可下载教学资料
http://www.tup.tsinghua.edu.cn

21世纪高等学校计算机专业实用规划教材

计算机网络安全技术

王　群　编著

清华大学出版社

21世纪高等学校计算机

计算机网络安全技术

王　群　编著

清华大学出版社
北京

内 容 简 介

本书是一本面向普通高等院校本科教学要求的教材，是理论与实践有机结合的研究成果，也是作者长期从事计算机网络教学、网络安全设计、网络管理与维护的经验总结。为了使内容安排符合教学要求，并尽可能地贴近实际应用，解决实际问题，本书在内容选择上既注重基本理论和概念的讲述，又紧紧抓住目前网络安全领域的关键技术和用户普遍关注的热点问题，对内容进行了合理规划。

本书共分 9 章，主要内容包括计算机网络安全概述、数据加密技术及应用、PKI/PMI 技术及应用、身份认证技术、TCP/IP 体系的协议安全、计算机病毒、木马和间谍软件与防治、网络攻击与防范、防火墙技术及应用、VPN 技术及应用等。

本书主要针对普通高等院校计算机及相关专业本科层次的教学要求而编写，其中大量的实训内容可供高职高专和有关培训机构使用，本书也可供从事网络安全设计和管理的技术人员阅读、参考。

图书在版编目(CIP)数据

计算机网络安全技术/王群编著. —北京：清华大学出版社，2008.8
(21 世纪高等学校计算机专业实用规划教材)
ISBN 978-7-302-17778-4

Ⅰ. 计…　Ⅱ. 王…　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(2008)第 078420 号

责任编辑：魏江江　薛　阳
责任校对：焦丽丽
责任印制：何　芊
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：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：19.25　**字　数**：469 千字
版　　次：2008 年 8 月第 1 版　　**印　　次**：2008 年 8 月第1 次印刷
印　　数：1～4000
定　　价：29.00 元

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

如今，计算机网络的应用已延伸到全球的各个角落和领域，正在对人们的工作、生活产生前所未有的影响，如同电力、交通一样日益成为人们生活中不可缺少的组成部分。与此同时，随着网络规模的不断扩大，以及人们对网络知识的了解越来越深入，网络中的攻击等不安全因素越来越多，已经严重威胁到网络与信息的安全。计算机网络的安全已经成为一个备受全球关注的问题。

计算机网络与信息安全技术的核心问题是对计算机和网络系统进行有效的防护。网络安全防护涉及的面非常广，从技术层面上分，主要包括数据加密、身份认证、入侵检测、入侵保护、病毒防护和虚拟专用网等方面，这些技术中有些是主动防御，有些是被动保护，有些则是为安全研究提供支撑和平台。本书在写作过程中强调了以下几点。

一是尽可能用通俗易懂的语言来描述晦涩的理论阐述。在计算机网络安全这门课程中涉及到了大量的概念、理论体系、算法和协议，如何用通俗易懂的语言来描述这些抽象的专业术语是本书的一个侧重点。为此，在写作过程中作者尽可能用简捷明快的语言来阐述理论，而不是照搬文献和标准文档。

二是通过大量直观的图例来描述复杂的工作原理和操作流程。在一些国家的计算机专业教育中，有图解(diagram)或映像(map)这门课，旨在通过易于理解的图例来直观地描述网络的结构、工作流程及实现原理。本书在写作过程中采用了大量的图例和表格来描述复杂的网络安全实现原理。

三是理论与实践的有机结合。理论与实践之间的脱节是目前许多计算机专业教材普遍存在的问题，有些教材过于强调理论阐述而忽视实践操作，而有些图书则只注重讲述操作步骤而忽视了理论讲解。本书一方面强调对基本概念、理论、算法和协议的讲解，同时尽可能地通过实际操作来验证相关的理论。

四是内容新颖翔实。计算机网络技术的发展非常迅速，为了使学生在走出校门后能够将所学知识应用到具体工作中，在教材内容的选择上必须考虑到与实际应用之间的有机结合。本书在写作过程中参阅了大量的研究成果和文献资料，以求内容新颖，讲解翔实。

五是注重内容讲解时的完整性。网络安全涉及的面较广，许多应用的实现需要大量理论的支持。本书在写作过程中充分考虑到内容完整性，对所涉及到的但在本书中没有单独讲述的内容进行了实时介绍或给出了文献出处，以便读者查阅。

本书共分为9章，主要内容包括计算机网络安全概述、数据加密技术及应用、PKI/PMI技术及应用、身份认证技术、TCP/IP体系的协议安全、计算机病毒、木马和间谍软件与防治、网络攻击与防范、防火墙技术及应用和VPN技术及应用等内容。

