

最新

魏亮 孙国梓 等编著

家用电脑网络安全 防护与隐私保护

掌中宝



中国水利水电出版社
www.waterpub.com.cn

家用电脑网络安全防护与 隐私保护掌中宝

魏亮 孙国梓 等编著

中国水利水电出版社

内容提要

全书分为网络安全基础篇、网络防护实战篇和个人隐私保护篇。从家用电脑使用过程中经常碰到的各类问题着手,针对与网络安全相关的病毒、黑客、木马、邮件炸弹、个人隐私等内容进行详细介绍,并提出了各种相关的防范措施。

本书适合于家用电脑网络用户以及有一定计算机操作经验并想迅速提高系统安全性的读者阅读。

图书在版编目(CIP)数据

家用电脑网络安全防护与隐私保护掌中宝/魏亮等编著. —北京:中国水利水电出版社, 2004

ISBN 7-5084-2394-1

I. 家… II. 魏… III. 计算机网络-安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2004) 第 099174 号

书 作 出 版 名 者 发 行	家用电脑网络安全防护与隐私保护掌中宝 魏 亮 孙国梓 等编著 中国水利水电出版社(北京市三里河路 6 号 100044) 网址: www. waterpub. com. cn E-mail: mchannel@263.net (万水) sales@waterpub. com. cn 电话: (010) 63202266 (总机) 68331835 (营销中心) 82562819 (万水)
经 售	全国各地新华书店和相关出版物销售网点
排 印 规 版 印 定	北京万水电子信息有限公司 北京市天竺颖华印刷厂 850mm×1168mm 64 开 7.25 印张 250 千字 2004 年 10 月第 1 版 2004 年 10 月第 1 次印刷 0001—8000 册 10.00 元

凡购买我社图书,如有缺页、倒页、脱页的,本社营销中心负责调换
版权所有·侵权必究

前 言

你打开 QQ，却发现密码是错的，你绞尽脑汁试遍了所有可能的密码还是报错，那么应该能肯定你的 QQ 被盗了。

你打开电子邮箱，却发现里面塞满了来自莫名其妙地址的信件，而你想要的信件却还没有收到。

你浏览网页时，电脑突然变得跟蜗牛一样慢，对你任何的操作都毫无反应，以至最后干脆死机。

如果你经常被以上问题困扰，那么我不得不提醒你提高网络安全意识，为你的个人电脑采取有效的网络安全保障措施。事实上，这些威胁着个人电脑用户安全的正是驻留本地计算机的特洛伊木马、大量经过电子邮件传播的各类病毒以及在网上聊天时不经意就来到身边的网络炸弹等。

现在，人们正在越来越多地依赖网络来改变自己的生活方式，例如网上购物、网上交易、网上投资和网上数据存储等。如果在访问 Internet 的过程中不注意网络安全，一旦重要的数据被破坏或被窃取，那么后果不堪设想。为了能够引起人们对网络安全问题的足够重视，并为大众介绍实用的网络安全和个人隐私防护技巧，我们编写了此书。本书的讲解详略得当，注重实际操作，适合具有一定计算机操作经验和 Internet 网络初步知识的广大读者，是个人和家庭用户不可多得的必备参考工具书。

参与本书编写并为本书编写提供资料的有魏亮、孙国梓、郝文博、范瑞涛、宋晓鹏、张勇、李强、胡创国、林丽、王晓青等人，由于作者水平有限，再加上时间仓促，本书难免有疏漏和不当之处，敬请各位读者指正。我们的联系方式：
xinyuanxuan@263.net。

编者

2004 年 4 月

目 录

前言

第一篇 网络安全基础篇

第 1 章	Internet 带来的隐患	2
1.1	个人计算机的本地防护	2
1.1.1	防范病毒	3
1.1.2	Windows 操作系统安全措施	4
1.1.3	用户个人隐私的保护	5
1.2	计算机的网络防护	6
1.2.1	黑客 (Hacker) 的兴起	6
1.2.2	黑客攻击的主要途径和方法	8
1.2.3	网络防范意识的建立	12
第 2 章	Internet 是怎么架设起来的	14
2.1	网络的七层结构是什么	14
2.2	计算机网络中的 TCP/IP 体系	17
2.3	TCP/IP 相关的常识	19
2.3.1	什么是计算机的 IP 地址	19
2.3.2	拨号用户的 IP 地址是固定的吗	19

