>>> 应用型人才培养
规划教材

普通高等学校应用型人才培养系列规划教材
丛书主编　陈明

网络安全技术与应用

WANGLUO ANQUAN JISHU YU YINGYONG

姚宣霞　刘振华　武　涛　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

普通高等学校应用型人才培养系列规划教材
丛书主编　陈明

网络安全技术与应用

姚宣霞　刘振华　武　涛　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

随着计算机网络技术的飞速发展，当今社会已成为一个网络化的社会，人们的日常生活越来越多地依赖于网络，随之而来的网络安全问题也日渐突出，因此人们对网络安全性的要求越来越高。

本书内容以编者多年教学经验为基础，涵盖了网络安全的主要内容，知识结构经过精心安排。在介绍网络安全基本理论的基础上，首先总体地介绍了 TCP/IP 网络安全的基本状况。然后分别从不同层次介绍了如何保障 TCP/IP 网络的安全，并以实例的形式帮助用户理解和掌握如何运用网络安全理论与协议来保障网络的安全。重点介绍了能够从整体上保障网络安全的两种安全产品：防火墙和入侵检测技术。分别举例说明了个人防火墙、企业防火墙和免费入侵检测工具 Snort 的部署、设置与使用方法。最后，详细分析了影响主机系统安全的内外因素，从操作系统安全、病毒与木马的防御等多个角度介绍了保障主机系统安全的方法。

本书适合作为高等院校计算机、信息安全、通信等专业高等院校本科生或研究生的教材或学习参考书。对于在计算机网络与安全领域从事教学、科研和工程技术工作的人员也有一定参考价值。

图书在版编目（CIP）数据

网络安全技术与应用 / 姚宣霞，刘振华，武涛编著.
— 北京：中国铁道出版社，2012.12
普通高等学校应用型人才培养系列规划教材

ISBN 978-7-113-15382-3

Ⅰ. ①网… Ⅱ. ①姚… ②刘… ③武… 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（2012）第 227073 号

书　　名：网络安全技术与应用
作　　者：姚宣霞　刘振华　武　涛　编著

策　　划：刘丽丽　　**读者热线：**400-668-0820
责任编辑：吴宏伟
编辑助理：刘丽丽
封面设计：付　巍
封面制作：白　雪
责任印制：李　佳

出版发行：中国铁道出版社（100054，北京市西城区右安门西街 8 号）
网　　址：http://www.51eds.com
印　　刷：三河市兴达印务有限公司
版　　次：2012 年 12 月第 1 版　　2012 年 12 月第 1 次印刷
开　　本：787mm×960mm　1/16　　**印张：**18　　**字数：**335 千
印　　数：1～3 000 册
书　　号：ISBN 978-7-15382-3
定　　价：35.00 元

普通高等学校应用型人才培养系列规划教材

编审委员会

序言

PREFACE

经过几十年的研究与探索，现代计算机系统功能越来越强大、应用越来越广泛。计算机的广泛应用一方面对人类社会的发展做出了卓越的贡献，另一方面也在推动计算机学科的高速发展，因而一直受到社会的高度关注。

由于计算机学科呈现出的学科内涵宽泛化、分支相对独立化、社会需求多样化、专业规模巨大化和计算教育大众化等特点，使得计算机企业成为了朝阳企业，这些 IT 企业需要大量的具有专门计算机技能的人才，但传统的研究型计算机教育是以学术教育为基础，以培养计算机精英为目的的计算机教育，与社会和行业对计算机高等教育人才的需求产生了矛盾——大学中单一的计算机精英型教育培养的人才已不能满足实际需要，凸显职业特征的计算机应用型教育异军突起，迅速发展，备受关注。这种矛盾促使教学模式呈现了职业性，并在培养面向知识应用和全面能力方面，提出了多种职业性教学模式，如网络工程师、软件工程师、动画设计师、硬件工程师等培养模式。因此，研究和实施计算机应用型人才培养模式势在必行。

什么是计算机应用型教育？我们通过长时间的教育研究和教学经验的总结，认为计算机应用型教育的培养目标可以利用知识、能力和素质三个基本要素来描述。

知识是基础、载体和表现形式，从根本上影响着能力和素质。学习知识的目的是为了获得能力和不断地提升能力。知识可以转化为能力和素质，能力对知识具有反作用，促进知识的不断发展。

