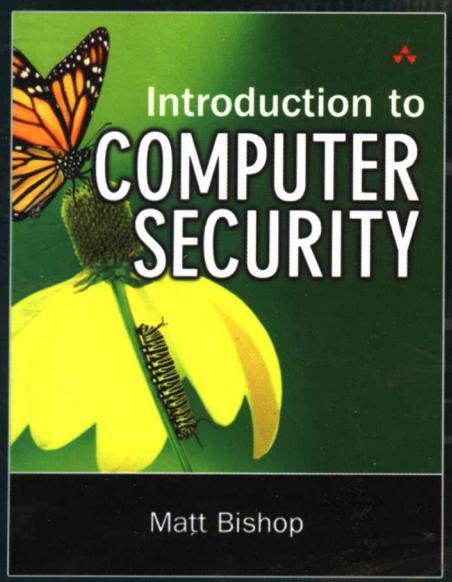
国外计算机科学教材系列

计算机安全学导论

Introduction to computer security



[美] Matt Bishop 著
王立斌 黄征 等译
陈克非 审校

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

国外计算机科学教材系列

计算机安全学导论

Introduction to Computer Security

[美] Matt Bishop 著

王立斌 黄征 等译

陈克非 审校

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书是一本全面系统地介绍计算机安全的基本原理与应用技术的权威教材。全书包括29章，主要探讨的是计算机安全领域中最基础、最普遍的问题。除了用少量篇幅介绍密码理论外，主要对非密码学的安全机制进行了详细的介绍，内容包括安全设计原则、身份表达、访问控制机制、信息流控制等。此外，还以专题的形式介绍了恶意代码、漏洞分析、系统审计、入侵检测等的原理与技术。本书对安全策略模型和安全保障体系也有比较深入的讨论，如各种安全模型、可信系统的构建以及安全系统评估的理论与技术等。

本书可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信等领域的科技人员参考。

版权贸易合同登记号　图字：01-2004-5791

图书在版编目（CIP）数据

计算机安全学导论 /（美）毕晓普（Bishop, M.）著；王立斌，黄征等译. -北京：电子工业出版社，2005.11
（国外计算机科学教材系列）

书名原文：Introduction to Computer Security

ISBN 7-121-01851-9

Ⅰ.计...　Ⅱ.①毕...　②王...　③黄...　Ⅲ.电子计算机-安全技术-教材　Ⅳ.TP309

中国版本图书馆CIP数据核字（2005）第119828号

责任编辑：许菊芳

印　　刷：北京市天竺颖华印刷厂

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

经　　销：各地新华书店

开　　本：787 × 1092　1/16　　印张：31　字数：794千字

印　　次：2005年11月第1次印刷

定　　价：48.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系电话：（010）68279077。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。

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

本书是一部全面系统地介绍计算机安全的基本原理与应用技术的权威教材。作者将源自计算机系统、网络、人类因素和密码学等不同领域的概念融为一体，从而有力地阐明了这样一个道理：计算机安全既是一门科学也是一门艺术。本书讨论的是计算机安全领域中最基础、最普遍的问题，除了密码理论外，主要对非密码学的安全机制进行了详细的介绍，内容包括安全设计原则、身份表达、访问控制机制、信息流控制等，同时还以专题的形式介绍了恶意代码、漏洞分析、系统审计、入侵检测等原理与技术。另外，本书对安全策略模型、安全保障体系也有比较深入的讨论，如各种安全模型、可信系统的构建与评估和可信系统评估标准等。

本书是《计算机安全学——安全的艺术与科学》的简写本，其目的在于满足不同读者的需求。本书省略了大量的数学表达与形式化证明，更适合于数学背景稍弱，或者对形式化方法不感兴趣，或者更关注实践而非理论的计算机安全工作者或学生。尽管是一本简写本，但它依然包括丰富的内容和大量详尽的实例，可作为研究生教材和从事信息安全、计算机、通信等领域的科技人员参考，具有很高的理论和实践参考价值。

