



普通高等教育“十一五”国家级规划教材
高等学校计算机科学与技术教材

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

信息与网络安全

□ 程光 张艳丽 江洁欣 编著

清华大学出版社

● 北京交通大学出版社



TP393.08/264

2008

普通高等学校“十一五”国家级规划教材
高等学校计算机科学与技术教材

信息与网络安全

程 光 张艳丽 江洁欣 编著

清华大学出版社

北京交通大学出版社

·北京·

内 容 简 介

本书是针对计算机和信息安全专业教学而编写的教材。通过该教材的学习,学生可以掌握计算机网络安全的基本概念,了解网络设计、维护及应用系统安全的基本手段和常用方法。

全书共14章,分为四个部分。第一部分概述信息与网络安全相关知识;第二部分分五章讲述信息安全技术相关内容,包括常规加密技术、DES数据加密标准、公钥加密技术,基于加密技术的数字签名、身份鉴别等网络安全应用,以及信息隐藏技术等;第三部分分四章介绍网络安全相关技术,这部分内容包括网络安全的防御技术和相关的网络安全协议等;第四部分分四章介绍信息与网络检测的相关实用技术,包括入侵检测技术、信息获取技术、安全信息取证和逆向工程等。

本书适合作为“信息与网络安全”课程的教材,也可供相关技术人员作为参考用书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13501256678 13801310933

图书在版编目(CIP)数据

信息与网络安全/程光,张艳丽,江洁欣编著. —北京:清华大学出版社;北京交通大学出版社,2008.6

(高等学校计算机科学与技术教材)

普通高等学校“十一五”国家级规划教材

ISBN 978-7-81123-309-4

I. 信… II. ①程… ②张… ③江… III. 电子计算机-安全技术-高等学校-教材
IV. TP309

中国版本图书馆CIP数据核字(2008)第063091号

责任编辑:谭文芳

出版发行:清华大学出版社 邮编:100084 电话:010-62776969 <http://www.tup.com.cn>

北京交通大学出版社 邮编:100044 电话:010-51686414 <http://press.bjtu.edu.cn>

印刷者:北京东光印刷厂

经 销:全国新华书店

开 本:185×260 印张:20.5 字数:525千字

版 次:2008年6月第1版 2008年6月第1次印刷

书 号:ISBN 978-7-81123-309-4/TP·417

印 数:1~5 000册 定价:32.00元

本书如有质量问题,请向北京交通大学出版社质监组反映。对您的意见和批评,我们表示欢迎和感谢。

投诉电话:010-51686043, 51686008; 传真:010-62225406; E-mail: press@bjtu.edu.cn。

前言

本书是普通高等教育“十一五”国家级规划教材。

随着互联网渗透到人们社会经济生活的各个方面,由于信息与网络的安全导致的损失日益加剧,信息与网络安全问题也越来越被人们所重视,已成为信息化建设的核心问题。鉴于目前信息与网络安全的重要性,培养和提高未来计算机专业人员信息和网络安全的基础理论和实践技能,已成为目前计算机专业教学的重点课程之一,不少高校已经开设信息与网络安全相关课程和专业。

由于互联网技术的快速发展,信息和网络安全技术有较强的时效性,而目前的教材不能很好地涵盖新的理论和技术,因此,有必要编写面向计算机和信息安全专业本科生的“信息与网络安全”教材。通过该教材的学习,学生可以掌握计算机网络安全的基本概念,并了解网络设计、维护及其应用系统安全的基本手段和常用方法。

本书作者一直参加“CERNET 华东北地区网络中心”和“江苏省计算机网络重点实验室”的建设和管理,具有长期从事计算机网络方面的研究和开发经历,以及多年管理运行区域性 IP 网络的经验;参加和主持过各类相关的国家级课题,开展过网络管理、网络安全体系结构、网络数据安全机制等方面的研究,具有丰富的网络理论、管理和使用经验;连续多年在东南大学进行了“信息与网络安全”等相关课程的教学工作,具有丰富的信息与网络安全教学经验。本书的主要内容已经作为讲义连续 4 年在课堂上先后对 800 多名本科学生进行了讲授,对学生展开课程设计和生产实践都有一定帮助。

