普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络信息安全技术

蔡皖东 编著

http://www.tup.com.cn

Information Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

网络信息安全技术

蔡皖东 编著

Information Security

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书从理论与应用相结合的角度，系统地介绍网络信息安全的基本理论和应用技术。在内容上，注重新颖性，尽量收录近几年发展起来的新概念、新方法和新技术；在形式上，侧重系统性，从系统体系结构的角度来介绍网络信息安全技术及其应用。因此，本书从形式到内容都有其独到之处。

全书共有 10 章，介绍网络信息安全概论、密码技术、网络层安全协议、传输层安全协议、应用层安全协议、系统安全防护技术、网络安全检测技术、系统容错容灾技术、信息安全标准、系统等级保护等内容。

本书主要作为高等院校相关专业本科生的教材，也可作为相关专业研究生的教材，同时还可供从事网络系统安全技术工作的广大科技人员参考。

图书在版编目(CIP)数据

网络信息安全技术/蔡皖东编著. —北京：清华大学出版社，2015
高等院校信息安全专业系列教材
ISBN 978-7-302-39151-7

Ⅰ. ①网… Ⅱ. ①蔡… 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(2015)第 017955 号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：梁　毅
责任印制：沈　露
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，010-62795954
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**：17.75　　**字　　数**：445 千字
版　　次：2015 年 4 月第 1 版　　**印　　次**：2015 年 4 月第1 次印刷
印　　数：1～2000
定　　价：35.00 元

产品编号：062654-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广。能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套。除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

近年来，随着信息化的发展，国内各行各业建设了大量的网络信息系统，信息安全问题变得日益突出。人们在享受网络所带来方便和效益的同时，也面临着网络安全提出的巨大挑战，如黑客攻击、病毒传播、非法联络、情报获取等，给网络信息安全带来严重的威胁，安全事件屡有发生，给国家安全、企业利益和个人权益带来极大的危害，并造成了巨大的经济损失。

为了应对信息安全方面的挑战，国家制定了两种信息系统安全保护制度：信息系统安全等级保护制度和涉密信息系统分级保护制度，并制定了一系列相关国家技术标准和法律法规，推动了网络信息安全技术发展和应用，规范了网络信息系统建设和管理。

随着我国信息化的发展和应用的普及，网络信息安全越来越重要，国家和业界都加大了对网络信息安全技术研发方面的投入，对网络信息安全专门人才的需求也越来越大。因此，在很多高校设置了信息安全、安全保密等专业，一些计算机、网络工程、电子商务、电子信息等相关专业开设了信息安全课程，加强了对网络信息安全人才的培养，对网络信息安全教材的需求也随之增加。

作者于2004年编写并出版了《网络与信息安全》，作为国防科工委“十五”规划教材。在10年间，我国在网络信息安全技术、应用和政策层面上都有了很大的发展和变化，教材内容也要与时俱进，吐故纳新，更好地服务于教学。因此，作者对原书进行了重新编写。

全书共有10章。第1章为网络信息安全概论，主要介绍网络安全威胁、网络攻击技术、信息安全技术、信息安全工程、信息安全法规等内容；第2章为密码技术，主要介绍对称密码算法、非对称密码算法、数字签名算法、单向散列函数等内容；第3章为网络层安全协议，主要介绍IPSec安全体系结构、安全联盟、安全协议、密钥管理、IPSec协议的应用等内容；第4章为传输层安全协议，主要介绍SSL握手协议、SSL记录协议、SSL支持的密码算法、SSL协议安全性分析、SSL协议的应用等内容；第5章为应用层安全协议，主要介绍S-HTTP协议、S/MIME协议、PGP协议等内容；第6章为系统安全防护技术，主要介绍身份鉴别技术、访问控制技术、安全审计技术、防火墙技术等内容；第7章为网络安全检测技术，主要介绍安全漏洞扫描技术、网络入侵检测技术等内容；第8章为系统容错容灾技术，包括数据备份技术、磁盘容错技术、系统集群技术、数据灾备技术等内容；第9章为信息安全标准，主要介绍

国内外信息安全标准、信息技术安全评估公共准则、系统安全工程能力成熟模型等内容；第10章为系统等级保护，主要介绍信息系统安全等级保护的基本概念、定级方法、基本要求、应用举例等内容。

本书强调理论联系实际，尽量避免理论与应用相脱节。在讲述网络信息安全理论的同时，还介绍了网络信息安全应用示例，以便于读者理解和掌握，也有利于自学，达到事半功倍的学习效果。

本书根据网络信息安全技术发展迅速的特点，还介绍了一些新概念、新方法和新技术，读者在系统地学习理论知识的同时，还能够了解到这一技术的前沿和发展趋势，并从中得到启迪和帮助。