本书主要由王立斌和黄征两位博士翻译，全书由陈克非统稿并审校。本次的翻译工作以《计算机安全学——安全的艺术与科学》中译本为基础，所以在此对参与了《计算机安全学——安全的艺术与科学》的翻译和校对工作的老师及同学表示感谢，他们是上海交通大学密码与信息安全实验室的博士后刘勇国，博士生杨礼珍、马昌社、雷飞宇、李世群、李晖、韩玮、李强以及硕士生曹立立、宋志高、洪璇、李敏、俞峰琳、王思佳、魏薇、潘军锋、叶永青、叶波、熊峻峰、严祥、张伟德等。由于译者的水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

前　言

2001年9月11日，恐怖分子劫持了四架飞机，其中三架撞向了建筑物，另一架坠毁，造成灾难性的人员伤亡。灾难发生后，公众开始重新审视社会各个方面的安全性与可靠性，其中一方面就是关于被广泛使用的计算机和计算机网络的安全问题。

这不是一个新问题。1988年，一种称为"蠕虫"的程序[386]在4小时内使Internet上的大约5000台计算机瘫痪①。这种程序的快速传播和巨大影响给计算机科学家敲响了警钟，但大多数人并不担心，因为这种蠕虫程序并不影响他们的生命或者工作。1993年，更多的计算机系统用户开始提防这种危险，因为此时出现了一种称为"嗅探器"的程序，它们被安置在许多网络服务提供商运营的计算机之中，不断记录着用户的登录名和口令[339]。

Tsutomu Shimomura在他的计算机遭到攻击后，使用了一种令人着迷的方法跟踪上攻击者，并使得攻击者被捕入狱[821]。这一事件最终激起了公众的兴趣与担忧。计算机现在是脆弱的，曾经一度令人放心的计算机防护性现在显得如此脆弱。

有几部电影探讨了这种公众担忧。比如，电影 *War Games* 和 *Hackers* 描述了那些能够随意在计算机和网络中游荡的人们，他们恶意地破坏或摧毁那些要花费几千万元才能收集到的信息。(关于电影 *Hackers* 有这样一件真实的事情，当时MGM/United Artists公司的万维网主页很快就被人更改了，被加上了一段对电影 *Hackers* 的不恭敬评论，并建议观众去看电影 *The Net*。Paramount电影公司否认对此事负责[399]。)另一部电影 *Sneakers* 则讲述了那些为自己和政府测试计算系统(和其他系统)安全性的人的故事。

本书目标

本书有三大目标。第一个目标是要展示理论和实践二者之间的重要性。通常的情况是，实干家认为理论毫无用处，而理论家认为实践太肤浅。事实上，理论与实践是共生的。例如，隐信道理论的目的是限制进程通过使用共享资源进行通信的能力，为评价那些限制进程的机制(比如沙箱和防火墙)的有效性提供依据。类似地，在商业领域中交易实践也会导致若干安全策略模型的发展，如Clark-Wilson模型和中国墙模型。反过来，这些模型又帮助安全策略的设计者更好地理解和评价这些用于提供安全保护的机制和规程。

第二个目标是要强调计算机安全与密码学是两个不同的领域。虽然密码学是计算机安全的核心部分，但它决不是惟一的部分。密码学为实现特定功能提供机制，如防止非授权用户读取或篡改网络消息等。但是，除非系统开发者理解他们运用的密码学技术所作用的特定环境，并且该密码协议与密码机制的假设基础也适用于这种特定环境，否则密码学技术不能为系统提高安全性有所贡献。一个典型的实例是在两个低安全等级的系统之间使用密码技术进行安全通信。如果只有可信用户可以访问这两个系统，密码技术确实能保护消息的传输。但如果

① 19.4节将讨论计算机蠕虫。

非可信用户也能访问这两个系统之一(通过合法账号,更可能的情况是入侵系统),则密码技术就不足以保护传输的信息,攻击者可在任意一个端点读取信息。

第三个目标是要阐明计算机安全学不仅仅是一门科学,而且还是一门艺术。计算机安全学之所以是一门艺术,是因为任何不经过使用性检测的系统都不能被认为是安全系统。"安全计算机"的定义要求系统需求的声明和表达必须以授权操作和授权用户的形式出现。(一台用于大学的计算机因为学校的工作性质,它可以被认为是安全系统。但是当将它用于军事装置中时,因为这种工作性质的改变,就可能会认为同一个系统不能提供足够的安全控制。)人应该如何像其他计算机一样与计算机系统交互呢?设计者设计出的接口必须具备何种程度的清晰性和限制性,才能使得在防止非授权用户访问系统数据和资源时不会导致系统失效?

