

系统管理人员进阶与提高黑皮书

全新推出
精心制作

Windows XP

网络安全

应用实践与精通

林山 主编
王兴成 岳玉梅 栾 毅 等编著



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



Windows XP 网络安全

应用实践与精通

林 山 主编

王兴成 岳玉梅 栾毅 等 编著

清华大学出版社
北 京

内 容 简 介

随着互联网及其他相关网络技术的发展,信息及网络的安全性越来越受到人们的关注,在市场上占有较大份额的 Windows 系列操作系统在网络安全方面功能日趋完善,不但拥有许多微软公司独有的安全技术,还支持绝大多数业内的网络安全标准。最新版 Windows XP 与 Windows .NET Server 2003 的推出,安全性得到更进一步的加强。本书从实用的角度出发,结合大量的实例,详细剖析了这两个操作系统有关网络安全的各项技术,帮助系统管理人员迅速掌握维持 Windows 网络安全的各项技巧。书中还特别提供了电子商务安全交易的概念和实例,对于实际应用环境极具参考价值。

本书主要针对中、高级计算机用户,内容翔实、实例丰富、可操作性强。在讲清概念的同时,又给出有很强实用价值的实例,便于读者快速掌握并熟练运用。本书适用于广大工程技术人员和计算机爱好者阅读、使用。

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。

图书在版编目(CIP)数据

Windows XP 网络安全应用实践与精通 /王兴成等编著. —北京:清华大学出版社,2003.7

(系统管理人员进阶与提高丛书/林山主编)

ISBN 7-302-06650-7

I. W... II. 王... III. ①窗口软件, Windows XP ②计算机网络—安全技术

IV. ①TP316.7 ②TP393.08

中国版本图书馆 CIP 数据核字(2003)第 037982 号

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.tsinghua.edu.cn>

<http://www.tup.com.cn>

责任编辑:田在儒

印刷者:北京密云胶印厂

发行者:新华书店总店北京发行所

开本:787×960 1/16 印张:31 字数:693 千字

版次:2003年7月第1版 2003年7月第1次印刷

书号:ISBN 7-302-06650-7/TP·4978

印数:0001~5000

定价:45.00 元

丛 书 序

操作系统一直以来都是计算机软件部分的核心内容，它既是指挥硬件协调工作的“大脑”，又是承载应用软件功能的“基石”。微软公司的 Windows 系列操作系统软件，在 PC 领域占据着绝对的统治地位；在工作站、服务器领域，也占有很大的装机比例。随着 Windows XP 的推出，其更强大的功能、更安全的特性、更友好的界面、更稳定的性能吸引了越来越多的使用者，无疑这将会掀起学习和使用 Windows 最新操作系统的热潮。本《系统管理人员进阶与提高黑皮书》系列丛书正是顺应这个形势而推出的。

无论是对家庭用户、企业用户还是计算机工程技术人员来说，一套全面、实用、深入讲解 Windows XP 及 Server 2003 技术的指导性书籍都是大有裨益的。本套丛书共 5 本，分别是：

- 《Windows XP 注册表应用实践与精通》
- 《Windows XP 网络信息服务应用实践与精通》
- 《Windows XP 网络安全应用实践与精通》
- 《Windows XP 规划管理应用实践与精通》
- 《Windows XP 局域网建设应用实践与精通》

本套丛书涉及的内容基本上涵盖了 Windows 2000、Windows XP 和 Server 2003 的各个方面。为了描述方便，各书内容基本以 Windows XP 为描述核心。但是 Windows XP 作为服务器的应用一般限于家庭和小型网络，具有实验的性质。对于大中型网络而言，Windows XP 是作为客户端操作系统使用的。为了描述上的完整性，本套丛书对于作为典型的服务器端操作系统使用的 Windows 2000 Server/ Server 2003 的相关内容也进行了详细介绍，并指明了它们在各种应用场合中与 Windows XP 之间的关系。

Windows XP 通过集成 Windows 2000 的强项（基于标准的安全性、可管理性和可靠性）与 Windows 9x 的最佳功能（即插即用、易用的用户界面、创新的支持服务），实现了 Windows 系统的完美统一，给使用者带来了激动人心的新功能。国内越来越多的家庭和企业用户把自己的计算机升级到了这个全新的操作系统上，因此 Windows XP 的应用、管理、维护、开发等各方面技术知识成了计算机从业人员和计算机技术爱好者兴趣的焦点。

