教育部高等学校管理科学与工程类学科专业
教学指导委员会推荐教材

网络安全管理及实用技术

Network Security Management and Practical Technology

贾铁军　主编

机械工业出版社
CHINA MACHINE PRESS

教育部高等学校管理科学与
工程类学科专业教学指导委员会推荐教材

网络安全管理及实用技术

主　编　贾铁军
副主编　嵩　天　常　艳
参　编　王　雄　俞小怡　刘雪飞
　　苏庆刚　宋少婷
主　审　薛一波

机械工业出版社

本书主要内容：网络安全管理及实用技术的基本知识；网络安全体系结构、无线网及虚拟专用网安全管理、IPv6 安全性；网络安全的规划、测评与规范、法律法规、体系与策略、管理原则与制度；黑客的攻防与入侵检测；身份认证与访问控制；密码与加密管理；病毒及恶意软件防护；防火墙安全管理；操作系统与站点安全管理、数据与数据库安全管理；电子商务网站安全管理及应用；网络安全管理解决方案等。包括“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技术应用。

本书主要特色：实用、新颖、操作性强。每章配有案例和同步实验指导、练习与实践习题等，通过机械工业出版社网站提供配套的多媒体课件和部分习题答案，方便选用。

本书可作为高等院校计算机与工程类、管理类、信息类和电子商务类专业的教材，也可作为培训及参考用书。

图书在版编目（CIP）数据

网络安全管理及实用技术/贾铁军主编. —北京：机械工业出版社，2010.8

教育部高等学校管理科学与工程类学科专业教学指导委员会推荐教材

ISBN 978-7-111-31065-5

Ⅰ.①网… Ⅱ.①贾… 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（2010）第 146373 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：易 敏 责任编辑：易 敏 封面设计：张 静

责任校对：纪 敬 责任印制：乔 宇

三河市国英印务有限公司印刷

2010 年 10 月第 1 版第 1 次印刷

184mm×260mm · 22.75 印张 · 562 千字

标准书号：ISBN 978-7-111-31065-5

定价：39.80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

社服务中心：（010）88361066

销 售 一 部：（010）68326294

销 售 二 部：（010）88379649

读者服务部：（010）68993821

网络服务

门户网：http://www.cmpbook.com

教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　言

在现代信息社会，随着信息化建设和 IT 技术的快速发展，计算机网络技术的应用更加广泛、深入，网络安全问题不断出现，致使网络安全管理的重要性更加突出。网络安全已经成为各国关注的焦点，它不仅关系到用户的信息和资产风险，而且也关系到国家安全和社会稳定，已成为热门研究和人才需求的新领域。只有在法律、管理、技术、道德各方面采取切实可行的有效措施，才能确保网络建设与应用又好又快地稳定发展。

网络安全已经成为 21 世纪世界十大热门课题之一，并成为社会关注的焦点。网络安全是一个系统工程，计算机网络安全管理已经成为网络管理的重要任务。网络安全管理涉及法规、政策、策略、规范、标准、机制、措施和管理技术等方面，是网络安全的重要保障。

网络安全管理（Network Security Management）通常是指以网络管理对象的安全为目标所进行的各种管理活动，是与安全有关的网络管理，简称安全管理。由于网络安全对网络信息系统的性能、管理及影响更复杂、更密切，致使网络安全管理逐渐成为网络管理技术中的一个重要分支，正受到业界及用户的广泛关注。网络安全管理是一种综合交叉学科，需要综合信息安全、网络管理、分布式计算、人工智能等多个领域知识和研究成果。其概念、理论和技术正在不断发展完善之中。

网络安全在企业管理机制下，借助技术手段得以实现。网络安全运作是指在日常工作中具体执行的网络安全管理和技术手段，是网络安全工作的关键，“七分管理，三分技术，运作贯穿始终”，管理是关键，技术是保障，可见网络安全管理的重要性。

