安全技术经典译丛

信息安全原理与实践（第2版）

Information Security: Principles and Practice, 2nd Edition

[美] Mark Stamp 著

张 戈 译

不可多得的信息安全技术专业级指南

既透彻讲解复杂的安全问题，又不陷于繁琐的细节

涵盖安全领域大多数主题，同时理论体系一脉相承

章末思考题发人深思，旨在引发讨论，动手实践

清华大学出版社

安全技术经典译丛

信息安全原理与实践

(第 2 版)

[美] Mark Stamp 著
张 戈 译

清华大学出版社
北 京

Mark Stamp
Information Security: Principles and Practice, 2nd Edition
EISBN：978-0-470-62639-9

北京市版权局著作权合同登记号 图字：01-2011-6159

图书在版编目(CIP)数据

信息安全原理与实践：第 2 版/(美)斯坦普(Stamp, M.) 著；张戈 译. —北京：清华大学出版社，2013.5
(安全技术经典译丛)
书名原文：Information Security: Principles and Practice, 2nd Edition
ISBN 978-7-302-31785-2

Ⅰ. ①信… Ⅱ. ①斯… ②张… Ⅲ. ①信息系统—安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2013)第 059893 号

责任编辑：王　军　李维杰
装帧设计：牛艳敏
责任校对：蔡　娟
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：31　　字　　数：754 千字
版　　次：2013 年 5 月第 1 版　　印　　次：2013 年 5 月第1 次印刷
印　　数：1～4700
定　　价：68.00 元

产品编号：042292-01

作 者 简 介

我在信息安全领域已有将近 20 年的经验了，其中包括在行业中和政府里从事的一些宽泛的工作内容。我的职业经历包括在美国国家安全局(National Security Agency，NSA)的 7 年多，以及随后在一家硅谷创业公司的两年时间。虽然关于我在 NSA 的工作，我不能说太多，但是我可以告诉你——我的职业头衔曾经是密码技术数学家。在这个行业当中，我参与设计并开发了一款数字版权管理安全产品。这段现实世界中的工作经历，就像三明治一样被夹在学术性的职业生涯之间。身处学术界时，我的研究兴趣则包含了各式各样广泛的安全主题。

当我于 2002 年重返学术界时，于我而言，似乎没有一本可用的安全教科书能够与现实世界紧密相连。我觉得我可以撰写一本信息安全方面的书籍，以填补这个空缺，同时还可以在书中包含一些对于处于职业生涯的 IT 专业人士有所裨益的信息。基于我已经接收到的反馈情况，第 1 版显然已经获得了成功。

我相信，从既是一本教科书，又可作为专业人员的工作参考这个双重角色来看，第 2 版将会被证明更具价值，但是因此我也会产生一些偏见。可以说，我以前的很多学生如今都从业于一些领先的硅谷科技公司。他们告诉我，在我的课程中学到的知识曾令他们受益匪浅。于是，我当然就会很希望，当我之前在业界工作时也能有一本类似这样的书籍作为参考，那样我的同事们和我就也能够受惠于此了。

除了信息安全之外，我当然还有自己的生活。我的家人包括我的妻子 Melody，两个很棒的儿子 Austin(他的名字首字母是 AES)和 Miles(感谢 Melody，他的名字首字母不至于成为 DES)。我们热爱户外运动，定期会在附近做一些短途的旅行，从事一些诸如骑自行车、登山远足、露营以及钓鱼之类的活动。此外，我还花了太多的时间，用在我位于 Santa Cruz 山间的一座待修缮的房子上。

致　谢

我在信息安全领域的工作始于我在读研究生的时候。我要感谢我的论文指导老师Clyde F. Martin，是他将我带领到这个引人入胜的主题当中。

在NSA的7年多时间，关于安全方面，我所学到的要比我在其他任何地方一辈子能够学到的都要多。从进入业界开始，我就要感谢Joe Pasqua和Paul Clarke，是他们给我机会能够参与到令人兴奋且富于挑战性的项目当中。

