模糊测试

强制性安全漏洞发掘

FUZZING Brute Force Vulnerability Discovery

(美) Michael Sutton
Adam Greene
Pedram Amini
著

黄陇 于莉莉 李虎 译

机械工业出版社
China Machine Press

掌握揭露安全性缺陷的最强大技术！

模糊测试现在已经发展成为一种最有效的软件安全性测试方法。模糊测试是指将一个随机的数据源作为程序的输入，然后系统地找出这些输入所引起的程序失效。著名的模糊测试专家将告诉你如何抢在别人之前使用模糊测试来揭示软件的弱点。

本书是第一部也是唯一一部自始至终讨论模糊测试的专著，将以往非正式的技巧转变为训练有素的最佳实践，进而将其总结为一种技术。作者首先回顾了模糊测试的工作原理并勾勒出模糊测试相比其他安全性测试方法的关键优势。然后，介绍了在查找网络协议、文件格式及Web应用安全漏洞中的先进的模糊测试，演示了自动模糊工具的用法，并给出多个说明模糊测试强大效力的历史案例。

本书主要内容包括：

- 为什么模糊测试能够简化测试设计并捕捉利用其他方法捕捉不到的软件缺陷。
- 模糊测试过程：从识别输入到评估“可利用性”。
- 理解实施有效模糊测试所要满足的需求。
- 比较基于变异的和基于生成的模糊器。
- 在模糊测试中应用并初始化环境变量和自变量。
- 掌握内存数据的模糊测试技术。
- 构建定制的模糊测试框架和工具。
- 实现智能的故障检测。

攻击者早已经开始使用模糊测试技术。当然，你也应该使用。不论你是一位开发者、一位安全工程师还是测试人员或QA专业人员，本书都将教会你如何构建安全的软件系统。

作者简介：

Michael Sutton是SPI Dynamics公司的安全布道师。他还是Web应用安全组织(WASC)的成员，负责其中的Web应用安全统计项目。

Adam Greene目前担任纽约某大型金融新闻公司的工程师。此前他曾经是iDefense公司的工程师，这是位于Reston, VA.的一家智能技术公司。Adam Greene在计算机安全领域的主要研究兴趣是可靠挖掘方法、模糊测试和基于UNIX系统的审核和挖掘开发。

Pedram Amini是TippingPoint公司的安全研究和产品安全评估组的项目领导。此前他曾经是iDefence实验室的主任助手，同时也是该实验室的创建者之一。他的主要兴趣是研究逆向工程——开发自动支持工具、插件和脚本。

