HZ BOOKS
华章教育

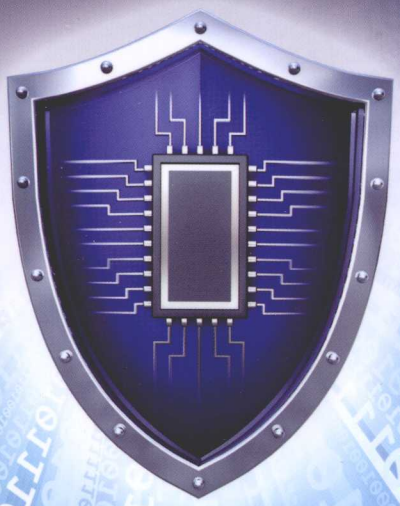
高等院校信息安全专业规划教材

网络安全技术教程

Network Security

Principles and Practices

吴英 ◎ 编著



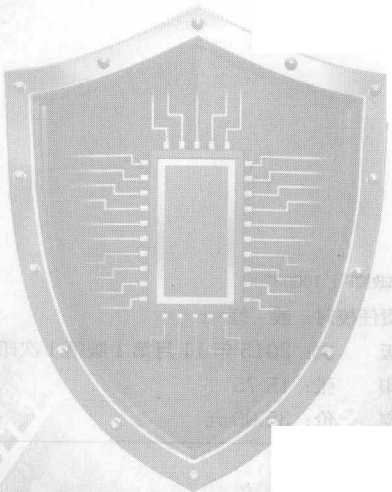
机械工业出版社
China Machine Press

网络安全技术教程

Network Security

Principles and Practices

吴英◎ 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络安全技术教程 / 吴英编著 . —北京：机械工业出版社，2015.10
（高等院校信息安全专业规划教材）

ISBN 978-7-111-51741-2

I. 网… II. 吴… 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（2015）第 239714 号

本书分为基础知识与编程实践两部分，在系统地讨论了网络安全概述、数据加密与认证技术、网络通信与应用安全技术、访问控制与防火墙技术、网络攻防与入侵检测技术、恶意代码与计算机病毒防护技术的基础上，以培养读者的网络安全软件编程能力为目标，给出了 6 个“近似实战”的网络安全软件编程题目。本书力求做到：结合网络安全课程的教学过程，通过完成实际的网络安全软件编程题目，加深对网络安全原理与实现方法的理解，逐步提高学生的网络软件编程能力。

本书内容贴近网络安全技术的最新发展，采用理论知识与编程实践相结合的方法，循序渐进地引导读者掌握网络安全相关知识。全书结构清晰，概念准确，语言流畅，涵盖了网络安全技术的主要知识点。

本书既可作为高等院校的计算机、网络工程、软件工程、信息安全、物联网工程及相关专业的研究生、本科生学习网络安全与网络软件编程技术的教材，也可作为网络安全与网络软件研发人员学习网络安全技术的参考资料。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：李 艺 责任校对：殷 虹
印 刷：中国电影出版社印刷厂 版 次：2015 年 11 月第 1 版第 1 次印刷
开 本：185mm×260mm 1/16 印 张：15.75
书 号：ISBN 978-7-111-51741-2 定 价：35.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：(010) 88378991 88361066 投稿热线：(010) 88379604
购书热线：(010) 68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前　言

随着计算机网络广泛应用于社会生活的各个领域，特别是在政府部门、金融机构、企事业单位与军事部门的应用，支持各种信息系统的计算机网络的地位变得越来越重要。小到家庭网络，大到电子政务网、电子商务网、金融网络、教育科研网，以及全国各地的电信网络、有线电视网络，整个社会对计算机网络的依赖程度越来越大。网络正在改变人们的工作、生活与思维方式，并对提高人们的生活质量产生了重要的影响。随着互联网、移动互联网、物联网技术与应用的快速发展，计算机网络的规模不断扩大、结构日趋复杂，这也对网络的可靠性与安全性提出越来越高的要求。