正如艺术家要在画布上描绘出他眼中的真实世界一样,安全领域的设计者也要清晰地表达出他对系统安全策略和安全机制中人机交互的具体理解。为达到同一个目的,两类设计者可能会做出两种完全不同的设计,正如两个艺术家为了表达同一个概念却使用了两个不同的主题一样。

计算机安全学也是一门科学,其理论基础是数学的构造、分析与证明,其系统是按照已被接受的工程实践标准来搭建的系统。计算机安全学从关键的公理出发,使用演绎与推理的方法检验系统的安全性,并揭示有关安全的基本原理。这些科学原理可以推广到非传统领域,并应用于新的理论、策略和机制。

指导思想

要理解计算机安全中存在的问题,关键是要认识到这些问题都不是新问题,它们都是老问题,可追溯到计算机安全的研究初期(实际上,这些问题源自于非计算机领域的并行问题)。但随着计算科学领域的变化,计算机安全的研究重点也在变化。在20世纪80年代中期以前,大型机和中型机统治着市场,计算机安全的问题和解决方案主要还是针对单个系统的文件安全和进程安全。随着网络和Internet的兴起,计算机安全的领域发生了变化。现在是工作站、服务器以及连接它们的网络基础设施统治着市场,计算机安全问题及其解决方案主要针对当前的网络环境。如果将工作站、服务器和网络基础设施视为一个单独的系统,则20世纪80年代中期以前发展起来的模型、理论和问题表达,同样也能很好地适用于现在的系统。

关于安全保障问题的研究就是一个例子。在早期,安全保障技术以几种形式出现:正确性的形式化方法和证明、对策略是否满足规范的验证、从可靠信源中采集数据和程序,等等。这些提供保障性的方法分析了单一系统、系统代码和可获得代码的信源(软件提供商或用户),以确保源代码的可信性或者可充分地限制程序的破坏性。到了后期,应用的还是同样的基础原理与技术,不同的是某些领域已经得到了巨大的扩展(从单一系统和少量的软件提供商发展到现在覆盖全球的Internet)。携带证明代码就是这样的一个例子,它是一种新发展起来的令人振奋的技术:可下载程序模块满足某种规定策略的证明与程序本身结合在一起①。携带证明代码扩展了证明程序与策略一致的概念,是对早期技术的扩展。但是要正确理解这种技术,就必须理解携带证明代码的基础思想和这些思想的早期版本。

① 19.6.5.1节将讨论携带证明代码。

另一个例子是 Saltzer 和 Schroeder 的安全设计原则[①]。这些原则发表于 1975 年，它们提倡简单性、限制性和可理解性。如果安全机制变得过于复杂，攻击者就能逃避或绕开它们。可惜的是，许多程序员和软件提供商只在自己的系统和服务器被攻击者入侵时才知道这个事实。认为这些原则老了，在某种程度上过时了的论调显得如此空洞，因为违反这些原则往往就意味着不安全系统的出现。

早期的研究工作往往针对于现在已经不存在的系统，或者针对那些和现代系统有许多区别的系统，但这无损于早期研究的思想与概念，它们依然是现在研究工作的基础。一旦可以正确地理解这些思想与概念，就可以将它们应用在大多数环境当中。而且，随着新的计算形式的出现，现在的机制与技术也会变得过时，只具历史意义，但基础原则将继续存在，成为下一代的计算技术的基础。

本书的指导思想是：确定的关键概念构成计算机安全所有领域的基础，对不同的计算机安全领域的研究也同时加深了对不同领域的理解。而且，对于安全相关技术和方法的应用和理解的评论也是对这些应用的基础理论的一种理解。

计算机安全理论的发展指明了安全系统的理论基础。抽象建模、为特定系统建模等的研究可使系统设计达到明确的、有益的目的。广义安全问题的不可判定性[②] 又指出了计算机安全的局限性。

这些理论成果的应用提高了被保护系统的安全质量。然而，问题是这些模型（和理论）的假设与这些理论所应用的实际环境在多大程度上保持一致？虽然该如何应用这些抽象概念的知识在不断增加，但是要正确地把真实框架中的相关信息转移到分析框架中去，却依然存在困难。这种抽象往往将重要信息排除在外，而那些被忽略的数据又以不明显的方式与安全相关。没有这些信息，分析就存在缺陷。

