高等学校**应用型特色**规划教材

计算机网络安全基础

JISUANJI WANGLUO ANQUAN JICHU

杜文才 主 编
顾 剑 周晓谊 副主编

赠 送
电子教案

以计算机网络安全理论为主线，从网络安全的基本概念入手，介绍计算机网络安全技术知识。

本书内容涵盖：计算机网络基础、网络安全基础、计算机网络安全威胁、网络安全评价标准、网络犯罪与黑客、恶意脚本、安全评估分析与保证、身份认证与访问控制、密码学、安全协议、防火墙技术、系统入侵检测与预防、网络取证、病毒与内容过滤、网络安全协议与标准、无线网络与设备的安全。

清华大学出版社

高等学校应用型特色规划教材

计算机网络安全基础

杜文才　主　编

顾　剑　周晓谊　副主编

常　颖　陈　丹　参　编

清华大学出版社

北 京

内 容 简 介

本书以计算机网络安全理论为主线，从计算机网络安全知识的基本概念介绍入手，引导开展计算机网络安全技术知识的学习。本书由 16 章组成，内容包括计算机网络基础、网络安全基础、计算机网络安全威胁、网络安全评价标准、网络犯罪与黑客、恶意脚本、安全评估分析与保证、身份认证与访问控制、密码学、安全协议、防火墙技术、系统入侵检测与预防、网络取证、病毒与内容过滤、网络安全协议与标准、无线网络与设备的安全。

本书贴近教育部颁布的新学科专业调整方案和高校本科建设目标，将计算机网络安全基础知识、技术与实践整合为一体，适合在校大学生学习，是比较全面的计算机网络安全理论基础的教材；对于普通大众，也是一本具有一定实践指导意义的学习辅导书。

图书在版编目(CIP)数据

计算机网络安全基础/杜文才主编. --北京：清华大学出版社，2016
高等学校应用型特色规划教材
ISBN 978-7-302-42884-8

Ⅰ. ①计… Ⅱ. ①杜… 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 030575 号

责任编辑：温　洁
封面设计：杨玉兰
责任校对：周剑云
责任印制：宋　林

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, 010-62791865

印 装 者：三河市少明印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张：**19.25　　**字　数：**460 千字
版　　次：2016 年 3 月第 1 版　　**印　次：**2016 年 3 月第 1 次印刷
印　　数：1～3000
定　　价：35.00 元

产品编号：052143-01

前　言

计算机网络已在普通民众身边存在很久，在我们还没有意识到其存在的时候，它就已经为我们默默服务多年了。但是，计算机网络给人们带来的已经不单单是它的优质服务，也带来了与日俱增的担忧，甚至是恐惧之心。计算机网络安全已经是摆在所有人面前的一道必须解决的难题。

本书就是为解决该难题而推出的。

不论是从技术角度讲，还是从社会角度讲，计算机网络安全都是一个范围十分广泛、具有一定深度的问题，也是很难描述清楚的，因此，本书着重从比较基础的技术角度来讲解和讨论这个问题。同时，对于常见的、普通民众经简单学习就可以遵循的部分实践，也进行了讲解和说明，并列举了一些代码和实验截图，还给出了一些与计算机网络安全有关的网站地址，以方便读者参考。

因此，本书对于在校大学生是本比较全面的计算机网络安全理论基础教材，对于普通大众，也是一本具有一定实践指导意义的辅导书。

1. 本书特色

(1) 高度贴近教育部颁布的新的学科专业调整方案和高校本科建设目标

本书以教育部颁布的新的学科专业调整方案和高校本科建设目标为指导，紧扣计算机网络安全基础知识，从基础理论与实践两个方面，强调对学生自学能力的培养，强调提高学生的应用素质，以培养“学术型”和“应用型”相结合的实用型人才。

(2) 以整合计算机网络安全基础知识、技术和实践于一体为原则

以计算机网络安全理论为主线，从计算机网络安全知识的基本概念介绍入手，引导开展计算机网络安全技术讲解，最后，结合一些实践，使基础知识、应用技术与实践有机地结合成一体。

(3) 基础理论坚实、实际应用贴近现实

本书在基础理论坚实、实际应用贴近现实的目标框架内，处理内容所涉及的计算机网络安全知识，注重理论与实践的有机结合，力求做到使读者既能掌握坚实的基础理论，又能学到一定的实践技术。本书通俗易懂，提供了对于理解计算机网络安全所必需的理论基础知识，并配有复习思考题，以帮助学生提高分析问题和解决问题的能力。

