

快速掌握 Windows^{xp} SP2 上网安全技巧

Time创作室 编著

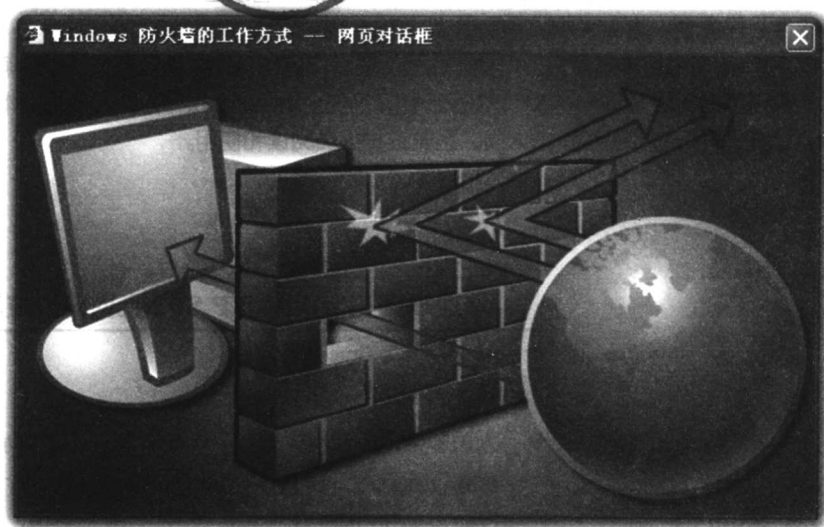


TP316.86
165

快速掌握 Windows^{xp} SP2 上网安全技巧



Time创作室 编著



北京信息工程学院图书馆



Z308291

人民邮电出版社

SJS353/06

图书在版编目(CIP)数据

快速掌握 Windows XP SP2 上网安全技巧 / Time 创作室编. —北京: 人民邮电出版社, 2005.1
ISBN 7-115-12939-8

I. 快... II. T... III. 窗口软件, Windows XP—安全技术 IV. TP316.7

中国版本图书馆 CIP 数据核字 (2004) 第 128641 号

内 容 提 要

我们在日常工作中都离不开网络。网络,不管是局域网还是 Internet,带给我们便利的同时也带来了各种各样的安全隐患和垃圾信息。病毒、蠕虫和特洛伊木马随时对我们的计算机构成威胁;黑客也在伺机入侵计算机、窃取重要数据;浏览网页时经常出现恼人的弹出广告、浮动广告;打开电子邮箱,可能已被垃圾邮件塞满;系统中可能还有一些无法察觉的间谍软件和广告软件在私下运行。Windows XP SP2 版的推出,在操作系统安全性方面迈出了一大步,能使计算机在复杂网络环境中更加安全。

本书从实用的角度出发,详细介绍了 Windows XP SP2 的安全特性,讲述了在 Windows XP SP2 下的各种网络安全防护技巧,如监视和清除病毒、拒绝黑客攻击、防止不当陷阱、拦截网上广告窗口、阻止垃圾邮件、保护个人隐私等。

本书内容丰富翔实,可操作性强。在写作风格上力求通俗易懂,避免照本宣科式的讲解,有利于读者快速掌握利用 Windows XP SP2 保护计算机安全的原理、操作方法和技巧。本书适合 Windows XP SP2 用户、计算机爱好者、工程技术人员、系统维护人员阅读和使用。

快速掌握 Windows XP SP2 上网安全技巧

◆ 编 著 Time 创作室

责任编辑 苏 欣

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@ptpress.com.cn

网址 <http://www.ptpress.com.cn>

读者热线 010-67132692

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

◆ 开本: 787×1092 1/16

印张: 14.75

字数: 348 千字 2005 年 1 月第 1 版

印数: 1—5 000 册 2005 年 1 月北京第 1 次印刷

ISBN 7-115-12939-8/TP · 4357

定价: 28.00 元

本书如有印装质量问题,请与本社联系 电话: (010) 67129223

前言

Windows XP SP2 (本书简称 SP2) 为用户的计算机建立了可靠的默认安全性设置, 有效地保护计算机不受黑客、病毒及其他安全问题的困扰。同时 Windows XP SP2 还添加了众多新的功能, 能够给用户提供更多的方便。Windows XP SP2 的发布表明微软操作系统的安全性能进入了一个“主动防护”的新阶段。Windows XP SP2 版发布以前的 Windows XP 正版用户都可以免费升级到 SP2 版, 使自己的计算机在日益复杂的网络环境中更加安全。

