

Microsoft® Press



精通

Microsoft®

Windows 2000 和 Windows XP 安全技术

- 阻挡间谍和垃圾邮件进入您的邮箱
- 监视系统出现的可疑行为并防御攻击
- 清除病毒、蠕虫和其他有害的Web软件
- 启动您的VPN、远程访问和无线网络服务
- 使用身份验证、证书和组策略，控制对共享资源的访问
- 加密数据、阻塞端口和锁定注册，采取多种安全性控制
- 从防火墙到监视软件——阻挡入侵者访问您的网络 and 私人数据

[美] Ed Bott, Carl Siechert 著
梁超 李钦 江楠 树军 译



清华大学出版社

精通 Microsoft Windows 2000 和 Windows XP 安全技术

[美]Ed Bott, Carl Siechert 著
梁超 李钦 江楠 树军 译

清 华 大 学 出 版 社
北 京

内 容 简 介

《精通 Microsoft Windows 2000 和 Windows XP 安全技术》是清华大学出版社“精通”系列丛书之一。本书针对 Windows XP Professional、Windows XP Home 和 Windows 2000 Professional 在日常使用中遇到的各种应该注意或亟待解决的安全问题，精心组织了数百条快捷的解决方案、提供解答疑难的专家提示，以及数目众多但方便易找的工作区示例，表述简捷，直指关键。本书将帮助用户找到执行日常安全任务的最快最好的方法，并将安全经验提升到一个更高的层次。

本书适合于所有重视安全问题，并使用 Windows 2000 和 Windows XP 操作系统的用户。对于企业的局域网或小型工作组的计算机用户而言，更是案头必备的安全参考手册。

Microsoft Windows Security Inside Out for Windows XP and Windows 2000(ISBN 0-7356-1632-9)

Microsoft Press

Copyright © 2002 by Microsoft Corporation

Original English language edition published by Microsoft Press, a Division of Microsoft Corporation

All rights reserved.

No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the Publisher. For sale in the People's Republic of China only.

本书中文简体版由 Microsoft Press 授权清华大学出版社在中国境内(香港、澳门特别行政区和台湾地区除外)独家出版发行，未经出版者书面许可，不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号：图 01-2003-0840 号

版权所有，翻印必究。

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

书 名：精通 Microsoft Windows 2000 和 Windows XP 安全技术

作 者：[美]Ed Bott, Carl Siechert

译 者：梁超 李钦 江楠 树军

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. com. cn](http://www.tup.com.cn)

[http:// www. tup. tsinghua. edu. cn](http://www.tup.tsinghua.edu.cn)

责任编辑：蔡颖

印 刷 者：国防工业出版社印刷厂

发 行 者：新华书店总店北京发行所

开 本：787×1092 1/16 **印张：**28.25 **字数：**952 千字

版 次：2003 年 6 月第 1 版 2003 年 6 月第 1 次印刷

书 号：ISBN 7-89494-093-3

印 数：0001~4000

定 价：54.00 元(含 1 张光盘)

前言

欢迎学习《精通 Microsoft Windows 2000 和 Windows XP 安全技术》一书。

您是否已经感到病毒、黑客、垃圾邮件和其他威胁对计算机安全带来的压力，而苦于没有有效的解决方法？没有关系，如果您已经熟悉了自己使用 Windows 的方式，那么现在来做进一步的探索，真正行使 Windows 的安全特性。本书针对您在日常使用中可能遇到的各种安全问题，一一做了描述和分析，同时利用精心组织的解决方案、解答疑难以及大量简单明了的图片示例和说明，帮助您找到执行日常安全任务的又快又好的方法，并将安全经验提升到一个更高的层次。

本书读者对象

本书主要面对一切日常使用 Windows 2000 或 Windows XP 操作系统的用户，最适用于有一定操作基础和使用经验，并且关注系统安全的人员。如果您已经意识到计算机安全的重要性，并希望能够获取更加科学合理的专家指导，从而快速有效地达到维护系统安全的目的，那么不要犹豫，快快开始本书的学习吧！

本书特色

本书共分为 5 个部分，其中每个部分有若干章节。第 1 部分介绍 Windows 安全基础，帮助您快速地熟悉与安全相关的主题和重点内容。第 2 部分介绍保障个人计算机安全的方法和技巧，避免遭受外来的侵害。第 3 部分针对的是联网安全性的问题，而第 4 部分则介绍了一些重要的安全解决方案。最后，本书还给出了安全性方面需要长期重视的 10 条原则，希望大家铭记，给予足够重视。本书讲解深入浅出，有数百条提供便利的参见信息、及时的提示帮助、颇具价值的疑难解答、内容丰富的技术内幕以及容易上手的操作步骤。同时，配以清晰明了的版式设计。通过本书的学习，您将发现对付复杂的安全性问题也会变得轻松有效，同时自己的安全经验也将上升到一个新的水平。