本书主要面向全国计算机专业和信息安全专业本科教学而编写。教材主要从先进性、实用性和培养学生多学科综合能力、解决实际问题等几个方面着手,力求通过科研和教学实践,不断完善该学科知识体系结构和内容,使该课程知识更为系统化和实用化,更能适合目前我国信息与网络安全工作和科研的需要。本教材从加密理论、安全协议、安全应用等几个大方向,强调本课程与专业间的逻辑关系,并以目前常见的安全问题实例为分析依据,使教材具有新颖性、知识性和实用性等特点。

本书主要特色体现在以下三个方面。

1. 技术方法的成熟与先进相互结合和补充,理论与实践相结合

本书涉及的内容和技术方法立足于学科前沿,且其理论和实践方法紧密联系信息与网络安全现状。每一章都包含相关理论与技术工具和习题,通过相关工具的学习和习题的完成,能帮助读者更深刻地理解所学习的知识,并学会使用现有的工具解决网络应用过程中所遇到的各类实际问题。

2. 取材先进,内容、体系具有创新性

本书在内容安排上,力求在全面的基础上突出实用性,强调教学与科研、理论和实际的紧密联系,注重书本知识与信息和网络安全的具体应用相结合。同时保留具有探索性、有待完善的国内外研究理论和应用研究方面的知识,力求达到丰富教学内容、加强基础知识教育

和拓宽学生思路,以及培养学生自主思考问题能力的培养目标。

3. 前瞻性

本书不仅对专业的基础理论进行归纳总结,而且对专业的发展趋势及当前热点问题进行了介绍,具有前瞻性。既可满足本科教学也可供专业的技术人员参考。

本书共14章,分为4个部分。第一部分概述信息与网络安全相关知识。第二部分(第2~6章)讲述信息安全技术相关内容,包括常规加密技术,DES数据加密标准,公钥加密技术,基于加密技术的数字签名、身份鉴别等网络安全应用,以及信息隐藏技术等。第三部分(第7~10章)介绍网络安全相关技术,这部分内容主要介绍网络安全的防御技术和相关的网络安全协议等。第四部分(第11~14章)介绍信息与网络检测的相关实用技术,包括入侵检测技术、信息获取技术、安全信息取证和逆向工程等。

本书由程光担任主编。第1~6章、第11~12章由程光编写,第7~10章由张艳丽、程光共同编写,第13、14章由江洁欣、程光共同编写。本书最后由程光进行统稿。

由于信息与网络安全内容发展很快,无法确保将这个领域中的精华全部荟萃。加上作者的水平有限,书中内容有不当之处,敬请广大读者批评指正。

2008年5月于东南大学

目 录

第1章 信息与网络安全概述	1
1.1 信息与网络安全现状	1
1.1.1 互联网的重要性	1
1.1.2 我国互联网现状	2
1.1.3 网络安全现状	3
1.1.4 我国网络安全现状	5
1.2 常见的网络攻击方法	5
1.2.1 暴力攻击和字典程序攻击	6
1.2.2 DoS 攻击	6
1.2.3 欺骗攻击	6
1.2.4 中间人攻击	7
1.2.5 探测攻击	8
1.2.6 垃圾邮件攻击	8
1.3 网络安全威胁和攻击	8
1.3.1 网络安全威胁	8
1.3.2 网络安全攻击	10
1.4 安全政策和机制	10
1.4.1 安全服务	10
1.4.2 安全机制	12
1.4.3 安全模式	13
1.4.4 安全评估	14
1.5 安全标准和组织	15
1.5.1 安全标准化组织	16
1.5.2 互联网相关的安全协议和机制	17
1.5.3 中国的信息安全标准	18
小结	20
习题	20
第2章 密码学基础	21
2.1 密码学的发展概况	21
2.1.1 第1阶段：古典密码	22
2.1.2 第2阶段：常规现代密码学	23
2.1.3 第3阶段：公钥密码学	23
2.2 密码技术的目标	23

