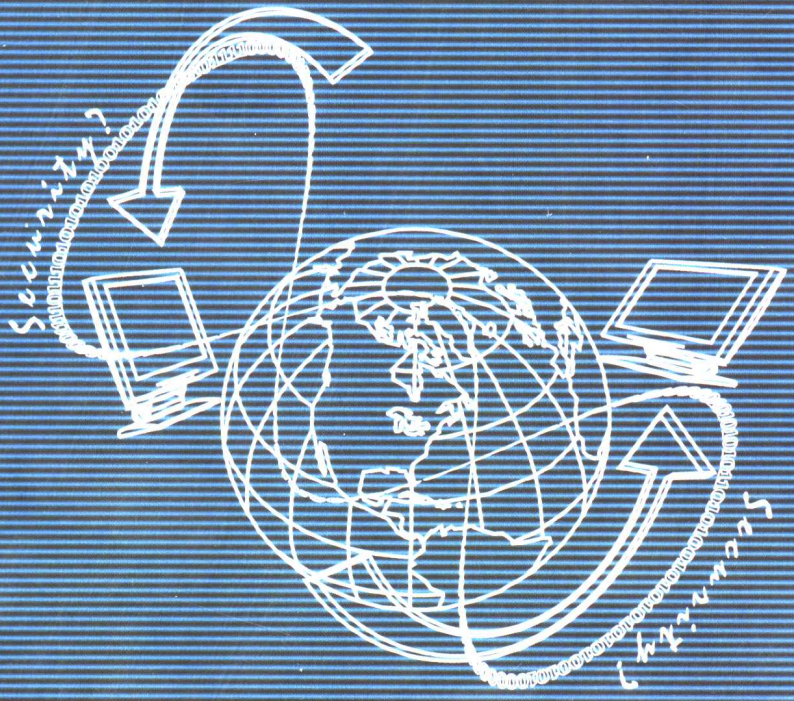
信息与通信技术

国防科工委"十五"规划教材

网络与信息安全

●蔡皖东 编著



西北工业大学出版社
北京航空航天大学出版社　北京理工大学出版社
哈尔滨工业大学出版社　哈尔滨工程大学出版社

国防科工委“十五”规划教材. 信息与通信技术

网络与信息安全

蔡皖东　编著

西北工业大学出版社

内容简介

本书从理论和实践相结合的角度，系统地介绍了网络信息安全的基本理论和应用技术。

全书分为上、中、下三篇共 11 章。上篇介绍网络信息安全基础，包括网络信息安全概论、网络信息安全威胁、密码技术、网络信息安全标准和模型等内容；中篇介绍信息交换安全技术，包括信息交换安全技术概述、数据链路层安全协议、网络层安全协议、传输层安全协议、应用层安全协议等内容；下篇介绍网络系统安全技术，包括网络系统安全技术概述、网络防护技术、网络检测技术、系统容灾技术等内容。

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，也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

网络与信息安全/蔡皖东编著. —西安：西北工业大学出版社，2004.4
国防科工委"十五"规划教材．信息与通信技术
ISBN 7-5612-1599-1

Ⅰ.网… Ⅱ.蔡… 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(2003)第 043914 号

网络与信息安全

蔡皖东 编著
责任编辑 王 璐 季 强
责任校对 耿明丽
西北工业大学出版社出版发行
西安市友谊西路 127 号(710072)
发行部电话：029-88493844
http://www.nwpup.com
西安东江印务有限公司印制 各地书店经销
开本：787 mm×960 mm 1/16
印张：23.5 字数：505 千字
2004 年 4 月第 1 版 2004 年 4 月第 1 次印刷
印数：1～3 000 册
ISBN 7-5612-1599-1 定价：32.00 元

总　序

国防科技工业是国家战略性产业，是国防现代化的重要工业和技术基础，也是国民经济发展和科学技术现代化的重要推动力量。半个多世纪以来，在党中央、国务院的正确领导和亲切关怀下，国防科技工业广大干部职工在知识的传承、科技的攀登与时代的洗礼中，取得了举世瞩目的辉煌成就。研制、生产了大量武器装备，满足了我军由单一陆军，发展成为包括空军、海军、第二炮兵和其他技术兵种在内的合成军队的需要，特别是在尖端技术方面，成功地掌握了原子弹、氢弹、洲际导弹、人造卫星和核潜艇技术，使我军拥有了一批克敌制胜的高技术武器装备，使我国成为世界上少数几个独立掌握核技术和外层空间技术的国家之一。国防科技工业沿着独立自主、自力更生的发展道路，建立了专业门类基本齐全，科研、试验、生产手段基本配套的国防科技工业体系，奠定了进行国防现代化建设最重要的物质基础；掌握了大量新技术、新工艺，研制了许多新设备、新材料，以“两弹一星”、“神舟”号载人航天为代表的国防尖端技术，大大提高了国家的科技水平和竞争力，使中国在世界高科技领域占有了一席之地。党的十一届三中全会以来，伴随着改革开放的伟大实践，国防科技工业适时地实行战略转移，大量军工技术转向民用，为发展国民经济作出了重要贡献。

