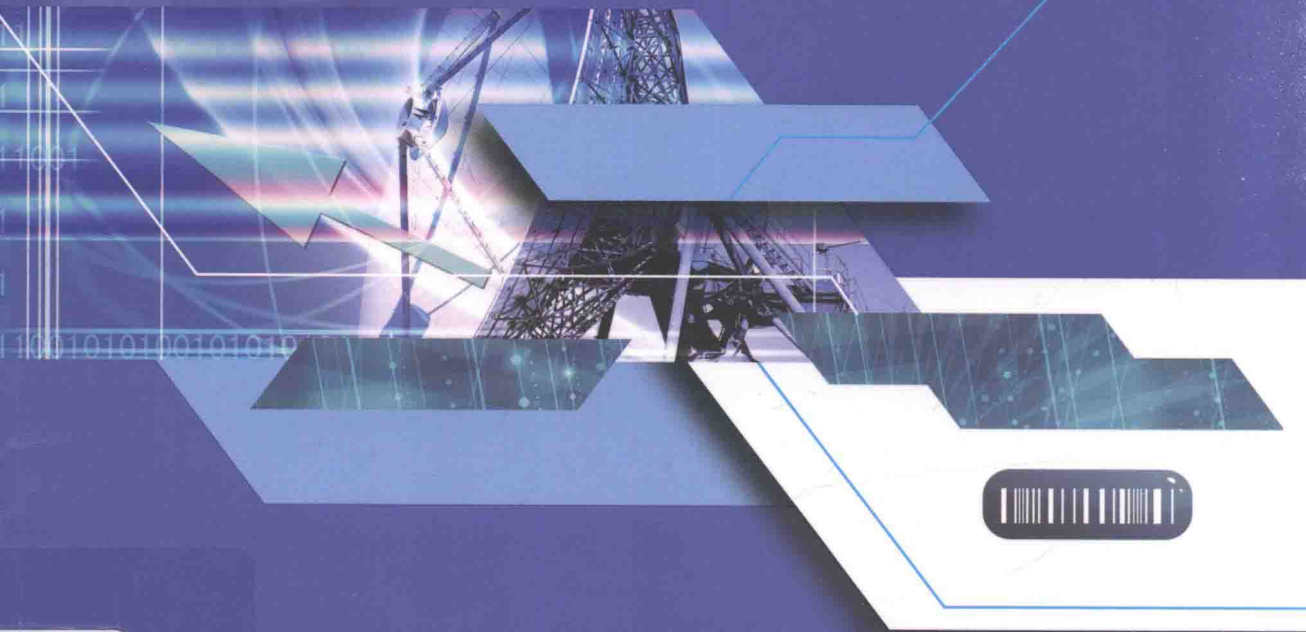
高等学校通信工程专业“十二五”规划教材

计算机通信网络安全

JISUANJI TONGXIN WANGLUO ANQUAN

王国才　施荣华　主编



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

高等学校通信工程专业“十二五”规划教材

计算机通信网络安全

王国才　施荣华　主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书较系统地讲述了计算机通信网络安全的基本技术及其原理和应用。全书共分为 10 章，具体内容包括网络安全概论、网络安全保密、网络安全认证、网络安全协议、网络安全访问、网络安全扫描、网络入侵检测、网络信息保护、网络设备安全及网络安全工程应用等，每章后均附有习题。

本书在介绍计算机通信网络安全的定义和安全体系结构后，以网络安全的保密技术作为基础，逐步介绍网络安全技术，力求基本原理与实际应用相结合。以实现条理清楚，便于读者对网络安全原理的理解及应用。

本书适合作为高等学校信息与通信类专业本科生和研究生网络安全课程的教材，也可作为从事计算机通信网络和信息安全工程技术人员学习、研究的参考书。

图书在版编目（CIP）数据

计算机通信网络安全/王国才，施荣华主编. —北京：中国铁道出版社，2016.9
高等学校通信工程专业“十二五”规划教材
ISBN 978-7-113-21485-2

