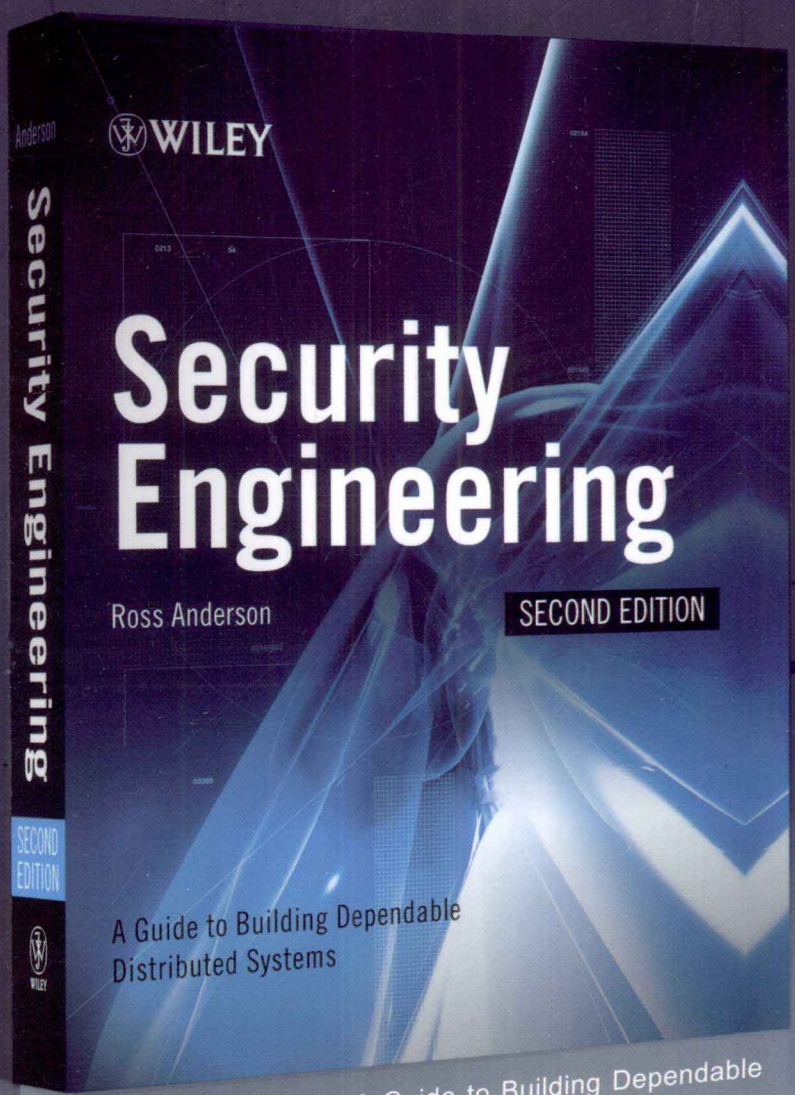
国外计算机科学经典教材

信息安全工程

(第2版)

(英) Ross Anderson 著　　齐宁 韩智文 刘国萍 译

UNIVERSITY OF CAMBRIDGE
Computer Laboratory



Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition

WILEY

清华大学出版社

国外计算机科学经典教材

信息安全工程

(第2版)

(英) Ross Anderson 著
齐宁 韩智文 译
刘国萍

清华大学出版社
北京

Ross Anderson
Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition
EISBN：978-0-470-06852-6

图书在版编目(CIP)数据

信息安全工程(第 2 版)/(英)安德森(Anderson, R.) 著；齐宁，韩智文，刘国萍 译.
—北京：清华大学出版社，2012.1
(国外计算机科学经典教材)
书名原文：Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition
ISBN 978-7-302-27115-4
Ⅰ. 信… Ⅱ. ①安… ②齐… ③韩… ④刘… Ⅲ. 信息安全 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2011)第 211673 号

责任编辑：王 军 韩宏志
装帧设计：孔祥丰
责任校对：成凤进
责任印制：李红英

出版发行：清华大学出版社 **地 址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn **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 装 者：清华大学印刷厂
经 销：全国新华书店
开 本：185×260 **印 张**：44.75 **字 数**：1117 千字
版 次：2012 年 1 月第 1 版 **印 次**：2012 年 1 月第1 次印刷
印 数：1～5000
定 价：80.00 元