然后要感谢的是圣何塞州立大学(San Jose State University)的同学们，他们为本书的第1版做出了巨大的贡献。他们是Fiona Wong、Martina Simova、Deepali Holankar、Xufen Gao、Subha Rajagopalan、Neerja Bhatnager、Amit Mathur、Ali Hushyar、Smita Thaker、Puneet Mishra、Jianning Yang、Konstantin Skachkov、Jian Dai、Thomas Nikl、Ikai Lan、Thu Nguyen、Samuel Reed、Yue Wang、David Stillion、Edward Yin和Randy Fort。

还有Richard Low，我在SJSU的同事，他为本书较早期的版本提供了富有价值的反馈信息。David Blockus(上帝保佑他安息)是值得特别提到的一位，在本书第1版写作过程中特别关键的一段时期，他为每一章都提供了详尽的注释。

对于这本书的第2版，我在SJSU的许多硕士研究生都“毛遂自荐”要充当校对。在对本书手稿进行错误修正的过程中，以下这些同学付出了时间和精力：Naidele Manjunath、Mausami Mungale、Deepti Kundu、Jianrui (Louis) Zhang、Abhishek Shah、Sushant Priyadarshi、Mahim Patel、Lin Huang、Eilbroun Benjamin、Neha Samant、Rashmi Muralidhar、Kenny Zhang、Jyotsna Krishnaswamy、Ronak Shah、Gauri Gokhale、Arnold Suvatne、Ashish Sharma、Ankit Patel、Annie Hii、Namrata Buddhadev、Sujandharan Venkatachalam和Sathya Anandan。此外，Piyush Upadhyay还在本书第1版中发现了几处错误。

还有许多其他人都为本书提供了建设性的意见和建议。在此，我想对Bob Harris(宾夕法尼亚州立大学)表示特别感谢，他为本书提供了视觉加密的例子和练习。另外，John Trono(圣迈克尔学院)也针对本书提出了许多的评论和问题，也要深表谢意。

毫无疑问，错误仍然在所难免。当然，所有尚存的疏漏和瑕疵均是我个人的责任。

推荐序

十年前我在北京大学为计算机系研究生讲授“网络与信息安全”课程，那段时间正是信息安全快速发展时期，许多新兴的网络攻击方法正在实践中不断浮现(比如 Code Red 攻击)，一些安全协议也正在形成并被采纳到实际的系统中(比如 Windows 2000 使用了 Kerberos v5)。当时找不到合适的教材能够涵盖除了密码学以外更丰富的内容，所以我不得不花大量的精力将这些内容组织起来，推荐学生使用的教材是 William Stallings 的 *Cryptography and network security: principles and practice* 以及一本讲述网络攻防技术的 *Hacking Exposed*。我整理出来的讲义在北京大学计算机研究所的网站上全部开放，至今还可以从 Internet 上下载到(当年的官方下载站点已不再可用，但通过搜索引擎仍可以在其他的安全网站上找到)。

即使在离开北京大学以后，我仍然能看到和听到这些讲义被其他的老师采用。我曾经努力找个机会将这套讲义中的内容编写成教材，以便可以受益更多的人。在某家知名的出版社，我提交了这一选题，但最终没能通过，原因是密码学部分的内容不能超过两章篇幅，而我坚持要三章。或许他们的确不认可我的选题，因而拒绝了我的出版请求，这让我很沮丧，后来我忙别的事情去了，放下了这一选题。

虽然放下了安全的选题，但我在多年来的研究开发工作中一直没有离开过安全这一话题，只不过更加注重实用性，譬如怎么自动找到代码中的缺陷、移动操作系统中的多账户隔离以及移动支付安全等。这些安全议题来源于工程实践和移动互联网络环境中新的需求，有些可以利用传统的安全技术加以改进来实现，有些则需要全新的设计。此外，软件的代码安全和缺陷分析是个不断深入的话题，随着计算能力的提高以及编程技术的发展，软件趋向于越来越安全，挖掘软件漏洞的成本也越来越高。

上个月张戈说他翻译了 Mark Stamp 的 *Information Security: Principles and Practice* 一书，并大略地介绍了这本书的内容，特别是该书引入了最近几年来一些新的安全技术。张戈十年前参加过我的网络与信息安全课程，并且跟我的一位研究生学生合作从事过生物特征认证用于 DRM 的研究课题。我相信他的判断，也相信他有能力翻译好这本书。

