

21

21世纪计算机专业大专系列教材

李大友 主编

计算机网络安全

戴英侠 许剑卓 翟起宾 连一峰 等 编著



清华大学出版社

21 世纪计算机专业大专系列教材

李大友 主编

计算机网络安全

戴英侠 许剑卓 翟起宾 连一峰等 编著

清华大学出版社
北京

内 容 简 介

本书是大专院校的教材,共14章。第1章主要介绍当前面临的安全威胁、安全的概念及安全策略。第2章阐述了密码学的数学基础,如模运算、数论、有限域等。第3、4章介绍密码学的算法。第5、6、7、8章介绍了密码算法及协议在网络安全和一些基础设施中的应用。第9、10两章主要介绍了攻击技术。第11、12、13章介绍了防火墙、入侵检测和取证技术。第14章介绍安全评估标准和风险评估技术。

本书内容丰富,结构合理,语言流畅,深入浅出;不但系统地介绍了网络安全的理论、概念、方法和体系结构,还列举了大量实例;适合作为大专院校的教材,也可供工程技术人员参考。

版权所有,翻印必究。举报电话:010-62782989 13901104297 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。

本书防伪标签采用清华大学核研院专有核径迹膜防伪技术,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/戴英侠等编著. —北京:清华大学出版社,2005.1

(21世纪计算机专业大专系列教材)

ISBN 7-302-09905-7

I. 计… II. 戴… 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(2004)第 118214 号

出 版 者:清华大学出版社

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

社 总 机:010-62770175

地 址:北京清华大学学研大厦

邮 编:100084

客户服务:010-62776969

组稿编辑:范素珍

文稿编辑:徐跃进

印 刷 者:北京密云胶印厂

装 订 者:北京市密云县京文制本装订厂

发 行 者:新华书店总店北京发行所

开 本:185×260 印张:20.5 字数:467千字

版 次:2005年1月第1版 2005年1月第1次印刷

书 号:ISBN 7-302-09905-7/TP·6811

印 数:1~5000

定 价:26.00元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770175-3103 或(010)62795704

《21 世纪计算机专业大专系列教材》

编辑委员会名单

主 编 李大友

编 委 (排名不分先后)

刘乐善 (华中理工大学)

刘惠珍 (北京工业大学)

陈 明 (石油大学)

邵学才 (北京工业大学)

蒋本珊 (北京理工大学)

匙彦斌 (天津大学)

葛本修 (北京航空航天大学)

彭 波 (中国农业大学)

徐孝凯 (中央广播电视大学)

策划编辑 范素珍

序

这套教材为 21 世纪高等学校计算机专业大专系列教材。

我们从 1995 年开始组织《计算机专业大专系列教材》。当时根据中国计算机学会教育委员会与全国高等学校计算机教育研究会联合推荐的《计算机学科教学计划 1993》的要求,组织了《计算机组成原理》等 13 本教材,并由清华大学出版社出版。这套教材出版后,受到了高等学校师生的广泛欢迎和好评。

在组织上述教材的时候,主要是按《计算机学科教学计划 1993》的要求进行的。而 1993 教学计划主要是参照美国 IEEE 和 ACM《计算机学科教学计划 1991》并结合我国高等教育当时的实际情况制定的,反映的是 20 世纪 80 年代末计算机学科的发展状况。

计算机学科是一个飞速发展的新兴学科,发展速度之快可谓一日千里。近 10 年来,计算机学科已发展成为一个独立学科,计算机本身向高度集成化、网络化和多媒体化迅速发展。但从另一个方面来看,高等学校的计算机教育一直滞后于计算机学科的发展,特别是教材建设,由于受时间和软硬条件的限制,更是落后于现实需要,而大专层次的教材建设问题尤其严重。为了改变这种状况,高等学校的教育工作者和专家教授们应当仁不让地投入必要的时间和精力来完成这一历史使命。

