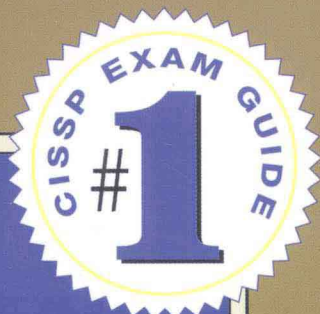


CISSP All-in-One Exam Guide, Sixth Edition

All in One

CISSP

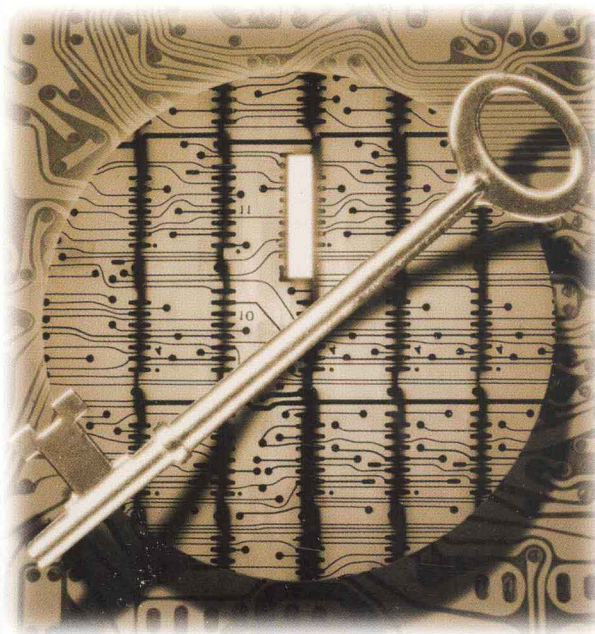
认证考试指南(第6版)



最新覆盖信息系统
安全认证的所有10
个专业领域

■
最理想的学习工具
和工作参考书

■
丰富的练习试题和
深入的解答



电子资料包含了:

- 1400多道练习试题
- Shon Harris的视频培训
- Adobe数字版格式的电子书-免费下载

[美] Shon Harris 著 张胜生 张博 付业辉 译

CISSP 认证考试指南 (第 6 版)

[美] Shon Harris 著

张胜生 张博 付业辉 译

清华大学出版社

北 京

Shon Harris

CISSP All-in-One Exam Guide, Sixth Edition

EISBN: 978-0-07-178174-9

Copyright © 2013 by McGraw-Hill Education..

All Rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation edition is jointly published by McGraw-Hill Education (Asia) and Tsinghua University Press Limited. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Copyright © 2013 by McGraw-Hill Education (Asia) and Tsinghua University Press Limited..

版权所有。未经出版人事先书面许可, 对本出版物的任何部分不得以任何方式或途径复制或传播, 包括但不限于复印、录制、录音, 或通过任何数据库、信息或可检索的系统。

本授权中文简体字翻译版由麦格劳-希尔(亚洲)教育出版公司和清华大学出版社有限公司合作出版。此版本经授权仅限在中华人民共和国境内(不包括香港特别行政区、澳门特别行政区和台湾)销售。

版权©2013 由麦格劳-希尔(亚洲)教育出版公司与清华大学出版社有限公司所有。

北京市版权局著作权合同登记号 图字: 01-2013-2510

本书封面贴有 McGraw-Hill Education 公司防伪标签, 无标签者不得销售。

版权所有, 侵权必究。侵权举报电话: 010-62782989 13701121933

图书在版编目(CIP)数据

CISSP 认证考试指南(第6版) / (美) 哈里斯(Harris, S.) 著; 张胜生, 张博, 付业辉 译. —北京: 清华大学出版社, 2014

书名原文: CISSP All-in-One Exam Guide, Sixth Edition

ISBN 978-7-302-34440-7

I. C… II. ①哈… ②张… ③张… ④付… III. ①信息系统—安全技术—资格考试—指南 IV. ①TP309-62

中国版本图书馆 CIP 数据核字(2013)第 270024 号



责任编辑: 王 军 于 平

装帧设计: 牛艳敏

责任校对: 邱晓玉

责任印制: 李红英

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: 北京市密云县京文制本装订厂

经 销: 全国新华书店

开 本: 185mm×260mm 印 张: 64.75 字 数: 1784 千字
(附光盘 1 张)