SP 是 Service Pack (服务包) 的缩写, SP2 表示这个服务包是 Windows XP 的第 2 个服务包, 也就是目前最新的服务包。服务包提供操作系统中各种错误修复补丁、安全漏洞补丁, 是微软操作系统技术支持服务的一项传统内容, Windows XP SP2 版的特别之处在于其重点从修复错误转移到提供更多的安全保障上面来, 无疑带给用户更好的安全体验。Windows XP SP2 已经不再是简单意义上的服务包, 它融合了很多精心研发的先进技术。Windows XP SP2 将以“未雨绸缪”的全新安全理念, 为用户构筑安全的防护体系。

虽然 Windows XP SP2 安全性大大增加, 默认的安全设置也能增强对用户计算机的保护, 但是用户绝对不能掉以轻心, 以为升级到 SP2 版就可以高枕无忧了。目前无论是局域网还是 Internet 上, 计算机所面对的攻击日趋复杂化, 用户如果了解各种攻击的机制, 没有安全意识, 不采用规范的安全操作方法, 自己的计算机随时都会受到威胁。

本书对 Windows XP SP2 的新安全特性进行透彻讲解的同时, 对计算机在网络环境中可能遭受的各种攻击机制进行了分析和示例, 这样就有利于读者增强安全意识、培养安全的操作习惯, 有针对性地使用 Windows XP SP2 防范各种安全问题, 保护自己的计算机。

虽然 Windows XP SP2 已经是微软公司提供的最安全的操作系统了, 不借助防病毒软件、防火墙软件、清除木马软件等工具, 还是无法保证系统的安全。本书对这些可以和 Windows XP SP2 结合起来抵御各种攻击的工具软件的使用和设置

也进行了详细的说明。

本书编排上首先是介绍 Windows XP SP2 本身的新安全特性和安全工具,帮助读者理解操作平台的变化,然后描述了在网络环境下计算机的各种安全问题及在 Windows XP SP2 下的解决方案,每种安全问题都列举了实例,给出一些操作技巧和注意事项。读者通读本书后,在计算机运行中遇到各种情况,都可以举一反三,从容处理。

本书以 Windows XP SP2 的安全特性和网络环境下的各种攻击威胁为主线,内容安排上循序渐进。读者只要具备基本的计算机知识和 Windows XP 使用经验就不会有阅读障碍。

本书共分为 9 章,涉及的内容包括 Windows XP SP2 全新的网络安全特性,Windows XP SP2 下功能强大的安全工具,Windows XP SP2 安装升级过程及故障排除,监视和清除病毒,抵御黑客的攻击,防止木马陷阱,拦截网上广告窗口,阻止垃圾电子邮件,保护个人隐私等。

在阅读本书的过程中,读者如果遇到问题,或者有什么意见和建议,可以访问 Time 创作室网站,在网站论坛或留言本上与我们联系。也可以使用电子邮件与我们联系,地址是: webmaster@timestudio.net。我们不仅欢迎您就本书提出问题,也欢迎您询问其他与电脑有关的问题。