(4) 配有很多实际动手实验的例子

计算机网络安全对于大部分人来说，都是一种实践课题，不论是否愿意，我们都必须亲身去实践和实验。因此，本书在具体操作方面，给出了作者做过的许多实验，并讲述了自己获得的经验，这也是本书的一个鲜明的特色。

(5) 众多与计算机网络安全有关的网站地址

在本书各章末尾推荐的参考资料中，给出了许多网站地址。这些网站包含了计算机网络安全理论和实践的最主要、最前端的文献。学习和参考这些网站的内容，是保证计算机网络安全的重要方法之一，希望能引起读者的充分重视。

2. 本书结构

本书由16章组成，简略描述如下。

第1章 计算机网络基础。系统地介绍计算机网络、设备的基本结构和组成知识，主要包括计算机网络结构组成、分类、体系结构、设备和应用模式。

第2章 网络安全基础。从整体上讨论网络安全的基本结构和知识，主要包括安全概述、安全模型、安全攻防技术、网络的层次体系结构和安全管理。

第3章 计算机网络安全威胁。系统地介绍网络安全威胁机制，主要包括威胁来源、威胁动机、威胁管理与防范和威胁认知。

第4章 计算机网络安全评价标准。介绍当前主要的网络安全评价标准，包括网络安全评价标准的形成、典型的评价标准、信息系统安全等级保护、信息安全保证技术框架等。

第5章 网络犯罪与黑客。介绍网络犯罪与黑客的基本概念，主要包括网络犯罪、黑客、不断上升的网络犯罪应对等。

第6章 恶意脚本。介绍脚本的基本知识，并给出常用平台Windows系列和Unix家族下的脚本实例，从脚本的本意和恶意两个角度，讲解脚本的应用现状。

第7章 安全评估分析与保证。从现实的角度，介绍安全评估分析与保证，主要包括安全隐患和评估方法、网络安全评估相关的法律法规，及安全相关的法律知识。

第8章 身份认证与访问控制。主要讲解身份认证和访问控制的理论与机制。

第9章 密码学。系统地介绍密码学的主要理论，主要包括密码学的发展历史、密码学基础、古典密码、对称和非对称密码体制、公钥基础设施和密码学应用。

第10章 安全协议。介绍网络安全协议的基本知识，主要包括安全协议概述、基本安全协议、认证与密钥建立协议和零知识证明等技术问题。

第11章 防火墙技术。系统地介绍防火墙技术，主要包括防火墙体系结构、防火墙技术、防火墙创建和防火墙技术应用。

第12章 系统入侵检测与预防。系统地介绍系统入侵检测与预防技术，主要包括入侵检测、入侵检测系统、入侵检测软件和手工入侵检测。

第13章 计算机网络取证。讲解计算机网络取证的基础知识，主要包括网络取证概述、TCP/IP基础、网络取证数据源、收集网络通信数据、检查和分析网络通信数据。

第14章 病毒与内容过滤。讨论计算机病毒的主要作用机理和防范，包括计算机病毒概述、计算机病毒的分类、计算机病毒的特点及危害、计算机病毒的防范、内容过滤技术和网络内容过滤技术。

第15章 计算机网络安全协议与标准。从计算机网络的角度出发，讨论计算机网络安全协议与标准。主要包括协议的概述、安全协议、常见的网络安全协议和网络安全标准及规范。

第16章 无线网络与设备的安全。这是本书的最后一章，也是当前人们最关心的问题之一。该章从无线网络基本知识开始，简单地介绍无线网络技术、无线局域网规格标准、无线网络的安全和无线网络安全解决方案等问题。

3. 本书作者

本书由澳门城市大学杜文才统筹策划并担任全书主编，顾剑和周晓谊担任副主编。其中第1、2、3章由杜文才编写，第4、5、8、9、10、11等章由周晓谊编写，第6、7、12、13、14、15、16等7章由顾剑编写。全书由杜文才、顾剑负责统稿。

在本书编写过程中，引用了一些成果和参考文献，在此，谨向被引用文献的著(作)者表示真挚的谢意。

本书是计算机网络安全教育工作者及实践者历年理论研究、教学及实践经验的成果，也是广大计算机网络安全教师关心和帮助的产物。由于作者水平有限，书中难免会有谬误或不足之处，敬请各位同仁、专家和使用者批评指正。

