世界著名计算机教材精选

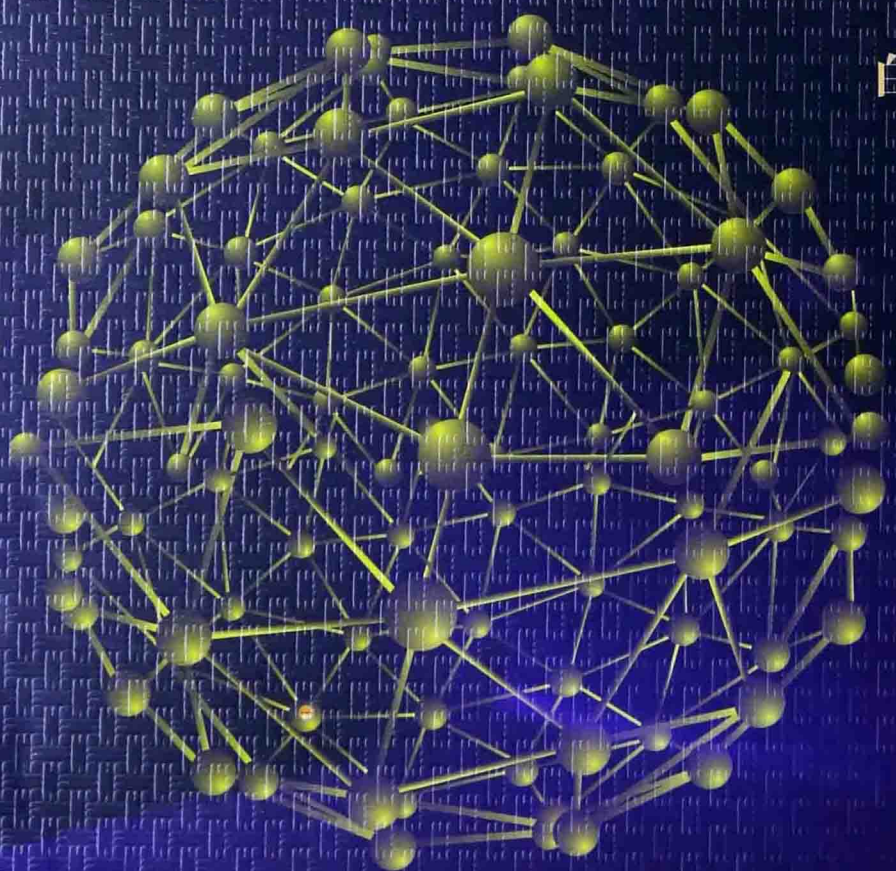
PEARSON

网络安全基础

应用与标准（第5版）

William Stallings 著

白国强 等译



NETWORK SECURITY ESSENTIALS APPLICATIONS AND STANDARDS

Fifth Edition

PEARSON

清华大学出版社

世界著名计算机教材精选

网络安全基础

应用与标准

（第5版）

William Stallings 著

白国强 等译

清华大学出版社

北京

Simplified Chinese edition copyright ©**2014 by PEARSON EDUCATION ASIA LIMITED and TSINGHUA UNIVERSITY PRESS.**

Original English language title from Proprietor's edition of the Work.

Original English language title: Network Security Essentials:Applications and Standards, Fifth Edition **by** William Stallings © **2013**

EISBN: 9780133370430

All Rights Reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Addison Wesley.

This edition is authorized for sale only in the People's Republic of China (excluding the Special Administrative Region of Hong Kong and Macao).

