国外计算机科学教材系列

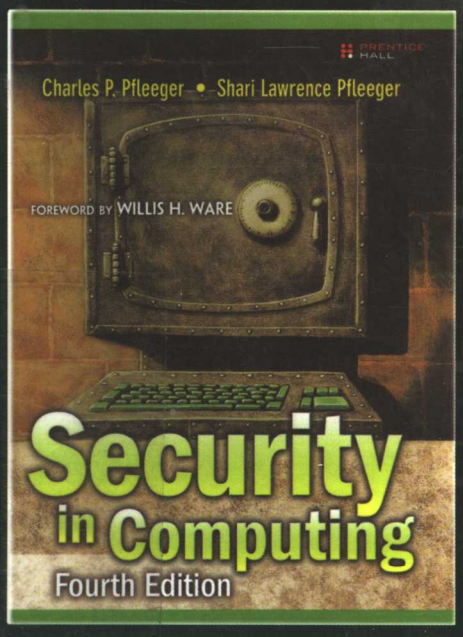
PRENTICE HALL

信息安全原理与应用

（第四版）

Security in Computing

Fourth Edition



[美] Charles P. Pfleeger
Shari Lawrence Pfleeger 著

李毅超 蔡洪斌 谭 浩 等译
秦志光 杨义先 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

国外计算机科学教材系列

信息安全原理与应用

（第四版）

Security in Computing

Fourth Edition

[美] Charles P. Pfleeger
Shari Lawrence Pfleeger 著

李毅超 蔡洪斌 谭 浩 等译

秦志光 杨义先 审校

电子工业出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书是一本信息安全的经典著作和权威指南，内容新颖丰富。全书系统地描述了计算安全的各方面问题，内容涉及计算机安全的概念和术语；密码学基础及应用；程序及软件安全；操作系统安全及可信任操作系统的设计；数据库及数据挖掘的安全；网络安全；安全管理；计算机安全经济学；计算安全中的隐私问题；计算安全中的法律和道德问题，最后对密码学进行了深入研究。

本书既可以作为信息安全或计算机专业本科生、研究生的教材，也可以作为相关领域研究人员和专业技术人员的参考用书。

版权贸易合同登记号　图字：01-2007-0517

图书在版编目（CIP）数据

信息安全原理与应用：第4版/（美）弗莱格（Pfleeger, C. P.）著；李毅超等译.
北京：电子工业出版社，2007.11
（国外计算机科学教材系列）
书名原文：Security in Computing, Fourth Edition
ISBN 978-7-121-05240-8
Ⅰ.信...　Ⅱ.①弗...　②李...　Ⅲ.信息系统－安全技术－教材　Ⅳ.TP309

中国版本图书馆CIP数据核字（2007）第162926号

责任编辑：李秦华　史　平
印　　刷：北京东光印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
开　　本：787 × 1092　1/16　　印张：38.75　　字数：1054千字
印　　次：2007年11月第1次印刷
定　　价：59.00元

凡所购买电子工业出版社的图书有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

继2004年翻译了本书的第三版之后，我们再次翻译了其第四版。原书得到美国著名信息安全专家Willis H.Ware教授(兰德公司)的热情推荐，畅销美国，并成为美国各大学院校广为使用的经典教材，更被业界视为计算机安全攻击和对策的权威指南。书中内容十分新颖丰富，循序渐进，并且案例翔实，深入浅出，有较大的深度和广度，读者可以随意选取自己感兴趣的主题阅读。特别值得一提的是，本书超过一半的篇幅都在探讨代码，因为有相当多的危险或多或少都是由计算机上执行的程序代码引起的。阅读本书唯一需要的背景知识就是要了解编程和计算机系统。本书适合于信息安全或计算机专业本科生、研究生、广大相关领域的研究人员和专业技术人员阅读和参考。

本书由电子科技大学计算机科学与工程学院李毅超、蔡洪斌、谭浩三位副教授共同负责翻译，由电子科技大学计算机科学与工程学院秦志光教授和北京邮电大学信息安全中心杨义先教授审校。