我阅读了张戈的译稿，有些图表和形式化描述尚未插入，不过并不影响我的阅读和理解。全书读下来的深切感受是，这正是当年我所需要的一本教材。如果现在让我再讲授网络与信息安全课程，我会毫不犹豫选择这本书作为教材。具体而言，我认为本书具有以下一些特点：

- 本书的内容结构符合信息安全的全局观，从基础的密码学，到实用系统中涉及访问控制的两个重要方面——身份认证和授权过程，再到具体的安全协议，最后讨论软件实现的各种问题和操作系统安全。尽管内容广博，作者恰当地选取了最为核心和实用的部分来展开讲述，而并非面面俱到地罗列各种安全技术。因而本书在

广度和深度方面做了极好的平衡。学生在阅读本书时，不仅可以学到信息安全理论，还可以掌握一些实用技能。

- 本书的叙述风格不同于一般的教科书，即使是一些偏理论性的内容，作者也采用文字描述和生活例子来讲述。相对地，在理论解释和形式化描述方面比较轻笔墨。我不确定这种风格是否优于严谨的形式化描述，但我相信许多工科(或文科)的学生比较偏爱这种形式，而数学系的学生可能不会欣赏(以我之心度他人)。此外，基于作者自身丰富的安全背景和见识，他在内容讲解过程中也穿插了许多实际发生过的案例，从而使得本书的内容更有可读性，并且作者展露的观点更有说服力。
- 本书也提供了大量丰富的参考资料和文献。如果仅仅作为一本教材，这可能并不必要，但是对于想要深入某一章节或者进一步理解某些话题的读者而言，这无疑是知识宝库了。因此，对于安全领域有经验的工程师或研究者，本书也是不错的参考书。
- 对最新安全技术的跟进。正如张戈向我介绍的，这本书还收进了最近几年关注的一些安全热点，以及实际发生的有关网络协议、软件缺陷等方面的攻击、防护和改进。仅此一点，我阅读完本书后，颇有收获。

从内容本身来看，译稿的质量非常到位，看得出张戈花了不少功夫来处理译文，并且是在理解原文的基础上进行转译的。这基本上印证了我最初听到他翻译本书的消息时所做的判断。

最后，无论是在校学生、工程师还是研究人员，若要全面地学习或理解信息安全，本书是不错的选择。

潘爱民

2013 年 5 月于北京

译者序

Stamp 博士的这本书是不可多得的一部信息安全技术的专业级指南。从全书来看，既具有科班的正统性，又足够通俗易懂，而且读来生动有趣，对有志于迈入信息安全这个专业领域的人士而言，确实可以作为非常不错的起点和重要的技术参考。

在前言中，作者提及了本书写作的两个目标，译者认为本书达成了既定的两个目标并实现了很好的平衡。简单地说，就是这本书既透彻讲解了复杂的问题，又不至于陷入繁琐的细节。对于读者来说，可以较小成本掌握足够多的信息，颇具性价比。

这本书涉及的内容比较宽泛，但同时架构又相当紧致。广泛的选材有助于信息的实例化表述，毕竟信息安全领域涉及的知识博杂，且注重实践。另一方面，收敛的结构则非常便于把握脉络，建立体系化观点，这也是作为专业安全人士所必须具备的。全书从密码学技术、访问控制、协议以及软件安全这 4 个大的方面进行素材组织和深入讲解，一些跨界和边缘性议题也分别根据各自特点归纳到了相应的章节之中。对于信息安全技术而言，这 4 个方面基本可以涵盖绝大多数主题，此为完整性；而从对于安全技术的理解和运用来说，这 4 个方面也可以构成一脉相承的理论体系，层次清晰，提纲挈领，此为系统性。

除了兼顾信息量充足和结构的系统化之外，本书的另一个特色是繁简有度。譬如关于分组密码技术的实例解析，关于高级密码分析技术，关于口令问题，关于 IPSec 协议，关于软件逆向工程和数字版权管理等主题，都通过条分缕析给出了详尽透彻的讲解；而关于某些众所周知的加密算法和哈希函数，关于各色行业标准，关于多级安全模型，关于入侵检测系统，关于软件开发安全和可信操作系统等主题，则采用了简单明快一语中的的叙述风格。诸如此类的例子还有很多，这样的安排容易让人既对重点内容印象深刻，又能于作者的快人快语之间把握相关的结论。

