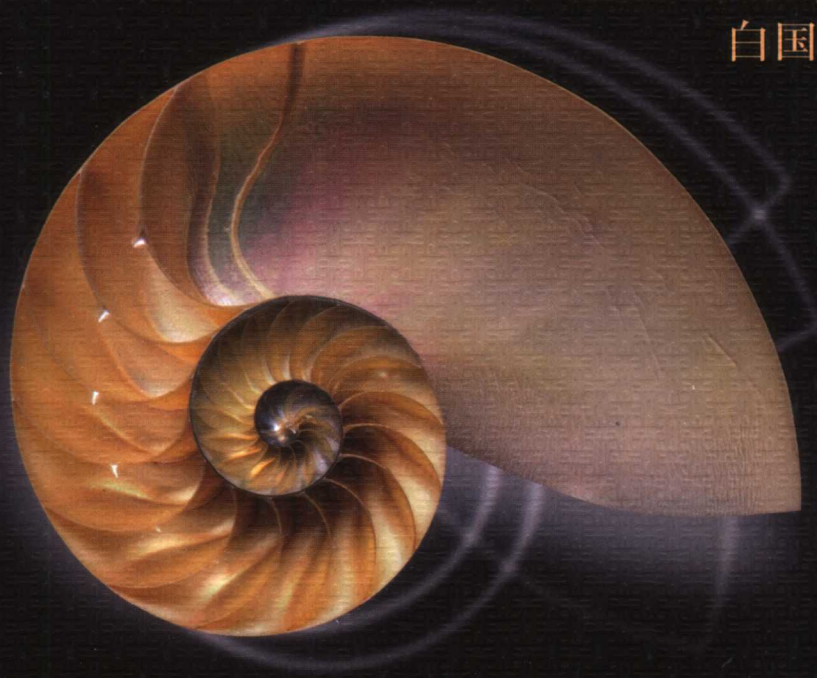
世界著名计算机教材精选

PEARSON Prentice Hall

网络安全基础

应用与标准（第3版）

William Stallings 著
白国强 等译



NETWORK SECURITY ESSENTIALS

Applications and Standards Third Edition

PEARSON Education

清华大学出版社

世界著名计算机教材精选

Network Security Essentials

Applications and Standards Third Edition

网络安全基础

应用与标准(第3版)

William Stallings 著

白国强 王海欣 陈弘毅 译

清华大学出版社

北京

EISBN: 0-13-238033-1

北京市版权局著作权合同登记号 图字 01-2006-6741 号

图书在版编目(CIP)数据

网络安全基础：应用与标准(第3版)/(美)斯托林斯(Stallings, W.)著；白国强等译. —北京：清华大学出版社，2007.7

书名原文：Network Security Essentials, 3e

ISBN 978-7-302-15435-8

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

中国版本图书馆 CIP 数据核字(2007)第 086866 号

责任编辑：龙啟铭

责任校对：张 剑

责任印制：王秀菊

出版发行：清华大学出版社

http://www.tup.com.cn

c-service@tup.tsinghua.edu.cn

社 总 机：010-62770175

投稿咨询：010-62772015

地 址：北京清华大学学研大厦 A 座

邮 编：100084

邮购热线：010-62786544

客户服务：010-62776969

印 刷 者：北京嘉实印刷有限公司

装 订 者：三河市新茂装订有限公司

经 销：全国新华书店

开 本：185×260 **印 张**：21.25

字 数：510 千字

版 次：2007 年 7 月第 1 版

印 次：2007 年 7 月第 1 次印刷

印 数：1～3000

定 价：39.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。

联系电话：010-62770177 转 3103 产品编号：022596-01

本书英文影印版已由清华大学出版社出版发行。

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年代，安全问题无关紧要的时代的确已不复存在。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流信息的依赖程度。这样，又进一步使得人们意识到需要保护数据和资源免遭泄漏，保障数据和信息的真实性，以及保护系统免受基于网络的攻击。第二，密码学和网络安全学科已经成熟，能够用于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。重点介绍已在互联网和公司网络中的广泛应用以及一些标准，尤其是那些已得到广泛使用的互联网标准。