版 次: 2014 年 1 月第 1 版 印 次: 2014 年 1 月第 1 次印刷

印 数: 1~4000

定 价: 128.00 元

产品编号: 051636-01

译者序

随着我国信息化技术的蓬勃发展，信息安全问题也越发严重，但信息安全工作还存在很多误区，比如：重技术，轻管理；重解决单个问题，轻规划方案；重计划，轻考核；重 IT 人员，轻业务人员教育；重建设，轻运维保障。这些问题困扰着信息安全从业人员，如何从信息安全原理上分析信息安全各个层面的问题，如何全面地审视信息安全威胁，如何将风险控制到可以接受的程度，《CISSP 认证考试指南(第 6 版)》给出了深入浅出的讲解。同时书中还强调了信息安全要从管理和业务层面入手，设计出信息安全策略，并根据策略进一步落实实施。作者的循序引导将给读者耳目一新的感觉，能够让读者快速建立起自己的信息安全知识体系，不愧是一本经典权威之作。

我从事信息安全工作 13 年，开展大中型企业的信息安全教学工作也已有 8 年，在与数万名学员的交流过程中，我学到了很多知识，我与我的师资团队一起开发了 15 门演练实战课和多门考试认证精讲类课程，在这其中我感受最深的是《CISSP 认证考试指南》中的知识精华给我带来的巨大帮助。

本书全面而细致地讲解了信息安全涵盖的 10 个领域，在每个领域中都贯穿了信息安全风险管理的精髓，作者通过大量案例不断帮助读者拓宽视野，了解行业中的管理和防御实践，本书是参加 CISSP 考试和提高信息安全水平的一本好书！

由于本书知识量大、涵盖面广，在阅读这本书的时候建议大家采用树型图软件梳理，当然关于知识汇总和大家的疑惑交流，也可以访问我的博客 <http://blog.sina.com.cn/anquan1000>。

本书的翻译过程很艰辛，在此我要特别感谢我的两位搭档：

张博：2005 年开始从事网络与信息安全工作，在一流的网络信息安全公司从事过大量安全项目的实施，并且曾经供职中国移动多年，有深厚的理论知识和丰富的实践经验，在书中的语言描述深入浅出。

付业辉：2002 年起，进入大型跨国企业并一直从事信息安全领域至今，拥有非常丰富的信息安全架构设计和大型安全项目的实施管理经验，对信息安全管理有着国际化的视野。

在翻译过程中，许多人给了我很多帮助，其中包括中国移动集团及各省公司的安全朋友们，向你们积极进取的精神致敬！最后还要感谢我的家人和我的学生们给予的支持和帮助。

本书博大精深，但在实际翻译过程中由于时间和能力所限，肯定存有各种不足之处，恳请读者理解和体谅，也欢迎读者对其中的问题给出批评指正，有关技术问题的交流信箱是 390890513@qq.com。

张胜生

CISSP/CISP/CISA/ISO27001 资深讲师
“红黑演义”云端攻防演练平台总设计师

从业人员对本书的赞誉

我和张胜生老师认识是在教育部 2009 年“第三届中国信息安全学科建设与人才培养研讨会”上，当时张老师在会上做了“大中型企业人才培养”专题发言，那时张老师已经是国内知名的 CISSP 讲师了。《CISSP 认证考试指南》作为行业认可的国际化 CISSP 教材，所涉及的知识领域十分广泛，既适合于行业人士深造所用，同时在校研究生和本科生教学过程中也可以作为选定教材和参考资料。

朱建明

中央财经大学信息学院院长/教授、博导

IT 和互联网技术已经渗透我们工作和生活的方方面面，互联网金融、手机支付、信息家电、智慧城市、物联网等新兴技术已经逐步由概念变为现实，IT 和互联网技术将与我们的身体健康、财产管理、日常工作、社交活动、休闲娱乐、个人消费等发生更多更加紧密的联系。因此，IT 和互联网是否安全可靠，将会成为决定我们工作和生活品质的重要因素，网络与信息安全问题已经被提升到了前所未有的高度，而且其重要性还在不断增加。现在很多从业人员、学生和爱好者们都在学习网络与信息安全技术，以实现自己在个人发展、工作需要或者兴趣爱好上的目标。而《CISSP 认证考试指南(第 6 版)》能够满足从业人员、学生和爱好者们的需要，可以在 CISSP 备考时起到极其重要的作用，也可以作为工具书和兴趣读物来使用。

孙晶

首都五一劳动奖章获得者

2010 年北京职工职业技能大赛信息安全比赛冠军

有幸认识张胜生老师是在 7 年前，他那时就已经在 CISSP 教学的第一线奋战多年，CISSP 的理念和知识已经深深融入张老师的血液中。虽然本书是一本国外教材的翻译版，但张老师在翻译本书的过程中，倾注了大量的心血，将自己对 CISSP 教学的丰富经验融入其中，使读者能够更加容易地理解本书原作者要表达的 CISSP 全部内容。

一本好书可以改变一个人的命运和前程，我认为《CISSP 认证考试指南(第 6 版)》就是一本这样的好书。作为 CISSP 认证考试的权威教材，本书以海一样广阔的胸怀容纳了安全行业的方方面面，从不同的角度，不同的主题系统化地阐述了建设和管控企业安全的方法和知识。

