Broadview
www.broadview.com.cn

WILEY
www.wiley.com

安全技术大系

Reversing:Secrets of Reverse Engineering

Reversing:逆向工程揭密

[美] Eldad Eilam 著
Elliot Chikofsky 作序
韩 琪 杨 艳 王玉英 李 娜 等译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

WILEY
www.wiley.com

安全技术大系

Reversing:Secrets of Reverse Engineering

Reversing:逆向工程揭密

[美] Eldad Eilam 著
Elliot Chikofsky 作序
韩 琪 杨 艳 王玉英 李 娜 等译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书描述的是在逆向与反逆向之间展开的一场旷日持久的拉锯战。作者 Eldad Eilam 以一个解说人的身份为我们详尽地评述了双方使用的每一招每一式的优点与不足。

书中包含的主要内容有：操作系统的逆向工程；.NET 平台上的逆向工程；逆向未公开的文件格式和网络协议；逆向工程的合法性问题；拷贝保护和数字版权管理技术的逆向工程；防止别人对你的代码实施逆向工程的各种技术；恶意程序的逆向工程；反编译器的基本原理以及它对逆向过程的影响。

本书适合软件逆向工程的从业人员以及软件开发者们阅读。

图书在版编目（CIP）数据

Reversing：逆向工程揭密 /（美）艾拉姆（Eilam,E.）著；韩琪等译.—北京：电子工业出版社，2007.9
（安全技术人系）
书名原文：Reversing: Secrets of Reverse Engineering
ISBN 978-7-121-04995-8

I. R… II. ①艾… ②韩… III. 工业产品－计算机辅助设计 IV. TB472-39

中国版本图书馆 CIP 数据核字（2007）第 139102 号

责任编辑：顾慧芳
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：38.75　字数：806 千字
印　　次：2007 年 9 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

译 者 序

记得第一次做与逆向有关的工作是 2000 年，当时由于项目的需要，做过一个钩子（hook）程序，用于截获一个第三方控件发出的消息，但是当时还不知道什么是逆向工程。第一次看到“逆向工程”这个词是在 2001 年的《机械工程学报》上的一篇文章中，主要是讲用三坐标测量仪测量产品中各个部件的三维尺寸并在计算机中快速建模、进而反推其设计思想和基本设计原则。第一次使用逆向工程工具也是在 2001 年，当时从网上下载了 Numega SoftICE，具体哪个版本已经记不清了，在家里的旧电脑上折腾了好几天，直到系统崩溃才罢手。

之后呢，只是零零星星地看过一些相关的资料。因此，当初电子工业出版社和我联系此书的翻译时，我有些犹豫——近 600 页的逆向工程“巨”著，而且该书无论从深度还是广度上都较其他有关逆向工程的书更胜一筹。但褚华博士和王玉英博士的“加盟”，让我心里踏实了许多，她俩做过系统的逆向工程和程序理解的研究工作，也发表过不少相关的研究论文。

逆向工程这一术语最早来源于机械工程领域（我的老本行）。随着软件业的发展，逆向工程被引入软件工程领域。对于软件逆向工程，IEEE 软件工程技术委员会行政秘书 E. J. Chikofsky 和 J. H. Cross 在他们的文章中给出了如下定义：软件逆向工程是分析目标系统，认定系统的组件及其交互关系，并且通过高层抽象或其他的形式来展现目标系统的过程。

经过十几年的发展，软件逆向工程领域已有不少研究成果和商业化的产品；但是软件逆向工程仍然算不上成熟，这主要表现在对理论和实践的研究都还处于早期的探究阶段，并未形成统一的、系统的、科学的软件逆向工程的理论和方法。从工程实际的角度来看，大体上可以将软件逆向工程分为两大类：

第一类是从已知软件系统的完整代码出发，生成对应系统的结构以及相关设计原理和算法思想的文档。实际上，学习和研究别人的源代码就属于此类。Chikofsky 在本书的序中特别指出：阅读别人写的代码或者自己以前写的代码实际上也是逆向工程在起作用。

第二类是从没有源代码的程序出发，生成对应的源程序、系统结构以及相关设计原理和算法思想的文档等，亦即本书重点讨论的二进制逆向工程。

本书共有 13 章和三个附录，涵盖了逆向工程的基础知识、应用、开发和拓展的方方面面问题。其中第 5 章、第 9 章和附录 A、B、C 由韩琪翻译，第 3 章、第 11 章和第 13 章由

