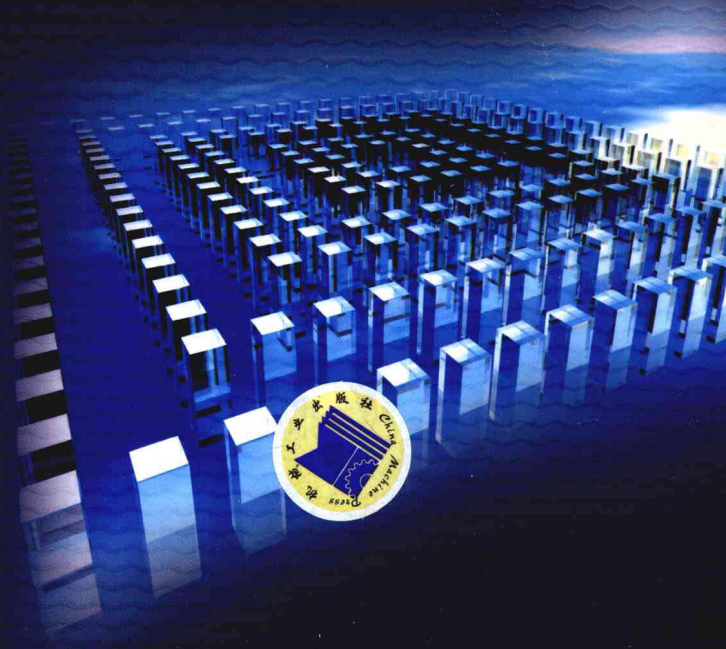
免费提供电子教案

高等院校规划教材

计算机科学与技术系列

网络安全技术及应用

贾铁军　主　编
沈学东　副主编
苏庆刚　王　坚　王小刚　参　编



机械工业出版社
CHINA MACHINE PRESS

高等院校规划教材·计算机科学与技术系列

网络安全技术及应用

贾铁军　主　编
沈学东　副主编
苏庆刚　王　坚　王小刚　参　编

机械工业出版社

本书突出“实用、新颖、有特色、操作性强”的特点。

全书共分12章，主要包括网络安全技术基础知识、网络安全管理技术、黑客攻防与入侵检测技术、身份认证与访问控制技术、密码与加密技术、病毒及恶意软件防护技术、防火墙应用技术、操作系统与站点安全技术、数据库系统安全技术、电子商务安全技术及应用等内容。

本书提供配套的电子教案，并配有辅助教材《网络安全技术及应用实践教程》，内容包括学习指导、实验教学、练习测试和课程设计等。

本书可作为应用型本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训及参考用书，还可作为高职院校相关专业师生的选修教材。

图书在版编目(CIP)数据

网络安全技术及应用/贾铁军主编. —北京:机械工业出版社,2009.2
(高等院校规划教材·计算机科学与技术系列)
ISBN 978-7-111-25930-5

Ⅰ.网… Ⅱ.贾… 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010397号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
责任编辑:陈 皓
责任印制:杨 曦
三河市宏达印刷有限公司印刷

2009年2月第1版·第1次印刷
184mm×260mm·25印张·618千字
0001-3000册
标准书号:ISBN 978-7-111-25930-5
定价:41.00元

凡购本书,如有缺页,倒页,脱页,由本社发行部调换
销售服务热线电话:(010)68326294 68993821
购书热线电话:(010)88379639 88379641 88379643
编辑热线电话:(010)88379753 88379739

出 版 说 明

计算机技术的发展极大地促进了现代科学技术的发展，明显地加快了社会发展的进程。因此，各国都非常重视计算机教育。

近年来，随着我国信息化建设的全面推进和高等教育的蓬勃发展，高等院校的计算机教育模式也在不断改革，计算机学科的课程体系和教学内容趋于更加科学和合理，计算机教材建设逐渐成熟。在“十五”期间，机械工业出版社组织出版了大量计算机教材，包括“21世纪高等院校计算机教材系列”、“21世纪重点大学规划教材”、“高等院校计算机科学与技术‘十五’规划教材”、“21世纪高等院校应用型规划教材”等，均取得了可喜成果，其中多个品种的教材被评为国家级、省部级的精品教材。

为了进一步满足计算机教育的需求，机械工业出版社策划开发了“高等院校规划教材”。这套教材是在总结我社以往计算机教材出版经验的基础上策划的，同时借鉴了其他出版社同类教材的优点，对我社已有的计算机教材资源进行整合，旨在大幅提高教材质量。我们邀请多所高校的计算机专家、教师及教务部门针对此次计算机教材建设进行了充分的研讨，达成了许多共识，并由此形成了“高等院校规划教材”的体系架构与编写原则，以保证本套教材与各高等院校的办学层次、学科设置和人才培养模式等相匹配，满足其计算机教学的需要。