参加本书翻译工作的还包括任云韬、梁晓、黄沾、何子昂、李晓冬、胡炜、肖武、钱彦江、阳广元、覃丽芳、刘凯、杨宇、徐胜、舒柏程、吴超、邱爽、周凌、康凯、申文迪、余三超等研究生。本书的出版得到了电子科技大学计算机科学与工程学院信息安全学科建设基金的支持，在此表示衷心的感谢。由于水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

序　言

在20世纪50年代，著名的计算机联合会议(Joint Computer Conferences，JCC)把计算机技术专业人员和用户召集在了一起。JCC一年举办两届，最初称为东部和西部JCC，后来改名为春季和秋季JCC，再后来又更名为全国计算机年会AFIPS。在这个背景下，计算机安全(后来被命名为信息系统安全，现在也称为"国家信息基础设施安全的保护")不再是机要部门、防卫部门关心的话题，而是开始走向公众了。

其时，兰德公司的Robert L.Patrick，John P.Haverty和我都在谈论着国家及其公共机构对计算机技术日益增长的依赖性。我们注意到，已安装的系统无法保证自身及其数据不受入侵攻击的破坏。我们认为，此时应该促使技术群体和用户群体开始关注计算机安全了。

(美国)国家安全局(National Security Agency，NSA)的远程访问分时系统的开发使这一设想成为现实。该分时系统具有一套完整的安全访问控制机制，运行在Univac 494机器上，为终端和用户提供服务——不仅针对马里兰州Fort George G.Meade总部内的终端和用户，而且面向世界范围的终端和用户。很幸运，我了解该系统的详细情况。

我在兰德公司另两位工作人员(Harold Peterson博士和Rein Turn博士)以及NSA的Bernard Peters的帮助下，组织了一批论文提交给了SJCC(春季JCC)大会的管理方，并建议由我来主持该届JCC的论文会议[1]。大会方接受了这个提议，会议于1967年在大西洋城(NJ)会议大厅举行。

此后不久，一个国防承包商要求一台运行在远程访问模式下的大型机能同时兼顾机密保护和商业应用。受这个要求的驱使，以及通过(美国)高级研究计划署(Advanced Research Projects Agency，ARPA)和后来的(美国)国防科学局(Defense Science Board，DSB)立案，(美国)国防部组织了一个委员会，由我担任主席，旨在研究计算机系统安全控制问题。委员会的目的是制定一个文档，使之可以作为(美国)国防部(DoD)在这个问题上政策立场的基础。

委员会的报告最初是作为一份机密文件出版的，并于1970年1月正式提交给发起者(DSB)。此报告后来解密，并于1979年10月由兰德公司再版。这份报告得到了广泛传播[2]，而且还得到了一个"警示报告"的绰号。如今，在兰德公司的网站上还可以找到这份报告及其相关的历史介绍[3]。

后来，美国空军(United States Air Force，USAF)资助了另一个由James P.Anderson担任主席的委员会。它的报告于1972年出版[4]，推荐了一个6年的研发安全计划，总共预算大约800万美元。美国空军根据这个安全计划投资了数个项目[5]，其中的三个为特定的计算机设计，并且用来实现一个带有安全控制的操作系统。

最终，这些举措促成了一个由NSA发起的"标准和评估"计划。该计划在1983年出版的"桔皮书"[6]和随后它所支持的"彩虹系列"的文件组中达到鼎盛[7]。后来，在20世纪80年代直至20世纪90年代期间，这个计划成为了一个国际性主题，并且成为ISO标准[8]。

了解系统安全研究在近数十年中的发展是很重要的。长期以来，防卫部门都以文档的形式来保护机密信息。而今，它已经演变为一个非常精细的方案，将各种需保护的信息划分成组、子组和超级组，所有组都必须是得到许可的人才能访问，而且有必要访问时才能访问[9]。由其所带给我们的加密技术和在传送过程中保护机密信息的经验，影响足以长达一个世纪。最后，由

此认识到安全中的人员问题以及在相关人员间如何建立可信度的必要性。当然，也认识到了物理安全的重要性。

因此，“这个”计算机安全问题，正如20世纪60年代及后来人们所理解的，就是：(1)如何在计算机系统中建立一组访问控制，这些访问控制实施或模仿的是以往纸介质环境中的处理流程；(2)一些相关问题，如保护软件免受未授权的修改、破坏或非法使用，以及将系统安置在一个安全的物理环境中，该环境有着适当的管理监控和操作规程。我们对安全方面的认识还不够深入，主要表现在软件及其相关硬件方面。也就是说，还存在着使软件的正常行为出错和被破坏的风险。在通信、人员和物理安全方面，有关规定和经验太多，但效果并不佳。把各个方面结合在一起，产生一个全面、安全的系统和操作环境是很重要的。

