Broadview
www.broadview.com.cn

微软MVP作品系列
——IT Professional

Microsoft Most Valuable Professional

Windows 安全指南

刘 晖 编著

MVP

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Windows 安全指南

Windows 安全指南

刘晖 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书分 4 部分介绍 Windows 安全问题。第 1 部分介绍有关 Windows 操作系统的安全问题：第 2 部分重点介绍局域网方面的安全问题：第 3 部分重点介绍如何防范目前层出不穷的间谍软件、恶意软件的传播和感染方式，以及防范办法；第 4 部分介绍 Windows 操作系其他安全问题。本书不仅仅介绍有关 Windows 本身的安全问题，还包含了一般用户在使用 Windows 操作系统完成日常工作过程中可能遇到的各种安全风险，以及解决和预防的办法。

本书的目标读者是使用 Windows 操作系统进行工作和娱乐的一般用户。即使完全没有计算机技术基础，只希望使用计算机完成自己工作的人，也完全可以通过本书了解如何操作才能提高计算机的整体安全性；对于希望“知其然，知其所以然”的人，将可以了解到一些深入的技术细节和原理，并通过这些信息更好地使用 Windows。

图书在版编目（CIP）数据

Windows 安全指南 / 刘晖编著. —北京：电子工业出版社，2008.2
（微软 MVP 作品系列）
ISBN 978-7-121-05688-8

I. W… II. 刘… III. 操作系统（软件），Windows－安全技术－指南 IV. TP316.7-62

中国版本图书馆 CIP 数据核字（2007）第 199167 号

责任编辑：李 冰
印 刷：北京东光印刷厂
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：28 字数：560 千字
印 次：2008 年 2 月第 1 次印刷
印 数：5000 册 定价：49.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

“微软 MVP 作品系列”丛书出版说明

“微软 MVP 作品系列”丛书的全部作者来自于历届微软最有价值专家，微软公司视所有的 MVP 为“最有价值合作伙伴”。电子工业出版社博文视点公司长期与微软最有价值专家有良好的合作，此次聚集力量，倾心为读者奉献一套涵盖系统、开发领域的各项微软公司核心技术的图书，希望每位读者都能从中受益。也希望对技术执着追求的您，踊跃参与微软最有价值专家的评选，也许下一个精彩来自于您！

微软最有价值专家（MVP）项目介绍

微软最有价值专家（MVP）是指具备一种或多种微软技术专业知识，并且积极参与在线或离线的社群活动，经常与其他专业人士分享知识和专业技能，受人尊敬、信任，而且平易近人的专家。

实际生活中，人们总是信任专家的建议和反馈。MVP 正是这样一群拥有丰富知识和实际经验的微软技术专家。他们不是微软的员工，但是非常乐于通过在线或离线社区的方式帮助技术人士。另一方面，微软公司时刻不忘倾听来自用户的意见反馈，不断开发新产品，改进技术，提高用户体验。MVP 代表来自社群的广大用户，他们的意见更能协助微软公司了解用户的真实需求。

Most Valuable Professionals（最有价值专家）是微软对上述专家在技术社群专业贡献的一种正式认同。该项目主要目的在于鼓励形成一个充满活力的全球性社群，使得微软和用户之间建立良好的相互关系，增进相互了解。目前主要策略为：

- 在全球范围内认可 MVP 并建立交流渠道——通过跨产品、服务和行业的广大社群，嘉奖有影响力和特殊贡献的专家，并赋予他们特殊的资源和权力。
- 贴近用户、提高体验——认可技术专家的特殊贡献，不论他们来自哪个领域、使用何种语言，致力于提高使用微软技术的亲身体验。
- 推动项目日臻完美——不断提高对技术专家的支持力度，在全球范围建立协调和沟通网络，增进微软和用户的相互了解。

该项目已经运作了 11 年，在全球 81 个国家拥有接近 3000 位最有价值专家。

谁是我们的微软最有价值专家（MVP）？

- 以微软技术为主题的作家、讲师、培训师。
- IT 业界的业内知名专业人士，通过印刷媒体、blog 或其他形式分享经验和观点。

- 参与和微软技术有关的项目，担任主要角色的技术和管理人员。
- 建立讨论微软技术的技术网站，担任主要角色的技术和管理人员。
- 参与微软中文新闻组，积极地帮助论坛用户解决疑难问题的技术论坛高手。
- 参与其他第三方的微软技术论坛，积极地帮助论坛用户解决疑难问题的技术论坛高手。