体例约定

本书使用了一些特殊的文本格式，使您更容易找到所需要的信息。

约 定	含 义
简写的菜单命令	本书使用的简写菜单命令，如“选择【工具】 【Internet 选项】 【安全】”，意思是您首先单击【工具】菜单，指向【Internet 选项】，然后单击【安全】标签
文本中的加号(+)	键名之间的“+”表示同时按下这些键，例如，“按下 Ctrl+Alt+Delete”表示您同时按下 Ctrl、Alt 和 Delete 键

特殊段落约定

技术内幕

本段文字引导您可以找到便捷的工具来解决软件存在的问题，通过这些信息，您可以了解某一特性的工作原理。

疑难解答

解决一些您可能遇到的常见问题。



提示 标有“提示”的注释为您提供了有用的帮助信息，或与所讨论主题相关的可选过程。



警告 标有“警告”的注释说明在您完成某项任务或解决某个问题时，必须注意一些可能会出现的问题。



参见光盘 本段文字说明您可以从本书附带的光盘中找到一些示例文字或文本信息。



注意 标有“注意”的注释为您提供与所谈论话题相关的其他信息。



参见 标有“参见”的注释将您引导到本书的其他章节中去查找与所讨论主题相关的信息。

运行本书光盘所需的最低要求

1. Microsoft Windows 95 或更高版本的操作系统(包括 Windows 98、Windows Me、安装了 Service Pack 3 的 Windows NT 4.0、Windows 2000 和 Windows XP)。
2. 至少 266 MHz 的 CPU。
3. 64MB RAM。
4. 8 倍速或更快的光盘驱动器。
5. 31 MB 剩余硬盘空间。
6. Microsoft Windows 兼容声卡和扬声器。
7. Microsoft Internet Explorer 4.0 或更高版本。
8. Microsoft 鼠标或兼容的其他指示设备。

本书历经半年的紧张翻译和编辑，终于得以出版。严谨、求实、优质一直是清华版图书的传统品质，同时也是我们在翻译工作中孜孜以求的目标，但软件的实效性不容我们精雕细琢，错误之处在所难免，欢迎广大读者批评指正。

感谢微软中国公司产品部对本书翻译工作的大力支持，同时也要感谢参与翻译的江南、李钦、梁超、赵慧娟、树军、王治国，对他们在本书翻译过程中所做的工作表示衷心的感谢。

需要说明的是，由于某些示意图涉及的情况比较特殊，在中文界面下很少出现，所以仍采用了原作的英文界面示意图，但不影响阅读，请读者谅解。

目 录

第 I 部分 Windows 安全基础

第 1 章 计算机安全：您的处境 是否危险？

1.1 安全与便利的权衡	4
1.2 了解您的敌人：对计算机安全的 7 种威胁	4
1.2.1 威胁 1：物理攻击	5
1.2.2 威胁 2：被窃取的密码	6
1.2.3 威胁 3：爱窥探的网络邻居	8
1.2.4 威胁 4：病毒、蠕虫程序以及其他的敌意程序	9
1.2.5 威胁 5：外部入侵者和特洛伊木马接管计算机	11
1.2.6 威胁 6：对个人隐私的入侵	13
1.2.7 威胁 7：电子邮件的威胁	14
1.3 怎样保护自己	14

第 2 章 Windows 安全工具及安全技术

2.1 什么是用户账户	17
2.1.1 本地账户和域账户	18
2.1.2 内置用户账户	19
2.1.3 安全组	20
2.2 控制登录及身份验证的过程	22
2.2.1 互动式登录是如何工作的	24
2.2.2 保护安全账户管理器	26
2.2.3 使用组策略来限制访问	26
2.3 确保文件的安全性	27
2.3.1 使用 NTFS 权限	28
2.3.2 在网络上共享文件	29
2.3.3 加密选项	29
2.4 保护您的计算机：检查清单	30
2.4.1 安装所有的 Windows 安全性补丁	30
2.4.2 删除或关闭不使用的账户	31

2.4.3 对所有用户账户设置坚固的密码	32
2.4.4 加强所有用户的登录安全性	32
2.4.5 安装并设置防火墙	33
2.4.6 安装并设置反病毒软件	35
2.4.7 对所有驱动器使用 NTFS 格式	35
2.4.8 检查所有文件目录的 NTFS 权限	35
2.4.9 检查所有的网络共享	36
2.4.10 将屏幕保护程序作为一种安全设备	37
2.4.11 创建备份	38
2.4.12 高级安全性选项	38

第 3 章 管理用户账户和密码

3.1 管理用户账户获得更好的安全性	42
3.1.1 查找账户管理工具	42
3.1.2 创建用户账户	46
3.1.3 禁用或删除用户账户	48
3.1.4 将用户账户指派到安全组中	50
3.1.5 为用户账户指定密码	54
3.1.6 保护 Administrator 账户	55
3.1.7 保护 Guest 账户	56
3.2 有效地使用密码	58
3.2.1 创建保险的密码	59
3.2.2 创建及强制使用密码策略	60
3.2.3 恢复丢失的密码	62
3.2.4 管理密码	65
3.3 配置登录过程以获得更好的安全性	67
3.3.1 提高欢迎屏幕的安全性	67
3.3.2 提高传统登录方式的安全性	68
3.3.3 控制自动登录	69
3.3.4 显示欢迎消息或警告	70