为组织好这套教材,我们认真地研究了全国高等学校计算机专业教学指导委员会和中国计算机学会教育委员会联合推荐的《计算机学科教学计划 2000》和美国 IEEE 和 ACM 两个学会最新公布的《计算机学科教学计划 2001》。这两个教学计划都是在总结了从《计算机学科教学计划 1991》到现在计算机学科十年来发展的主要成果的基础上诞生的。它们所提供的指导思想和学科所涵盖的内容,不仅适合于大学本科,也适合大学专科的需求,关键在于要对其内容的取舍进行认真的研究。

在我国的《计算机学科教学计划 1993》和美国 IEEE 和 ACM 两个学会提出的《计算机学科教学计划 1991》中,根据当时的情况,只提出了 9 个主科目。而在《计算机学科教学计划 2001》中,根据学科的最新发展状况,提出了 14 个主科目,其中 13 个主科目又为核心主科目。这 14 个主科目是算法与分析(AL)、体系结构(AR)、离散结构(DS)、计算机科学(CN)、图形学与可视化计算(GV)、网络计算(NC)、人机交互(HC)、信息管理(IM)、智能系统(IS)、操作系统(OS)、程序设计基础(PF)、程序设计语言(PL)、软件工程(SE)、社会、道德、法律和专业问题(SP),其中除 CN 为非核心主科目外,其他 13 个主科目均为核心主科目。

将美国 IEEE 和 ACM 的教学计划 2001 与 1991 计划进行比较可看出:在 1991 计划中,离散结构只是作为数学基础提出,未被列为主科目,在 2001 计划中,不但列为主科目,

而且为核心主科目。可见,已将离散结构提升为本学科的基础。

在 1991 计划中,未提及网络计算,在 2001 计划中,不但提出,而且被列为核心主科目,以适应网络技术飞速发展的需求。

图形学与可视化计算也是为适应发展需求新增的内容,并且列为主科目。

除此之外,2001 计划在下述 5 个方面做了增加或调整。

- 将程序设计语言引论调整为程序设计基础和程序设计语言两个核心主科目,显然,加强了对程序设计的要求。
- 将人-机通信调整为人机交互,反映了人-机通信的实质是人机交互。在图形界面迅速发展的今天,人机交互理论和方法的研究和应用变得十分重要。
- 将人工智能与机器人学调整为智能系统,拓宽了对智能系统的要求。
- 将数据库与信息检索调整为信息管理,因为后者不仅概括了前者,而且反映了数据库与信息检索的实质是信息管理。
- 将数值与符号计算调整为计算科学,更具有概括性。

总之,上述变化不仅更好地反映了计算机学科的发展现状,而且使 2001 教学计划具有更强的科学性和实用性。

由于这套系列教材主要面向的对象是计算机专业三年制大专(高职)学生,其培养目标也应属于高级技术人才的层次。他们既要有一定的理论基础(较本科弱),又要更强调实用性,要有明确的应用方向。我们将应用方向定位在信息管理和计算机网络两个方向。这两个应用方向占计算机应用总计的 90% 以上。

在系列教材的内容取舍上,2001 教学计划的 14 门主科目中,我们概括了除智能系统、计算科学和社会科学之外的其他 11 个主科目。在每个主科目中,都以其中的基本概念、基本理论和基本方法作为主线组织教材,使学生既能掌握基本的基础理论和方法,又能为他们进一步深造打下必要的基础;在信息管理和计算机网络技术两个应用方向上,他们的应用能力将得到加强。

根据上述指导思想,初步确定组织 20 本左右的教材供各高校选用。这些教材包括:《离散数学》、《计算机应用基础》、《计算机组织与结构》、《微机系统与接口技术》、《计算机网络与通信》、《网络管理技术基础》、《计算机网络系统集成技术》、《数据结构》、《操作系统原理》、《实用软件工程基础》、《数据库原理与应用》、《管理信息系统原理与应用》、《办公自动化实用技术》、《多媒体技术及其应用》、《Internet 技术及其应用》、《计算机维护技术》、《C 语言程序设计》、《Java 语言程序设计》、《C++ 语言程序设计》、《VB 语言程序设计》、《计算机英语》等。

