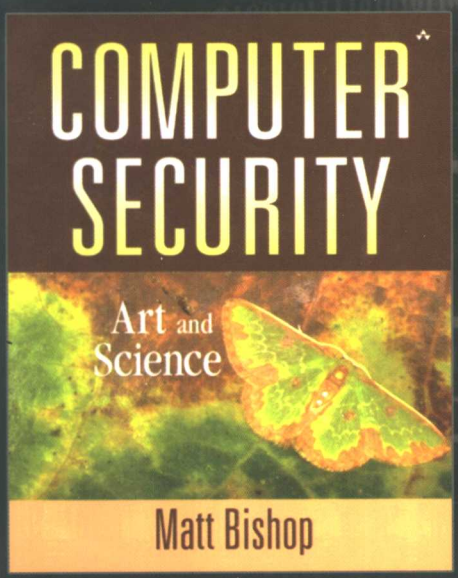
国外计算机科学教材系列

计算机安全学

——安全的艺术与科学

Computer Security

Art and Science



[美] Matt Bishop 著

王立斌 黄征 等译

陈克非 审校

PEARSON Addison Wesley

PHEI

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

——安全的艺术与科学

Computer Security

Art and Science

[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

本书系统地介绍了计算机安全的基本原理与应用技术。全书包括九大部分，其中安全策略模型部分详细讨论了多种不同安全策略模型的原理，包括Bell-LaPadula模型、Biba模型、中国墙模型、Clark-Wilson模型等。密码学部分重点介绍密码学的应用，包括密钥管理与密钥托管、密钥分配、网络中的密码系统以及认证理论等问题。非密码学的安全机制部分介绍计算机安全实现中的多方面内容，包括安全设计原则、身份表达、访问控制实施、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、审计、入侵检测等原理与技术。安全保障部分介绍可信系统的构建与评估的理论与技术，包括安全保障原理、形式化验证和可信系统评估标准等。本书还包含大量的实例、科技文献介绍以及实践内容，为帮助读者阅读，还介绍了书中用到的数学知识。

本书内容广博，实例详尽，具有很高的理论与实践参考价值，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。

Simplified Chinese edition Copyright © 2005 by PEARSON EDUCATION ASIA LIMITED and Publishing House of Electronics Industry.
Computer Security: Art and Science, ISBN: 0201440997 by Matt Bishop. Copyright © 2003.
All Rights Reserved.
Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Addison-Wesley.
This edition is authorized for sale only in the People's Republic of China (excluding the Special Administrative Region of Hong Kong and Macau).

本书中文简体字翻译版由电子工业出版社和Pearson Education培生教育出版亚洲有限公司合作出版。未经出版者预先书面许可，不得以任何方式复制或抄袭本书的任何部分。
本书封面贴有 Pearson Education 培生教育出版集团激光防伪标签，无标签者不得销售。

版权贸易合同登记号　图字：01-2003-6238

图书在版编目（CIP）数据

计算机安全学——安全的艺术与科学/（美）毕晓普（Bishop, M.）著；王立斌等译.
北京：电子工业出版社，2005.5
（国外计算机科学教材系列）
书名原文：Computer Security: Art and Science
ISBN 7-121-00780-0

Ⅰ.计...　Ⅱ.①毕...②王...　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035653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：46　字数：1178千字
印　　次：2005年5月第1次印刷
定　　价：65.00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

主　任　杨芙清　北京大学教授
中国科学院院士
北京大学信息与工程学部主任
北京大学软件工程研究所所长

委　员　王　珊　中国人民大学信息学院院长、教授

胡道元　清华大学计算机科学与技术系教授
国际信息处理联合会通信系统中国代表

钟玉琢　清华大学计算机科学与技术系教授
中国计算机学会多媒体专业委员会主任

谢希仁　中国人民解放军理工大学教授
全军网络技术研究中心主任、博士生导师

尤晋元　上海交通大学计算机科学与工程系教授
上海分布计算技术中心主任

施伯乐　上海国际数据库研究中心主任、复旦大学教授
中国计算机学会常务理事、上海市计算机学会理事长

邹　鹏　国防科学技术大学计算机学院教授、博士生导师
教育部计算机基础课程教学指导委员会副主任委员

张昆藏　青岛大学信息工程学院教授

试读结束，需要全本PDF请购买 www.ertongbook.com

译 者 序

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全关系到我们社会及我们每个人。在过去的十多年中，计算机和网络的安全面临着越来越严峻的挑战，如何保障计算机系统安全成为一个充满刺激并富有活力的研究领域。

