21世纪高职高专规划教材·计算机系列

网络安全技术

安洛生　主　编
王利敏　副主编

国防科技大学出版社

21世纪高职高专规划教材
计算机系列

网络安全技术

安洛生　主　编
王利敏　副主编

国防科技大学出版社

【内容简介】本书是为高职高专计算机及相关专业编写的教材。

本书以网络安全技术实际应用为主线，全面、系统地介绍了网络安全基本知识。本书的主要内容包括网络安全概述、网络入侵技术、数字加密与认证、防火墙技术、入侵检测系统、VPN 技术应用、计算机病毒及防治、Web 系统和无线网安全、Windows Server 2003 网络安全应用。

本书既可供高职高专学生使用，也可以作为广大工程技术人员和网络爱好者的参考用书。

图书在版编目(CIP)数据

网络安全技术/安洛生主编. —长沙：国防科技大学出版社，2010.4

ISBN 978-7-81099-744-7

Ⅰ. 网… Ⅱ. 安… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2010)第 051792 号

出版发行：国防科技大学出版社

网　　址：http://www.gfkdcbs.com

责任编辑：文　慧　　**特约编辑**：白毅娟

印 刷 者：北京振兴源印务有限公司

开　　本：787mm×1 092mm　1/16

印　　张：16

字　　数：399 千字

版　　次：2010 年 4 月第 1 版

印　　次：2010 年 4 月第 1 次印刷

定　　价：25.00 元

21世纪高职高专规划教材·计算机系列

编审委员会

出版说明

高职高专教育作为我国高等教育的重要组成部分，承担着培养高素质技术、技能型人才的重任。近年来，在国家和社会的支持下，我国的高职高专教育取得了不小的成就，但随着我国经济的腾飞，高技能人才的缺乏越来越成为影响我国经济进一步快速健康发展的瓶颈。这一现状对于我国高职高专教育的改革和发展而言，既是挑战，更是机遇。

要加快高职高专教育改革和发展的步伐，就必须对课程体系和教学模式等问题进行探索。在这个过程中，教材的建设与改革无疑起着至关重要的基础性作用，高质量的教材是培养高素质人才的保证。高职高专教材作为体现高职高专教育特色的知识载体和教学的基本工具，直接关系到高职高专教育能否为社会培养并输送符合要求的高技能人才。

为促进高职高专教育的发展，加强教材建设，教育部在《关于全面提高高等职业教育教学质量的若干意见》中，提出了“重点建设好 3 000 种左右国家规划教材”的建议和要求，并对高职高专教材的修订提出了一定的标准。为了顺应当前我国高职高专教育的发展潮流，推动高职高专教材的建设，我们精心组织了一批具有丰富教学和科研经验的人员成立了 21 世纪高职高专规划教材编审委员会。

编审委员会依据教育部高教司制定的《高职高专教育基础课程教学基本要求》和《高职高专教育专业人才培养目标及规格》，调研了百余所具有代表性的高等职业技术学院和高等专科学校，广泛而深入地了解了高职高专的专业和课程设置，系统地研究了课程的体系结构，同时充分汲取各院校在探索培养应用型人才方面取得的成功经验，并在教材出版的各个环节设置专业的审定人员进行严格审查，从而确保了整套教材“突出行业需求，突出职业的核心能力”的特色。

本套教材的编写遵循以下原则：

(1) 成立教材编审委员会，由编审委员会进行教材的规划与评审。

(2) 按照人才培养方案以及教学大纲的需要，严格遵循高职高专院校各学科的专业规范，同时最大程度地体现高职高专教育的特点及时代发展的要求。因此，本套教材非常注重培养学生的实践技能，力避传统教材“全而深”的教学模式，将“教、学、做”有机地融为一体，在教给学生知识的同时，强化了对学生实际操作能力的培养。

(3) 教材的定位更加强调“以就业为导向”，因此也更为科学。教育部对我国的高职高专教育提出了“以应用为目的，以必需、够用为度”的原则。根据这一原则，本套教材在编写过程中，力求从实际应用的需要出发，尽量减少枯燥、实用性不强的理论灌输，充分体现出“以行业为向导，以能力为本，以学生为中心”的风格，从而使本套教材更具实用性和前瞻性，与就业市场结合也更为紧密。

