HZ BOOKS
华章教育

计 算 机 科 学 丛 书

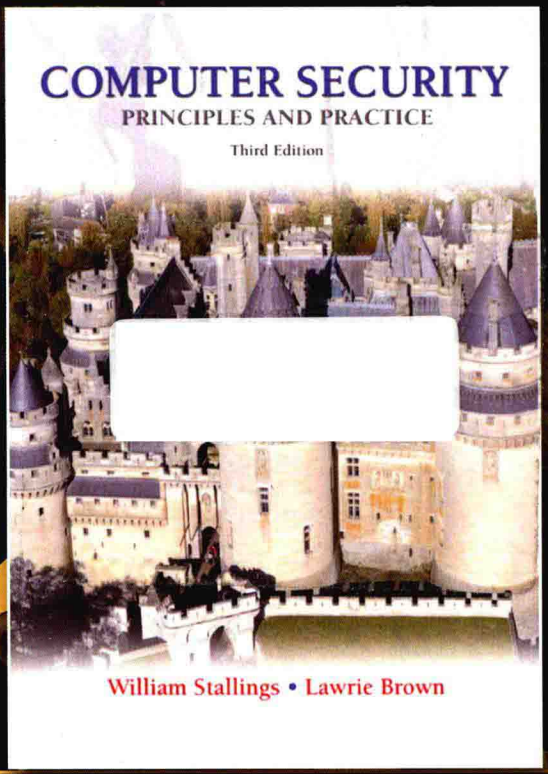
PEARSON

原书第3版

计算机安全
原理与实践

[美] 威廉·斯托林斯（William Stallings）
[澳] 劳里·布朗（Lawrie Brown）
著 贾春福 高敏芬 等译

Computer Security
Principles and Practice, Third Edition



机械工业出版社
China Machine Press

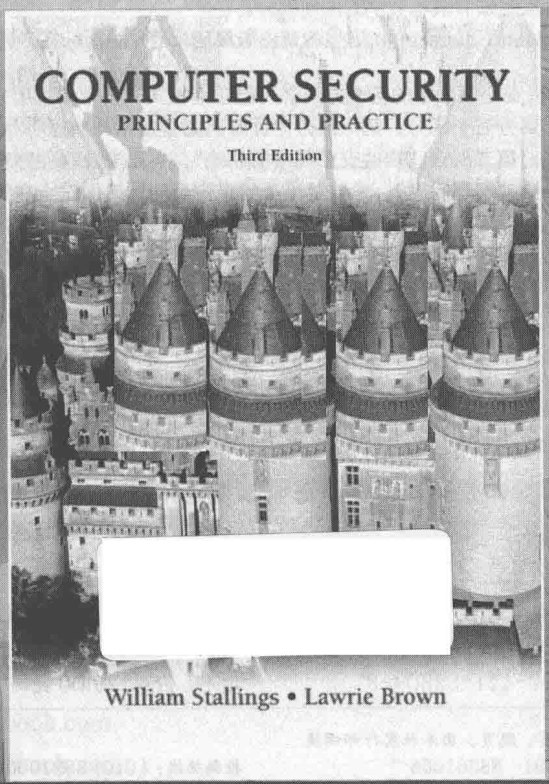
计 算 机 科 学 丛 书

原书第3版

计算机安全
原理与实践

[美] 威廉·斯托林斯（William Stallings）
[澳] 劳里·布朗（Lawrie Brown）
著 贾春福 高敏芬 等译

Computer Security
Principles and Practice, Third Edition



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

计算机安全：原理与实践（原书第3版）/（美）斯托林斯（Stallings, W.），（澳）布朗（Brown, L.）著；贾春福等译．—北京：机械工业出版社，2016.3
（计算机科学丛书）
书名原文：Computer Security: Principles and Practice，Third Edition