在本书的编写过程中，作者参考了大量的国内外文献资料，其中部分文献的出处并未全

部列出。对涉及到的每一个实验操作都在实验室或真实网络环境中进行了测试，以保证实验操作步骤和内容的正确性。其中，部分实验和应用来自作者单位真实的网络环境。

在本书编写过程中，得到了清华大学出版社的大力支持，也得到了作者家人及很多同事的帮助，其中李馥娟、郭亚峰、刘庆航、宋玲华、张卫东、聂明辉和陶慎亮等老师负责了部分实验的测试和文字的校对工作，借此机会向他们表示衷心的感谢。由于作者研究水平有限，书中难免还存在一些缺点和错误，殷切希望广大教师、科研人员和读者批评指正，作者的E-mail为wq@jspi.cn。

计算机网络安全与计算机网络管理属于同一范畴的两个研究和应用分支，两者之间的联系非常紧密，而且都在快速地发展。为此，作者同时编写了《计算机网络管理技术》一书，并由清华大学出版社出版。

目 录

第1章 计算机网络安全概述

今天，IP网络几乎成为现代计算机网络的代名词。IP网络存在的设计缺陷和安全隐患也逐渐暴露出来。随着计算机网络应用范围的不断扩展，大量基于IP网络的应用层出不穷，这更加剧了网络的负担，安全问题越加突出。本章将从网络安全概念、安全现状、安全策略和热点技术等方面，对计算机网络的安全进行综述性介绍。

1.1 计算机网络安全研究的动因

现在广泛使用的基于IPv4通信协议的网络，在设计之初就存在着大量缺陷和安全隐患。虽然下一个版本IPv6在一定程度上解决IPv4中存在的安全问题，但是IPv6走向全面应用还需要较长的时间。从IPv4网络的应用历史来看，许多安全问题也是随着应用的出现而暴露出来的，所以不能肯定地讲IPv6网络的应用就一定能够解决IPv4中存在的所有安全问题。

1.1.1 网络自身的设计缺陷

如果对比分析PSTN、ATM和FR等网络技术，就会发现IP网络在设计上存在的不足或缺陷。TCP/IP通信协议自20世纪60年代末诞生以来，已经历了30多年的实践检验，并成为Internet的基础。TCP/IP通信协议的不断发展和完善促进了Internet的发展，同时Internet的发展又进一步扩大了TCP/IP通信协议的影响。目前，几乎所有厂商的网络产品都支持TCP/IP，如硬件厂商Cisco、IMB等，数据库Oracle等，操作系统NetWare等。虽然TCP/IP取得了巨大的成功，但其存在的设计缺陷不可回避。分析目前广泛使用的IPv4协议，在应用中主要存在以下的安全问题。

1. 协议本身的不安全性

例如，在TCP/IP参考模型的传输层提供了TCP和UDP两种协议(2000年提出了SCTP协议，即流控制传输协议)，其中UDP本身就是一种不可靠、不安全的协议，而TCP当初力求通过三次握手机制保障数据传输的可靠性和安全性，但近年来利用TCP/IP三次握手出现的网络攻击现象频繁发生。再如，目前在局域网中泛滥的ARP欺骗和DHCP欺骗，其根源是这些协议在当初设计时只考虑到了应用，而没有或很少考虑安全。还有，如DNS、POP3、SMTP和SNMP等应用层的协议几乎都存在安全隐患。

2. 应用中出现的不安全因素

当初，设计Internet的前身ARPAnet的目的很单纯，根本没有考虑到Internet在几十年后会发展为今天这样的现状。最初，在Internet上传输的主要是一些以纯代码为主的文

本信息，Internet 主要应用于电子邮件的收发。随后要求在 Internet 传输一些图片和文档。再到后来就出现了多媒体应用，即多媒体网络，要求通过计算机网络能够同时处理和传输文字、音频、视频、图形、图像及动画等多种媒体信息。现在，在 VOD(视频点播)技术得到广泛应用的同时，研究者已开始关注 IPTV(网络电视)、VoIP(网络电话)等基于计算机网络的实时通信技术的应用。回顾计算机网络应用的发展历程，一方面是各种新的应用技术层出不穷，另一方面是 TCP/IP 通信协议等基本架构没有发生变化，而且越来越多的要求更高的应用都要争用有限的网络资源。这时研究者和用户开始发现在解决了应用功能的同时，安全问题随之而来。在这种情况下，像 VPN、IPSec 等安全协议开始出现，力求解决网络应用中存在的安全问题。但现实情况是，随着时间的推移及应用需求的不断发展，新的安全问题又会出现。针对这种现象，究其根源还是 IP 网络自身的缺陷，因为 IP 网络本身就是一个“尽力而为”的不可靠的网络，设计者在设计之初根本没有想到网络会成为今天这种现状，或者说 IP 网络本身就不适合于今天的许多网络应用。然而，当大量的应用强加到网络中的时候，带来的最大问题就是安全。

以 IPv4 为代表的 IP 网络目前遇到的困境与今天的道路交通非常相似。目前许多城市的道路还是几年前甚至是几十年前根据当时的交通需求而建设的，但最近几年来交通工具的快速发展导致交通堵塞和交通事故频繁发生。现代社会生活又离不开这些交通工具，所以只能在忍受交通堵塞带来的烦恼的同时，还要解决不断出现和可能遇到的安全问题。