本套教材包括计算机科学与技术、软件工程、网络工程、信息管理与信息系统、计算机应用技术以及计算机基础教育等系列。其中，计算机科学与技术系列、软件工程系列、网络工程系列和信息管理与信息系统系列是针对高校相应专业方向的课程设置而组织编写的，体系完整，讲解透彻；计算机应用技术系列是针对计算机应用类课程而组织编写的，着重培养学生利用计算机技术解决实际问题的能力；计算机基础教育系列是为大学公共基础课层面的计算机基础教学而设计的，采用通俗易懂的方法讲解计算机的基础理论、常用技术及应用。

本套教材的内容源自致力于教学与科研一线的骨干教师与资深专家的实践经验和研究成果，融合了先进的教学理念，涵盖了计算机领域的核心理论和最新的应用技术，真正在教材体系、内容和方法上做到了创新。同时，本套教材根据实际需要配有电子教案、实验指导或多媒体光盘等教学资源，实现了教材的“立体化”建设。本套教材将随着计算机技术的进步和计算机应用领域的扩展而及时改版，并及时吸纳新兴课程和特色课程的教材。我们将努力把这套教材打造成为国家级或省部级精品教材，为高等院校的计算机教育提供更好的服务。

对于本套教材的组织出版工作，希望计算机教育界的专家和老师能提出宝贵的意见和建议。衷心感谢计算机教育工作者和广大读者的支持与帮助！

机械工业出版社

前　言

随着计算机网络技术的快速发展，我国在网络化建设方面取得了令人瞩目的成就。电子银行、电子商务和电子政务的广泛应用，使计算机网络已经深入到国家的政治、经济、文化和国防建设的各个领域，遍布现代信息化社会工作和生活的各个层面，“数字化经济”和全球电子交易一体化正在形成。计算机网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及国家政治、军事和经济各个方面，而且影响国家的安全和主权。随着计算机网络的广泛应用和网络之间数据传输量的急剧增大，网络安全的重要性尤为突出。因此，网络技术中最关键也最容易被忽视的安全问题，正在危及网络的发展和应用，而且已经成为各国关注的焦点，也成为研究热点和人才需求的新领域。

随着信息技术的发展与应用，网络安全的内涵在不断地延伸。从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。网络安全是一个综合、交叉学科领域，要综合利用数学、物理、通信和计算机等诸多学科的长期知识积累和最新发展成果，不断发展和完善。为满足高校应用型人才培养的需要，我们编写了本书。本书的主要作者20多年来，在高校从事计算机网络与安全等领域的教学、科研和学科专业管理工作，特别是在公安院校多次主持过计算机网络安全方面的科研项目研究，积累了大量宝贵的实践经验。

全书共分12章，重点介绍了计算机网络安全的基本知识、原理及应用技术，主要内容包括：计算机网络安全概述和基本安全问题；网络安全技术的基本概念、内容和方法；网络协议安全、安全体系结构、网络安全管理技术、安全服务与安全机制、无线网安全技术及应用；入侵检测技术、黑客的攻击与防范技术；身份认证与访问控制技术；网络安全中的密码与加密技术；病毒及恶意软件的防护技术；防火墙技术及应用；操作系统与站点安全技术、数据与数据库安全技术；电子商务安全技术及应用等。书中给出了很多实例，以及作者经过多年的实践总结出来的案例及研究成果。书中带“*”部分为选学内容。

本书重点介绍了最新成果、防范技术、处理技术、方法和实际应用。其特点如下：

（1）内容先进，结构新颖。书中吸收了国内外大量的新知识、新技术、新方法和国际通用准则，注重科学性、先进性、操作性。

（2）注重实用性和特色。坚持“实用、特色、规范”原则，突出实用及素质能力培养，在内容安排上，通过大量案例将理论知识与实际应用有机结合。

（3）资源配套，便于教学。为了方便教学，本书还配备了电子教案，读者可登录机械工业出版社的教材网站（http://www.cmpedu.com）进行了下载。同时，在本书配套的辅助教材《网络安全技术及应用实践教程》中提供了同步实验、学习指导、练习测试等内容，供师生选用。

本书由贾铁军主编、统稿并编写第1～6、11、12章，沈学东任副主编并编写第10章，

王小刚编写第7章，王坚编写第8章并完成部分习题解答和课件制作，苏庆刚编写第9章。

叶春明对全书进行了审阅，于森参加了本书大纲的讨论、审校等工作，邹佳芹对全书的文字、图表进行了校对编排并完成了资料查阅等工作，在此一并表示感谢。同时，感谢对本书编著给予大力支持和帮助的上海电机学院有关领导和同仁。