遗憾的是，不可能有单独的著作能够覆盖计算机安全的所有领域，所以本书只关注计算机安全中——就作者的观点而言——最基础、最普遍的领域，并使用例子来证明这些原理的实用性。

本书组织

本书的组织反映了本书的指导思想。首先介绍的是基础与原理，目的是为安全的有效分析与建模设定界限。这些原理为表达、分析系统安全需求提供了理论框架。安全策略限定了系统禁止与允许的操作，机制为实现安全策略提供能力。机制在何种程度上实施了策略，而策略又在何种程度上满足系统的需求，这属于安全保障问题。接着讨论那些利用策略、实现和安全保障的漏洞而进行的攻击，同时也讨论了为这些攻击提供信息的若干机制。最后，作为总结，介绍若干理论与策略的应用，它们都针对现实的状况。这种自然递进的讲述方式强调了计算机安全领域中现有原理的发展与应用。

第 1 章描述计算机安全学所关心的问题，并探讨计算机安全所面临的问题和挑战。它为其他章节的展开打下了基础。

---

① 第 12 章将讨论这些原则。
② 见 3.2 节。

第 2 章和第 3 章处理一些基础问题，比如该如何清楚地、实用地定义“安全”？安全是否是现实的？安全是否可判定？

第 4 章到第 7 章探讨策略与安全之间的关系。安全的定义依赖于策略。这几章中将探讨若干策略类型，包括经常出现的信任的基础问题、策略分析和使用策略约束操作与转换等。

第 9 章到第 12 章讨论密码学及其在安全中的地位，重点关注应用以及密钥管理、密钥分配和网络中的密码系统等问题。最后简单介绍认证理论。

第 13 章到第 16 章研究如何使用面向系统的技术来实现策略所定义的需求。特定的设计原则是有效的安全机制的基础。策略定义了谁能进行操作、操作对象是什么，因此身份就是系统实现的关键。实现访问控制和信息流控制的机制从不同的侧面实施安全策略。

第 17 章和第 18 章介绍评估系统或产品满足其设计目标的概念与标准。

第 19 章到第 22 章讨论涉及计算机安全的其他方面。恶意代码挫败了许多安全机制。尽管我们尽最大的努力提供高安全保障性，但今天的系统还是充满了漏洞，为什么？怎么才能分析或检测出系统漏洞？哪些模型能帮助我们改善现状？给定安全漏洞，如何才能检测出利用这些漏洞的攻击者？对审计技术的讨论自然引出了对入侵检测技术的讨论。

第 23 章到第 26 章给出了一些实例，展示如何应用本书所讨论的原理。首先给出网络的实例，进而给出系统、用户和程序的实例。每一章都描述一种策略，然后显示如何将该策略转换成支持该策略的机制和规程。这一部分试图阐明适用于其他领域的资源能够、也应该能够被用于实践。

本书的每一章后都有一个小结和对进一步阅读的建议。每章小结进一步突出了本章的重要思想。感兴趣的读者如果想对某些主题做更深入的研究，可以参考这些推荐读物。这些推荐读物扩充了章节的内容，或提出了另外一些有趣的方法。

本书与《计算机安全学——安全的艺术与科学》的区别

本书与《计算机安全学——安全的艺术与科学》（由电子工业出版社翻译出版，书号：7-121-00780-0）的区别在于它们分别针对不同的读者。本书是后者的简写版，省略了大量的数学表达。本书更适合于数学背景稍弱，或者对数学表达不感兴趣，或者更关注实践而非理论的计算机安全工作者或学生。

本书的计算机安全基础与策略部分没有讲述涉及形式化模型和安全可判定性限制的推导的若干结论（尽管还是给出了中心结论，即广义可靠性问题是不可判定问题）。某些现在已经不再使用但在安全策略模型发展过程中起到重要作用的模型被省略了，比如不可推导模型和不干涉模型。而且，在安全保障部分省略了形式化方法的讲述和对安全系统设计、构建的详细讨论。本书保留了对基本概念和思想的讲解，尤其是与参考监视器相关的基本概念和思想，并且讨论了通常都会使用到的评价准则。