Ⅰ. ①计… Ⅱ. ①王… ②施… Ⅲ. ①计算机通信网－安全技术－高等学校－教材 Ⅳ. ①TN915.08

中国版本图书馆 CIP 数据核字（2016）第 030569 号

书　　名：计算机通信网络安全
作　　者：王国才　施荣华　主编

策　　划：曹莉群　周海燕　　**读者热线**：（010）63550836
责任编辑：周海燕　鲍　闻
封面设计：一克米工作室
责任校对：汤淑梅
责任印制：郭向伟

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：中国铁道出版社印刷厂
版　　次：2016 年 9 月第 1 版　　2016 年 9 月第 1 次印刷
开　　本：787 mm×1 092 mm　1/16　**印张**：21.5　**字数**：512 千
书　　号：ISBN 978-7-113-21485-2
定　　价：45.00 元

高等学校通信工程专业“十二五”规划教材

编审委员会

主　任：施荣华　李　宏

副主任：王国才　彭　军

主　审：邹逢兴

成　员：（按姓氏笔画排序）

王　玮　王　浩　石金晶　李　尹

李曦柯　杨政宇　张晓勇　赵亚湘

郭丽梅　康松林　梁建武　彭春华

董　健　蒋　富　雷文太

丛书序

在社会信息化的进程中，信息已成为社会发展的重要资源，现代通信技术作为信息社会的支柱之一，在社会发展、经济建设方面，起着重要的核心作用。信息的传输与交换的技术即通信技术得到了快速的发展，通信技术是信息科学技术发展迅速并极具活力的一个领域，尤其是数字移动通信、光纤通信、射频通信、网络通信使人们在传递信息和获得信息方面达到了前所未有的便捷程度。通信技术在国民经济各部门、国防工业及日常生活中得到了广泛的应用，通信产业正在蓬勃发展。随着通信产业的快速发展和通信技术的广泛应用，社会对通信人才的需求在不断增加。通信工程（也作电信工程，旧称远距离通信工程、弱电工程）是电子工程的一个重要分支，电子信息类子专业，同时也是其中一个基础学科。该学科关注的是通信过程中的信息传输和信号处理的原理和应用。本专业学习通信技术、通信系统和通信网等方面的知识，能在通信领域从事研究、设计、制造、运营及在国民经济各部门和国防工业从事开发、应用通信技术与设备。

社会经济发展不仅对通信工程专业人才有十分强大的需求，同样通信工程专业的建设与发展也对社会经济发展产生重要影响。通信技术发展的国际化，将推动通信技术人才培养的国际化。目前，世界上有 3 项关于工程教育学历互认的国际性协议，签署时间最早、缔约方最多的是《华盛顿协议》，也是世界范围知名度最高的工程教育国际认证协议。2013 年 6 月 19 日，在韩国首尔召开的国际工程联盟大会上，《华盛顿协议》全会一致通过接纳中国为该协议签约成员，中国成为该协议组织第 21 个成员。标志着中国的工程教育与国际接轨。通信工程专业积极采用国际化的标准，吸收先进的理念和质量保障文化，对通信工程教育改革发展、专业建设，进一步提高通信工程教育的国际化水平，持续提升通信工程教育人才培养质量具有重要意义。

为此，中南大学信息科学与工程学院启动了通信工程专业的教学改革和课程建设，以及 2016 版通信工程专业培养方案，与中国铁道出版社在近期联合组织了一系列通信工程专业的教材研讨活动。他们以严谨负责的态度，认真组织教学一线的教师、专家、学者和编辑，共同研讨通信工程专业的教育方法和课程体系，并在总结长期的通信工程专业教学工作的基础上，启动了“高等院校通信工程专业系列教材”的编写工作，成立了高等院校通信工程专业系列教材编委会，由中南大学信息科学与工程学院主管教学的副院长施荣华教授、中南大学信息科学与工程学院电子与通信工程系李宏教授担任主任，邀请国家教学名师、国防科技大学邹逢兴教授担任主审。力图编写