这三位作者经常出席Black Hat安全大会并在其中做主题报告。

www.Pearsonhighered.com

投稿热线：(010) 88379511
购书热线：(010) 68995259, 68995264
读者信箱：hzjsj@hzbook.com

华章网站 http://www.hzbook.com

网上购书：www.china-pub.com

封面设计：杨宇梅

上架指导：计算机/程序设计
ISBN 978-7-111-25755-4

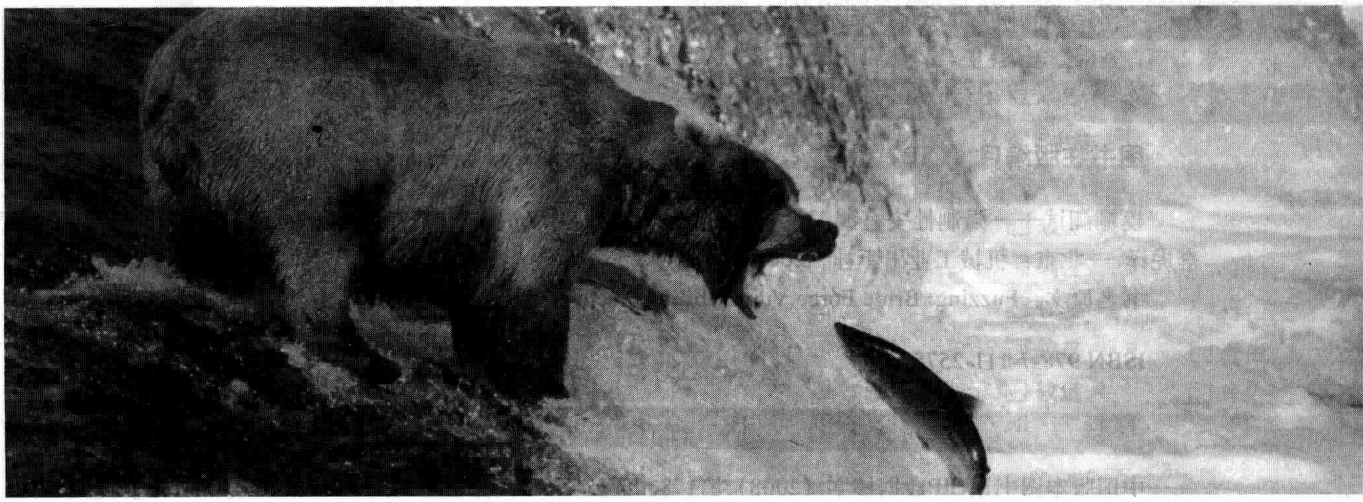
9 787111 257554

定价：59.00元

模糊测试

强制性安全漏洞发掘

FUZZING Brute Force Vulnerability Discovery



(美) Michael Sutton
Adam Greene
Pedram Amini
著

黄陇 于莉莉 李虎 译

机械工业出版社
China Machine Press

本书是讨论模糊测试的专著，主要内容包括：模糊测试的工作原理，模糊测试相比其他安全性测试方法的关键优势，模糊测试在查找网络协议、文件格式及Web应用安全漏洞中的技术现状等。演示了自动模糊工具的用法，并给出多个说明模糊测试强大效力的历史案例。

本书可作为开发者、安全工程师、测试人员以及QA专业人员的参考用书。

本书版权登记号：图字：01-2008-2959

图书在版编目（CIP）数据

模糊测试——强制性安全漏洞发掘 /（美）斯顿（Sutton, M）等著；黄陇，于莉莉，李虎译. —北京：机械工业出版社，2009.1

书名原文：Fuzzing: Brute Force Vulnerability Discovery

ISBN 978-7-111-25755-4

Ⅰ.模… Ⅱ.① 斯… ② 黄… ③ 于… ④ 李… Ⅲ.软件—测试 Ⅳ.TP311.5

中国版本图书馆CIP数据核字（2008）第198606号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：陈佳媛

北京瑞德印刷有限公司印刷

2009年1月第1版第1次印刷

186mm × 240mm · 23.75印张

标准书号：ISBN 978-7-111-25755-4

定价：59.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

译者序

模糊测试的基本思想是自动产生和发送大量随机的或经过变异的输入值给软件，如果发生失效或异常，便可挖掘出软件系统存在的薄弱环节和安全漏洞。这种方法由威斯康星州麦迪逊大学的Barton Miller教授首先发明，后来发展成为一种对软件质量有深远影响的测试技术。近年来，模糊测试方法及其支持工具受到研究人员和工程技术人员的日益关注，逐步成为软件测试和系统安全研究领域的一个重要分支。

本书是迄今为止有关模糊测试的第一部专著性参考文献。书中首次系统地阐述了模糊测试的基本概念、分类和实现技术，总结出模糊测试和其他安全性测试方法相比所具有的优点。本书的内容全面丰富，堪称模糊测试领域的“百科全书”，内容涉及模糊测试的定义、方法、分类和不同操作系统平台下模糊器的应用和开发技术，此外还穿插了许多典型历史案例以说明模糊测试的强大威力。对于从事软件测试、网络安全和信息安全领域的研究和工程人员来说，本书具有极高的参考价值。

译者所在单位北京航空航天大学软件测评实验室（附属于北航软件工程研究所）、总参陆航研究所、二炮软件测试中心等长期从事软件测试、质量保证方法及支持工具的研究开发。作为具有全军装备软件测评资质的军用软件测评实验室，北航软件测评实验室和二炮软件测试中心承担了大量关键软件的第三方测评任务，在软件安全漏洞的分析和发掘方面积累了一定的学术成果和工程经验，为了促进国内同行在这一领域的学习和交流，特组织翻译此书。

本书的主要内容由黄陇、于莉莉翻译，李虎完成了部分翻译工作并统校全书。参加本书技术校对的还有李晓丽、许福、宋淼、刘辉、王晓博、贾荣飞等。机械工业出版社华章公司的编辑为本书付出了大量辛勤努力，在此向他们表示诚挚的感谢！

由于译者水平有限，难免存在疏漏和错译之处，欢迎广大读者批评指正。

译者简介

黄陇，男，博士，中国人民解放军总参陆航研究所高级工程师，北京航空航天大学软件工程研究所出站博士后，在国内重要期刊和国际会议上发表论文20余篇，曾获得全军科技进步奖，长期从事软件测试理论、方法和技术工具的研究开发，出版多部该领域的译著。

