国家“十三五”重点出版规划项目获得者主编
上海市高等院校精品课程特色教材

高等院校信息技术规划教材

网络安全实用技术
（第2版）

贾铁军 主编

清华大学出版社

高等院校信息技术规划教材

网络安全实用技术

（第2版）

贾铁军 主编

俞小怡 罗宜元 侯丽波 副主编

常艳 宋少婷 参编

清华大学出版社

北京

内 容 简 介

本书全面介绍网络安全实用技术。全书共12章，主要内容包括网络安全的威胁及发展态势、网络协议安全及IPv6安全、安全体系结构与管理、无线网与WiFi安全、密码与加密技术、黑客攻防、身份认证与访问控制、入侵检测与防御、网络安全审计、计算机病毒防范、防火墙技术及应用、操作系统与站点安全、数据库安全技术、电子商务网站安全、网络安全解决方案及综合应用等，涵盖“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基本理论和实用技术，体现“教、学、练、做、用一体化”，突出“实用、特色、新颖、操作性”，力求技术先进、实用性强、资源丰富。

本书可作为高等院校计算机类、信息类、电子商务类、工程和管理类各专业的网络安全相关课程的教材，也可作为相关人员培训及自学参考用书。

图书在版编目(CIP)数据

网络安全实用技术/贾铁军主编. —2版. —北京：清华大学出版社，2016
高等院校信息技术规划教材
ISBN 978-7-302-43652-2

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(2016)第083602号

责任编辑：白立军　战晓雷
封面设计：常雪影
责任校对：李建庄
责任印制：刘海龙

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 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：24.75　　**字　　数**：615千字
版　　次：2011年8月第1版　2016年8月第2版　　**印　　次**：2016年8月第1次印刷
印　　数：1～2000
定　　价：49.00元

产品编号：068438-01

目录 contents

第1章 chapter 1

网络安全概述

网络安全问题已经成为世界各国关注的焦点，成为一项热门研究课题和人才需求的新领域。随着计算机网络技术的快速发展和广泛应用，网络资源共享和网络安全的矛盾不断加剧，网络安全的重要性和紧迫性更加突出，不仅关系到国家安全和社会稳定，也关系到信息化建设的健康发展、用户资产和信息资源的安全。

教学目标

- 掌握网络安全的概念、目标和内容。
- 理解网络安全面临的威胁及脆弱性。
- 掌握网络安全技术相关概念、种类和模型。
- 了解构建虚拟局域网 VLAN 的过程及方法。

1.1 网络安全的概念和内容

【案例 1-1】 我国网络遭受攻击近况。根据国家互联网应急中心(CNCERT)抽样监测结果和国家信息安全漏洞共享平台(CNVD)发布的一周(2016 年 1 月 4—10 日)数据，我国境内感染网络病毒的终端数约为 74.7 万个，较上周增长 31.6%，境内被篡改网站总数为 1143 个，被植入后门网站总数为 4569 个，新增信息安全漏洞 109 个。

1.1.1 网络安全的概念、目标和特征

1. 网络安全的有关概念

国际标准化组织(ISO)对于信息安全(information security)提出的定义是：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄漏。

我国在《计算机信息系统安全保护条例》中，定义信息安全为：计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统安全运行。主要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。

知识拓展 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3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。

网络安全(computer network security)是指利用网络管理控制和技术等措施，保证网络系统和数据的机密性、完整性、可用性、可控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(计算机或手机通信等)网络信息安全属性特征(机密性、完整性、可用性、可控性、可审查性)相关的理论和技术方法等，都是网络安全的研究领域。实际上，网络安全问题包括两方面的内容，一是网络系统的安全；二是网络信息(数据)的安全，而网络安全的最终目标和关键是保护网络信息的安全。

注意：实际上，网络安全是一个相对的概念，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。

知识拓展 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交叉学科，是计算机与信息科学的重要组成部分，也是近20年发展起来的新兴学科。需要综合信息安全、网络技术与管理、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. 网络安全的目标及特征

网络安全的目标是在网络的信息传输、存储与处理的整个过程中，提高物理上、逻辑上的防护、监控、反应恢复和对抗的能力。网络安全的最终目标就是通过各种技术与管理手段实现网络信息系统的机密性、完整性、可用性、可靠性、可控性和可审查性。其中保密性、完整性、可用性是网络安全的基本要求。以下的网络信息安全5大特征反映了网络安全的具体目标要求。

(1) 机密性(confidentiality)也称保密性，是不将有用信息泄漏给非授权用户的特性。可以通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段，主要强调有用信息只被授权对象使用的特征。

(2) 完整性(integrity)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、不丢失和信息未经授权不能改变的特性，也是最基本的安全特征。

(3) 可用性也称有效性(availability)，指信息资源可被授权实体按要求访问、正常使用或在非正常情况下能恢复使用的特性(系统面向用户服务的安全特性)，即在系统运行时能正确存取所需信息，当系统遭受意外攻击或破坏时，可以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。信息系统只有持续有效运行，授

权用户才能随时随地根据需求访问其提供的服务。

(4) 可控性(controllability)指信息系统对信息内容和传输具有控制能力的特性,指网络系统中的信息在一定传输范围和存放空间内可控的程度。可靠性(reliability)是指系统在指定的条件与时间内完成其功能的特性,是系统正常稳定运行的基本前提。

