大学本科计算机专业应用型规划教材

丛书主编：高林

计算机网络安全

顾巧论　高铁杠　贾春福　等编著

清华大学出版社

大学本科计算机专业应用型规划教材

丛书主编：高林

计算机网络安全

顾巧论　高铁杠　贾春福　等编著

清华大学出版社
北京

内 容 简 介

本书阐述了网络所涉及的安全问题，还通过实例、实训来增强读者的理解及动手能力。主要内容包括网络安全基础知识、物理与环境安全、操作系统安全、网络通信安全、Web 安全、数据安全、病毒及其预防、黑客攻击与防范、防火墙技术及有关网络安全的法律法规。

本书不仅适合应用型大学本科学生使用，同时也适合于对网络安全感兴趣的读者。

图书在版编目(CIP)数据

计算机网络安全/顾巧论等编著. —北京：清华大学出版社，2004.9
(大学本科计算机专业应用型规划教材/高林主编)
ISBN 7-302-09139-0

Ⅰ. 计…　Ⅱ. 顾…　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 076731 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：谢　泰
文稿编辑：汪汉友
印 刷 者：北京顺义振华印刷厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　印张：18　字数：406 千字
版　　次：2004 年 9 月第 1 版　2004 年 9 月第1次印刷
书　　号：ISBN 7-302-09139-0/TP・6445
印　　数：1～5000
定　　价：24.00 元

大学本科 计算机专业应用型规划教材

编 委 会

丛书序

大学本科计算机专业应用型规划教材

为适应我国“以信息业带动工业化，发挥后发优势，实现社会生产力的跨越式发展”以及大力发展制造业和优化产业结构的要求，应用型人才培养已成为高等学校人才培养的重要任务。

以微电子技术为基础、计算机技术为主体的信息技术，是当前人类社会中发展最快、渗透性最强、应用面最广的先导技术。信息技术的广泛应用推动着以信息产品制造业、软件业、信息系统集成业和信息咨询服务业为主体的信息产业的发展。在新的世纪里，信息已成为重要的生产要素和战略资源，信息技术成为先进生产力的代表，信息产业将发展成为现代产业的带头产业，人类即将跨越工业时代进入信息时代。因此，信息化成为当今世界经济和社会的发展趋势，大力推进社会和国民经济信息化是推进我国社会主义现代化建设的重要任务。计算机和信息技术的发展不仅需要大批专业技术人才，而且还产生了一批新的职业岗位，毋庸置疑，信息及其相关职业将成为未来最紧缺的职业。

计算机和信息技术与应用的人才需求将呈多元化、多层次趋势，表现在科学、技术、产业、应用、服务诸多方面。不仅需要从事科学、技术研发的人才，而且更需要把研发成果转变为现实产品的技术和管理人才；不仅要有能从事计算机和信息科学、技术工作的人才，而且更需要能从事计算机和信息产业、应用、服务工作的人才；以及在各类人才中的精英人才、领军人物。这实际是对我国计算机和信息类高等教育改革提出了新的要求和新的课题，要求我国高等教育进行结构调整，满足人才培养的多元化，大力培养具有计算机和信息技术专长的应用型人才——他们是这些领域的技术专家和管理专家，可以在相应的行业、企业担任各种技术工作。

目前，我国高等教育中应用型人才培养模式相对落后，如何发展应用型教育已成为课程改革的主要任务。本套教材是以培养计算机和信息类专业本科应用型人才为目的进行的课程与教材改革尝试。在本套教材的策划过程中，清华大学出版社多次组织了由行业企业专家和有丰富教学经验的一线教师参加的研讨会，对应用型高等教育的规律和在计算机教学中的体现进行了深入的研讨。在此基础上我们力求能从整体上把握计算机和信息类应用型人才培养的特征，并体现在这套教材的编写过程中：在教材编写的指导思想上，力求在保持学科科学性的同时，体现工程和技术学科的系统性；在教材

的内容组织上，尽量采用以问题为中心的写作方法，加强案例性教学；在理论联系实际和加强能力培养方面，增加方案性设计习题和实际训练性题目，以培养学生的专门技术能力和完成实际工作任务的能力。