之所以存在这些不同，是因为这两本书所针对的读者的背景不同。本书针对不具备高级数学概念的读者，也针对不包括形式化方法详细讲解的课程，比如某些课程可以不讲解开发高保障系统所必须的形式化方法，但又希望学生了解高保障系统的基本思想。这种情形经常出现，如果学生的知识背景不足以理解书中的理论细节，即使教师不讲解形式化方法，学生们也会对书中的形式化描述倍感压力。本书的前身则针对教师希望讲解而学生又具备能力自学大

量计算机安全数学背景和形式化方法的课程。

某些学生更适合通过主题的非形式化描述进行学习。该领域的基本思想和原理的直观表达是什么？实践工作者如何运用这些基本思想和原理来提高当前的技术水平？本书更适合于这一类学生。还有一类学生更喜欢教师将直观思路抽象到对基础概念的形式化描述。如何才能形式化这种直观描述？如何严格地应用这种思想来构建安全系统(对某种适合的安全定义)？《计算机安全学——安全的艺术与科学》一书更适合于这类学生。

实践工作者如果对计算机安全的基础原理的形式化讲解不感兴趣，那么本书将更适合他们。本书保留了对基本原理直观的、非形式化的讲解，但用到了少量的数学表达式。实践工作者会发现本书更精简，可能更容易阅读，因为不会受到他们认为不相关的内容的干扰。

特别致谢

Elisabeth Sullivan 写了本书的安全保障部分(第 17 章和第 18 章)。她为此写出了多份手稿，显示了她在计算机安全领域的广博知识及经验。我要尤其感激她所贡献出的在处理安全保障问题中的实际经验。通常，某些书籍只叙述安全保障的理论，而没有认识到某些其他方面也同等重要，且被更广泛地使用。感谢 Liz，她的特别贡献使得本书的安全保障这一部分显得尤为卓越。仿佛这还不够，她还为本书的策略部分提出了若干宝贵的改进意见。我将永远感激她的贡献和幽默，特别是她的友谊。

致谢

许多人为本书做出了贡献。Peter Salus 的建议首先激起了我写此书的意愿，Peter 促进了我与 Addison-Wesley 出版社的接触。在写作本书的过程中，Blaine Burnham 审阅了已完成部分和写作计划，并提出了几种重新组织本书内容的建议。本书现在的组织形式源于他的建议。Marvin Schaefer 以敏锐的眼光审阅了本书的若干部分，他的建议使得许多内容得到了改进，并一直激励我完成写作。感谢这三个人的贡献。

许多人以不同的方式为本书做出了贡献。特别感谢 Steven Alexander, Jim Alves-Foss, Bill Arbaugh, Andrew Arcilla, Alex Aris, Rebecca Bace, Belinda Bashore, Vladimir Berman, Ziad El Bizri, Logan Browne, Terry Brugger, Serdar Cabuk, Raymond Centeno, Lisa Clark, Michael Clifford, Christopher Clifton, Dan Coming, Kay Connelly, Crispin Cowan, Tom Daniels, Dimitri DeFigueiredo, Joseph-Patrick Dib, Jeremy Frank, Robert Fourney, Martin Gagne, Ron Gove, James Hinde, Xuxian Jiang, Jesper Johansson, Mark Jones, Calvin Ko, Mark-Neil Ledesma, Ken Levine, Karl Levitt, Yunhua Lu, Gary McGraw, Alexander Meau, Nasir Memon, Mark Morrissey, Ather Nawaz, Iulian Neamtiu, Kimberly Nico, Stephen Northcutt, Rafael Obelheiro, Josko Orsulic, Holly Pang, Ryan Poling, Sung Park, Ashwini Raina, Jorge Ramos, Brennen Reynolds, Peter Rozental, Christoph Schuba, David Shambroom, Jonathan Shapiro, Clay Shields, Sriram Srinivasan, Mahesh V. Tripunitara, Tom Walcott, James Walden, Dan Watson, Guido Wedig, Chris Wee, Patrick Wheeler, Paul Williams, Bonnie Xu, Xiaoduan Ye, Lara Whelan, John Zachary, Aleksandr Zingorenko。同样要感谢选择我的计算机安全课程的学生们，是他们(自觉或不自觉地)帮助我逐步完成并测试了本书的内容。

