Pearson

清华计算机图书·译丛

Corporate Computer Security

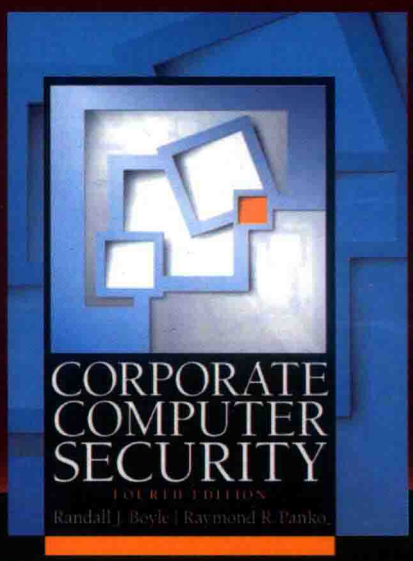
Fourth Edition

计算机安全

（第4版）

［美］ 兰迪·博伊尔（Randy J. Boyle）
雷蒙德·潘科（Raymond R. Panko） 著

葛秀慧 杨宏超 等译



清华大学出版社

清华计算机图书译丛

Corporate Computer Security

Fourth Edition

计算机安全

（第4版）

[美] 兰迪·博伊尔（Randy J. Boyle）
雷蒙德·潘科（Raymond R. Panko） 著

葛秀慧 杨宏超 等译

清华大学出版社
北京

北京市版权局著作权合同登记号　图字：01-2017-6938

图书在版编目（CIP）数据

计算机安全：第 4 版 /（美）兰迪·博伊尔（Randy J. Boyle），（美）雷蒙德·潘科（Raymond R. Panko）著；葛秀慧等译. —北京：清华大学出版社，2019
（清华计算机图书译丛）
书名原文：Corporate Computer Security, 4th Edition
ISBN 978-7-302-50308-8

Ⅰ. ①计…　Ⅱ. ①兰…　②雷…　③葛…　Ⅲ. ①计算机安全　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2018）第 115330 号

责任编辑：龙启铭
封面设计：傅瑞学
责任校对：时翠兰
责任印制：丛怀宇

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
课 件 下 载：http://www.tup.com.cn,010-62795954
印 装 者：三河市铭诚印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：38　　字　　数：924 千字
版　　次：2019 年 1 月第 1 版　　印　　次：2019 年 1 月第 1 次印刷
定　　价：128.00 元

产品编号：071533-01

译 者 序

当今网络环境不乏危险因素，数十亿的客户和其他商业伙伴都能通过互联网访问公司网络，这就给犯罪分子创造了机会，他们也能通过互联网访问数以百万计的公司和个人网络。犯罪分子甚至无须进入公司所在的国家，就能攻击其网站、数据库和核心的信息系统。目前，因为信息技术（IT）部分体现了公司的整体竞争优势，公司越来越依赖它。为了保护公司的 IT 基础设施免受各种威胁，保证公司的盈利能力，公司必须拥有全面的 IT 安全策略、完善的程序、强化的应用和安全的硬件，而本书，就是为应对这些问题而编写的。

当拿到本书进行略读时，我眼前一亮，就像打开了一个新视界。它不仅仅语言生动形象，娓娓道来，丝丝入扣，案例吸人眼球，更重要的是把技术和管理理念的诠释与整合上升到了新高度。更打动我的是，本书整体都围绕规划、保护、响应周期进行阐述，看似分散，实则紧凑，整本书的管理理念和技术水乳交融，既突出了组织为了保证安全应采取的策略，又使安全工作人员实施安全操作有章可循，使管理人员和技术人员将抽象的安全管理与实现，变成了组织普遍接受的日常行为，使组织获得最大的收益。本书的安全案例和项目，独特而有说服力，能解决许多 IT 从业人员及管理人员的困惑。

本书面向的读者是学生。学生学业有成后，要找工作。当学生咨询从事 IT 安全的专业人员，公司需要招聘什么样的新员工时，给出的答复是公司需要积极主动的员工，这些员工可以主动自主地学习，具备精湛的技术与技能，且有业务专长。业务专长并不意味着纯粹的管理专长，公司希望员工能深入了解安全管理。员工也想真正掌握防御性的安全技术。公司通常会讲，公司需要从“工蜂”开始的员工，工蜂员工是从技术开始的。总的来说，本书要为学生提供强有力的管理专长，同时还要使学生牢固掌握安全技术。