为什么要参与微软最有价值专家的评选？

- 成为微软全球 3000 位最有价值专家中的一员。

微软公司视所有的 MVP 为“最有价值合作伙伴”，目前全球仅有 3000 位 MVP。在 MVP 颁奖峰会上，您经常能够看见 Bill Gates, Steve Ballmer, Eric Rudder, Joe Peterson, Lori Moore 等微软的最高层领导出现在大会上，亲自向 MVP 致词。来自 MVP 的反馈、建议，一直都是微软高层和各个产品组极为重视的声音。

- 扩大您的专家关系网络。
- MVP 可以通过微软私有新闻组（private newsgroup）和 3000 多位世界各地的 MVP 在线交流。
- MVP 也可以通过中国地区的 MVP 邮件列表交流分享专业信息和资源。
- 分享微软最前沿的技术资源。
- 所有 MVP 将获赠价值人民币 32 000 元的 MSDN 光盘宇宙版或 TechNet 的一年免费订阅。
- 微软 MVP 可以在专有站点上下载微软最新的内部技术文档，访问合作伙伴级知识库（Partner Knowledge Base），并参加专门为 MVP 制作的在线学院培训。
- 微软总部的产品研发部门与 MVP 将保持密切的联系。MVP 将参与公司最新技术的审核和产品 Beta 测试，并可以通过特殊渠道对微软的各项产品、活动提出意见和建议。
- MVP 将被邀请参加微软公司在各地的大型市场活动，比如免费参加当年的 TechEd。
- 微软助您不断攀登新的职业高峰。
- 在本人允许的前提下，微软将在官方站点公开宣传 MVP 的个人信息，并在各类专业印刷媒体上开设 MVP 专栏，使 MVP 和 MVP 所在的企业更有知名度。
- MVP 能得到微软总部授予的全球统一的证书及精美纪念品。
- MVP 各地的项目主管会随时与 MVP 保持联系，协助 MVP 更好地获取资源和提供

反馈。

- 参与丰富多彩 MVP 的聚会。

年度 MVP 全球峰会是微软以最激动人心的方式，答谢最有价值专家做出的特殊贡献而举办的全球盛会。

我们时刻关注您的反馈

作为本书的读者，您是最重要的评论家和批评家。我们非常重视您的意见，并非常希望您告诉我们怎样才能做到最好。

对于本套丛书，我们组织了专门的项目团队，他们是——

组稿编辑：朱沭红　胡辛征　李冰　孙学瑛　高洪霞

市场推广：朱沭红　胡辛征　李冰　孙学瑛　高洪霞　谢丹丹　梁琪　刘琳

出版统筹：郭立

在本书的制作和推广过程中，还得到了许多热心的微软最有价值专家（MVP）、微软金牌讲师、微软特约讲师、博文视点的其他同事及各大网站站长和主编们的大力支持，在此表示感谢。电子工业出版社博文视点的同仁们欢迎读者提出自己的意见。

电子邮件：jsj@phei.com.cn

邮寄地址：北京万寿路 173 信箱（北京博文视点资讯有限公司）

邮政编码：100036

“微软 MVP 作品系列”优秀作者简介

排名不分先后

彭爱华 网名盆盆，四届微软最有价值专家、资深微软讲师、著名的 IT Pro 技术博客 ITECN 的站长（兼创始人）。参加过三次 Windows Vista 讲师培训、Windows Server 2008 专业讲师培训。在新加坡接受过由微软 Windows Vista 产品组提供的专门培训。在 2006 年 9 月的微软技术大会（Tech.Ed 2006）上担任讲师，并荣获最佳讲师第二名。应微软中国的邀请，担任《Windows Vista Product Guide》（产品手册）正式版的翻译工作，还担任该书中文版的技术审核工作。

王少葵 连续三届微软 Visual Developer - Visual C#方面最有价值专家（MVP），通过 MCP、MCDBA、MCSA、MCAD、MCSD 等多项微软认证，有 10 年 IT 行业从业经验，现为 ABB（中国）有限公司金属部高级工程师，为生产制造企业提供自动控制整体方案，与微软、宝信、用友等软件公司有良好的合作。