3.3.5 设置账户锁定策略.....72	5.6 管理打印机和外围设备..... 117
3.3.6 使用 Syskey 再增加 一层保护.....73	
第 4 章 安装和使用数字证书.....75	第 6 章 防止数据丢失.....119
4.1 什么是数字证书.....75	6.1 轻松的文件备份战略..... 120
4.1.1 证书的目的.....76	6.1.1 备份选定的文件夹和文件..... 121
4.1.2 证书存储.....77	6.1.2 备份完整的分区..... 124
4.1.3 证书颁发机构.....78	6.1.3 组合方法以实现最佳 备份战略..... 126
4.2 获取个人证书.....79	6.2 组织数据..... 127
4.3 管理您的证书.....81	6.2.1 排除不必要的数据..... 127
4.3.1 使用【证书】对话框.....82	6.2.2 为简单文件备份调整数据..... 128
4.3.2 使用【证书】管理单元.....83	6.2.3 创建文件备份分区..... 129
4.3.3 查看和修改证书属性.....86	6.3 执行常规备份..... 129
4.3.4 导出证书以备保管.....88	6.3.1 使用磁盘映像软件执行 完全备份..... 129
4.3.5 导入证书.....90	6.3.2 使用 Windows 备份执行 临时文件备份..... 131
4.3.6 复制或移动证书.....90	6.4 备份其他信息..... 135
4.3.7 删除证书.....90	6.4.1 执行特殊目的的文件备份..... 135
4.3.8 续订证书.....91	6.4.2 使用 Windows 包含的其他 预防数据丢失的工具..... 137
第 5 章 多用户电脑的安全性.....92	6.5 保护备份..... 139
5.1 应用 NTFS 权限进行访问控制.....93	6.6 恢复数据..... 140
5.1.1 基本和高级权限.....95	6.6.1 从备份文件中恢复 单个文件..... 140
5.1.2 查看和更改 NTFS 权限.....97	6.6.2 使用紧急修复盘还原系统..... 140
5.1.3 关闭 Windows XP 系统下的 简单文件共享界面.....97	6.6.3 使用自动系统恢复盘还原 系统..... 141
5.1.4 通过 Windows 资源管理器 设置 NTFS 权限.....98	6.6.4 从受损硬盘中恢复数据..... 141
5.1.5 用命令行工具设置 NTFS 权限.....100	第 7 章 维护系统安全.....142
5.1.6 通过继承将权限应用到 子文件夹.....102	7.1 使用 Windows Update 保持更新..... 142
5.1.7 复制或移动文件时权限 发生的变化.....104	7.1.1 自动更新..... 144
5.1.8 没有访问权限时如何进入 文件和文件夹.....105	7.1.2 为多个计算机下载 更新文件..... 146
5.2 锁定个人文档.....106	7.2 安全警报服务..... 147
5.2.1 Windows XP 中的【将这个 文件夹设为专用】.....106	7.2.1 通过 Windows Messenger 接收警报..... 147
5.2.2 在 Windows 2000 系统中 保护个人文件.....109	7.2.2 接收电子邮件警报..... 148
5.3 在多用户计算机中安全 共享文件.....110	7.2.3 其他安全警报的资源..... 149
5.4 限制对程序的访问.....113	7.3 测试和证实安全状态..... 150
5.5 限制对注册表的访问.....114	7.3.1 使用 Microsoft Baseline Security Analyzer 检测更新状态..... 150
	7.3.2 使用 MBSA 命令行选项..... 154
	7.3.3 学习 MBSA 的更多内容..... 154