ISBN 978-7-111-52809-8

I. 计… II. ① 斯… ② 布… ③ 贾… III. 计算机安全 IV. TP309

中国版本图书馆CIP数据核字（2016）第020365号

本书版权登记号：图字：01-2015-1915

本书系统介绍计算机安全领域中的各个方面，不但包括相关的技术和应用方面的内容，而且还包括管理方面的内容。本书共分五个部分：第一部分“计算机安全技术与原理”，涵盖了支持有效安全策略所必需的所有技术领域；第二部分“软件安全与可信系统”，主要涉及软件开发和运行带来的安全问题及相应的对策；第三部分“管理问题”，主要讨论了信息安全与计算机安全在管理方面的问题，以及与计算机安全相关的法律和道德方面的问题；第四部分“密码编码算法”，包括各种类型的加密算法和其他类型的密码算法；第五部分“网络安全”，关注的是为在Internet上进行通信提供安全保障的协议和标准及无线网络安全等问题。此外，各章后面都有一定数量的习题和复习题供读者练习，以加深对书中内容的理解。同时，各章后面还附上了一些极有价值的推荐读物。

本书覆盖面广，叙述清晰，可作为高等院校计算机安全课程的教材，同时也是一本有关密码学和计算机网络安全方面的非常有价值的参考书。

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：迟振春　　责任校对：董纪丽
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2016年3月第1版第1次印刷
开　　本：185mm×260mm　1/16　　印　　张：39.25
书　　号：ISBN 978-7-111-52809-8　　定　　价：129.00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

文艺复兴以来，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的优势，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自 1998 年开始，我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与 Pearson，McGraw-Hill，Elsevier，MIT，John Wiley & Sons，Cengage 等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出 Andrew S. Tanenbaum，Bjarne Stroustrup，Brain W. Kernighan，Dennis Ritchie，Jim Gray，Afred V. Aho，John E. Hopcroft，Jeffrey D. Ullman，Abraham Silberschatz，William Stallings，Donald E. Knuth，John L. Hennessy，Larry L. Peterson 等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力相助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专门为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

华章网站：www.hzbook.com
电子邮件：hzjsj@hzbook.com
联系电话：（010）88379604
联系地址：北京市西城区百万庄南街 1 号
邮政编码：100037

华章科技图书出版中心

译者序

Computer Security: Principles and Practice, Third Edition

在全球信息化大潮的推动下，计算机与网络技术迅速发展起来并得到广泛的应用，而今已经渗透到了整个社会的各个领域，从根本上改变了人们的生活和工作方式，人们对计算机和网络的依赖程度日益增强。与此同时，由于计算机在政治、经济和国防等国家关键领域中的应用，使得计算机安全问题越来越受到人们的关注。计算机信息系统的脆弱性，必然会导致信息化社会的脆弱性。目前世界各国计算机犯罪案件的不断增加，就充分说明了计算机安全问题的严重性。因此，人们对教育中计算机安全及相关主题的关注程度与日俱增。计算机安全理论和技术已经成为信息科学与技术中极为重要的研究领域之一。

为了满足教育中人们对计算机安全知识的需求，近年来国内出版了许多有关密码学、计算机网络安全和计算机系统方面的专业书籍、教材和科普读物等，特别是随着许多高校中信息安全专业的创建，国内还出版了多套信息安全专业教材系列丛书。这无疑对计算机安全教育起到了非常重要的作用。但很少有这样的一本参考书：它完全涵盖计算机安全的各个领域，不但包括相关的技术和应用方面的内容，同时还包含管理方面的内容，使得任何一个从事计算机安全领域研究和学习的人都能从中获取自己关心的知识；它深入浅出，无论是初涉计算机安全领域的学生，还是专业技术人员或者学术研究人员，通过阅读都会受益匪浅；它内容新，反映了计算机安全领域技术与管理的发展现状。本书就是这样一本具备了上述特点的非常有价值的参考书，你也可以精选其中的内容作为教材使用。

很多阅读过计算机数据通信与网络领域相关书籍的读者，可能早已知道了威廉·斯托林斯（William Stallings）的名字，本书是威廉·斯托林斯的又一力作。威廉·斯托林斯早年获得了麻省理工学院计算机科学博士学位。他是世界知名计算机学者和畅销教材作者，已经撰写了 18 部著作，出版了 70 多本书籍，内容涉及计算机安全、计算机网络和计算机体系结构等领域，堪称计算机界的全才。在过去的 30 多年中，威廉·斯托林斯博士曾经多次获得由美国“教材和学术专著作者协会”颁发的“年度最佳计算机科学教材”奖。目前，威廉·斯托林斯博士还创建并维护着计算机科学学生资源网站（Computer Science Student Resource Site）ComputerScienceStudent.com。这个网站为学习计算机科学的学生以及专业技术人员提供了他们感兴趣的各种主题的相关文档和链接，供学生在学习和研究过程中参考。