信息安全是一个在实践中不断发展的领域，而作者对这个领域知识的讲授方式也确实体现出了作为教师的职业经验和专长。对于许多主题的阐述，诸如经典加密技术和恶意软件等内容，读来均有娓娓道来水到渠成之感。不仅如此，又由于作者在安全行业的公司生涯以及在政府部门的研究经历，本书许多内容的组织都不乏案例性和实践感。比如，在第 5 章中介绍哈希函数及各色加密应用时，渗透着实战性，令人有“学以致用”的体悟；又比如第 9 章中对于安全协议设计的讲解，其步步为营的展开方式，颇有“授人以渔”之感。

思考题部分也是本书的一大亮点。这些题目不单单是对每章主要内容的回顾，其中有相当数量的题目都启人深思，甚至目的就是为了引发讨论，便于读者自发地学习和掌握相关知识。除此之外，还有不少题目都衍生出了新的概念和内容，成为扩展学习的最佳切入点。当然，从实践的角度看，很多习题也都提供了动手练习的机会，并准备了素材，甚至其中一些任务的完成，还需要读者展开一番较为深入的自学和研究。这也正体现了西方理工学科教育的优势和精髓，值得大家参考和借鉴。

值得一提的是，作为一部工程技术类专著，作者在行文中始终保持着风趣幽默的风格，这一方面令知识和技术生动起来，另一方面也令远隔千山万水的作者倍感亲切。

最后说说翻译。

通常来说，翻译工作追求的是“信、达、雅”三个目标。对于技术性读物的译作来说，大部分情况下都应确保前两个目标，而这两个目标，恰是对译者两个方面能力的要求：一是要充分了解该技术领域，要有专业性，如此方能“信”；二是对源和目标两种语言的完全掌握和熟练应用，这涉及思维水平和语言表达能力，是“达”的保证。于译者本人而言，在本书的翻译过程中，亦未敢怠慢，始终心存此念，力求不负所托。

实践中，在“信”和“达”之间的平衡，相信对于大多数译者来说都是一种挑战，这源自英语和汉语之间结构的巨大差异，本质上也是思维方式的不相适应。在实现这种语言映射的过程中，译者们既要恪守专业精神，又要发挥“人工智能”，在踌躇和思量之间进行着二次创作，其中有推敲琢磨殚精竭虑之苦，亦有水到渠成意境全生之快。译者本人虽不乏信心和勇气，但鉴于能力和时间有限，相信不当和疏漏之处仍不在少数，恳请读者谅解并批评指正，不胜感激。

另外，对于原文中存在的个别错误和疏忽，在译文中也已做了尽力修改。翻译方面的不足，译者自当一力承担。

感谢在本书翻译过程中给予我大力支持的家人和朋友。

希望您阅读愉快并有所收获。

张　戈

2012 年冬于北京

前　言

我讨厌黑盒子。我写作本书的目的之一就是要将某些惯用的黑盒子拆解开来，公之于众，这些黑盒子在当今的信息安全类书籍中比比皆是。另一方面，我也不希望你劳神费力地钻入牛角尖去对付那些琐碎的细枝末节(若你果真有此爱好的话，还可以移步去看相关的 RFC 文档)。所以，我通常会一笔带过那些我确信与当前所讨论主题并不相干的局部和详情。至于在上述两个貌似互斥的目标之间，我是否已实现了合理的平衡，还有赖于读者您的判定。

我已努力追求所提供的内容能够保持与时俱进，以便可以涵盖更加宽泛的诸多议题。我的目标是要对每一个议题覆盖得恰到好处，使得所提供的具体内容刚好足够你去领会相关的基本安全问题，同时又不至于陷入到无谓的细节当中不能自拔。我也会尝试对一些要点进行不断地强调和反复重申，以便那些关键性的信息不至于滑出你的视野。

我的另一个目标是要把这些主题以一种生动鲜活并且充满趣味的形式呈现出来。如果任何计算机科学的主题都能够做到富有乐趣并令人兴奋，那么信息安全也理应如此。安全是正在进行时，安全还处于新闻热议中——这个话题显然足够新鲜活泼，也足以激动人心。

