

# 系统防护与黑客攻防 网络安全 实用宝典

俞朝晖 王长征 赵怡程 编著



所有安全知识与技巧皆来自实践, 凝结作者多年经验



涉及网络管理和系统安全的方方面面, 真正的全面超值



尽可能详细地操作步骤和分解图片, 力争做到一目了然

本书为中小企业网络管理人员量身打造, 是计算机和网络安全的随身宝典。同时对于企业和家庭用户保护网络信息安全, 也有很好的实践指导意义。

Getting you the Best Book!



Sleep



Restart



Shut Down

# 系统防护 网络安全

# 黑客攻防

# 实用宝典

俞朝晖 王长征 赵怡程 编著

中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

## 内 容 简 介

一直以来, 计算机系统与网络安全问题都是困扰众多用户的难题。本书以计算机安全与黑客攻防技术为主题, 从计算机系统安全、网络应用安全、黑客攻防技术、办公和移动存储数据安全保护等几个方面, 全面详细地介绍了计算机网络安全和黑客攻防技术方面的应用技术。

本书在编写过程中突出知识的先进性和内容的实用性, 用大量的图片及实例分析, 使学习过程更加直观明了。全书语言生动、图文并茂、深入浅出; 不仅适合各类非计算机专业人员, 尤其适合计算机家庭用户和办公用户参考阅读。

### 图书在版编目 (CIP) 数据

系统防护、网络安全与黑客攻防实用宝典/俞朝晖,  
王长征, 赵怡程编著. — 北京: 中国铁道出版社,  
2013. 2

ISBN 978-7-113-15879-8

I. ①系… II. ①俞… ②王… ③赵… III. ①计算机  
网络—安全技术 IV. ①TP393.08

中国版本图书馆 CIP 数据核字 (2012) 第 305546 号

书 名: 系统防护、网络安全与黑客攻防实用宝典  
作 者: 俞朝晖 王长征 赵怡程 编著

责任编辑: 荆 波  
特邀编辑: 赵树刚  
责任印制: 赵星辰

读者服务热线: 010-63560056  
封面设计: 付 巍  
封面制作: 张 丽

出版发行: 中国铁道出版社 (北京市西城区右安门西街 8 号 邮政编码: 100054)

印 刷: 三河市华业印装厂

版 次: 2013 年 2 月第 1 版 2013 年 2 月第 1 次印刷

开 本: 787mm×1092mm 1/16 印张: 31.5 字数: 734 千

书 号: ISBN 978-7-113-15879-8

定 价: 69.00 元

版权所有 侵权必究

凡购买铁道版图书, 如有印制质量问题, 请与本社发行部联系调换。

## 网络安全现状

我们不妨做个小小的调查，观察一下身边同事同学、亲朋好友电脑屏幕的右下角，你会发现这个地方有着惊人的相似——“杀毒软件+安全卫士”的安全套装组合。这样的调查结果也充分说明了计算机在中国普及以及普遍连网之后，计算机网络的安全已经成为现今网络领域的主旋律。如今，关于网络安全的话题和热点事件也层出不穷，在各类媒体上均可见一斑。

虽然“杀毒软件+安全卫士”的安全套装组合足以抵挡大部分使用“傻瓜式”攻击软件的黑客，但是在信息数据爆炸和黑客攻击方式层出不穷的今天，系统安全与网络安全知识的普及仍然是一个非常严峻的问题。

同时，新的网络攻击技术也对计算机网络安全相关技术人员提出了更高的要求，需要我们不断学习，提升技术水平，掌握实用的解决网络安全故障类问题的方法。

## 我们的优势

本书由浅入深、循序渐进地介绍了计算机网络安全的知识体系。内容丰富、深入浅出，适合各个层次的读者学习。全书以操作为主，提供了尽可能详细的操作步骤和分解图片，使所有操作一目了然。书中所涉及的各个方面的安全问题都是用户所经常碰到的，并且是困扰用户的常见问题。通过本书，用户可以联系自己的实际情况，逐步深入地学习计算机网络安全方面的基本知识、方法和技巧。