苏鹏 连任 2006 年、2007 年 Visual Developer-ASP.NET 最有价值专家（MVP），通过 MCP，MCSE，MCDBA 等多项认证考试。现为中国网通有限公司奥运项目部系统集成顾问，曾参与微软亚洲工程院软件测试组工作。担任过 MSN 测试工作。微软 webcast 平台讲师，荣获 2006 财年微软最具人气讲师称号。同时义务为广大开发爱好者提供邮件技术支持。2 年内回复邮件超过 5000 封，还通过了 GPMP 项目管理认证。

刘辉 微软 Asp.net 方面最有价值专家（MVP），有 10 年 IT 行业从业经验，现为厦门渊博科技有限公司总经理，与微软公司有良好的合作关系，并担任厦门 .NET 俱乐部主席、微软 MSDN 论坛 ASP.NET 版主。热衷于研究新技术，给企业提供完整的微软解决方案，给程序员及企业之间，程序员之间，建立沟通的桥梁并帮助.NET 程序员解决疑难问题。

高海峰 2007 年微软最有价值专家（MVP），2006 年、2007 年微软中国 MCT 年度排名全国第三、微软 WinTEC 社区活跃成员、国内首批.NET 3.0 开发技术专职讲师、微软院校计划实施讲师、微软中国 DPE 特约讲师。先后参与和主持研发了若干大型应用系统，包括高性能计算（HPC）、办公自动化（OA）、图像处理（Imaging）、计算机通信集成（CTI）等诸多领域，具备丰富的软件开发和项目管理经验。

前　言

很多人都认为，Windows 操作系统的安全性太差。其实对于新的 Windows 操作系统，例如 Windows XP 和 Windows Vista，系统的安全性已经得到了空前的加强，然而依然有很多人在使用这些操作系统的时候因为安全问题而受到损失，原因到底是什么？

其实在计算机安全方面，也一直存在着“木桶原理”，就像一只用木板拼成的木桶，桶里能装多少水，并不取决于最长的木板，而取决于其中最短的木板。可能操作系统本身已经很安全，但因为使用的人缺乏安全意识，也有可能导致操作系统在提高安全性方面所作的全部努力付之东流。

在现在的 Windows 操作系统中，几乎所有选项的默认设置都是以保证安全性为前提的。然而安全性和易用性永远都是对立的，如果要实现更高的安全性，在易用性方面肯定会大打折扣。因此很多人在使用过程中，为了贪图方便，往往会修改一些默认的系统设置，导致系统变得不够安全。而一旦遇到安全性问题，往往会觉得这是操作系统做得不好，并不会想起正是因为自己修改的设置导致了一系列的安全问题。

对于使用 Windows 的大部分一般用户，他们并不需要对计算机有多么高深的了解，他们只需要像使用一般电器那样打开计算机，然后学习、工作或者娱乐，并在用完之后直接关掉就可以，Windows 可以很好地满足这些人的需求。也许有更加安全的操作系统，但对于大部分用户来说，这类系统无论是安装、设置还是使用，都存在不小的难度，甚至可能根本无法在这些操作系统上完成自己需要的工作。因此大部分人依然在使用 Windows，并希望努力让 Windows 变得更安全，或者至少不要因为自己的疏忽带来安全问题。

那么一般来说，如果希望自己的计算机更安全，我们应该从哪些方面着手？

- 随时保持操作系统和应用程序安装了最新的补丁：现在的软件越来越复杂，因此存在安全漏洞也是在所难免的。因此无论是操作系统还是一般应用程序，只要有安全方面的更新，我们就应该尽快安装，只有这样才能保护我们的计算机不被入侵或攻击。
- 给每个使用电脑的人创建自己的账户，并设置强密码：这样每个人的使用环境将会被隔离起来，并且我们可以根据不同的需要给不同用户指派不同的特权。这样才可以保证每个用户只能做自己需要的工作，而不会“越权”。同时强密码的存在也可以保证系统和数据不被未经授权的人访问。
- 安装反病毒软件、网络防火墙及反间谍软件：这三类软件可以保护我们的系统不被攻击和感染，但也不能忘了还得经常更新这类软件的库文件，只有这样才能监测到最新类型的攻击或病毒。
- 对于电子邮件中的可疑附件绝对不能轻易打开：很多病毒在通过电子邮件传播，有时候可能看似来自我们朋友的邮件，其实可能是对方感染病毒后不知情的情况下发