如果你是一个安全从业者，我认为这是一本温故而知新，每看一遍都有不一样体会的书。

如果你是一名安全初学者，我认为这是一本指导你走向安全岗位，并获得从业资格的宝典。

聂万泉

阿里巴巴高级安全专家

我是在 5 年前的 CISSP 培训课上认识张胜生老师的，他对信息安全深邃而独到的见解以及丰富的 CISSP 经验，给我留下了深刻的印象。《CISSP 认证考试指南》可以说是 CISSP 考试的宝典，而张老师翻译的《CISSP 认证考试指南(第 6 版)》和他更是相得益彰。

张健

完美世界信息安全总监

作者简介

Shon Harris 是 Shon Harris 安全有限责任公司和逻辑安全有限责任公司的创始人兼首席执行官，她是一名安全顾问，是美国空军信息作战部门的前任工程师，也是教师和作家。自 2001 年以来，Shon 拥有并经营着自己的培训和咨询公司，她为财富 100 强公司和政府机构广泛的安全问题提供咨询服务。她撰写了 3 本最畅销的 CISSP 图书，同时还是 *Gray Hat Hacking: The Ethical Hacker's Handbook* 和 *Security Information and Event Management(SIEM) Implementation* 的特约作者，*Information Security Magazine* 的技术编辑。她还为 Pearson 出版公司开发了许多数字化安防产品。

技术编辑简介

Polisetty Veera Subrahmanya Kumar 拥有 CISSP、CISA、PMP、PMI-RMP、MCPM、ITIL 认证证书，在信息技术领域拥有 20 多年的经验。他的专业领域包括信息安全、业务连续性、项目管理和风险管理。他最近担任项目管理协会 PMI-RMP(PMI-Risk Management Professional, 风险管理专业)资格认证委员会的主席，曾是 ISACA 印度 Growth Task Force 团队成员。过去他还曾担任各种 PMI 标准开发项目的内容开发团队负责人。他还是 PMI(美国项目管理协会)PMBOK(项目管理知识体系)培训的首席讲师。

致 谢

我要感谢所有在信息安全领域富有激情、具有奉献精神的行业开拓者。信息安全行业的精英就是那些追求道德成果的人。

我要感谢那么多的圈内人愿意花时间联系我，并让我知道我的工作直接影响着他们的生活。我感激人们花时间和精力反馈给我这些信息。

我也要感谢下列人士，在我撰写第 6 版时给我的帮助：

David Miller，他的工作热情、忠诚和友谊一直激励着我。能够与 David 共事，我觉得非常荣幸。没有他，我永远无法尝到龙舌兰酒的醇香。

Clement Dipuis，他待人热情，乐于助人，是一位不可多得的导师和朋友。

我公司的团队成员：Susan Young 和 Teresa Griffin，我无法表达对你们每个人深深的感激之情。

Greg Andelor，他是位图形艺术家，我这本书和我的其他项目很多图表都是出自他手，不幸的是他如此年轻就离我们远去了，我将永远怀念他。

Tom Modden 和 Randy Vickers，感谢他们为这本书写的精彩前言。

我的编辑 Tim Green 和我的出版合伙人 Stephanie Evans，他们在和我一起处理这些项目时总能耐心工作。

我最好的朋友和母亲 Kathy Conlon，即使她身体有时不太好，但总是陪伴在我身边。

特别是，我想要感谢我的丈夫 David Harris，谢谢他一直以来的支持与爱。没有他对我的坚定信心，我根本无法取得目前的成就。

前 言

我已经从事安全业务 39 年了，其中 26 年专注于信息安全。这些年我们已经看到了这个行业前所未有的变化：原来的计算机有一间屋子那么大，而且必须用水冷。到现在手机的计算能力已经超过了美国宇航局用于登陆月球所用的计算机。

我们敬畏地看着这一切，技术在发展，我们的生活质量也在不断提升。例如，我们可以通过手机来支付，我们的汽车也是计算机控制的，计算机控制带来了性能的优化和燃料的经济性，我们可以在酒店的房间办理登记手续并且得到登机牌。

但遗憾的是，一些人却通过技术和自己的优势找到漏洞，把这些进步变成了他们个人或组织谋取政治利益和经济利益的工具。

为了应对这些对手，信息安全专业出现了。第一个认识到信息安全专业的组织是(ISC)²，它成立于 1988 年。1994 年(ISC)²创建了注册信息系统安全专家(Certified Information System Security Professional, CISSP)认证并举行了第一次考试。这样就可以给经理和雇主(和潜在的雇主)一个保证，证实证书持有人对组成公共知识体(Common Body of Knowledge, CBK)中的 10 个领域都有基本的理解。