信息、物资、能源已经成为人类社会赖以生存和发展的三大支柱及重要保障，信息技术的快速发展为人类社会带来了深刻的变革。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等的广泛应用，使计算机网络已经深入到国家的政治、经济、文化和国防建设等多个领域，遍布现代信息化社会的工作和生活的每个层面，“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，而且影响到国家的安全和主权。随着计算机网络的广泛应用，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，网络安全及管理已经成为世界关注的焦点。

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。

为满足高校信息、管理、计算机、电子商务及工程类高级人才培养的需要，我们编写了本书。本书作者在高校从事了多年计算机网络与安全等领域的教学、科研及学科专业管理工作，特别是多次主持过计算机网络安全方面的科研项目研究，积累了大量的宝贵实践经验，谨以此书奉献给广大师生。

本书内容共分 12 章，重点介绍了计算机网络安全管理及技术的基本知识及其应用，主要包括：计算机网络安全管理概论和网络安全面临的威胁、网络安全管理现状及发展趋势等；网络安全管理基础、网络协议安全、安全体系结构及 IPv6 安全性、安全服务与安全机制、虚拟专用网技术、无线局域网安全及常用网络安全管理命令等；网络综合安全管理包括网络安全管理保障体系、网络安全法律法规、网络安全评估准则和方法、安全管理规范和策略、安全管理的原则制度及规划、实体与软件安全管理；黑客攻击的防范与入侵检测、防范攻击的策略和措施；身份认证与访问控制、网络安全审计；密码与加密管理；数据库系统安全管理；病毒及恶意软件的防护；防火墙安全管理；操作系统与站点安全管理；电子商务安全管理及网络安全管理解决方案等。书中给出了很多实例和同步实验，以及多年的实践总结出来的案例及研究成果，以便于实际应用。目录中带“＊”的部分为选学内容。

本书旨在重点介绍最新网络安全管理、技术、成果、方法和实际应用，其特点是：

（1）内容先进，结构新颖。本书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，图文并茂、学以致用。

（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，提供了大量案例和实验，在内容安排上将理论知识与实际应用有机结合。

（3）资源配套，便于教学。为了方便师生教学，本书配有多媒体课件，并提供配套的同步实验指导、练习与实践习题及部分答案等，使用本书作教材授课的教师可以通过机械工业出版社网站下载课件及答案。

本书由清华大学薛一波研究员主审，贾铁军教授任主编、统稿并编写了第 1 章和第 3 章，嵩天（北京理工大学）任副主编并编写了第 2 章和第 5 章，常艳（辽宁警官学院）任副主编并编写了第 4 章和第 6 章，王雄（北京电子科技学院）编写了第 7 章和第 10 章，俞小怡（大连理工大学）编写了第 11 章，刘雪飞（北京信息科技大学）编写了第 12 章，苏庆刚（上海电机学院）编写了第 9 章，宋少婷（辽宁师范大学）编写了第 8 章并完成了部分课件制作，于淼参加了本书大纲的讨论、编写、审校等工作，邹佳芹多次对全书的文字、图表进行了校对、编排，并做了查阅资料等工作。

非常感谢教育部高校管理与工程类学科专业教学指导委员会和机械工业出版社，他们为本书的编写和出版提供了许多重要帮助、指导意见和参考资料。非常感谢清华大学信息技术

研究院薛一波研究员担任本书主审，他提出了很好的重要意见和建议。同时，非常感谢对本书编著过程中给予大力支持和帮助的各位同仁。对编著过程中参阅了大量的文献资料，难以完全准确注明，在此向这些文献的编著者表示诚挚的谢意！

由于内容庞杂、技术更新迅速、作者水平及时间有限，书中难免存在不妥之处，敬请海涵，并欢迎提出宝贵意见和建议。

编　者

2010 年 8 月

目　录

第1章 网络安全管理概论

随着社会信息化及计算机网络技术的快速发展和广泛应用，网络安全成为21世纪世界十大热门课题之一，世界各国对网络安全更加关注，网络安全管理的重要性更加突出。它不仅关系到用户资产和信息的风险，而且也关系到国家安全和社会稳定。

