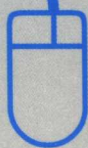


可下载教学资料

<http://www.tup.tsinghua.edu.cn>



高等学校教材
计算机科学与技术

计算机网络安全

刘远生 主编
辛一 薛庆水 副主编

清华大学出版社



高等学校教材
计算机科学与技术

计算机网络安全

刘远生 主编
辛一 薛庆水 副主编

清华大学出版社
北京

内 容 简 介

本书以网络安全通常采取的安全措施(对策)为主线,系统地介绍了网络安全知识和技术,重点介绍了网络系统的安全运行和网络信息的安全保护,内容包括操作系统安全、数据库与数据安全、网络实体安全、数据加密与鉴别、防火墙安全、网络病毒防治、入侵检测与防护、黑客攻击及防范、网络扫描和网络监听、Internet 服务安全和典型的网络安全应用实例等。

本书内容安排合理,逻辑性强,语言通俗易懂。着重介绍网络安全的概念和应用,书中实例的应用性和可操作性强。各章配有丰富的习题,便于教学和自学。

本书可作为高等院校计算机类专业本科生的教材,也可作为网络管理人员、网络工程技术人员和信息安全管理人员以及对网络安全感兴趣的一般读者的参考书。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

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。

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。

图书在版编目(CIP)数据

计算机网络安全/刘远生主编. —北京:清华大学出版社,2006.5

(高等学校教材·计算机科学与技术)

ISBN 7-302-12653-4

I. 计… II. 刘… III. 计算机网络—安全技术—高等学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2006)第 017809 号

出版者:清华大学出版社 地 址:北京清华大学学研大厦

<http://www.tup.com.cn> 邮 编:100084

社 总 机:010-62770175 客 户 服 务:010-62776969

责任编辑:付弘宇

印刷者:北京鑫丰华彩印有限公司

装订者:三河市化甲屯小学装订二厂

发 行 者:新华书店总店北京发行所

开 本:185×260 印张:22 字数:540千字

版 次:2006年5月第1版 2006年5月第1次印刷

书 号:ISBN 7-302-12653-4/TP·8090

印 数:1~4000

定 价:29.00元

编审委员会成员

(按地区排序)

清华大学	周立柱	教授
	覃 征	教授
	王建民	教授
	刘 强	副教授
	冯建华	副教授
北京大学	杨冬青	教授
	陈 钟	教授
	陈立军	副教授
北京航空航天大学	马殿富	教授
	吴超英	副教授
	姚淑珍	教授
中国人民大学	王 珊	教授
	孟小峰	教授
	陈 红	教授
北京师范大学	周明全	教授
北京交通大学	阮秋琦	教授
北京信息工程学院	孟庆昌	教授
北京科技大学	杨炳儒	教授
石油大学	陈 明	教授
天津大学	艾德才	教授
复旦大学	吴立德	教授
	吴百锋	教授
	杨卫东	副教授
华东理工大学	邵志清	教授
华东师范大学	杨宗源	教授
	应吉康	教授
东华大学	乐嘉锦	教授
上海第二工业大学	蒋川群	教授
浙江大学	吴朝晖	教授
	李善平	教授
南京大学	骆 斌	教授
南京航空航天大学	秦小麟	教授
南京理工大学	张功萱	教授

南京邮电学院	朱秀昌	教授
苏州大学	龚声蓉	教授
江苏大学	宋余庆	教授
武汉大学	何炎祥	教授
华中科技大学	刘乐善	教授
中南财经政法大学	刘腾红	教授
华中师范大学	王林平	副教授
	魏开平	教授
武汉理工大学	李中年	教授
国防科技大学	赵克佳	教授
	肖 依	副教授
中南大学	陈松乔	教授
湖南大学	林亚平	教授
	邹北骢	教授
西安交通大学	沈钧毅	教授
	齐 勇	教授
长安大学	巨永峰	教授
西安石油学院	方 明	教授
西安邮电学院	陈莉君	副教授
哈尔滨工业大学	郭茂祖	教授
吉林大学	徐一平	教授
	毕 强	教授
长春工程学院	沙胜贤	教授
山东大学	孟祥旭	教授
	郝兴伟	教授
山东科技大学	郑永果	教授
中山大学	潘小轰	教授
厦门大学	冯少荣	教授
福州大学	林世平	副教授
云南大学	刘惟一	教授
重庆邮电学院	王国胤	教授
西南交通大学	杨 燕	副教授