本套丛书的编写者由第一线系统工程人员、程序开发人员，以及大学计算机专业教师组成，所有参与编写的人员都怀着极大的热情，翻阅了大量的最新外文参考资料，力争使本套书做到实用性、全面性和时效性俱佳。

本套丛书的编者们也对 Windows Server 2003 的各个 Alpha、Beta 测试阶段进行了长达一年的跟踪测试，这个服务器端操作系统具有和 Windows XP 一样漂亮易用的外观界面，具有比 Windows 2000 Server 更强大的功能和更细分的应用市场。本套丛书在大中型网络技术或应用场合将其作为服务器端操作系统进行了介绍，这也是对实际应用中 Windows XP 的局限性的有益补充。

本套丛书的各种术语和定义基本符合大家约定俗成的习惯，为了让读者更好地使用本套丛书，下面对书中鼠标操作的表达方法做一简要介绍。

- 左键：一般指鼠标左按键。
- 右键：一般指鼠标右按键。
- 单击：按下鼠标左键，随之马上释放（松开）。除特别说明外，“单击”都指单击鼠标左键。
- 双击：快速重复两次单击操作。大多数情况下，双击操作对象等效于先单击选择操作对象，然后再单击“确定”按钮（或按 **Enter** 键）。
- 三击：快速重复三次单击操作（只在特殊软件的特殊用途中用到）。
- 右击：按下鼠标右键，随之马上释放（松开）。
- 指向：不按鼠标按钮的情况下移动鼠标到预期位置。
- 拖动：按住鼠标左键的同时移动鼠标。
- 释放：松开按住鼠标键的手指。
- 拖放：按住鼠标左键的同时移动鼠标，移到预期位置后松开按住鼠标键的手指（等同于拖动+释放）。
- 选择：选取操作对象。大多数选择操作都可通过单击操作对象进行。选择将使操作对象的外观发生变化，如呈反相显示或其周边出现选择框和选择块。

此外，本套丛书在版面设计上，力求活泼而不失典雅。为了突出书中的某些内容使用了一些特殊符号。



此外内容是注释部分。对书中涉及到的技术名词、术语和一些概念进行解释，以便于读者更好地理解上下文内容，或学习一些概念和基础知识。



此外内容是技巧部分。通过使用这些操作技巧，可提高读者完成任务的速度，或实现一些常规方法达不到的目的。



此外内容是警告部分。提醒读者需要小心操作的步骤，或者对于非常危险的操作可能产生的不良后果进行解释。



此外内容是疑难部分。主要解释一些需要具有一定计算机基础知识的读者才能理解的内容。一般读者可跳过此部分，不影响上下文的阅读。

经过将近一年时间的紧张编写，本套丛书终于全部完成了，由于作者水平有限，加上编写时间仓促，书中的缺点错误在所难免，恳请专家和广大读者热心指正。

编者

2002年6月

目 录

第 1 章 信息安全技术基础.....	1
1.1 安全概述.....	2
1.1.1 信息安全研究背景.....	2
1.1.2 什么是安全.....	4
1.1.3 信息安全的内涵.....	4
1.1.4 网络信息安全的威胁.....	5
1.1.5 安全策略.....	6
1.1.6 网络信息安全的技术范畴.....	6
1.1.7 安全服务、机制与技术.....	7
1.1.8 安全工作的目的.....	7
1.2 互联网时代的信息安全.....	8
1.2.1 发展现状.....	8
1.2.2 基本技术.....	10
1.2.3 几个问题.....	12
1.3 密码学基础.....	14
1.3.1 基本概念.....	15
1.3.2 对称加密技术.....	18
1.3.3 公钥加密技术.....	20
1.3.4 混合密码系统.....	21
1.3.5 散列函数.....	22
1.3.6 数字签名.....	23
1.4 证书和 CA 系统.....	25
1.4.1 数字证书.....	25
1.4.2 X.509 证书.....	25
1.4.3 证书机构 CA.....	28
1.5 网络安全技术.....	30
1.5.1 防火墙简介.....	31
1.5.2 防火墙基本类型.....	32
1.5.3 防火墙系统.....	35

