重点大学信息安全专业规划系列教材

计算机网络安全

彭飞　龙敏　编著

NLIC2970894748

清华大学出版社

重点大学信息安全专业规划系列教材

计算机网络安全

彭飞 龙敏 编著

清华大学出版社
北京

内 容 简 介

本书全面地介绍了计算机网络安全技术。全书共分为12章，第1章介绍计算机网络安全的基本概念、内容和方法，随后的11章分别从网络协议安全、信息加密与认证、访问控制、防火墙与入侵检测、数据备份与恢复、操作系统安全、Web站点安全、电子邮件安全、无线网络安全、恶意软件攻击与防治以及网络入侵与取证等不同层面对计算机网络安全的相关理论与方法进行了详细介绍。

本书适合作为信息安全专业本科高年级学生以及研究生的专业课教材，也可供从事信息安全专业的技术人员阅读参考。

图书在版编目(CIP)数据

计算机网络安全/彭飞，龙敏编著. —北京：清华大学出版社，2013.4
重点大学信息安全专业规划系列教材
ISBN 978-7-302-31125-6

Ⅰ. ①计… Ⅱ. ①彭… ②龙… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第315242号

责任编辑：魏江江　王冰飞
封面设计：常雪影
责任校对：白　蕾
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 刷 者：北京季蜂印刷有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.75　　**字　　数**：483千字
版　　次：2013年4月第1版　　**印　　次**：2013年4月第1次印刷
印　　数：1～3000
定　　价：34.50元

产品编号：045677-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21世纪高等学校信息安全专业规划教材
联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

随着信息技术与 Internet 的发展，计算机网络在给人们的生活和工作带来便利的同时，也面临着严重的安全威胁，例如非法侵入计算机系统窃取机密信息、篡改和破坏数据、病毒、蠕虫、垃圾邮件、僵尸网络等。网络安全已关系到国家安全和社会稳定等重要问题。

计算机网络安全作为信息安全领域的一个重要方面，其相关技术还在不断地研究与发展。本书作者结合所在单位信息安全专业本科生和相关方向研究生培养的实际情况，编撰和出版本书作为专业课程教材。

全书共分为 12 章，第 1 章介绍了计算机网络安全的基本概念、内容和方法，分析网络安全问题产生的根源，并对安全问题进行分类；另外，还介绍了网络安全的等级标准。第 2 章介绍了网络层安全协议 IPSec，传输层安全协议 SSL、TLS 和应用层安全协议 SET、Telnet、HTTP 等。第 3 章介绍了密码学的基本原理，主要包括古典密码技术、对称密码技术以及非对称密码技术、信息认证的基本概念，单向 Hash 函数与消息认证码的基本原理及典型的认证方法和技术。第 4 章介绍了访问控制的概念、模型及访问控制中涉及的 AAA 技术与 VPN 技术。第 5 章介绍了防火墙的基本概念和种类、防火墙的体系结构及功能、入侵检测技术的种类及各类技术的相关性能。第 6 章介绍了数据的基本概念及数据备份与恢复所需的相关基础知识、数据备份技术与数据恢复技术。第 7 章介绍了计算机操作系统安全的基本概念，包括安全操作系统评价标准、常见的系统安全保护方法、单点登录的访问管理以及主流操作系统的主要安全机制等方面的知识。第 8 章介绍了 Web 应用程序上的安全问题及漏洞，以及基于 IIS 和 ASP 网站安全体系的建立及技术实现。第 9 章介绍了电子邮件安全的基本特性及其面临的安全问题，对电子邮件的几种安全技术进行了全面介绍，包括 PGP、S/MIME、PEM、PKI 技术及安全防范措施等。第 10 章分析了当前无线网络所面临的安全威胁及其防范措施，对于无线网络的代表性技术 IEEE 802.11 安全和蓝牙安全进行了介绍。第 11 章对恶意软件的基本知识、恶意软件的相关危害及防治方法和典型恶意软件的攻防方法进行了介绍。第 12 章分析了导致网络脆弱的因素，对网络入侵的常用方法及防范措施、入侵检测系统的原理、结构和流程以及计算机取证的一般步骤和取证模型进行了介绍。

本书由彭飞负责编写，全书由龙敏负责整理修订。本书适合作为信息安全专业本科高年级学生以及研究生的专业课教材，也可供从事信息安全专业的技术人员和研究人员阅读参考。

本书作为教材适合于 48～64 学时的教学，建议的教学方式为课堂讲授与实验相结

合，教师可根据书上的思考题，指导学生进行编程或仿真实验，通过对原理和应用算法的实验，进一步加深学生对所学内容的理解。

本书作者多年来一直从事信息安全的教学和研究工作，本书也是网络与信息安全湖南省重点实验室全体师生多年从事数字内容安全研究工作成果的结晶。

在本书的编写过程中，钱勤、刘艳、陈丽、朱小文、李洪淋、刘娟、李姣婷等研究生参与了部分资料的收集与整理工作；清华大学出版社的魏江江主任为本书的高质量出版倾注了大量心血；此外，本书的编写还得到了湖南大学信息科学与工程学院李仁发教授、赵欢教授等的大力支持，在此对他们付出的辛勤劳动表示由衷感谢。

