普通高等教育“十一五”
国家级规划教材

21世纪高等学校计算机
专业实用规划教材

计算机网络安全
（第3版）

◎ 刘远生　主编　　李民 张伟　副主编

清華大學出版社

21世纪高等学校计算机
专业实用规划教材

计算机网络安全
（第3版）

◎ 刘远生　主编　　李民 张伟　副主编

清华大学出版社
北京

内 容 简 介

本书系统地介绍了网络安全的基本知识、安全技术及其应用。重点介绍网络系统的安全运行和网络信息的安全保护与应用，内容包括网络操作系统安全、网络实体安全、网络数据库与数据安全、数据加密技术与应用、网络攻防技术、互联网安全、无线网络安全和典型的网络安全应用实例。

本书讲解了网络安全的原理和技术难点，理论知识和实际应用紧密结合，典型实例的应用性和可操作性强。各章末配有多种习题，便于教学和自学。本书内容安排合理，逻辑性较强，通俗易懂。

本书可作为高等院校信息安全、计算机、通信等专业的教材，也可作为网络管理人员、网络工程技术人员和信息安全管理人员及对网络安全感兴趣的读者的参考书。

图书在版编目(CIP)数据

计算机网络安全/刘远生主编. —3 版. —北京：清华大学出版社，2018
(21 世纪高等学校计算机专业实用规划教材)
ISBN 978-7-302-48609-1

Ⅰ. ①计… Ⅱ. ①刘… Ⅲ. ①计算机网络－网络安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 253677 号

责任编辑：付弘宇　张爱华
封面设计：刘　键
责任校对：时翠兰
责任印制：杨　艳

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：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20　　**字　　数**：490 千字
版　　次：2006 年 5 月第 1 版　2018 年 8 月第 3 版　　**印　　次**：2018 年 8 月第1 次印刷
印　　数：40001～41500
定　　价：49.80 元

产品编号：070716-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程（简称‘质量工程’）”，通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

本系列教材立足于计算机专业课程领域，以专业基础课为主、专业课为辅，横向满足高校多层次教学的需要。在规划过程中体现了如下一些基本原则和特点。

（1）反映计算机学科的最新发展，总结近年来计算机专业教学的最新成果。内容先进，充分吸收国外先进成果和理念。

（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，融合先进的教学思想、方法和手段，体现科学性、先进性和系统性，强调对学生实践能力的培养，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，保证质量。规划教材把重点放在公共基础课和专业基础课的教材建设上；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教学质量和教学改革成果的教材。

（4）主张一纲多本，合理配套。专业基础课和专业课教材配套，同一门课程有针对不同层次、面向不同应用的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，实现教材系列资源配套。

（5）依靠专家，择优选用。在制定教材规划时要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、评审确定主题。书稿完成后要认真实行审稿程序,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。建立一支高水平教材编写梯队才能保证教材的编写质量和建设力度,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世纪高等学校计算机专业实用规划教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

前　言

Internet 已成为全球规模最大、信息资源最丰富的计算机网络，利用它组成的企业内部专用网 Intranet 和企业间的外联网 Extranet，也已经得到广泛应用。随着以移动互联网、云计算、大数据、物联网、车联网等为代表的新型网络形态及网络服务的兴起和推广应用，网络技术的发展日新月异，但随之而来的信息安全问题也越来越突出。黑客、间谍的组织性更强、技术更加专业，犯罪动机也比以往任何时候都来得强烈，作案工具也更加强大，作案手段更是层出不穷。相比于以往偶发的数据泄露或黑客攻击事件，云计算和大数据时代的网络系统一旦受到黑客攻击就会造成大量有价值的数据信息泄露，对整个企业甚至整个行业而言都是毁灭性的打击。云端的大数据对于黑客来说是极具吸引力的获取信息的目标，因此现代网络的安全防护是至关重要的。如何使计算机网络系统不受破坏、提高系统的安全可靠性，已成为人们关注和亟须解决的问题。每个网络系统的管理人员、用户和工程技术人员都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全、稳定地运行并提供正常的安全服务。编写本书的目的就是帮助读者了解和掌握一定的网络安全知识、技术和实用技能，以便在工作中能正确、及时地采取措施保护网络环境的安全可靠。