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，本书也可作为计算机科学、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。本书内容覆盖了信息技术知识体系的两个核心领域，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，适合于自学。

本书组成

本书由三部分组成：

- **第 1 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 2 部分：网络安全应用**。介绍各种重要的网络安全工具和应用，包括 Kerberos、X.509v3 数字证书、PGP、S/MIME、IPSecurity、SSL/TLS、SET 和 SNMPV3 等。
- **第 3 部分：系统安全**。简述系统级安全问题，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、常用缩略语表和参考文献。每章均包括有作业题、思考题、关键词、术语表、进一步阅读建议和推荐网址等。

还有，每部分开头还逐章给出了各章的内容概览。

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**：包括每章末的思考题和习题的答案。

- **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。
- **项目指南**：下面所列的是各类项目建议的项目作业。

教师可以和当地的Pearson教育出版集团或Prentice Hall代表联系，以便取得对这些材料的访问权限。

此外，本书的Web站点还为教师提供了下列支持：

- 使用本书讲授其他课程的网络链接。
- 教师的互联网邮件列表的签名信息。

教师和学生的互联网服务

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（Adobe Acrobat）格式存储的书中图、表、授课用的PPT幻灯片，网址为：http://WilliamStallings.com/NetSec/ NetSec3e.html。其中还建立了一个互联网邮件列表网页，可以让使用本书的教师与其他教师和作者交流信息、建议和问题。若发现印刷和其他错误，则在WilliamStallings.com上可以找到本书的一个勘误表。此外，计算机科学学生资源网 WilliamStallings.com/StudentSupport.html上提供了文档、信息和针对计算机科学学生和专业人士的其他有用的网络链接。

网络安全教学项目

对很多教师来说，密码学或安全课程的一个重要组成部分是一个项目或一组项目，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。本书对项目的组成提供了不同程度的支持。教师手册不仅包括如何构思和指定这些项目，还包括了一组覆盖广泛教材内容的建议项目：

- **研究项目**：一系列的研究型作业，引导学生就互联网的某个特定主题进行研究并撰写一份报告。
- **编程项目**：涵盖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。
- **书写作业**：按章给出的一组建议的书面作业。
- **阅读/报告作业**：一组来自文献的论文，每章一篇，可以指定让学生阅读，然后撰写一篇短报告。

第3版的新内容

自本书第2版出版后的3年来，这一领域仍在持续不断地创新和发展。在新版本中，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。这次再版，讲授过该课程的许多教授对第2版进行了充分审阅。此外，工作在这一领域的许多专业人士也对各章进行了审阅。经过审阅，使很多地方的叙述更加清楚与深入，说明更加详尽。另外，还增加了大量新“领域测试”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，修订版还包括一些贯穿全书的内容变动。具体如下：

- **流密码**：许多网络安全协议与应用中用到了流密码。第 3 版包括了这些内容并给出了最广泛使用的 RC4 算法描述。
- **公钥基础设施（PKI）**：新版本论及了这一重要主题。
- **分布式拒绝服务（DDoS）攻击**：近年来 DDoS 攻击日益增多。
- **信息技术安全评估通用准则**：该通用准则已成为表述安全需求和评估产品与各种实现的国际性框架。

此外，本书中很多其他材料也得到了更新或修订。

本书与 *Cryptography and Network Security* 一书的关系

本书是根据 *Cryptography and Network Security, Fourth Edition*（CNS4e）改编的。CNS4e 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。而本书仅在第 2 章和第 3 章中对这些内容做了简要概述。同时，本书不仅包括了 CNS4e 其余的全部内容，还增加了 CNS4e 中没有的 SNMP 安全。因此，本书更希望为那些主要对网络安全应用感兴趣，而又不需要或不希望更深入涉足密码编码学理论与原理的专业人士或学院课程提供一个教本。