本书的大部分内容都是介绍保护对策的技术。但是，即使是对策章节也要求学生学习如何掌握相关技术。本书分为 10 章，第 1 章，从宏观角度，描述了当前的威胁环境，从细微的员工威胁、恶意软件威胁、黑客攻击到国家层面的网络战与网络恐怖。第 2 章以 Bruce Schneier 的名言为纲展开：“安全是一个过程，而非产品。”这是信息安全管理界的至理名言。IT 安全专业人员的主要工作是防御。保护公司及其资产是一个复杂的过程。在掌握了防御原则并实施之后，要通过详细了解攻击，防御才会有针对性，才能真正保护公司的安全。同样，对股东而言，公司的主要目标是产生利润。IT 安全应该是强大且具有保护性的，但同时，IT 安全又是透明且不引人注目的。将 IT 安全比喻成防弹玻璃既形象又贴切。防弹玻璃能起到保护作用，同时又不影响日常工作。同样，IT 安全应该时刻保护公司，同时又不妨碍公司的主要目标——产生利润。第 3～10 章从技术层面，讲解安全相关知识。第 3 章介绍了密码学如何保护通信，确保消息的保密性、真实性和完整性。第 4 章重点分析网络所遭受的攻击以及攻击者如何恶意改变网络的正常运行。第 5 章介绍访问控制，它是对系统、数据和对话访问控制的策略驱动。访问安全是从物理安全开始。用保安和监控设备控制楼宇入口点的访问是非常重要的。在楼宇内部控制通向敏感设备的通道也非常重要。

控制垃圾处理也很重要，要使攻击者不能通过垃圾桶搜索查找信息。物理安全必须扩展到计算机机房、台式机、移动设备和可移动存储介质。第6章介绍防火墙。防火墙就像电子门的警卫，是任何公司安全的第一道防线。防火墙不仅能提供入侵过滤，阻止攻击包入侵公司，还能进行出口过滤，防止受感染计算机发动外部攻击，对探测攻击做出响应以及防止盗窃知识产权。公司必须仔细规划其防火墙架构，使配置的防火墙能提供最大限度的保护。防火墙通常要记录丢弃的攻击数据包，安全人员应经常查看这些日志记录。第7章介绍主机强化。主机是阻止攻击的最后一道防线。主机是具有IP地址的各种设备。重中之重是要强化所有的主机。对于服务器、路由器和防火墙的强化更应重视，但也不能忽视客户端PC、手机等的强化。鉴于主机强化的复杂性，最重要的是遵循主机正在使用特定版本的操作系统的安全基准，此外，还可以保存经过良好测试的主机映像，然后将这些磁盘映像下载到其他计算机，再对相应计算机进行强化。第8章介绍应用安全。由于在客户端和服务器上运行的应用很多，因此，与主机强化相比，应用的安全强化要做更多的工作。每个应用的强化难度几乎等同于主机的强化。第9章讨论了数据在业务中的作用以及数据的安全存储。第10章从一个典型的灾难响应：沃尔玛在2005年如何应对卡特里娜飓风灾难案例开始，通过讨论传统安全事件和灾难响应来完成整个计划-保护-响应周期，使整本书首尾呼应，默契地成为一个整体。

本书由葛秀慧、杨宏超主译。在翻译本书的过程中，译者尽最大努力忠实原著。参加本书翻译的还有田浩、朱书敏、崔国帅、康驻关、李志伟、张涵和张皓阳。鉴于译者的能力有限，译文难免会存在纰漏，希望各位同行和专家予以批评指正。最后，感谢清华大学出版社的龙启铭编辑，在翻译过程中给予的建议和支持，也感谢清华大学出版社负责本书审校工作的编辑，逐字逐句地仔细检查、校对和修改，提高了译文的质量。