3. 网络基础设施的发展带来的不安全因素

从应用的角度来看，早期的计算机网络多为有线网络。近年来，在铜缆、光纤等有线网络得到大量应用的同时，基于微波、无线电和红外线等无线介质的无线通信方式得到了快速发展，并逐步实现了与有线网络的融合。

从另外一个角度来看，早期计算机网络的应用有其局限性，主要供单位内部的近距离通信。后来，计算机网络的应用逐渐延伸到整个通信领域，通信方式从模拟到数字的转换已成为现实。今天，无论是计算机网络还是电信网络，不管是固定通信还是移动通信，已基本实现了全网的数字化。目前正在推广的 3G 网络，优于以前通信方式的最大特点是数字化和通信速度。但即将制订的 4G 通信标准，开始将无线局域网(Wireless LAN，WLAN)技术与移动通信技术进行融合，使终端的动态连接速率达到 100Mb/s，静态连接速率达到 1Gb/s。

在计算机网络技术的发展过程中，虽然针对有线网络的窃听和物理接入等不安全因素一直存在，但与今天无线通信中所存在和将要面对的安全问题相比，有线通信中存在的安全问题相对要少得多。然而，有线与无线的融合已成为不争的事实，所以随着网络基础设施的不断发展，出现更多的安全问题也是一个不争的事实。

1.1.2 Internet 应用的快速发展带来的安全问题

Internet 由创建于 1969 年的 ARPAnet(Advance Research Projects Agency Network)发展而来，ARPAnet 是由美国国防部出资兴建的，设计 ARPAnet 的最初目的是使各地研究人员在合作一个项目时能快速、灵活地共享代码和信息。当初所连接的节点数只有 4 个，所连接的是大型计算机，当时还没有今天的个人计算机和局域网。在网络中传输的主要是文本信息，数据量较少，应用非常单一。1980 年，ARPAnet 的所有主机都开始采用 TCP/IP 通信协议。在这种情况下，ARPAnet 很少考虑其安全问题。

1983年，在ARPAnet向TCP/IP的转换全部结束的同时，美国国防部国防通信局将ARPAnet分解成两部分：一部分供民用，名称仍然使用ARPAnet，另一部分供军方的非机密通信使用，称为MILnet。随着TCP/IP协议的标准化，ARPAnet的规模不断扩大，不仅美国国内有很多网络与ARPAnet连接，许多国家也通过远程通信线路将本地的计算机与网络接入ARPAnet，成为今天Internet的雏形。

Internet出现后，使用者主要是一些高校和科研院所的学者，主要用于科学研究和学术领域。但到了20世纪80年代末至90年代初期，Internet的商业应用快速发展，各个公司逐渐意识到Internet在产品推销、信息传播及商品交易等方面的价值。Internet的商业应用，致使用户数量不断增加、应用不断扩展、新技术不断出现、Internet的规模不断扩大，使Internet几乎深入到社会生活的每一个角落。在这种情况下，由于Internet本身存在的缺陷及Internet商业化带来的各种利益驱动，Internet上各种攻击和窃取商业信息的现象频繁发生，网络安全问题日益明显。

为此，可以将网络安全的动因主要归纳为三个方面：一是技术缺陷，该缺陷是IP网络与生俱来的，而且在今天的IPv4网络中更为明显；二是经济利益所驱，由于Internet的商业化及其效应不断显现，不法者开始利用Internet窃取个人或企业的信息，并从中非法获得经济利益，成为目前Internet和Intranet上的最大安全风险。例如，2006年10月在Internet上广泛传播的“熊猫烧香病毒”，通过盗取用户的QQ和游戏账号并从中获利；三是利用Internet炫耀个人才能，有些病毒、木马或攻击软件的开发者，其目的并不是为了进行破坏或取得经济利益，而是为了显现自己的计算机专业水平。例如，“硬盘终结者”病毒在发作时将弹出一个信息分析窗口，作者以此来炫耀自己的技术，并希望业内的病毒作者能与其合作。

1.2 网络安全的概念

安全的意义是将资源可能受到的威胁降到最低程度。随着计算机网络的不断发展，全球信息化已成为人类社会发展的大势所趋。但是，由于计算机网络具有连接形式多样、终端分布不均匀、网络系统开放及不同设备之间互连等特征，致使网络易受黑客、恶意软件和其他非法行为的攻击，所以网上信息的安全和保密已成为一个至关重要的问题。对于像银行系统等传输敏感数据的计算机网络系统而言，其网上信息的安全和保密显得尤为重要，因此这些网络必须具有足够强的安全措施。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素的脆弱性和潜在威胁，因此网络的安全措施应是能全方位地应对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

国际标准化组织(ISO)对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等现象。具体来讲，网络安全包括以下5个基本要素。

(1) 机密性。确保信息不暴露给未经授权的人或应用进程。