21世纪高等学校规划教材 | 计算机科学与技术

网络安全技术与应用实践

刘远生 主编
辛一 李民 副主编

清华大学出版社

网络安全技术与应用实践

刘远生 主编
辛一 李民 副主编

清华大学出版社
北京

内 容 简 介

本书从网络系统安全管理和应用的角度出发，重点介绍网络安全技术及其应用，各章在介绍网络安全技术后均配以相应的实践内容或应用实例，体现培养读者网络安全及管理技术的应用能力和实践操作技能的特色。

本书对原理、技术难点的介绍适度，将理论知识和实际应用紧密地结合在一起，典型实例的应用性和可操作性强；章末配有习题和思考题，便于学生学习和实践，内容安排合理，重点突出，文字简明，语言通俗易懂。

本书可作为普通高校计算机、通信、信息安全等专业的应用型本科、高职高专或成人教育学生的网络安全实践教材，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读者的参考书。

图书在版编目(CIP)数据

网络安全技术与应用实践/刘远生主编. —北京：清华大学出版社，2010.9
(21世纪高等学校规划教材·计算机科学与技术)
ISBN 978-7-302-22619-2

Ⅰ. ①网…　Ⅱ. ①刘…　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081858号

责任编辑：付弘宇　李玮琪
责任校对：白　蕾
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：20.5　**字　数**：498千字
版　　次：2010年9月第1版　　**印　　次**：2010年9月第1次印刷
印　　数：1～4000
定　　价：29.80元

产品编号：027865-01

编审委员会成员

（按地区排序）

清华大学	周立柱　教授
	覃　征　教授
	王建民　教授
	冯建华　教授
	刘　强　副教授
北京大学	杨冬青　教授
	陈　钟　教授
	陈立军　副教授
北京航空航天大学	马殿富　教授
	吴超英　副教授
	姚淑珍　教授
中国人民大学	王　珊　教授
	孟小峰　教授
	陈　红　教授
北京师范大学	周明全　教授
北京交通大学	阮秋琦　教授
	赵　宏　教授
北京信息工程学院	孟庆昌　教授
北京科技大学	杨炳儒　教授
石油大学	陈　明　教授
天津大学	艾德才　教授
复旦大学	吴立德　教授
	吴百锋　教授
	杨卫东　副教授
同济大学	苗夺谦　教授
	徐　安　教授
华东理工大学	邵志清　教授
华东师范大学	杨宗源　教授
	应吉康　教授
上海大学	陆　铭　副教授
东华大学	乐嘉锦　教授
	孙　莉　副教授

浙江大学	吴朝晖 教授
	李善平 教授
扬州大学	李 云 教授
南京大学	骆 斌 教授
	黄 强 副教授
南京航空航天大学	黄志球 教授
	秦小麟 教授
南京理工大学	张功萱 教授
南京邮电学院	朱秀昌 教授
苏州大学	王宜怀 教授
	陈建明 副教授
江苏大学	鲍可进 教授
武汉大学	何炎祥 教授
华中科技大学	刘乐善 教授
中南财经政法大学	刘腾红 教授
华中师范大学	叶俊民 教授
	郑世珏 教授
	陈 利 教授
江汉大学	颜 彬 教授
国防科技大学	赵克佳 教授
中南大学	刘卫国 教授
湖南大学	林亚平 教授
	邹北骥 教授
西安交通大学	沈钧毅 教授
	齐 勇 教授
长安大学	巨永峰 教授
哈尔滨工业大学	郭茂祖 教授
吉林大学	徐一平 教授
	毕 强 教授
山东大学	孟祥旭 教授
	郝兴伟 教授
中山大学	潘小轰 教授
厦门大学	冯少荣 教授
仰恩大学	张思民 教授
云南大学	刘惟一 教授
电子科技大学	刘乃琦 教授
	罗 蕾 教授
成都理工大学	蔡 淮 教授
	于 春 讲师
西南交通大学	曾华燊 教授

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。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前，针对计算机类和电子信息类相关专业成立了两个“编委会”，即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括：

