高等教育计算机学科“应用型”规划教材

网络安全技术及应用

郑秋生　主编
王清贤　主审

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

高等教育计算机学科“应用型”规划教材

网络安全技术及应用

郑秋生　主　编
王文奇　潘　恒　张志勇　副主编
王清贤　主　审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

随着信息技术与通信网络技术的迅猛发展，计算机网络正面临着前所未有的安全性挑战，网络安全的攻击、防御、保障技术也日新月异。本书主要从网络安全基础理论、典型攻击技术、安全防御技术及网络安全新技术四个方面，系统地阐述密码学基础理论与公钥基础设施体系，网络攻击方法及计算机病毒，防火墙应用与入侵检测，以及近年来涌现的可信计算与安全风险评估等新理论、新技术、新方法。本书以网络安全技术的应用性为主要特色，内容阐述深入浅出、问题分析清晰透彻，除了系统地介绍相关技术与理论外，每章还有具体的应用实例及实验环节部分，可进一步加深读者对内容的理解和掌握。

本书可以作为高等院校计算机科学与技术、信息安全、网络工程等相关专业本科生和专科生的教材或参考书，也可作为从事网络安全工程系统设计、应用开发、部署与管理工作的高级技术人员的培训参考书。

本书配有免费课件资源，有需要的读者可到华信教育资源网（www. huaxin. edu. cn 或者 www. hxedu. com. cn）下载使用。

图书在版编目（CIP）数据

网络安全技术及应用/郑秋生主编. —北京：电子工业出版社，2009. 8
高等教育计算机学科“应用型”规划教材
ISBN 978 - 7 - 121 - 09195 - 7

Ⅰ. 网… Ⅱ. 郑… 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（2009）第 109869 号

策划编辑：张 旭 何 况
责任编辑：侯丽平
印 刷：
装 订：北京京师印务有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787 × 1092 印张：17. 75 字数：454. 4 千字
印 次：2009 年 8 月第 1 次印刷
定 价：28. 00 元

凡所购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@ phei. com. cn，盗版侵权举报请发邮件至 dbqq@ phei. com. cn。

服务热线：（010）88258888。

编　委　会

出 版 说 明

高等教育的教学改革及课程建设总是伴随着科技的进步与生产的发展而发展的。当前高等教育既要培养理论基础扎实、高素质的科研型人才，也要培养具有一定的理论基础更具有较高工程能力的应用型人才。为了满足普通高等院校面向应用的需求，进一步提高高等院校教学质量和教学水平，河南省计算机学会与电子工业出版社共同组织了高等教育计算机学科“应用型”规划教材的编写和出版工作。

高等教育计算机学科“应用型”规划教材根据培养目标和对象不同，总结教学改革和教材建设经验，在基础理论方面做出了合理的取舍，同时融入了现代科技应用的成果。这是一种理论与实践、基础知识与现代技术有机结合的教材。

本套教材定位于国内普通高等院校本科、专科的学生，也适用于高职高专、成人教育的学生。教材内容充分考虑学生的知识水平、理解能力和教学要求，遵循由浅入深、循序渐进的原则，适合学生自学和教师教学。

本套教材符合相应教学大纲的基本要求，结合案例（实例）展开教学内容，侧重应用，突出实践，强调理论与实践结合。

本套教材努力从学习者（学生、自学者）的角度阐述理论知识，充分利用图表进行形象化表达，适当补充相关知识内容，引导读者阅读相关书籍。教材内容的选取注重帮助读者建立完整的知识结构，而不是仅仅掌握某个知识单元。教材内容关注计算机技术的迅猛发展，及时补充最新技术。

本套教材努力提供丰富的教学辅助资源，建立师生交流平台，以便于教师、学生使用。读者可以通过电子工业出版社的华信教育资源网站（www. huaxin. edu. cn 或 www. hxedu. com. cn）了解本套教材的出版和服务的动态信息。

河南省计算机学会

电子工业出版社

前　言

进入新世纪的近10年，信息技术与计算机网络技术的日新月异和迅猛发展，涌现出大量的面向大规模网络环境的应用，如电子商务、电子政务、移动计算、普适计算，以及企事业单位基于业务的Intranet构建等，使得整个互联网得到了空前的广泛应用。与此同时，网络安全问题也面临着严峻的考验，身份冒充、端口扫描、网络嗅探、分布式拒绝服务攻击等手段，以及木马、病毒、恶意程序的入侵，致使敏感的数据信息被窃取、篡改和滥用，计算机和网络的安全正遭受到严重威胁。因此，使计算机网络系统免受破坏，提高系统安全性已成为亟待解决的问题，读者也迫切需要一本理论与实际应用紧密结合的教材。