如今，世界已经发生了根本性的改变。桌上型计算机和工作站已经出现并且日益激增。因特网不断繁荣，万维网日益昌盛。网络在“爆炸”，计算机系统之间进行通信已成为必然。很多商业交易都基于网络，很多商业团体(特别是金融机构)都进入了网络。确切地说，世界上的任何一个人都可能是计算机“用户”。计算机联网是普遍现象，目标就是要使信息系统不断扩展和延伸。

随着网络的发展，基于计算机的信息系统(其硬件、软件、数据库和通信)都暴露在一个无法控制的环境中——终端用户、网络管理员、系统所有者甚至政府都无法控制。我们必须做的是，在社会可接受的法律框架下，提供适当的技术、规程、操作以及环境，来抵御各种可能出现的或潜在的威胁。

威胁来自个人和团体、国内和国外。恶意渗透系统或者编制恶意软件的动机(通常伴有攻击性或破坏性的结果)可能出于满足个人智力需求、间谍活动、经济回报、报复、非暴力反抗或其他原因。信息系统的安全环境已发生了很大变化：从在有限范围内只与彼此了解且遵纪守法的用户群体交互，到在全球范围内与不了解且不可信的用户进行交互。重要的是，现在的安全控制必须能够处理没有控制的情形及避免控制带来的负面影响。计算机安全和责任保险有很多相似之处：它们所处的环境容易被了解、充满威胁、被攻击的可能性很大；当然，攻击的细节、时间或其必然性是不同的，只有当事件发生时才清楚。

另一方面，信息及其交流不断繁荣：如今的世界、社会和机构，离开基于计算机通信的信息系统，就无法正常工作。因而，系统应得到全方位的保护——技术的、规程的、操作的和环境的。不管是所有者还是职员，都有责任对信息系统资产进行保护。

但是，计算机安全的发展很缓慢，主要原因是威胁的真实性和破坏性还没有得到充分认识。另外，全面实现信息系统安全的成本太高，超过了不采取措施可能面临的损失，尤其是财政损失。增强资金决策层对安全控制的信心是一个长期的过程。

本书致力于以下问题：威胁和系统漏洞的本质(第1章)；密码学(第2章和第12章)；通用标准(第5章)；万维网和因特网(第7章)；风险管理(第8章)；软件漏洞(第3章)；法律、道德和隐私问题(第10章和第11章)。本书也描述了目前可用的安全控制，如加密协议、软件开发实践、防火墙以及入侵检测系统。从总体上说，本书将为那些负责策划和/或组织、管理及实现一个全面的信息系统安全设计的专家，提供一个广泛而正确的基础。

信息安全还有很多技术方面的问题亟待解决，如硬件、软件、系统和体系结构的研发，以及相应的产品方面。但是，技术本身不是信息安全发展过程中的支柱，组织和管理者们完成安全工作的动机和承诺才是重点所在。今天，国家乃至世界的公共信息基础设施正在沿着“不断学习”这样的曲线缓缓上升；每一次恶作剧或者恶意的攻击事件都在推动它的进步。当今的恐怖

主义事件也起了推动作用。但是在系统安全和威胁之间，这条上升曲线是否已经达到了某一个恰当的平衡点了呢？答案是“不，还没有；我们还有很长的路要走[10]”。

Willis H. Ware
兰德公司

参考文献

1. “Security and Privacy in Computer Systems,” Willis H. Ware; RAND, Santa Monica, CA; P-3544, April 1967. Also published in Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 279 seq, Vol. 30, 1967.

   “Security Considerations in a Multi-Programmed Computer System,” Bernard Peters; Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 283 seq, vol 30, 1967.

   “Practical Solutions to the Privacy Problem,” Willis H. Ware; RAND, Santa Monica, CA; P-3544, April 1967. Also published in Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 301 seq, Vol. 30, 1967.