产品编号：030082-01

出版说明

近年来，我国的高等教育特别是计算机学科教育，进行了一系列大的调整和改革，亟需一批门类齐全、具有国际先进水平的计算机经典教材，以适应我国当前计算机科学的教学需要。通过使用国外优秀的计算机科学经典教材，可以了解并吸收国际先进的教学思想和教学方法，使我国的计算机科学教育能够跟上国际计算机教育发展的步伐，从而培养出更多具有国际水准的计算机专业人才，增强我国计算机产业的核心竞争力。为此，我们从国外多家知名的出版机构 Pearson、McGraw-Hill、John Wiley & Sons、Springer、Cengage Learning 等精选、引进了这套“国外计算机科学经典教材”。

作为世界级的图书出版机构，Pearson、McGraw-Hill、John Wiley & Sons、Springer、Cengage Learning 通过与世界级的计算机教育大师携手，每年都为全球的计算机高等教育奉献大量的优秀教材。清华大学出版社和这些世界知名的出版机构长期保持着紧密友好的合作关系，这次引进的“国外计算机科学经典教材”便全是出自上述这些出版机构。同时，为了组织该套教材的出版，我们在国内聘请了一批知名的专家和教授，成立了专门的教材编审委员会。

教材编审委员会的运作从教材的选题阶段即开始启动，各位委员根据国内外高等院校计算机科学及相关专业的现有课程体系，并结合各个专业的培养方向，从上述这些出版机构出版的计算机系列教材中精心挑选针对性强的题材，以保证该套教材的优秀性和领先性，避免出现“低质重复引进”或“高质消化不良”的现象。

为了保证出版质量，我们为该套教材配备了一批经验丰富的编辑、排版、校对人员，制定了更加严格的出版流程。本套教材的译者，全部由对应专业的高校教师或拥有相关经验的 IT 专家担任。每本教材的责编在翻译伊始，就定期不间断地与该书的译者进行交流与反馈。为了尽可能地保留与发扬教材原著的精华，在经过翻译、排版和传统的三审三校之后，我们还请编审委员或相关的专家教授对文稿进行审读，以最大程度地弥补和修正在前面一系列加工过程中对教材造成的误差和瑕疵。

由于时间紧迫和受全体制作人员自身能力所限，该套教材在出版过程中很可能还存在一些遗憾，欢迎广大师生来电来信批评指正。同时，也欢迎读者朋友积极向我们推荐各类优秀的国外计算机教材，共同为我国高等院校计算机教育事业贡献力量。

清华大学出版社

国外计算机科学经典教材

编审委员会

作者简介

为什么我应该是本书的撰写者？因为我在过去25年间积累的丰富经验和获得的认证资格满足了这种要求。20世纪70年代，我毕业于英国剑桥大学数学与自然科学专业，并获得了计算机工程领域的资格证书，我的第一份正式工作是有关航空电子系统方面的，从20世纪80年代中期我萌生了对密码学与计算机安全领域的兴趣。在银行业工作几年之后，我开始为那些银行装备设计公司担当顾问，之后在这一技术领域的其他应用领域(比如预付费电子仪表)工作。

1992年，我转向学术领域，但仍为安全技术行业做一些咨询工作。20世纪90年代，采用密码机制的应用领域快速增加，在防盗自动警铃、汽车门锁、公路收费标签以及卫星电视加密系统中，都可以看到密码学的应用。在伴随这些系统而来的首次合法性争论中，我很幸运地成为一些重要案例中的鉴定人。我领导的研究团队是幸运的，在恰当的时间和场合做了一些工作——当时正好是防篡改、数字水印等关键性技术成为热点的时候。

大概到1996年，我开始感觉到当时的教科书过于专业化。安全教科书重点介绍操作系统中的访问控制机制，而密码学书籍则十分详细地描述密码算法与协议的设计。这些主题是有趣的，也是重要的，但只是信息安全工程的一个组成部分。大多数系统设计者并不过分关注密码学或操作系统内部机制细节，而是关心如何有效地使用这些工具。他们这样做是有道理的，因为安全机制的不当使用是导致安全失败的主要诱因之一。在我当时撰写的大量关于安全工程方面的文章(从1993年的“为什么密码系统出现了故障”开始)取得成功的激励下，以及出于当时教授一个本科班安全课程的实际需要，我撰写了一些讲稿，这些讲稿构成了本书的一半内容。最后，在1999年，我开始为一些普通技术读者重写这些内容。