本书内容覆盖了计算机网络安全和黑客攻防技术的方方面面。知识面广，条理性强，从读者实际应用的角度出发，减少了枯燥死板的理论概念，加强了应用性和可操作性。使用大量形象、清晰的图片，加强了可读性，同时也会对读者的操作起到有效的参考作用。

## 通过本书你能学到什么

全书分为4篇，共24章，内容涵盖了计算机系统安全、网络应用安全、黑客攻防技术、办公和移动存储数据安全保护等多个方面。第1篇计算机系统安全篇，包括第1~8章，主要介绍了计算机系统安全方面的内容，包括密码设置、注册表和组策略安全方案、系统启动安全、病毒木马的查杀和防护、防火墙以及各类安全卫士的使用和设置等内容。第2篇网络浏览与应用安全篇，包括第9~13章，主要介绍了网络浏览与应用安全方面的内容，内容涵盖网络浏览、即时通信、网络邮件、网络购物、网上银行等方面。第3篇黑客攻防技术篇，包括第14~19章，主要介绍了黑客攻防技术方面的内容，包含安全漏洞与端口检查、黑客常用的命令与工具、黑客入侵前的准备工作、Windows系统防黑设置、远程控制攻防、各种常见密码的破解等方面的内容。第4篇办公和移动存储设备安全篇，包括第20~24章，主要介绍了办公和移动存储



数据的安全保护与恢复方面的内容，包括办公文档数据的保护和修复、重要文件和隐私保护、移动存储设备的安全保护和应用程序的备份和恢复方面的内容。

## 网络安全与职业提升

中小企业数量众多，但因为各种原因，不能招聘专职网络管理人员，或者其网络管理人员由其他非计算机专业人员转行而来，就是计算机专业科班出身的专业人员，由于计算机技术发展很快，其知识技能淘汰速度也很快。可以说，本书是中小企业网络管理人员的随身安全宝典，是具体工作实践中保证计算机网络安全的使用手册。同时，计算机普及程度日益深入，计算机使用者在安全方面的知识和技能盲点越来越多，企业和家庭用户也要充分考虑自己的数据和信息安全。

本书充分考虑了广大初、中级计算机用户在安全方面的根本需求，主要面对日常使用计算机的办公人员，具有一定计算机应用技能的读者。对广大的计算机用户来说，实际上对计算机安全、网络安全、黑客攻防、数据安全等并不精通，但又不可能花费太多精力去研习。因此，如何在最短时间内，花费不多的精力，可以学到最实用的计算机安全、网络安全、黑客攻防、数据安全知识，以保证办公计算机、个人计算机日常的使用，是急需解决的问题。本书就是针对此问题专门设计、编写的。

## 作者与感谢

本书由中国印刷科学技术研究所研发中心主任俞朝晖组织编写，人民日报社中闻集团信息化管理领导小组组长王长征和人民日报社中闻集团信息化管理领导小组副组长赵怡程参与编写。由于时间仓促，水平有限，书中难免会出现一些错误和缺漏，望广大读者朋友评判指正。