计算机网络在给广大用户带来方便的同时，也必然会给个别不法分子提供可乘之机。例如，不法分子可能通过网络非法获取政治、经济、军事、科技方面的情报，或进行信息伪造、金融诈骗、网络攻击等犯罪活动。计算机网络可能引起侵犯个人隐私的法律或道德问题，例如，发表不负责任的言论或损害他人利益的信息。另外，计算机网络还可能引起知识产权、著作权等方面的纠纷。网络安全概念涉及的内容很广泛，既包括用于解决网络应用中的安全威胁的各种技术或管理手段，也包括这些安全威胁本身以及相关活动。编者根据自己多年的教学与科研经验编写本书，希望为读者提供一本既能涵盖网络安全基础知识，又能反映网络安全技术发展现状的教材。

本书分为两部分：基础知识与编程实践。基础知识部分包括第 1 ～ 6 章（建议 24 学时），其中，第 1 章是网络安全概述，包括基本概念、安全体系与研究内容，是全书的基础（建议 4 学时）；第 2 章介绍数据加密与认证技术，包括对称加密、公钥加密、消息认证、密钥分发等技术（建议 4 学时）；第 3 章介绍网络通信与应用安全技术，包括数据链路层、网络层、传输层、应用层等的安全技术（建议 4 学时）；第 4 章介绍访问控制与防火墙技术，包括防火墙、NAT、物理隔离等技术（建议 4 学时）；第 5 章介绍网络攻防与入侵检测技术，包括网络攻击、入侵检测、计算机取证等技术（建议 4 学时）；第 6 章介绍恶意代码与计算机病毒防护技术，包括计算机病毒、网络蠕虫、木马与垃圾邮件等，以及恶意代码防护技术（建议 4 学时）。

编程实践部分包括第 7 ～ 12 章（建议 12 学时），其中，每章对应一个网络安全软件编程题目，包括编程要求、相关知识、程序设计、程序测试与扩展提高。第 7 章的编程题目是基于字符映射表的消息加密程序。第 8 章的编程题目是基于 DES 的消息加密程序。第 9 章的编程题目是基于 MD5 的文件完整性检测程序。第 10 章的编程题目是基于 RSA 的文件安全检测程序。第 11 章的编程题目是基于 OpenSSL 的 Web 服务器程序。

第 12 章的编程题目是基于图片的信息隐藏程序。任课教师可选择 2 ～ 3 个编程题目讲授编程思路，并且作为编程作业供学生在课下完成。

本书的前言、第 1 ～ 6 章与附录由吴英编写，第 7、8 与 11 章由王盛编写，第 9、10 与 12 章由刘婷婷编写。全书由吴英统稿。

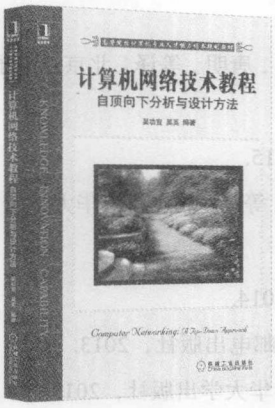
本书在编写过程中得到吴功宜教授、徐敬东教授、张建忠教授的很多帮助，在此表示衷心的感谢。