2.2.1	保密性	24
2.2.2	完整性	24
2.2.3	身份认证	24
2.2.4	认可	24
2.3	密码学基本概念	24
2.3.1	概念	25
2.3.2	密码系统分类	25
2.3.3	密码分析	26
2.4	替代技术	26
2.4.1	恺撒密码	26
2.4.2	单字母替代	27
2.4.3	单一字母密码破译	28
2.4.4	多字母替代密码	29
2.5	置换技术	29
2.5.1	栅栏技术	30
2.5.2	矩阵技术	30
2.6	转子机	31
2.6.1	转子机发展历史	31
2.6.2	转子机原理	32
2.7	明文处理方式	32
2.7.1	分组密码	32
2.7.2	流密码	33
	小结	33
	习题	34
第3章	常规现代加密技术	35
3.1	常规加密技术的概述	35
3.1.1	香农的 SP 网络	35
3.1.2	对称密码技术的密钥	35
3.1.3	对称密钥系统的弱点	36
3.2	分组加密的原理	36
3.2.1	分组密码的一般设计原理	36
3.2.2	Feistel 网络基本原理	37
3.3	简化的 DES 算法	38
3.3.1	S-DES 加密原理	38
3.3.2	S-DES 加密算法五个函数	39
3.3.3	S-DES 的密钥生成	41
3.4	DES 算法	42
3.4.1	DES 背景	42
3.4.2	DES 原理	42

45	3.4.3	DES 的函数	43
45	3.4.4	DES 的安全特性	46
45	3.5	DES 的工作模式	47
47	3.5.1	电子密码本 ECB	47
47	3.5.2	密码分组链接 CBC	48
47	3.5.3	密码反馈 CFB	49
48	3.5.4	输出反馈 OFB	49
48	3.6	多重 DES	51
48	3.6.1	两重 DES	51
48	3.6.2	三重 DES	52
48	3.7	常规加密的保密通信	52
48	3.7.1	链路层加密	52
48	3.7.2	端对端加密	53
48	小结		53
48	习题		54
48	第4章	公钥密码学技术	55
48	4.1	公开密码学概述	55
48	4.1.1	公钥密码学的基本概念	55
48	4.1.2	公钥算法的特点	55
48	4.1.3	常用公钥算法	57
48	4.1.4	基于公钥算法的密钥交换	57
48	4.2	Diffie-Hellman 密钥交换算法	57
48	4.2.1	单向陷门函数	58
48	4.2.2	Diffie-Hellman 密钥交换算法	58
48	4.3	RSA 算法	59
48	4.3.1	RSA 算法的实现	59
48	4.3.2	RSA 算法的安全性分析	60
48	4.4	DSA 算法	60
48	4.4.1	DSA 算法原理	60
48	4.4.2	DSA 算法签名应用	61
48	4.5	PGP 技术	61
48	4.5.1	PGP 概述	61
48	4.5.2	PGP 原理	62
48	4.5.3	PGP 密钥对	64
48	4.5.4	加密与签名	66
48	4.5.5	PGP 密钥	67
48	4.6	公钥基础设施 PKI	70
48	4.6.1	PKI 概念	70
48	4.6.2	CA 系统	72

