世界著名计算机教材精选

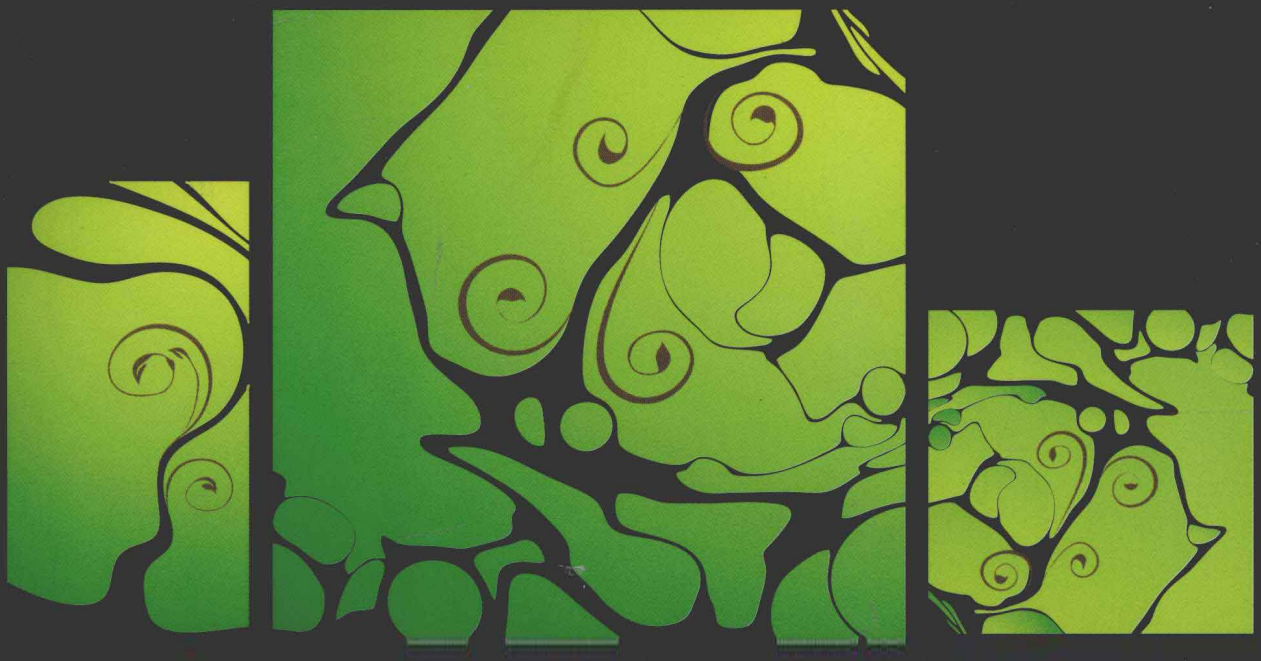
PEARSON

网络安全基础

应用与标准（第4版）

William Stallings 著

白国强 等译



Applications and Standards Fourth Edition

PEARSON Education

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4版）

William Stallings 著

白国强 等译

清华大学出版社

北京

EISBN:978-0-13-610805-4

图书在版编目(CIP)数据

网络安全基础:应用与标准:第 4 版/(美)斯托林斯(Stallings,W.)著;白国强等译. —北京:清华大学出版社,2011.1

(世界著名计算机教材精选)

书名原文:Network Security Essentials: Applications and Standards, Fourth Edition

ISBN 978-7-302-23916-1

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(2010)第 191875 号

责任编辑:龙啟铭

责任校对:焦丽丽

责任印制:李红英

出版发行:清华大学出版社 **地 址**:北京清华大学学研大厦 A 座

http://www.tup.com.cn **邮 编**:100084

社 总 机:010-62770175 **邮 购**:010-62786544

投稿与读者服务:010-62795954,jsjjc@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015,zhiliang@tup.tsinghua.edu.cn

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:185×260 **印 张**:22 **字 数**:528 千字

版 次:2011 年 1 月第 1 版 **印 次**:2011 年 1 月第 1 次印刷

印 数:1~3000

定 价:39.50 元

产品编号:037757-01

作 者 介 绍

William Stallings 已经在全面理解计算机安全、计算机网络和计算机架构的技术发展方面做出了突出贡献。他已是 17 部著作的作者，如果把修订版也算进去，则总共是该领域各方面 42 本书的作者。他的作品已经出现在相当多 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（Text and Academic Authors Association）颁发的最佳计算机科学教材年度奖。

在超过 30 年该领域工作的时间里，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。他在不同计算机和操作系统上，小到微计算机，大到大型机上，已经设计和实现了既基于 TCP/IP 的协议，又基于 OSI 的协议。作为顾问，在设计、选用和网络软件及产品的使用等方面，他一直服务于政府部门、计算机及软件供应商和大客户。