计算机和信息类应用型教材编写还处于改革的初步尝试阶段，希望使用这套教材的教师也能够参与到教材建设工作中来，并提出宝贵意见，以便推动课程改革并提高教材质量。

高　林

2004 年 5 月

前　言

在现代社会中，计算机已经深入到生活、工作的每个角落，人们用计算机进行通信、存储数据、处理数据等。然而，人们深深依赖的计算机网络，正面临着很多潜在的安全威胁。

影响计算机网络安全的因素很多，除了信息的不安全性以外，层出不穷的计算机病毒也给网络安全带来了威胁。另外，黑客对于网络安全的威胁则日趋严重。网络所面临的威胁很多，其中包括：物理威胁（偷窃、废物搜寻、间谍行为、身份识别错误）、系统漏洞（乘虚而入、不安全服务、配置和初始化）、身份鉴别威胁（口令圈套、口令破解、算法考虑不周、编辑口令）、线缆连接威胁（窃听、拨号进入、冒名顶替）、有害程序（病毒、代码炸弹、特洛伊木马）等。

从技术上讲，网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

当然，网络安全不仅是一个技术问题，也是一个社会问题和法律问题。要解决信息网络的安全问题，必须采取技术和立法等多种手段进行综合治理。

目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。有关网络安全的书籍也层出不穷。

本书作为应用型大学本科教材，围绕计算机网络所涉及的安全问题，讲述了各种相关的安全技术。为了加深学生对所学内容的理解，部分章节给出了实例。通过本书的学习，学生既可以获取计算机网络安全的相关知识，又可以提高对安全技术的实际运用能力。

本书第1章、第3章、第7章、第9章及附录A由顾巧论、高铁杠编写，第6章及附录B由贾春福、钟安鸣、徐伟编写，第8章及附录C由贾春福、钟安

鸣、段雪涛编写，第 2 章、第 4 章由张永哲编写，第 5 章、第 10 章由申莉莉编写，本书由顾巧论统稿。

本书在编写过程中，参考了大量书籍，在此对各部书的编著者表示感谢。

由于编者水平有限，书中错误和疏漏之处在所难免，恳请读者和各位专家给予指正。

作　者

2004 年 6 月

目　录

计算机网络安全

第1章 计算机网络安全

网络安全基础知识

计算机技术的普及和应用为人们的生活带来了方便，互联网技术的不断发展，使世界成为一个整体，人们通过网络学习、购物、交流，可以说，互联网的迅猛发展使人们享受到了前所未有的便利。然而，网络也不是完美无缺的，网络给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等严重威胁着网络的安全，也给人们的工作和生活带来了诸多烦恼，因此，网络安全问题已经成为许多国家的关注焦点，如何构建安全的网络成为世界各国研究的重要问题，网络的安全和保密技术成为了当今网络技术的一个重要研究课题。

1.1 网络安全简介

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题，网络信息的保密性、完整性、可用性、真实性和可控性等相关技术问题都成为网络安全研究的重要课题。

(1) 保密性。信息的安全性，即不能将信息泄露给非授权用户。

(2) 完整性。数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

(3) 可用性。可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性。能够对信息进行控制，保护其完整性和可用性，对信息的传播及内容具

有控制能力。

网络安全包括物理安全、逻辑安全、操作系统安全和联网安全。

1.1.1 物理安全

物理安全是指保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限、防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

1. 防盗

网络的硬件和软件设备与其他的物体一样，具有自身非常重要的价值，因此成为偷窃者窃取信息的首选目标，软硬盘、主板等都是计算机的关键部件，是窃贼窃取实物的首选。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

2. 防火

防火是计算机网络中心安全的头等大事，由于计算机机房和中心设有许多线路和电器设备，因此发生火灾的原因一般是由于电器原因、人为事故或外部火灾蔓延引起的。电器设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎，吸烟、乱扔烟头等，使充满易燃物质(如纸片、磁带、胶片等)的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

3. 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位(能量不大)，从而产生静电放电火花，造成火灾。它还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。因此机房和网络中心必须采取防静电措施，采用防静电设备进行装饰，以防止由于静电而产生不安全因素。

4. 防雷击

随着科学技术的发展，电子信息设备的广泛应用，对现代闪电保护技术提出了更高、更新的要求，利用传统的常规避雷针，已不能满足微电子设备的要求，而且带来很多弊端。利用引雷机理的传统避雷针防雷，不但增加雷击概率，而且产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。

雷击防范的主要措施是，根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点做分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多级层保护。