7.3.4 超越 MBSA	155	第 10 章 保护电子邮件的安全	205
第 11 部分 保护你的个人电脑		10.1 防范危险附件	205
第 8 章 加强 Internet Explorer 的安全性	159	10.1.1 附件和 Outlook 中的自动安全控制	206
8.1 当 Web 页出问题	160	10.1.2 判断是否安装了安全更新	206
8.2 使用安全区域	161	10.1.3 安全更新如何处理文件附件	207
8.2.1 配置【本地 Intranet】区域	162	10.1.4 安全更新如何处理 Microsoft Office 文档	208
8.2.2 把站点添加到区域中	163	10.1.5 Outlook 对象模型和安全更新	209
8.2.3 创建自定义的安全区域	164	10.1.6 在系统中添加安全更新	210
8.2.4 配置安全设置	167	10.1.7 在 Outlook 2002 中自定义安全更新	210
8.3 使用内容审查程序来阻止不良的内容	173	10.1.8 安全更新的工作区	211
8.3.1 阻止未分级的站点	175	10.1.9 不带有电子邮件安全更新的附件安全性	211
8.3.2 关闭阻止	176	10.1.10 Outlook Express 中的附件安全性	212
8.3.3 使用第 3 方内容筛选程序	176	10.2 防范欺诈性 HTML	214
8.4 管理 ActiveX 控件	176	10.2.1 改变安全区域	215
8.4.1 读取控件属性	178	10.2.2 激活 Outlook 2002 邮件中的脚本	215
8.4.2 “可安全初始化”和“可安全执行脚本”标志	179	10.3 安全地使用基于 Web 的电子邮件	215
8.4.3 删除已下载的 ActiveX 控件	180	10.3.1 登录进入 Hotmail	217
8.4.4 只允许管理员认可的 ActiveX 控件运行	180	10.3.2 处理附件和脚本	217
8.4.5 阻止 ActiveX 控件的活动	181	10.4 保护电子邮件免受窥视	218
8.5 管理 Java 小程序	182	10.4.1 获取公钥/私钥对	219
8.6 管理脚本	182	10.4.2 使用 S/MIME 发送加密消息	220
第 9 章 抵御病毒、蠕虫和特洛伊木马	184	10.4.3 加密所有待发邮件	221
9.1 恶意软件如何攻击计算机	185	10.4.4 读取加密邮件	221
9.1.1 附件传播型病毒	188	10.4.5 确保邮件的真实性和完整性	222
9.1.2 来自 Web 的攻击	189	10.4.6 对所有待发邮件签名	222
9.1.3 特洛伊木马程序	190	10.4.7 使用 PGP 来签名和加密	223
9.1.4 其他攻击	191	10.4.8 其他第 3 方加密工具	224
9.2 识别恶意软件	192	第 11 章 阻止垃圾邮件	226
9.3 选择反病毒程序	194	11.1 什么是垃圾邮件	227
9.4 保护您的计算机免受恶意软件的攻击	198	11.1.1 垃圾邮件制造者的秘密	228
9.4.1 培训用户避免病毒感染	199		
9.4.2 阻止危险附件	200		
9.4.3 使用备份和系统还原	202		
9.5 修复被感染的系统	203		

11.1.2	如何对电子邮件标头进行解码.....	228	13.3.2	在 Internet Explorer 5 中设置 cookie 首选项	277
11.1.3	在 Outlook Express 中查看邮件标头.....	229	13.3.3	在 Netscape 6.2/Mozilla 1.0 中设置 cookie 选项	278
11.1.4	在 Outlook 中查看邮件标头.....	230	13.3.4	Internet Explorer 5 或 Netscape/Mozilla 中的 cookie 策略	279
11.1.5	在其他电子邮件程序中查看邮件标头.....	230	13.3.5	在 Internet Explorer 6 中设置 cookie 选项	280
11.1.6	读取邮件标头.....	231	13.3.6	备份、恢复和删除 cookie.....	287
11.2	基本的垃圾邮件阻止技术.....	232	13.3.7	使用 cookie 管理程序	288
11.3	使用筛选器	234	13.4	监控网络 Bug.....	288
11.3.1	创建自定义筛选器.....	236	13.5	根除间谍程序.....	289
11.3.2	使用 Outlook 的垃圾邮件和成人内容筛选器.....	242	13.6	对付更阴险的“幽灵”软件	290
11.3.3	备份邮件规则.....	245	13.7	匿名浏览.....	291
11.4	第 3 方垃圾邮件处理方案.....	246	13.8	掩盖行踪.....	292
11.5	对垃圾邮件发起反击.....	246	13.8.1	清除 Internet Explorer 历史.....	292
第 12 章	防止黑客攻击	248	13.8.2	删除 Internet Explorer 自动完成历史	293
12.1	黑客攻击原理	249	13.8.3	关闭 Internet Explorer 中的直接插入自动完成	293
12.2	利用防火墙来阻止攻击.....	250	13.8.4	清除您最近的文档列表	293
12.2.1	数据包筛选.....	250	13.8.5	在退出时清除最近的文件历史.....	293
12.2.2	状态检查数据包筛选	251	13.8.6	清除应用程序最近使用内容的列表和【我最近的文档】菜单.....	294
12.2.3	应用程序筛选.....	251	13.8.7	使用第 3 方的清除软件	294
12.2.4	谁需要防火墙?	254	第 III 部分 网络保护		
12.2.5	在 Windows XP 中使用 Internet 连接防火墙	255	第 14 章 网络安全	299	
12.2.6	启动 Internet 连接防火墙.....	255	14.1	构建一个安全的网络.....	300
12.2.7	允许传入的连接.....	256	14.1.1	配置网络硬件.....	300
12.2.8	配置 ICMP 选项	259	14.1.2	协议和其他软件组件	302
12.2.9	选择第 3 方个人防火墙.....	260	14.1.3	在 Windows XP 上安装 IPX/SPX 或者 NetBEUI.....	304
12.2.10	使用硬件防火墙设备	262	14.1.4	在 Windows 2000 上安装 IPX/SPX 或者 NetBEUI.....	304
12.3	确定入侵者	262	14.1.5	取消 TCP/IP 上的文件共享	305
12.3.1	配置 Internet 连接防火墙日志.....	263	14.2	限制对文件和文件夹的网络访问.....	306
12.3.2	检查 Internet 连接防火墙日志.....	264	14.2.1	Windows 共享和安全模式.....	306
12.4	反击	266			
第 13 章	保护您的隐私	268			
13.1	保护您的身份信息.....	269			
13.2	保护孩子的安全和隐私.....	272			
13.3	管理 cookie.....	273			
13.3.1	对 cookie 的分析	274			