本书自 2006 年 5 月第 1 版、2009 年 6 月第 2 版问世以来受到了广大读者的肯定和欢迎，已印刷十余次。由于计算机网络安全的相关技术更新和发展很快，为了使读者能全面、及时地了解和应用计算机网络安全技术，掌握网络安全的实践技能和实际应用，应出版社的要求，编者在向部分使用本教材的院校进行书面调研和直接与一些有着丰富教学经验的教师讨论之后，确定了对本书第 2 版进行修订的大纲，由几位有实践经验的教师参与编写，形成了本书的再次修订版——第 3 版。

本次修订的基本思想是按照我国高等教育对应用型人才的培养目标和要求，在理论知识够用的基础上，增加实际应用的内容，使之更能体现对应用型人才注重实践、实际应用和技能的培养要求。本次修订主要做了如下工作。

(1) 减少了计算机网络理论部分的内容和难度，删除了过时的内容，简化了使用不多的部分内容。

(2) 对部分章节内容进行了合并，压缩了篇幅(如原防火墙的内容并入“网络攻防技术”一章)。

(3) 增加了一些新知识、新技术，对原版本中所涉及的软件工具内容进行了升级，重点增加了一些实用的网络安全新技术和软件的应用实践内容(如增加了“无线网络安全”和“网络安全实践”相关内容)。

本次修订中增加的“网络安全实践”一章，包括新增加的网络安全应用实例以及对原有网络安全应用实践进行升级的内容。这些应用实例的实用性和可操作性都较强。该章既可

作为与前面各章内容相对应的“实验指导书”,也可单独作为掌握一定网络安全基础知识的读者的网络安全实践教材或参考书。通过学习和实践这些相关实例,读者可以了解和掌握网络安全工具(软件)的应用和操作技能。

修订后全书共9章,内容包括网络安全概述、网络操作系统安全、网络实体安全、网络数据库与数据安全、数据加密技术与应用、网络攻防技术、互联网安全、无线网络安全和网络安全实践。

本书内容安排合理,逻辑性强,重点突出,通俗易懂。本书可作为高等院校信息安全、计算机、通信等专业的教材,也可作为网络管理人员、网络工程技术人员和信息安全管理人员及对网络安全感兴趣的读者的参考书。本书涉及的内容比较广泛,读者在学习和参考时,可在内容、重点和深度上酌情取舍。

本书由刘远生任主编,李民、张伟任副主编。刘远生编写了第1和第5章,李民编写了第3和第8章,张伟编写了第9章,韩长军编写了第2章,李荣霞编写了第4章,龙海燕编写了第6和第7章,全书由刘远生统阅定稿。

本书的修订编写得到了清华大学出版社的大力支持,在此表示衷心的感谢。

网络安全内容庞杂,技术发展迅速,由于编者水平有限,加之时间仓促,书中难免存在不当之处,殷切希望各位读者提出宝贵意见,恳请各位专家、学者给予批评指正。

本书的部分习题答案可以从清华大学出版社网站 www.tup.com.cn 下载。关于资源下载和本书使用中的问题,可以发邮件到邮箱 fuhy@tup.tsinghua.edu.cn。

编　者

2018年3月

目　录

第1章 网络安全概述

本章要点

- 网络安全的概念、特征和安全目标；
- 网络的安全的威胁和风险；
- 网络安全体系结构；
- 网络安全的策略和技术；
- 网络安全的评价准则；
- 网络系统安全的日常管理。

随着计算机网络技术的迅速发展和普及应用，人类已进入网络化、信息化和数字化时代，计算机网络技术的发展与应用已成为影响一个国家或地区政治、经济、军事、科学与文化发展的重要因素之一，也是影响人们日常生活的重要因素。但由于计算机网络具有开放性和互联性等特征，因此极易受到异常因素的影响，如网络受到黑客和病毒的攻击和入侵，使网络系统遭到破坏，导致信息的泄露或丢失。因此，如何有效地保证网络系统安全，已成为人们非常关注的问题。

本章主要介绍网络安全的概念、网络安全的威胁与风险管理、网络安全体系结构、网络安全策略与技术、网络安全级别和网络系统安全的日常管理等内容。

1.1 网络安全概论

网络安全是一门涉及领域相当广泛的学科，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。凡是涉及网络上信息的机密性、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的研究范围。