Shon Harris 撰著的《CISSP 认证考试指南》(*CISSP All-in-One Exam Guide*)是为应考者准备 CISSP 考试的指导书籍。我看到过许多类似的考试指南，Shon 的书和别人的区别是她的书并不教人们如何通过考试，而是教你要通过考试所需的知识和材料。这意味着，虽然可能已经通过考试并获得证书，但是 Shon 的书仍然会在你的书架上(或平板电脑中)作为一个有价值的参考指南。

我认识 Shon 已经将近 15 年了，感动我的是她的奉献精神、道德和荣誉。她是我们这个行业里我遇到的最专业的人。她不断工作来改进她的书以便所有水平的读者都能理解各个主题。她开发了一种学习模式，帮助确保一个组织从底层到最高管理层的每个人都知道对他们负责的数据尽职尽责是明智的选择。

很荣幸有机会帮助介绍 CISSP。我是 Shon 的忠实读者，我认为学习完这本书之后，你也会成为 Shon 的忠实读者。享受这段学习经历，为了这个证书而付出努力将物有所值。

Tom Madden, MPA, CISSP, CISM
疾病预防控制中心首席信息安全官

当今，网络安全环境不断变化，我们在很多正常活动时，比如收发电子邮件、上网冲浪等，都会遭受攻击。敌人可能会一直通过手机应用、电子邮件(钓鱼、垃圾邮件)、网站(重定向)或者其他工具对我们的日常活动发起攻击，来获得知识产权、个人信息或其他敏感数据。黑客行动主义者、罪犯和恐怖分子通过使用上述信息实现未经授权地访问系统和敏感数据。

黑客行动主义者通常使用攻击期间收集的信息来传递他们的消息，达到他们的目标。据赛门铁克的报告，在 2010 年，发现 163 个与移动计算相关联的新漏洞，286 亿个恶意软件变种，网络攻击数量增加了 93%，260 000 个身份信息泄漏。据迈克菲的报告，在 2011 年的前两个季度出现了 16 200 个恶意网站，平均每天有 2600 个钓鱼网站出现。

我们也看到了在我们的日常活动中新技术在不断发展。新的智能手机和平板电脑已经成为常见的家用电脑。但是新工具往往意味着新的漏洞，网络安全专家必须处理。信息技术实施人员需要快速设计和实施。其中关于新技术讨论最多的很可能对整个系统或组织造成风险。CSO/ CISO 会与技术部门一起寻找运用新技术的最佳方法，但物理安全和网络安全是部署策略中非常重要的部分。

培训是非常重要的，可以帮助最终用户、网络安全从业者，高级管理层明白他们的行为对组织内部有什么影响。甚至技术人员在家远程办公，连接到企业网络或将数据带回家都可能产生严重的后果。安全策略的推行将帮助建立一个更强的安全基线。组织已经意识到这个问题，很多组织已经开始编写可实现可接受的网络使用策略。这些策略如果执行得当，将有助于减少网络安全事件的发生。

一个解决方案是不可能解决网络安全问题的。深度防御、最佳业务实践、培训和意识教育、及时的信息共享等技术可以使网络攻击的影响降到最低。网络安全专家们需要使领导层及时了解最新的威胁和减少这些威胁影响的方法。由首席财务官、首席执行官、首席运营官做出的许多日常行为和决定，将会对任务实现产生影响；安全决策也应该成为这个流程的一部分。

在我获得证书后，《CISSP 认证考试指南》一直是我的一本重要参考资料。Shon Harris 创作并继续完善着这本全面的学习指南。组织机构各个层面的人，特别是网络安全人员，应该努力获得 CISSP 认证。这本学习指南是成功获得这个认证的关键，是网络专家准备和获得 CISSP 的工具包。CISSP 的 10 个相关领域将协助个人从许多角度来认识信息安全。我们不再仅仅关注信息安全领域的一个方面，它为我们提供了多个视角，提供了专业的、总体的网络安全。从策略领域到技术领域，CISSP 和这个学习指南涉及了网络安全的方方面面。即使这不属于你目前的培训计划，这本书将帮助任何人成为一个更好的安全从业者并且改善他们的组织安全状况。

Randy Vickers

Alexa Strategies, Inc.