Addison-Wesley 出版社的工作人员 Kathleen Billus, Susannah Buzard, Bernie Gaffney, Amy Fleischer, Helen Goldstein, Tom Stone, Asdis Thorsteinsson, 特别是本书的编辑 Peter Gordon 以不可置信的耐心给了我巨大的帮助，尽管我担心此书永远都不可能出版。本书得以出版，很大程度上得益于他们的辛勤工作与鼓励。我还要感谢 Rob Mauhar 和 Elizabeth Ryan 的出色工作。

Dorothy Denning，我研究生阶段的导师，在我接触计算机安全领域时，是她在为我指点迷津。Peter Denning, Barry Leiner, Karl Levitt, Peter Neumann, Marvin Schaefer, Larry Snyder 等人影响了我在这个领域中的研究道路。我希望本书能以某些方式反映出他们对我的影响，并能将这种影响的一小部分传递给我的读者。

还要感谢我的双亲 Leonard Bishop 和 Linda Allen。我父亲是一位作家，他教给我许多写作的技巧，我一直都在学习。我母亲是图书代理商，她帮助我熟悉图书出版的整个过程，并一直都在支持我。

最后，我要感谢我的家庭，是他们在支持着我的整个写作过程。有时，他们怀疑我是否可以完成这本书。我的妻子 Holly 和我们的孩子 Steven, David 和 Caroline 非常有耐心且善解人意，是他们保证我有时间来写这本书。我们的大女儿 Heidi 和她的丈夫 Mike 也给予我很多的关爱与鼓励。还有最奇妙的消遣：我们的孙子——Skyler。献给你们，我的爱与感激。

目　录

第 1 章　计算机安全概述 …… 1
1.1　基本安全服务 …… 1
1.2　威胁 …… 3
1.3　策略与机制 …… 5
1.4　假设与信任 …… 6
1.5　安全保障 …… 7
1.6　运作问题 …… 10
1.7　人为因素 …… 12
1.8　整合 …… 14
1.9　本章小结 …… 15
1.10　进阶阅读 …… 15
1.11　习题 …… 15

第 2 章　访问控制矩阵 …… 18
2.1　保护状态 …… 18
2.2　访问控制矩阵模型 …… 18
2.3　保护状态转换 …… 20
2.4　本章小结 …… 23
2.5　进阶阅读 …… 24
2.6　习题 …… 24

第 3 章　基础结论 …… 25
3.1　一般性问题 …… 25
3.2　基本结果 …… 26
3.3　本章小结 …… 29
3.4　进阶阅读 …… 29
3.5　习题 …… 30

第 4 章　安全策略 …… 31
4.1　安全策略 …… 31
4.2　安全策略的类型 …… 33
4.3　信任的角色 …… 34
4.4　访问控制的类型 …… 36
4.5　示例:学院式计算机安全策略 …… 37
4.6　本章小结 …… 39

4.7 进阶阅读 …… 39
4.8 习题 …… 40

第5章 保密性策略 …… 41
5.1 保密性策略的目标 …… 41
5.2 Bell-LaPadula 模型 …… 41
5.3 本章小结 …… 47
5.4 进阶阅读 …… 47
5.8 习题 …… 48

第6章 完整性策略 …… 49
6.1 目标 …… 49
6.2 Biba 完整性模型 …… 50
6.3 Clark-Wilson 完整性模型 …… 51
6.4 本章小结 …… 55
6.5 进阶阅读 …… 55
6.6 习题 …… 55

第7章 混合策略 …… 56
7.1 中国墙模型 …… 56
7.2 医疗信息系统安全策略 …… 59
7.3 创建者控制的访问控制 …… 61
7.4 基于角色的访问控制 …… 63
7.5 本章小结 …… 64
7.6 进阶阅读 …… 64
7.7 习题 …… 65

第8章 密码学基础 …… 66
8.1 什么是密码学 …… 66
8.2 古典密码系统 …… 67
8.3 公钥密码学 …… 77
8.4 密码校验和 …… 79
8.5 本章小结 …… 81
8.6 进阶阅读 …… 81
8.7 习题 …… 81

第9章 密钥管理 …… 84
9.1 会话密钥和交换密钥 …… 84
9.2 密钥交换 …… 85
9.3 密钥基础设施 …… 89
9.4 密钥备份与吊销 …… 93
9.5 数字签名 …… 94