(5) 可审查性又称拒绝否认性(no-repudiation)、抗抵赖性或不可否认性,指网络通信双方在信息交互过程中,确信参与者本身和其所提供的信息的真实同一性,即所有参与者不可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 网络安全的内容及侧重点

从不同角度可以划分网络安全涉及的内容和不同的保护范畴及侧重点。

1. 网络安全涉及的内容

通常,网络安全的内容包括操作系统安全、数据库安全、网络站点安全、病毒与防护、访问控制、加密与鉴别等方面,具体内容将在以后章节中分别进行详细介绍。从层次结构上,也可将网络安全所涉及的内容概括为以下 5 个方面。

(1) 实体安全。也称物理安全,指保护网络设备、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破坏的措施及过程。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,包括环境安全、设备安全和媒体安全三个方面。具体参见 1.6 节的介绍。

(2) 运行安全。包括网络运行和访问控制的安全,如设置防火墙实现内外网隔离,备份系统实现系统恢复。运行安全包括内外网的隔离机制、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、系统升级和补丁处理、跟踪最新安全漏洞、灾难恢复机制与预防、安全审计、系统改造、网络安全咨询等。

(3) 系统安全。主要包括网络系统安全、操作系统安全和数据库系统安全。主要以网络系统的特点、条件和管理要求为依据,通过有针对性地为系统提供安全策略机制、保障措施、应急修复方法、安全建议和安全管理规范等,确保整个网络系统安全运行。

(4) 应用安全。由应用软件平台安全和应用数据安全两部分组成。应用安全包括业务应用软件的程序安全性测试分析、业务数据的安全检测与审计、数据资源访问控制验证测试、实体的身份鉴别检测、业务现场的备份与恢复机制检查、数据的唯一性/一致性/防冲突检测、数据的保密性测试、系统的可靠性测试和系统的可用性测试等。

(5) 管理安全。也称安全管理,主要指对人员及网络系统安全管理的各种法律、法规、政策、策略、机制、规范、标准、技术手段和措施等内容。主要包括法律法规管理、政策策略管理、规范标准管理、人员管理、应用系统管理、软件管理、设备管理、文档管理、数据管理、操作管理、运营管理、机房管理、安全培训管理等。

广义的网络安全所涉及的相关内容及其关系如图 1-1 所示。在网络信息安全法律法规的基础上,以安全管理为保障,以实体安全为基础,以系统安全、运行安全和应用安全

确保网络正常运行与服务。网络安全具体内容及其相互关系如图 1-2 所示。

图 1-1　网络安全的主要内容

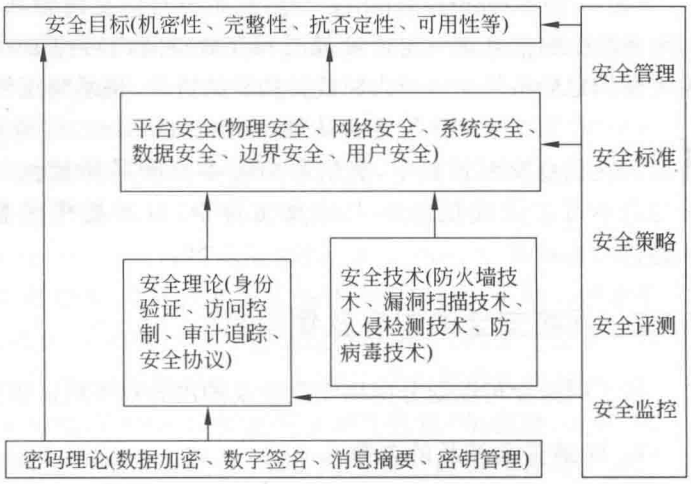

图 1-2　网络安全具体内容及其相互关系

知识拓展　国外从面向属性的网络信息安全框架角度将网络信息安全确定为“金三角”，即 3 个层次的结构：机密性、完整性和可用性。国内从面向应用的网络信息安全框架角度也可将网络信息安全分层结构从上至下分为内容安全、数据安全、运行安全和实体安全。国内也有一些专家或学者从不同的内涵和外延将网络信息安全分为 3 个层次：法律保障、安全管理和安全技术。国内一些专家也有将网络安全分成 4 个层次的安全：实体安全、逻辑安全、操作系统安全、联网安全。

2. 网络安全保护范畴及侧重点

网络安全与数据安全、计算机系统安全和密码安全密切相关，但涉及的保护范围不同。数据安全所涉及的保护范围包括所有数据资源；计算机系统安全的保护范围是系统硬件、软件、文件和数据，通过系统运行的实体环境限制、利用专用软件或操作系统来实现安全措施；密码安全是数据安全、网络安全和计算机系统安全的基础与核心，也是身份认证、访问控制、审查和防止信息失窃泄密的有效手段。

网络安全涉及的内容包括技术和管理等多个方面，需要相互补充，综合防范。技术方面主要侧重于如何防范外部非法攻击，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数据、提高网络系统的安全性已经成为必须解决的一个重要问题。

网络安全关键是确保网络系统中的信息资源安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和可审查性的理论、技术与管理都属于网络安全的研究范畴，对不同人员或部门，网络安全内容的侧重点有所不同。

(1) 网络安全研究人员比较关注从理论上采用数学等方法精确描述安全问题的属性特征，然后，通过安全模型等来解决具体的网络安全问题。

(2) 网络安全工程人员从实际应用角度出发，更注重成熟的网络安全解决方案和新