4.6.3	数字证书	74
4.6.4	CA 信任关系	75
4.7	密钥管理	77
4.7.1	密钥使用实例	77
4.7.2	密钥分发	78
4.8	工具介绍	79
	小结	82
	习题	82
第5章	数据保护技术	83
5.1	哈希函数	83
5.1.1	哈希函数的概念	83
5.1.2	MD5	84
5.1.3	H_{MD5}	85
5.1.4	MD5 的安全性	87
5.1.5	MD5 算法应用	88
5.2	数字签名	88
5.2.1	数字签名概念	88
5.2.2	直接数字签名	89
5.2.3	仲裁数字签名	90
5.2.4	数字签名算法	91
5.3	消息鉴别	92
5.3.1	消息鉴别概述	92
5.3.2	消息加密	92
5.3.3	消息鉴别码	94
5.3.4	哈希函数	94
5.4	身份认证	95
5.4.1	身份认证的概述	95
5.4.2	双向认证协议	96
5.4.3	单向认证协议	98
5.5	身份认证实例——Kerberos	99
5.5.1	身份认证存在问题	99
5.5.2	Kerberos 的解决方案	99
5.5.3	Kerberos V4	100
5.6	数据保护工具	101
5.6.1	Hash Calc	101
5.6.2	SSO Plus	102
	小结	102
	习题	103
第6章	数据隐藏技术	104

6.1	数据隐藏技术的基本概念	104
6.1.1	数据隐藏技术的实例	104
6.1.2	数据隐藏技术的基本特性	105
6.1.3	数据隐藏的原理	106
6.1.4	数据隐藏技术的应用	108
6.2	基于文本的数据隐藏技术	108
6.2.1	语义法	109
6.2.2	造句法	109
6.2.3	特征替换法	110
6.3	基于图像的数据隐藏技术	110
6.3.1	最低有效位法 (LSB)	110
6.3.2	图像频域变换方法	111
6.3.3	知觉掩饰方法	112
6.4	基于音频的数据隐藏技术	113
6.4.1	人类听觉系统	113
6.4.2	相位隐藏法	114
6.4.3	时域中的音频数据隐藏	114
6.4.4	回声隐藏方法	115
6.5	信息隐藏技术的攻击	115
6.5.1	鲁棒性攻击	116
6.5.2	对回音隐藏的攻击	116
6.5.3	其他普通攻击	117
6.5.4	其他类型攻击	117
6.6	数据文件隐藏工具	118
6.6.1	图像隐藏工具 JPHS	118
6.6.2	音频隐藏工具 MP3Stego	119
6.6.3	图像文本隐藏工具 wbStego	120
	小结	120
	习题	120
第7章	网络防御技术	122
7.1	网络访问认证	122
7.1.1	PPP 网络访问认证协议	122
7.1.2	AAA 网络访问认证协议	126
7.1.3	局域网访问认证协议	128
7.1.4	基于口令的用户认证	129
7.2	访问控制	131
7.2.1	访问控制方法	131
7.2.2	访问控制策略	132
7.2.3	Linux 的访问控制	134

401	7.2.4 Windows XP 的访问控制	135
401	7.3 防火墙技术	136
201	7.3.1 防火墙的功能	136
301	7.3.2 防火墙的体系结构	137
301	7.3.3 防火墙相关技术	139
301	7.3.4 个人防火墙设置	141
201	7.4 病毒和木马防范	143
201	7.4.1 病毒及木马概述	143
011	7.4.2 病毒和木马的预防	145
011	7.4.3 病毒防御的实例	147
011	7.4.4 病毒和木马举例	148
111	7.5 工具介绍	149
111	7.5.1 360 安全卫士	149
111	7.5.2 口令卡	150
111	小结	151
111	习题	152
	第8章 IP 和 TCP 层安全	153
211	8.1 TCP/IP 安全概述	153
211	8.1.1 TCP/IP 概述	153
011	8.1.2 TCP/IP 协议层次模型	155
011	8.1.3 TCP 协议和 IP 协议	156
711	8.1.4 TCP/IP 协议族中的安全问题	156
711	8.1.5 TCP/IP 协议安全问题解决办法	160
311	8.2 IPSec 概述	160
311	8.2.1 IPSec 的概念	160
011	8.2.2 安全关联	161
051	8.2.3 头部认证	163
051	8.2.4 封装安全载荷	166
051	8.2.5 Internet 密钥交换	170
551	8.2.6 IPSec 方案中的问题	171
551	8.3 SSL 协议	172
551	8.3.1 SSL 协议概述	172
051	8.3.2 SSL 协议的结构	172
851	8.3.3 SSL 协议的应用和安全性	174
051	8.4 SSH 协议	174
161	8.4.1 SSH 协议概述	175
161	8.4.2 SSH 协议结构	175
561	8.4.3 主机密钥机制和用户认证方法	176
421	8.4.4 SSH 协议工作过程	177