由于编写时间仓促,加上笔者水平有限,书中难免会有欠妥之处,恳请广大读者和专家批评指正。

Time创作室
2004 年 10 月

目 录

第 1 章	SP2 全新的网络安全特性	1
1.1	SP2 概述	2
1.1.1	操作系统需要保持最新	2
1.1.2	Windows XP 修补和更新	2
1.1.3	Service Pack 2 的新特点	4
1.2	IE 弹出窗口阻止器	5
1.2.1	如何设置 IE 阻止弹出窗口	6
1.2.2	其他功能	7
1.3	增强的下载监控功能	7
1.3.1	下载文件保存时的警示	7
1.3.2	阻止来自特定发布者的下载内容	9
1.3.3	安全状态图标	10
1.3.4	阻止未请求文件的下载	11
1.4	Internet Explorer 信息栏	12
1.4.1	什么时候可以看到信息栏	13
1.4.2	如何使用信息栏	13
1.4.3	关闭信息栏	14
1.4.4	不使用信息栏阻止文件下载	14
1.4.5	信息栏显示内容及操作	15
1.5	加载项管理器	18
1.5.1	加载项管理器概述	18
1.5.2	加载项管理	19
1.5.3	加载项管理器工作模式	22
1.5.4	加载项崩溃检测	23
1.6	其他浏览安全功能	23
1.6.1	二进制行为安全设置	23
1.6.2	ActiveX 安全模型应用范围更广	24
1.6.3	锁定本地计算机区域	24
1.6.4	应用 MIME 处理	25
1.6.5	对象缓存特性	26
1.6.6	阻止区域提升	26

1.6.7	窗口限制.....	27
1.6.7.1	使用脚本对 Internet Explorer 窗口重新定位.....	27
1.6.7.2	使用脚本改变 Internet Explorer 窗口的大小.....	27
1.6.7.3	利用脚本管理 Internet Explorer 状态栏.....	28
1.6.7.4	Internet Explorer 弹出窗口的位置.....	28
1.7	电子邮件安全处理.....	29
1.7.1	纯文本模式.....	29
1.7.2	不下载外部 HTML 内容.....	30
1.7.3	附件管理器.....	32
第 2 章	功能强大的安全工具.....	35
2.1	Windows 安全中心.....	36
2.1.1	Windows 安全中心的作用.....	36
2.1.2	深入理解安全中心.....	37
2.1.2.1	对防火墙的监控.....	37
2.1.2.2	对自动更新的监控.....	38
2.1.2.3	对防病毒软件的监控.....	39
2.1.3	禁用安全中心警报.....	39
2.2	Windows 防火墙.....	41
2.2.1	防火墙基础知识.....	41
2.2.2	Windows 防火墙新特性.....	43
2.2.3	防火墙安全警报.....	43
2.2.4	设置防火墙选项.....	44
2.2.4.1	设置常规选项.....	45
2.2.4.2	设置例外选项.....	46
2.2.4.3	高级选项设置.....	50
2.2.5	防火墙的组策略部署.....	51
2.3	自动更新增强功能.....	52
2.3.1	新 Windows Update 提供的服务.....	53
2.3.2	更新功能的新特性.....	54
2.3.3	新自动更新界面.....	55
2.3.4	内容组织和导航方式.....	56
2.3.5	可支持性.....	57
2.3.6	使用自动更新.....	57
2.3.7	常见问题.....	59
2.4	数据执行保护.....	60
2.4.1	数据执行保护的概念.....	61
2.4.2	数据执行保护的新功能.....	61

2.4.3	兼容性问题.....	62
2.4.4	软件 DEP	63
2.5	Windows Messenger 更安全	64
2.5.1	软件功能概述.....	64
2.5.2	阻止传输不安全的文件.....	64
2.5.3	要求用户显示名称.....	65
2.5.4	Windows Messenger 和 Windows 防火墙.....	66
第 3 章	SP2 安装升级过程及故障排除.....	67
3.1	安装前注意事项.....	68
3.1.1	了解最低系统需求.....	68
3.1.2	什么情况下可升级.....	69
3.1.3	检查硬件和软件兼容性.....	69
3.1.4	获得网络信息.....	70
3.1.5	备份文件.....	71
3.1.6	其他重要准备措施.....	72
3.1.7	规划安装方式.....	72
3.2	安装和设置过程.....	73
3.2.1	全新安装和设置.....	73
3.2.2	旧版系统升级注意事项.....	77
3.2.2.1	MS-DOS 升级注意事项	77
3.2.2.2	Windows 9X 升级注意事项	78
3.2.2.3	Windows 2000 升级注意事项	80
3.2.3	SP2 软件包升级步骤及注意事项.....	80
3.2.3.1	升级步骤.....	80
3.2.3.2	升级注意事项.....	82
3.3	安装问题及解决.....	83
3.3.1	干净启动能解决部分问题.....	83
3.3.2	无法自动更新 SP2 的解决方案.....	85
3.3.3	安装过程中遇到文件复制错误	87
3.3.4	计算机挂起或停止响应并出现黑屏	87
3.3.5	获得 Windows XP 启动软盘	88
3.3.6	安装 SP2 未完成并无法启动.....	89
3.3.7	激活 SP2 的问题	90
3.4	卸载 SP2	91
3.4.1	用控制面板卸载 SP2	91
3.4.2	命令行方式卸载 SP2	92
3.5	制作集成安装 CD	93