本书中文简体翻译版由 Pearson Education（培生教育出版集团）授权给清华大学出版社在中国境内(不包括中国香港、澳门特别行政区)出版发行。

北京市版权局著作权合同登记号　图字：01-2013-6755 号

本书封面贴有 Pearson Education（培生教育出版集团）激光防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

网络安全基础：应用与标准（第 5 版）/（美）斯托林斯（Stallings, W.）著；白国强等译. —北京：清华大学出版社，2014

（世界著名计算机教材精选）

书名原文：Network Security Essentials: Applications and Standards, 5e

ISBN 978-7-302-34807-8

Ⅰ. ①网…　Ⅱ. ①斯… ②白…　Ⅲ. ①计算机网络–安全技术–教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 301319 号

责任编辑：龙启铭
封面设计：何凤霞
责任校对：梁　毅
责任印制：何　芊

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 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：22.25　　**字　　数**：551 千字
版　　次：2014 年 5 月第 1 版　　**印　　次**：2014 年 5 月第 1 次印刷
印　　数：1～2000
定　　价：49.00 元

产品编号：054405-01

作 者 介 绍

William Stallings 编写出版了 17 部著作，经修订再版累计超过 40 本，书籍的内容涉及计算机安全、计算机网络和计算机体系结构。他的作品已经无数次出现在 ACM 和 IEEE 出版物中，包括 *Proceedings of the IEEE* 和 *ACM Computer Reviews*。

他已经 11 次获得了由教材与学术作者协会颁发的最佳计算机科学教材年度奖。

在过去的 30 年里，他曾在该领域的数个高科技企业中担任技术骨干、技术管理者和技术执行领导。他设计和实现了适用于从微型机到大型机的各种类型的计算机和操作系统，既基于 TCP 协议，又基于 OSI 协议。

在该领域超过 30 年工作的时间里，他一直是技术贡献者、技术管理者和一些高技术企业的运营者。在不同计算机和操作系统上，小到微计算机，大到大型机，他已经设计和实现了既基于 TCP/IP 的协议，又基于 OSI 的协议。他作为顾问，为政府部门、计算机及软件供应商和广大用户提供包括设计、选用和网络软件及产品的使用的咨询服务。

他创立和维护着计算机科学学生资源网站：WilliamStallings.com/studentSupport.html。该网站为计算机科学学生（和专业人士）在该领域的各个方面提供文档和网络连接。他是专注于密码学各个方面的学术性期刊 *Cryptologia* 的编委会成员。

Stallings 是麻省理工学院（MIT）计算机科学的博士及 Notre Dame 电气工程的学士。

译 者 序

由 William Stallings 编著的这本书已成为网络安全方面最重要、影响最广泛的教科书，2013 年第 5 版已出版发行。现在我们仍把它翻译为中文并推荐给读者，希望它在我国普及网络安全基础知识和培养网络与信息安全专业人才方面继续发挥应有作用。

正如译者在该书第 4 版序言中所说，在网络技术飞速发展、应用领域和范围迅猛扩大以及网络安全教学实践的时间还很短的今天，要编写一本既能赶上技术变化，又能包含成熟教学经验的网络安全教材是一件很困难的事情。与第 4 版相比，第 5 版的主要变化有：

（1）增加了新的一章（第 5 章）“网络访问控制和云安全”，使全书由原来的 11 章变成 12 章；

（2）对原第 6 章“无线网络安全”的内容进行了较大幅度的改写，增加了无线安全概述和移动设备安全两节内容，同时为保持原来篇幅，删减了无线应用协议的内容；

（3）极大地充实了“恶意软件”这一章内容并把其放在系统安全的最前面，以突显该章内容的重要性。

该版整体结构维持了第 4 版情况，即全书主体仍由三个部分共 12 章另加两个附录组成。与第 4 版一样，作者把一部分内容编辑为在线章节。这些内容未包括在印刷版中，它们被放在网上。限于篇幅，翻译时我们也未把这些内容包括在内。总体而言，与第 4 版相比，第 5 版的变化不如第 4 版与第 3 版相比那么大。

在该书第 4 版出版后的四年多里，云计算和云安全、智能手机的发明与迅速普及、网上支付以及网店的极速火爆是这一时期互联网最重要的新应用。在网络应用不断普及的情况下，网络安全越来越受到了人们的重视，尤其是去年在全球范围内曝光的重大窃听事件，把网络安全的重要性推到了前所未有的地位。相信该书的出版发行能够较好地满足读者对网络安全基础知识的需求。