编 者

2012年12月

## 第 1 篇 计算机系统安全篇

## 第 1 章 密码是保障计算机安全的基础

1.1	设置系统登录密码 .....	2
1.1.1	创建账户 .....	2
1.1.2	设置账户登录密码 .....	4
1.2	设置系统启动密码 (Syskey) .....	6
1.3	设置 BIOS 开机密码 .....	7
1.3.1	设置进入 CMOS 的密码 .....	8
1.3.2	设置开机密码 .....	8
1.4	设置屏保密码 .....	9
1.5	快速锁定系统 .....	10
1.5.1	快捷方式法 .....	10
1.5.2	“Win+L”键法 .....	11
1.5.3	使用“Ctrl+Alt+Delete”组合键 .....	11
1.5.4	使用休眠功能 .....	11
1.5.5	使用“关机”菜单 .....	13
1.6	开启 Windows 7 超级管理员账户 .....	13
1.6.1	从“计算机管理”中开启 Administrator 账户 .....	13
1.6.2	使用命令启用 Administrator 账户 .....	14
1.7	更改默认账号设置 .....	15
1.7.1	Administrator 账号 .....	15
1.7.2	Guset 账号 .....	17
1.7.3	为用户设置合适的身份 .....	18
1.8	禁止/关闭/删除未使用和不需要的服务及进程 .....	21
1.8.1	查看正在启用的服务项目 .....	21
1.8.2	关闭、禁止与重新启用服务 .....	22
1.8.3	Windows 7 系统服务优化设置 .....	23

## 第2章 注册表安全策略

2.1 认识注册表.....	28
2.1.1 注册表的功能.....	28
2.1.2 注册表的基本结构.....	30
2.1.3 注册表的编辑.....	31
2.2 注册表的备份和恢复.....	36
2.2.1 使用系统自带工具备份和恢复注册表.....	36
2.2.2 使用第三方软件备份和恢复注册表.....	37
2.3 设置注册表加强网络安全.....	39
2.3.1 网络连接限制.....	39
2.3.2 系统启动时弹出对话框.....	40
2.3.3 IE 默认连接首页被修改.....	40
2.3.4 篡改 IE 的默认页.....	41
2.3.5 IE 右键菜单被修改.....	42
2.3.6 IE 工具栏被添加网站链接.....	42

## 第3章 组策略安全策略

3.1 认识组策略.....	43
3.1.1 组策略与注册表.....	43
3.1.2 组策略的运行方式.....	44
3.2 用策略增强系统安全防护.....	46
3.2.1 禁止运行指定程序.....	46
3.2.2 禁止修改系统还原配置.....	47
3.2.3 保护虚拟内存页面文件中的秘密.....	48
3.2.4 阻止访问命令提示符.....	49
3.2.5 锁定注册表编辑器.....	50
3.2.6 禁止用户访问指定驱动器.....	51
3.2.7 防止搜索泄露隐私.....	52
3.2.8 记录上次登录系统的时间.....	52
3.2.9 限制密码“尝试”次数.....	53
3.3 “桌面”、“任务栏”和“开始”菜单安全策略.....	54
3.3.1 拒绝使用没有签证的桌面小工具.....	54
3.3.2 我的桌面你别改.....	55
3.3.3 关闭“气球”通知.....	55

3.3.4	不保留最近打开文档的历史.....	56
3.3.5	阻止用户重新安排工具栏.....	56
3.4	移动存储设备安全策略.....	57
3.4.1	禁止数据写入 U 盘.....	57
3.4.2	完全禁止使用 U 盘.....	57
3.4.3	禁止安装移动设备.....	58
3.4.4	禁用移动设备执行权限.....	59
3.4.5	禁止光盘自动播放.....	59
3.5	IE 安全策略.....	60
3.5.1	锁定主页.....	60
3.5.2	禁止更改分级审查.....	61
3.5.3	禁止保存密码.....	62
3.5.4	禁用更改高级页设置.....	62
3.5.5	禁用“Internet 选项”菜单选项.....	63

## 第 4 章 深入挖掘系统启动项

4.1	病毒木马的温床——启动项.....	64
4.2	经典的“启动”文件夹.....	64
4.3	Msconfig.....	65
4.3.1	Windows XP 中的 Msconfig.....	65
4.3.2	Windows 7 中的 Msconfig.....	66
4.4	注册表中的启动项.....	67
4.4.1	“Load”键值.....	67
4.4.2	“Userinit”键值——用户相关.....	67
4.4.3	“Run”子键.....	68
4.4.4	“RunOnce”子键.....	69
4.4.5	Windows 中加载的服务.....	70
4.4.6	Windows Shell——系统接口.....	70
4.4.7	BootExecute——属于启动执行的一个项目.....	70
4.4.8	组策略加载程序.....	71