   “System Implications of Information Privacy,” Harold E. Peterson and Rein Turn; RAND, Santa Monica, CA; P-3504, April 1967. Also published in Proceedings of the 1967 Spring Joint Computer Conference (later renamed to AFIPS Conference Proceedings), pp 305 seq, vol. 30, 1967.

2. “Security Controls for Computer Systems,” (Report of the Defense Science Board Task Force on Computer Security), RAND, R-609-1-PR. Initially published in January 1970 as a classified document. Subsequently, declassified and republished October 1979.

3. http://rand.org/publications/R/R609.1/R609.1.html, “Security Controls for Computer Systems”; R-609.1, RAND, 1979

   http://rand.org/publications/R/R609.1/intro.html, Historical setting for R-609.1

4. “Computer Security Technology Planning Study,” James P. Anderson; ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA; October 1972.

5. All of these documents are cited in the bibliography of this book. For images of these historical papers on a CDROM, see the “History of Computer Security Project, Early Papers Part 1,” Professor Matt Bishop; Department of Computer Science, University of California at Davis. http://seclab.cs.ucdavis.edu/projects/history

6. “DoD Trusted Computer System Evaluation Criteria,” DoD Computer Security Center, National Security Agency, Ft George G. Meade, Maryland; CSC-STD-001-83; Aug 15, 1983.

7. So named because the cover of each document in the series had a unique and distinctively colored cover page. For example, the “Red Book” is “Trusted Network Interpretation,” National Computer Security Center, National Security Agency, Ft. George G. Meade, Maryland; NCSC-TG-005, July 31, 1987. USGPO Stock number 008-000-00486-2.

8. “A Retrospective on the Criteria Movement,” Willis H. Ware; RAND, Santa Monica, CA; P-7949, 1995. http://rand.org/pubs/papers/P7949/

9. This scheme is nowhere, to my knowledge, documented explicitly. However, its complexity can be inferred by a study of Appendices A and B of R-609.1 (item [2] above).

10. “The Cyberposture of the National Information Infrastructure,” Willis H. Ware; RAND, Santa Monica, CA; MR-976-OSTP, 1998. Available online at: http://www.rand.org/publications/MR/MR976/mr976.html. Also available as http://rand.org/publications/MR/MR976/mr976.pdf.

前　言

当前，新闻媒体越来越关注计算机安全对我们日常生活的影响。例如，仅2006年6月某一天，《华盛顿邮报》就刊登了三篇与安全有关的重要文章。头版中的一篇文章讨论了一台保存有2650万名退伍老兵个人数据的便携式计算机丢失。另外一篇在商业部分头版的文章中，描述了微软的新产品套件可以防止恶意代码、间谍行为及其操作系统中不安全的漏洞。再后面，第三篇文章报告了一个主要的消费者电子产品零售商因为疏忽在顾客的计算机上安装了不良软件，使这些计算机成为被入侵的从属计算机网络的一部分。令人担忧的是，类似这样的新闻几乎天天出现，并已经持续了许多年。

虽然计算机安全中如“病毒”、“特洛伊木马”、“钓鱼”和“间谍软件”等术语很常见，但计算机安全解决方案的应用却是罕见的。此外，新的攻击往往是旧问题的巧妙应用。很多情况下，新产品或新版本投入市场的压力迫使开发商无法顾及仔细研究产品的潜在弱点和对策的安全需求。最后，很多人并不承认，他们经常充满快意地忽视不安全的计算可能造成的严重危害。

为什么要阅读本书

计算对数据或计算机操作的隐私和完整性造成了严重威胁。危险是生活的一部分：过马路很危险，或许在某个地方比其他地方更危险，但你还是要过去。小时候，你学会了在过马路前要停下来，左右看看。等大了之后，你学会了估计来往车辆的速度并决定是否有时间通过。在一定的程度上你形成了某种感觉：来往的车辆是否会慢下来或者避让。我们希望你永远不必实践这些，但有时候，你必须判断突然横穿马路而不左右看是不是最佳的躲过危险的方法。关键是所有这些都取决于你的知识和经验。我们希望本书能帮助你形成关于安全计算的知识和经验。

如何控制计算机安全面临的威胁？

- 了解计算机安全所面临的威胁。
- 通过研究在计算机开发和使用过程中如何引入了脆弱性，从而理解导致这些威胁发生的原因。
- 调查能够减少或者阻止这些威胁的控制手段。
- 无论是作为一名使用者、开发者、管理者、消费者还是拥护者，都要培养一种能平衡安全与危险的计算方式。