传统的安全解决方案，如密码学、防火墙与入侵检测、防病毒软件等在网络安全防御上发挥了重要的作用，减少了上述的不安全隐患。此外，近年来可信计算、蜜罐网络及安全风险评估等技术的发展，促使从根源的终端安全出发解决网络安全问题，并建立主动的安全防御体系，实施有效的系统安全风险识别与规避。因此，系统、全面地了解和掌握网络安全技术，特别是它们的具体应用，是非常必要和实用的。

本书的撰写以应用性为目的，通过丰富的应用实例介绍和实验环节设计，深入理解和掌握网络安全技术与相关理论，也使得相关技术的学习变得生动、可再现，而不再枯燥和晦涩。本书的主要作者都是来自高等院校从事计算机与网络安全教学和科研的一线教师，他们结合多年来在课堂教学和实验教学等环节中的丰富经验和体会，并考虑到学生在理解和掌握相关技术上遇到的问题和难点，阐述深入浅出，力求重点突出、层次清晰、分析透彻。本书有以下鲜明特点。

首先，本书以网络安全相关基础知识、网络攻击技术、安全防御技术及新技术为主线，模块化清晰，有助于读者由浅入深地学习和理解相关技术与理论，同时也便于学生自学和实践。

其次，本书以网络安全技术及其应用为主线，每章所设计的实验环节有利于教师实验教学和学生实践。此外，每章所附习题也有助于学习和掌握重点、难点知识，提高解决实际问题的能力。

再次，本书最后用一个章节的篇幅，概括性地介绍了近年来涌现的网络安全新理论、新技术，使得读者在学习和掌握了传统网络安全技术之后，对未来安全技术的发展动向有所了解和把握，激发他们进一步地学习与求知。

最后，本书阐述内容的语言平实、生动而精炼，对基本概念、基础理论的解释力求准确和完整，相关图表的绘制清晰而简洁。

本书可大致分为四篇，分别为网络安全基础篇、网络攻击篇、安全防御篇和网络安全新技术篇。其中第1章为网络安全概述，主要使读者对网络安全相关概念和体系结构有概貌性的了解；第2、3章侧重于密码学理论的应用和实践，尽量避免繁杂、晦涩的密码学算法设计，使得读者有兴趣进一步学习下去；第4、5章分别介绍了典型的网络攻击技术和计算机病毒，使读者了解和掌握这些基本的攻击方法和过程；接下来的第6～8章主要探讨系统安全与防御技术，

主要涉及操作系统安全、防火墙及其应用，以及入侵检测系统等，这些安全防御技术的融合是构建网络安全平台的基础方法和手段；最后一章，主要介绍近年来网络安全新技术的发展，使得读者了解和把握网络安全的新动向和新思路。

为了方便使用本书的教师备课和课程教学，我们提供了配套的电子教案，公开在网站上，供任课教师自由下载使用，也可来函索取。相信我们多年的教学实践经验会对广大师生的教学活动有所帮助和启迪。建议使用本书的教学学时为 60 个学时，其中理论教学 40 学时，实验教学 20 学时，学生课外学习与实践不少于 20 学时。

第 1 章和第 8 章由翟光群副教授编写，第 2 章由潘恒博士编写，第 3 章和第 9 章第 4 节由郑秋生教授编写，第 4 章由李玉青老师编写，第 5 章和第 9 章第 2 节由王文奇博士编写，第 6 章由张新刚老师编写，第 7 章和第 9 章的第 1、3 节由张志勇博士编写。本书由中原工学院郑秋生教授担任主编并统稿，由解放军信息工程大学王清贤教授担任主审。本书的策划得到了河南省计算机学会和电子工业出版社的大力支持和帮助，中原工学院的苗凤君、孙飞显、潘磊、裴斐、张书钦等老师和陈帅研究生等也参与了研讨和校稿工作，在此对他们一并表示衷心的感谢。

由于编者水平有限，加之时间仓促，书中难免有不妥和疏漏之处，敬请广大读者指正。作者的 E-mail：zqs65@ yahoo. com. cn。

作　者

2009 年 5 月

目　录

第1章

网络安全概述

学习目标

本章介绍了网络安全的相关基本概念，使学生理解网络安全的内涵和属性，掌握网络安全的基本安全策略、安全服务和安全机制，了解网络的各种安全威胁，以及网络安全的体系结构和评估准则。

教学方式

以教师讲解为主。

知识点

- 网络安全的内涵
- 网络安全的属性
- 网络安全主要威胁
- 网络安全策略
- 网络安全服务和相关机制
- 网络安全体系结构
- 网络信息安全评价标准

1.1　网络安全的内涵和属性

1.1.1　网络安全的内涵

21 世纪是信息时代，网络已经成为人们快速、全面获取信息的主要渠道，成为人们日常生活和工作不可或缺的组成部分。人们在充分享受网络带来巨大便利的同时，也深刻感受到网络安全事件和黑客攻击的烦恼。