书中难免存在不足和疏漏之处，欢迎广大读者批评指正。

最后，感谢西北工业大学规划教材出版基金对本书的大力资助。

作　者

2014年盛夏于西北工业大学

目 录

第1章 网络信息安全概论

1.1 引言

随着互联网技术的不断发展，越来越显示出计算机网络在社会信息化中的巨大作用，计算机网络已经成为当今社会经济活动和社会生活的基础设施，推动了工业信息化、新兴服务业、信息产业的快速发展，带动了国民经济发展和社会进步。

由于网络系统的开放性，以及现有网络协议和软件系统存在的安全缺陷，使任何一种网络系统都不可避免地、或多或少地存在着一定的安全隐患和风险，使人们在享受网络所带来的方便和效益的同时，也面临着网络安全提出的巨大挑战，黑客攻击、病毒传播、非法联络、情报获取等给网络信息安全带来严重的威胁。网络安全事件屡有发生，给国家安全、企业利益和个人权益带来了极大的危害，并造成了巨大的经济损失。

以获取经济利益为目的的黑客经济兴起，网络侵权和犯罪活动屡禁不止，手法日益翻新，包括篡改网站内容、攻击网络服务器、传播盗版数字作品、窃取网银账号、组建僵尸网络等，直接危害了网络安全和社会和谐。

不法分子利用互联网传播黄色信息、邪教信息、虚假新闻、政治攻击、垃圾邮件等有害信息，严重扰乱了人们的思想，特别是给青少年的身心健康带来了极大的损害。

国内外敌对势力和恐怖组织利用互联网进行非法联络，通过加密邮件、即时通信、语音通信、P2P 通信、社交网络等手段进行秘密联络，策划和实施恐怖活动，直接威胁着国家安全和社会稳定。

网络间谍利用互联网盗窃国家机密信息、企业内部信息和个人隐私信息，网络窃密和泄密事件不断发生。尤其是海外间谍机关利用木马技术有预谋性地窃取国家的政治、军事和经济情报，直接危害了国家安全和利益。

美国和中国台湾地区的军方分别组建了网络信息战组织，称为老虎部队（Tiger Team），其中一项重要任务就是利用互联网和木马技术有预谋地窃取中国大陆的政治、军事和经济情报，对要害部门和重要人员进行重点布控，试图通过植入木马来窃取重要情报。根据国家安全保密部门统计，在我国每年发生的泄密案件中，70％是海外间谍机关通过互联网和木马来窃取的，并且有逐年增长的趋势，对国家安全和利益造成极大的危害。在这些窃密木马中，大部分由中国台湾地区和美国所控制，其中中国台湾地区占 65％，美国占 8％。网络窃密问题已经给国家安全和利益带来了极大的危害。

2013 年 5 月发生了轰动世界的“棱镜门”事件，由美国国家安全局前雇员爱德华·斯诺登披露了美国正在实施的互联网、电话网、手机网等网络监听项目，不仅对美国国内实

施网络监听，还对包括中国在内的多个国家的网络基础设施和服务器实施网络入侵，获取所需要的信息，对国家安全和利益构成极大的威胁。

针对不断增长的信息安全挑战，必须采取有效的信息安全技术来提高信息系统安全防护和入侵检测能力，保障信息系统安全。信息系统安全保护工作是一项系统工程，需要采用工程化方法来规范信息系统安全建设，将信息安全技术贯穿于信息系统建设的各个阶段，而不是单一信息安全技术的简单应用，这样才能达到信息系统安全保护的整体要求。