14.2.2	Windows XP 的简单文件共享模式.....	307	16.5	远程访问注意事项.....	342
14.2.3	Windows XP Professional 和 Windows 2000 的高级共享模式.....	307	16.5.1	建立虚拟专用网络.....	342
14.2.4	在 Windows 95/98/Me 系统中共享文件夹.....	310	16.5.2	连接到 VPN.....	344
14.2.5	建立共享文件夹.....	310	16.5.3	保护拨号连接的安全.....	345
14.2.6	在 Windows XP 系统中共享文件夹.....	310	第 IV 部分 极限安全		
14.2.7	通过简单文件共享模式设置共享文件夹.....	312	第 17 章 保护端口和协议的安全性.....349		
14.2.8	使用经典安全模式共享文件夹.....	314	17.1	端口和协议如何允许访问计算机.....	350
14.2.9	隐藏共享文件夹.....	315	17.1.1	端口号是如何分配的.....	350
14.2.10	删除共享资源.....	315	17.1.2	非正式使用的端口.....	351
14.2.11	给共享文件夹分配权限.....	315	17.1.3	如何连接到端口.....	352
14.3	管理共享文件夹.....	317	17.2	确定哪个端口是活动的.....	352
14.3.1	管理型共享.....	317	17.3	限制对端口的访问.....	356
14.3.2	创建一个新共享.....	318	17.3.1	用 Internet 连接防火墙限制端口.....	356
14.3.3	管理会话和打开文件.....	319	17.3.2	用 TCP/IP 筛选限制端口.....	356
14.4	工作组和域.....	320	17.3.3	用硬件防火墙限制端口.....	357
第 15 章 共享 Internet 连接.....321			17.3.4	用 IP Security 限制端口.....	358
15.1	将网络连接到 Internet.....	321	17.4	为什么阻止端口还不够.....	364
15.2	在局域网中使用直接 Internet 连接.....	323	17.5	关闭不需要的服务.....	364
15.2.1	配置拨号连接.....	323	17.5.1	理解 Windows 服务.....	365
15.2.2	配置宽带连接.....	323	17.6	加强 Internet 信息服务的安全性.....	372
15.2.3	添加防火墙保护.....	324	17.6.1	管理 IIS 服务.....	372
15.3	在局域网中建立直接 Internet 连接.....	326	17.6.2	运行 IIS 锁定工具.....	373
15.4	通过硬件共享 Internet 连接.....	327	17.6.3	阻止匿名访问 IIS.....	374
15.4.1	配置路由器或本地网关.....	328	17.6.4	使用服务器日志.....	376
15.4.2	加强路由器的安全性.....	329	17.6.5	保持最新的 IIS 安全补丁.....	377
15.5	通过软件共享 Internet 连接.....	330	第 18 章 加密文件和文件夹.....378		
15.5.1	在 Windows XP 中设置 Internet 连接共享.....	331	18.1	使用加密文件系统.....	380
15.5.2	在 Windows 2000 Professional 中设置 Internet 连接共享.....	333	18.1.1	在开始之前: 了解 EFS 的危险.....	380
第 16 章 无线网络和远程接入.....335			18.1.2	加密数据.....	381
16.1	无线网络的风险.....	336	18.1.3	使用加密数据.....	384
16.2	控制与无线接入点的连接.....	337	18.1.4	恢复加密数据.....	388
16.3	加密无线传输.....	339	18.1.5	禁用或者重新启用 EFS.....	388
16.4	无线网络的安全性.....	341	18.1.6	强化 EFS 保护.....	390
			18.2	创建数据恢复代理.....	391
			18.2.1	生成一个文件恢复证书.....	391
			18.2.2	指派数据恢复代理.....	391
			18.2.3	删除私钥.....	392
			18.3	备份证书.....	393
			18.3.1	备份文件恢复证书.....	394
			18.3.2	导出个人加密证书.....	394