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，是 Notre Dame 电子工程的学士。

译 者 序

由 William Stallings 编著的这本书，已成为网络安全方面最重要的一本教科书。2007年笔者曾与其他人合作把本书第3版翻译为中文并推荐给读者。现在它的第4版也已出版发行，我们再次把它（第4版）翻译为中文，希望它仍能够作为我国高校相关课程的教材使用，或作为普通网络安全爱好者学习和了解网络安全基本知识的参考书。

该书第4版保持了其一贯的特点，即完全从实用的角度出发，尽量用较小的篇幅对网络安全解决方案中实际使用的主要算法、重要协议和系统管理方法等方面的原理做全面而详细的介绍。全书仍分为3大部分：第1部分为密码学，非常简要地介绍了常用的对称加密、消息认证和公钥密码等；第2部分为网络安全应用，介绍了各种重要网络安全工具和应用，包括密钥分配与用户认证、传输层安全、无线网络安全、电子邮件安全和IP安全等；第3部分为系统安全，简述了系统级安全问题，包括网络入侵、恶意软件和防火墙等。

与第3版相比，第4版变化很大，总结起来主要体现为如下几个方面。

1. 大幅度地调整了内容，包括：（1）在内容总量和一定篇幅下，作者采用“在线章节”（online chapters）的方法，直接删除了第3版中的部分章节和附录，把它们放在了网上；（2）增加了对随机数和伪随机数的介绍；（3）把第2部分网络安全应用的叙述由原来的自下而上顺序（从IP层到应用层及网络管理安全）改为自上而下（从用户认证到IP层安全）；（4）新增一章（第6章）专门介绍无线网络安全。

2. 改写和充实了大部分章节，主要包括：（1）调整部分章内叙述顺序，使其更符合初学者逻辑；（2）对材料的叙述更符合实际情况，如IEEE、NIST标准等；（3）增加和更新叙述，使介绍的内容尽可能地符合最新的网络安全实际状况，如改IPv4为IPv6；（4）引入用户认证概念；（5）删除了SET（安全电子交易），改为对安全盾（SSH）的介绍等。

3. 大量地充实了习题。与第3版比较，各章习题几乎都得到了很大的扩充，随着教学实践的进行，这充分说明该书作为教材，其教学经验得到了积累。

当前，互联网技术及其网络安全技术一直处于快速发展状态，网络安全教学实践的时间很短。这种情况下，编写一本既能赶上技术的变化，又能包含成熟教学经验的网络安全教材是一件很有挑战性的工作。该书系列版本的推出正反映了这种发展变化状况。笔者觉得，该书当前的第4版在既反映最新技术，又体现教学经验积累方面是成功的。当然，随着技术的发展和经验的积累，该书定会继续推出后续新版本。

第4版与原作者的另一本书《密码学与网络安全》相辅相成。与其相比，该书不仅省

去了学习部分密码算法需要的数学基础，也对密码算法的叙述更加简明扼要，以便把重点放在对网络安全协议的介绍上。因此，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。

参加该书部分初稿翻译的有马骁、李若绪和冉彤。翻译过程中，我们对原书中一些明显的错误做了修订，对打印错误做了更正翻译。清华大学出版社的龙啟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，书中难免有错误和不妥之处，恳请读者批评指正。

译　者

于北京清华园

前　言

在这样一个全球电子互连，电脑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漏，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。其重点在于已广泛使用在Internet 和公司网络中的应用和标准（尤其是 Internet 标准）。

本书读者

本书适合研究人员和专业人士阅读。如果用作教材，本书也作为计算机科学、计算机工程和电子工程专业本科生一学期网络安全课程的教材使用。本书内容也覆盖了信息技术知识群的两个核心领域，其中一个是 IAS2 Security Mechanisms，另一个是 NET4 Security。这些学科领域都是 ACM/IEEE 计算机协会计算课程 2005 年草案中的部分内容。

本书还可用作基本的参考书，也可用于自学。

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、Hash 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、PGP、S/MIME、IPSec、SSL/TLS、SET 和 SNMPV3 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一些问题。

学生在线文档

这次新版，数量巨大的第一手辅助材料按照下面的分类已放在网上。

- **在线章节**：为限制书的篇幅和成本，该书有两章以 PDF 文件格式提供。一章是 SNMP 安全，另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。所以对有兴趣的同学，有 6 个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。
- **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。
- **核心论文**：为进一步阅读，提供了 24 篇来自专业文献的论文，其中有很多是不容易找到的。

教师教学辅助材料

为帮助教师教学，我们还提供了下列材料：

- **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 幻灯片。
- **PDF 文件**：专门制作的书中所有图和表的 PDF 文件。