## 第 5 章 病毒的查杀和防护

5.1	病毒是什么.....	73
5.1.1	什么是计算机病毒.....	73
5.1.2	计算机病毒的特点.....	74



5.1.3	病毒对计算机的危害	75
5.2	病毒的防治常识	77
5.2.1	计算机病毒类型的识别	78
5.2.2	计算机病毒防治建议	79
5.3	卡巴斯基杀毒软件的使用	81
5.3.1	安装卡巴斯基安全部队 2012	81
5.3.2	及时更新杀毒软件	83
5.3.3	全盘扫描	83
5.3.4	关键区域扫描	84
5.3.5	自定义扫描	84
5.4	金山毒霸的使用	85
5.4.1	安装金山毒霸 2012 (猎豹)	85
5.4.2	查杀病毒	86
5.4.3	给软件做安检	87
5.4.4	使用强力查杀清除顽固病毒	87

## 第6章 木马的查杀和防护

6.1	认识木马	89
6.1.1	木马简介	89
6.1.2	木马的危害	91
6.1.3	木马的类型	91
6.1.4	中木马病毒后出现的状况	93
6.2	找出计算机中的木马	93
6.2.1	木马常用端口	93
6.2.2	木马运行机制	96
6.2.3	木马隐身方法	97
6.3	手动查杀病毒木马的弊端	99
6.4	使用 Windows 木马清道夫查杀木马	100
6.4.1	安装 Windows 木马清道夫 2010	100
6.4.2	查杀进程中的木马	101
6.4.3	扫描硬盘	102
6.5	使用 360 安全卫士查杀木马	103
6.5.1	安装 360 安全卫士	104
6.5.2	使用 360 安全卫士查杀木马	105

6.5.3 使用强力查杀模式.....	106
6.5.4 使用 360 急救箱.....	107

## 第 7 章 防火墙是一道很好的屏障

7.1 防火墙概述.....	109
7.1.1 什么是防火墙.....	109
7.1.2 防火墙的分类.....	109
7.1.3 防火墙的主要功能.....	115
7.2 瑞星个人防火墙的使用.....	116
7.2.1 安装瑞星个人防火墙 2012.....	116
7.2.2 常用功能设置.....	119
7.2.3 设置防火墙的安全规则.....	121
7.2.4 设置浏览器高强度防护.....	123
7.2.5 防黑客设置.....	123
7.2.6 黑白名单设置.....	124
7.2.7 联网规则设置.....	126
7.3 诺顿智能防火墙的使用.....	128
7.3.1 诺顿智能防火墙概述.....	128
7.3.2 防火墙高级设置.....	128
7.3.3 程序控制设置.....	131
7.3.4 入侵防护设置.....	132

## 第 8 章 给电脑请一个安全卫士

8.1 360 安全卫士.....	134
8.1.1 360 安全卫士简介.....	134
8.1.2 电脑体检.....	135
8.1.3 木马查杀.....	135
8.1.4 插件清理.....	136
8.1.5 漏洞修复.....	137
8.1.6 系统修复.....	138
8.1.7 垃圾清理.....	140
8.1.8 优化加速.....	143
8.1.9 功能大全.....	145
8.1.10 软件管家.....	147
8.2 金山卫士.....	151

8.2.1	金山卫士简介.....	151
8.2.2	首页（体检）.....	151
8.2.3	系统优化.....	152
8.2.4	垃圾清理.....	152
8.2.5	查杀木马.....	153
8.2.6	修复漏洞.....	154
8.2.7	百宝箱.....	154
8.2.8	软件管理.....	156
8.2.9	专家加速.....	156