(4) 采用“以案例导入教学”的编写模式。本套教材力图突破陈旧的教育理念，在讲解的过程中，援引大量鲜明实用的案例进行分析，紧密结合实际，以达到编写实训教材的

目标。这些精心设计的案例不但可以方便教师授课，同时又可以启发学生思考，加快对学生实践能力的培养，改革人才的培养模式。

本套教材涵盖了公共基础课系列、财经管理系列、物流管理系列、电子商务系列、计算机系列、电子信息系列、机械系列、汽车系列和化学化工系列的主要课程。目前已经规划的教材系列名称如下：

财经管理系列

- 财经管理基础课
- 工商管理类
- 财务会计类
- 经济贸易类
- 财政金融类
- 市场营销类

机械系列

- 机械基础课
- 机械设计与制造类
- 数控技术类
- 模具设计与制造类
- 机电一体化类

计算机系列

- 公共基础课
- 计算机专业基础课
- 计算机网络技术类
- 计算机软件技术类
- 计算机应用技术类

公共基础课系列

物流管理系列

电子商务系列

电子信息系列

化学化工系列

汽车系列

对于教材出版及使用过程中遇到的各种问题，欢迎您通过电子邮件及时与我们取得联系（联系方式详见“教师服务登记表”）。同时，我们希望有更多经验丰富的教师加入到我们的行列当中，编写出更多符合高职高专教学需要的高质量教材，为我国的高职高专教育做出积极的贡献。

21世纪高职高专规划教材编审委员会

序

21世纪是科技和经济高速发展的重要时期。随着我国经济的持续快速健康发展，各行各业对高技能专业型人才的需求量迅速增加，对人才素质的要求也越来越高。高职高专教育作为我国高等教育的重要组成部分，在加快培养高技能专业型人才方面发挥着重要的作用。

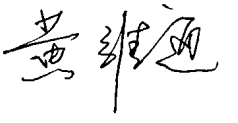
与国外相比，我国高职高专教育起步时间短，这种状况与我国经济发展对人才大量需求的现状是很不协调的。因此，必须加快高职高专教育的发展步伐，提高应用型人才的培养水平。

高职高专教育水平的提高，离不开课程体系的完善。相关领域人才的培养需要一批兼具前瞻性和实践性的优秀教材。教育部高教司针对高职高专教育人才培养模式提出了“以就业为导向”的指导思想，这也正是本套高职高专教材的编写宗旨和依据。

如何使高职高专教材既突出行业的需求特点，又突出职业的核心能力？这是教材编写的过程中必须首先解决的问题。本系列教材编委会深入研究了高职高专教育的课程和专业设置，并对以往的教材进行了详细分析和认真考察，力图在不破坏教材系统性的前提下，加强教材的创新和实践性内容，从而确保学生在学习专业知识的同时多动手，增强自己的实践能力，以加强“知”与“行”的结合。

同时，本系列教材在编写过程中还充分重视群体和类别的差异性，面对不同学校和不同专业方向的定位差异，精心设计了与其相配套的辅助实验指南及相关的习题解答等。这些栏目的设计使本系列教材内容更加丰富，条理更为清晰，为老师的讲授和学生的学习都提供了很大的便利。

经过编委会的辛勤努力，本套教材终于顺利出版了，相信本套教材一定能够很好地适应现代高职高专教育的教学需求，也一定能够在高职高专教育计算机课程的改革中发挥积极的推动作用，为社会培养更多优秀的应用型人才。

全国计算机基础教育研究会副秘书长 

前　言

随着网络技术与应用的不断发展，计算机网络在日常生活中已经变得越来越普遍。随着 Internet 在世界范围内的普及，计算机网络逐渐成为人们获取信息、发布信息的重要途径，与此同时，也出现了威胁网络安全的各种计算机病毒、恶意软件以及各种方式的网络攻击行为，还有针对这些威胁的各种安全技术、设备、软件和应用配置方法。因此，有必要在以素质、技能教育为核心的高职高专教育中涉及网络安全的内容。

本书的特点主要体现在以下 3 个方面：

首先是侧重实践。本书注重网络安全的理论知识和实际案例相结合，具有很强的可操作性，在编写形式上突出了应用需求，并配有实践项目，帮助学生巩固和掌握所学知识。

其次是层次分明。本书先介绍网络安全的基础知识和入侵防范，然后介绍现今流行的网络安全的主要技术，最后讲述了网络安全应用知识。通过阅读本书，读者可以了解计算机网络安全的基础知识，并掌握维护网络安全的主要手段和在实际中的应用方法。