网络安全的知识既包括一般原理性知识，也包括特定算法、协议和工业标准的内容。在该书涉及算法、协议和工业标准的内容中，除一部分是国际通行内容外，也有大量是国外政府公布的算法和标准。特别在可替换的密码算法方面，由于过去我国没有自己的算法标准，只能选讲国外算法。现在，我国政府已公布了我们自己的各种密码算法（SM2、SM3 和 SM4 等）标准。随着我国经济实力的提升和技术水平的提高，应该大力推广我们自己的算法和标准。我们应该有这样的自信。为此，建议使用该书作为教材的老师，在讲到密码算法和相关标准时可以考虑更多地讲授一些与我们自己有关的内容。

该书与作者的另一本书《密码学与网络安全》相辅相成。该书重点讲述网络安全的基础知识，《密码学与网络安全》重点讲述密码学内容。阅读该书并不需要太多的专门知识。对我国大学一、二年级本科生和对计算机网络知识有一般了解的读者完全可以阅读该书。

试读结束：需要全本请在线购买： www.ertongbook.com

参加该书部分初稿翻译的有赵振伟、邱爽和张丹，赵振伟参与了全书的统稿和修订。翻译过程中我们对原书中一些明显的错误做了改正，对打印错误做了更正翻译，对个别叙述不清楚的地方做了解释说明。清华大学出版社的龙启铭编辑对该书的翻译出版给予了大力支持和帮助，在此表示感谢。

由于译者水平有限，书中难免有错误和不妥之处，肯请读者批评指正。

译　者

2014年3月

于北京清华园

前　言

在这样一个全球电子互连、计算机病毒和电子黑客充斥、电子窃听和电子欺诈肆虐的时代，安全不再是问题的确已经过去。两大趋势使本书所讨论的内容显得尤为重要。第一，计算机系统及其网络互连的爆炸性增长已经增强了机构和个人对利用这些系统存储与交换信息的依赖程度。这样，进一步又使得人们意识到对保护数据和资源免遭泄露，保障数据和信息的真实性，以及保护基于网络的系统免受攻击等问题的必要性。第二，密码学和网络安全已经成熟，并正在开发实用而有效的应用来增强网络安全。

本书目的

本书的目的是对网络安全应用与标准提供一个实用的概览，重点介绍已广泛使用在Internet和公司网络中的应用和标准（尤其是Internet标准）。

第5版新增内容

自从第4版出版的4年以来，这个领域持续创新和提高。在第5版中，试图捕捉这些变化，同时仍能够广泛和全面地覆盖这个领域。在开始修订的时候，第4版的内容已经被许多讲授这门课程的教授以及在这个领域工作的教授详细审查了。结果是，在许多地方，叙述更加清楚和紧凑，图解效果也有所提高。

除了这些细化内容从而提高教学和用户友好程度外，整本书有许多改变的地方。所有章节的组织结构大体没有改变，但是许多内容被修订了，添加了一些新内容。最值得一提的改变如下：

- **网络访问控制**：这是新增加的一章，提供了网络访问控制的概述，包括可扩展认证协议和IEEE 802.1X协议的简单介绍。
- **云安全**：也是新增加的一章，包括了云计算安全问题。
- **SHA-3**：在线章节，介绍了新的密码散列标准，SHA-3在2012年被采用。
- **移动设备安全**：移动设备安全已经成为企业网络安全的很重要的组成部分。新的一章介绍了这个话题。
- **恶意软件**：这一章节提供了跟第4版不同的视角。我们越来越多地看到后门/rootkit类型的恶意软件被社会工程安装所攻击而非蠕虫和病毒直接感染。网络钓鱼也越来越突出。这些趋势都在本书中覆盖了。
- **示例教学大纲**：这本书的内容一个学期内不容易学完。因此向教师提供了一些示例教学大纲，可以在有限的时间内（如16周或者12周）好好利用这本书。这些示例