## 第2篇 网络浏览与应用安全篇

### 第9章 网络浏览安全

9.1	网页浏览安全概述.....	160
9.1.1	网络广告.....	160
9.1.2	恶意网站.....	161
9.1.3	网络偷窥.....	162
9.2	浏览器安全防范.....	163
9.2.1	Cookies 问题.....	163
9.2.2	浏览器设置.....	164
9.2.3	网页脚本.....	166
9.2.4	使用第三方浏览器.....	168
9.3	浏览器修复.....	176
9.3.1	修复首页更改.....	176
9.3.2	修复右键菜单.....	177
9.3.3	修复工具栏.....	177
9.3.4	锁定 IE 主页.....	178

### 第10章 即时通信安全

10.1	即时通信盗号木马的防范.....	180
10.2	QQ 安全基本设置.....	181
10.2.1	安全设置.....	181
10.2.2	隐私设置.....	185
10.3	玩转 QQ 安全中心.....	185

10.3.1	登录 QQ 安全中心.....	186
10.3.2	使用密保工具设置密码保护.....	186
10.3.3	设置账号保护.....	191
10.3.4	QQ 密码管理.....	194
10.4	MSN 安全防范.....	199
10.4.1	防范 MSN 密码被盗.....	199
10.4.2	找回丢失的密码.....	201

## 第 11 章 网络邮件安全

11.1	电子邮件的安全问题.....	203
11.1.1	垃圾邮件.....	203
11.1.2	邮件病毒.....	205
11.1.3	申请电子邮件不安全的因素.....	206
11.2	Web 邮件的安全设置.....	207
11.2.1	QQ 邮箱反垃圾邮件设置.....	207
11.2.2	QQ 邮箱账户安全设置.....	210
11.2.3	网易邮箱反垃圾邮件设置.....	211
11.2.4	网易邮箱账户安全设置.....	213
11.3	Foxmail 的安全设置.....	217
11.3.1	设置 Foxmail 中的账号密码.....	217
11.3.2	在 Foxmail 中设置垃圾邮件过滤.....	219

## 第 12 章 网络购物安全

12.1	网络购物概述.....	222
12.1.1	网络购物的优点.....	222
12.1.2	网络购物的缺点.....	223
12.2	网络购物的一般流程.....	223
12.2.1	注册用户.....	224
12.2.2	注册网上银行.....	226
12.2.3	在线购物流程.....	227
12.3	网上购物的安全隐患.....	229
12.3.1	虚假信息.....	230
12.3.2	支付安全.....	231
12.3.3	钓鱼式陷阱.....	231
12.4	安全交易措施.....	232



12.4.1	详细了解商品.....	232
12.4.2	了解商家信誉.....	232
12.4.3	货到付款.....	233
12.4.4	维护正当权益.....	234
12.5	网上个人信息的保密.....	234
12.5.1	设置 IE 防止 Cookie 泄露个人资料.....	234
12.5.2	修改注册表防止 Cookie 泄露个人资料.....	234
12.5.3	使用隐私保护器保护网络隐私.....	235
12.6	用户账号、密码的保密和保管.....	238
12.6.1	删除保存用户上网登录账号和密码的临时文件.....	238
12.6.2	使用“金山密码专家”保护密码.....	239
12.7	使用“金山网购保镖”保障网购安全.....	241
12.7.1	设置网购保护.....	241
12.7.2	使用网购敢赔功能.....	242

## 第 13 章 网上银行安全

13.1	网上银行安全防护的几种方法.....	244
13.2	工商银行网上银行安全使用实例.....	246
13.2.1	开通工商银行网上银行.....	246
13.2.2	U 盾和电子银行口令卡.....	247
13.2.3	使用网银助手安装控件.....	249
13.2.4	使用电子银行口令卡进行支付.....	251
13.2.5	使用 U 盾进行支付.....	252
13.2.6	通过安全中心加强账户安全.....	254
13.3	建设银行网上银行安全使用实例.....	258
13.3.1	建设银行安全策略.....	258
13.3.2	建行网银盾和动态口令卡.....	259
13.3.3	安装 E 路护航网银安全组件.....	260
13.3.4	使用建行网银盾进行支付.....	262