改革开放以来,特别是党的十五大以来,我国教育事业取得了举世瞩目的辉煌成就,高等教育实现了历史性的跨越,已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上,高等教育规模取得如此快速的发展,创造了世界教育发展史上的奇迹。当前,教育工作既面临着千载难逢的良好机遇,同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾,是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001年8月,教育部下发了《关于加强高等学校本科教学工作,提高教学质量的若干意见》,提出了十二条加强本科教学工作提高教学质量的措施和意见。2003年6月和2004年2月,教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件,指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007年教育振兴行动计划》的重要组成部分,精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间(2003—2007年)建设1500门国家级精品课程,利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放,以实现优质教学资源共享,提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作,提高教学质量的若干意见》精神,紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”,在有关专家、教授的倡议和有关部门的大力支持下,我们组织并成立了“清华大学出版社教材编审委员会”(以下简称“编委会”),旨在配合教育部制定精品课程教材的出版规划,讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师,其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求,“编委会”一致认为,精品课程的建设工作从开始就要坚持高标准、严要求,处于一个比较高的起点上;精品课程教材应该能够反映各高校教学改革与课程建设的需要,要有特色风格、有创新性(新体系、新内容、新手段、新思路,教材的内容体系有较高的科学创新、技术创新和理念创新的含量)、先进性(对原有的学科体系有实质性的改革和发展、顺应并符合新世纪教学发展的规律、代表并引领课程发展的趋势和方向)、示范性(教材所体现的课程体系具有较广泛的辐射性和示范性)和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

- (1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。
- (2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。
- (3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。
- (4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。
- (5) 高等学校教材·信息管理与信息系统。

清华大学出版社经过近 20 年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材经过 20 多年的精雕细刻,形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会
E-mail: dingl@tup.tsinghua.edu.cn

计算机网络的发展,特别是 Internet 的发展和普及,为人类带来了新的工作、学习和生活方式,人们与计算机网络的联系也越来越密切。计算机网络系统提供了丰富的资源以方便用户共享,提高了系统的灵活性和便捷性,但也正是这些特点,增加了网络系统的脆弱性、网络受威胁和攻击的可能性以及网络安全的复杂性。因此,随着资源共享程度的加强,计算机网络系统的安全问题也变得日益突出和复杂。在计算机网络应用过程中,人们发现自己的系统不断受到侵害,系统信息不断遭到破坏,其形式的多样化、技术的先进和复杂化,令人防不胜防。因此,使计算机网络系统免受破坏,提高系统的安全可靠性,已成为人们关注和亟须解决的问题。每个网络机构的管理人员、网络系统用户和工程技术人员都应该掌握一定的计算机网络安全技术,以使自己的信息系统能够安全稳定地运行并提供正常的安全服务。

当然,解决网络系统的安全问题是一个系统工程,它不仅涉及到技术问题,还涉及到管理、法律和道德,因而也是一个社会问题。

本书以网络安全通常采取的防护、检测、响应和恢复措施(对策)为主线,较系统地介绍网络安全知识和技术,重点介绍了网络系统的安全运行和网络信息安全保护。全书共有 10 章,内容包括:计算机网络安全概述,网络操作系统安全,计算机网络实体安全,数据库与数据安全,数据加密与鉴别,防火墙,计算机病毒及其防治,安全检测与响应,Internet 安全和网络安全应用实例。

通过对本书的学习,可使学生较全面地了解网络系统安全的基本概念、网络安全技术和应用,也使学生增强对网络安全工具(软件)应用的认识,了解和掌握对网络安全进行有效保护的实际操作技能。