能力是核心，是应用型人才特征的突出表现。从计算机学科而言，培养的人才应具备计算思维能力、算法设计与分析能力、程序设计与实现能力、系统能力（系统的认知、设计、开发、应用能力）。而计算机应用型人才的能力有着其独特的属性，主要包括应用能力（专业能力）和通用能力。应用能力主要是指用所学知识解决专业实际问题的能力。通用能力是指跨职业能力，并不是具体的专业能力和职业技能，而是对不同职业的适应能力，也就是当职业发生变更时，这些能力依然在从业者身上起作用。计算机应用型本科人才所应具备的三种通用能力是：学习能力、工作能力和创新能力。

素质要素主要是指基本素质，即具有良好的公民道德和职业道德，具有合格的政治思想素养，遵守计算机法规和法律，具有人文、科学素养和良好的职业素质等。计算机应用型人才素质主要是指工作的基本素质，且要求在从业中必须具备责任意识，能够对自己职责范围内的工作认真负责地完成。

与此同时，我们认为计算机应用型教育培养目标的实现关键在于课程体系的构建，即课程内容

和课程性质的确定。因此，我们将计算机应用型教育课程分为通用课程、基础课程、专业核心课程、专业选修课程、应用课程、实验课程、实践课程等，并建立了相应的教育课程体系，如公共基础课程平台、专业基础课程平台、专业选修课程平台、基本素质平台等，力图通过相应的课程开展来实现培养目标。

目前，应用型人才培养的研究方兴未艾，我们也将会在较长一段教学实践中继续探讨和总结经验。此次组织的这套“普通高等学校应用型人才培养系列规划教材”是应社会需求而建设的，经过系统规划与设计，定位于高等院校计算机应用型人才的培养，整套丛书从架构和具体教材的编写上都力求突出能力培养的理念。本系列教材现正在陆续出版中，希望各位老师和读者指正。

“普通高等学校应用型人才培养系列规划教材”丛书主编

前言

FORWORD

随着电子商务、电子政务、网上银行以及网络证券等网络应用的快速发展，网络安全问题受到空前的重视。因为网络安全不仅仅是一个技术问题，更重要的是它已成为影响社会稳定与发展的政治问题和经济问题。目前，社会上急需大量的网络安全人才。鉴于此，网络安全被大多数高校的计算机及相关专业列为必修课程。

现有的网络安全教材大致可以分为两类：一类偏重于介绍网络安全的基本理论和技术，与实际应用存在脱节现象；另一类偏重于特定的攻防技术，以解决或防范一些安全问题为目标。这两类教材都不适于进行研究型教学和应用型网络安全人才的培养。本书结合这两类网络安全教材的特点，以适于开展研究型教学和培养应用型网络安全人才为目的，对作者多年来讲授“网络与信息安全”课程的经验进行了深入总结，主要可分为四个方面的内容：一是网络与信息安全的基本理论，包括网络安全的基本情况、密码学的基础知识、认证和 Hash 函数等；二是在分析 TCP/IP 网络的安全体系结构的基础上，分别从互联层、传输层和应用层讲解了保障 TCP/IP 网络安全的协议、内容和方法；三是从系统的角度介绍了保护 TCP/IP 网络安全的两种常用产品：防火墙和路由器，并重点讲解对它们的部署和配置方法；四是主机系统的安全防护，从操作系统安全、病毒与木马防护的角度分别阐明了对主机系统进行安全保护的方法和措施。

本书主要特点可以概括为以下四个方面：

① 注重理论与实际相结合，便于学生掌握并在实际中应用网络安全的技术与知识，非常适合作为研究型教学和应用型人才培养的教材或参考书。

② 注重应用实际案例进行说明，加深读者对所学知识的理解和掌握，激发读者的学习兴趣。

③ 内容贴近实际应用，使读者尽快将所学知识付诸于实践，增强学生应用和创新的积极性。

④ 可读性强，全书采用简捷、通俗的语言进行描述，并基于从简单到复杂的思路安排内容，同时结合图和案例来帮助读者学习和理解。

建议本书的教学学时为 40～45 学时，实验学时 10～15 学时。其中第 1 章 1～2 学时，第 2 章 5 学时，第 3 章 4～5 学时，第 4 章 5～6 学时，第 5 章 5 学时，第 6 章 5 学时，第 7 章 5～6 学时，第 8 章 5～6 学时，第 9 章 5 学时。

本书的编写获北京科技大学 211 三期创新人才项目资助，由姚宣霞、刘振华、武涛编著。姚宣霞老师承担了第 3～9 章的编写工作，中华女子学院的武涛老师编写了第 1 章和第 2 章，中华女子学院的刘振华老师承担了部分书稿的校对工作。