国防科技工业是知识密集型产业，国防科技工业发展中的一切问题归根到底都是人才问题。50 多年来，国防科技工业培养和造就了一支以“两弹一星”元勋为代表的优秀的科技人才队伍，他们具有强烈的爱国主义思想和艰苦奋斗、无私奉献的精神，勇挑重担，敢于攻关，为攀登国防科技高峰进行了创造性劳动，成为推动我国科技进步的重要力量。面向新世纪的机遇与挑战，高等院校在培养国防科技人才，生产和传播国防科技

新知识、新思想，攻克国防基础科研和高技术研究难题当中，具有不可替代的作用。国防科工委高度重视，积极探索，锐意改革，大力推进国防科技教育特别是高等教育事业的发展。

高等院校国防特色专业教材及专著是国防科技人才培养当中重要的知识载体和教学工具，但受种种客观因素的影响，现有的教材与专著整体上已落后于当今国防科技的发展水平，不适应国防现代化的形势要求，对国防科技高层次人才的培养造成了相当不利的影响。为尽快改变这种状况，建立起质量上乘、品种齐全、特点突出、适应当代国防科技发展的国防特色专业教材体系，国防科工委全额资助编写、出版200种国防特色专业重点教材和专著。为保证教材及专著的质量，在广泛动员全国相关专业领域的专家学者竞投编著工作的基础上，以陈懋章、王泽山、陈一坚院士为代表的100多位专家、学者，对经各单位精选的近550种教材和专著进行了严格的评审，评选出近200种教材和学术专著，覆盖航空宇航科学与技术、控制科学与工程、仪器科学与工程、信息与通信技术、电子科学与技术、力学、材料科学与工程、机械工程、电气工程、兵器科学与技术、船舶与海洋工程、动力机械及工程热物理、光学工程、化学工程与技术、核科学与技术等学科领域。一批长期从事国防特色学科教学和科研工作的两院院士、资深专家和一线教师成为编著者，他们分别来自清华大学、北京航空航天大学、北京理工大学、华北工学院、沈阳航空工业学院、哈尔滨工业大学、哈尔滨工程大学、上海交通大学、南京航空航天大学、南京理工大学、苏州大学、华东船舶工业学院、东华理工学院、电子科技大学、西南交通大学、西北工业大学、西安交通大学等，具有较为广泛的代表性。在全面振兴国防科技工业的伟大事业中，国防特色专业重点教材和专著的出版，将为国防科技创新人才的培养起到积极的促进作用。

党的十六大提出，进入21世纪，我国进入了全面建设小康社会、加快推进社会主义现代化的新的发展阶段。全面建设小康社会的宏伟目标，对国防科技工业发展提出了新的更高的要求。推动经济与社会发展，提

升国防实力，需要造就宏大的人才队伍，而教育是奠基的柱石。全面振兴国防科技工业必须始终把发展作为第一要务，落实科教兴国和人才强国战略，推动国防科技工业走新型工业化道路，加快国防科技工业科技创新步伐。国防科技工业为有志青年展示才华，实现志向，提供了缤纷的舞台，希望广大青年学子刻苦学习科学文化知识，树立正确的世界观、人生观、价值观，努力担当起振兴国防科技工业、振兴中华的历史重任，创造出无愧于祖国和人民的业绩。祖国的未来无限美好，国防科技工业的明天将再创辉煌。