于莉莉，女，中国人民解放军第二炮兵软件测试中心资深软件测评工程师，北京航空航天大学软件工程研究所博士研究生，自2005年起先后负责十余项大型分布式军事系统软件测试项目，特别是在安全性测试领域积累了丰富的研究和工程经验。

李虎，男，博士，北京航空航天大学计算机学院讲师，北航软件测评实验室测评工程部负责人，近年来先后发表论文20余篇，其中大多被EI等著名检索机构收录，多个著名计算机科学类杂志的审稿人，主持包括国家自然科学基金在内的多项国家级科研项目，曾获国防科学技术三等奖，申请国家技术发明专利2件，获得发明专利1件，在软件工程、软件测试和质量保证领域出版专译著十余部。

序　言

安全漏洞是研究安全问题的生命线。无论是执行渗透测试、评价新产品还是审核关键构件的源代码，安全漏洞都驱动着我们的决策，让我们有理由花费时间，并且很多年来一直影响着我们的选择。

源代码审核是一种白盒测试技术，这是一种很长时间以来都流行的软件产品安全漏洞检测方法。这种方法需要审核者了解编程概念和产品功能的每一个细节，深入洞察产品的运行环境。除此之外，源代码审核还有一个显而易见的缺陷——必须首先要获得产品的源代码。

幸运的是，除了白盒技术外，我们还可以使用不需要访问源代码的黑盒技术。模糊测试就是黑盒技术中的一种可选方法，这种方法在发掘那些用审核方法无法发现的产品关键安全漏洞方面被证明是成功的。模糊测试是这样的一个过程：向产品有意识地输入无效数据以期望触发错误条件或引起产品的故障。这些错误条件可以指导我们找出那些可挖掘的安全漏洞。

模糊测试没有实际的执行规则。它是一种技术，测试结果是这种技术的成功性的唯一度量。任意一个给定的产品都可能接受无限的输入。模糊测试技术旨在预测产品中可能存在的编程错误以及什么样的输入可能会触发错误。正因为如此，与其说它是一门学科，不如说它是一种技术。

模糊测试可以简单到只是随意敲打键盘来输入随机数据。我的一个朋友有个3岁的儿子，他就是用这么简单的手段发现了Mac SO X操作系统的屏幕界面锁定功能中的一个漏洞。我的朋友锁定了屏幕界面然后到厨房找酒喝。当他回来的时候，他的儿子已经设法成功地解除了锁定，并且打开了浏览器，所用的方法正是随意敲打键盘。

过去的几年里，我用模糊测试技术和模糊工具在大量的软件中发现了数百个漏洞。2003年12月，我编写了一个简单的程序向一个远程服务发送随机UDP 包流。结果这个程序发现了Microsoft WINS服务器的两个新的漏洞。该程序后来又帮助我在其他产品中找出了少量的缺陷。最后的结果证明，用简单的随机UPD包流能够发现计算机协会的多个产品中的漏洞，包括Norton Ghost管理服务和OS X操作系统的一个公共服务。

模糊器对发现网络协议以及其他许多产品都有效。在2006年的第一季度，我精心设计了3个不同的浏览器模糊工具，结果发现了多种浏览器中的缺陷。2006年第二季度，我又编写了一个Active X模糊器（AxMan），仅在Microsoft的产品中就发现了超过100个缺陷。这些缺陷许多都是在“Month of Browser Bugs”项目中形成的，结果导致该项目组又进一步开发了“Metasploit”框架中的模块。在最初开发AxMan后的接近一年的时间里，我还利用模糊测试发现了AxMan本身所包含的一些漏洞。模糊器真是一个能够不断赐予我们新礼物的工具。

本书是一部真正让我们有理由相信模糊测试是一门技术的专著。书中所介绍的内容涵盖了对新产品执行模糊测试以及创建有效的模糊工具所需要的全部知识。有效模糊测试的关键在于明确对什么样的产品使用什么样的测试数据，以及需要什么工具来操纵、监控和管理模糊测试过程。本书的作者是模糊测试技术的先锋，在阐明模糊测试的复杂过程方面作出了卓越贡献。