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，或通过点击本书网站“WilliamStallings.com/Crypto/Crypto5e.html”中的按钮“Book Info and More Instructor Resources”获得。要访问 IRC，通过网站

pearsonhighered.com/educator/replocator/requestSalesRep.page

请与您 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。

教师和学生 Internet 服务

本书的网页可为学生和教师提供支持。该网页包括了相关的站点、以 PDF 文件存储的书中图、表、授课用的 PPT 文件等，网址为：

WilliamStallings.com/NetSec4e.html

一个可以让使用本书的教师与其他教师和作者交换信息、建议和问题的电子信箱列表网页已经建立。若发现印刷和其他错误，则在 WilliamStallings.com 可以找到本书的一个错误列表。此外，计算机科学学生资源网 WilliamStallings.com/studentSupport.html 可以提供

文档、信息和关于计算机科学学生和专业人士的其他有用网络链接。

网络安全教学项目

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如下：

- **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。
- **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。
- **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。
- **实验练习**：一系列涉及到编程和书中概念训练的项目。
- **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。
- **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，然后撰写一份短的报告。

第 4 版亮点

这次新版中的变化要比任何之前的版本变化来得广泛和充实。

从第 3 版出版的 4 年之中，该领域持续取得了创新和提高。在第 4 版中，在继续保持全面覆盖本学科主要内容的情况下，我也试图把这些变化包括在内。在开始修订时，第 3 版已经经过一定的讲授该课程教授们的详细审阅。另外，工作在该领域内的一些教授审阅了单个章节。结果是，有很多地方的叙述得到了澄清和加强，说明得到了提高。进一步，增加了相当数量的“领域测试”习题。

除通过上述努力以增强本书对教师和使用者的可读性外，修订版也包括了一些贯穿全书的内容变化。具体如下：

- **伪随机数产生和伪随机函数（修订）**：该重要主题在第 2 章已被扩充，增加了新材料，并列了一个新的附录。
- **密码散列函数和消息认证码（修订）**：关于散列函数和 MAC 的材料已进行了修订和重组，使其变得更清楚、更系统。
- **密钥分配和远程用户认证（修订）**：在第 3 版中，这部分内容散在三章中。第 4 版我们对材料做了修订并将其归入一章中，对其进行了系统、完整的处理。
- **联合身份（新）**：新增的一节，内容涵盖多企业、多应用、支持数千，甚至百万用户的普通身份管理架构。
- **HTTPS（新）**：新增加的一节，内容涵盖为在 Web 浏览器和服务器之间提高安全通

信的协议。

- **安全盾（新）**：SSH，加密技术最普遍深入的应用之一，在新增的一节里介绍。
- **域名密钥标识邮件（新）**：新增加的一节，内容涵盖 DKIM，它已成为邮件认证方法的标准。
- **无线网络安全（新）**：新增加的一章，内容包括网络安全中的这一重要领域。该章涉及无线局域网中的 IEEE 802.11（WiFi）安全标准，以及一个移动 Web 浏览器与一个服务器之间通信的无线应用协议（WAP）安全标准。
- **IPSec（修订）**：IPSec 这一章几乎是完全重写。现在它的内容涵盖 IPSecv3 和 IKEv2。另外，讲义稿也做了修改以使其内容更宽泛和清楚。
- **法律和伦理问题（新）**：新增的一章，是在线的，内容涵盖这方面的重要主题。
- **在线附录（新）**：6 个在线附录在很多方面能对有兴趣的学生进行加宽和加深。
- **附答案的家庭作业习题**：一套独立的家庭作业习题（附答案）通过在线为学生提供。
- **防火墙（修订）**：关于防火墙的这一章做了明显的扩充。

每次新版时都会有在保持一定页面数的情况下增加新内容的两难。部分地，这一目标这次通过去除陈旧材料和紧缩叙述得到了实现。今次版本，一些较少兴趣的章节和附录已经作为独立的 PDF 文件放在了网上。这使得在未增加篇幅和成本的情况下对内容做了扩充。

本书与《密码学与网络安全》的关系

本书与《密码学与网络安全（第 5 版）》（CNS5e）互为补充。CNS5e 更侧重于密码编码学内容的阐述，包括详细的算法分析和重要的数学基础，全书将近 400 页。而本书第 4 版（NSE4e）仅在第 2 章和第 3 章对这些内容作了简要概述。同时，NSE4e 不仅包括了 CNS5e 其余的全部内容，也增加了 CNS5e 中没有的 SNMP 安全。因此，NSE4e 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个教本。

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。

有了这些帮助，我也没有什么可以居功自傲的。但是，无论如何我还是要自豪地说，如果没有这些帮助，我依然选择所有的这些内容。

目　录

第 2 部分　网络安全应用