的安全和结构审查、渗透测试以及为世界各地的多家最大规模的电子商务公司设计企业级入侵侦测系统。

除了作为本书的主要作者和 USENIX 协会的杂志《;login:》的特色专栏作家之外，他还担任《SANS NT Digest》的编委。Philip 还是全球关于 UNIX 和 Windows 安全问题的主要会议（如 USENIX、SANS、NetWorld-Interop 以及 The Information Security Conference）的最有声望和最知名的发言人。

Philip 拥有计算机科学硕士学位，目前是 Microsoft 认证系统工程师（MCSE）。您可以通过以下地址与他联系：Phil.Cox@SystemExperts.com。

Tom Sheldon

Tom Sheldon 在计算机行业并不是一个陌生的名字。自 20 世纪 70 年代起，他就是一位计算机程序员、顾问和网络管理员。自从人们发明以太网以来，他就一直在设计和建立网络。Tom 已编写过 30 本书，他的文章发表在《PC World Magazine》、《PC Magazine》、《Byte Magazines》、《Windows NT Magazine》以及《Windows Pro Magazine》上。他的最新著作是《McGraw-Hill Encyclopedia of Networking》，现在已经是第三版。

Tom 还负责一个计算机和软件测试实验室，为 Microsoft、Novell 以及其他公司做研究。他指导过许多主要网络的安装，包括 Lockheed Space Operations 站点和西海岸的多个政府和教育组织的站点。

成千上万的计算机用户通过观看 Tom 的最畅销教育录像带学习计算机和 Windows，从而熟悉了 Tom。

他居住在加利福尼亚 Big Sur 海岸，喜欢骑自行车登山、乘小艇出海钓鱼和打高尔夫球。

合著者简介

Dallas Bishoff

Dallas Bishoff 具有 10 多年在联邦政府部门和私营企业作为信息安全顾问的经验。他是认证的信息系统安全专家（Certified Information Systems Security Protessional，

CISSP)、Microsoft 认证因特网系统工程师（MCSE + I)、Microsoft 认证培训师（Microsoft Certified Trainer, MCT)、Citrix 认证管理员（Citrix Certifiecl Administrator, CCA)、Internet 安全系统认证工程师（Internet Security Systems Certified Engineer, ICE)、Check Point 认证安全工程师（Check Point Certified Security Engineer, CCSE)、Nokia 安全管理员（Nokia Security Administrator, NSA）和教师（Instructor）以及 RSA 认证讲师（RSA Certified Instructor）和 SecurID 支持工程师（SecurID Support Engineer)。他还完成了美国国家安全局的 INFOSEC 评估方法（INFOSEC Assessment Methodology,IAM)课程，该方法用来审核联邦信息系统。您可以通过以下地址与他联系：Dallas _ Bishoff@Hotmail.com。

David Bork

David Bork 是 SystemExperts 公司的顾问。他是一位非常出色的安全专家，在入侵侦测、密码学以及在 Sun Solaris、IBM 的 AIX、Cisco 路由器和 Windows NT 上的安全代码开发等领域具有丰富的经验。David 为 IBM 和 AT&T 做了一些网络安全方面的工作，对他们目前使用的入侵侦测系统进行结构设计、编程、维护和提供支持。

在 David 的众多项目中，他帮助编写了 AT&T 的现行 PKI 解决方案的 AT&T CP 和 CPS，并设计了保护 CA 的分层安全基础设施。David 为悉尼奥运会和长野冬奥会提供安全分析和支持。在 IBM 与 AT&T 的网络业务合并之后，David 使用 Cisco PIX 防火墙对双方各自的客户网络进行了设计、集成和实施。David 参与了 Microsoft 公司的 Windows 和 Windows NT 的 beta 版测试。在从事入侵侦测工作之前，David 领导过与许多数据库有关的项目，并开发了网络管理系统的实时接口，以便存储网络状态并自动恢复网络。

Paul B. Hill

Paul B. Hill 是一位高级程序分析员，他是 MIT 的 Kerberos 开发小组的领导人之一，他不但自 1992 年起就一直参与 Kerberos 的开发，还参与了 MIT 的 Windows 2000 开发项目。Paul 也是系统安全方面的顾问。