致谢

本书新版得益于众多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。

对新版本习题做出贡献的有 J. B. Holden（罗斯-哈尔曼技术学院）、K. Gaj（乔治-麻荪大学）和 J. Muir（滑铁卢大学）。

普度大学的 S. Rao 和 R. Torres 开发了教师辅助材料中出现的实验室练习题。下列人士对教师辅助材料中的项目作业做出了贡献，他们是 H. Schulzrinne（哥伦比亚大学），C. K. Koc（俄勒冈州立大学）和 D. Balenson（可信信息系统和乔治华盛顿大学）。

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。他们是 Prentice Hall 的员工，特别感谢产品经理 R. Kerman、我的编辑 T. Dunkelberger 以及她的助手 C. Lee 和 C. Snyder。此外，P. M. Daly 做了文字编辑工作。

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

译 者 序

近十年来互联网在我国的发展速度和普及应用几乎超出了所有人的预想。十年前，上网和收发电子邮件只是一些研究机构和高等院校中的一部分人才能享受到的奢侈行为，现在网络已经成了大部分普通人生活中不可缺少的一部分。网络正在改变着人们的生活习惯、思维方式，也改变着社会氛围。伴随着互联网发展并引起人们普遍关注的问题是网络安全。网络病毒、黑客攻防、垃圾邮件、网上欺诈、网络盗窃等行为不仅严重影响了网络功能的正常发挥，也影响了人们对网络的信赖。网络安全不仅事关社会稳定，也关系到国家的政治、经济和文化安全。网络安全已成为信息安全中最重要的内容之一。信息安全也因为互联网安全问题的严重性而引起了人们的高度重视。我国政府已把信息安全视为事关国家安全的一项战略内容。

为适应信息安全的这种发展需求，尤其是为了有效地解决网络安全问题，近年来国内已经出版了大量密码学和网络安全方面的专业书籍、教材和普及读物。为满足社会对这方面人才的需求，国内不少高校也已开办了信息安全专业。但在所有这些出版物中既能满足一般读者对网络安全技术的了解，又能作为网络安全的一本入门教材使用的书籍并不多。

这本由 William Stallings 编写，由世界著名教材出版商“培生教育出版集团”出版的图书既能用作我国高校相关课程的教材，又是一本满足普通网络安全爱好者学习和了解网络安全基本知识的优秀书籍。为此，我们组织力量把它翻译为中文并推荐给读者，希望能对读者学习和了解网络安全基础知识有所帮助。

本书完全从实用的角度出发，用较少的篇幅对当前网络安全解决方案中使用的主要算法、重要协议和系统管理方法等内容做了全面而详细的介绍。全书共分为三部分：（1）密码算法和协议，包括网络安全应用中最常用的密码算法和协议；（2）网络安全应用，介绍了网络安全解决方案中使用的各种安全协议，如 Kerberos、PGP、S/MIME、IPSec、SSL/TLS 和 SET 等；（3）系统安全，介绍了一些系统级的安全问题，如网络入侵、恶意软件和防火墙等。每章后面都提供了一定数量的推荐读物、网址、思考题和习题等。全书最后还提供了一定数量的项目作业。为方便把本书作为教材使用的教师搞好教学，培生教育出版集团还提供了较为完整的配套服务。与本书的前两版相比，第 3 版除在语言和叙述方面做了进一步的改进之外，还增加了一些内容，主要包括 RC4 算法、公钥基础设施（PKI）、分布式拒绝服务攻击（DDoS）和信息技术安全评估通用准则等。

本书与原作者的另一本书 *Cryptography and Network Security* 相辅相成。与这本书相比，本书不仅省去了学习部分密码算法需要的数学基础，也更加简明扼要地叙述了密码算法，以便把重点放在对网络安全协议的介绍上。因此，阅读本书并不需要太多的专业知识。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。