在撰写过程中，我自己也学到了很多——将自己思考的内容写出来是发现自己欠缺哪些知识的绝佳途径。从中我也享受到了很多乐趣，期待读者在阅读本书时也能尽情体验愉悦和快乐。

译者简介

齐宁，1978 年 5 月生，河北保定人。2006 年获得解放军信息工程大学计算机软件与理论博士学位。求学及工作期间的主要研究方向包括计算机安全、可信计算、二进制翻译、高性能计算等。主要译著有《SQL Server 2005 性能调优》和《C++多核高级编程》等。

韩智文，计算机科学与技术专业博士，网络系统分析师，长期从事网络通信和信息安全领域工作，参加了多项国家“863”和国防研究项目，为政府信息化建设提供咨询服务。主要研究领域包括网络安全、策略管理和下一代互联网技术等，已在国家核心期刊上发表研究论文十余篇，出版译著两部。

中国电信北京研究院商业客户部技术与产品研发部高级工程师。本硕毕业于中国人民解放军信息工程大学，获得中科院研究生院空间技术与方法专业博士学位。博士研究期间，曾参与国家大型项目“中国探月工程” 一期工程的地面通信网络部分的设计工作。2004 年进入中国电信北京研究院工作，从事互联网业务和网络安全技术研究及相关产品的研发工作。

他序

在与Roger Needham合著的一篇论文中，Ross Anderson创造了短语“给撒旦的计算机编程”，用于描述计算机安全工程师面临的问题。想到Ross，我的脑海里就浮现出这幅图景，自那时起我也开始使用这个短语。

给计算机编程是直接的：不断地排除问题，直至计算机完成了需要完成的任务。大型应用程序与操作系统更复杂一些，但方法基本相同。编写可靠的计算机程序更难，因为程序需要在面对随机错误和失误时仍能有效工作：墨菲的计算机。关于可靠的软件设计，已经有大量的研究，也有很多关键业务软件应用程序在设计上可以抵抗墨菲定律。

编写安全(secure)的计算机程序完全是另一码事。安全不仅涉及让确定的事情有效进行，也不仅是处理随机错误，更要面对的情况是，智能的恶意对手总是一再试图在最糟糕的时间以最糟糕的方式让事情无法进行。这确实是在为撒旦的计算机编程。

安全工程不同于任何其他类型的编程。这是我在专著 *Secrets and Lies*、月刊 *Crypto-Gram* 和我撰写的其他作品中一再强调的观点。这也是Ross在本书每一章中强调的一点。这也是为什么在你完成安全工程方面的工作，或在思考做安全工程方面的工作时需要阅读本书的原因。这是第一本，也是唯一一本关于端对端现代安全设计与工程的书籍。

本书的撰写可谓恰逢其时。可将Internet的历史划分为三个阶段。第一阶段集中于大型机和终端，那时计算机昂贵稀缺；第二阶段大概从1992年到现在，集中于个人计算机、浏览器以及大型应用程序；第三阶段从现在开始，我们将看到目前在专用网络、独立的、非计算化环境中的所有类型设备连接在一起。到2003年，连接到Internet中的移动电话要多于计算机。我们将在几年内看到，世界上很多电冰箱、心脏监控器、公交车票与火车票配售机、防盗警铃和电子仪表都将使用IP进行通信。个人计算机在Internet中的地位将逐渐弱化。

安全工程，特别是在Internet历史的第三阶段的大环境下，需要采用不同的思考方式。你不仅需要设计事物的正常运作流程，还要考虑哪些因素会导致异常。必须假设系统内部存在智能的、恶意的对手(回想一下撒旦的计算机)，对手在不断寻找迂回绕行的新途径。你必须考虑可能导致系统失败的各种因素，其中大部分都与设计本身无关。你必须对每件事情都由表及里、自上而下、从左到右地进行全方位衡量，你必须像外星人一样进行思考。

就像最近科幻小说编辑John W. Campbell所说的：“外星人和人类一样也会思考，但与人类的思考方式不同”，计算机安全与此很类似。Ross是少数可像外星人一样思考问题的人之一，并可将这种思考方式向普通人解释清楚。请享受学习的乐趣吧。