第 4 章 监视和清除病毒	97
4.1 计算机病毒概述	98
4.1.1 计算机病毒的演变	98
4.1.2 什么是恶意软件	99
4.1.3 特洛伊木马	100
4.1.4 蠕虫	101
4.1.5 病毒	102
4.1.6 恶意软件的特征	103
4.1.6.1 目标环境	103
4.1.6.2 携带者对象	103
4.1.6.3 传输机制	104
4.1.6.4 负载	105
4.1.6.5 触发机制	106
4.1.6.6 防护机制	107
4.1.7 防病毒软件	107
4.1.8 恶意软件典型生存期	108
4.2 令人厌恶的非恶意软件	109
4.2.1 玩笑软件	109
4.2.2 恶作剧	110
4.2.3 网上欺诈	110
4.2.4 垃圾邮件	110
4.2.5 间谍软件	111
4.2.6 广告软件	111
4.2.7 Internet Cookie	111
4.3 如何在 Windows XP 中防御病毒	112
4.3.1 应用安全更新	112
4.3.2 减少攻击面	113
4.3.3 启用 Windows 防火墙	114
4.3.4 安装防病毒软件	114
4.3.5 测试漏洞扫描程序	115
4.3.6 使用最少特权策略	117
4.3.7 限制未授权的应用程序	117
4.3.8 应用程序的防病毒设置	118
4.3.8.1 电子邮件客户端	118
4.3.8.2 桌面应用程序	120
4.3.8.3 即时消息应用程序	121
4.3.8.4 Web 浏览器	122

4.3.8.5 对等应用程序.....	123
4.4 在 SP2 中设置防病毒软件.....	124
4.4.1 查明是否安装了防病毒软件.....	124
4.4.2 安全中心病毒防护报告.....	126
4.4.3 无法识别时取消状态监视.....	127
4.4.4 病毒防护状态与应对.....	128
第 5 章 防止黑客的攻击.....	131
5.1 黑客概述.....	132
5.1.1 黑客的含义.....	132
5.1.2 “怪客”与“骇客”.....	132
5.1.3 黑客的形成.....	133
5.1.4 黑客的应具备技能.....	133
5.1.4.1 程序设计基础.....	133
5.1.4.2 了解并熟悉各种操作系统.....	133
5.1.4.3 互联网的全面了解与网络编程.....	134
5.1.5 总结.....	134
5.2 远程攻击和缓冲溢出.....	134
5.2.1 远程攻击.....	134
5.2.1.1 收集目标信息.....	134
5.2.1.2 关于 finger 查询.....	135
5.2.1.3 关于操作系统.....	135
5.2.1.4 进行测试.....	135
5.2.1.5 各种相关工具的准备.....	135
5.2.1.6 攻击策略的制定.....	136
5.2.1.7 扫描结束后.....	136
5.2.2 缓冲溢出.....	137
5.2.2.1 缓冲溢出的概念与原理.....	137
5.2.2.2 缓冲溢出的危害.....	137
5.2.2.3 缓冲溢出漏洞及攻击.....	137
5.2.2.4 缓冲区溢出的保护方法.....	138
5.3 黑客常见破解及攻击手法.....	138
5.3.1 炸弹攻击.....	138
5.3.1.1 邮件炸弹.....	139
5.3.1.2 聊天室炸弹.....	139
5.3.1.3 其他炸弹.....	140
5.3.2 获取密码的几种方法.....	140
5.3.2.1 穷举法与字典穷举法.....	140