计算机安全领域变化很迅速，但是底层的大部分问题保持不变。本书将系列地引导你理解当前复杂的攻击。你会发现，它们经常是非常基础的概念的实例。

本书的使用者及用途

本书用于学习信息安全或计算机安全。大专院校的在校生、计算机方面的专业人员、管理人员等各种使用计算机系统的用户中，很多人都想学习计算机安全知识。所有的人都想了解怎

样控制计算机面临的安全危险。但对于特定主题，不同的人想要了解的程度是有所不同的：有些想要进行广泛浏览，而另一些人则想要集中研究某个特定主题，如网络或程序开发。

本书能够提供大多数读者想要的广度和深度。本书是按计算的一般领域来组织的，因而，有特殊兴趣的读者能够很容易地找到想要的信息。本书的章节按照一定的顺序循序渐进地展开，从一般的安全考虑到应用的特定需求，最后到管理和法律方面的问题。因此，本书覆盖了5个关键领域：

- **简介**：威胁、弱点以及各种控制。
- **密码学**：安全控制的“瑞士军刀”。
- **代码**：程序中的安全，包括应用软件、操作系统、数据库管理系统以及网络。
- **管理**：构造和管理从一台计算机到由成千上万台计算机组成的计算机网络系统，理解计算机安全经济学。
- **法律、隐私和道德**：一些社团用以控制计算机安全风险的非技术方式。

本书对以上领域的讨论深度是不一样的。例如，超过一半的篇幅都在研究代码，因为有相当多的危险或多或少地都是由计算机上执行的程序代码引起的。

本书的第1章介绍了计算机安全概念和基本词汇。第2章让读者了解了什么是密码学，如何使用，以及它是如何被误用的。就像驾驶员的手册没有提出如何设计或者制造一辆汽车一样，第2章面向的是密码学的使用者而不是密码学的设计者。第3章到第7章涵盖了软件的大多数方面：单独的程序、操作系统、复杂的应用软件（如数据库管理系统），最后是网络，它是一个复杂的分布式系统。第8章讨论了安全的管理和实施，并在威胁和控制之间找到了一个可接受的平衡点。通过探究计算机安全经济学，第9章提出了一个重要的管理问题：对成本和利益的理解和沟通。在第10章，回到了计算机安全的个人方面，我们考虑怎样才能安全，以及安全欠缺对个人隐私的影响。第11章涵盖了整个社会处理计算机安全的所有普遍方式，即通过法律和道德。最后，第12章又回到密码学，研究加密算法的细节问题。

在这样的组织结构中，读者可以任意翻看，精选特别感兴趣的主题。每个人都应该阅读第1章以丰富你的词汇和建立知识基础。由于密码学出现在相当多的不同控制技术中，所以也应该阅读第2章。一般来说，读者应该从小程序逐步过渡到大型的复杂网络，但是也可以不按顺序来阅读第3章到第7章，或者只选取其中最感兴趣的主题。相对于前面章节中的技术控制手段，第8章和第9章可能对那些需要非技术控制手段作为补充的专业人员来说刚好合适。这几章对于那些学习计算机科学但只知道字节和协议的学生开阔视野可能非常重要。我们向所有人推荐第10章和第11章，因为这两章涉及了人的方面的安全：法律、隐私和道德。第12章是为那些想了解一些跟密码学有关的数学和逻辑知识的读者而编写的。

阅读本书需要哪些背景知识呢？唯一的要求就是要了解编程和计算机系统。计算机专业的大学在校生和大学毕业生当然拥有这些背景知识，专业设计人员和计算机系统的开发人员也一样。想了解更多关于程序工作方式的用户也可以从本书中学到知识。另外，有时我们也会在解决相关安全问题之前，提供与操作系统或网络概念相关的、必要的背景知识。

本书可作为信息安全或计算机安全专业的教材，供一个或两个学期的教学使用。本书同样也可以作为计算机专业人员的参考书，或者大强度培训教程的补充。目录和广泛的参考书目使本书可作为一本手册，该手册对文献中关键文章的重要主题和知识点进行了解释。本书可在全世界范围内的课堂上使用；教师可设置一个学期的课程，集中讲解学生们特别感兴趣的主题，或者与其他课程紧密相关的主题。

