New Riders

北京科海培训中心

Windows 2000 安全技术

[美] Roberta Bragg 著
倪晓强 沈立 译
杨洪涛 审校

- 理解核心安全概念，例如密码学、安全协议、PKI 和 Kerberos
- 利用 Kerberos、加密文件系统、NTFS、本地安全策略和 Windows 2000 专用的安全工具控制对 Windows 2000 系统的访问
- 通过 RRAS、VPN、RADIUS 和终端服务建立安全的远程访问
- 使用域账户策略、IPSec、PKI 和组策略等分布式安全服务保护网络的安全
- 实现安全的安装和升级，维护和审核你的安全策略
- 配置访问策略、受限组成员以及系统服务安全
- 保护局域网、IRDA 连接、终端服务和互操作服务的安全

清华大学出版社
http://www.tup.tsinghua.edu.cn

NRP

北京科海培训中心

Windows 2000 安全技术

[美] Roberta Bragg 著

倪晓强 沈立 译

杨洪涛 审校

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：01-2000-2751

内 容 提 要

本书从实用的角度出发，全面地介绍了关于 Windows 2000 的信息系统安全，介绍了大量有关 Windows 2000 安全的工具、特性及结构方面的信息。

全书分四部分，分别介绍了安全的基本概念与定义、操作系统安全的保护、本地网络安全的保护以及实际网络安全的保护。内容包括：密码学简介、相关的安全协议、公钥体系及其建立过程、Kerberos、加密文件系统、NTFS、安全策略及安全工具；此外，还介绍了 Windows 2000 域的安全管理与保护、低级 Windows 客户的保护、新的分布式文件系统；最后，还深入探究了使用 RADIUS 和 RRAS 来保护远程访问、Web 安全以及互操作性方面的内容。

本书通过案例分析进行讲解，文笔流畅，通俗易懂。适合管理和支持 Windows 2000 的网络管理员、欲将网络升级到 Windows 2000 的管理人员、系统安全及审计方面的专业人员学习使用。学习本书不要求具有 Windows NT 及其安全或密码学方面的知识，但需具备基本的网络知识。

书　名：Windows 2000 安全技术

作　者：Roberta Bragg

译　者：倪晓强　沈立

出版者：清华大学出版社（北京清华大学校内，邮编 100084）

印刷者：北京门头沟胶印厂

发行者：新华书店总店北京科技发行所

开　本：787×1092 1/16　印张：26.125　字数：635 千字

版　次：2002 年 1 月第 1 版　　2002 年 1 月第 1 次印刷

印　数：0001～5000

书　号：ISBN 7-302-05085-6/TP・2974

定　价：43.00 元

关 于 作 者

Roberta Bragg 自 1985 年起就使用一台便携式计算机经营着她的咨询公司——Have Computer Will Travel 公司。另外，她还当过销售员、系统管理员、开发人员、专栏评论员、大学教师、商业学校教师以及技术培训员。她当前获得的证书包括 MCSE（Windows NT 3.5.1、4.0 与 Windows 2000）、MCT、MCP＋Internet 和 CTT，曾涉足 Mainframe moonlanding，80 column cards 与 Fortran 等领域。读者可以在 www.mcpmag.com 发现她是一名专栏评论员，可以在 www.spu.edu 上发现她是一位教师，可以在 www.peaceweaver.com 上发现她是一名安全福音传道者。

关于技术评论家

下列这些评论家为《Windows 2000 安全技术》的整个发展过程贡献了他们相当多的专家意见。在此书写作期间，这些热心的专家们对书中技术内容、组织方式及写作方式进行了评阅。他们的反馈意见对保证《Windows 2000 安全技术》满足读者对最高质量的技术信息的需求是非常关键的。

David Shackelford 是 ChoicePoint 公司的子公司 IRSC 的网络与计算机业务主管。他的经历包括：当过一名养蜂人，为一家通俗诗杂志筛选来稿，并在 Hewlett-Packard 与 Intel 公司教授过网络课程。他已经作为一名教员、系统工程师、网络设计人员及安全管理员在计算机界工作了十年。David 拥有英语硕士学历，是一名微软认证的系统工程师及培训员，是 New Riders 出版的《Windows 2000 Essential Reference》一书的作者之一，也是 New Rider 出版的《Inside Windows 2000 Server》的一名技术编辑。

Mich Kabay 在 15 岁时就开始学习汇编程序，在 1966 年就在 McGill 大学学习 FORTRAN IV G。在 1976 年，他从 Dartmouth 大学获得了应用统计与无脊椎动物学的博士学位。在 1979 年，他加入了美国一个编译器组，研究一种新的 4GL 与 RDBMS，并负责开发统计句法、编写语法分析器、错误捕捉以及命令语言中的统计功能的代码生成。Kabay 博士于 1980 年加入 Hewlett-Packard 并成为一名性能专家，赢得了 1982 年的系统工程师年度奖。他曾为《Computer World》、《Network World》、《Computing Canada》、《Secure Computing Magazine》、《NCSA News》、《Information Security Magazine》及几种其他的商业杂志撰写过专栏。他在 1997 年获得了认证系统安全专家（Certified Systems Security Professional，CISSP）的证书。Kabay 博士已发表了 220 多篇关于业务管理与安全的论文，并完成了一本大学教材《The NCSA Guide To Enterprise Security: Protecting Information Assets》（ISBN0－07－033147－2），该教材由 McGraw-Hill 于 1996 年 4 月出版。他是 ICSA 实验室从 1991 年到 1999 年（以前的 NCSA，然后是 ICSA）的教育主管。在 2000 年 1 月，他加入了 Atomtic Tangerine 公司的 INFOSEC 组，担任安全领导。