在此，对所有为本书做出贡献的人员表示衷心感谢，没有他们的督促和帮助就没有本书的出版。同时，希望广大读者对本书提出意见和建议。

编　者

2012 年 5 月

目录

CONTENTS

第1章 网络安全概述

当今社会是一个网络化的社会，人们的日常生活越来越多地依赖于计算机网络。从而对网络的安全性要求也越来越高，网络安全问题不只是一个技术问题，已成为影响社会稳定和发展的政治问题和经济问题。本章从网络安全的概念和网络安全的目标出发，介绍了网络安全的现状和信息安全技术的发展趋势，讨论了保障网络安全的基本技术，使读者能够较全面地了解网络安全的相关知识。

本章要点：

- 理解网络安全的含义及其目标；
- 了解网络安全的形势；
- 了解网络安全的基本技术。

1.1 网络安全的概念

网络安全的概念是随着计算机网络的发展而产生和发展的，从不同的角度有不同的定义。例如，从用户的角度来说，网络安全是指涉及用户隐私或利益的信息能在网络上安全传输，不被他人或对手窃听、冒充、篡改或抵赖。从网络安全工作者的角度来说，网络安全是指网络系统的安全，主要包括信息的存储安全和信息的传输安全。他们希望能够对网络信息的访问进行有效地保护和控制，避免出现非法存取、拒绝服务和非法控制等威胁。从安全保密部门的角度来说，网络安全是指对有害的、涉及国家机密的信息进行过滤，避免对社会产生危害和机要信息的泄露。

一般而言，网络安全是指网络系统中的硬件、软件和数据受到保护，不因偶然的或恶意的原因而遭受到破坏、更改、泄露，系统能连续可靠正常地运行，网络服务不中断。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、真实

性和可控性的相关技术和理论都是网络安全的研究领域。它是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、数学等多学科的综合性学科。

1.2 网络安全的目标

随着网络技术的不断发展与应用，网络安全的内涵不断延伸，其目标也在不断发生变化。通俗地说，网络安全的目标就是要保护网络系统，使其没有危险、不受威胁、不出事故。从技术角度来说，主要表现在网络中信息的保密性、完整性、可靠性、可用性、不可抵赖性和身份验证等六大方面。

1. 保密性

保密性是指要保证在公网上传输的数据不被第三方窃取，即确保网络中的信息不泄露给非授权的用户、实体或者过程，而只能被经过允许的人员，以经过允许的方式来使用。常用的保密技术包括：

① 防止硬件辐射泄露，网络截获和窃听。使对手侦听不到有用的信息，防止有用信息以各种途径辐射出去。

② 信息的加密解密。在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息。

③ 物理保密。利用各种物理方法，如限制、隔离、掩蔽等措施，或者划分信息的秘密等级，为用户分配不同的权限，对不同权限的用户授予不同的访问权，避免信息越权获取。

2. 完整性

完整性是指网络信息在存储或传输过程中不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入或丢失等。它要求能保持信息的原样。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改。保障网络信息完整性的主要方法有：

① 协议：通过安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

② 密码手段：抗篡改的重要手段。

③ 数字签名：可保障信息的真实性。

3. 可靠性

可靠性是指能够确保在规定条件下和规定的时间内完成规定的功能的特性，主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演着非常重要的角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性

是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

4．可用性

可用性是指网络中的信息可被授权实体访问并按需求使用的特性。即无论何时，只要用户需要，信息系统必须是可用的，授权用户或实体能正常使用资源的特性，即使是网络部分受损，甚至发生突发事件如供电中断、自然灾害、事故或攻击等，仍能为授权用户提供有效的服务，不能拒绝服务。我们知道，网络系统最基本的功能是向用户提供服务，而可用性是面向用户的安全性能，用户的需求是随机的、多方面的，有时还有时间要求。由此可见，可用性是衡量网络性能的一个重要指标，它一般用系统正常使用时间和整个工作时间之比来度量。攻击者通常采用占用资源等手段阻碍授权者的工作，一般可以采用访问控制机制阻止未授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

5．不可抵赖性

不可抵赖性又称不可否认性，它与其他几个安全目标有着本质的不同。其主要目的是保护通信用户免遭来自系统中其他合法用户的威胁，而不是来自攻击者的威胁。“否认”指的是参与某次通信的一方事后不承认，否认曾经发生过这次通信。不可否认就是用来避免这种行为的。为了实现不可否认，在网上开展业务的各方在进行数据传输时，必须带有自身特有的、无法被别人复制的信息，以保证发生纠纷时有所对证。即在网络信息交互过程中，所有参与者都不可能否认或抵赖曾经完成的操作和承诺。也就是对自己所做过的事无法抵赖。