本章主要介绍网络安全威胁、网络攻击技术、信息安全技术、信息安全工程以及信息安全法规等，使读者对信息系统安全问题有整体上的了解和认知。

1.2 网络安全威胁

1.2.1 网络环境下的安全威胁

所谓的安全威胁是指对系统安全性的潜在破坏。一个系统可能受到各种各样的安全威胁，只有认识到这些安全威胁，才能采取相应的安全措施进行防范。

通常，在开放的网络环境中，可能面临以下的安全威胁。

(1) 身份假冒：一个实体通过身份假冒而伪装成另一个实体，威胁源是用户或程序。

(2) 非法连接：在网络实体与网络资源之间建立非法逻辑连接，威胁源是用户或程序。

(3) 非授权访问：入侵者违反访问控制规则越权访问网络资源，威胁源是用户或程序，威胁对象是各种网络资源。

(4) 拒绝服务：拒绝为合法的用户提供正常的网络服务，威胁源是用户或程序。

(5) 操作抵赖：用户否认曾发生过的数据报发送或接收操作，威胁源是用户或程序。

(6) 信息泄露：未经授权的用户非法获取了信息，造成信息泄密，威胁源是用户或程序，威胁对象是网络通信中的数据报或数据库中的数据。

(7) 通信业务流分析：入侵者通过观察和分析通信业务流(如信源、信宿、传送时间、频率和路由等)获得敏感信息，威胁源是用户或程序，威胁对象是网络通信中的数据报。

(8) 数据流篡改：对正确的数据报序列进行非法修改、删除、重排序或重放，威胁源是用户或程序，威胁对象是网络通信中的数据报。

(9) 数据篡改或破坏：对网络通信中的数据报和数据库中的数据进行非法修改或删除，威胁源是用户或程序，威胁对象是网络通信中的数据报或数据库中的数据。

(10) 信息推测：根据公布的概要信息(如统计数据、摘要信息等)来推导出原有信息中的数据值，威胁源是用户或程序，威胁对象是数据库中的数据。

(11) 程序篡改：篡改或破坏操作系统、通信软件或应用软件，威胁源是用户或程序，威胁对象是系统中的程序。

1.2.2　TCP/IP 协议安全弱点

在制定 TCP/IP 协议之初，并没有过多地考虑安全问题。随着 TCP/IP 协议的广泛应用，尤其成为互联网的基础协议后，TCP/IP 协议暴露出一些安全弱点，被攻击者利用作为攻击网络系统的重要手段。

TCP/IP 协议的安全弱点主要表现在两个方面。一是没有提供任何安全机制，如数据保密性、数据完整性以及身份真实性等保证机制，不能直接用于建立安全通信环境，必须通过附加安全协议来提供安全机制和安全服务，如 IP 安全(IPSec)协议、安全套接层(SSL)协议等都是基于 TCP/IP 协议的安全协议。二是本身有安全隐患，往往被攻击者利用作为攻击网络系统的一种手段，如 IP 地址欺骗、ICMP Echo flood、TCP SYN flood 和 UDP flood 攻击等，它们大都属于拒绝服务(DoS)攻击。

所谓 DoS 攻击是指非法占用和消耗一个系统资源，使该系统不能提供正常的服务，造成该系统暂时瘫痪，严重时可能引起系统崩溃。DoS 攻击有很多方法，其中 ICMP Echo flood、TCP SYN flood 和 UDP flood 等都是基于 TCP/IP 协议的 DoS 攻击。下面简要介绍 ICMP Echo flood 和 TCP SYN flood 攻击的基本原理。

1. ICMP Echo flood 攻击

ICMP Echo flood 攻击是一种常见的 DoS 攻击，它利用了 ICMP 中的回送(Echo)请求/响应报文实现 DoS 攻击。

ICMP Echo 报文主要用于测试网络目的节点的可达性。源节点向某一指定的目的主机发送 ICMP Echo 请求报文，目的节点收到请求后必须使用 ICMP Echo 响应报文进行响应。在 TCP/IP 实现系统中，Ping 命令就是利用这种 ICMP Echo 报文来测试目的可达性的。

由于一个主机所创建的接收缓冲区总是有限的，如果攻击者在短时间内向一个主机发送大量的 ICMP Echo 请求报文，则会造成该主机的接收缓冲区阻塞和溢出，使它无法接收其他正常的处理请求，于是便产生拒绝服务，造成该主机的网络功能暂时瘫痪。

2. TCP SYN flood 攻击

TCP SYN flood 攻击是一种常见的 DoS 攻击，它利用 TCP 协议在建立连接时的“三次握手”过程实现 DoS 攻击。

TCP 协议为什么要通过“三次握手”过程建立连接呢？主要为了防止因 TCP 报文的延迟和重传可能带来的不安全因素。由于 TCP 报文是在 IP 通信子网上进行传输的，如果通信子网比较拥挤，则 TCP 报文将被延迟，进而产生重复的 TCP 报文。对于 TCP 数据报文，可以通过报文中的序号滤除重复的 TCP 报文。对于 TCP SYN 报文(建立连接)和 TCP FIN 报文(关闭连接)，重复的 TCP 报文将带来一定的安全隐患。例如，在电子交易中，一个客户与银行建立一个 TCP 连接，客户通知银行给某个商家的账户里转入一大笔款，然后便释放该连接。如果在建立连接时产生了重复的 TCP SYN 报文和数据报文，并因网络拥挤被暂存在某个路由器上，在该连接释放后，这些被重复的报文却又顺序地到达目的端，请求建立一个新的连接并再次转账，结果给客户造成了很大的损失。因此，