本书由白国强、王海欣组织翻译。参加翻译工作的还有王缔郦、朱莹、李康、谷荧柯、

张春明、张晓峰、岳耀等。在翻译过程中，我们对原书中一些明显的错误做了修订，对印刷错误做了更正。全书最后由白国强、王海欣、陈弘毅统稿和审校。清华大学出版社的龙启铭编辑对本书的翻译出版给予了大力支持和帮助，在此表示感谢。

鉴于译者水平有限，加之时间紧迫，书中难免有错误和不妥之处，恳请读者批评指正。

译 者

北京清华园

目　录

第 2 部分 网络安全应用

第1章

引　言

在过去的几十年中，一个机构内部对**信息安全**的要求经历了两个重大的变革。在广泛应用数据处理设备之前，对机构非常重要的信息安全保障主要是靠物理和管理方法实现的。前者的一个例子是用于存储敏感文档的带有组合锁的档案柜的应用。而后者的一个例子是在聘用过程中使用的人事屏蔽步骤。

在引入计算机之后，对于用来保护存储在计算机上的文件和其他信息的自动工具的需求变得显而易见。对于共享系统则更是如此，例如分时共享系统，对于能通过公共电话网络、数据网络或者互联网访问的系统而言这种需求甚至更加迫切。用于保护数据安全和防范黑客的工具集合的通用名称便是**计算机安全**。

第二个影响安全的重大变化是分布式系统的引入和网络以及在计算机终端用户与计算机之间、计算机与计算机之间进行通信的工具的应用。在数据传输过程中，网络安全方法需要被用来保护数据。事实上，**网络安全**这个术语在某种程度上存在一些误导性，因为事实上所有的商务、政府以及学术机构都是通过互连网络集合与其数据处理设备进行互联的。这样一种集合通常是指互连网[1]（internet），而通常使用术语**互连网安全**。

这两种安全范畴之间没有明确的界定。例如，最为张扬的一种信息系统攻击方法是计算机病毒。当一种病毒到达一个系统的硬盘或光盘并在以后加载到计算机上时，它便被物理地导入系统中。病毒同样可以通过互连网进行传播。无论如何，一旦病毒感染了计算机系统，内部计算机安全工具便需要去检测病毒感染并进行恢复。

本书集中讨论互连网安全，它包含阻止、预防、检测和纠正信息传输的安全冲突的各种方法。这是一个涵盖许多可能性的广泛的讨论范畴。为了使读者对所讨论的范畴有一个直观的认识，请考虑以下安全冲突的范例：

（1）用户A发送文件给用户B。这份文件包含需要防止解密的敏感信息（例如：薪水册记录）。没有被授权阅读这份文件的用户C能够监视该文件的整个传输过程并在传输过程中获得一份文件副本。

（2）网络管理员D需要在他的管理下发送一条消息给计算机E。这条消息指示计算机E更新一份包含一系列可以访问这台计算机的新用户属性的授权文件。用户F截取了这条消息并改变了其中的内容（如添加或删除一些条目），之后把修改后的消息发送给计算机E。后者接收这份消息并认为它来自于网络管理员D，之后相应地更新授权文件。

（3）用户F直接编撰了一份自己的消息而不是截取消息，并且把编撰的消息以管理员D的名义发送给E。计算机E接受了消息并且相应地更新授权文件。

（4）某个雇员毫无征兆地被解雇了。人事经理发送一条消息给系统服务器以注销该雇员的账户信息。当注销过程完成后，服务器会向该雇员的档案中发送一份通知以确认这个过程。被解雇的雇员能够截取这条消息并且将该消息延迟足够长的时间以访问系统并取回敏感信息。之后，这份消息被送到服务器，服务器发送确认通知。可能在相当长的时间内，都不会有人察觉到这个被解雇的雇员的行为。

（5）把一份包含有对若干交易进行指示的消息从一个客户发送到一个股票经纪人。客户向股票经纪人发送了一条包含若干交易指示的消息。后来投资失败，同时客户否认发送过该消息。

1　我们使用术语互连网，是指任意互连的网络结构。公司内部的局域网便是互连网；而互联网是由一个机构或组织用来构建其互连网的工具。