5.3.2.2	密码文件破解法.....	140
5.3.2.3	特洛伊木马法.....	141
5.3.3	网络监听.....	142
5.3.3.1	网络监听的原理.....	142
5.3.3.2	网络监听被黑客利用的危害	143
5.3.3.3	检测网络监听的方法	144
5.3.4	拒绝服务攻击.....	144
5.3.4.1	拒绝攻击服务的类型	144
5.3.4.2	针对网络的拒绝服务攻击	145
5.3.5	DDoS 攻击.....	146
5.4	黑客常用工具.....	146
5.4.1	黑客工具概述.....	146
5.4.2	密码破解工具.....	147
5.4.2.1	Soft-ICE	147
5.4.2.2	Web Cracker 4.....	147
5.4.2.3	EmailCrack	149
5.4.3	远程控制工具.....	150
5.4.3.1	Back Orifice 2000	150
5.4.3.2	网络神偷.....	151
5.4.4	网络监听工具.....	153
5.4.4.1	Winshell	153
5.4.4.2	Sniffer Pro 4.7	153
5.4.5	踢人工具.....	153
5.4.5.1	WinNuke	153
5.4.5.2	Teardrop	154
5.4.6	字典制作工具.....	154
5.4.6.1	万能钥匙 xkey.....	154
5.4.6.2	易优超级字典生成器	154
5.5	系统漏洞.....	155
5.6	在 Windows XP 下防止黑客攻击	155
5.6.1	使系统保持最新.....	155
5.6.2	安装防病毒软件.....	156
5.6.3	安装防火墙软件.....	156
5.6.4	不运行来历不明程序.....	156
5.6.5	知己知彼方能防身.....	157

第 6 章 防止木马陷阱 159

6.1	特洛伊木马的传播形式.....	160
-----	-----------------	-----

6.1.1	物理地复制木马.....	160
6.1.2	隐藏在下载软件中.....	160
6.1.3	电子邮件附件.....	161
6.1.4	聊天室或其他哄骗方式.....	161
6.1.5	即时消息传递服务.....	161
6.1.6	网页木马.....	161
6.2	特洛伊木马的种类.....	162
6.2.1	玩笑木马程序.....	162
6.2.2	破坏性的木马程序.....	162
6.2.3	盗取重要信息的木马程序.....	163
6.2.4	远程访问的特洛伊木马.....	163
6.3	黑客编写特洛伊木马的方式.....	164
6.4	防范特洛伊木马.....	165
6.4.1	防范的基本常识.....	165
6.4.2	还原程序.....	165
6.4.3	防病毒软件.....	168
6.4.4	防火墙软件.....	168
6.4.5	反特洛伊木马程序.....	169
6.4.6	安全性总结.....	170
第 7 章	拦截网上广告窗口	171
7.1	常见的网络广告形式.....	172
7.1.1	传统网络广告形式.....	172
7.1.2	弹出广告窗口.....	174
7.1.3	信使服务窗口.....	175
7.1.4	插件安装弹出窗口.....	178
7.1.5	浮动广告窗口.....	180
7.1.6	遮幅广告.....	181
7.1.7	其他网上广告形式.....	182
7.2	Windows XP SP2 如何应对.....	184
7.2.1	引子.....	184
7.2.2	应对手段.....	185
7.2.2.1	阻止弹出窗口.....	185
7.2.2.2	阻止信使服务窗口.....	186
7.2.2.3	阻止插件安装弹出窗口	186
7.2.2.4	无法阻止其他网上广告	186
7.3	用户该如何设置.....	186
7.3.1	允许任何网站的弹出窗口.....	187