2.3.3	每个网卡可以绑定几个 IP 地址.....	20
2.3.4	怎么才能知道计算机的 IP 地址.....	20
2.3.5	什么是 MAC 地址	20
2.3.6	如何查询自己计算机的 MAC 地址	22
2.3.7	IP 地址与 MAC 地址在互联网中的作用...	23
2.3.8	根据 IP 地址判断对方是否在网上.....	23
2.3.9	子网掩码和 IP 地址的关系.....	24
2.3.10	什么是 TCP 和 UDP 协议.....	26
2.3.11	端口 (Port) 有哪几类.....	27
2.3.12	端口有什么用处	27
2.3.13	什么是 Proxy 代理服务.....	30
2.4	Internet 上的各种应用服务.....	31
2.4.1	WWW 服务.....	32
2.4.2	电子邮件服务	33
2.4.3	FTP 服务和 TFTP 服务	34
2.4.4	Telnet (远程登录协议)	35
2.4.5	DNS (域名服务)	35
2.4.6	finger 服务	36
2.4.7	其他的安全性极差的服务	37
2.5	TCP/IP 的缺陷.....	37
第 3 章	网络为什么会如此脆弱	40
3.1	操作系统的缺陷.....	40
3.1.1	Windows 操作系统的漏洞	41

3.1.2	Unix、Linux 操作系统的漏洞.....	44
3.2	网络设备的缺陷.....	44
3.3	应用软件的缺陷.....	45
3.3.1	Office 严重漏洞.....	45
3.3.2	Netscape 浏览器严重漏洞.....	46
3.3.3	QQ 漏洞.....	46
3.3.4	IE HTTPS 认证漏洞.....	48
3.3.5	IE 6.0 信息泄露漏洞.....	49
3.3.6	OutLook Express 6 的安全漏洞.....	49
3.4	网络服务的缺陷.....	50
3.4.1	FTP 服务器.....	50
3.4.2	E-mail 服务器.....	52
3.4.3	IIS 服务.....	55
3.5	管理上的缺陷.....	58

第二篇 网络防护实战篇

第 4 章	千奇百怪的计算机病毒.....	61
4.1	计算机病毒概述.....	61
4.2	计算机病毒从何而来.....	62
4.3	计算机病毒的分类.....	63
4.4	计算机病毒的危害.....	66
4.5	计算机病毒的防治策略和检测.....	68
4.5.1	计算机病毒的防治策略.....	68

4.5.2	计算机病毒的检测	69
4.6	预防病毒的几个忠告	75
第 5 章	自我保护措施: 反病毒常识	78
5.1	怎么知道自己的电脑染上病毒了	78
5.1.1	计算机病毒的一般特征	78
5.1.2	计算机染毒后的一些特征	79
5.1.3	计算机染毒后的应急处理	80
5.2	怎样对付普通病毒	81
5.2.1	对普通病毒的防护	81
5.2.2	对普通病毒的查杀	82
5.3	怎样处理电子邮件病毒	83
5.3.1	病毒是怎么通过电子邮件传播的	83
5.3.2	怎样防范电子邮件蠕虫	83
5.3.3	怎样彻底删除电子邮件附件	85
5.3.4	常见邮件病毒的防范	87
5.4	怎样对付宏病毒	90
5.5	几种典型流行病毒的介绍和查杀	93
5.5.1	欢乐时光	93
5.5.2	尼姆达	96
5.5.3	求职信	99
5.5.4	红色代码	101
5.6	怎样使用反病毒软件查杀病毒	103
5.6.1	启动 Norton AntiVirus	104