杨艳翻译，第 7 章、第 8 章和第 10 章由王玉英翻译，第 4 章和第 6 章由李娜翻译，第 1 章由褚华翻译，第 2 章由陈贵敏翻译，第 12 章由辛健斌翻译；全部译稿的校对由陈贵敏和褚华完成。所有的翻译和校对工作历时半年多，在此，我要感谢为本书的出版付出辛勤汗水的电子工业出版社博文视点的工作人员，特别要感谢本书的策划编辑朱沐红老师和责任编辑顾慧芳老师，她们的严谨认真工作使该译本可读性更高，她们的鼓励更使我信心百倍。

由于译者水平所限，加之时间仓促，译文中肯定存在错误和疏漏，敬请读者批评指正。我的 E-mail：efoxxx@126.com。

陈贵敏

2007 年 5 月于西安电子科技大学

序

当我们意识到我们所运行的软件中有多少我们不确信它在做什么时，我们一定会大吃一惊，甚至会惊慌失措。我们从货架上购买收缩塑料包装的软件，运行安装程序，以便在计算机上安装大量的文件、修改系统设置、删除或禁止该软件的以前版本和被替代的工具、并修改关键的注册表文件。每当我们访问某个网站的时候，我们会调用数十个程序和代码片断或者与它们进行交互，这是获得预期的感观、感受及行为所必需的。我们会购买包含成千上万个游戏和工具的光盘，或者从网上下载共享软件。我们在试用同事和朋友的有用程序的部分功能后，会与他们交换这些程序。

还有，我们下载更新程序和安装补丁程序，完全相信供应商能确保这些对程序的修改是正确和完善的。我们盲目地希望每个程序的最新修改会与我们系统中所有的其他程序保持兼容。我们太信赖自己并不了解甚至一无所知的软件了。

我指的不仅仅是我们用的个人台式机或笔记本电脑。普遍计算（ubiquitous computing，或者说“软件无处不在”）的概念促使软件控制和软件互连快速地占领了我们生存的环境中形形色色的设备。如今，普通汽车的引擎控制所需软件代码的行数要比过去将 Apollo（阿波罗号）上的宇航员着陆月球所需的代码行数还要多。

现今的软件已经变得非常复杂且相互关联在一起，甚至连开发人员都不知道他们所开发的应用程序中到底有哪些特性，以及该程序对系统或其他软件有哪些影响。要测试程序的所有控制通路以及所有的用户选项组合通常是不太现实的，这需要耗费太多的财力和时间。多层架构和软件运行并与之交互的巨大的网络平台使得检查和测试所有的组合简直是天方夜谭。像事先检测药物之间的相互作用所面临的问题一样，许多软件系统也存在着许多未知的和无法预测的问题。

逆向工程是了解软件“所作所为”的一套最重要的技术和工具。正式地讲，逆向工程是“通过分析目标系统以识别系统的组件以及这些组件之间的相互关系并创建该系统另一种形式的表示或更高级的抽象的过程”（IEEE 1990）。这使得我们能够想像出软件的结构，它的工作方式以及驱动其行为的特性。分析技术和软件自动检测工具的应用程序，为我们理解软件的复杂度和弄清“真相”提供了切实可行的方法。

逆向工程应该算是我们的老朋友了。每当某人阅读其他人编写的代码时，实际上就是逆向过程在起作用。当一个开发者阅读自己数天前写的代码时，也是在应用逆向工程。逆

向工程是一个发现的过程。当我们着手阅读一份代码，无论它是我们自己写的还是别人写的，我们总会找到、学到、看到我们从未想到过的东西。

软件逆向工程是在1990年发展起来的，现在它已经成为一些会议和计算机用户组的专题会议的主题。它受到工程领域的认可的标志是在*IEEE Software*杂志上发表了一篇有关逆向工程和设计恢复概念分类学的文章。其后，研究逆向技术、软件可视化、程序理解、数据逆向工程、软件分析以及相关工具和方法的研究人员越来越多。各种各样的研究讨论会，比如说一年一度的国际逆向工程工作会议（Working Conference on Reverse Engineering，WCRE），不断地在探索、延伸、扩展现有技术的价值。现在人们对二进制逆向（即本书的主要内容）的研究兴趣越来越浓，这是为了支持平台移植、互操作、恶意软件检测以及问题断定。