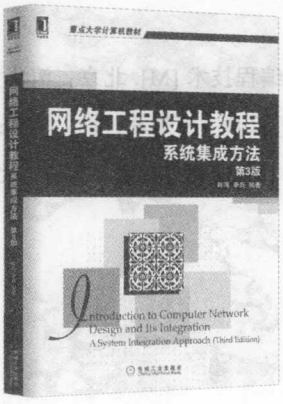
由于编者水平有限，疏漏与不妥之处在所难免，敬请读者批评指正。

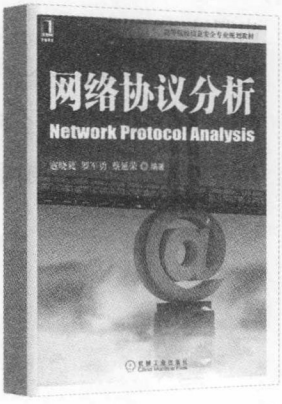
编者

2015 年 7 月

推荐阅读







计算机网络技术教程——自顶向下分析与设计方法

作者：吴功宜 等 ISBN：978-7-111-28297-6 定价：33.00元

计算机网络技术教程例题解析与同步练习

作者：吴英 ISBN：978-7-111-27675-3 定价：25.00元

计算机网络应用软件编程技术

作者：吴英 ISBN：978-7-111-30756-3 定价：23.00元

网络管理技术教程

作者：吴英 等 ISBN：978-7-111-34187-1 定价：33.00元

网络工程设计教程：系统集成方法 第3版

作者：陈鸣 等 ISBN：978-7-111-46695-6 定价：45.00元

网络协议分析

作者：寇晓蕤 等 ISBN：978-7-111-26832-1 定价：33.00元

推荐阅读

计算机网络：自顶向下方法（原书第6版）

作者：James F. Kurose Keith W. Ross
译者：陈鸣
书号：978-7-111-45378-9
定价：79.00元

计算机网络：系统方法（原书第5版）

作者：Larry L. Peterson Bruce S. Davie
译者：王勇 张龙飞 李明 薛静锋 等
书号：978-7-111-49907-7
定价：99.00元

计算机网络：一种开源的设计实现方法

作者：Ying-Dar Lin 等
译者：陈向阳 等 李琼 审校
书号：978-7-111-42604-2
定价：79.00元

计算机网络教程：自顶向下方法

作者：Behrouz A. Forouzan Firouz Mosharraf
译者：张建忠 等
书号：978-7-111-40088-2
定价：99.00元

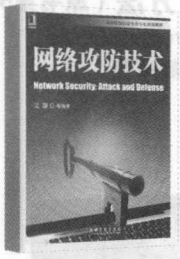
推荐阅读

信息安全导论

作者：何泾沙 ISBN：978-7-111-36272-2 定价：33.00元

金融信息安全工程

作者：李改成 ISBN：978-7-111-28262-4 定价：35.00元

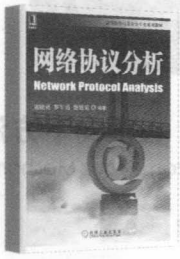


网络攻防技术

作者：吴灏 ISBN：978-7-111-27632-6 定价：29.00元

数字图像隐写分析

作者：刘粉林 刘九芬 罗向阳 ISBN：978-7-111-30517-07 定价：29.00元



网络协议分析

作者：寇晓蕤 罗军勇 蔡延荣 ISBN：978-7-111-26832-1 定价：33.00元

目　录

第二部分 编程实践

第一部分　基础知识

第 1 章　网络安全概述

随着计算机网络的快速发展和广泛应用，网络安全问题越来越受到网络用户的重视。本章在讨论网络安全重要性的基础上，系统地介绍了网络面临的主要安全威胁、主要的网络安全技术，以及网络安全方面的标准。

1.1　网络安全的背景

1.1.1　网络安全的重要性

计算机网络的应用对经济、文化、教育、科学等领域有重要影响。互联网技术发展促进电子商务技术的成熟，大量的商业信息与资金通过网络在世界各地流通。政府上网工程的实施使各级政府、部门之间可通过网络实现网上办公，以及通过网络向普通民众提供政务信息。远程教育使得数以千万计的学生可以在不同的地方，通过网络进行课堂学习、查阅资料与提交作业。电子邮件、即时通信等服务的出现为用户提供了新的交流途径。网络正在改变人们的工作、生活与思维方式，提高人们的生活质量。

虽然计算机网络的应用对社会发展有着积极作用，但我们还必须注意到它所带来的负面影响。用户可通过网络快速地获取、传输与处理各种信息，涉及政治、经济、教育、科学与文化等领域。但是，计算机网络在给广大用户带来方便的同时，也必然会给个别不法分子带来可趁之机。例如，犯罪分子可通过网络窃取商业机密、传播虚假信息、执行网络攻击等。网络用户也可能在无意中侵犯他人的隐私或发表不恰当的言论。另外，计算机网络还可能引起知识产权、著作权等方面的纠纷。

目前，计算机犯罪正在引起整个社会的普遍关注，而计算机网络已成为犯罪分子攻击的重点。计算机犯罪是一种高技术型犯罪，其隐蔽性对网络安全构成很大威胁。根据有关统计资料表明，计算机犯罪案件以每年超过 100% 的速度增长，网站被攻击的事件以每年 10 倍的速度增长。从 1986 年发现首例计算机病毒以来，计算机病毒的类型和数量一直在逐年快速增长。根据国家计算机病毒应急处理中心发布的病毒预报，每周都有大量新病毒以及旧病毒的变种出现。攻击者在世界各地疯狂寻找攻击网络的机会，他们的活动几乎到了无孔不入的地步，政府网络与金融系统已成为这些人的主要目标。