5.6.2	查看系统当前状态	104
5.6.3	扫描病毒	106
5.6.4	查看 Norton 的报告	112
5.6.5	更新病毒库 (LiveUpdate)	116
5.6.6	Norton AntiVirus 的配置	118
5.6.7	使用瑞星杀毒软件 2004	120
5.6.8	如何选择一款适合你的查毒软件	128
5.7	教你几招防毒小窍门	130
5.7.1	为何安装防病毒软件后还会被感染	130
5.7.2	如何备份病毒库	132
5.7.3	怎么防治利用系统漏洞传播的病毒	133
5.7.4	怎样防治经共享和弱口令传播的病毒	134
5.7.5	怎样防止病毒再感染	135
5.7.6	防治脚本病毒的小窍门	137
5.7.7	怎样防范引导型病毒	139
5.7.8	发送“纯文本”电子邮件	140
5.7.9	怎样应对“冲击波”	140
5.7.10	OutLook 防毒防垃圾大法	142

第 6 章 无孔不入的计算机黑客 146

6.1	计算机的刽子手：计算机黑客	146
6.1.1	什么是计算机黑客	146
6.1.2	黑客可以分为哪几种类型	148
6.1.3	黑客有什么样的危害	150

6.2	黑客入侵的一般步骤	150
6.3	黑客入侵的原理和手法	153
6.3.1	什么是口令入侵	153
6.3.2	什么是特洛伊木马程序	155
6.3.3	什么是欺骗技术	156
6.3.4	什么是电子邮件攻击	157
6.3.5	通过一个节点来攻击其他节点	158
6.3.6	网络监听是怎么回事	159
6.3.7	利用黑客软件攻击	160
6.3.8	安全漏洞攻击	160
6.3.9	端口扫描攻击	161
6.3.10	什么是后门程序	162
6.3.11	什么是拒绝服务攻击	162
6.3.12	什么是炸弹攻击	163
6.4	计算机黑客的最爱：黑客入侵工具	165
6.4.1	安全扫描类（包含端口扫描工具）	166
6.4.2	远程控制类工具（木马类）	178
6.4.3	网络嗅探器工具（sniffer）	186
第 7 章	拒绝黑客的拜访	194
7.1	如何知道你的计算机已经被黑客入侵	194
7.1.1	检查网络的连接状态	195
7.1.2	计算机关机时是否有联机记录	197
7.1.3	检查系统“启动”菜单中程序	198

7.2	个人计算机防黑教你 13 招	203
7.2.1	正确使用资源共享	203
7.2.2	不轻易运行不明真相的程序	206
7.2.3	拒绝可能有威胁的站点对自己的访问	207
7.2.4	定期清除临时文件	208
7.2.5	屏蔽 Cookie 信息.....	208
7.2.6	屏蔽 ActiveX 控件.....	209
7.2.7	出现故障时要及时检查系统信息	210
7.2.8	定期更新病毒库及扫描计算机病毒	211
7.2.9	定期更新防火墙规则	211
7.2.10	Windows 2000 中如何关闭 ICMP (ping)	213
7.2.11	不随意透露任何个人信息	217
7.2.12	慎选电子商务交易网站	218
7.2.13	加密重要的邮件	220
7.3	反黑客的护盾 Lockdown2000	221
7.3.1	Lockdown 的获得与安装	222
7.3.2	Lockdown 的界面介绍	223
7.3.3	Lockdown 的使用方法	224
7.3.4	Lockdown 的卸载.....	225
7.4	网络安全工具 NetSpider.....	225
7.4.1	NetSpider 简介	226
7.4.2	主要功能介绍	226

7.5	养成良好的维护习惯	240
7.5.1	查看防毒软件功能的安全强度	241
7.5.2	查看防火墙功能的安全强度	242
7.5.3	主机存取权限管理	243
7.5.4	系统数据备份	244
第 8 章	小心特洛伊木马	246
8.1	什么是特洛伊木马	246
8.2	木马的工作原理	247
8.2.1	木马的基本机制	247
8.2.2	木马的种类	249
8.2.3	木马的伪装方法	250
8.2.4	木马为什么会在你的系统之中	252
8.2.5	木马能干什么	254
8.3	一些典型木马简介、预防和清除	255
8.3.1	木马的通用防范、清除方法	256
8.3.2	一些典型木马的防范、清除	267
8.3.3	常见特洛伊木马程序的缺省端口	276
8.3.4	常见特洛伊木马的进程名称	281
8.3.5	防范木马的根本方法：良好的上网习惯	282
第 9 章	网络炸弹的防范	286
9.1	电子邮件炸弹	286
9.1.1	电子邮件炸弹的概念与危害	287
9.1.2	电子邮件炸弹工具：KaBoom 3.0	288