6．身份验证

身份验证是指由于网上的通信双方互不见面，必须在相互通信时（交换敏感信息时）确认对方的真实身份的过程。

通过上面的叙述可以看出，网络安全的目标就是要保证信息在公用网络中传输、交换和存储的过程中，不被窃取或重放，不被更改，能正常使用并能够被合理控制，同时，用户对其所作所为不可否认，能够识别与其通信的对方的真实身份等。

1.3　网络安全的现状

20 世纪 90 年代以来，针对计算机网络与利用计算机网络从事刑事犯罪的数量，在许多国家（包括我国）都以较大的比例快速增长。随着我国教育信息化的快速发展，使用网络的人越来越多，网络为大众提供信息资源和多样化服务的同时，无时不在威胁着广大用户。网络安全事件的发生仍然呈上升趋势。

据相关部门评测统计，仅 2007 年 1 月国家互联网安全中心共收到网络安全事件报告 4 757 件，其中网站网页被篡改事件为 4 611 件，占所有网络安全事件的 97%，原国防科工委 2007 年 1 月监测发现并成功防御了对原国防科工委非涉密网络系统的攻击 2.7 万余次，其中高风险等级攻击 1.8 万

余次。此外，原国防科工委外网邮件系统共拦截病毒邮件 102 万余封，过滤垃圾邮件 4.2 万余封。近年随着社交网站的风靡，智能手机和平板电脑等便携式网络终端设备的推广，生活变得越来越“网络化”，网络安全成为头等大事。

2012 年初，QQ 电脑管家与艾瑞咨询联合发布《2011 下半年个人网络安全报告》，对 2011 年下半年的个人网络安装状况做出了系统的数据分析和总结。《报告》显示，我国网民对网络安全相关的专业术语有着极高的认知度，这标志着近年来在政府和安全厂商的共同推动下，全民性的网络安全问题普及教育取得了良好成果，网民的网络安全意识得到提升。

但 2011 年下半年相继发生的“微博蠕虫事件”和“CSDN 600 万用户资料泄露的蝴蝶效应”使人们对网络安全的关注达到了前所未有的高度，给中国互联网安全敲响了警钟。目前，虽然网民有了较高的认知网络安全意识，但却没能将其有效转化为安全防范意识，并落实在网络行为上。网民的安全意识主要体现在对可见的安全危害的关注，如计算机系统瘫痪、经济损失等实实在在可以感受到的危害，而对网络隐私等不可见或具有潜在危险的感知较低。大部分人只有在涉及金钱等重要信息时，才会有将安全意识转化为防范行为的举动。因此，网民的安全意识转化为防范行为的过程尚需引导与教育。

有专家指出，2012 年网络安全形势将会更加严峻。要保护个人隐私，维护互联网安全，用户首先要加强自身对网络安全的重视程度，在提升网络安全意识的同时安装安全防护软件，将是改善网络安全环境的最好选择。

1.4 网络安全的发展趋势

网络安全技术在近几年得到快速发展，同时，网络安全问题日益突出，网络安全企业不断跟进最新安全技术，推出满足用户需求、具有时代特色的安全产品，进一步促进了网络安全技术的发展。

从技术层面来看，目前网络安全产品在发展过程中面临的主要问题是：以往人们主要关心系统与网络基础层面的防护问题，而现在人们更加关注应用层面的安全防护问题，安全防护已经从底层或简单数据层面上升到了应用层面，这种应用防护问题已经深入到业务行为的相关性和信息内容的语义范畴，越来越多的安全技术已经与应用相结合。

从用户的角度来看，网络安全问题已经渗透到网络生活的方方面面，在传统木马、蠕虫病毒的防杀之外，围绕网络安全产生的“使用困扰”促使用户向安全防护厂商提出了更高的要求，伴随着个人网络安全意识的全面提升，密码保护、支付安全、清理优化成为用户的主流需求。

1．密码保护

历经 2011 年 12 月的“密码门”事件后，中国网民对密码安全的关注达到了前所未有的高度。在 2011 年，有超过 60%的用户会利用密码分级或设置不同密码来保护个人信息安全。在“密码门”事件的警示下，使用更高级别密码的同时借助安防软件进行信息保护的用户数量会进一步增加。