7.3.2	显示已阻止的弹出窗口.....	187
7.3.3	允许特定网站上的弹出窗口	188
7.3.4	阻止任何弹出窗口.....	189
7.3.5	其他常见问题.....	189
7.4	功能更强的拦截工具.....	190
7.4.1	Google 工具栏.....	191
7.4.2	广告杀杀杀 (Ad Blocker)	193
7.4.3	Alexa 工具栏	194
7.4.4	3721 上网助手.....	195
第 8 章	抵制垃圾电子邮件	199
8.1	垃圾邮件概述.....	200
8.1.1	垃圾邮件的定义.....	200
8.1.2	垃圾邮件起源.....	200
8.1.3	垃圾邮件发展状况.....	201
8.1.4	垃圾邮件渠道和技术.....	202
8.1.5	垃圾邮件的危害.....	203
8.1.6	抵制垃圾邮件.....	204
8.2	阻止垃圾邮件.....	205
8.2.1	反垃圾邮件常识性技巧.....	205
8.2.2	邮箱的反垃圾设置.....	206
8.2.3	收发邮件客户端设置.....	208
8.2.4	防病毒软件反垃圾邮件.....	210
8.2.5	反垃圾邮件专用软件.....	211
8.2.6	未来技术发展.....	212
8.3	通用反垃圾邮件技术.....	213
8.3.1	实时黑名单技术.....	213
8.3.2	邮件过滤技术.....	214
第 9 章	保护个人隐私	215
9.1	个人隐私的泄漏风险.....	216
9.1.1	风险无处不在.....	216
9.1.2	IP 地址锁定计算机	216
9.1.3	Cookies 滥用.....	217
9.1.4	病毒、木马、间谍软件.....	217
9.1.5	网络监听.....	218
9.1.6	远程控制.....	218

9.1.7	黑客攻击.....	218
9.1.8	总结.....	218
9.2	保护个人隐私.....	219
9.2.1	管理 Cookie	219
9.2.2	清空“历史记录”	220
9.2.3	防止非法使用.....	221
9.2.4	谨慎输入真实信息.....	221
9.2.5	防病毒和防火墙软件.....	221

第1章

SP2 全新的网络安全特性

将最结果要需知悉知悉

本章要点

- ◎ IE 弹出窗口阻止器
- ◎ 增强下载监控功能
- ◎ IE 信息栏的作用
- ◎ 加载项管理器
- ◎ 电子邮件安全处理

随着 Windows XPSP2 版本的推出, Windows XP 在保护个人计算机安全方面达到了一个新的高度。在 Windows XP SP2 版本中融合了许多先进的安全防护技术, 以“主动防护”的全新安全理念, 为用户构筑安全的防护体系, 能真正实现个人信息安全。本章将先给读者理清几个基本概念, 然后重点谈谈 Windows XP 在 Internet 浏览及通信方面都有哪些安全措施, 是如何保证个人信息安全的。

1.1 SP2 概述

SP2 是 Service Pack (服务包) 2 的英文缩写。许多读者可能都对 Windows XP 这个名称很熟悉, 但是对 Service Pack 2 这个名称的含义不了解, 也不知道它和 Windows XP 之间的关系。本书基本上是以 Windows XP 的 SP2 版本进行讲解的, 下面就先给大家理清一些相关的概念。

1.1.1 操作系统需要保持最新

操作系统是用户和计算机硬件系统之间的接口, 或者说是协调者, 是其他应用程序的支撑环境, 可以说是所有计算机资源 (包括硬件和软件) 的管理者, 通过它, 用户可以操纵计算机, 实现各种计算和应用, 例如从事科学研究、办公甚至娱乐。

目前微软公司的 Windows 系列操作系统占据了个人计算机操作系统的绝大多数市场, 随着计算机软硬件技术的发展变化, Windows 也从早期的 Windows 3.X 逐步升级到 Windows 9X, 直至升级到了目前的 Windows XP。Windows 最初版本发展到目前的 Windows XP 经历了十多年的时间。每一个操作系统从开始研发到调试成熟, 直至最终包装上市, 都需要几年的时间, 这相对于飞速发展的计算机技术而言, 其实是一个漫长的时间。在新操作系统还没上市之前, 如果旧操作系统无法完全切合新技术的需要或用户的需求, 往往就要进行小的改进和修正。根据惯例, 这样的改进和修正都是免费提供给购买了正版产品的用户的。

近几年的操作系统功能强大, 结构非常复杂, 源代码达到数千万行, 开发过程中要数百甚至上千程序员协同完成, 开发周期也往往很长, 出现某些缺陷、漏洞造成系统不稳定、有安全隐患或功能不完整是不可避免的, Windows XP 也是如此。况且随着计算机软硬件技术的飞速发展, 操作系统作为软硬件工作的平台也必须不断调整更新才能使软硬件更好的工作。自从 Windows XP 正式问世以来, 微软公司就不断提供修补程序、驱动程序和安全更新程序, 以完善和增强 Windows XP 的功能。