计算机网络安全技术日新月异，限于作者水平和经验，书中难免出现疏漏之处，望读者提出宝贵意见，以便再版时修改和完善。

编　者

2012 年 10 月

目　录

第1章　计算机网络安全概述

本章学习目标

计算机网络安全问题是随着信息技术和网络技术的发展而出现的，网络安全涉及各行各业的许多重大利益问题，因此计算机网络的安全防护已得到广泛重视。本章介绍计算机网络安全的基本概念、内容和方法，分析网络安全问题产生的根源，并对网络安全问题进行分类，介绍网络安全的等级标准。

通过对本章的学习，应掌握以下内容：

(1) 网络安全问题的产生与分类。

(2) 计算机网络安全的基本概念、内容、目标和要求。

(3) 计算机网络安全体系结构与基本方法。

(4) 计算机网络安全评估的概念与方法。

(5) 网络安全等级标准。

信息技术的发展给人们的生活、工作等方面带来了便捷和好处。然而，计算机信息技术是一把双刃剑，它在为人们提高工作效率，为社会创造更多财富的同时，也为一些人利用它进行非法勾当提供了可能。例如非法侵入计算机系统窃取机密信息、篡改和破坏数据等。这些非法行为将给社会造成难以估量的损失。据统计，全球约每20秒钟就有一次计算机入侵事件发生，Internet上的网络防火墙约有1/4曾被突破过，大约有70%以上的网络管理人员报告曾因机密信息泄露而受到了损失。

在当前的数字化时代，信息技术和网络技术与人们的生活和工作息息相关、密不可分。因此，网络安全已关系到国家安全和主权、社会的稳定、民族文化的继承和发扬等重要问题。网络安全的涉及面很广，包含了计算机科学、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。同时，除了技术上的问题，还有法律的问题、管理的问题等。

1.1　计算机网络安全的基本概念

1.1.1　网络安全的定义

计算机网络是指将地理位置不同的具有独立功能的多台计算机及其外部设备通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传输的计算机系统。

从一般意义来看，安全是指没有危险和不出事故。对于计算机网络而言，其安全问题是指网络系统的硬件、软件及其系统中的数据受到保护，不遭到偶然的或者恶意的原因破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。从广义上来说，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所要研究

的领域。

计算机网络的安全实际上包括两方面的内容：一是网络的系统安全，二是网络的信息安全。由于计算机网络最重要的资源是它向用户提供的服务及其所拥有的信息，因而计算机网络的安全性可以定义为：保障网络服务的可用性和网络信息的完整性。前者要求网络向所有用户有选择地随时提供各自应得到的网络服务，后者则要求网络保证信息资源的保密性、完整性、可用性和准确性。可见，建立安全的网络系统要解决的根本问题是如何在保证网络的连通性、可用性的同时对网络服务的种类、范围等进行适当程度的控制从而保障系统的可用性和信息的完整性不受影响。

由此可见，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，二者相互补充，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。

1.1.2 网络安全的基本特征

一个安全的计算机网络通常应具有以下几个特点。

1. 保密性

保密性是指网络信息不被泄露的特性。保密性是保证网络信息安全的一个非常重要的手段。保密性可以保证即使信息泄露，非授权用户在有限的时间内也无法识别真正的信息内容。常用到的保密措施主要包括：信息加密和物理保密（限制、隔离、隐蔽、控制），防辐射，防监听等。

2. 完整性

完整性是指网络信息未经授权不能进行改变的特性，即网络信息在存储和传输过程中不被删除、修改、伪造、乱序、重放和插入等操作改变，保持信息的原样。影响网络信息完整性的主要因素包括设备故障、误码、人为攻击以及计算机病毒等。

3. 可用性

可用性是指网络信息可被授权用户访问的特性，即网络信息服务在需要时能够保证授权用户使用。这里包含两个含义：当授权用户访问网络时不致被拒绝；授权用户访问网络时要进行身份识别与确认，并且对用户的访问权限加以规定的限制。

4. 可控性

可控性是指可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。可控性要求能对信息的传播及内容具有控制能力。

5. 可靠性

可靠性是网络系统安全最基本的要求，主要是指网络系统硬件和软件无故障运行的性能。提高可靠性的具体措施主要包括：提高设备质量，配备必要的冗余和备份，采取纠错、自愈和容错等措施，强化灾害恢复机制，合理分配负荷等。

6. 不可抵赖性

不可抵赖性也称作不可否认性，主要用于网络信息的交换过程，保证信息交换的参与者