TURING 图灵程序设计丛书

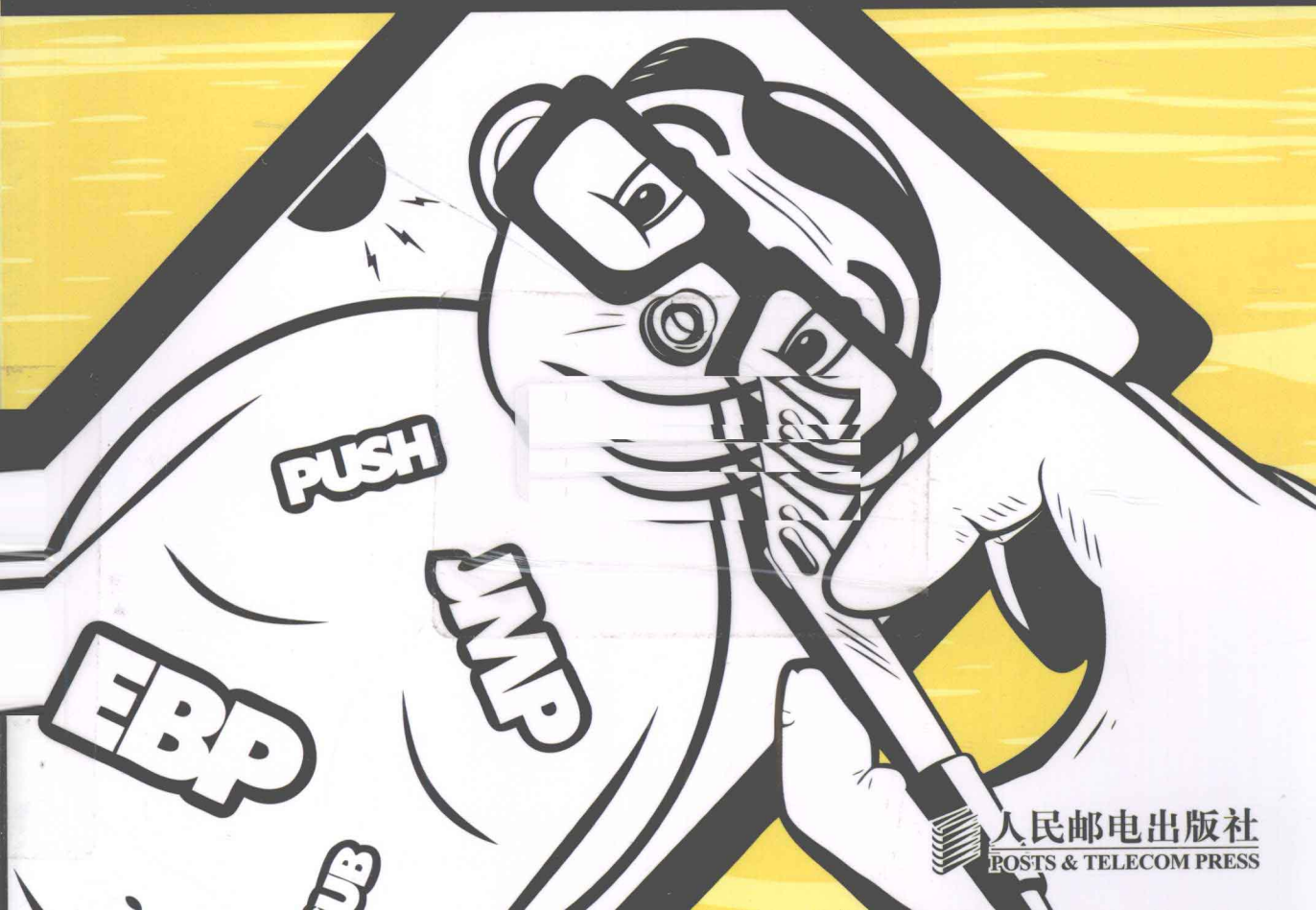
no starch press

The IDA Pro Book

The Unofficial Guide to the World's Most Popular Disassembler Second Edition

IDA Pro权威指南（第2版）

[美] Chris Eagle 著
石华耀 段桂菊 译



人民邮电出版社
POSTS & TELECOM PRESS

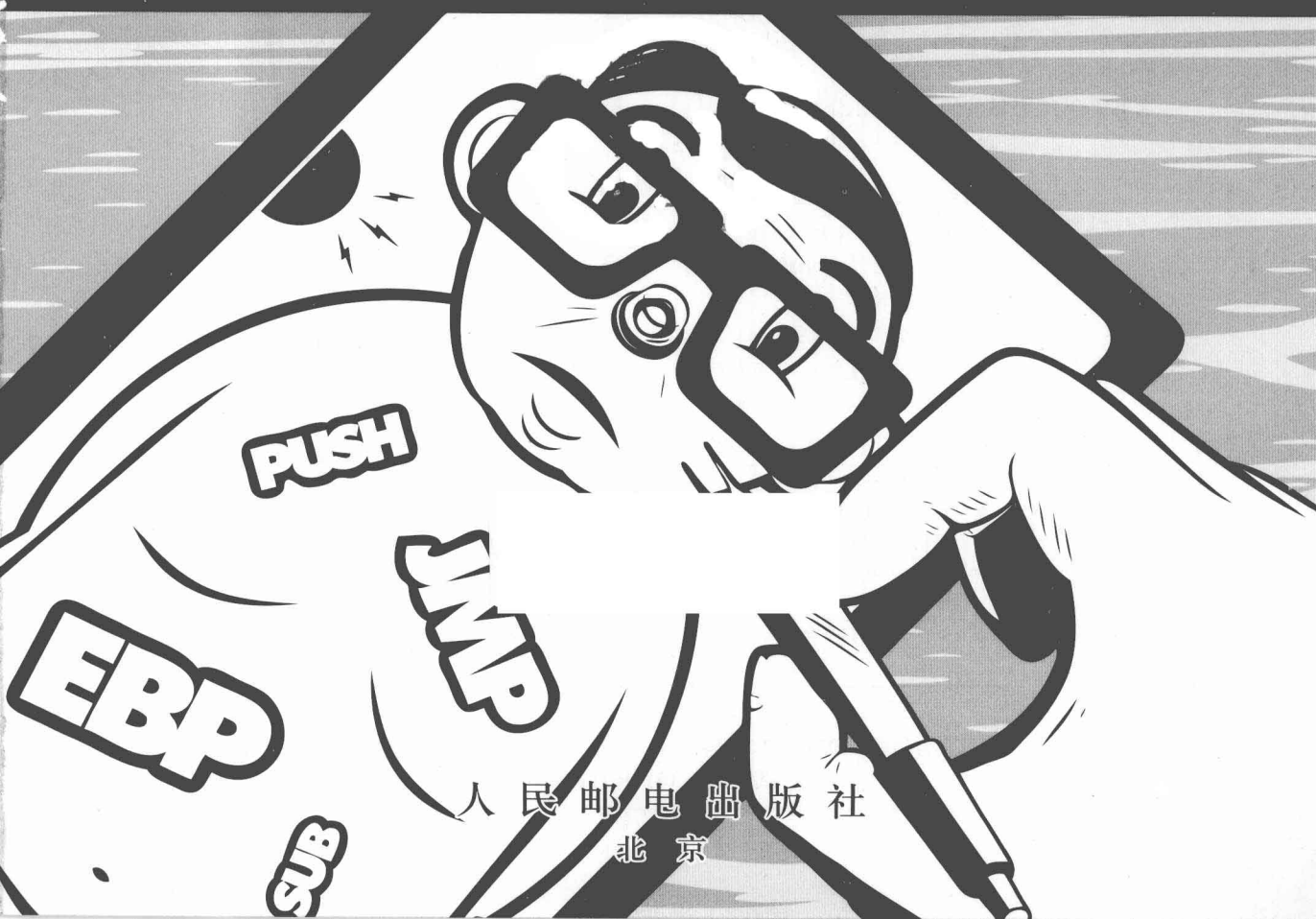
TURING 图灵程序设计丛书

The IDA Pro Book

The Unofficial Guide to the World's Most Popular Disassembler Second Edition

IDA Pro权威指南（第2版）

[美] Chris Eagle 著
石华耀 段桂菊 译



人民邮电出版社
北京

图书在版编目（CIP）数据

IDA Pro权威指南 /（美）伊格尔（Eagle,C.）著；石华耀，段桂菊译. -- 2版. -- 北京 : 人民邮电出版社，2012.2
（图灵程序设计丛书）
书名原文：The IDA Pro Book : The Unofficial Guide to the World's Most Popular Disassembler Second Edition
ISBN 978-7-115-27368-0