一套通信工程专业的知识结构简明完整的、符合工程认证教育的教材，相信可以对全国的高等院校通信工程专业的建设起到很好的促进作用。

本系列教材拟分为三期，覆盖通信工程专业的专业基础课程和专业核心课程。教材内容覆盖和知识点的取舍本着全面系统、科学合理、注重基础、注重实用、知识宽泛、关注发展的原则，比较完整地构建通信工程专业的课程教材体系。第一期包括以下教材：

《信号与系统》《信息论与编码》《网络测量》《现代通信网络》《通信工程导论》《计算机通信网络安全》《北斗卫星通信》《射频通信系统》《数字图像处理》《嵌入式通信系统》《通信原理》《通信工程应用数学》《电磁场与微波技术》《电磁场与电磁波》《现代通信网络管理》《微机原理与接口技术》《微机原理与接口技术实验指导》。

本套教材如有不足之处，请各位专家、老师和广大读者不吝指正。希望通过本套教材的不断完善和出版，为我国计算机教育事业的发展和人才培养做出更大贡献。

高等学校通信工程专业“十二五”规划教材编委会

2015 年 7 月

前　言

Internet 是一个覆盖全球的计算机通信网络，为当今信息时代的人们在全世界范围内的信息交流铺设了四通八达的“高速公路”。Internet 改变了人们的工作方式、生活方式和联系方式。Internet 在为人们带来巨大便利的同时，也隐藏着巨大的风险，有些风险已经造成了巨大的损失，这就是说，计算机通信网络的安全问题是十分严峻的，是迫切需要解决的。

本书内容共分为 10 章。第 1 章为网络安全概论，主要讲述计算机通信网络安全的定义和解决网络安全问题的基本思路，包括网络安全的重要性、网络安全的实质与网络不安全的客观性，以及解决网络安全问题的总体思路：网络安全体系结构、网络安全的非技术问题。第 2 章为网络安全保密，主要讲述实现保密的基础理论和常用方法。介绍密码学的基本术语后，介绍对称密码体制中的常用密码算法 DES、AES，非对称密码体制中的 RSA 算法、ElGamal 加密算法和椭圆曲线（ECC）密码体制，以及密码算法的应用模式和密钥管理、密钥分发、密钥托管等，还介绍了量子密码的概念。第 3 章为网络安全认证，介绍认证所需要应用的 MD-5、SHA 等杂凑函数，RSA 数字签名算法、ElGamal 数字签名、Schnorr 数字签名等数字签名算法，消息认证方法，身份认证方法、公钥基础设施等，也介绍了实现网络安全认证的方法。第 4 章为网络安全协议，讲述保证网络中通信各方安全地交换信息的方法，介绍安全协议的概念和执行方式，介绍了几个典型的应用协议，如 Kerberos 认证等身份认证协议、SET（Secure Electronic Transcation，安全电子交易协议）等电子商务协议、传输层安全通信的 SSL 协议、网络层安全通信的 IPSec 协议，还有 BAN 逻辑等安全协议的形式化证明方法。第 5 章为网络安全访问，主要讲述网络中实现网络资源共享安全的方法，介绍安全访问时常用口令的选择与保护方法，访问控制技术与安全审计技术，以及防火墙技术、VPN 技术和网络隔离技术。第 6 章为网络安全扫描，介绍网络安全扫描的概念、常见的扫描技术及其原理、安全扫描器的设计与应用，还介绍了反扫描技术。第 7 章为网络入侵检测，讲述网络中的不安全操作，介绍网络中常见的不安全操作，包括黑客攻击、病毒感染等，以及入侵检测的原理、方法，入侵检测系统的设计方法，检测出入侵后的响应方法，以及计算机取证和密网技术。第 8 章为网络信息保护，主要讲述保证网络信息的可用性技术，介绍保障传输和存储的信息的可用性，以及保护数字产品的版权问题、信息被破坏后的恢复技术，包括信息隐藏、盲签名、数字水印、数据库的数据备份与数据恢复。第 9 章为网络设备安全，介绍了保证网络中各种硬件