David Mackey

David Mackey 现在是科罗拉多州 Boulder 的一家《财富》500 强公司的项目经理。在空闲时间，他是一位系统顾问、Web 站点管理员和作家。他的最新著作包括 Que 公司出版的《Special Edition Using Windows 2000 Server》（他对该书做出贡献)、Jamsa Press 出版的《1001 Windows 2000 Professional Tips》（与他人合著)。David 还与他人共同创立了著名的 Windows Troubleshooting 站点 http://www.FixWindows.com，提供免费的故障诊断信息，为疲惫不堪的 Windows 用户提供帮助。他在教育方面的追

求使他获得了科罗拉多州 Boulder 大学的俄罗斯研究中心（Russian Studies）的文学学士学位、Microsoft 认证系统工程师证书以及 Novell 授权网络管理员（Certified Novell Administrator）证书。在消遣时间，David 喜欢弹吉他或与妻子 Andrea 和儿子 Nathan 一起度过时光。

Ken Sandlin

Ken Sandlin 是计算机安全公司 Bluekey.net，Inc. 的总裁和共同创办人。他是一位 Microsoft 认证系统工程师（MCSE）、Microsoft 认证培训师（MCT）、Check Point 认证安全工程师（CCSE）、RSA 认证的 SecurID 支持工程师（Certified SecurID Suppot Engineer，CSSE），并通过了 RealSecure、SAFESuite Decisions、Internet Scanner、System Scanner 和 Database Scanner 方面的 Internet 安全系统认证，他还是 Citrix 认证管理员（CCA）、Citrix 认证教师（Citrix Certified Instractor，CCI）、FBI InfraGard 计算机安全程序的纽约市分会会员以及国家讲演者协会（www.nsaspeaker.com）的专家成员（Protussional Member of the National Speakers Association）。他是华盛顿特区的州政府和联邦航空管理部门的联邦政府承包商，他的项目小组获得了 FAA 的杰出小组奖（Team Excellence Award）。他目前正致力于 Internet 上的 126 个公共 A 类网络之一的 Windows 2000 公钥基础设施（Public Key Infrastructure，PKI）的保护工作。您可以通过以下地址与他联系：ksandlin@bluekey.net。

技术评论员简介

Eric Schultze

在过去 9 年里，Eric Schultze 一直从事信息技术和安全方面的工作，他的大多数时间都致力于评估和保护 Microsoft 技术和平台。他经常在安全会议（包括 NetWorld Interop、USENIX、BlackHat、SANS 和 MIS）上发言，他还是 Computer Security Institute 的资质教师。Schultze 先生还出现在电视和许多公共媒体中，包括 NBC、CNBC、《TIME》、《ComputerWorld》和《The Standard》。Schultze 先生的主要工作经历包括在 Foundstone，Inc.、SecurityFocus.com、Ernst & Young、Price Waterhouse、Bealls Inc. 以及 Salomon Brothers 等公司任职。他是《Hacking Exposed》第一版的合著者，他目前是 Microsoft 公司的安全程序经理。

致谢

感谢 SystemExperts 公司的 Jon Gossels 给我时间和信心完成这项工作，感谢 Brad Johnson 督促我做得更完美。感谢 SystemExperts 公司的其他成员：Dick Mackey、Mark Mellis、Cheng Tang 和 Jason Reed，感谢你们更正我在写作时犯下的错误。衷心感谢 Jane Brownlow，她尽了最大努力让我保持奋进的心态，衷心感谢 Tara Davis、LeeAnn Pickrell、Ross Doll、产品部全体努力工作的同事以及 Osborne 的所有员工。感谢 Eric Schultze 表现出的专业知识以及为保持内容中肯所提供的巨大帮助。

——Phil

感谢 Phil！你的专业知识、辛勤工作以及所花费的时间使得本书第二版的完成成为现实。

——Tom

简介

本书介绍 Microsoft Windows 2000 计算机的安全性，包括独立的台式机以及联网的工作站和服务器。这里提供的信息可以促使你采取行动保护自己的系统，还将向你展示如何使防范成为一个整体。