译者

作者简介

Randy J. Boyle 是 Longwood 大学商业与经济学院的教授。2003 年，他获得 Florida State 大学的管理信息系统（MIS）博士学位。他还拥有公共管理硕士学位和金融学士学位。他的研究领域包括计算机媒介环境中的欺骗检测、信息保证策略、IT 对认知偏见的影响以及 IT 对知识工作者的影响。他在 Huntsville 的 Alabama 大学、Utah 大学和 Longwood 大学都获得了大学教育奖。他的教学主要集中在信息安全、网络和管理信息系统。他是《应用信息安全》和《应用网络实验室》的作者。

Raymond R. Panko 是 Hawaii 大学 Shidler 商学院的 IT 管理教授。他讲授的主要课程是网络和安全。在来到大学之前，他是斯坦福研究所（现为 SRI 国际）的项目经理，在研究所，他为鼠标的发明者 Doug Englebart 工作。他获得了 Seattle 大学的物理学学士学位和工商管理硕士学位。他还拥有斯坦福大学的博士学位，他的学位论文是根据美国总统办公室的合同完成的。他作为高级优秀教师，被授予 Shidler 商学院 Dennis Ching 奖，他还是 Shidler 研究员。

致　谢

我们要感谢本书前几版的所有审稿人。他们多年使用本书的前几版，对书的内容了解透彻。他们的建议、推荐和批评使本书得以出版。本书来源于更大的社区，是学术界和研究人员共同的成果。

我们还要感谢为本版图书做出贡献的行业专家。其专业知识和观点增加了对现实世界的反思，这些经验和观点源于多年的实践经验。感谢 Matt Christensen，Utah Vally 大学的 Dan McDonald，Paraben 公司的 Amber Schroader，BlueCoat Systems 公司的 Chris Larsen，Grant Thornton 的 David Glod，Digital Ranch 公司的 Andrew Yenchik，Stephen Burton 和 Susan Jensen，以及 Teleperformance Group 公司的 Morpho 和 Bruce Wignall。

我们感谢编辑 Bob Horan 的支持和指导。一位优秀的编辑才能出版优秀的图书。Bob Horan 是一位优秀的编辑，所以能出版优秀的书籍。他已经从事编辑工作多年，我们以能与 Bob Horan 合作为荣。

特别感谢 Denise Vaughn、Karin Williams、Ashley Santora 和本书的制作团队。大多数读者不能完全体会将作者提供的“原始”内容转换成读者手中完整图书的过程中，编辑和制作团队所付出的辛勤工作以及他们的奉献精神。Denise、Karin、Ashley 和 Pearson 制作团队的承诺和对细节的关注使本书成为一本优秀的图书。

最后，最重要的是，我（Randy）要感谢 Ray。和读者一样，我已经多年使用 Ray 的书。Ray 的写作风格让学生感觉内容易懂，形象直观。Ray 的书很受欢迎，被全美国的教师广泛采用。他的书已成为目前行业中许多从业人员的网络和安全知识的来源。

我很感谢 Ray 对我的充分信任并和我一起完成本书。我希望本版图书延续了 Ray 其他书籍的写作风格，内容易懂且实用。与像 Ray 这样优秀的人一起工作是我的荣幸。

Randy J. Boyle
Raymond R. Panko

前　言

在过去的几十年中，IT 安全行业发生了巨大的变化。现在，安全漏洞、数据窃取、网络攻击和信息战已成为主流媒体中的常见新闻报道。以前，在大型组织中，只有少数专家才关注 IT 安全的专业知识，但现在，安全专业知识已与每个员工息息相关。

IT 安全行业的这些巨大变化成为本书出版的原动力。目前，除了已有的攻击之外，新攻击也层出不穷。我们希望本书的最新版本能体现安全行业的这些新变化。

本版的新内容

如果读者使用过本书以前的版本，则会发现自己所熟悉的内容几乎保持未变。但根据审稿人的建议，本书新增了部分内容。更具体地说，审稿人建议书中增加新的案例，每章的最后应有商业案例研究、新的实践项目、最新的新闻文章以及更多与认证相关的信息。