第 2 章 活动目录概念及管理	37
2.1 活动目录特性	38
2.2 活动目录概念	42
2.2.1 目录服务	42
2.2.2 域、域树、森林	44
2.2.3 信任关系	45
2.2.4 组织单元	47
2.2.5 站点	47
2.3 活动目录的安装与配置	48
2.4 活动目录管理	51
2.4.1 活动目录用户和计算机	51
2.4.2 活动目录域和信任关系	58
2.4.3 活动目录站点和服务	59
第 3 章 服务器安全技术概要	62
3.1 活动目录技术	63
3.1.1 活动目录基础	63
3.1.2 域间的信任关系	64
3.2 Kerberos 认证	64
3.2.1 Kerberos 基础和背景	65
3.2.2 Kerberos 交互性	66
3.2.3 Kerberos 的公钥扩展	67
3.3 公钥基础设施 PKI	67
3.3.1 互操作性	69
3.3.2 安全性	69
3.3.3 灵活性	70
3.3.4 易用性	71
3.4 智能卡技术	72
3.5 加密文件系统 EFS	72
3.6 安全设置模板	74
3.7 Windows 中的网络安全	75
3.8 多协议支持和可扩展结构	75
第 4 章 操作系统中的 PKI 技术	77
4.1 PKI 基础	78
4.2 CA 系统	80

4.2.1	证书层次结构.....	81
4.2.2	企业 CA 的配置.....	82
4.2.3	多 CA 层次结构的信任关系.....	83
4.3	PKI 功能.....	84
4.3.1	密钥产生.....	84
4.3.2	密钥备份和恢复.....	85
4.3.3	证书申请和更新.....	85
4.3.4	密钥和证书的存储与使用.....	86
4.3.5	证书废除.....	87
4.4	PKI 应用.....	87
4.4.1	Web 安全.....	87
4.4.2	E-mail 安全.....	88
4.4.3	加密文件系统 EFS.....	89
4.4.4	智能卡登录.....	89
第 5 章	证书服务基础.....	91
5.1	证书服务概述.....	92
5.1.1	Windows CA 策略.....	92
5.1.2	企业 CA.....	93
5.1.3	独立 CA.....	94
5.2	CA 系统的安装和测试.....	95
5.2.1	CA 系统的结构和类型.....	95
5.2.2	CA 系统的安装.....	97
5.2.3	CA 系统的测试.....	102
5.3	基于 Web 的证书服务.....	103
5.3.1	Web 页面证书服务简介.....	103
5.3.2	证书申请 Web 页面的配置和连接.....	104
5.3.3	安装 CA 证书.....	106
5.3.4	请求证书.....	109
5.3.5	高级证书请求.....	111
5.3.6	使用 PKCS #10 请求文件申请证书.....	112
5.4	证书服务管理.....	113
5.4.1	CA 服务管理.....	114
5.4.2	CA 证书管理.....	117
5.4.3	高级证书管理.....	119

第 6 章 系统中的证书应用	124
6.1 Web 服务器中的证书安全配置	125
6.2 IE 中基于证书的客户端认证	129
6.2.1 IE 浏览器证书管理	129
6.2.2 拥有公钥证书的 IE 安全实例	131
6.3 OE 中的证书和公钥技术应用	132
6.3.1 配置 Outlook Express	132
6.3.2 安全电子邮件应用	134
6.4 Outlook 2002 中的证书和公钥技术应用	135
6.4.1 安全配置	135
6.4.2 发送 S/MIME 加密和签名的电子邮件	136
6.5 证书到用户账号的映射	137
6.5.1 将证书映射到活动目录中的用户账号	138
6.5.2 将证书映射到 IIS 中的用户账号	139
第 7 章 加密文件系统应用	143
7.1 EFS 概述	144
7.1.1 EFS 简介	144
7.1.2 文件加解密	145
7.1.3 文件恢复	146
7.2 EFS 结构	146
7.3 使用加密文件系统 EFS	149
7.3.1 文件或文件夹加密	149
7.3.2 文件或文件夹解密	151
7.3.3 使用命令行工具加解密	152
7.3.4 加密文件或文件夹的使用	153
7.3.5 加密证书和私钥的备份与还原	157
7.3.6 EFS 文件恢复操作	163
第 8 章 智能卡技术应用	166
8.1 智能卡技术基础	167
8.2 PC/SC 技术简介	168
8.2.1 集成电路卡 ICC	170
8.2.2 接口设备 IFD	170
8.2.3 接口设备处理器	170
8.2.4 ICC 资源管理器	170