Bruce Schneier

自序

《信息安全工程》第一版于2001年5月出版，从那时至今，世界已经发生了巨大变化。

那时，系统安全在微软是最后考虑的事项，而现在则是最优先考虑的要素之一。恶意软件的数量不断增长，带来的麻烦不断增多。尽管已做了大量的防御工作——我们已经看到，Windows NT被XP取代，之后是Vista，并且偶尔发布的服务补丁也被每月发布的安全补丁所替代——但攻击者在攻击方面付出的努力要更大。那些编写病毒的人不再是为了乐趣，而是为了追逐利益，最近几年中，已经可以看到各领域专业人士共同完成攻击行为的犯罪经济学的影子。垃圾邮件制造者、病毒编写者、钓鱼者、经济诈骗犯以及间谍彼此之间频繁地进行交易。

密码学也在不断向前发展。高级加密标准已嵌入到越来越多的产品中，公钥领域也取得了很多有趣的进展。但在算法问题得到解决后，我们又面临着大量的实现问题，隐通道、设计存在漏洞的API以及协议失败等都不断地对系统造成破坏。与以前相比，应用密码学更难以实现安全目标。

普适计算也带来了新挑战。随着计算机与通信设备越来越多地以不可见的方式嵌入到大量领域，过去只是影响“相应计算机”的问题开始影响所有类型的设备。对热敏电阻温度计或空调机而言，安全又有怎样的内涵？

智能设备的多样性带来了不同的兴趣和参与者。安全不仅是关于怎样将破坏分子拒于门外，而且日益与权力和控制的争夺关联在一起。DRM导致内容与平台产业相互之间以及与消费者之间的明争暗斗；附件控制用于将打印机与其销售商提供的耗材绑定，但导致了反垄断诉讼。安全还与汽车乃至电子医疗保健设备的安危相关。安全工程需要理解的不仅是密码学和操作系统，还要理解经济学和人为因素。

数字设备的无处不在意味着，“计算机安全”不再仅仅是少数系统专家研究的问题。几乎所有的白领犯罪(以及大部分严重暴力类型的犯罪行为)都涉及计算机或移动电话，因此，就像需要知道如何驾车一样，侦探也需要理解计算机取证方式。越来越多的律师、会计师、管理人员和其他没有经过正规工程训练的人都将不得不理解系统安全问题，以便完成自己的工作。

在线服务的快速增长——从Google、Facebook到大规模的多方游戏，也在改变着世界。在线应用程序中的错误在被发现后可以快速地进行修复，但随着应用程序日趋复杂，其负面效应难于预测。对操作系统或银行服务而言，我们对其安全的内涵可能有合理的理解，但对在线服务而言则不敢下此断言，因为在其生命周期内都是不断演化的。我们正在进入一个社会-技术系统不断演化的新世界，并且需要理解这种演化如何推动以及由谁控制的深奥问题。

然而，最大的变化是由 2001 年 9 月 11 日的恐怖袭击事件以及我们对该事件的反应驱动的。这已经以多种方式改变了感觉和优先级，并改变了安全产业的形态。恐怖主义不仅是关于风险的，还涉及对于风险的感知、对感知的操纵等，从而向安全内涵中添加了心理学与政治等因素。对政治争论，安全工程师也有责任。在对恐怖主义犯罪不当反应导致巨大资源浪费与非受迫性策略错误的地方，我们不得不向人们问一些简单的问题：我们要防止的是什么？已提出的机制能否真正奏效？

Ross Anderson

法律声明

有一点怎么强调都不过分：本书介绍的技术完全是为了帮助构建更出色的系统，绝非是为了帮助突破系统、绕过版权保护机制或从事任何不符合伦理的、非法的行为。

在可能的地方，我尝试在一定细节程度上给出的案例记录都是描述底层的原理，而非“黑客食谱”。

出版本书的原因

有人认为本书包含的知识不应公开出版。这是一个自古就有的争论点，在前几个世纪中，人们就反对过出版关于锁匠的书籍，他们认为这对坏人的帮助要多于对好人的帮助。

我认为，第一部讨论密码学的英文著作已经对这些恐惧做了回答，这是 Bishop John Wilkins 在 1641 年撰写的一部关于光学与声频电报的专著[805]。其中回顾了埃及牧师反对按字母顺序撰写的历史，因为牧师认为这会在普通人群中传播读写能力，从而滋生异议。他这样说：