除了上述的内容变化之外，还增加了补充资料，以便本书更适于学生使用，对学生更具吸引力。下面介绍本版新增的内容。

开放案例

第 1 章的开放案例涉及一系列的数据泄露，它是迄今为止已知的最大数据丢失案例之一。该案例先分析了索尼公司的三次数据泄露事件，然后分析攻击者如何窃取数据，查明攻击背后的可能动机，对攻击者实施逮捕和惩罚，并探究事件对索尼公司的影响。这个案例是当今公司所面临真实威胁环境的一个例证。

商业案例研究

本版在每章的最后都增加了真实的案例研究，以便使商业内容成为焦点。案例研究旨在说明本章所讲的内容如何直接对实际的公司产生影响。在研究每个案例之后，我们会在突出的年度行业报告中找到与案例和章节内容相关的重要结论。案例研究与相关行业报告重要结论的结合，为课堂讨论提供了充足的资料，包括的开放性案例问题也成为指导案例讨论的有力支撑。同时，商业案例研究还为学生提供了应用、分析和综合本章所学内容的机会。

新的实践项目

每一章都有新的或更新的实践项目，这些项目使用最新的安全软件。每个项目都与章节内容直接相关。我们指导学生以屏幕截图来展示自己完成的项目。项目设计要求每个学生在完成项目之后都要有与众不同的屏幕截图。学生所提交的任何共享或重复项目都将一目了然。

最新的新闻文章

每一章都包含扩展和最新的 IT 安全新闻文章。本书超过 80%的新闻文章引自上一版

出版之后所发生的故事。

认证的扩展内容

前一版的审稿人建议提供更多的与IT安全认证相关的内容。我们生活在一个靠凭证证明技能以及经验具有合法性的世界。在这方面，安全领域也没有什么不同。为此，我们更新并扩展了第10章的认证相关的热点文章。在IT安全行业中求职的学生很可能需要其中的某种认证。

选用本书的原因

预期的读者

本书是为一学期的IT安全入门课程编写的。主要读者是主修信息系统、计算机科学或计算机信息系统的高年级本科生。本书还适用于信息系统硕士（MSIS）、工商管理硕士（MBA）、会计硕士（MAcc）或其他渴求更多IT安全知识的硕士研究生。