网络安全(Network Security)涉及计算机科学、通信技术、密码理论、信息论等多个学科，因此迄今为止，学术界对网络安全仍没有一个统一的定义。

要了解网络安全的内涵，首先要了解计算机网络的概念。计算机网络是地理上分散的多台自主计算机互联的集合。从该定义中我们可以了解到计算机网络安全涉及的内容，包括计算机主机软硬件系统安全、通信系统安全，以及各种网络应用和服务的安全。

计算机是网络的基本组成元素，现代数据处理系统都是建立在计算机网络基础上的。因此，网络安全的研究内容也包括计算机信息系统安全。国际标准化组织(ISO)将计算机信息系统安全定义为："为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。"

网络是信息的重要载体，因此从信息系统特点和运行过程出发，网络安全的研究内容可大致分为四个方面：实体安全、运行安全、数据安全和管理安全。

(1) 实体安全是指保护计算机设备、网络设施及其他媒介免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施及过程。

(2) 运行安全是指为保障系统功能的安全实现，提供一套安全措施(如安全评估、审计跟踪、备份与恢复、应急措施等)来保护信息处理过程的安全。

(3) 数据安全是指防止信息资源被故意或偶然地非授权泄露、更改、破坏、被非法系统辨识、控制和否认，即要确保信息的机密性、完整性、可用性、可控性和不可否认性。

(4) 管理安全是指有关的法律法令和规章制度及安全管理手段，确保系统安全生存和运营。

1.1.2　网络安全的属性

从技术角度上讲，网络安全的主要属性表现在网络信息系统的机密性、完整性、可用性、可控性、不可抵赖性等方面。

1. 机密性

机密性是指网络信息不被泄露给非授权的用户，即信息只能被授权用户所使用的特性。

常用技术包括：防侦听，使敌人侦听不到有用的信息；防辐射，防止有用信息以各种途径辐射出去；信息加密，在密钥的控制下，用加密算法对信息进行加密处理，使敌人即使获取到密文信息，也会因为没有密钥而无法获取有效信息；物理保密，利用限制、隔离、隐蔽、控制等各种物理方法保护信息不被泄露。

2. 完整性

完整性是保证网络信息未经授权不能进行改变的特性，即网络信息能从真实信源无失真

地到达真实信宿的特性。要求信息在存储或传输过程中不会遭受偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏。完整性是一种面向信息的安全特性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。

完整性与机密性不同，机密性可以防止被动攻击，要求信息不被泄露给未授权的人，而完整性主要防止各种主动攻击，要求信息不受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障、误码、计算机病毒、木马等。保障网络信息完整性的主要方法有：安全协议、纠错编码、数字签名和第三方公证等。

3. 可用性

可用性是指网络信息可被授权用户按需使用的特性，即保证信息及信息系统不被非授权者非法使用，同时防止由于计算机病毒或其他人为因素造成的系统拒绝服务，影响授权用户的合法使用等。它是信息系统面向用户的安全特性。

保证可用性的主要方法有：身份认证、访问控制、业务流控制、路由选择控制、审计跟踪等。

4. 可控性

可控性是指控制网络信息的内容及其传播的能力，即对信息及信息系统实施安全监控管理。

5. 不可抵赖性

不可抵赖性也称做不可否认性，是指在网络信息系统的信息交互过程中，所有参与者都不能否认或抵赖曾经完成过的操作和承诺。通常，采用数字签名和可信第三方等方法可以保证信息的不可抵赖性。

1.2　网络安全的威胁

网络安全面临的威胁来自多方面，并且随着时间的变化而变化。总体说来，这些威胁可以宏观地分为人为威胁和自然威胁（如图 1－1 所示）。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射、电磁干扰、网络设备自然老化等。这些事件有时会直接威胁网络安全，影响信息的存储媒介。本节主要介绍人为威胁（也称为人为攻击）。

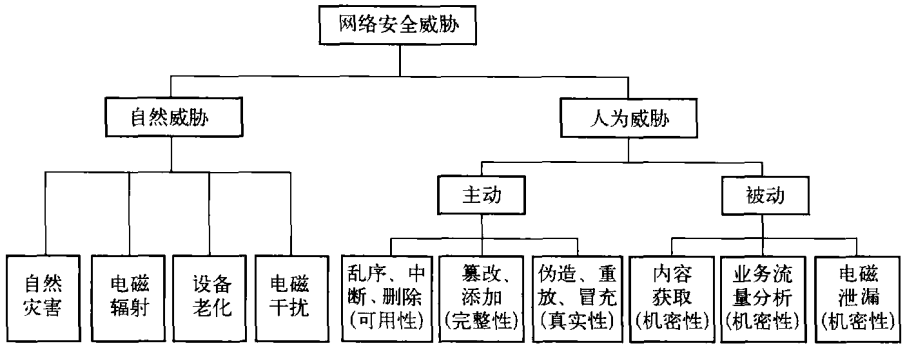

图 1－1　网络安全威胁分类