本书的特点是内容详尽、覆盖面广，阐述条理清晰、深入浅出、易于理解，系统地概览了计算机安全领域的最新发展状况和趋势。通过阅读本书，读者可以全面深入地了解计算机安全领域中涉及的绝大部分知识。

本书第 3 版在第 1 版和第 2 版的基础上对内容进行了修订，特别补充了计算机安全领域的新进展和新技术，并对前两版的内容进行了优化，使内容更为系统和紧凑，更适合读者阅读或参考。

全书共包含以下五个部分：第一部分“计算机安全技术与原理”，涵盖了支持有效安全策略所必需的所有技术领域；第二部分“软件安全与可信系统”，主要涉及软件开发和运行带来的安全问题及相应的对策；第三部分“管理问题”，主要讨论了信息安全与计算机安全在管理方面的问题，以及与计算机安全相关的法律和道德方面的问题；第四部分“密码编码算法”，包括各种类型的加密算法和其他类型的密码算法；第五部分“网络安全”，关注的是为在 Internet 上进行通信提供安全保障的协议和标准及无线网络安全等问题。此外，各章后面都有

一定数量的习题和复习题供读者练习，以加深对书中内容的理解。同时，各章后面还附上了一些极有价值的参考文献，利用这些资源，有兴趣的读者可以进一步对计算机安全方面的一些技术细节进行深入学习和研究。

本书由贾春福和高敏芬组织翻译，参加翻译的人员还包括刘春波、李同、宗楠、马昊玉、刘露、梁爽、陈喆、杨骏、蔡亚运等。王晓初、黄志鹏、吕童童和李瑞琪等也参与了部分翻译工作或者校对工作。全书最后由贾春福和高敏芬统稿和审校。在翻译过程中，我们对书中出现的错误做了修正。在本书的翻译过程中得到了机械工业出版社华章公司温莉芳总编辑、朱劼编辑的关注和支持，在此表示感谢。

翻译国外著名作家的经典书籍是极具挑战性的，因为经典书籍不仅具有深度，在内容上也是各具特色，常常是引经据典，这对我们的翻译工作产生了不小的压力。我们本着对读者认真负责的宗旨，力求做到技术内涵的准确无误以及专业术语的规范统一，力求达到“信达雅”的翻译水准。但是，限于译者水平，加之时间仓促，翻译不妥和疏漏之处在所难免，敬请阅读本书的读者予以批评指正。

译者

于天津南开园

第 3 版新增内容

自本书第 2 版出版以来，计算机安全领域又持续性地出现了一些改进和创新。在新版本中，我们试图展现这些改进和创新，同时，力求在深度和广度上涵盖整个计算机安全领域。在第 3 版修订之初，许多讲授该领域课程的教授和从事该领域工作的专业人士又重新仔细地审查了本书的第 2 版。第 3 版修订和完善了其中多处描述，并对相关的图表也进行了改进。