1.1.1 网络安全的概念

网络安全本质上就是网络上的信息系统安全。网络安全包括系统安全运行和系统信息安全保护两方面。信息系统的安全运行是信息系统提供有效服务(即可用性)的前提，信息的安全保护主要是确保数据信息的机密性和完整性。

从不同的角度来看，网络安全又具有不同的含义。

从用户(个人、企业等)的角度来讲，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改或抵赖等手段对用户的利益和隐私造成损害，同时也希望当信息保存在某个网络系统中时，不受其

他非法用户的非授权访问和破坏。

从网络运行和网络管理者的角度来讲,他们希望对本地网络信息的访问操作能够得到保护和控制,避免遭受病毒、非法存取、拒绝服务或网络资源的非法占用及非法控制等威胁,制止和防御网络黑客的攻击。

对安全保密部门来讲,他们希望对非法的、有害的或涉及国家或地区机密的信息进行过滤和防护,防止其通过网络泄露,避免由于这类信息的泄露对社会产生危害,给国家造成巨大的经济损失,甚至威胁到国家安全。

从社会教育和意识形态角度来讲,网络上不健康的内容会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

由此可见,网络安全在不同的环境和具体的应用中可以有不同的解释。

1.1.2 网络安全目标

网络安全的目标主要表现在系统的可用性、可靠性、机密性、完整性、不可抵赖性及可控性等方面。

1. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。网络最基本的功能就是为用户提供信息和通信服务,而用户对信息和通信的需求是随机的(内容的随机性和时间的随机性)、多方面的(文字、语音、图像等),有的用户还对服务的实时性有较高的要求。网络必须能保证所有用户的通信需要,一个授权用户无论何时提出要求,网络都必须是可用的,不能拒绝用户的要求。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。对于此类攻击,一方面要采取物理加固技术,保障物理设备安全、可靠地工作;另一方面要通过访问控制机制,阻止非法用户进入网络。

2. 可靠性

可靠性是指网络信息系统能够在规定条件下和规定时间内,实现规定功能的特性。可靠性是网络安全最基本的要求之一,是所有网络信息系统建设和运行的目标。目前,对于网络可靠性的研究偏重于硬件方面,主要采用硬件冗余、提高可靠性和精确度等方法。实际上,软件的可靠性、人员的可靠性和环境的可靠性在保证系统可靠性方面也是非常重要的。

3. 机密性

机密性是网络信息不被泄露给非授权用户和实体,或供其利用的特性。这些信息不仅指国家或地区的机密,也包括企业和社会团体的商业和工作秘密,还包括个人的秘密(如银行账号)和个人隐私等。机密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现,它是在可用性和可靠性的基础上,保障网络信息安全的重要手段。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性。网络信息在存储或传输的过程中应保证不被偶然或蓄意地篡改或伪造,确保授权用户得到的信息是真实的。如果信息被未经授权的实体修改了或在传输的过程中出现错误,信息的使用者应能够通过一定的方式判断出信息是否真实可靠。

5. 不可抵赖性

不可抵赖性也称可审查性,是指通信双方在通信过程中,对自己所发送或接收的消息不

可抵赖，即发送者不能否认其发送过消息的事实和消息的内容，接收者也不能否认其接收到消息的事实和内容。

6. 可控性

可控性是对网络信息的内容及其传播具有控制能力的特性。保障系统依据授权提供服务，使系统在任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

1.2 网络安全面临的威胁与风险

网络的开放性和共享性在方便人们使用的同时，也使得网络系统容易受到黑客攻击。网络的安全威胁是指对网络系统的网络服务、网络信息的机密性和可用性产生不利影响的各种因素。网络威胁也包括缓冲区溢出、假冒用户、电子欺骗等安全漏洞。

1.2.1 网络安全漏洞

目前，没有安全漏洞的计算机网络几乎是不存在的。而正是因为这些漏洞才使得攻击能够成功，从而引起了攻击者的兴趣。安全漏洞是网络被攻击的客观原因，它与许多技术因素有关。

1. 漏洞的概念

从广义上讲，漏洞是在硬件、软件、协议的具体实现或系统安全策略以及人为因素上存在的缺陷，从而可以使攻击者能够在未经系统合法用户授权的情况下访问或破坏系统。全世界的路由器、服务器和客户端软件、操作系统和防火墙等每时每刻都会有很多漏洞出现，它们会影响到很大范围内的网络安全。