最后是选材新颖。计算机网络安全技术发展非常迅速，本书在内容选择上尽量向新知识和新技术靠近，能够反映当前网络安全的最新发展成果和方向。

全书共分为 9 章：第 1 章介绍了网络安全的基础知识；第 2 章介绍了网络入侵的基本原理，并对入侵的主要过程进行了详细的剖析；第 3 章介绍了数字加密的主要原理与认证技术；第 4 章介绍了防火墙的基本知识以及当今主流防火墙应用的关键技术、体系结构和部署原则；第 5 章介绍了入侵检测的基本知识、关键技术和体系，并分析了入侵检测和防火墙的关系；第 6 章介绍了 VPN 的基本知识和关键技术，并以实例简单介绍了 VPN 的配置和应用；第 7 章介绍了计算机病毒的基本知识，分析了病毒的基本工作原理，并有针对性地阐述了病毒的防范技术和反病毒软件的使用方法；第 8 章介绍了 Web 系统和无线网络的安全问题；第 9 章介绍了 Windows Server 2003 操作系统的网络安全应用。

本书由具有丰富教学经验、长期工作在教学第一线的教师编写。本书由安洛生任主编，王利敏任副主编，参加编写工作的还有王祥雒和匡春临，具体分工如下：第 1 章、第 6 章和第 8 章由安洛生编写，第 2 章和第 7 章由王利敏编写，第 3 章和第 4 章由王祥雒编写，第 5 章和第 9 章由匡春临编写。

由于编者水平有限，加之网络安全是一个不断变化和发展的全新课题，书中难免存在一些疏漏和不妥之处，在此恳请广大读者和同行批评指正，万分感谢！

编　者

目　录

第 1 章　网络安全概述

进入 21 世纪，随着计算机网络的飞速发展，社会的经济、文化和军事越来越多地依赖于计算机网络。然而，计算机网络在给人类生活带来极大便利的同时，网络安全也面临着极大的挑战。敏感信息的泄露、信息的篡改、数据的破坏和计算机病毒的发作都会给社会生活带来难以估量的损失，解决开放式网络环境下的网络安全问题刻不容缓。网络安全作为一门综合的、交叉的学科，涉及数学、物理、管理、信息技术和计算机技术等多个学科领域。

1.1　网络安全的基础知识

“某银行的客户数据被黑客窃取”、“QQ 号码被别人盗用”等是生活中遇到的网络信息安全事件。而网络安全，从本质上讲就是网络上的信息安全，凡涉及网络信息的保密性、完整性、可用性的网络技术和理论都是网络安全研究的领域，是信息安全在当前网络环境下最重要的研究领域。

1.1.1　网络安全的定义

国际标准化组织 ISO7498-2 标准中对安全的定义是：安全就是最大限度地减少数据和资源被攻击的可能性。由于 Internet 的开放性和超越组织与国界等特点，使它在安全性的保障上存在一系列的隐患。那么，什么是网络安全呢？

目前，网络安全并没有公认和统一的定义，现在采用比较多的定义是：网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里信息数据的机密性、完整性、可使用性、真实性和可控性受到保护。

从内容上看，网络安全包括以下 4 个方面：

(1)物理安全：计算机机房的物理条件、环境和设施的安全，计算机硬件、配套设备及网络传输线路的安全。

(2)数据安全：保护数据不被非法存取，确保数据的完整性、一致性和机密性等。

(3)软件安全：保护网络系统不被非法侵入，系统软件与应用软件不被非法复制和篡改，不受病毒的侵害。

(4)安全管理：运行时对突发事件的安全处理等，包括采用计算机安全技术及规范安全管理制度，开展安全审计和进行分析等措施。

1.1.2　网络安全的需求

进入 21 世纪，随着 Internet 的发展，以网络技术及服务为代表的第二次“信息革命”浪潮席卷全球，迅速渗透到政府、企业、经济以及与日常生活息息相关的各个领域。网络上信

息的广泛传播给用户带来了极大的方便，但同时，也给用户带来了安全问题。

过去的网络大多是封闭式的，因而简单的安全性设备就足以确保其安全。然而，当今的网络已发生了变化，确保网络的安全性已成为更加复杂而且必需的任务。用户每次连接到网络上，原有的安全状况就会发生变化。简单的安全措施和设备已对现有的网络安全问题无能为力了。所以，很多网络频繁地成为网络犯罪的牺牲品。