8.4.5	SSH 协议扩展性和应用	178
	小结	178
	习题	179
第9章	应用层安全	180
9.1	应用层安全概述	180
9.1.1	应用层安全问题	180
9.1.2	应用层安全防御方法	182
9.2	S-HTTP 协议	183
9.2.1	S-HTTP 简介	183
9.2.2	S-HTTP 协议	184
9.2.3	S-HTTP 加密参数	185
9.2.4	S-HTTP 的连接过程	186
9.3	S/MIME 协议	186
9.3.1	S/MIME 概念	186
9.3.2	S/MIME 基本功能	187
9.3.3	S/MIME 消息产生	187
9.3.4	S/MIME 报文准备	188
9.4	SET 协议	189
9.4.1	SET 协议概述	189
9.4.2	SET 协议的安全技术	191
9.4.3	SET 的交易流程	194
9.4.4	SET 交易的购买请求过程	195
	小结	196
	习题	197
第10章	安全网络技术	198
10.1	VPN 技术	198
10.1.1	VPN 的概念	198
10.1.2	VPN 的作用	199
10.1.3	VPN 的分类	199
10.1.4	VPN 实现技术	200
10.2	无线网络安全	202
10.2.1	无线网络分类	202
10.2.2	无线网络安全技术	204
10.2.3	无线网络监视工具	206
10.2.4	增强无线网络安全方法	207
10.3	IPv6 的安全	208
10.3.1	IPv6 介绍	208
10.3.2	IPv6 与 IPSec	209
10.3.3	IPv6 安全问题	211

851	10.4 VoIP 的安全	213
851	10.4.1 VoIP 概述	213
951	10.4.2 VoIP 系统	213
081	10.4.3 H.323 和 SIP 介绍	216
081	10.4.4 VoIP 的安全	218
021	10.5 工具介绍	222
581	小结	225
681	习题	226
	第11章 入侵检测技术	227
481	11.1 入侵检测系统的基本原理	228
281	11.1.1 入侵检测系统的概述	228
081	11.1.2 入侵检测系统的术语	228
081	11.1.3 入侵检测体系结构	229
081	11.2 入侵检测系统的分类	231
781	11.2.1 按技术分类	231
781	11.2.2 按照数据来源分类	233
881	11.3 入侵检测系统的技术指标	234
081	11.3.1 误报	234
981	11.3.2 漏报	235
101	11.3.3 管理能力	235
401	11.3.4 鲁棒性	236
201	11.4 入侵检测的标准化和发展方向	236
001	11.4.1 入侵检测工作组	236
701	11.4.2 通用入侵检测框架	237
801	11.4.3 入侵检测系统的技术难点	237
801	11.4.4 入侵检测发展趋势	238
801	11.5 入侵检测系统的实例	240
001	11.5.1 LIDS	240
001	11.5.2 Snort	244
005	11.5.3 一个基于异常检测实例	247
505	小结	251
505	习题	251
	第12章 网络信息获取技术	252
205	12.1 网络信息收集	252
705	12.1.1 信息	252
805	12.1.2 社会信息	252
805	12.1.3 Whois	253
005	12.1.4 DNS 查询	254
115	12.2 网络扫描技术	255