9.6 本章小结 …… 96
9.7 进阶阅读 …… 97
9.8 习题 …… 98

第 10 章 密码技术 …… 99
10.1 问题 …… 99
10.2 流密码和分组密码 …… 100
10.3 网络与密码学 …… 104
10.4 协议实例 …… 106
10.5 本章小结 …… 115
10.6 进阶阅读 …… 115
10.7 习题 …… 116

第 11 章 认证 …… 117
11.1 认证基础 …… 117
11.2 口令 …… 117
11.3 挑战-应答 …… 127
11.4 生物测定学 …… 129
11.5 地理位置 …… 131
11.6 多重认证方法 …… 132
11.7 本章小结 …… 133
11.8 进阶阅读 …… 133
11.9 习题 …… 134

第 12 章 设计原则 …… 136
12.1 概述 …… 136
12.2 设计原则 …… 137
12.3 本章小结 …… 141
12.4 进阶阅读 …… 141
12.5 习题 …… 141

第 13 章 身份表达 …… 143
13.1 什么是身份 …… 143
13.2 文件与客体 …… 143
13.3 用户 …… 144
13.4 群组与角色 …… 145
13.5 命名与证书 …… 145
13.6 应用于 Web 的身份 …… 149
13.7 本章小结 …… 158
13.8 进阶阅读 …… 158
13.9 习题 …… 159

第 14 章　访问控制机制 …… 160
14.1　访问控制列表 …… 160
14.2　能力表 …… 166
14.3　锁与钥匙 …… 170
14.4　基于环的访问控制 …… 172
14.5　传播性访问控制列表 …… 173
14.6　本章小结 …… 174
14.7　进阶阅读 …… 175
14.8　习题 …… 175

第 15 章　信息流 …… 177
15.1　基础与背景 …… 177
15.2　基于编译器的机制 …… 178
15.3　基于执行的机制 …… 188
15.4　信息流控制实例 …… 191
15.5　本章小结 …… 192
15.6　进阶阅读 …… 193
15.7　习题 …… 193

第 16 章　限制问题 …… 194
16.1　限制问题的由来 …… 194
16.2　隔离 …… 196
16.3　隐信道 …… 198
16.4　本章小结 …… 206
16.5　进阶阅读 …… 206
16.6　习题 …… 206

第 17 章　安全保障导论 …… 208
17.1　安全保障与信任 …… 208
17.2　构建安全可信的系统 …… 212
17.3　嵌入或添加安全机制 …… 218
17.4　本章小结 …… 220
17.5　进阶阅读 …… 220
17.6　习题 …… 220

第 18 章　系统评估 …… 222
18.1　形式化评估的目标 …… 222
18.2　TCSEC:1983－1999 …… 223
18.3　FIPS 140:1994－现在 …… 229
18.4　通用标准:1998－现在 …… 230
18.5　SSE-CMM:1997－现在 …… 239

18.6 本章小结 …… 241
18.7 进阶阅读 …… 242
18.8 习题 …… 242

第 19 章 恶意代码 …… 244
19.1 简介 …… 244
19.2 特洛伊木马 …… 244
19.3 计算机病毒 …… 245
19.4 计算机蠕虫 …… 251
19.5 其他形式的恶意代码 …… 252
19.6 恶意代码的防御 …… 253
19.7 本章小结 …… 259
19.8 进阶阅读 …… 259
19.9 习题 …… 260

第 20 章 漏洞分析 …… 261
20.1 简介 …… 261
20.2 渗透研究 …… 262
20.3 系统漏洞分类 …… 271
20.4 框架 …… 273
20.5 本章小结 …… 281
20.6 进阶阅读 …… 282
20.7 习题 …… 282

第 21 章 审计 …… 284
21.1 定义 …… 284
21.2 剖析审计系统 …… 285
21.3 设计审计系统 …… 287
21.4 事后设计 …… 291
21.5 审计机制 …… 293
21.6 实例:审计文件系统 …… 295
21.7 审计信息浏览 …… 300
21.8 本章小结 …… 302
21.9 进阶阅读 …… 302
21.10 习题 …… 303

第 22 章 入侵检测 …… 304
22.1 原理 …… 304
22.2 基本的入侵检测 …… 304
22.3 模型 …… 306
22.4 体系结构 …… 310