8.2.5 服务提供者	171
8.2.6 ICC 应用	172
8.3 Windows 2000 Server/Server 2003 中的智能卡技术	172
8.3.1 智能卡系统结构和组件	173
8.3.2 智能卡读写器的安装	174
8.3.3 智能卡证书申请	176
第 9 章 Kerberos 认证系统	181
9.1 概述	182
9.1.1 Windows 2000 Server/Server 2003 中的认证方法	182
9.1.2 Kerberos 认证的特点	183
9.1.3 Kerberos 协议标准和扩展	183
9.2 Kerberos 认证系统	184
9.2.1 Kerberos 简介	184
9.2.2 Kerberos 协议原理	185
9.2.3 Kerberos 安全性	188
9.3 Windows 2000 Server/Server 2003 中的 Kerberos 系统	188
9.3.1 密钥分配中心 KDC	188
9.3.2 账号数据库	189
9.3.3 Kerberos 策略	190
9.3.4 身份验证的委派	191
9.4 交互式登录	192
9.4.1 登录过程	192
9.4.2 口令登录	193
9.4.3 智能卡登录	195
9.5 远程登录	196
9.5.1 安全支持提供者接口 SSPI	196
9.5.2 远程登录示例	197
第 10 章 Windows 服务器网络安全技术	199
10.1 IPsec 基础	200
10.1.1 概述	200
10.1.2 IPsec 协议	201
10.1.3 IPsec 模式	202
10.2 Windows 2000 中 IPsec 的配置和使用	204
10.2.1 Windows 2000 中的 IPsec 操作模式	204

10.2.2	测试准备	206
10.2.3	使用内置 IPSec 策略	208
10.2.4	定制 IPSec 策略	210
第 11 章	虚拟专用网络	222
11.1	VPN 技术基础	223
11.1.1	概述	223
11.1.2	VPN 原理	224
11.1.3	VPN 类型	226
11.1.4	VPN 协议	228
11.2	Windows 2000 Server/Server 2003 中的 VPN	230
11.2.1	Windows 2000 Server 中的 VPN 组成	230
11.2.2	Windows 2000 Server/Server 2003 中的 VPN 新特性	231
11.3	VPN 连接的建立和配置	232
11.3.1	配置 VPN 服务器	232
11.3.2	配置 VPN 客户端	236
11.3.3	VPN 端口管理	239
第 12 章	Internet 连接共享	242
12.1	连接共享简介	243
12.2	ICS 主机配置	243
12.2.1	设置 Internet 连接和 ICS	244
12.2.2	利用网络向导配置 ICS 主机	246
12.3	使用 ICS 的浏览器配置	249
第 13 章	Internet 连接防火墙	251
13.1	防火墙简介	252
13.2	启用 ICF	253
13.3	ICF 高级设置	254
13.3.1	设置服务	254
13.3.2	日志配置	256
13.3.3	ICMP 设置	258
第 14 章	Windows XP 账户管理	260
14.1	Windows XP 中的账户	261
14.2	新账户创建	266

14.3	更改账户.....	268
14.4	设置 Windows Server 2003 护照.....	270
14.5	用户登录和注销.....	276
第 15 章	IE 6.0 隐私策略.....	279
15.1	Cookie 与隐私设置.....	280
15.2	隐私保护.....	285
15.2.1	P3P.....	286
15.2.2	隐私摘要.....	287
15.2.3	Cookie 管理.....	287
15.3	安全技术.....	290
15.4	OE 6.0 安全特性.....	291
第 16 章	软件限制与签名验证.....	294
16.1	软件安全技术.....	295
16.1.1	软件限制策略.....	295
16.1.2	安全级别.....	296
16.1.3	更改默认限制.....	297
16.1.4	其他规则.....	298
16.2	文件签名验证.....	302
16.3	加密文件系统 EFS.....	305
第 17 章	电子商务概述.....	306
17.1	电子商务的产生、发展.....	307
17.1.1	电子商务的产生.....	307
17.1.2	电子商务的发展历程.....	308
17.2	电子商务的定义.....	311
17.2.1	电子商务的定义.....	311
17.2.2	电子商务的内涵.....	313
17.3	电子商务的分类.....	315
17.3.1	按照商业活动的运作方式分类.....	315
17.3.2	按照开展电子交易的范围分类.....	315
17.3.3	按照商务活动的内容分类.....	316
17.3.4	按照使用网络的类型分类.....	317
17.3.5	按照交易对象分类.....	317
17.3.6	按照采用的技术标准和支付角度分类.....	318