教学大纲都是第1版讲授时的切身经验。

- **学习目标**：每一章都是从学习目标开始。

ACM/IEEE 2013 计算科学课程支持

这本书本意是为专业的读者而写。作为教科书，它可以作为密码学和网络安全、计算机工程、电气工程等专业大学生一个学期的课程教材。该版的改变之处原本是为 ACM/IEEE 2013 计算科学课程（CS2013）的草案提供支持。CS2013 为当前的推荐课程增加了信息保证和安全（IAS）作为计算科学领域的知识。CS2013 声明，由于 IAS 在计算科学教学中的关键作用，IAS 现在是推荐课程的一部分。CS2013 将所有的课程分为三类：核心层 1（所有内容都应被包含在该课程中），核心层 2（应该包括所有或者大部分话题），可选层（提供的深度和宽度可选）。在 IAS 领域，CS2013 推荐在核心层 1 和 2 中的基本概念和网络安全，密码内容是可选的。这本书涵盖了在 CS2013 列出的所有内容。

本书同样可以为自学者提供一个基本的参考书籍。

本 书 组 成

本书由如下三部分组成。

第一部分，密码学。简要概述密码算法和用于网络安全的密码协议，包括加密、散列函数、数字签名和密钥交换等。

第二部分，网络安全应用。介绍了各种重要网络安全工具和应用，包括 Kerberos、X.509v3 数字证书、可扩展认证协议、S/MIME、IPSec、SSL/TLS 和 IEEE 802.11i WiFi 安全等。

第三部分，系统安全。简述了系统级安全问题，包括网络入侵和病毒的威胁与对策，防火墙应用和可信系统等。

此外，本书还附有术语表、缩略语表和参考文献。每章包括了作业题、思考题、关键词、术语表、进一步阅读建议和推荐网址等。还有，每章都为教师提供了题库。

教师教学辅助材料

这本书的主要目标是为教师教学提供一个有效的教学工具。这个目标在本书的结构和支持材料上都有反映。为帮助教师教学，还提供了下列材料：

- **习题答案**：包括每章后的思考题和习题的答案。
- **项目指南**：建议的项目作业，随后按一定分类列出。
- **PPT 幻灯片**：适合授课用的各章 PPT。
- **PDF 文件**：书中所有图和表的 PDF 文件。
- **题库**：每一章节的问题集合以及答案。

- **实例教学大纲**：这本书的内容一个学期内不容易学完。因此我们向老师提供了一些示例教学大纲，可以在有限的时间内好好利用这本书。这些示例教学大纲都是第 1 版讲授时的切身经验。

所有这些辅助材料都能够在本书的教师资源中心（Instructor Resource Center，IRC）找到，这可以通过链接 pearsonhighered.com/stallings，或通过单击本书网站“WilliamStallings.com/Crypto/Crypto5e.html”中的“Book Info and More Instructor Resources”按钮获得。要访问 IRC，通过如下网站

pearsonhighered.com/educator/replocator/requestSalesRep.page

请与 Pearson Hall 经销商的地方代表联系，或直接拨 1-800-526-0485，找 Pearson Hall Faculty Services 联系。

在 WilliamStallings.com/NetworkSecurity 配套网站上包含下列内容：

- 到使用这本书作为教材的其他课程的网站链接。
- 使用这本书的其他老师的邮件列表。

项目和其他学生练习

对很多教师来说，讲授密码学或安全课程的一个重要组成是项目或一组项目，学生通过完成这些项目可以得到直接的训练，以加深学生对书中概念的理解。教师手册对项目的组成提供了不同程度的支持。该书不仅包括如何构思和指定这些项目，也包括了一组能够广泛覆盖教材内容的项目建议：

- **黑客项目**：设计这个练习的目的是希望阐明入侵检测和保护中的关键问题。
- **实验练习**：能够涉及本书概念的一系列编程和实验项目。
- **研究项目**：一系列的研究型作业，引导学生就 Internet 的某个特定题目进行研究并撰写一份报告。
- **编程项目**：能够涉及广泛主题的一系列编程项目。这些项目都可以用任何语言在任何平台上实现。
- **实际安全评估**：一组用于检查当前一个已存在组织的安全设备及实际状况。
- **防火墙项目**：提供了一个可移动网络防火墙可视化模拟器，以及为讲授防火墙基本概念而准备的习题。
- **案例学习**：真实世界案例的集合，包括学习目标、案例描述和一系列案例讨论问题。
- **写作作业**：按章给出的一组写作作业。
- **阅读/报告作业**：来自文献的一组论文，每章一篇，可以指定让学生阅读，然后撰写一份简短的报告。