18.3.3 导入个人加密证书.....395

18.3.4 创建新的个人加密证书.....396

第 19 章 通过组策略和安全模板**管理安全**.....397

19.1 探索有关安全的策略.....398

19.1.1 探索用户权利.....399

19.1.2 探索安全选项.....401

19.1.3 探索其他组策略.....407

19.2 使用组策略管理单元.....412

19.2.1 使用安全设置扩展.....413

19.2.2 如何应用策略.....414

19.2.3 对远程计算机使用

组策略.....415

19.3 使用安全模板.....416

19.3.1 使用安全模板管理单元.....418

19.3.2 检查账户策略、本地策略、

事件日志和系统

服务设置.....419

19.3.3 控制安全组成员关系..... 419

19.3.4 配置文件夹、文件和

注册表权限..... 420

19.3.5 应用模板设置..... 420

19.4 分析系统安全..... 421

第 20 章 监视安全事件.....423

20.1 审核安全事件..... 423

20.1.1 启用安全审核..... 423

20.1.2 配置对文件、打印机和

注册键访问的审核..... 425

20.1.3 决定审核内容..... 428

20.2 查看安全事件日志..... 428

20.2.1 使用有日志记录的事件..... 429

20.2.2 使用日志文件..... 431

20.3 查看其他和安全相关的日志..... 434

第 V 部分 附录**附录 安全性的 10 条不变法则**.....436

第 I 部分

Windows 安全基础

第 1 章 计算机安全：您的处境是否危险？

第 2 章 Windows 安全工具及安全技术

第 3 章 管理用户账户和密码

第 4 章 安装和使用数字认证

第 5 章 多用户电脑的安全性

第 6 章 防止数据丢失

第 7 章 维护系统安全



安全与便利的权衡

认识您的对手：对计算机安全的 7 种威胁

怎样保护自己

计算机安全：您的处境是否危险？

个人计算机每一年都会变得更强大、更复杂，而且与外界相联接更紧密，也更容易受到攻击。

1995 年，当时 Internet 还处于婴儿时期，一家处于领先地位的计算机安全信息交换中心 CERT Coordination Center 的报告声称，已发现有 171 项系统易受攻击的弱点，而“小偷”和“强盗”们则可以利用这些缺陷对已经广为使用的操作系统及应用程序发起攻击。2000 年，新发现的系统弱点跃升至 1090 种，而到了 2001 年，总数已升至 2500 种以上，其中 37 种缺陷的危险程度足以发布正式的安全性警报。安全专家预计在计算机操作系统及网络中的新漏洞还会继续增加。

当然，这些安全警报所面向的不只是我们这样运行 Windows 的用户，还有多种操作系统及硬件平台的使用者。但是这个世界上最流行的操作系统确实是一个十分有诱惑力的目标。有破坏性、快速传播的病毒以及新发现的 Windows 操作系统中的缺陷都会变成有声有色的头条新闻，但是对应着每一条晚间新闻中的安全性警告，有 100 多个安全性威胁只在面向安全性专业人员的 Web 站点及邮件列表中发布。要记住：人们不知道的事物也可能会使他们受到伤害。

随着个人计算机越来越多地融入到我们的社会及经济生活中，来自于病毒、恶意的 Web 站点、网络“强盗”以及网络“窃贼”的潜在的危险也随之增多了。一个成功的攻击者可以销毁计算机上的数据文件并删除已安装的程序，从他人在线银行及金融账户中提取钱款，发送看起来是来自某地址的伪造的电子邮件，窃取他人的 Internet 连接以攻击其他计算机和网络。病毒和蠕虫程序会把数据变得一团糟，并使整个网络数日不能正常工作。

在一种新病毒或蠕虫程序大规模爆发之后进行清理的开销是十分惊人的。2001 年夏天，在两个星期之内，Code Red (红色代码)蠕虫程序感染了数十万计的计算机。据 Internet 研究机构 Computer Economics 估计，用于删除蠕虫程序、进行软件更新以改正安全性缺陷以及将这些系统恢复到正常的服务状态的直接开销达到了 10 亿美元，而且期间由于该蠕虫程序间接导致的生产力丧失还造成了 14 亿美元的损失。即使对于一台单独的

计算机,这种开销也可能是很大的。可以想象一下处理事务的计算机数日或一个星期不能工作,并且保存的所有文件都被损坏将会为用户带来多大的损失。

幸运的是,您并不需要多么高深的计算机知识就能保护您的计算机。本书就是要帮助普通的 Windows 用户排除这些错误信息、离奇信息和技术性问题的干扰,这些内容涉及到现今关于 Windows 安全性方面的大部分信息。如果您希望控制好个人电脑,并且保护自己不会受到网络上的威胁,那么本书是一个很好的选择。我们的焦点集中在会影响到使用 Windows XP (Home Edition 和 Professional Edition)或 Windows 2000 Professional 的用户的系统弱点和产生威胁的地方。我们会解释每个系统弱点的工作方式,它们有怎样的影响,以及如何填补该系统漏洞。



注意 本书的内容着重于 Windows XP (Home Edition 和 Professional Edition)及 Windows 2000 Professional。如果您使用 Windows 95、Windows 98 或 Windows Me,本书中的某些内容会与您有关,但我们提出的大多数建议都依赖于 Windows XP 和 Windows 2000 所特有的功能。这两种操作系统从底层上看就是考虑到安全性来设计的,诸如 NTFS 文件系统、内置加密功能以及对多用户的支持,这样的特性组成了一个综合的计算机安全程序的基础部分。如果您十分认真地希望保护您的个人电脑,但还在使用旧版本的 Windows,我们可以建议您升级。

本章会介绍对于计算机安全性最常见的威胁,并列举出安全系统所应采取的步骤。在第 2 章,我们会介绍各种 Windows 2000 和 Windows XP 内置的安全工具及技术,并告诉您如何更好地使用它们。在本书的其他部分,我们会详细地探索每种类型的威胁,提供深入的技术信息、专家提示、资源信息以及检查清单,通过这些技术您可以阻止最顽固的入侵者。