并非所有可能会被滥用的事物都必须压制……如果可能被滥用的所有有用的发明都被压制，就不会存在任何合法的科学或艺术了。

到 19 世纪，这一问题再次被提及，一些好心人试图阻止出版有关锁匠方面的书籍。对于这一问题，当时的一位作者是这样回应的[750]：

很多好心人都怀疑关于破坏锁的安全性的讨论会为恶意行为提供机会，因为这种讨论会向人们展示怎么进行恶意破坏。这是一个误解。坏人对专业技能的理解是非常敏锐的，并且实际上知道的要比我们讨论中所透露的几种技能要多。在锁匠们对锁的破坏进行讨论之前，坏分子们已经掌握了很多……如果说这种讨论存在危害，也不如人们从中掌握的防范知识多。

这些观点都是伴随长期的经验而产生的。从我个人经历而言，我曾有三年半的时间为两家银行做取款机安全方面的工作，但我从一个在美国监狱系统服刑的银行卡诈骗分子撰写的一篇文档中学到了很多重要的新技巧。很多机构现在开始认同这一观点。

总之，尽管一些恶意分子会从这样的书中获益，但他们大都已经知道了这些技巧，而好人们获得的收益会多得多。

前言

近几个世纪以来人们使用锁、栅栏、签名、封印、账册和仪表等来保护自己的财产和隐私，并得到从国际条约到国际法到礼节和风俗等的大量社会结构的支持。

这一切处于快速的变革中。大多数记录现在都实现了电子化，从银行账号到土地财产登记册都如此；随着 Internet 购物的流行，交易也日趋电子化。还有很多也很重要但不那么明显的是，很多日常系统也已经悄悄地实现了自动化处理。防盗自动警铃不再会惊醒邻居的美梦，而是悄悄地向警察发送消息；学生们不再需要使用硬币来为其宿舍内的洗衣机和干衣机付费，而是用可在大学书店充值的智能卡进行记账；锁不再是简单的机械设施，而是可以通过远程电子控制或刷卡进行操纵；数百万的人们不再需要租赁录像带，而是通过卫星或电缆来观看电影。甚至普通钞票也不再只是纸上印着墨汁，而是包含了数字水印信息，以便机器检测很多伪造行为。

那么，这些新的安全技术效果如何？遗憾的是，真实的答案是“与预期的良好作用相距甚远”。新系统通常很快就被攻破，同样的基础性错误在不同的应用程序中不断重复出现。通常需要经过四五次尝试才能实现安全的设计，而这实在太多了。

媒体经常报告 Internet 上的安全漏洞，银行为取款机上的“错误提款”与客户争论不休，VISA 报告了 Internet 上有争议的信用卡交易数量的显著增长，卫星电视公司追索复制其智能卡的盗版者，执法机构试图通过控制加密机制使用的法律来监视计算机领域的恐怖主义行为。更糟糕的是，各种功能之间存在很多交互——偶然按到了移动电话的重拨键只是一个小小的麻烦，而在发明了一种机器且该机器在每次电话号码被呼叫时就提供一罐软饮料时，情况就不那么简单了，当你突然发现你的电话账单上有 50 罐可乐时，谁应该对此负责？电话公司？手持设备制造商？还是销售机操作员？一旦几乎所有影响生活的电子设备都连接到 Internet 上(Microsoft 预计这将在 2010 年出现)，“Internet 安全”对个人意味着什么，怎样应付这个问题？

除系统故障外，还有很多系统不能有效工作。医疗记录系统不允许医生按需共享个人健康信息，但仍不能防止这些信息被不择手段的私家侦探获取。Zillion-dollar 军事系统阻止不具备绝密级许可权限的任何人获取情报数据，但通常在设计上几乎要求所有人都具备绝密级许可权限才能完成任何工作。乘客售票系统在设计上试图防止客户欺骗，但当反垄断官员打破了铁路的统一后，无法阻止新的铁路公司彼此之间的欺骗。如果设计者知道其他地方有哪些做法已经被尝试过并失败过，就可以预见其中很多失败。