系列教材并不是教学计划,由于各高校情况不同,培养方向的侧重面也不一样,因此教学计划也不会雷同。教材按系列组织,力图能够反映计算机学科大专层次的总体要求,同时采用大拼盘结构,各校可根据自身情况选择使用。例如,语言类教材,我们就准备了多本,各校可选择其中的一本或两本,其他依此类推。

这套教材均由高等学校具有丰富教学实践经验的老师编写。所编教材体系结构严谨、层次清晰、概念准确、理论联系实际、深入浅出、通俗易懂。相信一定能够得到专科院校计算机专业师生的欢迎。

全国高等学校计算机教育研究会副理事长
课程与教材建设委员会主任

李大友

2001.6

前 言

当前,信息化把人们带进高速度、多媒体、智能化、个人化、全球一体化的信息环境,网络以前所未有的速度渗透到人们的工作和日常生活当中。随着网上银行、电子书店等网络手段的运用和普及,网络在新世纪扮演一个举足轻重的角色。但是,在网络给人们带来便利的同时,人们也发现网络中处处潜藏着威胁:如上网账号被盗用、信用卡透支、企业网站被黑客攻击,甚至国家某些绝密文件也会不翼而飞……这些使人们提高了警惕,对网络安全提出了各种各样的要求。

什么是计算机网络安全呢?本书分别从加密、认证、入侵检测等方面进行阐述,以帮助读者全面地认识安全,理解安全。本书是大专院校的教科书,各章都附有习题,可以帮助学生更好地掌握该门功课。

全书共分14章,第1、3、7及13章由许剑卓编写,第2章由翟起宾编写,其他章节由连一峰、左晓栋、庞南、胡艳、冯萍慧及李闻等编写,最后由戴英侠统稿。

作 者

2004年9月

目 录

第 1 章 信息系统安全概论	1
1.1 历史与现状	1
1.1.1 历史.....	1
1.1.2 现状与威胁.....	2
1.1.3 现状与行动.....	4
1.2 安全是什么	6
1.2.1 真正的安全.....	6
1.2.2 从经济学角度定义安全.....	8
1.3 安全机制和安全政策.....	10
1.3.1 安全机制	10
1.3.2 安全政策	11
1.4 一些基本概念.....	13
1.4.1 密码学基本概念	13
1.4.2 攻击	14
1.4.3 恶意代码	16
1.5 安全标准.....	17
1.5.1 国际标准化组织	17
1.5.2 国际电报和电话咨询委员会	18
1.5.3 电气和电子工程师学会	19
1.5.4 Internet 体系结构委员会	19
1.5.5 美国国家标准局与美国商业部国家技术标准研究所	20
1.5.6 美国国防部及国家计算机安全中心	21
1.5.7 其他有关密码的协议	22
1.5.8 我国的信息安全标准化工作	23
习题	24
第 2 章 数学基础	26
2.1 数的整除性.....	26
2.1.1 除数(因子)和整除的概念	26
2.1.2 素数(质数)的概念	27
2.1.3 互为素数	28
2.2 带余除法和欧几里德算法.....	28
2.3 模运算.....	30