(1) 21 世纪高等学校规划教材·计算机应用——高等学校各类专业，特别是非计算机专业的计算机应用类教材。

(2) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与计算机应用。

(7) 21 世纪高等学校规划教材·电子商务。

清华大学出版社经过二十多年的努力，在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌，为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格，这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人：魏江江

E-mail：weijj@tup. tsinghua. edu. cn

前言

随着 Internet 的发展和计算机网络的普及应用，人们的学习、工作和生活方式有了极大的改变。在计算机网络为人们带来方便的同时，网络系统的安全问题也变得日益突出和复杂。解决网络安全问题更多地涉及网络安全技术、网络系统管理和实际应用。每一位相关专业的学生、网络机构的管理人员、工程技术人员，乃至普通网络用户都应该掌握一定的计算机网络安全知识和技术，以使自己的信息系统能够安全、稳定地运行，并提供正常的服务。当然，解决网络系统的安全问题是一个系统工程，它不仅涉及技术问题，还涉及管理、法律和道德，是一个社会问题。

目前关于网络安全的教材和参考书已很多，但一般都是理论知识和技术原理介绍得较多较深，网络安全的实际案例、软件工具应用和实际操作技能介绍得较少，比较适合于研究型大学的本科生或研究生使用。而对于应用型本科和高职、大专学生而言，在了解简单的网络安全知识和技术原理的基础上，应重点掌握和熟练运用相关的网络安全技术和实际解决方案。

本书在介绍网络安全基本知识的基础上，重点介绍了网络安全技术及其应用。在内容上除第 1 章简单介绍有关网络安全的概念、安全策略和安全管理知识外，此后各章在介绍的相关网络安全技术后均配以相应的实践内容或应用实例，旨在培养学生的实际动手能力和解决问题的操作技能。

本书从网络系统安全管理和应用的角度出发，强调理论联系实际，体现培养学生的网络管理、安全技术应用能力和实践操作技能的特色。全书共有 9 章，内容包括网络安全概述、网络设备的安全与应用实践、网络操作系统安全与管理实践、数据加密技术与应用实践、软件安全技术与应用实践、网络攻防技术与应用实践、VPN 安全技术与应用实践、无线网络的安全与应用实践和电子邮件安全与应用实践等。

本书对网络安全的理论和技术原理等介绍适度，典型实例的应用性和可操作性强，章末配有习题和思考题，便于学生学习和实践。本书可作为普通高校计算机专业、通信专业及相关专业的本科生、大专生教材，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以及对网络安全感兴趣读者的参考书。

本书由刘远生任主编，辛一、李民任副主编，参加编写的还有薛庆水、张明辉、丛晓红、刘芊麟、刘野等，全书由刘远生统阅定稿。在本书的编写过程中得到了清华大学出版社编辑的大力支持和帮助，在此表示衷心的感谢。

由于编者水平有限，书中难免存在缺点和不足之处，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。编者也希望与各位读者多多交流，联系邮箱为 ysliu@sjtu.edu.cn。

本书的配套课件等资料可以从清华大学出版社网站(http://www.tup.tsinghua.edu.cn)下载，相关问题联系 fuhy@tup.tsinghua.edu.cn。

编者

2010 年 4 月

于上海交通大学

目 录

第1章 网络安全概述

计算机网络技术是由现代通信技术和计算机技术的高速发展、密切结合而产生和发展起来的，是20世纪最伟大的科学技术成就之一。计算机网络的发展速度又超过了世界上任何一种其他科学技术的发展速度。计算机技术与通信技术的结合使计算机的应用范围得到了极大的开拓。

计算机网络的发展，特别是Internet的发展和普及应用，为人类带来了新的工作、学习和生活方式，计算机网络和人们的工作与生活的联系也越来越密切。计算机网络系统提供了丰富的资源以便用户共享，提高了系统的灵活性和便捷性。通过网络，人们可以与远在天涯的朋友互发函件，可以足不出户地浏览世界各地的报纸杂志，搜索自己所需的信息，可以在家里与世界各个角落的陌生人打牌下棋……但与此同时，人们也发现自己的计算机信息系统不断受到侵害，其形式多样化，技术先进且复杂化，令人防不胜防。