祝各位猎捕Bug愉快！

——H. D. Moore

前　言

我知道“人类和鱼类能够和平共处”。

——George W. Bush, 2000年9月29日

简介

模糊测试的概念至少已经流传了20年，但是直到最近才引起广泛的关注。安全漏洞困扰了许多流行的客户端应用程序，包括Microsoft的Internet Explorer、Word和Excel，它们中的许多漏洞在2006年通过模糊测试技术发现。模糊测试技术的有效应用产生了许多新的工具和日益广泛的影响。本书是第一部公开发表的关于这一主题的专著，这一尴尬事实同时也预示着未来人们将会对模糊测试产生更浓厚的兴趣。

多年来，我们参与了许多有关安全漏洞的研究工作，并且在日常工作中使用了各种不同的模糊测试技术，从不成熟的、凭借个人嗜好的项目到高端的商业产品，都用到过模糊测试。每一位作者都曾参与开发过自用版本的和公开发行版本的模糊器。这本书凝聚了我们以往的实践经验和正在进行的研究项目所花费的心血，我们希望读者能够从中获益。

目标读者

安全性领域的书籍和文章通常由这一领域的研究者所撰写，以方便该领域的其他研究者参考。我们坚信，只要安全性领域的研究小组把解决安全性问题视为其唯一责任，那么安全性问题的数量和严重程度就会随着时间的推移而继续增长。因此，我们付出巨大的努力以使本书能够服务于更多的读者，既包括模糊测试的新手也包括早已对本领域有所了解的读者。

假设我们只是将开发完成的应用程序提交给一个安全小组，然后让他们在产品发布之前对其进行一个快速审核，相信这样的过程能够产生安全的应用程序显然是不现实的。当开发者或QA组的组员说：“安全根本不是问题——我们有个安全小组关心这件事呢”，如此这般，日子就会一天一天的过去。安全性必须融入软件开发生命周期（SDLC），而不是到了最后才草率处理。

让开发组和QA组把注意力集中在安全性问题上可能是个过高的要求，特别是对那些以往没有这么做的开发组和QA组来说尤其如此。我们认为模糊测试是一种独一无二的安全漏洞发掘方法学，由于它能够高度自动化，因此学习和掌握这种方法学的读者可以相当广泛。我们希望经验丰富的安全领域的研究者可从本书获得有价值的东西，同样希望开发人员和QA人员从中获益。模糊测试可以并且应该是任何完整SDLC的一部分，不仅在测试阶段需要考虑，在开发阶段也同样需要考虑。缺陷发现得越及时，修补缺陷的成本就越低。

预备知识

模糊测试是一个广泛的主题。尽管本书会介绍一些不专属于模糊测试的背景内容，但是我们仍然假设读者应该拥有这一领域的预备知识。在学习本书之前，读者至少应该对程序设计和计算机网络有一定的基本了解。模糊测试涉及自动化安全测试，这本书的内容自然要包括如何构造自动化工具。我们有目的地选择了多种编程语言来完成这个任务。语言的选择是根据具体任务的，这也说明了模糊测试可以用多种方法实现。当然，没有必要一一罗列所用到的所有编程语言的背景知识，但是介绍一两种语言无疑会帮助读者从这些章节中获益。

本书自始至终都贯穿着对各种安全漏洞的详细描述，并讨论如何通过模糊测试来识别这些漏洞。然而，定义或剖析安全漏洞本身的性质并不是本书的目标。一些优秀的书籍是专门讨论这一主题的。如果需要寻找一部关于软件安全漏洞的初级读本，可以参阅Greg Hoglund、Gray McGraw所著的《Exploiting Software》和Jack Koziol、David Litchfiel等的《Shellcoder's Handbook》，它们都是极好的参考读物。

学习方法

如何最好地利用本书，这取决于读者的背景和目的。如果你是一位模糊测试的初学者，我们推荐你按顺序逐章消化理解，因为本书的内容进行了精心编排，前面先介绍一些必要的背景信息，随后转入高级主题。反之，如果你已经在使用各种模糊测试工具方面花费了一些时间，那么请不要犹豫，可以直接进入感兴趣的主题，因为本书的不同逻辑章节的划分大致上是相互独立的。

本书的第一部分主要介绍不同的、具体的模糊测试类型，这些模糊测试类型将在随后的章节中逐一讨论。如果读者对模糊测试比较陌生，可以考虑把这一部分作为必读章节。模糊测试可以作为多种目标下的安全性测试方法，不过这些目标下的方法都遵循相同的基本原则。在第一部分，我们试图将模糊测试定义为一种安全漏洞发掘方法并详细介绍相关的知识，不考虑这种方法运用于何种目的。