本书旨在为学生提供与企业安全相关的IT安全知识。本书的学习将为进入IT安全领域的学生奠定坚实的知识基础。本书也可以作为网络安全的读本。

先修课程

本书适用于先修了信息系统入门课程的学生。但是在学习本书之前，建议最好先修完网络课程。对于没有学习网络课程的学生，模块A给出了与网络安全相关的重要概念。

即使网络是你学过的先修课程或先修的核心课程，我们仍建议你好好学习模块A。这有助于刷新和强化网络的概念。

技术与管理内容的平衡

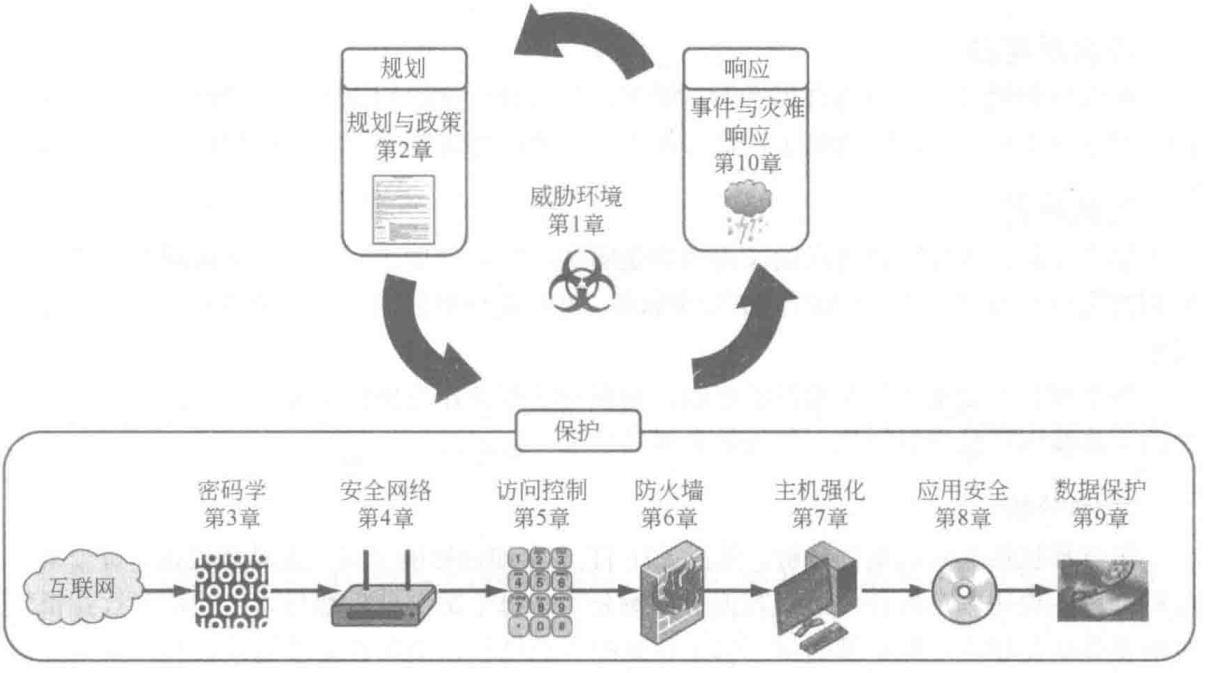
我们的学生需要找工作。当学生咨询从事IT安全的专业人员，公司需要招聘什么样的新员工时，给出的答复是非常相似的。公司需要积极主动的员工，这些员工可以主动自主地学习，具备精湛的技术与技能，且有业务专长。

业务专长并不意味着纯粹的管理专长。公司希望员工能深入了解安全管理。员工也想真正掌握防御性的安全技术。公司经常抱怨学过管理课程的学生甚至不知道如何操作状态包检测防火墙，也不知道如何操作其他类型的防火墙。一种常见的说法是“我们不会雇用这样的孩子作为安全管理者”。之后公司通常会讲，公司需要从“工蜂”开始的员工，工蜂员工是从技术开始的。

总的来说，我们要使学生具有强有力的管理专长，同时还要使学生牢固掌握使用安全工具的技术。本书的大部分内容都是介绍保护对策的技术。但即使是对策章节也要求学生学习如何掌握相关技术。读者可以通过用或不用每章最后的实践项目来“限制”技术内容。

本书的组织

本书从分析当今企业所面临的威胁环境开始，这有利于引起学生的关注，然后介绍本书后面要用到的术语。通过讨论威胁环境，知道为了保证安全，需要后面章节所讲的防御。



本书的其余部分按照原有良性的规划-保护-响应周期进行组织。第 2 章讲规划，第 10 章介绍事件和灾难响应。第 3～9 章介绍保护信息系统的对策。

对策部分从密码学一章开始，之所以从密码学开始，是因为加密是与许多其他对策密不可分的部分。密码学后的章节依次介绍安全网络、访问控制、防火墙、主机强化、应用安全和数据保护。总结一下，本书内容是按数据流的流向进行组织的，数据源于网络，通过防火墙，到达主机，最终主机对数据进行处理和存储。

用本书作为教材

本书的内容需要在一学期内完成。这一学期还要留出部分学时用于考试、演示、特邀发言人、实践项目或模块中的资料。为了激发学生的学习兴趣，最好每节课都从一个实践项目的演示开始。

在学习新课程之前，学生最好先预习相关的课程内容。每章都有贴近案例研究的技术和概念资料。我们建议教师在讲授每一章内容之前，先进行简短的阅读测验，或要求学生上交对相关理解题的测试。

幻灯片和要仔细学习的图

幻灯片讲义几乎涵盖了书中的所有内容，当然也包含书中的图。要仔细学习的图可以说是关键内容的总结。幻灯片讲义和书中的图成为学习本书的最大助力。

测试理解题

在每小节后都有对问题理解的测试。通过测试，使学生知道自己是否真正理解了所学内容。如果没能理解，则需要复习。掌握相关内容后，再继续学习新内容。测试项目文件由具体的测试理解题体现。如果学生没有学习某些内容，则会知道某些多选题不会做。