目　录

第 1 章　计算机网络基础

计算机网络已经扩展到日常生活的各个层面，时刻影响着人们的行为方式。无论在家里、单位，还是在路上，人们都离不开网络，网络已成为生活和工作中重要的组成部分。网络新技术的发展让这个数字化的世界变得越来越丰富。

从某种意义上来说，计算机网络的发展水平不仅反映出一个国家计算机和通信技术的水平，而且已成为衡量国家综合实力乃至现代化程度的重要标志之一。

1.1　计算机网络概述

计算机网络是将若干台独立的计算机通过传输介质相互物理地连接，并通过网络软件逻辑地相互联系到一起而实现信息交换、资源共享、协同工作和在线处理等功能的计算机系统。它给人们的生活带来了极大的便利，如办公自动化、网上银行、网上订票、网上查询、网上购物等。计算机网络不仅可以传输数据，也可以传输图像、声音、视频等多种媒体形式的信息，计算机网络不仅广泛应用于政治、经济、军事、科学等领域，而且已应用于社会生活的方方面面。

1.1.1　计算机网络的基本概念

计算机网络(Computer Network)是利用通信线路和通信设备，把分布在不同地理位置的具有独立功能的多台计算机、终端及其附属设备互相连接，按照网络协议进行数据通信，利用功能完善的网络软件实现资源共享的计算机系统的集合。计算机网络是计算机技术与通信技术结合的产物。

在计算机网络中，多台计算机之间可以方便地互相传递信息，因此，资源共享是计算机网络的一个重要特征。用户能够通过网络来共享软件、硬件和数据资源。

现代计算机网络可以提供多媒体信息服务，如图像、语音、视频、动画等。各种新的网络应用也不断出现，如视频点播 VOD(Video On Demand)、网上交易(E-Marketing)、视频会议(Video Meeting)等。

1.1.2　计算机网络的演变

进入 21 世纪以来，计算机网络获得了飞速的发展。回顾 20 世纪 90 年代，在我国还很少有人接触网络。而现在，计算机通信网络和 Internet 已成为我们日常生活的一部分。网络被应用于工商业的各个方面，包括电子银行、电子商务、现代化的企业管理、信息服务业等，都以计算机网络系统为基础。从学校远程教育到政府日常办公，乃至现在的电子社区，很多方面都离不开网络技术。可以毫不夸张地说，计算机网络在当今世界无处不在。

20 世纪 50 年代中期，美国半自动地面防空系统(Semi-Automatic Ground Environment，SAGE)开始了计算机技术与通信技术相结合的尝试，在 SAGE 系统中，把远程的雷达和其

他测控设备的信息经由线路汇集至一台 IBM 计算机上进行集中处理与控制。

世界上公认的、成功的第一个远程计算机网络，是在 1969 年由美国高级研究计划署(Advanced Research Projects Agency，ARPA)组织研制成功的。该网络被称为 ARPAnet，它是 Internet 的前身。

随着计算机网络技术的快速发展，计算机网络的发展大致可以划分为以下 4 个阶段。

1. 诞生阶段

20 世纪 60 年代中期之前的第一代计算机网络，是以单台计算机为中心的远程联机系统。典型应用是由一台计算机和全美范围内 2000 多个终端组成的飞机订票系统。终端是一台计算机的外部设备，包括显示器和键盘，无 CPU 和内存。随着远程终端的增多，为了减轻中心计算机的负载，在通信线路和计算机之间设置了一个前置处理机(Front End Processor，FEP)或通信控制处理机(Communication Control Processor，CCP)，专门负责与终端之间的通信控制，使数据处理和通信控制分开。在终端机较为集中的地区，采用了集中管理器(集中器或多路复用器)，用低速线路把附近群集的终端连起来，通过 Modem 及高速线路与远程中心计算机的前端机相连。这样的远程联机系统，既提高了线路的利用率，又节约了远程线路的投资。

当时，人们把计算机网络定义为：以传输信息为目的而连接起来的、实现远程信息处理或进一步实现资源共享的系统。这样的通信系统已经具备了网络的雏形。

2. 形成阶段

20 世纪 60 年代中期至 70 年代的第二代计算机网络，是以多台主机通过通信线路互连起来的，为用户提供服务，典型的代表是美国国防部高级研究计划局协助开发的 ARPAnet。主机之间不是直接用线路相连，而是由接口报文处理机(Interface Message Processor，IMP)转接后互连。IMP 和它们之间互连的通信线路一起负责主机间的通信服务，构成了通信子网。通信子网互连的主机负责运行程序，提供资源共享，组成了资源子网。这个时期，网络的概念为：以能够相互共享资源为目的互连起来的，具有独立功能的计算机的集合体。这就形成了计算机网络的基本概念。