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。每个网络机构的管理人员、网络系统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。

1.1 网络安全概论

计算机网络系统的安全问题变得日益突出和复杂。一方面，计算机网络系统提供了丰富的资源以便用户共享；另一方面，也增加了网络系统的脆弱性和网络安全的复杂性，资源共享增加了网络受威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全的问题也日益突出。因此，为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必须解决的问题。每个计算机用户也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。

1.1.1 网络安全的概念

1. 网络安全的含义

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息论、应用数学、信息安全技术等多种学科的综合性学科。网络安全是指利用各种网络管理、控制和技术措施，使网络系统的硬件、软件及其系统中的数据资源受到保护，不因一些不利因素影响而使这些资源遭到破坏、更改、泄露，保证网络系统连续、可靠、安全地运行。

计算机网络安全归根到底就是：确保计算机网络环境下信息系统的安全运行和在信息系统中存储、处理和传输的信息受到安全保护，这就是通常所说的保证网络系统运行的可靠性，确保信息的保密性、完整性、可用性和真实性。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、可控性和真实性的相关技术和理论都是网络安全的研究领域。

由于现代的数据处理系统都是建立在计算机网络基础上的，计算机网络安全也就是信息系统安全。网络安全同样也包括系统安全运行和系统信息安全保护两方面，即网络安全是对信息系统的安全运行（系统的可靠性）和运行在信息系统中的信息进行安全保护（包括信息的保密性、完整性和可用性保护）的统称。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保密性和完整性。

2. 网络安全的特征

由上述可知，网络安全的主要特征就是保证网络安全的主要目标，即保证系统的可靠性、软件及数据的完整性。

（1）网络系统的可靠性（reliability）是系统正常运行的特性，即指保证网络系统不因各种因素的影响而中断正常工作。

（2）信息的完整性（integrity）是信息未经授权不能进行改变的特性。一方面是指在系统中存储和传输的信息不被非法操作，即保证信息不被插入、更改、替换和删除，数据分组不丢失、乱序，数据库或系统中的数据不被破坏；另一方面是指信息处理方法的正确性，因为不当的操作可能使数据文件丢失。

（3）信息的可用性（availability）是可被授权实体访问并按需求使用的特性，即指信息和相关的信息资产在授权人需要时可以立即获得，在保证信息完整性的同时，能使这些信息被正常地利用和操作。

（4）信息的保密性（confidentiality）是信息不泄露给非授权用户、实体或过程的特性。利用密码技术对数据进行加密处理后，即可保证信息仅仅为那些被授权使用的人得到，而不被非授权人识别。

1.1.2 网络安全需求与安全目标

网络安全是一个系统的概念，有效的安全策略的制定是网络信息安全的首要目标。通过对网络结构、网络安全的风险分析，对于不同的安全风险可以采用不同的安全措施加以解决，使网络安全达到一定的安全目标。

1. 安全需求

（1）物理安全需求

针对重要信息可能通过电磁辐射或线路干扰等泄露的问题，需要对存放机密信息的机房进行必要的干扰和屏蔽设计。采用辐射干扰机，防止电磁辐射泄露机密信息；通过对其他重要设备进行备份，对重要系统进行备份等进行安全保护。

(2) 访问控制需求

访问控制包括防范非法用户对网络的非法访问、防范合法用户对网络资源的非授权访问和防范假冒合法用户对网络的非法访问。非法用户对网络的访问多为黑客或间谍的攻击行为；合法用户的非授权访问是指合法用户在没有得到许可的情况下访问了他本不该访问的资源；假冒合法用户对网络的非法访问是指非网络用户假冒网络用户的 IP 地址或用户名等资源对网络进行的访问。

(3) 加密设备需求

加密传输是保护网络信息安全的重要手段之一。信息的泄露很大程度上都是因为在链路上被搭线窃取的，数据也可能因为在链路上被截获、篡改后传输给对方，使其真实性、完整性得不到保证。如果利用加密设备对传输的数据进行加密，使得在网上传输的数据以密文形式出现，则即使这些信息在传输过程中被截获，入侵者也读不懂，而且加密机还能通过先进的技术手段对数据传输过程中的完整性、真实性进行鉴别。可以保证数据的保密性、完整性及可靠性。因此，必须配备加密设备对数据进行传输加密。