目前，一个以密码为核心技术，以访问控制为基本手段，包括实现系统保护、事件检测、应急响应、灾难恢复等内容的安全理论体系正在形成，计算机安全已经从早期过多依赖于个人灵感和智慧的经验积累，逐步发展成为建立在数学和逻辑基础上、有一套严格的形式化方法、较为完整的实验手段的科学体系。

1984 年，本书作者 Matt Bishop 在美国普度大学获得博士学位，现在是加州大学 Davis 分校计算机科学系教授，是计算机安全领域国际顶尖的专家，他在漏洞分析、系统安全、访问控制的形式化方法、用户认证等方面取得了业界公认的成就。

本书是迄今为止比较全面系统地介绍计算机安全的基本原理与应用技术的教材，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，从而有力地阐明了计算机安全学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、访问控制实施、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、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、形式化验证和可信系统评估标准等。本书内容丰富，并有大量详尽的实例，可作为高年级本科生、研究生和从事信息安全、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，同时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、张伟德等也参与了本书部分章节的翻译和校对工作。全书由陈克非统稿并审校。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[432]① 在 4 小时之内使 Internet 上的大约 5000 台计算机瘫痪。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[374]。

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，最终导致攻击者被捕[914]。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[448]。）另一部电影 *Sneakers* 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。

目标

本书有三大目标。第一个目标是要展示理论和实践相互之间的重要性。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）的有效性而提供依据。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。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。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，更可能的情况是侵入系统），则密码技术就不足以保护消息传输。攻击者可在任意一个端点读取信息。

① 22.4 节将讨论计算机蠕虫。

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，是因为如果系统不经过使用性检测，则没有任何系统可被认为是安全的。“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大学的工作性质，它可以被认为足够安全。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。）人应该如何与其他计算机一样，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，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画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。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。

主导思想

要理解计算机安全学中存在的问题，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。随着网络与 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备统治着市场，计算机安全问题及其解决方案主要针对当前的网络环境。但是，如果将工作站、服务器和网络支持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。

例如，关于安全保障问题的研究。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。

另一个例子是 Saltzer 和 Schroeder 的安全设计原则②。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。那些

① 22.7.5.1 节将讨论携带证明代码。
② 第 13 章将讨论这些原则。

说这些原则老了，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，只具历史性意义，但基础原则将继续存在，成为下一代的——当然是下一个时代的——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，并且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、为特定系统建模等研究可使系统设计达到明确的、有益的目的。策略复合的理论[①] 和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。很多研究工作正在不断地尝试突破这些局限。

这些理论结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，可是，没有这些信息，分析就存在缺陷。

实践工作者必须同时具备两个方面的知识：计算机安全科学与艺术的理论与实践。理论阐明什么是可能的，而实践知识表明什么是可行的。理论家需要理解理论应用的限制和理论中隐含假设的真实程度，以及将理论转变为实践工具与技术的方法，本书正努力满足这些要求。

可惜，不可能有单独的著作能够覆盖计算机安全的所有领域，所以本书关注于计算机安全中——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应用。

本书组织

本书的组织反映了本书的指导思想。首先介绍的是数学基础与原理，目的是为安全的有效分析与建模设定界限。这些数学原理为表达、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，则属于安全保障问题。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，它们都针对于现实状况。这种自然递进的讲述方式强调了计算机安全领域中现存原理的发展与应用。