漏洞是由于系统设计人员、制造人员、检测人员或管理人员的疏忽或过失而隐藏在系统中的。发现漏洞的人主要包括计算机专家、黑客、安全服务商、安全组织、系统管理员和个人用户等。当发现漏洞时，计算机专家和安全服务商组织通常会向安全组织机构发出警告。黑客发现新漏洞后会采用新的攻击方法进行网络攻击，新的攻击方法意味着新漏洞的发现，因此黑客是通过网络攻击活动间接发布漏洞信息的。

1988 年美国的莫里斯蠕虫事件，导致上千台计算机崩溃，造成了巨大的损失，使人们认识到网络安全状况的脆弱性和突发性，以及对网络安全事件进行紧急响应的重要性。在美国国防部资助下，卡内基梅隆大学软件工程研究中心成立了世界上第一个计算机紧急响应小组(Computer Emergency Response Team，CERT)。这些年来，CERT 在反击大规模的网络入侵方面起到了重要作用。CERT 是著名的信息安全组织，专门处理计算机网络安全问题。CERT 主要提供针对新的安全漏洞发布建议，24 小时全天候为遭受破坏的用户提供重要技术意见，利用它的 Web 站点提供有用的安全信息等服务。

2. 漏洞类型

根据漏洞的载体(网络实体)类型，漏洞主要分为操作系统漏洞、网络协议漏洞、数据库漏洞和网络服务漏洞等。

1) 操作系统漏洞

任何操作系统都可能存在漏洞，这些漏洞产生的原因很多，主要有以下几种。

(1) 操作系统陷门。一些操作系统为了安装其他公司的软件包而保留了一种特殊的管理程序功能,尽管此功能的调用需要以特权方式进行,但如果未受到严密的监控和必要的认证限制,就有可能形成操作系统陷门。

(2) 输入输出的非法访问。有些操作系统一旦输入/输出(I/O)操作被检查通过后,该操作系统就会继续执行下去而不再检查,从而造成后续操作的非法访问。还有些操作系统使用公共系统缓冲区,任何用户都可以搜索该缓冲区,如果该缓冲区没有严格的安全措施,那么其中的机密信息(如用户的认证数据、口令等)就有可能被泄露。

(3) 访问控制的混乱。在操作系统中,安全访问强调隔离和保护措施,而资源共享要求开放。如果在设计操作系统时不能处理好这二者之间的矛盾关系,就可能出现安全问题。

(4) 不完全的中介。完全的中介必须检查每次的访问请求以进行适当的审批,而某些操作系统却省略了必要的安全保护。要建立安全的操作系统,必须构造操作系统的安全模型和不同的实施方法。另外,还需要建立和完善操作系统的评估标准、评价方法和测试质量。

2) 网络协议漏洞

TCP/IP 的目标是保证通信和传输。TCP/IP 没有内在的控制机制支持源地址的鉴别,这是 TCP/IP 存在漏洞的根本原因。黑客就会利用 TCP/IP 的漏洞,使用侦听方法来获取数据,对数据进行检查、推测 TCP 的序列号、修改传输路由、修改鉴别过程、插入黑客指令等。

3) 数据库漏洞

数据库管理系统(DBMS)作为操作系统的应用程序,其库文件可以被看作操作系统上的一个客体,其应用进程又是操作系统的主体。因此,数据库的安全是以操作系统的安全为基础的,没有操作系统的安全,就谈不上数据库的安全。但是,并不是有了安全的操作系统,就能绝对保证数据库的安全。由于对数据库的管理是建立在分级管理的概念上的,所以其安全性不是绝对的。

4) 网络服务漏洞

(1) 匿名 FTP。匿名 FTP 是人们常用的一种 FTP 服务方式。多数 FTP 服务器可以用 Anonymous 用户名登录,这样就存在用户破坏系统和文件的可能性。另外,上传的软件可能具有破坏性,大量上传的文件还会耗费磁盘空间。建立匿名服务器时,应当确保用户不能访问系统的重要部分,尤其是包含系统配置信息的文件目录。如果没必要使用匿名登录,应将其关闭,并定时检查服务器日志。