安全工程是从这些混乱中涌现出的一门新学科。

尽管大多数底层技术(如加密学、软件可靠性、防篡改、安全打印和审计等)较容易理解，但如何有效应用这些技术则更难。由于从机械机制向数字机制的转变几乎无处不在，使得很多经验教训没有足够的时间在工程团体内被学习和接受。我们一次又一次地看到很多做法在不同场合重复。

最有能力应对变迁的行业通常是那些从其他领域学习了适当技术的行业，比如，银行取款机(甚至预付费煤气表)就重用了军事领域敌我识别装备中的技术。因此，即便某位安全设计人员在某个特定领域拥有出色的技能——不管是操纵密码的数学家还是开发钞票墨水的化学家——对整个主题有全局的理解还是有意义的。良好的安全工程的实质是理解系统面临的潜在威胁，之后运用技术上和组织上合适的混合防护措施，来对这些威胁进行控制。了解在其他应用中哪些措施是有效的，更重要的是了解哪些措施是无效的，这对开发会很有帮助，并且可以省下一大笔钱。

本书旨在为安全工程奠定坚实的基础，这也是我们在 21 世纪初对安全工程的理解。希望本书可以起到以下四个层面的作用：

(1) **作为一本教科书，可作为本主题的入门读物，可在数天内全部读完。**本书主要面向需要了解这一主题的 IT 专业人士，也可作为大学教材(一学期课程)。

(2) **作为一本参考书，用于大致了解某特定类型系统的工作原理和过程。**这些系统包括取款机、出租车计价表、雷达干扰器和匿名医疗记录数据库等。

(3) **作为介绍底层技术的入门书籍，如加密、访问控制、推理控制、防篡改和封印等技术。**由于篇幅所限，无法进行特别深入的探讨，但对于每个主题都给出了基本的路线图，并为感兴趣的读者给出了参考读物列表(对未来的毕业生，还给出了开放研究问题列表)。

(4) **作为一本原创的科学文献，在其中，我试图勾勒出作为安全工程基础的通用原理，以及人们在构建某种类型系统时应该从其他系统中吸取的教训。**在我从事安全工作的多年经历中，我一直试图说出这些。比如，设计通用防空火力控制雷达的人不知道对流密码的简单攻击方法，使得雷达很容易受到干扰；而雷达社区中人们熟悉的技巧也没有被印钞机和设计版权标记框架的人所理解，从而导致对大多数数字水印的非常常见的攻击。

本书源于我在剑桥所教授的安全工程课程，但我重新撰写了教案，使其更容易理解，并添加了一些必要的素材。对专业安全管理人员或顾问来讲，本书是一本极富价值的最前沿的参考书；对从事密码学研究的计算机科学教授、试图了解最新计算机骗术的警察侦探、想要清除密码学与匿名性立法方面冲突的政策人员来讲，本书应该都是有用的。最重要的是，本书的主要读者群是在职的程序员或工程师，他们正在试图设计实际系统，并努力保证系统在客户、管理人员和任何其他人的操作下都能正常运行。

本书分为三个部分：

- 第 I 部分介绍一些基本概念，从安全协议的一些中心概念开始，到人机界面问题、访问控制、密码学与分布式系统问题。该部分不要求读者具备特定的技术背景，只要求掌握计算机基础知识。本部分是以我给二年级学生所教授的安全课程为基础的。
- 第 II 部分较详细地讲述了大量重要的应用，比如军事通信、医疗记录系统、取款机、移动电话以及付费电视等，这些系统用于引入更多高级技术和概念。本部分还从公司、消费者、犯罪分子、警察、间谍等大量不同团体的视点分析了信息安全问题。这些素材源于我在安全方面的高级课程讲义、研究工作和咨询工作等。
- 第 III 部分讲述了组织与策略问题：计算机安全怎样与法律、证据和公司政治生态交互作用；怎样确保系统可以按照设计的目标工作；怎样对安全工程的整个过程进行最有效的管理。

我相信，构建在面对恶意行为时仍能可靠运行的系统是工程师们在 21 世纪面临的最重要、最有趣、最困难的任务之一。

参考文献

在阅读过程中，你会发现正文中的一些地方出现了用方括号括住的编号，即[*]，这些代表参考文献号，你可以在书末的“参考文献”查阅书名。

目录

第Ⅰ部分