## 第 3 篇 黑客攻防技术篇

### 第 14 章 安全漏洞与端口检查

14.1	认识安全漏洞.....	266
------	-------------	-----

14.1.1	安全漏洞的产生	266
14.1.2	安全漏洞的分类	267
14.1.3	漏洞等级评定	268
14.2	系统安全漏洞扫描	268
14.2.1	使用检查电脑系统安全	269
14.2.2	使用 Nmap 扫描系统安全漏洞	272
14.3	服务端口检查	275
14.3.1	计算机端口概述	275
14.3.2	监视计算机端口	275
14.3.3	在线检测计算机端口	276

## 第 15 章 黑客常用的命令与工具

15.1	黑客常用的 DOS 命令	279
15.1.1	DOS 命令的格式	279
15.1.2	黑客常用的目录操作命令	280
15.1.3	黑客常用的文件操作命令	287
15.2	黑客常用的网络命令	293
15.2.1	远程登录命令——Telnet	293
15.2.2	文件上传、下载命令——FTP	296
15.2.3	显示和修改本地 ARP 列表——ARP	298
15.2.4	计划管理程序——AT	299
15.2.5	网络测试命令	302
15.2.6	使用 net 命令管理网络	308
15.3	黑客常用工具介绍	313
15.3.1	流光扫描器的使用	313
15.3.2	HostScan 扫描器	316
15.3.3	网络神偷远程控制器的使用	318

## 第 16 章 黑客入侵前的踩点工作

16.1	采集相关信息	321
16.1.1	使用 Ping 命令获取 IP 地址	321
16.1.2	使用网站获取 IP 地址	322
16.1.3	使用工具获取目标的物理位置	322
16.1.4	通过网站查询 IP 地址所在地理位置	323
16.1.5	查询网站备案信息	323

16.2	对系统漏洞进行检测.....	324
16.2.1	使用 X-Scan 检查系统漏洞.....	324
16.2.2	使用瑞星安全助手扫描系统漏洞.....	327
16.3	对系统服务和端口进行扫描.....	328
16.3.1	使用 SuperScan 扫描器扫描服务和端口.....	328
16.3.2	使用局域网查看工具 (LanSee) 查看他人主机中的端口.....	330
16.3.3	使用黑客字典编辑弱口令的扫描规则.....	332
16.3.4	使用弱口令扫描器获取口令.....	333

## 第 17 章 Windows 系统防黑设置

17.1	熟悉系统进程.....	335
17.1.1	查看系统中运行的进程.....	335
17.1.2	关闭正在运行的危险进程.....	337
17.1.3	新建系统进程.....	339
17.1.4	查杀病毒进程.....	339
17.2	修补系统漏洞防范黑客.....	340
17.3	系统方面的防黑设置.....	341
17.3.1	查看和关闭默认共享.....	341
17.3.2	设置代理服务器隐藏 IP 地址.....	342
17.4	注册表防黑设置.....	343
17.4.1	禁止远程修改注册表.....	343
17.4.2	永久关闭默认共享.....	343
17.4.3	禁止普通用户查看事件记录.....	344
17.4.4	找出隐藏的超级用户.....	345

## 第 18 章 远程控制攻防

18.1	Windows 7 远程桌面连接的使用.....	347
18.1.1	开启远程桌面连接.....	347
18.1.2	使用远程桌面连接功能.....	348
18.1.3	向远程桌面传送文件.....	349
18.2	Windows 7 远程协助的使用.....	351
18.2.1	远程协助和远程桌面连接的区别.....	351
18.2.2	允许远程协助.....	351
18.2.3	邀请他人远程协助.....	351
18.2.4	利用远程协助帮助他人.....	352