作为一个管理和信息技术的顾问，经常有人问我："你怎么能容忍逆向工程？"并寻根究底地问："你开发并销售过软件，你不想别人尊重和保护你的版权和知识产权？"这样的讨论通常是从术语逆向工程的负面内涵引出的，特别是针对软件许可协议中的某些条款。然而，在许多方面，逆向工程技术对软件供应链上的制造商和消费者来说都是有价值的。

比如说听诊器，盗贼可以用它听保险箱上锁机构的倒拨开关落回原位的声音，而家庭医生可以用它检测呼吸和心脏问题，或者计算机技术人员还可以用它诊断密封磁盘驱动器的故障而无需将磁盘暴露在具有潜在危险的粉尘之中——通过仔细聆听它的运行声音。工具本身并没有好坏之分，问题在于用它来做什么。

在20世纪80年代初期，IBM决定不再向用户公开其大型机操作系统的源代码。大型机用户过去在解决问题的过程中总是依赖于参考源代码，他们根据源代码定制、修改和扩展IBM的操作系统。我还从IBM用户组Share中得到我的座右铭，即使用枪支控制法的反对者在一次著名的辩论中的一句话："如果SOURCE是违法的，那只有亡命之徒会有SOURCE"。将这句话应用于目前的软件，意指黑客和恶意代码的开发人员知道许多破解其他人开发的软件的技术。当然，好人也有必要知道这些技术。

逆向工程在现代软件分析中有着广泛的用途：

- 查找恶意代码。许多病毒和恶意代码的探测技术使用逆向工程来理解那些令人憎恶的代码是怎样构成和运作的。通过逆向找出可用作特征码的可识别模式用于驱动商业探测器和代码扫描器。
- 发现意想不到的缺陷和错误。即使是设计最完美的系统也可能存在漏洞，这是由于我们使用的"前向工程"开发技术所固有的特点导致的。逆向工程可以帮助我们在发生致命的软件失效前识别缺陷和错误。
- 查找是否使用了其他人所写的代码。搞清楚在应用程序的哪里使用了受保护的代码和技术，这对于保护知识产权不被滥用是很重要的。逆向工程技术可用于检测应用程序是否包含所关心的软件单元。

- 寻找对共享软件和开放源码的使用（在不该使用的地方）。与侵犯代码版权相反的是，如果一个产品以安全和专用为目的，是否有可公开获取的代码可能是大家关心的问题。逆向工程能够用于检测代码复制问题。
- 从其他（不同领域或用途的）产品中学习。逆向工程技术使我们能够学习先进的软件方法，还允许新学员研究大师的作品。这对于学习和积累不断发展的代码知识来说是非常有用的。许多网站是通过参考其他网站的做法建立的。许多网页开发人员是通过阅读其他网站的源代码学习 HTML 和网页编程技术的。
- 发现原开发人员以前没有意识到的特性或机遇。代码复杂性可以促进新的创新。现有的技术可以在新的场合再次使用。逆向工程可以引领新的软件发现并创造新的创新机遇。

在计算机辅助软件工程（computer-aided software engineering，CASE）方法和自动代码生成的应用中，无论是新系统开发还是软件维护，我一直声称我们创建的任何系统都应立即用一套逆向工程工具“检阅”一遍。那些在“检阅”过程中暴露出来的漏洞和问题会为用户、客户以及客户服务人员节省大量用于检测问题和解决问题的时间。更好地理解代码有可能为整个产业界节省大量的资金。

我参与软件逆向工程的研究与应用已有 30 年之久，包括在大型机、中等级别的系统以及 PC 机上，从程序语言语句、二进制模块、数据文件到作业控制流。这期间，我听到过许多成熟的方法，也见过许多人们尝试过的技术。尽管有这些基础，我还是从这本书以及书中对逆向技术的观点中学到很多。我相信你也会的。

Elliot Chikofsky
工程管理和集成公司（弗吉尼亚州，Herndon 镇）
再工程论坛主席
IEEE 软件工程技术委员会行政秘书

致　谢

首先，我要感谢我所钟爱的 Odelya（“Oosa”）Buganim，谢谢你不懈的支持和鼓励——没有你就没有此书！

我还要感谢我的家人，谢谢你们的耐心与支持：我的祖父母 Yosef 和 Pnina Vertzberger，我的父母 Avraham 和 Nava Eilam-Amzallag，我的哥哥 Yaron Eilam。