因作者水平有限，书中难免存在不妥之处，欢迎提出宝贵意见和建议。

编　者

目　录

第1章　网络安全概论

计算机网络安全不仅关系到国计民生，还与国家安全密切相关；不仅涉及国家政治、军事和经济各个方面，而且影响国家的安全和主权。随着计算机网络的广泛应用和网络之间数据传输的急剧增加，网络安全的重要性尤为突出。因此，现代网络技术中最关键也最容易被忽视的安全性问题，已经成为各国关注的焦点，也成为热门研究和人才需求的新领域。只有在法律、管理、技术、道德各个方面采取切实可行的有效措施，才能构筑全社会的信息安全体系，以确保网络建设与应用“又好又快”地顺利发展。

本章要点

- 网络安全的概念、技术特征、研究目标及内容
- 网络面临的威胁及其因素分析
- 网络安全模型、网络安全保障体系和关键技术
- 保护网络信息安全法律法规
- 安全技术评估标准和准则
- 网络安全设计与建设的原则和步骤

教学目标

- 掌握网络安全的概念、技术特征、研究目标及内容
- 了解网络面临的威胁及其因素分析
- 掌握网络安全模型、网络安全保障体系和关键技术
- 了解保护网络信息安全法律法规
- 理解安全技术评估标准和准则
- 掌握网络安全设计与建设的原则和步骤

1.1　网络安全概述

信息安全（Information Security）是指防止信息财产被故意或偶然的非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，即确保信息的完整性、保密性、可用性和可控性。信息安全是计算机、通信工程、数学等领域的交叉学科。

信息安全技术（Information Security Technology）是指在信息系统的物理层、应用层，以及对信息自身的保护（数据层）及攻击（内容层）的层面上，所反映出的对信息自身与信息系统在可用性、保密性与真实性方面的保护与攻击的技术。

信息安全技术在发展过程中经历了以下3个阶段。

（1）通信保密阶段（Communication Security）

20世纪初期，对安全理论和技术的研究只侧重于密码学，这一阶段的信息安全可以简单地称为通信安全。

（2）信息安全阶段（Information Security）

20 世纪 60 年代后，人类将信息安全的关注扩展为以保密性、完整性和可用性为目标的信息安全阶段。

（3）信息保障阶段（Information Assurance）

20 世纪 90 年代也称网络信息系统安全阶段，信息安全的焦点衍生出可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障阶段。

1.1.1 网络安全的概念及技术特征

1. 网络安全的概念

计算机网络安全（Computer Network Security，简称网络安全）是指利用网络管理控制和技术措施，保证在网络环境中数据的保密性、完整性、网络服务可用性和可审查性受到保护。保证网络系统的硬件、软件及其系统中的数据资源得到完整、准确、连续运行和服务不受到干扰破坏和非授权使用。网络的安全问题实际上包括网络的系统安全和网络的信息安全两方面的内容，而保护网络的信息安全是网络安全的最终目标和关键。因此，网络安全的实质是网络的信息安全。其中的网络系统或计算机信息系统（Computer Information System）是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

从狭义的保护角度来看，网络安全是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害。从广义的角度来说，凡是涉及计算机网络上信息的保密性、完整性、可用性、可控性、不可否认性的相关技术和理论都是计算机网络安全的研究领域。现在通常所称的“网络安全”如无特别声明，一般均指广义的定义。

计算机网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、应用数学、密码技术和信息论等多学科的综合性学科，是信息安全学科的重要组成部分。

随着信息技术的发展与应用，信息安全的内涵在不断地延伸和变化。从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。信息安全是一个综合、交叉学科领域，它要综合利用数学、信息学、通信和计算机诸多学科的长期知识积累和最新发展成果。因此，网络安全的概念、理论和技术正在不断地发展完善之中，很多观点、技术和方法也不尽一致，而且具有其特殊性。

网络安全需求定义包括网络安全硬件、网络安全软件和网络安全服务。其中，用于保护计算机信息系统安全的专用硬件和软件，属于计算机信息系统安全专用产品（Security Products for Computer Information Systems）。由于网络安全与国家安全密切相关，所以各国的关键技术并不公开，有的国家对出口的密码等产品作了各种限制，甚至有的在一些出口的网络安全系统中设置了“系统中的系统”，以获取和控制他国的信息或技术。因此，既不能使用难以监控的信息网络安全技术和产品，也不能照搬照抄国外的网络安全技术，必须把发展网络安全立足于本国的自主创新上。

2. 网络安全的技术特征

网络安全定义中的保密性、完整性、可用性、可控性、不可否认性，反映了信息安全的基本特征和目标，其中前 3 个为信息安全的基本要求。保证信息安全最根本的就是保证信息安全的基本特征发挥作用。因此，如下的网络信息安全的 5 大特征，也反映了网络安全的基

