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和私人数据

[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。

北京市版权局著作权合同登记号：图 01-2003-0840 号

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.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？

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

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，这种开销也可能会是很大的。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 Wnidows 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和您有关，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% 都受到过来自内部的(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。

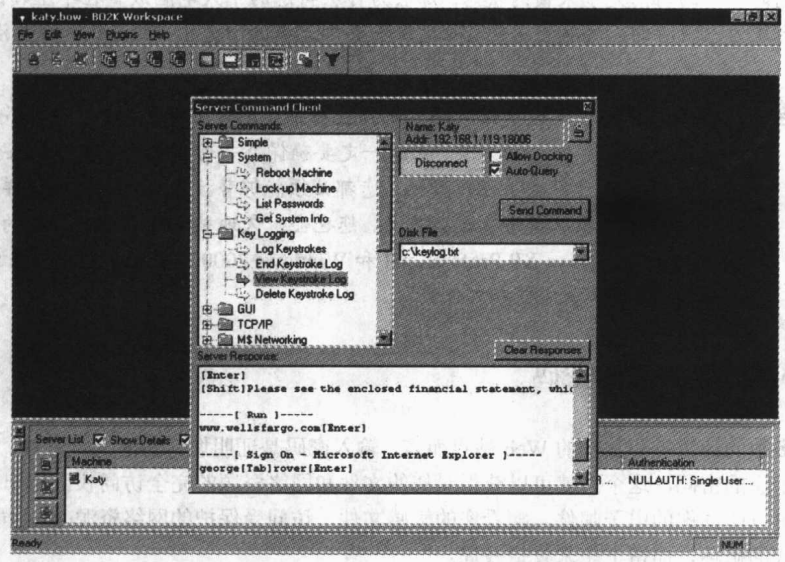

图 1.1　Back Orifice 的远程控制台

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，访问受保护的网络资源(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