本书可作为高等院校计算机专业、通信专业及相关专业的本科生、大专生教材,也可作为网络管理人员、网络工程技术人员和信息安全管理人员以及对网络安全感兴趣的读者的参考书。本书涉及的内容比较广泛,读者在学习和参考时,可在内容、重点和深度上酌情选取。

本书由刘远生任主编,辛一、薛庆水任副主编。刘远生编写了第 1、3、4、7、8、9 章,辛一编写了第 2、10 章,薛庆水编写了第 5、6 章,全书由刘远生统阅定稿。

在本书的立项、大纲编写和内容的确定以及全书的编写过程中得到了清华大学出版社各位同志的大力支持和帮助,在此编者表示衷心的感谢。

由于时间仓促且编者水平有限,书中难免存在缺点和不足之处,恳请各位学者、专家、老师和同学提出宝贵意见。

编者

2005年8月
于上海交通大学

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后给您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便于我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 517 (100084) 市场部收

电话：(010) 62770175-4518

电子邮件：fuhy@tup.tsinghua.edu.cn

教材名称：计算机网络安全

ISBN：7-302-12653-4/TP·8090

个人资料

姓名：_____ 年龄：_____ 所在院校/专业：_____

文化程度：_____ 通信地址：_____

联系电话：_____ 电子信箱：_____

您使用本书是作为：指定教材 选用教材 辅导教材 自学教材

您对本书封面设计的满意度：

很满意 满意 一般 不满意 改进建议_____

您对本书印刷质量的满意度：

很满意 满意 一般 不满意 改进建议_____

您对本书的总体满意度：

从语言质量角度看 很满意 满意 一般 不满意

从科技含量角度看 很满意 满意 一般 不满意

本书最令您满意的是：

指导明确 内容充实 讲解详尽 实例丰富

您认为本书在哪些地方应进行修改？(可附页)

您希望本书在哪些方面进行改进？(可附页)

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案，有需求的教师可以与我们的联系，我们将向使用本教材进行教学的教师免费赠送电子教案，希望有助于教学活动的开展。相关信息请拨打电话 (010) 62770175-4518 或发送电子邮件至 fuhy@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页(<http://www.tup.com.cn>)上查询。

目 录

高等学校教材·计算机科学与技术

引言	1
第 1 章 计算机网络安全概述	3
1.1 计算机网络安全的概念	3
1.1.1 计算机网络概述	3
1.1.2 网络安全的含义	6
1.1.3 网络安全的特征	7
1.2 网络面临的不安全因素	7
1.2.1 网络系统的脆弱性	7
1.2.2 网络系统的威胁	9
1.3 网络安全体系结构	10
1.3.1 网络安全模型	10
1.3.2 网络信息安全框架	11
1.3.3 OSI 网络安全体系	12
1.3.4 P2DR 模型	16
1.4 网络安全措施	18
1.4.1 安全立法	18
1.4.2 安全管理	19
1.4.3 实体安全技术	22
1.4.4 访问控制技术	22
1.4.5 数据保密技术	23
1.5 网络安全级别	23
1.5.1 可信计算机标准评价准则	23
1.5.2 普通评价准则	24
1.5.3 计算机信息安全保护等级划分准则	24
习题和思考题	25
第 2 章 网络操作系统安全	27
2.1 网络操作系统的概念	27

2.2	操作系统的安全与访问控制	28
2.2.1	操作系统安全的概念	28
2.2.2	访问控制的概念及含义	29
2.2.3	访问控制的类型	29
2.2.4	访问控制措施	30
2.3	Windows NT 系统安全	33
2.3.1	Windows NT 的安全基础	33
2.3.2	Windows NT 的安全漏洞	35
2.3.3	Windows NT 的安全性机制和技术	37
2.3.4	Windows NT 的安全管理措施	39
2.3.5	Windows NT 的数据保护	40
2.4	Windows 2000 系统安全	42
2.4.1	Windows 2000 的安全漏洞	42
2.4.2	Windows 2000 的安全性措施和技术	45
2.5	其他网络操作系统的安全	48
2.5.1	NetWare 系统安全	48
2.5.2	UNIX 系统安全	50
2.5.3	Linux 系统安全	54
	习题和思考题	57