17.4 迎接电子商务时代.....	319
第 18 章 信息流、资金流、物流	322
18.1 传统商务的运作内容.....	325
18.1.1 商务活动主体.....	325
18.1.2 商务活动内容.....	326
18.1.3 传统商务运作方式的特点.....	327
18.2 传统商务的运作流程.....	328
18.2.1 商场商务流程.....	328
18.2.2 连锁超市商务流程.....	329
18.3 电子商务流程.....	329
18.3.1 电子商务的通用流程.....	330
18.3.2 业务过程的实现.....	331
18.3.3 电子商务下的贸易方式.....	332
18.4 电子商务的运行模式.....	334
18.4.1 支付系统无安全措施的模式.....	334
18.4.2 通过第三方经纪人支付的模式.....	335
18.4.3 电子现金支付模式.....	335
18.4.4 支付系统使用简单加密的模式.....	335
18.4.5 SET 模式.....	336
18.5 信息流、资金流、物流.....	337
18.5.1 信息流.....	338
18.5.2 资金流.....	339
18.5.3 物流及标识技术.....	340
第 19 章 电子支付与电子转账	346
19.1 电子货币.....	347
19.1.1 电子货币介绍.....	347
19.1.2 电子资金转账.....	349
19.2 银行卡.....	350
19.2.1 银行卡介绍.....	350
19.2.2 银行卡组织.....	352
19.2.3 银行卡应用系统.....	355
19.3 SWIFT 金融电子通信服务系统.....	357
19.3.1 金融通信服务组织 SWIFT.....	357
19.3.2 SWIFT 服务内容.....	361

19.3.3	SWIFT 标准化体系	364
19.3.4	SWIFT 的发展	364
19.4	电子交易协议与 CA 认证	365
19.4.1	安全电子交易规范	365
19.4.2	CA 认证系统	368
第 20 章	EDI 技术	371
20.1	EDI 概述	372
20.1.1	EDI 的概念	372
20.1.2	EDI 的特点	374
20.1.3	EDI 的构成要素	376
20.1.4	EDI 的类型	376
20.1.5	贸易伙伴间的 EDI 应用系统	377
20.2	EDI 标准	378
20.2.1	EDI 标准体系结构	379
20.2.2	EDI 基础标准	379
20.2.3	EDI 应用标准	387
20.2.4	流通领域电子数据交换规范	389
20.3	EDI 系统的组成	396
20.3.1	EDI 系统的组成	396
20.3.2	EDI 报文的产生与传输	397
20.4	EDI 的实施	404
20.4.1	实施 EDI 的困难	405
20.4.2	EDI 实施中的准备工作	409
20.4.3	EDI 实施的步骤	411
20.4.4	EDI 系统软硬件的选择	411
20.5	EDI 应用案例	417
20.5.1	新奥尔良港的 CRESCENT 系统	417
20.5.2	香港的 TRADELINK/CETS	418
20.5.3	海关 EDI 通关系统开发应用情况	418
20.5.4	北美飞利浦公司案例	422
20.6	Internet 上的 EDI——XML/EDI	425
第 21 章	电子商务的安全与法律	426
21.1	电子商务的安全	427
21.1.1	信息安全技术	427

21.1.2	网络安全技术	432
21.2	电子商务的法律	437
21.2.1	电子商务交易合同的法律问题	437
21.2.2	网络交易安全的法律保障	442
21.2.3	我国电子商务交易安全的法律保护	447
21.2.4	EDI 的法律问题	452
21.2.5	电子商务交易合同的取证问题	453
第 22 章	建立电子商务系统	454
22.1	电子商务系统的建立策略	455
22.1.1	企业目标和战略	455
22.1.2	内部和外部环境分析	457
22.1.3	成本与效益分析	457
22.2	企业内部网的建设	458
22.2.1	企业内部网 Intranet	459
22.2.2	Intranet 提供的服务	460
22.3	电子商务系统的实现	462
22.3.1	因特网的地址结构	462
22.3.2	域名注册和申请	465
22.3.3	两个合理选择	474

第1章

信息安全技术基础

本章要点

安全概述
信息安全基础
密码学基础
证书和 CA 系统
网络安全技术