除了这些适用于教学和便于阅读方面的改进外，本书也对一些实质性的内容进行了修订。下面列出的是其中一些最显著的修订：

- **基本安全设计原则**：第 1 章新增加了一节有关基本安全设计原则的内容，这一原则被美国国家安全局和美国国土安全部联合创建的信息保障 / 网络防御国家卓越学术中心（National Center of Excellence in Information Assurance/Cyber Defense）列为基本原则。
- **攻击面**（attack surface）和**攻击树**（attack tree）：第 1 章新增一节来描述这两个概念，这对于评估和分类安全威胁具有非常重要的作用。
- **用户认证模型**：第 3 章新增一个小节用于描述用户认证的一般模型，这有利于统一探讨用户认证的不同方法。
- **基于属性的访问控制**（ABAC）：第 4 章新增了一节关于日益普及的基于属性的访问控制的内容。
- **身份、凭证和访问管理**（ICAM）：第 4 章新增一节关于 ICAM 的内容，这是管理和应用数字身份（和相关属性）、证书和访问控制的综合方案。
- **信任框架**：第 4 章新增一节关于开放式身份信任框架的内容，这是一种用于值得信任的身份和属性交换的开放式和标准化的方法，该方法正得到广泛的应用。
- **SQL 注入攻击**：第 5 章增添了一节关于 SQL 注入攻击的内容，SQL 注入攻击是最为流行、最为危险的基于网络的安全威胁方式之一。
- **云安全**：对第 5 章关于云安全的内容进行了修正，并扩展了反映其重要性和近期进展的内容。
- **恶意软件**：调整恶意软件的内容和入侵者的分类，使其能够反映恶意软件最新的发展，包括高级持续性威胁（APT），它已引起了国家层面的高度重视。
- **入侵检测 / 入侵防护系统**：修改了关于 IDS/IPS 的内容以反映该领域的新进展，包括协助实现深度防护策略的基于主机的入侵检测系统的最新研究进展。
- **人力资源**：由于人为因素和社会工程导致的安全丧失逐渐成为人们关注的内容，包括几个近期发生的由内部人员引起的大量数据渗漏案例，用以强调说明这些安全丧失问题需要程序上和技术控制方面的融合来解决。而这些内容在几个重要的小节都有阐述。
- **移动设备安全**：移动设备安全已成为企业网络安全的重要方面，尤其是那些被称为“自带设备”（BYOD）的一类设备。第 24 章用了新的一节阐述了这些重要的内容。
- **SHA-3**：这一最近被采用的密码编码散列标准被安排在了附录中。

背景

近年来，人们在高等教育中对计算机安全及相关主题的关注程度与日俱增。导致这一状况

的因素很多，以下是其中两个突出的因素：

1. 随着信息系统、数据库和基于 Internet 的分布式系统与通信广泛应用于商业领域，再加上愈演愈烈的各种与安全相关的攻击，各类组织机构开始意识到必须拥有一个全面的信息安全策略。这个策略包括使用特定的软硬件和培训专业人员等。

2. 计算机安全教育，也就是通常所说的信息安全教育（Information Security Education）或者信息保障教育（Information Assurance Education），由于与国防和国土安全密切相关，在美国和其他许多国家已经成为一个国家目标。NSA/DHS 信息保障 / 网络防御国家卓越学术中心以政府的身份负责计算机安全教育标准的制定。

由此可预见，关于计算机安全的课程在未来的大学、社区学院和其他与计算机安全及相关领域相关的教育机构中会越来越多。

目标

本书的目标是概览计算机安全领域的最新发展状况。计算机安全设计者和安全管理者面临的中心问题主要包括：定义计算机和网络系统面临的威胁，评估这些威胁可能导致的风险，以及制定应对这些威胁的恰当的、便于使用的策略。

本书将就以下主题进行讨论：

- **原理**：虽然本书涉及的范围很广，但有一些基本原理会重复出现在一些领域中，比如，有关认证和访问控制的原理。本书重点介绍了这些原理并且探讨了这些原理在计算机安全的一些特殊领域中的应用。
- **设计方法**：本书探讨了多种满足某一特定方面的计算机安全需求的方法。
- **标准**：在计算机安全领域中，标准将越来越重要，甚至会处于主导地位。要想对某项技术当前的状况和未来的发展趋势有正确的认识，需要充分理解与该项技术相关的标准。
- **实例**：书中的许多章中都包含一节来展示相关原理在真实环境中的应用情况。

对 ACM/IEEE 计算机科学课程 2013 的支持

本书是为学术研究人员和专业技术人员编写的。作为教科书，它面向的对象主要是计算机科学、计算机工程和电子工程专业的本科生，授课时间可以是一或两个学期。本书第 3 版的设计目标是支持 ACM/IEEE 计算机科学课程 2013（CS2013）推荐的内容。CS2013 课程推荐的内容首次包含了信息保障和安全（IAS），将其作为知识领域列入了计算机科学知识体系之中。CS2013 将所有需要讲授的课程内容分为三类：核心 1 级（Core-Tier 1）（所有的主题都应涵盖在课程体系中），核心 2 级（Core-Tier 2）（全部或大部分主题应当包含在课程体系中），选修内容（具有一定广度和深度的选修主题）。在 IAS 领域中，CS2013 包含了 3 个核心 1 级的主题、5 个核心 2 级的主题和许多选修主题，每一个主题都包含一些子主题。本书包含了 CS2013 的核心 1 级和核心 2 级的全部内容，同时也包含了 CS2013 的许多选修主题。