第3章 计算机网络实体安全

3.1	网络机房及环境安全	58
3.1.1	机房的安全等级	58
3.1.2	机房的安全保护	59
3.1.3	机房的温度、湿度和洁净度	60
3.1.4	机房的接地系统	61
3.1.5	机房的电源保护	62
3.1.6	机房的环境设备监控系统	63
3.1.7	机房的空调系统	63
3.2	自然与人为灾害的防护	64
3.2.1	机房的防火	64
3.2.2	机房的防水	65
3.2.3	机房的电磁干扰防护	65
3.2.4	机房的雷电防护	66
3.3	机房的静电和电磁辐射防护	67
3.3.1	机房的静电防护	67
3.3.2	机房的电磁辐射防护	68
3.4	存储介质的保护	69
3.5	软件和数据文件的保护	70

3.6 网络系统安全的日常管理	71
习题和思考题	73
第4章 数据库与数据安全	75
4.1 数据库安全概述	75
4.1.1 数据库安全的概念	76
4.1.2 数据库管理系统及特性	77
4.1.3 数据库系统的缺陷和威胁	79
4.2 数据库的安全特性	81
4.2.1 数据库的安全性	81
4.2.2 数据库的完整性	83
4.2.3 数据库的并发控制	85
4.2.4 数据库的恢复	86
4.3 数据库的安全保护	88
4.3.1 数据库的安全保护层次	88
4.3.2 数据库的审计	89
4.3.3 数据库的加密保护	90
4.4 数据的完整性	93
4.4.1 影响数据完整性的因素	93
4.4.2 保证数据完整性的方法	95
4.5 数据备份和恢复	97
4.5.1 数据备份	97
4.5.2 数据恢复	100
4.6 网络备份系统	101
4.6.1 单机备份和网络备份	101
4.6.2 网络备份系统的组成	102
4.6.3 网络备份系统方案	103
4.7 数据容灾	104
4.7.1 数据容灾概述	104
4.7.2 数据容灾技术	108
习题和思考题	111
第5章 数据加密与鉴别	113
5.1 数据加密概述	113
5.1.1 密码学的发展	113
5.1.2 密码学的基本概念	114
5.1.3 密码的分类	116
5.2 传统密码技术	117
5.2.1 数据的表示	117

5.2.2	替代密码	118
5.2.3	移位密码	120
5.2.4	一次一密钥密码	121
5.3	对称密钥密码体制	122
5.3.1	对称密钥密码的概念	122
5.3.2	DES 算法	123
5.3.3	对称密码体制的其他算法简介	129
5.4	公开密钥密码体制	131
5.4.1	公开密钥密码的概念	131
5.4.2	数论基础	132
5.4.3	RSA 算法	135
5.4.4	混合加密方法	137
5.5	密钥管理	138
5.5.1	密钥的产生	138
5.5.2	密钥的保护和分发	138
5.5.3	网络环境下的密钥管理算法	139
5.6	网络保密通信	139
5.6.1	通信安全	139
5.6.2	通信加密	140
5.7	加密软件 PGP	144
5.7.1	PGP 概述	144
5.7.2	PGP 提供的服务	145
5.7.3	PGP 密钥的分发和保护	146
5.8	鉴别与认证技术	147
5.8.1	鉴别技术概述	147
5.8.2	数字签名	150
5.8.3	CA 认证	153
5.8.4	电子商务安全技术	158
5.8.5	安全套接层协议(SSL)	159
5.8.6	安全电子交易协议(SET)	161
	习题和思考题	163
第 6 章	防火墙	165
6.1	防火墙概述	165
6.1.1	防火墙的概念	165
6.1.2	防火墙的发展	167
6.1.3	防火墙的功能	167
6.1.4	防火墙的局限性	168
6.1.5	个人防火墙	169