第一部分描述什么是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。

第二部分处理一些基础问题，比如，如何正确地、实用地定义“安全”？安全是否是现实的？是否是可判定的？什么样的安全是可判定的，在何种条件下它是可判定的？如果不可判定，如何限制定义使得它可被判定？

① 见第8章。
② 见3.2节。

第三部分探讨了策略与安全之间的关系。“安全”的定义依赖于策略。这一部分探讨了若干策略类型，包括经常存在的信任的基础问题、策略分析和使用策略约束操作与转换等。

第四部分讨论了密码学及其在安全中的地位。本部分重点关注于应用，并讨论密钥管理与密钥托管、密钥分配和网络中的密码系统等问题。最后简单介绍了认证理论。

第五部分研究如何使用面向系统的技术来实现策略所带来的需求。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方面实施安全策略。

第六部分介绍评价系统或产品满足目标程度的方法与技术。介绍完特定的背景知识后，为了准确地解释什么是“安全保障”，本部分还讨论了可满足不同等级安全保障需求的系统构建艺术。形式化验证方法占据了重要地位。第六部分还显示，标准的发展提高了人们对安全保障技术的理解。

第七部分讨论了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？怎么分析才能检测出系统漏洞？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？本部分对审计技术的讨论自然引出了对入侵检测技术的讨论。

第八部分给出实例，展示如何应用本书所讨论的原理。首先给出网络的实例，然后给出系统、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。第八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，还有对一些研究议题的描述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。研究议题是现在的“热点课题”或者是那些可被证明是推动计算机安全学发展的沃土课题。感兴趣的读者如果想对这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。

阅读建议

本书既是一本参考书也是一本教材，它的读者是本科生、研究生和实践工作者。本节为着手阅读本书的读者提出一些建议。

依赖关系

第 1 章是全书的基础，应首先阅读。之后，读者就不需要按章节顺序阅读。每章之间的依赖关系如下所示。

第 3 章依赖于第 2 章，并且要求相当程度的数学知识。相反，第 2 章则不这样要求。第 3 章的内容在很大程度上并不会被其他章节使用(虽然第一节中的关键结论的存在性、不可判定定理会不断地被提及)。如果读者的兴趣不在这个方面，可放心地跳过这一章的内容。

第三部分的各章之间相互关联。第 5 章的形式化方法还会在第 19 章、第 20 章中被使用，但仅此而已。除非读者打算钻研这些章节的定理证明和形式化映射，否则这些形式化方法也可跳过。第 8 章的内容要求一定程度的数学知识，且这些内容在其他章节使用得很少。像第 3 章那样，如果读者的兴趣不在这些内容上面，第 8 章也可跳过。

第 9 ~ 11 章也是按顺序前后关联的。这些章节的内容对于学过基础密码学的读者将会比较简单，但这些内容不要求第 3 章和第 8 章的数学基础。第 12 章不需要使用第 10 章和第 11 章的内容，但它要用到第 9 章的知识。

第 13 章的知识在整个第五部分都要用到。如果读者曾经学过本科水平的操作系统课程，那么他对第 15 章就不会感到困难。第 14 章使用了第 11 章的内容；第 16 章建立在第 5,13,15 章的基础之上；而第 17 章使用了第 4,13,16 章的内容。

第 18 章依赖于第 4 章的知识。第 19 章建立在第 5,13,15,18 章之上。第 20 章介绍了高度抽象的数学概念，并使用第 18,19 章的内容。第 21 章基于第 5,18,19 章的内容，但它不要求第 20 章的内容。软件工程的知识将非常有助于整个第五部分的学习。

第 22 章吸收利用了第 5,6,9,13,15,17 章的思想和知识(要理解 22.6 节，读者必须读 3.1 节的内容)。第 23 章是自包含的，虽然它隐含地使用了许多来自安全保障机制的思想。第 23 章还要求编译器、操作系统和某些网络的指导性知识。因为很多的系统漏洞都来自不同版本 UNIX 系统或 Windows 系统，所以对这两种系统的工作经验将有助于理解这一章的某些内容。第 24 章使用了第 4 章的知识，而第 25 章使用了第 24 章的知识。