黑客（hacker）的出现是信息社会不容忽视的现象。黑客一度被认为是计算机狂热者的代名词，他们大多是对编程有浓厚兴趣的大学生。后来，人们对黑客有了进一步的认识：黑客中的大部分人不伤害别人，但是也会做一些不该做的事情；部分黑客不顾法律与道德的约束，为了寻求刺激、被非法组织收买或出于报复心理，而肆意攻击与破坏

一些企业、组织的网络。近年来，黑客攻击的目的从最初的破坏网站、阻止网络服务，转变为盗取用户密码、银行账号的有组织的经济犯罪。

互联网的广泛应用开始影响企业网的开发模式，用户希望在任何地方都可以方便地访问企业网中的计算机。但是，对于企业来说，将自己的企业网连入互联网也可能是一场噩梦。大多数的企业都有一些重要的内部资料，如市场策略报告、客户名单、财务报表、产品开发计划等，这些经济情报的泄露对企业是致命的危险。如果企业网中的计算机遭到攻击，轻者会造成内部信息丢失或被篡改，重者会导致整个管理信息系统瘫痪，这些都会给相关企业带来严重的经济损失。

电子商务的兴起使得对网站的安全性要求越来越高。2001 年，在美国的很多知名网站被袭事件中，Amazon、eBay、Yahoo 等网站接连遭到黑客攻击，这些网站大多被迫中断服务长达几个小时，据估算造成的经济损失高达 12 亿美元。网站被袭事件使人们对网络安全的信心受到重创。这种以瘫痪网络为目标的攻击，破坏性大、造成危害速度快、影响范围广，并且难于防范与追查。攻击者本身所冒的风险非常小，甚至在攻击开始前就已消失得无影无踪，被攻击者几乎没有对其实施追踪的可能。

近年来，工业控制系统正在成为新的攻击热点。2010 年 6 月，“震网”成为第一个将目标锁定在工业控制网络的计算机病毒。2012 年 5 月，“火焰”被发现在目标网络中潜伏长达 5 年之久。随着过程控制技术在工业中的广泛应用，很多大型企业在整个生产过程中采用该技术。对于那些涉及国家安全的企业（如核电站、兵工厂等），它们的生产过程自动控制与企业管理系统，必定会成为“某些人”通过网络入侵，窃取情报和监控的对象。目前，过程控制已开始应用于智能楼宇、城市供电等领域，攻击者完全可以采取网络攻击的手段，破坏或干扰这些控制系统，这样可能对社会稳定造成巨大影响。

进入互联网与移动互联网时代，过去我们认为可以信赖的办公室、家庭与卧室，以及保护我们不被外人窥探的篱笆、院墙、门窗与防盗门已无法遮挡外部的视线，传统意义上的私密空间已经发生改变。过去写在日记中的文字、贴在影集中的照片，在数字化之后都会成为在网络上传输的数据。隐私保护出现了严重挑战，这绝不是危言耸听。美国东北大学的研究者通过跟踪研究 10 万名欧洲手机用户，分析 1600 万条通话记录与位置信息，得出的结论是：预测某人在未来某时刻的位置准确率可达到 93.6%。

恰恰是在现代隐私权概念的原产地——美国，曝光出最严重的互联网环境中的侵犯隐私丑闻。2013 年 7 月，美国前 FBI 雇员披露美国政府侵犯公民隐私权，威胁各国信息安全的“棱镜门”事件。在过去的 6 年中，美国国家安全局的“棱镜（PRISM）”绝密电子监听计划，通过进入 Microsoft（微软）、Google（谷歌）、Apple（苹果）、Yahoo（雅虎）等网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频与照片等资料。2009 年以来，美国黑客针对中国网络发动大规模攻击，攻击目标主要是主干路由器与各种服务器，窃取的信息主要是用户数据与身份信息。由此可见，隐私保护已成为网络安全研究必须面对的问题。