详见第 0 章有关本书涵盖 CS2013 的内容。

覆盖 CISSP 科目领域情况

本书涵盖了 CISSP（注册信息系统安全师）认证所规定的所有科目领域。国际信息系统安全认证协会（ISC）^{2} 所设立的 CISSP 认证被认为是信息安全领域认证中的“黄金准则”。CISSP 认证是安全产业唯一一个被广泛认可的认证。包括美国国防部和许多金融机构在内的组织机构，时下都要求其网络安全部门的人员具有 CISSP 认证资格。2004 年，CISSP 成为首个

获取 ISO/IEC 17024（General Requirements for Bodies Operating Certification of Persons）官方认证的信息技术项目。

CISSP 考试基于公共知识体系（CBK），信息安全实践大纲由国际信息系统安全认证协会（ISC）[2] 开发和维护，这是一个非营利组织。CBK 制定了组成 CISSP 认证要求的知识体系的 10 个领域。有关本书涵盖 CBK 的详细情况，请参见第 0 章。

本书内容

本书分为五个部分（具体情况见第 0 章）：

- 计算机安全技术与原理
- 软件安全与可信系统
- 管理问题
- 密码编码算法
- 网络安全

本书还配有一些在线章节和附录，介绍一些选定的主题。

本书附有常用的缩略语表和参考文献。此外，每章均包括习题、复习题和关键术语表以及推荐读物。

教学辅助材料[⊖]

本书的主要目标是尽可能地为令人兴奋的、高速发展的信息安全学科提供一个有效的教学工具。这一目标不仅体现在本书的组织结构上，也体现在教学辅助材料上。本书提供了以下补充资料，以便教师组织教学工作。

- **项目手册**（Projects manual）：项目手册包括文档和便于使用的软件，以及后续列出的为每类项目推荐的项目任务。
- **解决方案手册**（Solutions manual）：每章章末的复习题和习题的答案或解决方案。
- **PPT 幻灯片**（PowerPoint slides）：涵盖本书所有章节的幻灯片，适合在教学中使用。
- **PDF 文件**（PDF files）：本书中所有的图片和表格。
- **练习库**（Test bank）：每章都有一组用于练习的问题。
- **教学大纲样例**（Sample syllabuses）：本书包含的内容超出了一学期所能讲授的内容。为此，本书提供了一些教学大纲样例，目的是为教师在有限时间内使用本书提供建议，这些样例都是基于教授使用本书第 1 版的真实教学经历给出的。

所有教辅材料都可以在本书的教师资源中心（Instructor Resource Center，IRC）获得，可以通过出版商网站 www.pearsonhighered.com/stallings 或者点击本书的网站 WilliamStallings.com/ComputerSecurity 中的 Pearson Resources for Instructors 链接获得。

另外，本书的 Web 站点 WilliamStallings.com/ComputerSecurity（点击 Instructor Resources 链接）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信息。
- 提供给使用本书教师的 Internet 邮箱列表的签名信息，这使得使用本书的教师之间、教师与本书作者之间可以交换信息，交流对本书的建议，探讨其中的问题等。

⊖ 关于本书教辅资源，用书教师可向培生教育出版集团北京代表处申请，电话：010-5735 5169/5735 5171，电子邮件：service.cn@pearson.com。——编辑注

学生资源

在第 3 版中，大量的面向学生的原始辅助材料都可以在两个网站上获取。本书的配套网站 WilliamStallings.com/ComputerSecurity（点击 StudentResources 链接）中包括一系列按章节组织的相关链接，以及本书的勘误表。

Premium Content 站点包含了如下资料[⊖]：

- **在线章节**（Online chapters）：为了控制本书的内容容量和销售价格，本书有两章内容以 PDF 文件的形式提供。这些章节已在本书的目录中列出。
- **在线附录**（Online appendices）：本书教学辅助资料中引用了大量有趣的主题，但在印刷版中没有详细地展开。为此，我们为感兴趣的学生提供了有关这些主题的 9 个附录，这些附录也在本书的目录中列出。
- **课后问题及答案**（Homework problems and solutions）：提供了一组独立的课后问题并配有答案，便于学生检查自己对课本内容理解的情况。