第八部分的章节都是自包含的，不需要除了第 1 章以外的其他章节。然而它们也指出了其他章节中相关的内容，这些内容扩充了这一章的知识，并且(希望是)提高了读者对这些知识的理解。

背景知识

本书的内容处于高年级本科生水平。整本书都假设读者熟悉基础编译器、计算机体系结构(比如程序栈的使用)和操作系统等课程。读者也应当对模数运算(用于密码学部分)具备一定的基础。某些内容，比如形式化方法(见第 20 章)和计算机安全的数学理论(第 3 章和策略模型的形式化表达)，要求一定的数学基础。其他特定的背景知识都在各章的先头章节进行介绍。第九部分的内容将对那些缺乏某些背景知识的读者起到帮助作用。

本书的实例来自于多种系统。许多实例来自 UNIX 操作系统或它们的变形系统(如 Linux 系统)。其他的来自于 Windows 系列系统。熟悉这些系统将有助读者更容易、迅速地理解许多实例。

本科程度

本科生的课程一般更注重于理论的应用及学生如何使用教材。对课程内容的特定选择与安排依赖于课程所关注的焦点，但课程必须覆盖某些基础内容，特别是第 1,9,13 章的内容和 2.1 节，2.2 节讨论的访问控制矩阵的概念。

提出真实的问题和解决方案通常比抽象的表达更能激发本科生的兴趣。特别专题和实践科目为此提供了大量的实践问题和方法。这也自然而然地引出更深层次的问题：策略、密码学、非密码学机制和安全保障机制。以下章节适合用于非数学专业本科生的课程。

- **策略**：4.1～4.4 节描述了策略的概念。教师应该从 5.1,5.2.1,6.2,6.4,7.1.1,7.2 节中选取一到两个实例，非形式化地描述若干策略模型。7.4 节讨论了基于角色的访问控制。
- **密码学**：10.1 节和 10.2 节讨论密钥分配，而在 10.4.2 节讨论了一种一般形式的公钥基础设施(PKI)。11.1 节指出使用密码技术的若干普遍错误。11.3 节展示如何在网络中使用密码技术，教师应当选用 11.4 节中的某个协议作为例子讲解。第 12 章介绍了多种形式的认证方法，其中包括非密码学的方法。

试读结束，需要全本PDF请购买 www.ertongbook.com

- **非密码学机制**:身份是许多访问控制机制的基础。14.1 ~ 14.4 节讨论了系统中的身份,而 14.6 节讨论了 Web 中的身份和匿名性。15.1 节,15.2 节探讨了两种控制文件访问的机制,而 15.4 节讨论了了基于环的机制,它是多级权限概念的基础。如果需要,教师可使用 17.1 节和 17.2 节来讲述沙箱,但因为 17.2 节使用了 4.5 节和 4.5.1 节中的内容,所以教师还需要同时介绍这些章节的内容。
- **安全保障机制**:第 18 章是安全保障机制的基础绪论,这些主题经常被忽视。

研究生程度

通常,研究生的介绍性课程要比本科生的课程更注重于主题的深度。如本科生课程一样,研究生课程也应当包括第 1,9,13 章。同样重要的还有 3.1 节和 3.2 节的不可判定结论,这些内容需要用到第 2 章的内容。除此以外,教师还可从大量的专题中选择需要的内容,以适当的深度进行讲述。以下章节适合于研究生教学。