我还要感谢 Wiley 的编辑们：我的执行总编 Bob Elliott，是他给了我写这本书并与他合作的机会；我的开发编辑 Eileen Bien Calabro，谢谢你对我这样一个新手作者的耐心与谅解，而且我对文字的理解仅限于在软件行业中数年工作所学到的。

许多才华横溢朋友花了大量的时间和经历审阅此书，并帮我确保书中内容的正确性和趣味性。我要特别感谢 David Sleeper，他花费了很长的时间审阅了全部书稿，还有 Alex Ben-Ari，感谢他有成效的投入和有价值的见解。谢谢 George E. Kalb，他审阅了本书的第三部分，谢谢 Mike Van Emmerik，他审阅了反编译一章，还要谢谢 Roger Kingsley 博士细致的审阅和投入。最后，我要谢谢 Peter S. Canelias，他审阅了本书中有关法律方面的内容。

要不是 Avner（“Sabi”）Zangvil 最初建议写一本有关逆向工程的书并鼓励我去写它的话，可能压根就不会有这本书。

我还要谢谢我的好朋友，他们是 Adar Cohen 和 Ori Weitz，谢谢你们的友谊和支持。

最后但同样重要的是，要谢谢我们迷人的猫咪 Bookey，如果它不是很安静的话，这本书估计不会是现在这个样子的。在我写这本书的过程中，Bookey 很多时候都是爬在我的膝盖上呼呼大睡的。

简　介

欢迎你阅读《逆向：逆向工程揭密》一书。本书是在我参与了多年的软件开发项目之后写的，这些项目由于各种各样的原因需要反复地对第三方代码进行逆向工程。起初，我觉得这是一个非常单调乏味的过程，只是在没有替代方法来获取信息的情况下才不得已使用它。后来，一霎那间我破除了某个思维障碍，我发现自己迅速地“驰骋”于无正式文献记录的机器码中，快速地破译了代码的涵义并得到我想要的有关代码功能和用途的答案。这时候，我逐渐明白这是一种威力强大的技术，因为这意味着不管我有什么样的有关要处理软件的问题，我都可以非常容易地找到答案，即使我没有看过任何相关的文献资料或者正在处理的程序的源代码。本书就是要为每一个对软件有深刻理解的读者能够这样做提供相关的知识和技术。

其思想很简单：我们应当对底层软件有深入的理解，还要学习那些能够让我们轻松进入任何程序的二进制码并获取信息的技术。不知道系统为什么会以它那样的工作方式运转而且其他人也不知道答案的话，怎么办？没问题——你完全可以自己深入研究并找到答案。这听起来有点恐怖和不现实，是吗？一点儿也不，我写这本书的目的就是向你讲解并示范平常就可以用于解决各种各样问题的逆向工程技术。

不过我总是急于求成。也许你以前没有接触过软件逆向工程的概念，我在这里先简要介绍一下。

逆向工程和底层软件

在开始进入本书所讨论的各部分内容之前，我们应当正式地介绍一下该书的主题：逆向工程。逆向工程是指将工程制品（比如汽车、喷气发动机或者软件程序）以揭示其最底层的细节（如其设计和架构）的方式进行解构的过程。这与研究自然现象的科学研究有些类似，区别就在于一般没有人会把科学研究看做逆向工程，这仅仅是因为没有人确切地知道自然算不算是工程制品。

对软件而言，逆向工程归结起来就是拿一个既没有源代码又没有准确文献资料的现成程序，尝试恢复出它的设计和实现细节。在某些情况下，可以找到程序的源代码，但是找

不到最初的开发人员了。本书所讨论的就是通常所说的二进制逆向工程。二进制逆向工程技术的目标是从没有源代码的程序中提取有价值的信息。在有些情况下可以从程序的二进制代码中恢复出准确的源代码（或者接近高级表示的代码），这会大大简化逆向工作，因为阅读用高级语言写的代码要比阅读低级汇编语言代码容易得多。在其他情况下，我们最终得到的只是用晦涩难懂的汇编语言程序清单。本书将讲述这一过程以及程序为什么这样运行，同时还将详细描述如何在各种不同的环境中破解程序代码。