网络安全分析师和顾问

CERT 美国的前总裁，国防部 CERT(JTF-GNO)前首席

目 录

第 1 章 成为一名 CISSP	1
1.1 成为 CISSP 的理由	1
1.2 CISSP 考试	2
1.3 CISSP 认证的发展简史	5
1.4 如何注册考试	6
1.5 本书概要	6
1.6 CISSP 应试小贴士	6
1.7 本书使用指南	8
1.7.1 问题	8
1.7.2 答案	16
第 2 章 信息安全治理与风险管理	17
2.1 安全基本原则	18
2.1.1 可用性	18
2.1.2 完整性	19
2.1.3 机密性	19
2.1.4 平衡安全	20
2.2 安全定义	21
2.3 控制类型	22
2.4 安全框架	26
2.4.1 ISO/IEC 27000 系列	28
2.4.2 企业架构开发	32
2.4.3 安全控制开发	41
2.4.4 COSO	44
2.4.5 流程管理开发	45
2.4.6 功能与安全性	51
2.5 安全管理	52
2.6 风险管理	52
2.6.1 谁真正了解风险管理	53
2.6.2 信息风险管理策略	53
2.6.3 风险管理团队	54
2.7 风险评估和分析	55
2.7.1 风险分析团队	56

2.7.2 信息和资产的价值	56
2.7.3 构成价值的成本	56
2.7.4 识别脆弱性和威胁	57
2.7.5 风险评估方法	58
2.7.6 风险分析方法	63
2.7.7 定性风险分析	66
2.7.8 保护机制	69
2.7.9 综合考虑	71
2.7.10 总风险与剩余风险	71
2.7.11 处理风险	72
2.7.12 外包	74
2.8 策略、标准、基准、指南和过程	75
2.8.1 安全策略	75
2.8.2 标准	78
2.8.3 基准	78
2.8.4 指南	79
2.8.5 措施	79
2.8.6 实施	80
2.9 信息分类	80
2.9.1 分类级别	81
2.9.2 分类控制	83
2.10 责任分层	84
2.10.1 董事会	84
2.10.2 执行管理层	85
2.10.3 CIO	86
2.10.4 CPO	87
2.10.5 CSO	87
2.11 安全指导委员会	88
2.11.1 审计委员会	89
2.11.2 数据所有者	89
2.11.3 数据看管员	89
2.11.4 系统所有者	89

2.11.5 安全管理员	90	3.5.1 规则型访问控制	167
2.11.6 安全分析员	90	3.5.2 限制性用户接口	167
2.11.7 应用程序所有者	90	3.5.3 访问控制矩阵	168
2.11.8 监督员	90	3.5.4 内容相关访问控制	169
2.11.9 变更控制分析员	91	3.5.5 上下文相关访问控制	169
2.11.10 数据分析员	91	3.6 访问控制管理	170
2.11.11 过程所有者	91	3.6.1 集中式访问控制管理	171
2.11.12 解决方案提供商	91	3.6.2 分散式访问控制管理	176
2.11.13 用户	91	3.7 访问控制方法	176
2.11.14 生产线经理	92	3.7.1 访问控制层	177
2.11.15 审计员	92	3.7.2 行政管理性控制	177
2.11.16 为何需要这么多角色	92	3.7.3 物理性控制	178
2.11.17 人员安全	92	4.7.4 技术性控制	179
2.11.18 招聘实践	93	3.8 可问责性	181
2.11.19 解雇	94	3.8.1 审计信息的检查	183
2.11.20 安全意识培训	95	3.8.2 保护审计数据和日志信息	184
2.11.21 学位或证书	96	3.8.3 击键监控	184
2.12 安全治理	96	3.9 访问控制实践	185
2.13 小结	100	3.10 访问控制监控	187
2.14 快速提示	101	3.10.1 入侵检测	187
2.14.1 问题	103	3.10.2 入侵防御系统	194
2.14.2 答案	110	3.11 对访问控制的几种威胁	196
第 3 章 访问控制	115	3.11.1 字典攻击	196
3.1 访问控制概述	115	3.11.2 蛮力攻击	197
3.2 安全原则	116	3.11.3 登录欺骗	198
3.2.1 可用性	116	3.11.4 网络钓鱼	198
3.2.2 完整性	117	3.11.5 威胁建模	200
3.2.3 机密性	117	3.12 小结	202
3.3 身份标识、身份验证、授权与可问责性	117	3.13 快速提示	202
3.3.1 身份标识与身份验证	119	3.13.1 问题	204
3.3.2 密码管理	127	3.13.2 答案	211
3.3.3 授权	149	第 4 章 安全架构和设计	215
3.4 访问控制模型	161	4.1 计算机安全	216
3.4.1 自主访问控制	161	4.2 系统架构	217
3.4.2 强制访问控制	162	4.3 计算机架构	220
3.4.3 角色型访问控制	164	4.3.1 中央处理单元	220
3.5 访问控制方法和技术	166	4.3.2 多重处理	224
		4.3.3 操作系统架构	226