9.1.3	如何防范电子邮件炸弹的攻击	291
9.1.4	清除工具: Spam Exterminator	295
9.2	QQ 炸弹攻防	299
9.2.1	如何“炸”别人	299
9.2.2	常见的 QQ 炸弹工具	302
9.2.3	如何防范 QQ 炸弹	307
9.3	新闻组炸弹	310
9.3.1	集束炸弹	310
9.3.2	JAVA 炸弹	311
9.4	其他网络炸弹	312
9.4.1	ping 炸弹	312
9.4.2	Nuke	312
第 10 章	如何建立个人防火墙	313
10.1	什么是防火墙	313
10.1.1	防火墙的概念	313
10.1.2	防火墙的起源与发展	315
10.1.3	防火墙中用到的术语	316
10.1.4	防火墙的体系结构	317
10.1.5	防火墙的分类	319
10.2	防火墙能帮你做什么	323
10.3	什么样的防火墙才是你需要的	324
10.4	常用防火墙简介	324
10.4.1	个人防火墙需要进行的配置	325

10.4.2	Norton Internet Security	325
10.4.3	瑞星个人防火墙 2004	339
10.4.4	ZoneAlarm.....	343
10.4.5	BlackICE Defender	350
10.4.6	McAfee VirusScan DAT.....	356
10.4.7	Sygate Personal Firewall	361

第三篇 个人隐私保护篇

第 11 章	你的电脑完美无瑕吗	372
11.1	计算机操作系统的安全	372
11.1.1	清除共享文件夹的安全隐患	372
11.1.2	转换文件系统格式	377
11.1.3	关机时清除系统的页面文件	378
11.1.4	禁止 Windows 创建转储文件	379
11.1.5	关闭无用的 Windows 服务	381
11.2	利用注册表设置 Windows 的安全	382
11.2.1	如何在局域网中隐藏计算机名称	382
11.2.2	如何抵御后门程序的破坏	383
11.2.3	如何屏蔽对软盘的网络访问	383
11.2.4	如何屏蔽对控制面板的访问	384
11.2.5	如何禁止访问“文件系统”选项	385
11.2.6	如何限制用户使用指定程序	385
11.2.7	如何恢复对注册表的错误修改	386

11.3	系统账户的安全	387
11.3.1	如何禁用 Guest 账户	387
11.3.2	如何管理 Administrator 账户	387
第 12 章	个人隐私保护	389
12.1	先从你的操作系统入手	389
12.1.1	选择更为安全的磁盘格式 NTFS	389
12.1.2	Windows 系统隐私保密技巧	393
12.2	怎样安全使用你的邮件系统	410
12.2.1	共用计算机时邮箱怎样保密	410
12.2.2	如何为你的邮件加上数字签名	411
12.2.3	给你的电子邮箱加上过滤网	413
12.2.4	如何保护好你存储邮件的文件夹	414
12.2.5	禁止邮件中的弹出式广告	418
12.2.6	让可恶的垃圾邮件销声匿迹	421
12.3	让 QQ 更安全	423
12.3.1	如何隐藏你上网的 IP 地址	423
12.3.2	如何在 QQ 中隐藏你的 IP	424
12.3.3	对付盗取 QQ 木马的终极办法	426
12.3.4	“网吧族”的 QQ 防范措施	430
12.3.5	QQ 安全防范四种武器	432
12.4	如何让网上浏览更安全	437

第一篇 网络安全基础篇

此篇为计算机网络的初学者介绍了计算机网络中的基本概念，并且以实际的操作例程让读者对这些知识能够掌握得更加牢固，理解更为透彻。同时，还介绍了关于网络安全的背景知识，比较系统地分析了导致网络安全问题的各种原因。通过本篇的学习，读者将对网络的脆弱性有一个清醒的认识，从操作系统到网络设备到应用软件，网络服务无处不存在安全漏洞，这些都给黑客带来了可乘之机，所以无论是网络安全的管理人员，还是使用计算机的普通个人用户，都要增强安全意识并采取一定的防范措施，才不至于被黑客随便入侵。