12.2.1	扫描器	255
12.2.2	主机扫描技术	256
12.2.3	端口扫描技术	257
12.2.4	栈指纹技术	259
12.2.5	NMAP	260
12.3	网络流量侦听技术	261
12.3.1	Linux 的侦听技术	261
12.3.2	Windows 的侦听技术	262
12.3.3	网络流量侦听工具	263
12.4	高速网络测量技术	264
12.4.1	测量技术的发展	264
12.4.2	主动测量技术	265
12.4.3	被动测量技术	265
12.4.4	抽样测量技术	266
12.4.5	网络分布式测量平台	267
12.5	网络测量常用工具	268
12.5.1	ping	268
12.5.2	traceroute	269
12.5.3	netstat 工具	269
12.5.4	SNMP 协议	269
12.6	案例分析	270
12.6.1	主机故障的诊断案例	270
12.6.2	网络故障的诊断案例	271
	小结	272
	习题	272
第 13 章	逆向工程	273
13.1	逆向工程概述	273
13.1.1	机械和军事中的逆向工程	273
13.1.2	软件逆向工程	274
13.1.3	逆向工程的历史	275
13.2	调试器与反汇编器	275
13.2.1	调试器	275
13.2.2	反汇编器	277
13.3	逆向分析方法实例	279
13.3.1	Win32 进程内存空间	279
13.3.2	破解简单 CrackMe	279
13.3.3	从注册信息到注册码计算	281
13.4	断点	286
13.4.1	断点的概念	286

13.4.2	实例三: WinAPI 断点	286
13.5	专用工具	289
13.5.1	PE 信息查看工具	289
13.5.2	用 DEDE 工具分析 Delphi 程序	289
	小结	290
	习题	291
第 14 章	计算机取证	292
14.1	计算机取证基础	292
14.1.1	计算机取证概述	292
14.1.2	取证工作流程	293
14.1.3	取证模型	294
14.2	计算机操作系统	295
14.2.1	Windows 操作系统	295
14.2.2	UNIX 操作系统	296
14.3	文件系统	297
14.3.1	文件系统概述	297
14.3.2	主引导记录	298
14.3.3	FAT 文件系统	299
14.3.4	NTFS 文件系统	302
14.4	数据恢复和收集	305
14.4.1	数据恢复	305
14.4.2	数据收集	307
	小结	308
	习题	309
	参考文献	310

网络资源日益丰富,网络中信息量急剧增加,其安全问题日益突出。网络中信息量急剧增加,其安全问题日益突出。网络中信息量急剧增加,其安全问题日益突出。

第1章 信息与网络安全概述

本章要点

- ☑ 信息与网络安全现状
- ☑ 常见的网络攻击方法
- ☑ 网络安全威胁和攻击
- ☑ 安全政策和机制
- ☑ 安全标准和组织

我们现在生活在各种类型的电子信息和网络环境中,如:办公室和家庭的个人计算机;数据库服务器,如数据库、Web 服务器;电话系统;移动电话;便携式设备,如笔记本、PDA(Personal Digital Assistant,个人数字助理)、GPS(Global Positioning System,全球定位系统);无线网络;公用信息系统,如银行 ATM 系统;有线电视系统;汽车和家庭设备中内嵌式系统;智能卡系统;等等。在享受网络丰富的信息资源给用户带来了极大方便的同时,计算机病毒、黑客入侵及木马控制、垃圾邮件等也给互联网的运行系统、基于互联网的重要应用系统和广大互联网用户带来了越来越多的麻烦。因此,保证互联网的健康发展,信息与网络安全是首先要解决的问题。

网络安全面临着多个方面的挑战:

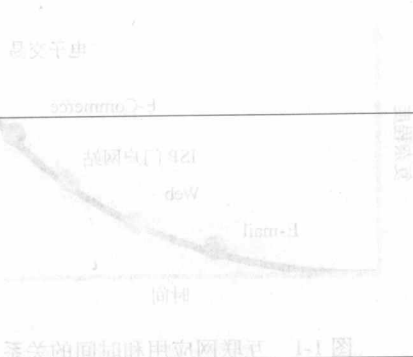
- ☞ 保护大量不同的安全系统;
- ☞ 保护不同系统之间的接口;
- ☞ 不同的系统具有不同的安全目标 and 需求;
- ☞ 攻击者寻找系统中最薄弱的环节进行攻击;
- ☞ 需要保护系统中每个环节的安全性;
- ☞ 维护系统的稳定性;
- ☞ 控制系统安全维护的代价等。

另外,在网络防御方面,人们所要面临的安全问题往往是难以预测的,因此需要网络安全人员保持警惕,以使信息网络风险降低至最小程度。同时反病毒措施落后于病毒的发展速度已经是不争的事实,因此仅仅依靠给系统打补丁、安装网络防火墙等常规措施,将使用户长期处于被动地位。

1.1 信息与网络安全现状

1.1.1 互联网的重要性

图 1-1 所示为互联网应用与时间的关系,它表明互联网变得越来越重要,对人们的生活影



响也越来越大。互联网开始仅提供信息交流的工具,如发送、接收电子邮件,然后逐渐发展成为信息发布平台,再发展成和人们生活密切相关的电子交易平台。另外,互联网的应用也越来越复杂,最初的 E-mail 应用不涉及任何安全问题,只是简单的数据收发;现在的电子交易涉及很多网络安全技术,如加密、鉴别、访问控制、数据签名,等等。



图 1-1 互联网应用和时间的关系

图 1-2 是 Internet 软件联盟 (Internet Software Consortium, ISC) 2007 年 7 月根据 DNS (Domain Name System, 域名系统) 服务器中主机数据,统计的全球互联网主机的数量。1993 年 1 月全世界互联网主机是 1 313 000 台,到 2008 年 1 月发展到有 541 677 360 台,互联网主机的发展速度以指数方式递增。互联网主机的增加,使得互联网能够影响更多人的生活和工作,同时互联网的安全也愈加重要。

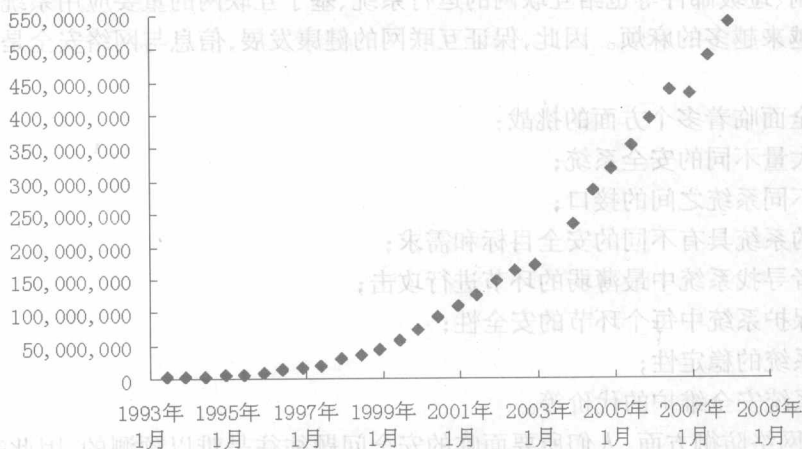


图 1-2 Internet 软件联盟统计的全球互联网主机数量

1.1.2 我国互联网现状

根据中国互联网络信息中心 (China Internet Network Information Center, CNNIC) 的调查分析,截至 2007 年 12 月 31 日,中国网民的数量已经达到 2.1 亿 (见图 1-3),位居世界第二,是仅次于美国 (2.15 亿) 的网民规模。比 2006 年年末新增了 7300 万网民。2007 年中国网民年增长率达到 53.3%,步入新一轮的快速增长阶段。