第二部分关注模糊测试的各种相关应用目标。每种目标的介绍跨越了两到三章。最前面的一章介绍每类目标的背景信息，随后的各章集中介绍这些目标下的模糊测试自动化，详细阐述如何针对这种目标构造模糊器。当认为有必要分别介绍Windows平台和UNIX平台下的模糊器工具时，这两个主题分别安排在有关自动化的两章。例如，以第11章“文件格式模糊测试”为例，该章详细描述有关模糊文件分析器的内容，第12章“文件格式模糊测试：UNIX平台上的自动化测试”则深入介绍基于UNIX的文件模糊器的实用程序设计，第13章“文件格式模糊测试：Windows平台上的自动化测试”讲解运行在Windows环境中的文件格式模糊器如何构造。

第三部分讨论模糊测试领域的高级主题。对于那些已经牢固掌握模糊测试背景知识的读者，可以直接跳入第三部分，不过大部分读者很可能需要先了解第一部分和第二部分，然后再学习第三部分。第三部分关注的是近年来浮现出的新技术，这些技术刚刚得到实施，但是未来将成为安全漏洞发掘的高级工具可以利用的模糊测试技术。

最后，在第四部分，我们将总结学习过本书后的收获，然后深入洞察未来的发展方向。尽管模糊测试并不是一个新概念，但是这一领域仍然有足够的发展空间，并且我们希望本书将为未来的研究空间注入一丝灵感。

少许幽默

写书是一件严肃认真的工作，尤其是对诸如模糊测试这样的复杂主题。这就是说，我们希望尽量给随后的读者（实际上这些人可能比写书的人更重要）带来一些乐趣，同时也尽最大的努力让写作的过程更愉快。出于这样的考虑，我们决定在每一章的开头引用美国第43届总统George W. Bush（别名Dubya）的一段话。不论你的政治倾向或信仰是什么，没人能够否定Bush先生在过去几年中所炮制出的一些引文，这些引文甚至能够写满一年的日历！我们从中挑选了一些最喜欢的引文与读者分享，希望读者和我们得到同样的快乐。读完本书后，读者会发现模糊测试可以被应用于各种不同的目标，显然也可以应用到对英语的模糊测试。

关于封面

有时，安全漏洞经常被称为“鱼”（例如，可以参见DailyDave安全性邮件列表中关于“The L Word & Fish”的提示线索）。这是一个有用的类比，在讨论安全性和安全漏洞时可以被应用到这个问题的各个方面。可以把这一领域的研究者比喻为钓鱼者。对应用程序的汇编代码实施逆向工程，逐行分析查找安全漏洞，这样的人可比喻为“深海钓鱼者”。同许多其他的审核手段相比，模糊测试充其量只是海面搜索，并且通常只对“容易抓的鱼”更有效。此外，大灰熊是一个著名的“模糊动物”，当然也是强大的动物。本书的封面中有一个模糊的动物，正在捕捉一条鱼，后者代表一个安全漏洞。

配套站点

站点www.fuzzing.org绝对是本书不可分割的一部分，并不仅仅起到补充资源的作用。除了包含本书出版后的勘误表外，该站点还是书中所有源代码和工具的一个中央资源仓库。经过一段时间的努力，我们打算让这个站点从一个以图书为中心的资源站点发展成为模糊测试这一学科的资源、工具和信息的有价值的社区。我们欢迎读者提出反馈信息，以帮助我们让该站点成为一个有价值的、开放的知识库。

致　谢

全体作者致谢

尽管只有三个人的名字出现在封面上，但是许多在幕后提供支持的人让本书从设想变成了现实。首先是我们的朋友和家人，他们付出了很多夜晚和周末来支持我们写书。在完成本书的过程中，我们亏欠了家人许多啤酒、电影和宁静的夜晚，但是不要怕，这些亏欠终究要得到补偿。尽管我们损失了许多个星期六的晚上，为的是就本书而举行讨论会，同时我们也承认，别人不会损失星期六的夜晚。