送的。因此在收到任何人发来的邮件时都要谨慎，在打开之前最好使用反病毒软件彻底检查。

- 小心朋友通过 IM 软件发来的网页链接：如果朋友通过 IM 软件发来了某个网页的链接，在打开前最好先问问对方是否发送过这样的东西，因为有时候这可能是对方系统感染了病毒后自动发送的，如果直接点击这样的链接，我们的系统也有可能会中毒。
- 安装软件一定要小心：现在的很多软件的安装程序中都捆绑有其他非必要的软件，这类软件一旦安装，往往很难卸载，并且可能会给系统中带来很多麻烦。因此在安装软件的时候一定要小心查看所有选项，并尽量不要安装来自陌生网站的软件。

其实现在很多人已经开始意识到这个问题，但关键在于，并不是每个人都能充分理解系统中不同选项对于安全性的影响。而且很多人对于目前层出不穷的新安全问题也并不了解，因此本书的主要目的就是向大家介绍这些选项，并通过实例告诉大家在网络上遇到这类问题后应该怎么办。

本书主要内容

在本书的第 1 部分，我们介绍了有关 Windows 操作系统本身的安全问题，毕竟 Windows 是基础，只有做好 Windows 本身的安全问题后才可以考虑其他方面的安全。在第 1 章，我们可以了解到如何将 Windows 的更新程序直接集成到安装文件里，这样安装好的系统就已经包括了所有需要的更新，因此更方便，也更安全；另外还可以了解到在安装 Windows 的过程中需要注意的安全问题，以及安装好后需要留意的设置。在第 2 章，我们会详细了解到 Windows 中有关用户账户的内容，毕竟用户账户机制才是实现 Windows 安全性的基础，而在这一章我们将可以了解到如何创建和管理用户账户，以及 Windows Vista 中新增的用户账户控制功能有什么用。在第 3 章，则重点介绍了 Windows 中上百条的安全策略，因为通过这些策略可以改变 Windows 在安全性方面的很多选项，然而长时间以来，很少有人注意过这里，因此本书对其中一些策略进行了详细的介绍。在第 4 章，我们将了解到对 Windows 系统进行更新的必要性，以及如何更好地进行更新。在第 5 章，我们可以了解如何利用 NTFS 文件系统的各种特性保护文件安全，例如我们可以设置访问权限，或者直接使用 EFS 功能对文件进行加密。另外还可以了解到 Office 文档的安全问题，以及文件被彻底删除和误删除后的恢复方法。

在本书的第 2 部分，我们重点关注的是本地局域网方面的安全问题。其中在第 6 章，我们可以了解到使用无线 WiFi 网络时可能遇到的安全问题，以及如何避免因为这些问题受到攻击。在第 7 章，我们可以了解到在使用局域网共享文件时需要注意的安全问题，以及如何通过共享权限和 NTFS 权限配合限制网络共享的访问。在第 8 章，则介绍了 Windows 自带的 Windows 网络防火墙的使用方法。

本书的第 3 部分，重点介绍了如何防范目前层出不穷的间谍软件及恶意软件的传播和感染方式，以及防范的办法。在第 9 章，我们会介绍如何在浏览网页、收发邮件、网络聊天以及安装软件的时候保护自己系统安全。在第 10 章，我们可以了解到如何使用反病毒软件保护自己

的系统安全。在第 11 章，我们可以了解到如何防范恶意软件。

本书的第 4 部分则介绍了一些不属于上述类别的问题。在第 12 章，我们可以了解到如何使用 Windows Vista 中新增的家长控制功能对小孩使用计算机进行限制和约束。在第 13 章，我们可以了解到如何利用 Windows Vista 中新增的 BitLocker 功能保护系统不受脱机攻击。在第 14 章，则可以了解到如何利用系统自带的或者第三方程序备份自己的文档或整个系统，并在需要的时候进行还原。