6.1.6	内部防火墙	170
6.2	防火墙技术	171
6.2.1	防火墙的分类	171
6.2.2	包过滤技术	171
6.2.3	代理服务技术	174
6.2.4	状态检测技术	177
6.2.5	自适应代理技术	179
6.3	防火墙的体系结构	179
6.3.1	过滤路由器结构	179
6.3.2	双穴主机结构	180
6.3.3	主机过滤结构	180
6.3.4	子网过滤结构	181
6.3.5	不同结构防火墙的组合结构	182
6.4	防火墙的选择	182
6.4.1	防火墙的比较	182
6.4.2	防火墙的选择	183
6.5	防火墙技术的发展趋势	185
	习题和思考题	187
第7章	计算机病毒及其防治	188
7.1	计算机病毒概述	188
7.1.1	计算机病毒的概念	188
7.1.2	计算机病毒的产生	189
7.1.3	计算机病毒的特征	190
7.1.4	计算机病毒的分类	191
7.1.5	计算机病毒的传播	193
7.1.6	计算机病毒的危害	193
7.2	网络病毒及其预防	195
7.2.1	网络病毒概述	195
7.2.2	网络病毒的预防	197
7.2.3	网络病毒的检测	199
7.2.4	网络病毒的清除	202
7.3	恶意代码	204
7.3.1	常见的恶意代码	204
7.3.2	木马	205
7.3.3	蠕虫	211
7.4	计算机病毒的现状和发展趋势	216
7.4.1	计算机病毒的现状	216
7.4.2	计算机病毒的发展趋势	217

7.4.3	计算机病毒的防范对策	218
	习题和思考题	219
第 8 章	安全检测和响应	220
8.1	入侵检测与入侵防护系统	220
8.1.1	入侵检测系统概述	221
8.1.2	入侵检测技术及发展趋势	224
8.1.3	入侵防护系统	226
8.2	网络扫描和网络监听	229
8.2.1	网络系统漏洞	229
8.2.2	网络扫描	232
8.2.3	网络监听	238
8.2.4	网络嗅探器(sniffer)	241
8.3	计算机紧急响应	244
8.3.1	紧急响应	244
8.3.2	应急处理技术	248
	习题和思考题	250
第 9 章	Internet 安全	252
9.1	TCP/IP 协议及其安全	252
9.1.1	TCP/IP 的层次结构	252
9.1.2	TCP/IP 的主要协议及其功能	253
9.1.3	TCP/IP 层次安全	255
9.2	Web 站点安全	257
9.2.1	Web 概述	257
9.2.2	Web 的安全需求	259
9.3	黑客与网络攻击	261
9.3.1	黑客与入侵者	261
9.3.2	网络攻击的类型	262
9.3.3	黑客攻击的目的、手段和工具	265
9.3.4	黑客的攻击及防范措施	267
9.3.5	系统被入侵后的恢复	275
9.4	电子邮件安全	276
9.4.1	电子邮件的安全漏洞	276
9.4.2	电子邮件欺骗	278
9.4.3	电子邮件病毒	279
9.4.4	电子邮件加密	280
9.5	Internet 欺骗及防范	281
9.5.1	ARP 电子欺骗	282

9.5.2	DNS 电子欺骗	283
9.5.3	IP 电子欺骗	285
9.5.4	Web 电子欺骗	287
	习题和思考题	289
第 10 章	网络安全应用实例	290
10.1	天网个人版防火墙	290
10.2	加密软件——PGP 的应用	296
10.3	sniffer 工具——tcpdump 的应用	299
10.4	入侵检测工具——snort 的应用	303
10.5	数据包嗅探工具——NetXray 的应用	307
10.6	扫描之王——nmap 的应用	309
10.7	远程安全扫描器——nessus 的应用	314
10.8	反黑精英——Trojan Ender 的应用	317
10.9	查看开放端口——判断木马的方法	320
10.10	常见国产木马的清除方法	322
	习题和思考题	327
	习题答案	328
	参考文献	330
	网络资源	331