3. 互连互通阶段

20 世纪 70 年代末至 90 年代的第三代计算机网络，是具有统一的网络体系结构并遵循国际标准的开放式和标准化的网络。ARPAnet 兴起后，计算机网络发展迅速，各大计算机公司相继推出了自己的网络体系结构及实现这些结构的软硬件产品。由于没有统一的标准，不同厂商的产品之间互连很困难，人们迫切需要一种开放性的标准化实用网络环境，在这种情况下，两种国际通用的最重要的体系结构应运而生，即 TCP/IP 体系结构和国际标准化组织的 OSI 体系结构。

4. 高速网络的技术阶段

20 世纪 90 年代末至今的第四代计算机网络，是随着网络技术的不断发展出现的高速网络技术，如千兆网、万兆网、3G 乃至 4G 网络，并且网络功能向综合化方向发展，支持多种媒体信息传输，并且速度越来越快。

1.1.3　计算机网络的基本功能

计算机网络最主要的功能，是资源共享和通信，除此之外，还有负荷均衡、分布处理和提高系统安全与可靠性等功能。其基本功能表现如下。

1. 软、硬件共享

计算机网络允许网络上的用户共享网络上各种不同类型的硬件设备，可共享的硬件资源有：高性能计算机、大容量存储器、打印机、图形设备、通信线路、通信设备等。共享硬件的好处是提高硬件资源的使用效率、节约开支。

现在已经有许多专供网上使用的软件，如数据库管理系统、各种 Internet 信息服务软件等。共享的软件允许多个用户同时使用，并能保持数据的完整性和一致性。特别是伴随客户机/服务器(Client/Server，C/S)和浏览器/服务器(Browser/Server，B/S)模式的出现，人们可以使用客户机来访问服务器，而服务器软件是共享的。在 B/S 方式下，软件版本的升级修改，只要在服务器上进行，全网用户可立即享受。可共享的软件种类很多，包括大型专用软件、各种网络应用软件、各种信息服务软件等。

2. 信息共享

信息也是一种资源，Internet 就是一个巨大的信息资源宝库，其上有极为丰富的信息，它像是一个信息的海洋，有取之不尽、用之不竭的信息和数据。每一个接入 Internet 的用户都可以共享这些信息资源。可共享的信息资源有：搜索与查询的信息，Web 服务器上的主页及各种链接，FTP 服务器中的软件，各种各样的电子出版物，网上消息、报告和广告，网上大学，网上图书馆等。

3. 通信

通信是计算机网络的基本功能之一，它可以为网络用户提供强有力的通信手段。建设计算机网络的主要目的，就是让分布在不同地理位置的计算机用户能够相互通信、交流信息。计算机网络可以传输数据以及声音、图像、视频等多媒体信息。利用网络的通信功能，可以发送电子邮件、打电话、在网上举行视频会议等。

4. 负荷均衡与分布处理

负荷均衡是指将网络中的工作负荷均匀地分配给网络中的各计算机系统。当网络上某台主机的负载过重时，通过网络和一些应用程序的控制及管理，可以将任务交给网络上其他的计算机去处理，充分发挥网络系统上各主机的作用。分布处理将一个作业的处理分为三个阶段：提供作业文件、对作业进行加工处理、把处理结果输出。在单机环境下，上述三步都在本地计算机系统中进行。在网络环境下，根据分布处理的需求，可将作业分配给其他计算机系统进行处理，以提高系统的处理能力，高效地实现一些大型应用系统的程序计算以及大型数据库的访问等。

5. 系统的安全与可靠性

系统的可靠性对于军事、金融和工业过程控制等领域的应用特别重要。计算机通过网

络中的冗余部件，能够大大提高可靠性。例如，在工作过程中，一台计算机出了故障，可以使用网络中的另一台计算机；网络中一条通信线路出了故障，可以取道另一条线路，从而提高网络系统的整体可靠性。

1.1.4 计算机网络的基本应用

随着现代社会信息化进程的推进，通信和计算机技术迅猛发展，计算机网络的应用变得越来越普及，几乎深入到社会的各个领域。

1. 在教育、科研中的应用

通过全球计算机网络，科技人员可以在网上查询各种文件和资料，可以互相交流学术思想和交换实验资料，甚至可以在计算机网络上进行国际合作研究项目。在教育方面，可以开设网上学校，实现远程授课，学生可以在家里或其他可以将计算机接入计算机网络的地方，利用多媒体交互功能听课，有什么不懂的问题，可以随时提问和讨论。学生可以从网上获得学习参考资料，并且可通过网络交作业和参加考试。