本书特色

虽然这本书的名称是《Windows 安全指南》，然而本书并不仅仅介绍有关 Windows 本身的安全问题，还包含了一般用户在使用 Windows 操作系统完成日常工作的过程中可能遇到的各种安全风险，以及解决和预防办法。

因此通过阅读本书，我们将可以保证自己的计算机整体环境更安全，也更可靠。

读者对象

本书的目标读者是使用 Windows 操作系统进行工作或娱乐的一般用户。即使完全没有计算机技术基础，只希望使用计算机完成自己工作的人，也完全可以通过本书了解如何操作才能提高计算机的整体安全性；而对于希望“知其然，知其所以然”的人，将可以了解到一些深入的技术细节和原理，并能通过这些信息更好地使用 Windows。

致谢

本书的编写过程得到了电子工业出版社博文视点郭立总经理、李冰编辑，以及我的家人刘宝良、王凤霞、刘斯琰、刘步庭等人的大力帮助，在这里再次对这些人的帮助表示衷心的感谢，没有你们的帮忙，本书的顺利出版是不可能的。

在写这本书的时候我已经尽了最大的努力保证在技术和文字上没有什么错误或者疏漏，但由于水平有限，难免会出现一些错误或者不足，还望见谅。如果在阅读本书的过程中你有什么疑难问题，请发邮件到 jsj@phei.com.cn，并使用“《Windows 安全指南》技术问题”作为邮件主题，方便及时处理。

刘晖

2007 年 12 月

目　录

第 1 部分　Windows 安全

第 2 部分 网络安全

第 3 部分 病毒和恶意软件

第 4 部分 其他安全问题

窍门目录

1

第 1 部分 Windows 安全

对于计算机来说，操作系统是其他所有应用的基础。无论使用计算机做什么，如果操作系统不安全，那么其他应用和数据就会受到影响。因此，对于需要更安全计算环境的用户，首先需要保证 Windows 的安全。

然而长久以来，因为各种原因，很多人对 Windows 的安全性有一个误解，认为和其他操作系统相比，Windows 不够安全，其他系统更安全。其实这个观点在很大程度上都是站不住脚的。

首先我们必须知道，Windows 是全世界使用率最高的操作系统，很多人都在研究和破解 Windows 的各种安全功能，以达到各自的目的。设想这样一种比较极端的情况：有一种全新的操作系统，存在比较严重的漏洞，但全世界只有一两个人在使用这个系统，并且主要用于娱乐用途，那么会有人对这种操作系统的漏洞感兴趣吗？很显然，不会，因为没有价值。

那么 Windows 呢？情况有些复杂。很多人在用 Windows，我们会在 Windows 下进行网络理财、股票交易，会在 Windows 下处理公司的财务数据，会在 Windows 下撰写新计划的企划书，会在 Windows 下玩网络游戏，打造可以卖钱的极品装备…… 总之在 Windows 下进行了太多有价值的应用，因此研究 Windows 各种功能和漏洞的人最多，进而 Windows 上出现的安全问题也最容易被怀有恶意的人利用，这些因素更让 Windows 显得不够安全。

其次，Windows 是由人编写的，一套非常庞大的操作系统。而只要是人就难免犯错误，再加上数量庞大的代码，因此 Windows 下暴出安全漏洞也并不奇怪。其实其他任何软件产品也是如此，只不过有些软件的用户数量太少，因此问题不那么突出罢了。不过好在微软有一套相当成熟的补丁管理机制，可以在发现新的安全漏洞后的最短时间里发布相应的补丁程序。我们只需要及时安装新的补丁程序，就可以将风险扼杀在摇篮中。

最后，为了保证一定的易用性，在 Windows 中，很多默认的设置都是不够安全的。虽然在 Windows XP 和 Windows Vista 中这种情况有所好转，不过问题依然存在。更重要的是，系统的安全性很大一部分情况下都取决于使用这套系统的人，不管多安全的操作系统，如果让不懂技术的人使用，都有可能因为改变了设置或者错误的使用习惯而导致原本安全的系统变得不再安全。

因此，就算我们选择使用 Windows，也不用因为上述内容而沮丧。因为通过本书我们会了解到怎样进一步提高 Windows 的安全性，同时本书还会介绍怎样让我们在 Windows 下进行的其他操作更安全。