1.1 安全与便利的权衡

有一个简单但不可逃避的事实:就像没有完全安全的房子那样,同样没有完全安全的个人电脑。

使您的个人数据和 Internet 连接保持安全,不受攻击性软件及不受欢迎的访问者的侵害,这从定义上来说就是一个进行权衡的操作。Windows 具有的某些功能尽管可以使您的在线活动更加方便,但它们也会不经意地将保密的信息暴露给不可靠的陌生人。比如, Internet Explorer 有一个称为自动完成的功能允许您可以使用保存在 Web 站点上的登录名和密码,从而不需记住密码并且不必每次进行输入,只需单击一下就可以直接访问。但是这种节省时间的简便方法对于每个坐在您计算机前面的人都一样适用。只要几分钟,任何一个从物理上访问您的计算机的人都可以浏览您的银行档案,记录下敏感的信息,甚至进行资金的划转。

为了保护自己,可以禁用操作系统及其组件所提供的那些会给安全性带来不必要风险的功能。可以增加用于访问计算机和在线账户的密码的复杂度,也可以增添第 3 方的安全性软件及硬件设备,从而增加入侵者的工作难度。但遗憾的是,每增加一层安全性,都会使原本简单的操作过程更加的复杂困难。(关于这种基本的安全性概念有更为详细的讨论,请参见附录中的“安全性的 10 条不变法则”。)

那么怎样找到安全性和便利性之间的平衡点呢?计算机所扮演的角色和存放在其中的数据的价值决定着其安全级别。如果您是一名中央情报局的分析员或是跨国银行的的审计员,那么您需要的是世界级的安全性,并且要准备好为这种级别的保护措施支付很高的费用。另一方面,如果只是在您的小房间中的家庭计算机,只有您的家人才能对它访问,那么则可以将权衡的天平向便利性方面倾斜。

在决定如何保护自己之前,需要了解一下每个计算机用户每天都会面对的不同的威胁。

1.2 了解您的敌人:对计算机安全的 7 种威胁

如果您只注意主流的媒体,可能会认为您的计算机和数据所面对的威胁只是信用卡窃贼以及随电子邮

件携带的病毒。但事实上有些情况是很严重的。攻击者可能会来自任何地方，甚至包括您自己的办公室。根据 Computer Security Institute 和 FBI 旧金山办事处 2002 年的研究报告，接受调查的商业机构中有 38% 都受到来自内部的(现在或过去对公司不满的员工)对其系统及数据的未授权访问。而且近年来全球互联网中最严重的攻击事件都是一些经验并不丰富的业余攻击者通过在 Windows 计算机上植入“特洛伊木马”程序来实现的。

在本节中，我们会列举出您可能会遇到的 7 种常见类型的安全性威胁。

1.2.1 威胁 1：物理攻击

对计算机安全性最基本的破坏方式根本不需要攻击者具有任何技术水平。如果您把笔记本电脑不加照看地放在一个繁忙的机场或者火车站，甚至只要几秒钟，小偷就可以拿起它直接带走，当然同时还带走了您所有的个人数据以及存放在计算机中的所有密码。偷走一台台式电脑从逻辑上来说更加具有挑战性，但是其结果也会是损失惨重的。此外，不要假定一个复杂的、难以猜到的密码或是良好地加密过的文件可以受到保护。如果一个技术水平不错的窃贼能够拿走您的计算机，他(绝大多数的恶意黑客以及高科技窃贼都是男性)可以在上面花费几天或是几个星期；只要有足够的时间，这些人可以侵入任何一台计算机，无论它保护得多么好。

事情确实就像听起来这么糟糕，而且有些对计算机的物理攻击方式甚至更加具有破坏性。请考虑一下这种情况的后果：您出去吃午饭或是参加会议的时候没有将办公室的门锁上，并且您的计算机是打开且处于完全开放的状态。就是这短的间歇时间，也足以允许一个入侵者潜入您的办公室，坐在键盘前面，将数据文件复制到软盘上或是通过 Internet 上传到另一台计算机。恶意的入侵者还可能通过修改电子表格中的某些数字或是修改合同或信件上的措辞来暗中破坏您的工作。而一个真正下定决心的间谍甚至会安装监控软件，这种软件会在您的计算机的后台运行，并且可以将信息发送至远程的计算机。

例如，声名狼藉的远程控制程序 Back Orifice，图 1.1 显示了它的远程控制台。这个服务器端程序体积小得可以装入一张软盘，能在几秒内安装完毕，并且它在目标计算机上运行时几乎是无法被察觉的。通过所示的远程控制台，攻击者可以取得目标计算机的完全控制权：传送文件和文件夹，修改 Windows 注册表，并且(使用所示的控制功能)记录每次击键的细节信息，包括密码、信用卡号码、秘密的备忘录、在线聊天会话以及书信。