- **策略模型**:第三部分包括了许多一般性的策略模型,有形式化模型也有非形式化模型。一旦理解了非形式化模型,就可更容易地理解形式化模型。5.4 节的讨论对于没有考虑过策略的地位和性质的学生显得特别有启发性。第 8 章是对策略的基础的高度形式化讨论,适合于具备形式化数学知识的学生。没有这种背景的学生将会觉得它非常困难。
- **密码学**:第四部分的重点是密码学的应用,而不是密码学的数学基础①。此部分讨论的是密码学应用的关键领域,比如密钥管理和某些应用于网络的基础密码协议。
- **非密码学机制**:身份及验证问题是复杂的,且普遍没有得到良好的理解。14.5 节包含这些问题。将这部分的内容与 Web 身份问题的讨论(14.6 节)结合,就可提出信任与命名的问题。第 16 章和第 17 章探讨了信息流及限制信息流的问题。
- **安全保障机制**:传统上,安全保障是作为形式化方法来讲授的,并且第 20 章也是为这个目的服务的。然而,在实践中,安全保障机制更常使用的方法是结构化过程和技术,或者合理性证明、映射和分析等非形式化但论证严格的方法。第 21 章讨论了评价标准,它依赖于第 18 章和第 19 章的内容以及第 20 章的某些思想。
- **其他专题**:22.6 节介绍了一种一般性判定问题的证明,即一个一般程序是否是病毒实际上是一个不可判定的问题。在 23.2 节研究的渗透理论和 23.5 节介绍的更形式化的方法阐明了系统的漏洞分析。如果教师想更深入地介绍入侵检测(第 25 章),他必须知道这种讨论要大量使用审计的内容(第 24 章)。
- **实践**:第八部分将本书之前的内容与现实世界的实例联系起来,并强调之前讨论的理论与方法的应用。

实践工作者

计算机安全领域的实践工作者可在本书找到许多他们感兴趣的内容。目录可以帮助他们查找特定的专题。一个更通用的方法是:从第 1 章开始阅读,然后立刻跳到第八部分。这一部分的所有章节都有对本书其他部分的引用说明,可解释清楚这些内容的基础所在。这使得读者可更深入地理解,为什么在实践中要运用这些策略、设置、配置和建议。这种方法也使得读者可以更关注于他们感兴趣的专题。

---

① 感兴趣的读者可以找到有关这方面内容的大量书籍,如[240,590,695,702,888,897,998]。

特别致谢

Elisabeth Sullivan 写了本书的第六部分。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。我要尤其感激她贡献出她在处理安全保障问题中的实际经验。通常，某些书籍只借助于安全保障的理论，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愿望，Peter 促进了我与 Addison-Wesley 出版社的接触。在写作的中途，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自于他的建议。Marvin Schaefer 以敏锐的眼光审阅了本书的若干部分，他的建议使得许多部分得到改进，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 Jim Alves-Foss，Bill Arbaugh，Andrew Arcilla，Rebecca Bace，Belinda Bashore，Logan Browne，Terry Brugger，Michael Clifford，Christopher Clifton，Crispin Cowan，Dimitri DeFigueiredo，Jeremy Frank，Robert Fourney，Ron Gove，Jesper Johansson，Mark Jones，Calvin Ko，Karl Levitt，Gary McGraw，Alexander Meau，Nasir Memon，Mark Morrissey，Ather Nawaz，Stephen Northcutt，Holly Pang，Sung Park，Ashwini Raina，Brennen Reynolds，Peter Rozental，Christoph Schuba，Jonathan Shapiro，Clay Shields，Tom Walcott，Dan Watson，Chris Wee，Paul Williams，Bonnie Xu，Xiaoduan Ye，Lara Whelan，John Zachary，Aleksandr Zingorenko，和在我计算机安全课上的所有人，他们（自觉不自觉地）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，特别是我的编辑 Peter Gordon 以不可置信的耐心给予我巨大的帮助，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。我还要感谢在 Argosy 的出版人员，特别是 Beatriz Valdés 和 Craig Kirkpatrick，感谢他们出色的工作。

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。

我还要感谢我的父母 Leonard Bishop 和 Linda Allen。我父亲是一位作家，他教给我许多写作的技巧，我一直在学习。我母亲是图书代理商，她帮助我了解图书出版的整个过程，并一直在支持我。

最后，我要感谢我的家庭，是他们支持我的整个写作过程。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 非常耐心而善解人意，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

第一部分　绪论

第二部分　基础知识

第三部分　策略

第四部分 实现 I:密码学

第五部分 实现 II: 系统

试读结束，需要全本PDF请购买 www.ertongbook.com