我决定将这本书取名为“逆向（Reversing）”，这一叫法被许多在线社区用来描述逆向工程。因为你可以把逆向看做是逆向工程的别名，故我将在本书中交换使用这两种叫法。

大多数人在尝试想像从可执行二进制程序中提取有意义的信息的时候会变得有些焦虑，因此，我把这本书的首要任务定为证明这种害怕是没有必要的。二进制逆向工程如果行得通的话，它通常能解决用其他方法解决起来极其困难的问题，而且如果方法得当的话它也没有你想像的那么复杂。

本书主要讨论逆向工程，但事实上书中所讲述的内容要比逆向工程多得多。在软件行业内，逆向工程被频繁地应用于各种场合，本书的主要目标之一就是在讲授逆向工程的同时研究这些领域。

下面简要地列出了本书要讨论的一些主题：

- IA-32 兼容处理器的汇编语言以及如何阅读编译器生成的汇编语言代码；
- 操作系统内幕以及如何对操作系统实施逆向工程；
- .NET 平台上的逆向工程，包括.NET 开发平台的简介及.NET 平台汇编语言：MSIL（Microsoft 中间语言）；
- 数据逆向工程：如何破译未公开的文件格式或者网络协议；
- 逆向工程的合法性问题：什么情况下是合法的，什么情况下是非法的？
- 拷贝保护和数字版权管理技术；
- 破解人员是如何应用逆向工程使拷贝保护技术失效的；
- 防止人们对代码实施逆向工程的技术并认真尝试评价这些技术的有效性；
- 目前恶意程序的基本原理以及如何应用逆向工程研究并清除这样的程序；
- 一个真实恶意程序的现场剖析和展示，以及揭示了攻击者是怎样通过程序通信获得被感染系统的控制权的；
- 反编译器背后的理论和原则，以及它们对各种低级语言代码进行反编译的有效性。

本书的组织

本书共分四部分。第 1 部分提供了学习后边部分所需的基础知识，其他三个部分分别讲述了不同的逆向工程情景，并展示了真实的案例研究。每一部分的详细描述如下。

- **第 1 部分—逆向 101**：本书是从讨论理解底层软件所需的所有基础知识开始的。你必定能想像到，这几章不可能包含所有相关的知识，你只需将这些内容看作是对以前学过的材料重新整理。如果本书前三章讲述的所有内容或者大部分内容对你来说都是全新的，那么这本书不适合你。这几章的主要内容有：介绍了逆向工程及其各种应用（第 1 章），底层软件的概念（第 2 章），并以 Microsoft Windows 为重点介绍了操作系统内部结构（第 3 章）。总的来说，如果你精通这些内容以及底层软件，你基本上可以跳过这几章。第 4 章讨论了各种类型的常用逆向工程工具，并为各种情况推荐了适合的专用工具。这些工具的大部分都在本书展示的逆向工程实例过程中使用过。
- **第 2 部分——应用逆向**：本书的第 2 部分演示了在真正的软件上实施的逆向工程项目。这部分的每一章分别讨论一种不同类型的逆向工程应用。第 5 章讨论了最常见的情境——对操作系统或第三方代码库进行逆向工程，以便更好地利用它的内部服务和 API。第 6 章展示了如何应用数据逆向工程技术破解无正式文档记录的专用文件格式。第 7 章展示了漏洞研究人员如何使用逆向工程技术在二进制代码可执行程序中寻找漏洞。这部分的最后一章，第 8 章讨论了恶意软件，如病毒和蠕虫，并简要介绍了这一内容。这一章还展示了对真正的恶意程序进行逆向工程的实例过程，这实际上就是恶意软件研究人员为了研究恶意程序、估计它们带来的危险、并研究如何清除它们所必须经历的过程。
- **第 3 部分——盗版和拷贝保护**：这一部分主要讨论与安全相关的代码的逆向工程，如拷贝保护和数字版权管理（Digital Rights Management，DRM）技术。第 9 章简要介绍了盗版和拷贝保护并讨论了拷贝保护技术的基本原则。第 10 章讲述了反逆向工程技术，如在拷贝保护和 DRM 技术中常常采用的技术，并评价它们的有效性。第 11 章讨论了“破解者”是怎样使用逆向工程破解拷贝保护机制并窃取拷贝保护内容的。
- **第 4 部分——反汇编之外**：本书的最后部分所讲述的内容已经超出了可执行程序的简单反汇编。第 12 章讨论了在 Microsoft .NET 开发平台上开发的虚拟机程序的逆向工程过程。这一章简单介绍了.NET 平台及其低级的汇编语言 MSIL（Microsoft 中间语言，Microsoft Intermediate Language）。第 13 章论讨论了有关反编译的更理论化的主题，并说明了反编译器是怎样工作的以及反编译本地汇编语言代码为什么那么具有挑战性。