4.3.4	存储器类型	235
4.3.5	虚拟存储器	245
4.3.6	输入/输出设备管理	246
4.3.7	CPU 架构	248
4.4	操作系统架构	251
4.5	系统安全架构	260
4.5.1	安全策略	260
4.5.2	安全架构要求	261
4.6	安全模型	265
4.6.1	状态机模型	266
4.6.2	Bell-LaPadula 模型	268
4.6.3	Biba 模型	270
4.6.4	Clark-Wilson 模型	271
4.6.5	信息流模型	274
4.6.6	无干扰模型	276
4.6.7	格子模型	276
4.6.8	Brewer and Nash 模型	278
4.6.9	Graham-Denning 模型	279
4.6.10	Harrison-Ruzzo-Ullman 模型	279
4.7	运行安全模式	280
4.7.1	专用安全模式	280
4.7.2	系统高安全模式	281
4.7.3	分隔安全模式	281
4.7.4	多级安全模式	281
4.7.5	信任与保证	283
4.8	系统评估方法	283
4.8.1	对产品进行评估的原因	284
4.8.2	橘皮书	284
4.9	橘皮书与彩虹系列	288
4.10	信息技术安全评估准则	289
4.11	通用准则	291
4.12	认证与认可	295
4.12.1	认证	295
4.12.2	认可	295
4.13	开放系统与封闭系统	296
4.13.1	开放系统	296
4.13.2	封闭系统	297
4.14	一些对安全模型和架构的威胁	297

4.14.1	维护陷阱	297
4.14.2	检验时间/使用时间攻击	298
4.15	小结	299
4.16	快速提示	300
4.16.1	问题	302
4.16.2	答案	307
第 5 章	物理和环境安全	311
5.1	物理安全简介	311
5.2	规划过程	313
5.2.1	通过环境设计来预防犯罪	316
5.2.2	制订物理安全计划	320
5.3	保护资产	331
5.4	内部支持系统	332
5.4.1	电力	333
5.4.2	环境问题	337
5.4.3	通风	339
5.4.4	火灾的预防、检测和扑灭	339
5.5	周边安全	345
5.5.1	设施访问控制	346
5.5.2	人员访问控制	352
5.5.3	外部边界保护机制	353
5.5.4	入侵检测系统	360
5.5.5	巡逻警卫和保安	362
5.5.6	安全狗	363
5.5.7	对物理访问进行审计	363
5.5.8	测试和演习	363
5.6	小结	364
5.7	快速提示	364
5.7.1	问题	366
5.7.2	答案	371
第 6 章	通信与网络安全	375
6.1	通信	376
6.2	开放系统互连参考模型	377
6.2.1	协议	378
6.2.2	应用层	379
6.2.3	表示层	380
6.2.4	会话层	381
6.2.5	传输层	383

6.2.6	网络层	384	6.8	内联网与外联网	486
6.2.7	数据链路层	385	6.9	城域网	487
6.2.8	物理层	386	6.10	广域网	489
6.2.9	OSI 模型中的功能和协议	387	6.10.1	通信的发展	490
6.2.10	综合这些层	389	6.10.2	专用链路	492
6.3	TCP/IP 模型	390	6.10.3	WAN 技术	495
6.3.1	TCP	391	6.11	远程连接	513
6.3.2	IP 寻址	395	6.11.1	拨号连接	513
6.3.3	IPv6	397	6.11.2	ISDN	514
6.3.4	第 2 层安全标准	400	6.11.3	DSL	515
6.4	传输的类型	402	6.11.4	线缆调制解调器	516
6.4.1	模拟和数字	402	6.11.5	VPN	518
6.4.2	异步和同步	404	6.11.6	身份验证协议	523
6.4.3	宽带和基带	405	6.12	无线技术	525
6.5	布线	406	6.12.1	无线通信	526
6.5.1	同轴电缆	407	6.12.2	WLAN 组件	528
6.5.2	双绞线	407	6.12.3	无线标准	534
6.5.3	光缆	408	6.12.4	WLAN 战争驾驶攻击	538
6.5.4	布线问题	409	6.12.5	卫星	538
6.6	网络互联基础	411	6.12.6	移动无线通信	539
6.6.1	网络拓扑	412	6.12.7	移动电话安全	543
6.6.2	介质访问技术	414	6.13	小结	545
6.6.3	网络协议和服务	425	6.14	快速提示	546
6.6.4	域名服务	433	6.14.1	问题	549
6.6.5	电子邮件服务	440	6.14.2	答案	556
6.6.6	网络地址转换	444			
6.6.7	路由协议	446	第 7 章	密码术	561
6.7	网络互联设备	449	7.1	密码学的历史	562
6.7.1	中继器	449	7.2	密码学定义与概念	566
6.7.2	网桥	450	7.2.1	Kerckhoffs 原则	568
6.7.3	路由器	451	7.2.2	密码系统的强度	568
6.7.4	交换机	453	7.2.3	密码系统的服务	569
6.7.5	网关	457	7.2.4	一次性密码本	570
6.7.6	PBX	459	7.2.5	滚动密码与隐藏密码	572
6.7.7	防火墙	462	7.2.6	隐写术	573
6.7.8	代理服务器	480	7.3	密码的类型	575
6.7.9	蜜罐	482	7.3.1	替代密码	575
6.7.10	统一威胁管理	482	7.3.2	换位密码	575
6.7.11	云计算	483	7.4	加密的方法	577