张华祝

前　言

近几年，随着 Internet 的发展，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 21 世纪知识经济社会运行的必要条件和基础设施。由于计算机网络系统的开放性，以及现有网络协议和软件系统固有的安全缺陷，使任何一种网络系统都不可避免地、或多或少地存在一定的安全隐患和风险。特别是 Internet 在使用和管理上的无政府状态，使人们在享受网络所带来方便和效益的同时，也面临着网络信息安全方面的巨大挑战。各种计算机病毒和黑客攻击已经对网络安全构成严重的威胁，安全事故屡有发生，造成了巨大经济损失。由于人们的社会和经济生活越来越多地依赖于计算机网络，如电力系统、运输系统或其他重大基础设施等都与计算机网络密切相关，网络空间(Cyber Space) 正在成为网络恐怖主义分子发动信息战的主战场，通过攻击一个国家的网络基础设施和关键信息系统，将会对国家安全构成很大的威胁。可见，网络信息安全已经和一个国家的安全与利益紧密联系在一起了。

从国家安全的角度考虑，以网络空间为平台的信息对抗正在演化成新的战争样式，网络信息战、网络恐怖战争以及黑客大战等无一不反映出网络安全对一个国家的政治、军事、经济以及社会生活所产生的重要影响。随着网络攻击力和破坏性的增强，使网络安全面临着更加严峻的局面，已经引起国际上高度的重视。基于网络信息战和网络反恐怖战争的需要，世界上一些主要的信息大国都在采取积极的网络安全防御策略，投入大量的人力和物力培养信息战专门人才，成立信息战军种，研究信息战战法，开发网络攻击和防御技术，美国甚至还招募黑客专门研究和开发网络攻击武器及其防御方法。

随着我国 Internet 事业的发展和网络应用的普及，网络信息安全越来越重要，它已经成为电子商务网、电子政务网、电子金融网、企业信息网以及军用信息网等必备的网络基础设施。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，很多高校的相关专业都开设了网络信息安全的本科生或研究生课程，加强了对网络信息安全人才的培养。近年来，国内出版了一些有关网络信息安全技术方面的图书，但大多数都是技术手册类图书，难以满足教学的要求。

本书是作者基于多年的教学实践和研究成果编写而成的。在内容安排和组织结构上，考虑到网络信息安全技术的内涵和特点，将全书分为上、中、下三篇，共11章。上篇介绍网络信息安全基础，共有4章。第1章为网络信息安全概论，包括OSI网络体系结构及其安全性、TCP/IP及其安全性和网络信息安全基础等内容；第2章为网络信息安全威胁，包括分布式拒绝服务攻击、缓冲区溢出攻击、IP欺骗攻击和计算机病毒等内容；第3章为密码技术，包括对称密码算法、非对称密码算法、数字签名算法、单向散列函数和身份认证技术等内容；第4章为网络信息安全标准和模型，包括网络信息安全标准概况、信息技术安全评估公共准则、系统安全工程能力成熟模型、信息安全准则的应用和信息安全模型等内容。中篇讲述信息交换安全技术，共有4章。第5章为数据链路层安全协议，包括局域网安全协议和远程通信安全协议等内容；第6章为网络层安全协议，包括IPSec安全体系结构、安全联盟、安全协议、密钥管理和IPSec协议的应用等内容；第7章为传输层安全协议，包括SSL握手协议、SSL记录协议、SSL支持的密码算法、SSL协议安全性分析和SSL协议的应用等内容；第8章为应用层安全协议，包括PGP，S-MIME协议和S-HTTP等内容。下篇讲述网络系统安全技术，共有3章。第9章为网络防护技术，包括接纳控制技术和防火墙技术等内容；第10章为网络检测技术，包括安全漏洞扫描技术和网络入侵检测技术等内容；第11章为系统容灾技术，包括基于数据备份的系统容灾技术、基于磁盘容错的系统容灾技术、基于集群系统的系统容灾技术、基于NAS的系统容灾技术和基于SAN的系统容灾技术等内容。

本书强调理论联系实际，尽量避免理论与实际相脱节。在讲述网络信息安全理论的同时，还介绍了有关网络信息安全产品及其应用技术，以便于读者理解和掌握，也有利于自学。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。

由于不同专业在课程设置、授课对象、学时数以及教学大纲上可能存在一定的差异，全书的内容安排和组织结构分成三篇，每篇自成体系，既保持了内容的系统性和完整性，又有一定的可伸缩性，因此便于教师根据教学实际需要有选择地组织教学。

由于作者水平有限，书中难免存在不足之处，欢迎广大读者批评指正。

编著者

2002 年于西安

国防科工委“十五”规划教材编委会

（按姓氏笔画排序）

目　录

上篇　网络信息安全基础

中篇 信息交换安全技术

下篇 网络系统安全技术