21世纪计算机专业大专系列教材

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。

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　　**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
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

《21世纪计算机专业大专系列教材》
编辑委员会名单

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、冯萍彗及李闻等编写，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　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，编写这样的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。