1.1.2 Windows XP 修补和更新

Windows XP 问世已经 2 年多了, 随着计算机软硬件技术的发展, 这套操作系统本身也在不断发展完善, 微软公司不断提供有关 Windows XP 的各种 Service Pack、修补程序、安全补丁程序等, 这些操作系统修补程序进一步扩展或增强了系统功能, 增加了系统安全性和稳定性。

早在 Windows 9X 时代, Windows 操作系统中就具有“Windows Update (Windows 更新)”的功能,通过用户手工或系统自动更新,操作系统总能保持在最新状态。在 Windows XP 中可以设置系统自动更新,也可以通过“开始”>“所有程序”>“Windows Update”链接访问 Windows 更新网站,如图 1.1 所示,查找自己需要的更新组件并进行安装。

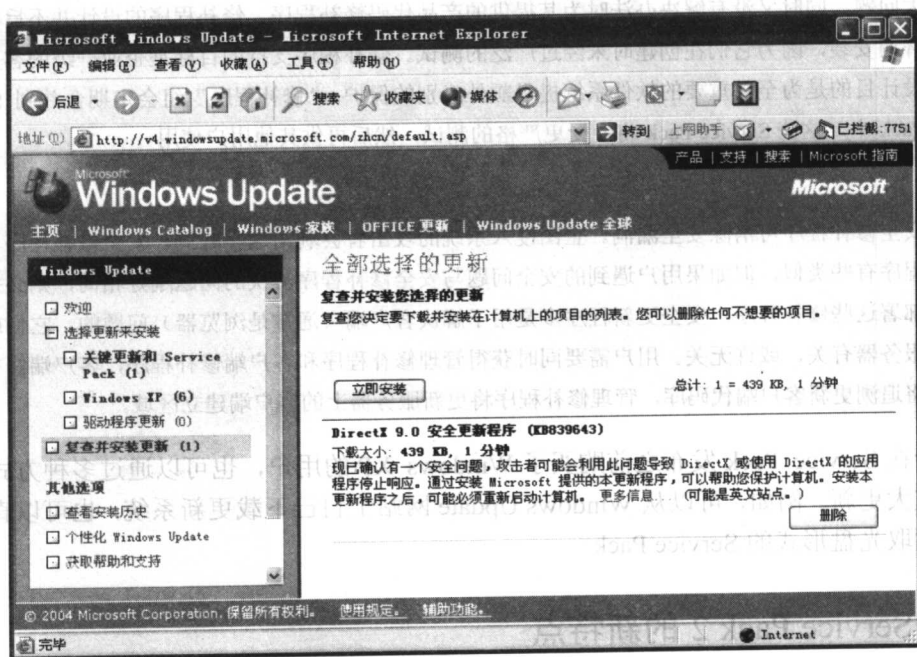


图 1.1 Windows 更新网站

自从 Windows XP 发布以来,每隔几个星期,甚至每隔几天或几个小时,微软就会在 Windows 更新网站上发布相关的各种修补程序,以解决系统漏洞、安全问题、功能缺陷等,Service Pack 是各种修补程序的集合,每隔一段比较长的时间会发布一个 Service Pack 版本,可以说 Service Pack 是阶段性的大规模的系统更新。

Service Pack 更正已知问题并提供扩展操作系统功能的工具、驱动程序和更新,这些功能扩展包括产品发布之后开发的增强功能,它们使用户能得到最新代码库。Service Pack 使 Windows XP 保持最新状态,Service Pack 的更新组件、系统管理工具、驱动程序和附加组件被方便地捆绑在一起,易于下载。

Service Pack 是特定于软件产品的,因此不仅仅 Windows XP,许多软件产品都有其单独的 Service Pack,例如 Office 2003 或金山词霸等。不过,“特定于”并不意味着它们是特定于 SKU (Stock-Keeping Unit) 的。例如,Windows XP Professional 和 Home Edition 将使用同一 Service Pack。

Service Pack 具累积性。每个新的 Service Pack 中不仅包含所有新的修补程序,同时还包含以前 Service Pack 中的所有修补程序。安装最新版本之前不必安装以前版本的 Service Pack。目前 Windows XP 已经陆续发布了 Service Pack 1 和 Service Pack 2,简称为 SP1 和 SP2。