项目和其他学生练习

对许多教师来说，计算机安全课程的一个重要组成部分是一个项目或一组项目。通过这些可以自己动手实践的项目，学生可以更好地理解课本中的概念。本书对项目的组件提供了不同程度的支持。教学辅助材料不仅包括如何构思和指定这些项目，而且还包含不同项目类型及作业的用户手册。这些都是专门为本书设计的。教师可以按照以下分类布置作业：

- **黑客练习**（Hacking exercises）：有两个项目可以帮助学生理解入侵检测和入侵防御。
- **实验室练习**（Laboratory exercises）：一系列涉及编程和书中概念训练的项目。
- **安全教育项目**（Security education(SEED) projects）：一系列动手练习或实验，涵盖了安全领域广泛的主题。
- **研究项目**（Research projects）：一系列研究型作业，引导学生就 Internet 的某个特定主题进行研究并撰写一份报告。
- **编程项目**（Programming projects）：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。
- **实用安全评估**（Practical security assessments）：一组分析当前基础设施和现有机构安全性的实践活动。
- **防火墙项目**（Firewall projects）：提供了一个可移植的网络防火墙可视化模拟程序，以及防火墙原理教学的相关练习。
- **案例分析**（Case studies）：一系列现实生活中的案例，包括学习目标、案例简介和一系列案例研讨问题。
- **阅读 / 报告作业**（Reading/report assignment）：一组论文清单，可以分配给学生阅读，要求学生阅读后写出相应的报告，此外还有与教师布置作业相关的内容。
- **写作作业**（Writing assignment）：一系列写作方面的练习，用于加强对书中内容的理解。
- **计算机安全教学网络广播**（Webcasts for teaching computer security）：为强化课程，提供了网络广播地址目录。使用该目录的高效方法是选取或者允许学生选取一个或几个视频观看，然后写一篇关于该视频的报告或分析。

这一整套不同的项目和其他学生练习，不仅是本书的丰富多彩学习体验的一部分，而且从

⊖ 如需要这部分付费内容，读者可联系培生教育出版集团北京代表处购买，电话：010-5735 5169/5735 5171，电子邮件：service.cn@pearson.com。——编辑注

这些项目和练习出发，还可以方便地根据实际情况制定不同的教学计划，以满足不同教师和学生的特殊需求。更为详细的内容请参见附录 A。

致谢

本书第 3 版受益于很多人的评论，他们付出了大量的时间和精力。以下是审阅了本书全部或者大部分手稿的教授和教师：Stefan Robila（蒙特克莱尔州立大学）、Weichao Wang（北卡罗来纳大学夏洛克分校）、Bob Brown（南方理工州立大学）、Leming Zhou（匹兹堡大学）、Yosef Sherif（Mihaylo 商业经济学院）、Nazrul Islam（美国法明代尔州立大学）、Qinghai Gao（美国法明代尔州立大学）、Wei Li（诺瓦东南大学）、Jeffrey Kane（诺瓦东南大学）、Philip John Lunsford II（美国东卡罗来纳大学）、Jeffrey H. Peden（朗沃德大学）、Ratan Guha（中佛罗里达大学）、Sven Dietrich（斯蒂文斯理工学院）和 David Liu（普度大学韦恩堡校区）。

还要感谢那些审阅本书的一章或几章的技术细节的人，他们是：Umair Manzoor（UmZ）、Adewumi Olatunji（FAGOSI Systems, Nigeria）、Rob Meijer、Robin Goodchil、Greg Barnes（Inviolate Security 有限责任公司）、Arturo Busleiman（Buanzo 咨询）、Ryan M. Speers（达特茅斯学院）、Wynand van Staden（南非大学计算机学院）、Oh Sieng Chye、Michael Gromek、Samuel Weisberger、Brian Smithson（理光美洲公司，CISSP）、Josef B.Weiss（CISSP）、Robbert-Frank Ludwig（Veenendaal, ActStamp 信息安全公司）、William Perry、Daniela Zamfiroiu（CISSP）、Rodrigo Ristow Branco、George Chetcuti（技术编辑，TechGenix）、Thomas Johnson（一家位于芝加哥的银行控股公司的信息安全主管，CISSP）、Robert Yanus（CISSP）、Rajiv Dasmohapatra（Wipro 有限公司）、Dirk Kotze、Ya'akov Yehudi 和 Stanley Wine（巴鲁克学院杰克林商学院计算机信息系统部门客座教师）。