7.4.1 对称算法与非对称算法	577	7.11 链路加密与端对端加密	625
7.4.2 对称密码学	577	7.12 电子邮件标准	627
7.4.3 非对称密码学	579	7.12.1 多用途 Internet 邮件 扩展(MIME)	627
7.4.4 分组密码与流密码	581	7.12.2 可靠加密	628
7.4.5 混合加密方法	586	7.12.3 量子密码学	629
7.5 对称系统的类型	591	7.13 Internet 安全	630
7.5.1 数据加密标准	591	7.14 攻击	640
7.5.2 三重 DES	597	7.14.1 唯密文攻击	640
7.5.3 高级加密标准	597	7.14.2 已知明文攻击	640
7.5.4 国际数据加密算法	598	7.14.3 选定明文攻击	640
7.5.5 Blowfish	598	7.14.4 选定密文攻击	640
7.5.6 RC4	598	7.14.5 差分密码分析	641
7.5.7 RC5	599	7.14.6 线性密码分析	641
7.5.8 RC6	599	7.14.7 旁路攻击	641
7.6 非对称系统的类型	600	7.14.8 重放攻击	642
7.6.1 Diffie-Hellman 算法	600	7.14.9 代数攻击	642
7.6.2 RSA	602	7.14.10 分析式攻击	642
7.6.3 El Gamal	604	7.14.11 统计式攻击	642
7.6.4 椭圆曲线密码系统	604	7.14.12 社会工程攻击	643
7.6.5 背包算法	605	7.14.13 中间相遇攻击	643
7.6.6 零知识证明	605	7.15 小结	644
7.7 消息完整性	606	7.16 快速提示	644
7.7.1 单向散列	606	7.16.1 问题	646
7.7.2 各种散列算法	610	7.16.2 答案	651
7.7.3 MD2	611	第 8 章 业务连续性与灾难恢复	655
7.7.4 MD4	611	8.1 业务连续性和灾难恢复	656
7.7.5 MD5	611	8.1.1 标准和最佳实践	659
7.7.6 针对单向散列函数的攻击	612	8.1.2 使 BCM 成为企业安全计划的 一部分	661
7.7.7 数字签名	613	8.2 BCP 项目的组成	664
7.7.8 数字签名标准	615	8.2.1 项目范围	665
7.8 公钥基础设施	616	8.2.2 BCP 策略	666
7.8.1 认证授权机构	616	8.2.3 项目管理	666
7.8.2 证书	619	8.2.4 业务连续性规划要求	668
7.8.3 注册授权机构	619	8.2.5 业务影响分析(BIA)	669
7.8.4 PKI 步骤	620	8.2.6 相互依存性	675
7.9 密钥管理	621	8.3 预防性措施	676
7.9.1 密钥管理原则	622		
7.9.2 密钥和密钥管理的规则	623		
7.10 可信平台模块	623		