偏执是一件好事情。你越偏执，就越有可能保护自己的系统不受攻击。阅读本书并仅仅关注安全性是一个好的开始。事实上，你需要在开始规划和管理网络时将安全作为头等大事。许多网络管理员都太关注于获得很高的性能或其他目标，而使他们的系统为攻击敞开了大门。如果一些未知用户随时都可以关闭系统，从而拒绝合法用户的访问，那么最快的服务器或网络又有什么用呢？

随着网络变成计算机（例如 Microsoft 新开发的 .NET），对安全的需求将显著增加。过去几年里，因为企业感受到连接 Internet 的需要，所以安全已经越来越成为主要的考虑事项。由于总体上网络使用（特别是 Internet 的使用）的增加，需要努力做好安全方面的工作。

所有人都知道安全威胁来自 Internet 或源于内部。内部人员会造成严重的威胁已是人所共知的事实。首先，内部用户对系统和重要数据的存储位置了解得更清楚。其次，由于实施了不适当的防范措施，因此内部用户更倾向于窃取其他用户的账号或访问某些系统。你可能信任许多同事，但在一个开放的 Internet 网络环境中，需要重新考虑希望提供的信任程度。另外，由于网络的快速扩张以及许多网络间的协作，内部用户与外部用户之间的界限开始变得模糊，不再像以前那样清晰。

本书的内容

本书主要介绍如何加强 Windows 2000 系统和网络的安全性，以便防止恶意用户攻击系统和重要数据。本书包含以下六部分：

- **第一部分：安全的基础知识** 提供对网络（特别与 Internet 连接的网络）的安全问题的总体描述。你将学习关于黑客和解密高手的攻击的可怕真相以及避免遭受这种攻击的方法。你还将学习管理安全策略的重要性。
- **第二部分：Windows 2000 安全性** 提供了 Windows 2000 安全性的更详细信息。你将学习 Windows 2000 中的安全特性以及 Windows 2000 提供的联网服务。我们将介绍特定的 Windows 2000 风险及其解决办法。
- **第三部分：保护 Windows 2000** 介绍 Active Directory 中的安全特性，还将讨论使用组策略以及用户管理和组管理。这部分的最后一章介绍了登录身

份验证、文件系统、资源共享以及审核。

- **第四分：保护 Windows 2000 网络** 介绍企业内联网、Internet 和 TCP/IP 特有的安全威胁和相应措施。还将了解到如何在网络与 Internet（或自己的内部网络）之间建立防火墙，如何在 Internet 上安全而保密地开展业务，以及如何使用 Microsoft Proxy Server 保护网络。这部分将讨论虚拟专用网络（Virtual Private Network，VPN）和远程访问问题。还将介绍企业环境中的安全性以及保护客户的特殊考虑。
- **第五部分：其他问题** 介绍正确安装和保护 Microsoft Internet 信息服务器（Internet Information Server，IIS）5.0 以及 Windows 2000 为容错和数据保护提供的工具及技术，还有专门的一章介绍如何加强 Windows 2000。
- ▲ **第六部分：附录** 如果你想要学习管理、监视和审核，Microsoft Internet Security and Acceleration（ISA）服务器或者入侵侦测，则可以参考附录。你还将找到可以帮助你保护系统的有用工具和技术的相关讨论。

注意：要记住，本书指出了已知的安全问题并给出有助于保护系统和网络的建议。不过，每一个环境都是不同的，这里提出的一些建议可能不适合你的情况。在实际系统上实施更改之前，一定要在一个非生产型测试平台上对本书中提到的任何更改或安全性建议进行测试。

相应的 Web 站点

有一些额外的章节和附录只发布在 Web 上，其主题包括：

- ▼ 第 1 章：Certificate Server（证书服务器）
- 附录 A：Win2k Services（Windows 2000 服务）
- ▲ 附录 B：Ports and Protocols in TCP/IP（TCP/IP 中的端口和协议）

可以在 www.osborne.com 上找到以上内容以及其他内容。

快速目录

第一部分　安全的基础知识

第二部分　Windows 2000 安全性

第三部分　保护 Windows 2000

第四部分　保护 Windows 2000 网络

第五部分 其他问题

第六部分 附录

目　录

第二部分 Windows 2000 安全性