2. 在办公中的应用

计算机网络可以使单位内部实现办公自动化，实现软、硬件资源共享。如果将单位内部网络接入 Internet，还可以实现异地办公。如通过 WWW 或电子邮件，公司可以很方便地与分布在不同地区的子公司或其他业务单位建立联系，及时地交换信息。在外地的员工通过网络还可以与公司保持通信，得到公司的指示和帮助。企业可以通过 Internet 搜集市场信息，并发布企业产品信息。

3. 在商业上的应用

随着计算机网络的广泛应用，电子数据交换(Electronic Data Interchange，EDI)已成为国际贸易往来的一个重要手段，它以一种被认可的数据格式，使分布在全球各地的贸易伙伴可以通过计算机传输各种贸易单据，代替了传统的贸易单据，节省了大量的人力和物力，提高了效率。通过网络，可以实现网上购物和网上支付，例如，登录“当当”网上书城(www.dangdang.com)购买图书等。

4. 在通信、娱乐上的应用

在过去的 20 世纪中，个人之间通信的基本工具是电话，而 21 世纪中，个人之间通信的基本工具是计算机网络。目前，计算机网络所提供的通信服务包括电子邮件、网络寻呼与聊天、BBS、网络新闻和 IP 电话等。

目前，电子邮件已广泛应用。Internet 上存在着很多的新闻组，参加新闻组的人可以在网上对某个感兴趣的问题进行讨论，或是阅读有关这方面的资料，这是计算机网络应用中很受欢迎的一种通信方式。

网络寻呼不但可以实现在网络上进行寻呼的功能，还可以在网友之间进行网络聊天和文件传输等。IP 电话也是基于计算机网络的一类典型的个人通信服务。

家庭娱乐正在对信息服务业产生着巨大的影响，它可以让人们在家里点播电影和电视节目。新的电影可能成为交互式的，观众在看电影时，可以不时地参与到电影情节中去。

家庭电视也可以成为交互式的，观众可以参与到猜谜等活动中。

家庭娱乐中最重要的应用可能是在游戏上，目前，已经有很多人喜欢上玩多人实时仿真游戏。如果使用虚拟现实的头盔和三维、实时、高清晰度的图像，我们就可以共享虚拟现实的很多游戏和进行多种训练。

随着网络技术的发展和各种网络应用需求的增加，计算机网络应用的范围在不断扩大，应用领域越来越拓宽，越来越深入，许多新的计算机网络应用系统不断地被开发出来，如工业自动控制、辅助决策、虚拟大学、远程教学、远程医疗、信息管理系统、数字图书馆、电子博物馆、全球情报检索与信息查询、网上购物、电子商务、电视会议、视频点播等。

1.2 计算机网络的结构组成

一个完整的计算机网络系统是由网络硬件和网络软件所组成的。网络硬件是计算机网络系统的物理实现，网络软件是网络系统中的技术支持。两者相互作用，共同完成网络的功能。

(1) **网络硬件**：一般指网络的计算机、传输介质和网络连接设备等。

(2) **网络软件**：一般指网络操作系统、网络通信协议等。

1.2.1 网络硬件系统

计算机网络硬件系统是由计算机(主机、客户机、终端)、通信处理机(集线器、交换机、路由器)、通信线路(同轴电缆、双绞线、光纤)、信息变换设备(Modem，即编码解码器)等构成的。

1. 主计算机

在一般的局域网中，主机通常被称为服务器，是为客户提供各种服务的计算机，因此，对其有一定的技术指标要求，特别是主、辅存储容量及其处理速度要求较高。根据服务器在网络中所提供的服务的不同，可将其划分为文件服务器、打印服务器、通信服务器、域名服务器、数据库服务器等。

2. 网络工作站

除服务器外，网络上的其余计算机主要是通过执行应用程序来完成工作任务的，我们把这种计算机称为网络工作站或网络客户机，它是网络数据主要的发生场所和使用场所，用户主要是通过使用工作站来利用网络资源并完成自己的作业的。

3. 网络终端

网络终端是用户访问网络的界面，它可以通过主机连入网内，也可以通过通信控制处理机连入网内。

4. 通信处理机

通信处理机一方面作为资源子网的主机、终端连接的接口，将主机和终端连入网内；