8.4 恢复战略.....	676	9.4.4 专利.....	741
8.4.1 业务流程恢复.....	680	9.4.5 知识产权的内部保护.....	742
8.4.2 设施恢复.....	680	9.4.6 软件盗版.....	743
8.4.3 供给和技术恢复.....	685	9.5 隐私.....	745
8.4.4 选择软件备份设施.....	689	9.5.1 对隐私法不断增长的需求.....	746
8.4.5 终端用户环境.....	691	9.5.2 法律、指令和法规.....	747
8.4.6 数据备份选择方案.....	691	9.6 义务及其后果.....	756
8.4.7 电子备份解决方案.....	694	9.6.1 个人信息.....	759
8.4.8 高可用性.....	697	9.6.2 黑客入侵.....	759
8.5 保险.....	699	9.6.3 第三方风险.....	760
8.6 恢复与还原.....	700	9.6.4 合同协议.....	760
8.6.1 为计划制定目标.....	703	9.6.5 采购和供应商流程.....	761
8.6.2 实现战略.....	704	9.7 合规性.....	762
8.7 测试和审查计划.....	706	9.8 调查.....	763
8.7.1 核查性测试.....	707	9.8.1 事故管理.....	763
8.7.2 结构化的排练性测试.....	707	9.8.2 事故响应措施.....	766
8.7.3 模拟测试.....	707	9.8.3 计算机取证和适当的证据收集.....	769
8.7.4 并行测试.....	708	9.8.4 国际计算机证据组织.....	770
8.7.5 全中断测试.....	708	9.8.5 动机、机会和方式.....	771
8.7.6 其他类型的培训.....	708	9.8.6 计算机犯罪行为.....	771
8.7.7 应急响应.....	708	9.8.7 事故调查员.....	772
8.7.8 维护计划.....	709	9.8.8 取证调查过程.....	772
8.8 小结.....	712	9.8.9 法庭上可接受的证据.....	777
8.9 快速提示.....	712	9.8.10 监视、搜索和查封.....	780
8.9.1 问题.....	714	9.8.11 访谈和审讯.....	781
8.9.2 答案.....	720	9.8.12 几种不同类型的攻击.....	781
第 9 章 法律、法规、合规和调查.....	725	9.8.13 域名抢注.....	783
9.1 计算机法律的方方面面.....	725	9.9 道德.....	783
9.2 计算机犯罪法律的关键点.....	726	9.9.1 计算机道德协会.....	784
9.3 网络犯罪的复杂性.....	728	9.9.2 Internet 架构研究委员会.....	785
9.3.1 电子资产.....	730	9.9.3 企业道德计划.....	786
9.3.2 攻击的演变.....	730	9.10 小结.....	786
9.3.3 国际问题.....	733	9.11 快速提示.....	787
9.3.4 法律的类型.....	736	9.11.1 问题.....	789
9.4 知识产权法.....	739	9.11.2 答案.....	794
9.4.1 商业秘密.....	739	第 10 章 软件开发安全.....	797
9.4.2 版权.....	740	10.1 软件的重要性.....	797
9.4.3 商标.....	740	10.2 何处需要安全.....	798

10.2.1	不同的环境需要不同的安全	799	10.11.1	Java applet	849
10.2.2	环境与应用程序	799	10.11.2	ActiveX 控件	851
10.2.3	功能与安全	800	10.12	Web 安全	852
10.2.4	实现和默认配置问题	800	10.12.1	针对 Web 环境的特定威胁	852
10.3	系统开发生命周期	801	10.12.2	Web 应用安全原则	859
10.3.1	启动	803	10.13	数据库管理	860
10.3.2	购买/开发	804	10.13.1	数据库管理软件	861
10.3.3	实现	805	10.13.2	数据库模型	862
10.3.4	操作/维护	805	10.13.3	数据库编程接口	866
10.3.5	处理	805	10.13.4	关系数据库组件	867
10.4	软件开发生命周期	807	10.13.5	完整性	869
10.4.1	项目管理	807	10.13.6	数据库安全问题	871
10.4.2	需求收集阶段	808	10.13.7	数据仓库与数据挖掘	875
10.4.3	设计阶段	809	10.14	专家系统和知识性系统	878
10.4.4	开发阶段	811	10.15	人工神经网络	880
10.4.5	测试/验证阶段	813	10.16	恶意软件	882
10.4.6	发布/维护阶段	815	10.16.1	病毒	883
10.5	安全软件开发最佳实践	816	10.16.2	蠕虫	885
10.6	软件开发模型	818	10.16.3	rootkit	885
10.6.1	边做边改模型	818	10.16.4	间谍软件和广告软件	886
10.6.2	瀑布模型	819	10.16.5	僵尸网络	886
10.6.3	V 形模型(V 模型)	819	10.16.6	逻辑炸弹	888
10.6.4	原型模型	820	10.16.7	特洛伊木马	888
10.6.5	增量模型	821	10.16.8	防病毒软件	889
10.6.6	螺旋模型	822	10.16.9	垃圾邮件检测	892
10.6.7	快速应用开发	823	10.16.10	防恶意软件程序	892
10.6.8	敏捷模型	824	10.17	小结	894
10.7	能力成熟度模型	825	10.18	快速提示	894
10.8	变更控制	827	10.18.1	问题	897
10.9	编程语言和概念	829	10.18.2	答案	903
10.9.1	汇编程序、编译器和解释器	831	第 11 章	安全运营	909
10.9.2	面向对象概念	832	11.1	运营部门的角色	909
10.10	分布式计算	841	11.2	行政管理	910
10.10.1	分布式计算环境	841	11.2.1	安全和网络人员	912
10.10.2	CORBA 与 ORB	842	11.2.2	可问责性	913
10.10.3	COM 与 DCOM	844	11.2.3	阈值级别	913
10.10.4	Java 平台, 企业版本	845	11.3	保证级别	914
10.10.5	面向服务架构	846	11.4	运营责任	914
10.11	移动代码	849			