教学目标

- 掌握网络安全管理的概念、目标、任务及内容
- 了解网络面临的威胁及脆弱性问题
- 掌握网络安全管理技术概念、模型及规划
- 了解构建虚拟局域网（VLAN）的方法

1.1 网络安全管理概述

信息安全（Information Security）是指防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保信息的完整性、保密性、可用性和可控性。信息安全的发展经历了通信保密、信息安全（以保密性、完整性和可用性为目标）和信息保障三个阶段。

随着信息技术的快速发展与广泛应用，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、可控性和可审查性，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，综合利用了数学、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。

1.1.1 网络安全管理的概念及目标

1. 网络安全管理的概念

计算机网络安全（Computer Network Security，简称网络安全）是指利用计算机网络管理控制和技术措施，保证网络系统及数据的保密性、完整性、网络服务可用性和可审查性受到保护，即保证网络系统的硬件、软件及系统中的数据资源得到完整、准确、连续运行与服务不受干扰破坏和非授权使用。狭义上，网络安全是指计算机及其网络系统资源和信息资源不受有害因素的威胁和危害。广义上，凡是涉及计算机网络信息安全属性特征（保密性、完整性、可用性、可控性、可审查性）的相关技术和理论，都是网络安全的研究领域。实际上，网络的安全问题包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而网

络安全的最终目标和关键是保护网络的信息安全。

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、计算数学、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。

按照国际标准化组织（ISO）的定义，网络管理（Network Management）是规划、监督、组织和控制计算机网络通信服务，以及信息处理所必需的各种活动。狭义的网络管理主要是指对网络设备运行和网络通信量的管理。现在，网络管理已经突破了原有的概念和范畴，其目的是提供对计算机网络的规划、设计、操作、运行、管理、监视、分析、控制、评估和扩展的手段，从而合理地组织和利用系统资源，提供安全、可靠、有效和良好的服务。网络管理的实质是对各种网络资源进行监测、控制、协调、报告故障等。网络管理技术是重要的网络技术，“三分技术，七分管理”说明管理是关键，技术是保证。

网络安全管理（Network Security Management）通常是指以网络管理对象的安全为任务和目标所进行的各种管理活动，是与安全有关的网络管理，简称安全管理。由于网络安全对网络信息系统的性能、管理的关联及影响更复杂、更密切，网络安全管理逐渐成为网络管理中的一个重要分支，正受到业界及用户的广泛关注。网络安全管理是一个综合交叉学科，需要综合信息安全、网络管理、分布式计算、人工智能等多个领域知识和研究成果，其概念、理论和技术正在不断发展完善之中。

2. 网络安全管理的目标

计算机网络安全是一个相对性的概念，世上没有绝对的安全可言，过分提高安全性不仅浪费资源和代价，而且也会降低网络传输速度等方面的性能。

网络管理的目标是确保计算机网络的持续正常运行，使其能够有效、可靠、安全、经济地提供服务，并在计算机网络系统运行出现异常时及时响应并排除故障。

网络安全管理的目标是在计算机网络的信息传输、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、可用性、可控性和可审查性。其中保密性、完整性、可用性是信息安全的基本要求。以下的网络信息安全五大特征，反映了网络安全管理的具体目标要求。

（1）保密性

网络信息安全的保密性也称机密性，是指不将有用信息泄漏给非授权用户及过程，强调有用信息只被授权对象使用的特征。

（2）完整性

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，保持信息不被破坏或修改、不丢失的原样性特性，这是最基本的安全特征。

（3）可用性

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网络系统中的信息在一定传输范围和存放空间内可控程度。在网络系统中传输的信息及具体内容能够进行有效控制的特性，即除采用常规传播站点和内容监控形式外，采用加密等策略，并将其算法交第三方托管时，严格执行可控规程。