2.3.1	模运算操作	30
2.3.2	模运算的性质	31
2.4	数论中一些有用的定理	33
2.4.1	费马定理	33
2.4.2	欧拉函数	34
2.4.3	欧拉定理	34
2.4.4	中国剩余定理	36
2.5	群论中的若干基本概念	37
2.6	环和域的基本概念	39
2.6.1	环	39
2.6.2	整环	39
2.6.3	子环和环同构	40
2.7	有限域	42
	习题	48
第3章	对称密码算法	50
3.1	简介	50
3.1.1	引论	50
3.1.2	经典密码算法	51
3.1.3	分组密码算法与流密码算法	52
3.1.4	符号	55
3.1.5	加密算法的破解	55
3.2	分组密码算法模式	57
3.2.1	电子码本模式	58
3.2.2	密码分组链接模式	59
3.3	DES 算法	61
3.3.1	概述	61
3.3.2	DES 算法的基础结构	62
3.3.3	多轮运算	63
3.3.4	轮密钥的生成	64
3.3.5	F 函数	65
3.3.6	初始置换和末置换	68
3.3.7	关于 S 盒安全性的讨论	69
3.3.8	3DES	69
3.3.9	相关概念	70
3.4	其他对称密码算法	70
3.4.1	IDEA	70
3.4.2	AES 算法	71
3.4.3	RC4 算法	71

3.5 密钥的管理	71
3.5.1 口令作为密钥使用的安全性	72
3.5.2 随机密钥	72
3.5.3 密钥共享	72
3.5.4 密钥托管	73
习题	73
第4章 非对称密码体制	75
4.1 什么是非对称密码体制	75
4.2 RSA 密码体制	77
4.2.1 RSA 算法	77
4.2.2 RSA 数字签名方案	79
4.3 ElGamal 体制	80
4.3.1 ElGamal 算法	80
4.3.2 ElGamal 签名方案	81
4.3.3 ElGamal 签名方案的安全性	81
4.4 椭圆曲线密码体制	83
4.4.1 有关的基本概念	83
4.4.2 有限域上椭圆曲线的 $\oplus$ 运算	86
4.4.3 椭圆曲线密码体制	87
4.4.4 椭圆曲线的同构	88
习题	89
第5章 数字签名、哈希函数和 PKI	91
5.1 数字签名	91
5.1.1 数字签名标准	91
5.1.2 一次数字签名方案	92
5.1.3 不可否认的数字签名方案	93
5.2 哈希函数及其评价方法	96
5.2.1 哈希函数	96
5.2.2 生日攻击	98
5.3 公开密钥基础设施	99
5.3.1 公开密钥基础设施简要介绍	99
5.3.2 PKI 的主要组成部分和简要功能描述	100
5.3.3 现有的 PKI 多级信任模型	101
习题	105
第6章 安全协议与电子商务安全	106
6.1 网络安全	106

6.1.1	概述	106
6.1.2	安全威胁	106
6.1.3	安全服务和安全机制	106
6.2	安全协议	108
6.2.1	协议及其分类	108
6.2.2	通信协议及其分类	108
6.2.3	密码协议及其分类	108
6.2.4	安全协议的安全性	109
6.2.5	安全协议的分析	110
6.3	SSL 协议	111
6.3.1	SSL 概述	111
6.3.2	SSL 规范	111
6.3.3	相关技术	114
6.4	SET 协议	115
6.4.1	SET 概述	115
6.4.2	SET 规范	115
6.4.3	SET 的安全性	117
6.5	SSL 与 SET 的比较	120
6.6	电子商务安全	122
6.6.1	概述	122
6.6.2	电子商务的安全需求	122
6.6.3	电子商务采用的安全技术	125
6.7	电子商务系统实例分析	128
6.8	小结	129
	习题	130
第 7 章	网络协议与网络安全基础知识	131
7.1	OSI7 层模型	131
7.1.1	物理层	131
7.1.2	链路层	132
7.1.3	网络层	133
7.1.4	传输层	134
7.1.5	会话层	135
7.1.6	表示层	135
7.1.7	应用层	135
7.2	TCP/IP 协议	135
7.2.1	地址空间	136
7.2.2	直接连接的节点之间的通信	137