(4) 入侵检测系统需求

防火墙是实现网络安全最基本、最经济、最有效的措施之一，它可对通过它的所有访问进行严格控制(允许、禁止、报警)。若以为网络配了防火墙就安全了的想法是错误的。因为网络安全是整体的、动态的，不是单一产品能够完全实现的。防火墙不可能完全防止所有的攻击，特别是新的攻击，也不能阻止那些绕过它的攻击。所以确保网络更加安全必须配备入侵检测系统，应对透过防火墙的攻击进行检测并做相应反应(记录、报警、阻断)。

(5) 安全风险评估系统需求

网络系统存在安全漏洞和操作系统漏洞，这是黑客等入侵者攻击屡屡得手的重要原因。入侵者通常是通过一些程序来探测网络系统中存在的安全漏洞，然后对这些漏洞采取相应的技术进行攻击。因此，必须配备网络安全扫描系统检测网络中存在的安全漏洞，采用相应的措施填补系统漏洞，并对网络设备等存在的不安全配置重新进行安全配置。

(6) 防病毒系统需求

针对网络病毒危害性大且传播迅速的特点，必须配备从单机到服务器的整套防病毒软件，实现全网的病毒安全防护。

2. 安全目标

基于以上的需求分析，网络系统可以实现以下安全目标。

- 保护网络系统中存储和传输信息的保密性和完整性。
- 保护网络系统的可用性。
- 保护网络系统服务的可靠性。
- 保证网络资源访问的可控性(防范非法访问及非授权访问)。
- 防范入侵者的恶意攻击与破坏。
- 防范病毒的侵害。
- 保证网络系统的灾难恢复能力。
- 实现网络的安全管理。

1.2 网络的不安全因素

影响网络系统安全的因素很多，但不外乎来自网络系统外部的威胁、破坏和来自系统内部的缺陷（脆弱性）。下面就网络系统的脆弱性和网络系统受到的主要威胁进行探讨。

1.2.1 网络系统的漏洞

计算机网络本身存在一些固有的弱点（脆弱性），非授权用户利用这些脆弱性可对网络系统进行非法访问，这种非法访问会使系统内数据的完整性受到威胁，也可能使信息遭到破坏而不能继续使用，更为严重的是有价值的信息被窃取而不留任何痕迹。

网络系统的脆弱性主要表现为以下几方面。

1. 操作系统的脆弱性

网络操作系统体系结构本身就是不安全的，具体表现如下。

（1）动态连接

为了系统集成和系统扩充的需要，操作系统采用动态连接结构，系统的服务和 I/O 操作都可以补丁方式进行升级和动态连接。这种方式虽然为厂商和用户提供了方便，但同时也为黑客提供了入侵的方便（漏洞），这种动态连接也是计算机病毒产生的温床。

（2）创建进程

操作系统可以创建进程，而且这些进程可在远程节点上被创建与激活，更加严重的是被创建的进程又可以继续创建其他进程。这样，若黑客在远程将“间谍”程序以补丁方式附在合法用户，特别是超级用户上，就能摆脱系统进程与作业监视程序的检测。

（3）空口令和 RPC

操作系统为维护方便而预留的无口令入口和提供的远程过程调用（RPC）服务都是黑客进入系统的通道。

（4）超级用户

操作系统的另一个安全漏洞就是存在超级用户，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者。

2. 计算机系统本身的脆弱性

计算机系统的硬件和软件故障可影响系统的正常运行，严重时系统会停止工作。系统的硬件故障通常有硬盘故障、电源故障、芯片主板故障、驱动器故障等；系统的软件故障通常有操作系统故障、应用软件故障和驱动程序故障等。

3. 电磁泄露

计算机网络中的网络端口、传输线路和各种处理机都有可能因屏蔽不严或未屏蔽而造成电磁信息辐射，从而造成有用信息甚至机密信息泄露。