本书新增内容

这是本书的第四版，第一版于 1989 年出版。从那时起到现在，尽管很多基本概念都没有改变，但特定的威胁、弱点以及控制都发生了变化。

对熟悉前三版的读者来说，本版两处最明显的变化就是新增加了两章关于计算机安全经济学和隐私的内容。这两个领域在计算机安全团体和其余用户群里受到了越来越多的关注。

这次修订也同时更新了其他章节。从 2003 年本书前一版开始，计算系统的攻击和威胁发生了很多变化，所以我们介绍了关于威胁和控制的很多类型的新内容。这些改变包括：

- 从出于个人原因的单个黑客向为获得经济利益的攻击者团体转变。
- 导致安全故障的编程错误，主要有中间人攻击（man-in-the-middle）、时间攻击（timing）和权限提升攻击（privilege escalation）的错误。
- 最近的恶意代码攻击，比如伪界面和键盘记录器攻击。
- 提高代码质量的方法，包括软件工程、测试和责任方法。
- Rootkit，包括那些意想不到的攻击。
- Web 应用程序的威胁和弱点。
- 数据挖掘中的隐私问题。
- WiFi 无线网络安全。
- 针对 RSA，DES 和 SHA 主流算法的密码分析学攻击，更安全地使用它们。
- 由被入侵的系统组成的网络：僵尸（bot）、僵尸网络（botnet）和 drones。
- 根据 AES 最初这些年的使用经验对 AES 的更新。
- 可靠鉴别方法和用户行为之间的分界。
- 生物特征鉴别的能力和局限。
- 数字内容（比如音频和视频）高效生产和使用之间的冲突和防盗版。

除了这些主要的改变之外，还有很多小的纠正和澄清，范围从用词的改变到出于教学原因而进行的细小的符号更改，再到章节的替换、删除、重新安排以及扩展。

致谢

要想感谢所有对本书产生了影响的人，已变得日益困难了。因为我的同事和朋友们常常在不知情的情况下，贡献了他们的学识。通过争论一个要点或分享一个概念，这些同事让我们不得不对自己已知的事物进行质疑和再思考。

作者要在至少两个方面感谢我们的同事。首先，尽量引用他们那些对本书产生影响的著作。正文所引用的参考文献特别列举了与某些特定想法和概念相关的论文，但是本书最后的参考文献包括了更为广泛、对形成我们讨论安全的方法起微妙作用的著作。因此，所有被引用的著述的作者，其中包括很多朋友或同事，衷心感谢你们对本书做出的积极贡献。特别要感谢的是，兰德公司允许作者在第 8 章中列出其弱点、评价和缓解方法的材料，并将其政府电子邮件分析作为一个学习案例。其次，除了感谢个人外，还要感谢一些组织，在其中我们同充满着创造精神、青春活力和挑战精神的人们相互共勉，并学到了很多东西。这些组织包括可信信息系统公司、Contel 技术中心、伦敦城市大学软件可靠性中心、Arca 系统、Exodus 通信、兰德公司以及有线

与无线公司。如果你曾经在这些地方工作过,那么就很可能对本书产生了某种影响。对那时发生的所有闲谈、争辩和度过的愉快时光,都将表示感谢。另外,感谢 Roland Trope 和 Richard Gida 对本版的第 9 章和第 10 章提出了非常有益的建议。

所有作者都是他们所处环境的产物。写本书的目的是教育人们,因为我们自己接受过良好的教育,并认为回报良好教育最好的方式就是把它传授给其他人。作者的父母,Paul 和 Emma Pfleeger 以及 Emanuel 和 Beatrice Lawrence,一直非常支持我们,并且鼓励我们尽力争取接受最好的教育。Robert L. Wilson 教会 Chuck 怎样学习计算机的相关技能,而 Libuse L. Reed 则教会他如何把内容书写出来。Florence Rogart, Nicholas Sterling 和 Mildred Nadler 则教会 Shari 怎样进行分析和探索。

谨对所有这些人,致以我们最衷心的感谢。

Charles P. Pfleeger
Shari Lawrence Pfleeger

目　录