7.2.3	IP 协议报文格式	138
7.2.4	路由协议	140
7.2.5	TCP 协议	142
7.2.6	UDP 协议	145
7.3	应用层协议	145
7.3.1	DNS 服务	145
7.3.2	SMTP 协议	147
7.3.3	Telnet 服务的安全问题	148
7.3.4	FTP 协议的安全问题	148
7.3.5	RPC 服务	149
	习题	149
第 8 章	VPN 技术	151
8.1	VPN 的基本概念	151
8.1.1	VPN 的定义	151
8.1.2	VPN 出现的背景	151
8.1.3	VPN 的架构	151
8.1.4	实现 VPN 的主要问题	153
8.2	VPN 的实现技术	154
8.2.1	网络地址翻译	154
8.2.2	隧道技术	155
8.2.3	VPN 中使用的安全协议	155
8.3	基于 IPSec 协议的 VPN	158
8.3.1	IPSec 的基本原理	158
8.3.2	IPSec 的标准化	158
8.3.3	安全关联	160
8.3.4	认证头协议	161
8.3.5	封装安全载荷协议	164
8.3.6	Internet 密钥交换	167
8.3.7	在 VPN 中使用 IPSec 协议	169
8.4	链路层 VPN 的实现	172
8.4.1	PPTP	172
8.4.2	L2F	173
8.4.3	L2TP	173
8.5	VPN 的应用方案	174
8.5.1	VPN 的应用类型	174
8.5.2	部署 Intranet 型 VPN	174
8.5.3	部署远程访问型 VPN	175

8.5.4 部署 Extranet 型 VPN	177
习题	178
第 9 章 系统入侵技术	180
9.1 概述	180
9.2 扫描器	181
9.2.1 简介	181
9.2.2 秘密扫描和 OS 指纹探测	183
9.2.3 网络拓扑探测	184
9.3 利用脚本漏洞入侵	185
9.3.1 SQL 插入	185
9.3.2 CGI 的基本概念和漏洞举例	187
9.4 缓冲区溢出和格式化字符串漏洞	189
9.4.1 缓冲区溢出攻击	189
9.4.2 格式化字符串攻击	190
9.5 特洛伊木马	193
9.5.1 简介	193
9.5.2 反弹端口木马	198
习题	202
第 10 章 拒绝服务攻击	203
10.1 简介	203
10.2 常见拒绝服务攻击	204
10.2.1 flood	204
10.2.2 smurf	205
10.2.3 OOB Nuke	205
10.2.4 teardrop	206
10.2.5 land	206
10.2.6 kiss of death	206
10.3 拒绝服务攻击的防范方法	207
习题	207
第 11 章 防火墙技术	208
11.1 防火墙综述	208
11.1.1 防火墙相关概念	208
11.1.2 防火墙技术的发展	209
11.1.3 防火墙的部署结构	212
11.2 防火墙技术原理	214

11.2.1	包过滤	214
11.2.2	应用代理	215
11.2.3	状态检测包过滤	216
11.2.4	与防火墙相关的网络管理技术	217
11.3	防火墙的应用	218
11.3.1	防火墙应用的误区	218
11.3.2	安全性考虑	219
11.3.3	网络传输性能	220
11.3.4	防火墙产品介绍——CheckPoint firewall-1	221
11.4	防火墙技术的发展趋势	222
	习题	223
第 12 章	入侵检测技术	225
12.1	网络安全体系结构	225
12.2	入侵检测的产生	226
12.2.1	安全审计	226
12.2.2	IDES 的诞生	227
12.3	入侵检测的实现	228
12.3.1	基本原理	228
12.3.2	系统模块	228
12.3.3	检测过程	229
12.3.4	入侵检测系统的分类	231
12.4	研究现状	232
12.4.1	误用检测	232
12.4.2	异常检测	236
12.4.3	其他检测技术	238
12.4.4	分布式入侵检测	241
12.4.5	商业化产品	248
12.5	小结	249
	习题	249
第 13 章	调查取证过程与技术	250
13.1	概述	250
13.1.1	简介	250
13.1.2	调查取证过程	251
13.1.3	调查取证技术	251
13.2	初步响应阶段	252
13.2.1	基础过程	252