各种各样的项目集和其他学生练习，可以把这本书作为丰富学习经验的一部分，同时可以裁剪教学计划，从而满足老师和学生的特殊要求。更多详细内容见附录 B。

学生在线文档

在第5版中，数量巨大的第一手辅助材料按照下面的分类放在配套网站WilliamStallings.com/NetworkSecurity（单击学生资源链接）上，包括按章组织的相关链接列表以及本书的勘误表。

- **在线章节**：为限制书的篇幅和成本，该书有三章以PDF文件格式提供。一章是SHA-3，另一章是SNMP安全，最后一章是关于法律和伦理问题的。
- **在线附录**：有大量支持教材的内容，把它们包括在印刷本中是不适宜的。对有兴趣的同学，有许多在线附录涵盖了这些主题。
- **作业习题和答案**：为帮助学生理解内容，提供了一套相对独立的家庭作业习题，并附答案。这能让学生检查自己对内容的理解。
- **核心论文**：为进一步阅读，提供了许多篇来自专业文献的论文，其中有很多是不容易找到的。
- **支持性文档**：不少在教材参考文献中指出的文档也通过在线提供了。

本书与《密码学与网络安全》的关系

本书改编自《密码学与网络安全（第6版）》（CNS6e）。CNS6e更侧重于密码编码学、密钥管理、用户认证等内容的阐述，包括详细的算法分析和重要的数学基础，全书将近500页。本书（NSE5e）仅在第2章到第4章简要概述这些内容。同时，NSE5e不仅包括了CNS6e其余的全部内容，也增加了CNS6e中没有的SNMP安全。因此，NSE5e更希望为那些主要兴趣在网络安全应用，而又不需要或不希望对密码编码学理论与原理涉足更深内容的专业人士或学院课程提供一本教材。

致　　谢

本书新版得益于不少专业人士的慷慨奉献。下列人士审阅了本书全部或大部分手稿：Marius Zimand（Towson State University）、Shambhu Upadhyaya（University of Buffalo）、Nan Zhang（George Washington University）、Dongwan Shin（New Mexico Tech）、Michael Kain（Drexel University）、William Bard（University of Texas）、David Arnold（Baylor University）、Edward Allen（Wake Forest University）、Michael Goodrich（UC-Irvine）、Xunhua Wang（James Madison University）、Xianyang Li（Iliinois Institute of Technology）和 Paul Jenkins（Brigham Young University）。

还要对很多提供一章或多章详细技术审查的人给予感谢：Martin Bealby、Martin Hlavac（Department of Algebra, Charles University in Prague, Czech Republic）、Martin Rublik（BSP Consulting and University of Economics in Bratislava）、Rafael Lara（President of Venezuela's

Association for Information Security and Cryptography Research)、Amitablh Saxena 以及 Michael Spatte（Hewlett-Pachard Company)。我要特别感谢 Nikhil Bhargava（IIT Delhi）对本书各章进行了详尽的审阅。

Nikhil Bhargava（IIT Delhi）建立了网上家庭作业及其答案。Dakota State University 的 Sreekanth Malladi 教授建立了黑客攻击练习。普渡大学的 Ruben Torres 建立了放在 IRC 上的实验室练习题。

下面是对项目作业做出贡献的人：Henning Schulzrinne（Columbia University)、Cetin Kaya Koc（Oregon State University）和 David Balenson（Trusted Information Systems and George Washington University)。Kim Mclaughlin 建立了测试包。

最后，我还要感谢负责本书出版的人们。所有这些人都出色地完成了他们的日常工作。他们包括我的编辑 Tracy Dunkelberger 和她的助理 Melinda Hagerty 与 Allison Michael，还有 Jake Warde 的监审。

试读结束：需要全本请在线购买：　www.ertongbook.com

目　录

第 2 部分　网络安全应用

试读结束：需要全本请在线购买： www.ertongbook.com