互联网犹如一柄“双刃剑”，为人们工作带来便利的同时，伴随着日趋严重的网络入侵安全问题。一些公用站点，既要访问 Internet 的共享信息资源，又要使 Intranet 的一部分信息对外提供服务，资源共享的同时也带来了安全问题。政府部门内部网关系到很多政府机密、政府形象等敏感信息，网络的安全性更为重要。因此，保护政府内部网络的信息安全，防范来自外部网络的黑客和非法入侵者的攻击，建立强健的网络信息安全防范系统，在某种程度上决定着政府部门信息化建设的成败。

另外，随着企业网上业务的不断扩大和电子商务的发展，对网络的安全服务也提出了新的要求。严防黑客入侵、切实保障网络交易的安全，不仅关系到个人的资金安全和企业的数据安全，还关系到国家的经济安全、国家经济秩序的稳定，网络安全问题已成为亟待解决的问题。

对于个人用户而言，涉及个人隐私的信息在网络上传输时应受到保护，避免其他人利用窃听、冒充、篡改和抵赖等手段侵犯其隐私，同时也避免其他用户的非授权访问和破坏。

由此可见，目前整个 Internet 的安全问题不容乐观。而且网络安全的内涵也发生了根本的变化，它不仅从个别的防卫变成了一种非常普遍的防范，而且还从一种专门的领域变成了无处不在，有网络的地方就有网络安全问题。

1.1.3 网络安全的目标

从技术角度来说，网络信息安全的目标主要表现在以下 6 个方面。

1. 保密性

保密性是网络信息不被泄露给非授权的用户、实体或供其利用的特性。即防止信息泄露给未授权用户或实体，信息只为授权用户使用的特性。破坏信息的保密性是对信息发动攻击的最终目的。

2. 完整性

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成以及正确存储和传输。

保证完整性的目的就是保证计算机系统上的数据和信息处于一种完整和未受损害的状态，这就是说，数据不会因有意或无意的事件而被改变或丢失，信息完整性的丧失直接影响到数据的可用性。完整性与保密性不同，保密性要求信息不被泄露给未授权的用户或实体，而完整性则要求信息不受各种原因的破坏。

3. 可靠性

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定功能的特性。它是网络系统安全的最基本要求之一，是所有网络信息系统建设和运行的目标。网络系统的可靠性主要体现在以下 3 个方面：

(1)抗毁性是指系统在人为破坏下的可靠性。例如，部分线路或结点失效后，系统是否

仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害(战争、地震等)造成的大面积网络瘫痪事件。

(2)生存性是在随机破坏下系统的可靠性,主要反映随机性破坏和网络拓扑结构改变对系统可靠性的影响。

(3)有效性主要反映在网络信息系统部件失效的情况下满足业务性能要求的程度。例如,网络部件失效虽然没有引起连接性故障,但是却造成质量指标下降、平均延时增加、线路阻塞等现象的发生。

4.可用性

可用性是网络信息可被授权用户或实体访问并按需求使用的特性。即网络信息服务在需要时,允许授权用户或实体使用的特性,或者是网络部分受损或需要降级使用时,仍能为授权用户或实体提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。

网络信息系统最基本的功能是向用户提供服务,而用户的需求是随机的、多方面的,有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

5.不可抵赖性

不可抵赖性也称不可否认性。在网络信息系统的信息交互过程中,确信参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息,利用递交接收证据可以防止收信方事后否认已经接收信息。

6.可控性

可控性是对网络信息的传播及内容具有控制能力的特性。

网络信息安全与保密的核心是通过计算机、网络、密码技术和其他安全技术保护在公用网络信息系统中传输、交换和存储消息的保密性、完整性、可靠性、可用性、不可抵赖性和可控性等。

1.2　威胁网络安全的因素

随着 Internet 的发展,人们的生活发生了许多变化。银行存款的通存通兑、网上汇款、上网冲浪、网上购物等无不给人们的生活带来便利。但是,在享受计算机网络带来方便和快捷的同时,网络病毒、网络攻击以及网络犯罪也达到空前猖獗的程度,网络本身所具有的脆弱性也日益显现出来。

1.2.1　网络安全的主要威胁

目前,计算机网络所面临的安全威胁很多,主要有以下几个方面。

1.对加密算法的攻击

数据加密技术是最基本的网络安全技术,被誉为信息安全的核心。最初主要用于保证数据在存储和传输过程中的保密性。网络中使用的加密算法,从加密的种类上来分主要包括对称加密和非对称加密。公钥密码(非对称加密)体系能适应网络的开放性要求,密钥管理简单,并且可方便地实现数字签名和身份认证等功能,是目前电子商务等技术的核心基础。