13.2.2	评估基本情况	252
13.2.3	制定响应策略	253
13.2.4	收集信息	255
13.3	计算机证据分析阶段	258
13.3.1	再现犯罪和再现调查过程	258
13.3.2	计算机证据分析体系的构成	259
13.3.3	证据固定层	259
13.3.4	证据恢复层	260
13.3.5	证据解码层	262
13.3.6	证据分析层	263
13.3.7	综合分析层	268
13.3.8	通过网络查找相关的信息	268
13.4	用户行为监控阶段	269
13.4.1	目的	269
13.4.2	工具	269
13.4.3	监视注意事项	269
13.5	拒绝服务攻击的调查	270
13.5.1	概述	270
13.5.2	stepstone 技术	271
13.5.3	backscatter 技术	272
	习题	273
第 14 章	系统安全评估技术	275
14.1	信息安全评估国际标准	275
14.1.1	TCSEC	275
14.1.2	ITSEC	278
14.1.3	CC	282
14.2	计算机信息系统安全等级保护	286
14.2.1	计算机信息系统安全等级保护框架	286
14.2.2	GB 17859	288
14.2.3	计算机信息系统安全等级保护通用技术要求	291
14.3	信息系统安全风险评估	296
14.3.1	风险评估的概念	297
14.3.2	风险评估的步骤	297
	习题	307
	参考文献	308

第 1 章 信息系统安全概论

1.1 历史与现状

1.1.1 历史

信息革命正在改造我们的生活,这场革命早在工业化进程中就开始孕育。20 世纪 50 年代前的电报电话等基础通信技术和计算机技术的出现,为 20 世纪 60 年代计算机联网实验提供了最初的条件,20 世纪 70 年代半导体微电子技术的飞跃以及数字化技术的成熟为计算机网络走出军事的封闭环境、研究所和校园的象牙之塔奠定了技术基础。美国著名的未来学家阿尔温·托夫勒很早就预感到信息革命的巨大影响,出版了他的“第三次浪潮”等名著。他深刻地指出:“电脑网络的建立与普及将彻底地改变人类的生存及生活模式,而控制与掌握网络的人就是人类未来命运的主宰。谁掌握了信息,控制了网络,谁就拥有整个世界”。

为了发掘信息革命的巨大潜能,美国率先提出了信息高速公路的构想,倡导实施国家信息基础设施(NII),西方发达国家紧跟着提出全球信息基础设施(GII)的倡议。我国也大力推动信息化,从“三金工程”(金卡、金关、金桥)的最初倡议发展到今天十几个金字号工程,我国的电信业务以全球最快的速度蓬勃发展。普通百姓在家里上 Internet 周游世界已成为今天的社会现实。人们热情高涨地推动着信息化,期盼着信息化带来的理想成真。

信息技术一方面促进了生产力的发展,提高了生产效率,但同时对社会稳定、生产秩序、经济基础的威胁也在加大。从历史上可以看到,每次生产力的飞跃往往带来更为残忍的战争,使人类遭受更大的痛苦。而信息革命是否会带来灾难呢?谁都很难给出答案。事实上从已经发生的一些事件可以看到信息社会可能面临的威胁。图 1-1 是近几年来几种蠕虫病毒给全球造成的经济损失(注意图中显示的损失金额以亿美元为单位)。设想一下,以普通的犯罪方式,要造成 8 亿美元的损失会比登天还难,而在信息社会中要造成这样的破坏只是编写一个简单的蠕虫病毒即可,对于一个熟悉病毒制作的人,编写这样一个蠕虫可能只需要一个星期。注意这些蠕虫多数只是利用了一到两个安全漏洞实施攻击并进行传播。而究竟有多少漏洞可以利用呢?如图 1-2 是近几年来公布的安全漏洞的数目,利用一两个安全漏洞已经能够造成如此大规模的损失,如果这些安全漏洞都被利用起来,后果很难设想,实际上这里讲到的损失可能只是现实损失的一小部分。