18.3	使用腾讯 QQ 进行远程协助.....	354
18.3.1	使用腾讯 QQ 实现远程协助.....	354
18.3.2	使用 QQ 远程控制获取被控端主机文件.....	356
18.4	使用 pcAnywhere 实现远程控制.....	358
18.4.1	主控端和被控端的安装.....	358
18.4.2	建立一个新的连接并连接到远程计算机.....	361
18.4.3	优化连接速率.....	363
18.4.4	对被控端计算机进行远程管理.....	364
18.4.5	在 主控端和被控端之间实现文件传送.....	366

## 第 19 章 密码的破解

19.1	BIOS 密码的破解.....	368
19.1.1	使用放电的方法破解 BIOS 密码.....	368
19.1.2	使用跳线短接法破解 BIOS 密码.....	369
19.2	破解 Windows XP 系统登录密码.....	370
19.2.1	使用密码重设盘破解密码.....	370
19.2.2	使用 Windows PE 重新设置密码.....	372
19.2.3	使用 Active@ Password Changer 清除密码.....	373
19.3	破解 Windows 7 系统登录密码.....	375
19.3.1	利用密码重置盘破解.....	375
19.3.2	利用 Windows 7 PE 破解密码.....	378
19.4	办公文档密码的破解.....	381
19.4.1	Passware Password Recovery Kit 简介.....	381
19.4.2	使用预定设置破解 Word 文档打开密码.....	382
19.4.3	使用向导破解 Excel 文档打开密码.....	384
19.4.4	使用破解编辑器破解 WinRAR 压缩文件密码.....	386

## 第 4 篇 办公和移动存储设备安全篇

### 第 20 章 办公文档的安全

20.1	Word 文档安全.....	390
20.1.1	隐藏文档记录.....	390
20.1.2	躲开他人视线.....	391
20.1.3	给文档设置密码.....	392



20.1.4	限制编辑文档.....	393
20.1.5	设置文档自动保存时间间隔.....	394
20.1.6	宏病毒的防范.....	395
20.2	Excel 电子表格安全.....	395
20.2.1	设置允许用户进行的操作.....	395
20.2.2	隐藏含有重要数据的工作表.....	396
20.2.3	指定工作表中的可编辑区域.....	397
20.2.4	设置可编辑区域的权限.....	398
20.2.5	保护工作簿不能被修改.....	399
20.2.6	设置工作簿修改权限密码.....	399
20.2.7	设置工作簿打开权限密码.....	399
20.2.8	保护公式不被更改.....	400
20.2.9	禁用文档中的 ActiveX 控件.....	401
20.3	PowerPoint 演示文稿安全.....	401
20.3.1	将演示文稿设置为最终状态.....	401
20.3.2	恢复受损的演示文稿.....	402
20.3.3	设置保存时从文件属性中删除个人信息.....	402
20.3.4	为演示文稿加密.....	403
20.4	压缩文件安全.....	404
20.4.1	设置 WinRAR 压缩密码.....	404
20.4.2	设置 WinZip 压缩密码.....	406

## 第 21 章 修复办公文档数据

21.1	Word 文档的修复.....	407
21.1.1	使用自动恢复功能修复 Word 文档.....	407
21.1.2	手动打开恢复文件修复 Word 文档.....	408
21.1.3	“打开并修复”文件修复 Word 文档.....	410
21.1.4	从任意文件中“恢复文本”修复 Word 文档.....	410
21.1.5	禁止自动运行宏修复损坏的 Word 文档.....	411
21.1.6	文档格式法修复损坏的 Word 文档.....	412
21.1.7	重设格式法修复损坏的 Word 文档.....	412
21.1.8	创建新的 Normal 模板修复损坏的 Word 文档.....	413
21.2	Excel 文档的修复.....	413
21.2.1	转换格式修复 Excel 文档.....	413
21.2.2	转换为较早的版本修复 Excel 文档.....	414