我也尝试在这些素材当中注入一点点的幽默感。人们说，幽默源自伤痛。所以，其中的冷暖，请根据我开玩笑的水平细细品味，我只能说我所引领的是一种令人向往的梦幻生活。不管怎样，大部分真正不良的俏皮话都挤在狭小的脚注里，所以倒不至于太跑题。

有些信息安全的教科书会堆砌大块干燥乏味且一无是处的理论说辞。任何一本这样的著作，读来都会像研读一本微积分教材那般充满刺激和挑战。另外的一些读本所提供的内容，则看起来就像是一种对于信息的随机性收集，而其中的信息却是显然毫不相干的事实罗列。这就会给人们留下一种印象，安全实际上根本不是一个有机结合的主题。此外，还有一些书籍，会将一些高级的管理学上的老生常谈汇集到一起作为主题来介绍。最后，另有一些文本和教义选择聚焦在信息安全领域中与人相关的因素上面。虽然所有的这些教授方法都有其自身的定位，但我还是认为，首先并且也最为重要的是：对于处在基础层面的技术的固有优势和不足，安全工程师必须要有扎扎实实的理解。

信息安全是一个庞大的主题，而且又不像其他更为成熟的一些学科领域，所以对于像这样的一本书究竟应该包含哪些素材，或者到底如何组织才最佳，也都无法给出清晰明确的回答。我选择围绕以下 4 个主要议题来组织本书：

- 密码学技术
- 访问控制
- 协议
- 软件安全

根据我的习惯，这些议题都是相当有弹性的。举个例子，在访问控制这一议题之下，我包含了有关身份认证和授权相关的传统主题，同时也包含了诸如防火墙和 CAPTCHA 验证码之类的非传统主题。关于软件的议题尤其灵活，其中包含了形形色色的多个主题，就像安全软件开发、恶意软件、软件逆向工程以及操作系统之类的内容。

虽然这本书是着眼于对实践问题的研究，但我还是尽量覆盖了足够多的基本原理，以备你可以在这个领域中展开更深入的研究。而且，我也力争尽可能地最小化所需要的背景

知识。特别是，对于数学形式的表达，已经控制到了最低限度(在附录中有简要的回顾，其中包含了本书中涉及的所有数学主题)。尽管存在这些自我强加的限制因素，但我仍然相信，相比除此之外的大部分安全类书籍，这本书容纳了更具实质性的密码学技术相关内容。此外，所需要的计算机科学知识背景也被降到了最低——入门级的计算机组成原理课程(或是与此相当的经验)已经是绰绰有余了。如果有一些编程经验，再加上一点儿汇编语言的基本知识，将会有助于更好地理解某几个小节的内容，不过这都不是必需的。还有几个小节会涉及一些网络技术基础知识，所以在附录中也包含简短的关于网络技术的回顾，提供了足够多的背景材料。

如果你是一名信息技术方面的专业人士，正在尝试学习更多有关安全的内容，那么我建议你完整地阅读本书。不过，如果你想躲过那些最有可能带来羁绊，同时又对全书的整体性阅读不会产生重要影响的素材，那么你大可以放心地跳过4.5节、整个的第6章(虽然6.6节值得强力推荐)以及8.4节。

如果你正在讲授一门安全课程，那么你需要认识到，这本书所包含的素材已经超过了一个学期的课程所能涵盖的内容。通常情况下，在我的本科生安全课程中，我所遵循的课程计划就如表Q-1中给出的课程表。这个课程安排允许有充足的时间去覆盖一些可选的主题。

如果认为表Q-1中所示的课程表过于繁忙(共需40个课时)，你可以砍掉第8章的8.9节，以及第12章和第13章中的某些主题。当然，关于这个课程表，还有许多其他的调整也都是可行的。

表Q-1　推荐的课程安排

章　名	学　时	说　明
第1章 引言	1	讲解全部
第2章 加密基础	3	讲解全部
第3章 对称密钥加密	4	跳过3.3.5节
第4章 公开密钥加密	4	跳过4.5节
第5章 哈希函数及其他	3	跳过5.6节、5.7节中攻击细节部分以及5.9.1节
第6章 高级密码分析	0	跳过整章
第7章 认证	4	讲解全部
第8章 授权	2	跳过8.4.1、8.4.2和8.10节
第9章 简单认证协议	4	跳过9.4节
第10章 真实世界中的安全协议	4	跳过WEP或GSM部分
第11章 软件缺陷和恶意软件	4	讲解全部
第12章 软件中的安全	4	跳过12.3节
第13章 操作系统和安全	3	讲解全部，如果时间允许的话