Lawrie Brown 博士首先感谢 Bill Stallings，感谢在一起写作的过程中他所带来的快乐。也想感谢澳大利亚国防大学工程与信息技术学院的同事们，感谢他们的鼓励和支持。

最后，我们也想感谢那些负责本书出版的人们，他们的工作都很完美。这些人包括培生出版公司的员工，特别是编辑 Tracy Dunkelberger、项目经理 Carole Snyder 和出版经理 Bob Engelhardt。也要感谢 Jouve India 的生产人员出色、高效的工作。同时感谢培生出版公司市场营销人员，没有他们的努力这本书是不可能这么快到达读者手中的。

威廉·斯托林斯（William Stallings）博士已撰写著作 18 部，再加上这些著作的修订版，共出版 70 多本计算机方面的书籍。他的作品出现在很多 ACM 和 IEEE 的系列出版物中，包括《IEEE 会议论文集》（Proceedings of the IEEE）和《ACM 计算评论》（ACM Computing Reviews）。他曾 11 次获得“教材和学术专著作者协会”（Text and Academic Authors Association）颁发的“年度最佳计算机科学教材”奖。

在计算机领域的 30 多年中，威廉·斯托林斯博士曾经做过技术员、技术经理和几家高科技公司的主管。他曾为多种计算机和操作系统设计并实现了基于 TCP/IP 和基于 OSI 的协议组，从微型计算机到大型机都有涉及。目前，他是一名独立技术顾问，其客户包括计算机与网络设备制造商和用户、软件开发公司和政府的前沿领域研究机构等。

威廉·斯托林斯博士创建并维护着计算机科学学生资源网站 ComputerScienceStudent.com。这个网站为学习计算机科学的学生（和专业技术人员）提供了各种主题的相关文档和链接。威廉·斯托林斯博士是学术期刊《Cryptologia》的编委会成员之一，该期刊涉及密码学的各个方面。

劳里·布朗（Lawrie Brown）博士是澳大利亚国防大学工程与信息技术学院的高级讲师。

他的专业兴趣涉及通信和计算机系统安全以及密码学，包括通过代理证书进行客户端认证、电子商务和 Web 环境下的可信及安全、使用函数式编程语言 Erlang 设计安全的远端代码执行环境，以及 LOKI 族分组密码的设计与实现。

当前，他所教授的课程包括网络安全和数据结构，曾教授过密码学、数据通信和 Java 编程等。

符 号

Computer Security: Principles and Practice, Third Edition

记 号	表 达 式	含 义
D, K	$D(K,Y)$	对称密码体制中，使用密钥 K 解密密文 Y
D, PR_a	$D(PR_a, Y)$	非对称密码体制中，使用用户 A 的私钥 PR_a 解密密文 Y
D, PU_a	$D(PU_a, Y)$	非对称密码体制中，使用用户 A 的公钥 PU_a 解密密文 Y
E, K	$E(K, X)$	对称密码体制中，使用密钥 K 加密明文 X
E, PR_a	$E(PR_a, X)$	非对称密码体制中，使用用户 A 的私钥 PR_a 加密明文 X
E, PU_a	$E(PU_a, X)$	非对称密码体制中，使用用户 A 的公钥 PU_a 加密明文 X
K		密钥
PR_a		用户 A 的私钥
PU_a		用户 A 的公钥
H	$H(X)$	对消息 X 进行散列运算
$+$	$x + y$	逻辑或运算 OR：x OR y
$\cdot$	x · y	逻辑与运算 AND：x AND y；
~	$\sim x$	逻辑非运算 NOT：NOT x
C		特征公式，它是由数据库中的属性值的逻辑公式构成的
X	$X(C)$	特征公式 C 的查询集，满足 C 的记录集合
$\lvert, X$	$\lvert X(C) \rvert$	$X(C)$ 的数量：$X(C)$ 中记录的数目
$\cap$	$X(C) \cap X(D)$	交集：集合 $X(C)$ 与 $X(D)$ 中记录的交集
$\lVert$	$x \lVert y$	x 与 y 串接