本属性、要素与技术方面的重要特征。

（1）保密性

网络信息安全的保密性，是指网络信息按给定要求不泄露给非授权的个人、实体或过程，或提供其利用的特性，即杜绝有用信息泄露给非授权个人或实体，强调有用信息只被授权对象使用的特征。

（2）完整性

网络信息安全的完整性，是指信息在传输、交换、存储和处理过程中保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储、传输，这是最基本的安全特征。

（3）可用性

网络信息安全的可用性，是指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。

（4）可控性

网络信息安全的可控性，是指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息在一定的传输范围和存放空间内可控。除了采用常规的传播站点和传播内容监控形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

（5）不可否认性

网络信息安全的不可否认性又称可审查性，是指网络通信双方在信息交互过程中，确信参与者本身以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

1.1.2 网络安全的研究目标及内容

1. 网络安全的研究目标

网络安全的研究目标是：在覆盖计算机和通信领域的信息传输、存储与处理的整个过程中，提供物理上、逻辑上的防护、监控、反应恢复和对抗的能力，以保护网络信息资源的保密性、完整性、可控性和抗抵赖性。网络安全的最终目标是保障网络上的信息安全。解决网络安全问题需要安全技术、管理、法制、教育并举，从安全技术方面解决信息网络安全问题是最基本的方法。

2. 网络安全的内容

一般情况下提到的“网络安全”主要是从自然科学方面介绍其相关的内容。网络信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别等7个方面。

信息安全各部分的内容及其相互关系如图1-1所示。

网络安全所涉及的内容可以概括为以下5个方面。具体内容将在第3章和以后章节进行系统介绍，在此重点介绍网络安全技术的相关内容。

（1）实体安全（Physical Security）

实体安全也称物理安全，是指保护计算机设备、设施（含网络）以及其他媒体免遭地

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、过程，包括环境安全、设备安全和媒体安全3个方面。实体安全是信息系统安全的基础。依据实体安全国家标准，将实施过程确定为检测与优化项目：机房安全、场地安全、机房环境、设施安全、设备可靠性、通信线路安全性、辐射控制与防泄露、动力、电源/空调、灾难预防与恢复等，检测优化实施过程按照国家相关标准和公安部的实体安全标准。

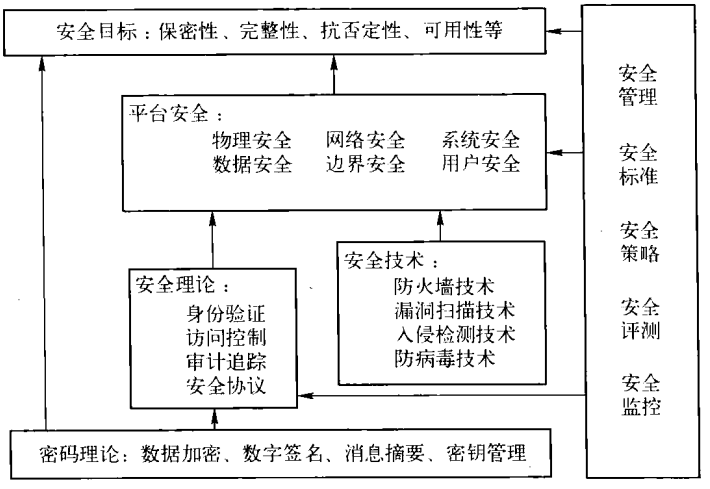


图1-1 信息安全内容及相互关系

（2）运行安全（Operation Security）

为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急等）来保护信息处理过程的安全。运行安全包括网络运行和网络访问控制的安全，如设置防火墙实现内外网的隔离、备份系统实现系统的恢复。

运行安全可保障系统的稳定性，较长时间内将网络系统的安全控制在一定范围内。运行安全提供的实施措施包括应急处置机制和配套服务、网络系统安全性监测、网络安全产品运行监测、定期检查和评估、系统升级和补丁提供、跟踪最新安全漏洞、灾难恢复机制与预防、系统改造管理、网络安全专业技术咨询服务。

（3）系统安全（System Security）

系统安全包括操作系统安全、数据库系统安全和通信系统安全。也有的将其分为3个独立部分，其内容实质是一样的。

（4）应用安全（Application Security）

应用安全由应用软件开发平台安全和应用系统安全两部分组成。应用安全可保障相关业务在网络系统上安全运行，它的脆弱性可能给信息化系统带来致命威胁。以业务运行面临的威胁为依据，为应用安全提供的评估措施有业务软件的程序安全性测试、业务交往的抗抵赖测试、业务资源的访问控制验证测试、业务实体的身份鉴别检测、业务现场的备份与恢复机制检查、业务数据的唯一性/一致性/防冲突检测、业务数据的保密性测试、业务系统的可靠性测试、业务系统的可用性测试。测试实施后，可有针对性地为业务系统提供安全建议、修复方法、安全策略和安全管理规范。