- **附录**：本书共包含三个附录，可以作为破解 Intel IA-32 汇编语言程序的有价值的参考资料。这几个附录远远超出了简单的汇编语言参考向导，讲述了公共代码段（common code fragments）和常用编译器对几种典型的代码序列表现出来的编译器习性（complier idioms），并介绍了识别和破解它们的方法。

谁应当阅读此书

本书所揭示的技术能够让各行各业的人受益。软件开发人员想要提高他们对软件底层知识的理解：如操作系统、汇编语言、编译，等等，这本书无疑会让他们受益匪浅。更重要的是，该书能够让所有对开发技术感兴趣的人们快速而高效地研究和考察现有代码，不管是操作系统代码、软件库代码还是软件组件代码。除了这些技术以外，本书还提供了诸如安全、版权控制等许多主题的精彩讲述。即使对逆向工程不是很感兴趣，只是在书中找到一处或多处感兴趣的内容，你就可能从中获益。

就预修知识而言，本书涉及到一些相当高级的技术材料，我已经试着尽可能让它们在内容上保持独立。所需的大多数基础知识都包含在本书的第 1 部分中。当然，要想真正从本书中获益，你还得有一定的软件开发知识和经验，这也是很重要的。如果你一点专业的软件开发经验都没有，但是现在正在学习这方面的知识，那也为时不晚。相反地，如果你没有正规地学习过计算机，只做过几年的程序设计，那你也可能从本书中获益。

最后，对于那些已经具有底层软件和逆向工程经验的高级读者而言，他们希望学习一些有趣的高级技术和如何从现有代码中提取非常详细的信息，本书也会对他们有所帮助。

工具和平台

实施逆向工程需要各种各样的工具。本书通篇介绍和讨论了大量这样的工具，而且我有意地在大部分范例中使用免费工具，这样读者就可以照着范例实践而不需要在工具上花

Broadview®
www.broadview.com.cn

《Reversing：逆向工程揭密》读者调查表

尊敬的读者：

感谢您对我们的支持与爱护。为了今后为您提供更优秀的图书，请您抽出宝贵的时间将您的意见以下表的方式及时告知我们（可另附页）。我们将从中评选出热心读者若干名，免费赠阅我们以后出版的图书。

姓名：	性别：☐ 男 ☐ 女	年龄：	职业：
通信地址：			邮政编码：
电话：	传真：	E-mail：	

1. 影响您购买本书的因素（可多选）：

☐ 封面封底　☐ 价格　☐ 内容提要、前言和目录　☐ 书评广告　☐ 出版物名声
☐ 作者名声　☐ 正文内容　☐ 其他_____

2. 您对本书的满意度：

从技术角度　☐ 很满意　☐ 比较满意　☐ 一般　☐ 较不满意　☐ 不满意
☐ 改进意见_____

从文字角度　☐ 很满意　☐ 比较满意　☐ 一般　☐ 较不满意　☐ 不满意
☐ 改进意见_____

从版面、封面设计角度　☐ 很满意　☐ 比较满意　☐ 一般　☐ 较不满意
☐ 不满意　☐ 改进意见_____

3. 您最喜欢书中的哪篇（或章、节）？请说明理由。

_____

_____

4. 您最不喜欢书中的哪篇（或章、节）？请说明理由。

_____

_____

5. 您希望本书在哪些方面进行改进？

_____

_____

6. 您感兴趣或希望增加的图书选题有：

_____

_____

通信地址：北京万寿路 173 信箱　博文视点（100036）　电话：010-51260888

如果您对我们出版的图书有任何意见和建议，也可以发邮件给我们，我们将及时回复。

E-mail：jsj@phei.com.cn，editor@broadview.com.cn

反侵权盗版声明

目　录

第 1 部分　逆向 101

第 2 部分 应用逆向