设备正常运行的相关因素，介绍网络设备安全的有关技术，主要包括保证网络设备运行环境的物理安全，以及网络设备配置安全的技术，如交换机的安全配置技术、路由器的安全配置技术、操作系统的安全配置技术以及 Web 服务器的安全配置和管理技术；还介绍了可信计算平台的概念和方法，以构建真正安全的网络设备。第 10 章为网络安全工程应用，主要讲述应用网络安全技术建设安全的网络信息系统的一般方法，介绍网络安全工程的基本概念和信息系统建设的方法，从网络安全需求分析开始建设一个安全的网络信息系统的一般过程及其基本方法。

本书具有以下特点：

（1）在介绍计算机通信网络安全基本思路后，以网络安全的保密技术为基础，逐步介绍网络安全技术，以求条理清楚，便于读者对网络安全原理的理解。

（2）力求基本原理与实际应用相结合。

本书适合作为高等学校信息与通信类专业本科生和研究生计算机通信网络与信息安全课程的教材，教学中可以根据具体情况对书中的内容进行适当取舍。本书也可作为从事计算机通信网络和信息安全工程技术人员学习、研究的参考书。

本书由王国才、施荣华主编，主要编写人员分工如下：提纲由施荣华和王国才商议，各章由王国才撰写，施荣华修订，国防科技大学邹逢兴教授主审。参加编写的还有柯福送、王芳、刘美兰、陈思、陈再来。康松林、杨政宇对本书的编写提供了很多宝贵的建议，中国铁道出版社的有关负责同志对本书的出版给予了大力支持，并提出了很多宝贵意见，本书在编写过程中参考了大量国内外计算机网络文献资料，在此，谨向这些作者及为本书出版付出辛勤劳动的同志一并表示感谢！

本书凝聚了编写人员多年的计算机通信网络安全方面的教学经验和应用经验，由于编者水平所限，书中难免存在不足和疏漏之处，殷切希望广大读者批评指正。

编　者

2016 年 1 月

目 录

CONTENTS

第 1 章 网络安全概论

网络安全事关网络的正常运行和正常使用。本章介绍网络安全的基本问题，包括网络安全的重要性，网络安全的实质与网络不安全的客观性，以及解决网络安全问题的总体思路——网络安全体系结构、网络安全的非技术问题。

1.1 网络安全问题的提出

我们经常在媒体上看到有关网络安全事件的报道，比如某大型网站遭到黑客攻击、某种新型病毒破坏网络系统、犯罪分子利用通信网络诈骗钱财等。无疑，网络的正常运行和正常使用存在着非常多的威胁。

Norton 有关安全威胁的有用信息列出了 20 项，具体如下：

① 偷渡式下载：偷渡式下载是一种计算机代码，它利用 Web 浏览器中的软件错误使浏览器执行攻击者希望的操作，例如运行恶意代码、使浏览器崩溃或读取计算机中的数据。可被浏览器攻击利用的软件错误也称为漏洞。

② 网页仿冒攻击：当攻击者冒充受信任的公司来显示网页或发送电子邮件时，即发生网页仿冒攻击。这些网页或电子邮件要求不知情的客户提供敏感信息。这种网站通常被叫作“钓鱼网站”。

③ 间谍软件：间谍软件是跟踪个人身份信息或保密信息并将这些信息发送给第三方的任何软件包。

④ 病毒：病毒是一种恶意代码或恶意软件，通常由其他计算机通过电子邮件、下载和不安全网站进行传播。

⑤ 通过启发方式检测到的病毒：通过启发方式检测到的病毒是根据病毒表现的恶意行为发现的。这些行为可能包括企图窃取个人的密码或信用卡号等敏感信息。

⑥ 蠕虫：蠕虫是另一种类型的恶意代码或恶意软件，主要目标是向其他容易受到攻击的计算机系统进行传播。它通常通过电子邮件、即时消息或其他某种服务向其他计算机发送其副本而进行传播。

⑦ 未经请求的浏览器更改：未经请求的浏览器更改是指网站或程序在未经用户同意的情况下更改 Web 浏览器的行为或设置。这可能导致主页或搜索页更改为其他网站，通常是为