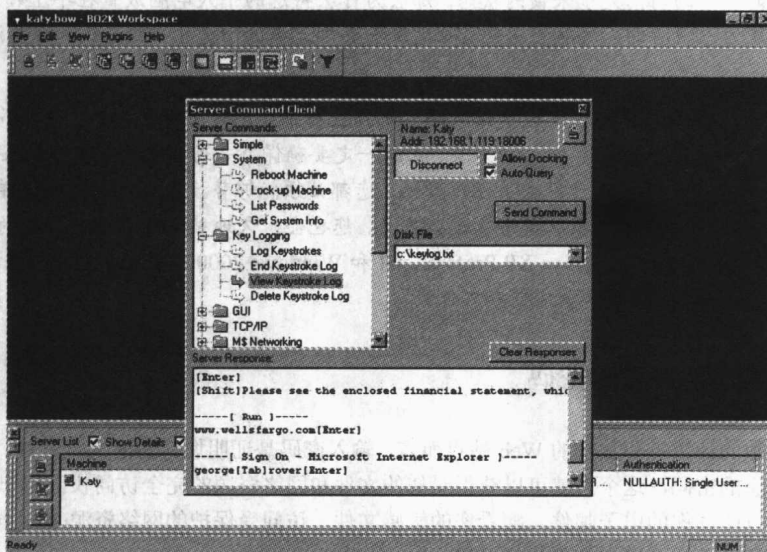


图 1.1 Back Orifice 的远程控制台



参见 关于如何检测并删除特洛伊木马程序以及其他的远程控制软件, 请参见第 9 章的 9.5 节“修复被感染的系统”。

物理安全检查清单

微软安全响应中心的专家说过, 如果坏人可以对您的计算机未加限制地进行物理访问, 那么它就不再是您的计算机了。这也就是为什么对于整套计算机安全计划而言, 绝对的第 1 条防线就是确保您的计算机在物理上是受到保护的。请依照下列的指导原则:

- 将存有敏感信息的计算机放在上锁的房间, 小卧室对于试图闯入的入侵者来说是太容易了。
- 在人流密集的地方, 应使用外部的加锁装置将计算机固定到写字台。这样额外的保护虽不能阻止决意冒险的专业窃贼, 但是可以防止在有机可乘时实施的犯罪。
- 采取额外的预防措施来保护便携计算机及掌上设备, 特别是当它们含有敏感信息的时候。可以考虑采用无线电控制的警报装置, 比如 TrackIT Corporation (<http://www.trackitcorp.com>)提供的设备, 这种装置在您和您的笔记本携带箱被意外地分开时就会发出声音。
- 工作时, 应该养成每次离开办公桌的时候都注销或是锁定计算机的习惯。偶然的窥探者即便不碰到键盘, 只是看到文件和文件夹的名称就能够得到很多的信息了。
- 小心那些试图通过观察您登录时手指的动作以窃取密码的“肩膀后面的偷窥者(shoulder surfer)”。安排一下您的工作空间使别人不会清楚地看到您的键盘。
- 使用带密码保护的屏幕保护程序。将屏幕保护程序设置为在短时间(不多于 10 分钟)没有动作之后就开始执行, 并且选择相应的选项使计算机退出屏幕保护程序继续工作时会显示出输入密码的提示。
- 将 FAT32 的磁盘转换成 NTFS 格式来防止窥探者使用软盘启动从而不经过登录就可以访问到数据文件。(关于进行转换的细节, 请参见第 2 章的 2.4.7 节“对所有驱动器使用 NTFS”)。
- 如果您的计算机上存放有极为敏感的数据, 可以考虑使用加密的文件系统(这方面的细节, 请阅读第 18 章“加密文件和文件夹”), 并且添置一台基于硬件的登录设备, 比如智能卡(smart card)或是生物信息识别系统。

上面的预防措施有些听起来太极端了吗? 不, 实际上, 这个建议的大多数内容是基本的常识。您肯定不会在晚上睡觉时使您的前门处于未锁的状态。那么为什么将您的个人电脑放置在不上锁的状态, 特别是当您知道可能会成为入侵者的人经常在旁边徘徊, 试探各个虚拟的门把手, 试图找到那些没有保护的计算机呢?



警告 只要您能够记住要设置保险的密码并且在不使用计算机时进行注销, 那么加密数据是防止窃贼的一个极好的方法。但是一定要确保有一份备用的密钥! 如果含有 Windows 系统文件的硬盘发生了任何事情, 您都必须能够替换密钥。如果不这样做, 即便您可以将加密的数据从备份中进行恢复, 您也会永久地被封锁在所有加密的文件之外。在考虑使用 Windows XP Professional 和 Windows 2000 内置的加密文件系统之前, 请阅读第 18 章“加密文件和文件夹”。

1.2.2 威胁 2: 被窃取的密码

对于绝大多数的计算机和加密的 Web 站点而言, 输入密码是证明您身份的惟一方法。如果有人借走、窃取或是猜到了您的密码, 这个人就可以获得对您的文件和网络资源的完全访问权。用您的密码登录后, 恶意的入侵者可以阅读您的电子邮件, 翻看您的敏感文件, 访问受保护的网路资源(如公司的数据库), 以及进行各种形式的破坏, 而留下您来收拾残局。

令人吃惊的是, Windows 最新、最安全的版本 Windows XP, 事实上在鼓励着懒惰的密码习惯。在一台没连接到 Windows 域的计算机上安装 Windows XP(Professional 或 Home Edition), 安装程序会创建具有