Peter DeVries有一次说到，“我喜欢成为作者，但是却不能承受文字工作之苦“。对这一点我们不能苟同。有了好的想法和思路只是战役的一半。一旦草稿写成，就需要一小队评阅人员加入这场战役，以便让人们相信我们确实能够完成一本书的写作。在此，我们希望向本书的技术编辑表示感谢，他们尽最大的努力指出了本书的某些错误，并对我们的一些假设提出质疑。这其中最值得一提的是Charlie Miller，他竭尽全力帮助我们让这本书成为“锋利的刀刃”。我们还要诚挚地感谢H.D. Moore，感谢他对本书所做的评审并撰写前言。我们还要感谢Addison-Wesley出版社的工作组指导我们完成图书出版过程，其中包括Sheri Cain、Kristin Weinberger、Romny French、Jana Jones和Loris Lyons。最后，至少还要专门感谢的是本书的责任编辑Jessica Goldstein，感谢他给了有着疯狂想法并且天真的认为写书并不是一件难事的三位作者一个机会。

Michael的致谢

我希望借此机会感谢我的妻子Amanda，感谢她在写作本书的过程中给予我的耐心和理解。在本书写作过程中的大部分时间里，我们一直在计划举行婚礼，本来应该在门廊里畅饮一杯白酒，但是却花费了太多的时间对着计算机屏幕。我还要真诚地感谢所有家庭成员给我的支持，他们鼓励我从事这项事业并坚信我能做好它。感谢iDefense Labs组和我在SPI Dynamics的同事，在本书写作的全过程他们给予我了支持和启发。最后，感谢带我上路的合作者，为我提供了GOYA讲演、激发我的灵感并完成了大量我自己根本无法完成的工作。

Adam的致谢

我应该感谢我的家庭（尤其是我的姐姐和父母）、老师和JTHS的顾问，包括Mark Chegwidden、Louis Collucci、Chris Burkhart、sgo、Nadwodny、Dave Aitel、Jamie Breiten、Davis家、Brothers Leondi、Reynolds、Kloub和AE、Lusardi、Lapilla，当然，最后一定还要感

谢Richard。

Pedram的致谢

感谢本书的合作者，他们给了我机会一起写这本书并且让我在写书的漫长过程中始终干劲十足。感谢我在TippingPoint的工作组，包括Pierce、Cameron Hotchkies和Aaron Portnoy，感谢他们的聪明才智和为本书所做的技术评审。感谢Peter Silberman、Jamie Butler、Greg Hoglund、Halvar Flake和Ero Carrera，感谢他们的鼓励和永远不停的款待。专门感谢David Endler、Ralph Schindler、Sunil James和Nicholas Augello，他们是我同父异母兄弟，总能够让我依靠。最后，衷心地感谢我的家庭，感谢他们在我因写书而不在家时给予的耐心。

专业成就人生
立体服务大众

HZ BOOKS

www.hzbook.com

填写读者调查表　加入华章书友会
获赠精彩技术书　参与活动和抽奖

尊敬的读者：

感谢您选择华章图书。为了聆听您的意见，以便我们能够为您提供更优秀的图书产品，敬请您抽出宝贵的时间填写本表，并按底部的地址邮寄给我们（您也可通过www.hzbook.com填写本表）。您将加入我们的“华章书友会”，及时获得新书资讯，免费参加书友会活动。我们将定期选出若干名热心读者，免费赠送我们出版的图书。请一定填写书名书号并留全您的联系信息，以便我们联络您，谢谢！

书名：　　书号：7-111-(　　)

姓名：	性别：☐男　☐女	年龄：	职业：
通信地址：		E-mail：	
电话：	手机：	邮编：	

1. 您是如何获知本书的：

☐朋友推荐　☐书店　☐图书目录　☐杂志、报纸、网络等　☐其他

2. 您从哪里购买本书：

☐新华书店　☐计算机专业书店　☐网上书店　☐其他

3. 您对本书的评价是：

技术内容	☐很好	☐一般	☐较差	☐理由_____
文字质量	☐很好	☐一般	☐较差	☐理由_____
版式封面	☐很好	☐一般	☐较差	☐理由_____
印装质量	☐很好	☐一般	☐较差	☐理由_____
图书定价	☐太高	☐合适	☐较低	☐理由_____

4. 您希望我们的图书在哪些方面进行改进？

_____

_____

5. 您最希望我们出版哪方面的图书？如果有英文版请写出书名。

_____

_____

6. 您有没有写作或翻译技术图书的想法？

☐是，我的计划是_____　☐否

7. 您希望获取图书信息的形式：

☐邮件　☐信函　☐短信　☐其他_____

请寄：北京市西城区百万庄南街1号　机械工业出版社　华章公司　计算机图书策划部收
邮编：100037　电话：（010）88379512　传真：（010）68311602　E-mail: hzjsj@hzbook.com

目　录