综合思考题

在每章的最后，都有综合思考题，学生需要综合所学的知识才能完成这些习题。这样的习题本质上更有用，因为除了记忆课本内容之外，还需要应用所学的知识。

实践项目

学生经常评论他们最喜欢的课程内容是实践项目。学生之所以喜欢实践项目，是因为他们要用与章节内容相关的流行 IT 安全软件。每章至少都有两个应用项目和后续的项目思考题。

每个项目都要求学生在项目结束时，用独特的截图作为他们完成项目的证明。每个学生的屏幕截图将包括时间戳、学生姓名或其他唯一标识符。

案例分析

每章都包括真实的案例分析，重点关注 IT 安全如何影响公司。更具体地说，每个案例分析都旨在说明本章所介绍的内容如何影响公司。每个案例分析都与突出的年度行业报告中的重要结论相关。每章都提供了每个行业报告的链接，用作补充的阅读资料。案例分析和相关行业报告的重要结论也为课堂讨论提供了充足的资料。

案例讨论题

案例分析之后是一系列的开放式问题，用于指导基于案例的课堂讨论。它们为学生提供在真实世界商业案例背景下，应用、分析和综合本章所学内容的机会。

反思题

每章都有两个常见问题，要求学生反思他们到底学到了什么。这些问题使学生有机会在更高层次上全面地思考每章的内容。

嘿！所有攻击软件在哪里

这本书不教学生如何攻入计算机。有专门设计的软件来利用漏洞和访问系统，但本书不包括这类软件。本书的重点是如何主动保护企业系统免受攻击。

有效地保护企业信息系统是一个复杂的过程。要学会如何保护企业信息系统需要学习整本书。一旦学生对如何保护公司系统有了深入的了解，他们就可以准备分析渗透测试软件了。

在第 10 章，教师有时间可介绍一些攻击。但是如果教导犯罪，请一定要小心。用攻击工具是上瘾的，因为小实验室是学校网络和互联网之间的气隙网络，学生很少只满足在小实验室使用攻击工具。学生的一些公开攻击会导致 IT 安全课程的禁课。

教师资料

这是一门很难的课程。我们已尽己所能为教师提供资料支持。我们的目标是减少教师准备这门课程必须花费的时间，以便把更多的精力用于讲课。

学习新课程的资料、监测当前事件和管理活跃的研究议程是非常耗时的。我们希望所准备的教师资料，能使教师用最少的准备时间，讲授最高质量的课程。

在线教师资源

在 Pearson 高等教育网站（http:// www.pearsonhighered.com）上，有下面介绍的所有资料。资料包括幻灯片讲义、测试项目文件、TestGen 软件、教师手册和教学大纲示例。

幻灯片讲义

每章都有幻灯片讲义。它们不是“几个选定的幻灯片”。它们是完整的讲义，有详细的图和解释。在幻灯片中有来自书中漂亮的图。我们创建的幻灯片非常漂亮是不言自明的。

测试项目文件

本书的测试项目文件使具有挑战性的多项选择题考试出题变得很容易。测试项目文件中的问题直接涵盖每一章的测试理解题。这意味着考试直接与本章所讨论的概念相关。

教师手册

教师手册给出了如何讲授本书内容的建议。例如，本书从威胁开始。在第一堂课中，建议教师可以先让学生列出可能攻击自己的人，然后让学生想出一组可能攻击他们的方式。沿着这个思路，自然而然地课堂讨论会触及本章中的概念，如病毒和蠕虫之间的区别。

教学大纲示例

如果你是第一次教这门课程，我们给出了教学大纲的示例。它可以指导你构建课程，也能减少你的课程准备时间。

学生文件

通过访问 www.pearsonhighered.com/boyle，可下载 Word 格式的学习指南和家庭作业文件。

通过电子邮件联系我们

请随时给我们发电子邮件。你可以发邮件给 BoyleRJ@Longwood.edu 联系 Randy，或者发邮件 Ray@Panko.com 联系 Ray。如果有问题，也请随时与我们联系。我们也欢迎你提出对下一版的建议和对本版的其他支持。

目　录