(2) 电子邮件。电子邮件服务器本身就存在安全漏洞,一旦漏洞被黑客利用就可能对网络造成巨大的威胁。如 UNIX/Linux 系统的邮件服务器 Sendmail 是以 root 账号运行的,如果黑客掌握了这个漏洞就可以利用它来攻击系统。曾经就有蠕虫病毒利用 Sendmail 的安全缺陷使大批的网络服务器陷于瘫痪的案例。

(3) 域名服务(DNS)。DNS 需要用户提供用户机器的硬件和软件信息。黑客经常把它作为一种攻击目标。假冒的 DNS 服务器可能会提供一些错误的信息甚至错误的域名解析,这样就造成了 DNS 欺骗。

(4) Web 服务。Web 服务器本身存在一些漏洞,如 IIS(运行于 Windows 下)和 Apache(运行于 UNIX 下)本身的漏洞,使得黑客能入侵到主机系统,破坏一些重要数据,甚至造成

系统瘫痪。另外，程序员在编写 CGI 程序时会留下一些 bug，从而为网络攻击者创造了条件。

3. 典型的网络结构及安全漏洞

典型的网络结构及安全漏洞如图 1.2.1 所示，这些安全漏洞及其原因有：

(1) 不充分的路由器访问控制。配置不当的路由器 ACL 会使 ICMP、IP 和 NetBIOS 信息泄露，从而导致对目标网点 DMZ 上服务器所提供的服务进行未授权的访问。

(2) 未实施安全措施且无人监管的远程访问网点，容易成为攻击者进入网络的入口。

(3) 操作系统和应用程序版本、用户或用户组、共享资源、DNS 信息以及运行中的服务(如 SNMP)等信息不经意地泄露给攻击者。

(4) 运行非必要服务(如 FTP 等)的主机提供了进入内部网络的通路。

(5) 客户机上级别低的、易于被猜中或重用的口令使服务器易被入侵。

(6) 具有太多特权的用户账号或测试账号。

(7) 配置不当的 Internet 服务器，特别是 Web 服务器上 CGI 脚本和匿名 FTP。

(8) 配置不当的防火墙或路由器允许直接侵入某个服务器后访问内部系统。

(9) 没有打过补丁的、过时的、脆弱的或遗留在默认配置状态的软件。

(10) 过度的文件和目录访问控制。

(11) 过度的信任关系将给攻击者提供未授权访问敏感信息的机会。

(12) 不加认证的服务。

(13) 没有采纳公认的安全策略、规程、指导和最低基线标准。

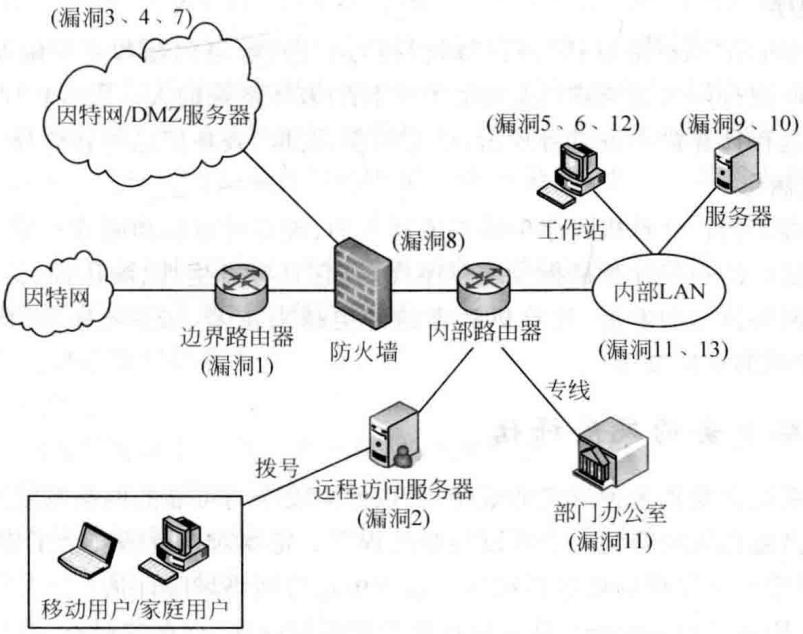

图 1.2.1 典型的计算机网络结构及安全漏洞

1.2.2 网络安全的威胁

网络安全的威胁来自于网络中存在的不安全因素。网络不安全因素有两方面：一方面是网络本身的不可靠性和脆弱性；另一方面是人为破坏，这也是网络安全的最大威胁。网