安全不是旁观者的运动——进行大量的课后问题练习，对于学习本书中提供的素材是非常有必要的。有许多主题，在课后的思考题中会展现得更加淋漓尽致，并且常常还会引入一些附加主题。归结到一点，就是你解决的问题越多，你就能够学到越多。

基于这本书的一门安全课程，对于个人和团体项目而言，都会是理想的选择。第6章

的内容对于加密类的项目来说就是非常好的资源，而附注的参考书目则提供了一个查找更多其他项目主题的出发点。此外，许多课后思考题本身就能很好地融入课堂讨论当中，或是非常适合作为课内的作业安排(例如，可以参见第 10 章中的思考题 19，或者第 11 章中的思考题 33)。

这本教科书的网站地址是：http://WWW.cs.sjsu.edu/-stamp/infosec/。在这里，你可以找到 PowerPoint 幻灯片文件，在课后思考题中提到的所有文件、勘误表等等。如果我是第一次讲授这门课程，我会特别愿意使用这些 PowerPoint 幻灯片文件，毕竟它们已经历了“实战”的千锤百炼，并且经过了若干轮的反复改进。此外，出版方还可以为教师提供一本问题解答手册。

关于如何使用附录也值得在此做些说明。附录 F.1 与第 8 章 8.9 节和 8.10 节的内容相关，也与整个第 III 部分内容有关。即便在网络技术方面有扎实的基础，这部分素材也很可能仍然是值得去回顾的，因为网络术语并不总是能够保持一致，并且这里的内容聚焦于安全方面。

附录 F.2 的数学基础则要负责对贯穿全书的多个不同地方提供解释和支持。基本的模运算(附录 F.2.2)分别出现在第 3 章和第 5 章的几个小节当中，而相对比较高级的一些概念则是第 4 章和第 9 章的 9.5 节中所必需的。我已经发现，我的绝大多数学生都需要重新温习有关模运算的基础知识。其实，只需要花上大约 20 到 30 分钟的课堂时间，就可以遍历有关模运算的这些素材。相比不管不顾一头扎到公开密钥加密技术当中，花这点儿时间还是很值得的。请相信我。

在附录 F.2.3 中，我们就排列置换进行了简要的讨论，这是第 3 章中最为凸显的一个概念。而基本的离散概率知识(附录 F.2.4)则在本书中多处都会遇到。最后，附录 F.2.5 中提供的基础线性代数理论只有在 6.5 节才需要用到。

就像任何庞大而且复杂的软件组件必然会包含有 bug 一样，这本书也不可避免地会有错误。我真心地希望听到你找出了任何的错误——无论大或小。我将会在本教材的网站上维护一个持续更新的勘误表。另外，如果你对这本书未来的版本有任何意见或建议，请不要犹豫，立刻告诉我。

第 2 版有什么新的内容呢？

对于第 2 版来说，一个主要的变化就是，课后思考题的数量和分类都有大幅增加。除了新增的和改进的课后思考题之外，也增加了一些新的主题，还有一些新的背景知识和素材也被包含了进来。实际上，所有现存的内容都经过了更新和澄清，并且所有已知的错误均已获得了修正。新加入的主题的例子包括实际的 RSA 计时攻击、关于僵尸网络的讨论以及安全证书涉及的范围等。新增加的背景素材包括关于 Enigma 密码机的一小节内容，另外还有一部分内容谈到了经典的“橘皮书”之安全观。

信息安全是一个快速发展的领域，自本书第 1 版于 2005 年出版以来，业界已经发生了不少重大的变化。但是不管怎样，本书的基本结构仍然保持不变。我相信本书的组织和议题的列举在过去这 5 年当中已经受住了考验。正因为如此，第 2 版在内容上的改变更多是一种进化，而并非革命。

目　录

第Ⅳ部分 软件