Brendan McTague 是 Perot Systems 公司的 Gloabal Financial Service 部门的高级系统工程师。他目前为一家主要的欧洲银行的投资银行分部管理一个跨平台的 Internet 工程组。Brendan 从 Temple 大学毕业并获得计算机科学学士学位。他已经在 Windows NT 到 Windows 2000 上工作了超过 5 年，并在 1995 年早期获得了 MCSE 证书。当他不工作时，Brendan 喜欢与他的妻子及儿子在芝加哥郊外的家中度过。欢迎给他提意见，他的电子邮件地址是 brendan.mctague@mindspring.com。

前　言

信息系统安全已经成为每个人都必须关心的话题。只知道口令的用法及文件权限设置已经远远不能满足需要了。如果用户管理、设计、实现、安装或者使用计算机系统，则他有权利、也有义务尽可能保护计算机系统的安全（包括在系统中存储和移动的信息）。

Windows 2000 的设计十分注重安全。存在很多新的特性，对老版本的许多功能也做了增强。如果这些特性被恰当和正确地实现，则它们就能够保护系统与数据。然而，只知道这些特性及如何使用它们还不够：网络管理员必须知道使用它们的理由和场合。最后，网络管理员必须以人们能够理解与维护的方式来实现系统安全。

本书提供了关于 Windows 2000 安全的各个方面的内容，但我们并未打算使它成为一本包罗万象的 Windows 2000 指南，而只是集中讨论了可用来保护 Windows 2000 网络安全的一些服务与工具。

本书的读者

Windows 2000 网络的管理员，或者希望向 Windows 2000 迁移的网络管理人员都可以从本书中找到关于 Windows 2000 安全的安全工具、特性以及构架方面的可靠信息。Windows NT 4.0 爱好者也能从中找到相关的知识。

另外，本书假定读者有一定的网络知识，因此只在活动目录的体系结构方面提供了一些介绍性的内容。需要更多知识的读者可在很多资源（包括附录中列出的）中查找。因此，本书一开始就为那些不了解密码学知识的人提供了一些介绍性的材料。

信息系统安全和审计方面的专业人士会从中找到 Windows 2000 安全所提供的全部细节。如果读者对这个领域并不陌生，则可以跳过关于密码学的介绍性材料。Windows 2000 安全的具体内容在后面的几章中有详细的介绍。

本书的组织结构

本书分成如下的四个部分。

第 1 部分　概念与定义

本部分包括安全的基本概念、密码学、安全相关协议、公钥体系及 Kerberos 等几章。如果读者对这些主题有深入的了解，建议直接跳过，这几章之后提供了 Windows 2000 特有的内容。在与 Windows NT 管理员和 Windows 体系支持者的很多谈话中，我发现他们中有很多人对这些问题并没有什么背景知识，但他们还必须处理 Kerberos 或 PKI，或选择加密算法，这就是本书为什么包括介绍性内容的原因。后面的几章将讨论 Windows 2000 如何实

现一个标准，以及如何提供选择，这部分比较冗长，任何已掌握这些概念的读者都可以直接跳到第 2 部分。如果碰到了不熟悉的术语或概念，再回来看看就行了。

第 2 部分　保护操作系统的安全

任何安全程序的第一步都应该是保护基本操作系统的安全。这一部分研究了 Windows 2000 所有版本的公共特征，并涉及了独立系统的安全问题。这一部分主要涵盖 Windows 2000 中的 Kerberos 认证、加密文件系统、NTFS、本地计算机安全策略和 Windows 2000 自带的安全工具方面的内容。

第 3 部分　保护 Microsoft 局域网的安全

现今已很少有未上网的计算机了。计算机的连接范围很广，在世界范围内，网络将家庭用户、企业用户和网络服务提供商连接起来。连接的方式也很多，从拨号连接、局域网连接到包含多种操作系统的广域网连接等等都是其中的一种方式而已。这一部分专门介绍 Windows 局域网，涉及 Windows 2000 域安全管理与保护的内容。另外，还有关于保护低级 Windows 客户及新的分布式文件系统的内容。

第 4 部分　保护现实世界网络的安全

网络大多由多种操作系统组成并涉及大量的计算机。这一部分探究 Windows 2000 保护现实网络安全的特性，从中可以找到关于使用 RADIUS 和 RRAS 来保护远程访问、建立公钥体系、Web 安全以及互操作性方面的内容。

目 录

第1部分 概念与定义

第2部分 保护操作系统的安全

第3部分 保护Microsoft本地局域网的安全

第4部分 保护现实世界网络的安全