Ⅰ. ①I… Ⅱ. ①伊… ②石… ③段… Ⅲ. ①反汇编程序 Ⅳ. ①TP313

中国版本图书馆CIP数据核字(2012)第004334号

内 容 提 要

本书共分为六部分，首先介绍了反汇编与逆向工程的基本信息和IDA Pro的背景知识，接着讨论了IDA Pro的基本用法和高级用法，然后讲解了其高扩展性及其在安全领域的实际应用，最后介绍了IDA的内置调试器（包括Bochs调试器），一方面让用户对IDA Pro有全面深入的了解，另一方面让读者掌握IDA Pro在现实中的应用。相比上一版，这一版以IDA6.0为基础，介绍了它的新的、基于Qt的图形用户界面，以及IDAPython插件。

本书适合IT领域的所有安全工作者阅读。

图灵程序设计丛书

IDA Pro权威指南（第2版）

◆ 著 [美] Chris Eagle
译 石华耀 段桂菊
责任编辑 王军花
执行编辑 丁晓昀

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：31.75
字数：750千字 2012年2月第2版
印数：4 801－7 800册 2012年2月北京第1次印刷

著作权合同登记号 图字：01-2011-7808号

ISBN 978-7-115-27368-0

定价：89.00元

读者服务热线：(010)51095186转604 印装质量热线：(010)67129223
反盗版热线：(010)67171154

版权声明

谨以此书献给我的母亲。

对上一版的赞誉

“我衷心地向所有IDA Pro用户推荐《IDA Pro权威指南》一书。”

——Ilfak Guilfanov，IDA Pro的开发者

“本书内容精练而且结构合理……包括逐步深入的示例以及IDA各个方面所必需的详细信息，是你学习IDA的最佳选择。”

——Cody Pierce，TippingPoint DVLabs

“Chris Eagle无疑是一名杰出的教育工作者，因为他能够使深奥晦涩的技术材料变得简单易懂，并且总是能够提供适当的示例。”

——Dino Dai Zovi，Trail of Bits博客

“本书不仅能够帮助你全面了解IDA Pro，而且能够帮助你了解整个PE流程。”

——Ryan Linn，*The Ethicai Hacker Network*

“本书内容翔实，信息全面!”

——Eric Hulse，Carnal0wnage博客

“迄今为止最全面、最准确、最优秀的IDA Pro著作。”

——Pierre Vandevenne，DataRescue SA股东兼CEO

“无论是IDA Pro的初学者还是经验丰富的使用者，我强烈建议你们阅读本书。”

——Dustin D. Trammell，安全研究员

“我强烈建议大家购买本书。它结构合理，而且据我所知，它比任何其他文档（包括IDA Pro手册）都更加全面。”

——Sebastian Porst，微软高级软件安全工程师

“无论是处理严重的运行时缺陷，还是由内而外地检查应用程序的安全，IDA Pro都是你的首选工具，而本书则是你尽快学习IDA Pro的指南。”

——Joe Stagner，微软程序经理

致　谢

和第1版一样，我想感谢家人在我撰写本书时给予我的支持。我对他们的忍耐和宽容深表感谢。

我还要感谢那些推动第1版取得成功的人们，特别是广大的读者们，希望我的著作能够为他们学习逆向工程提供帮助。没有他们的支持和建议，我不可能撰写第2版。

我要再次感谢技术编辑Tim Vidas，感谢他努力工作，还要感谢他的妻子Sheila对我们工作的支持。

我还要感谢Hex-Rays的开发人员，不仅感谢他们开发出优秀的产品，而且谢谢他们容忍我那“漏洞百出”的报告，事实证明，其中许多报告都是错误警报。感谢Ilfak投入大量时间，感谢Elias、Igor和Daniel提供的深刻见解。正是因为他们的努力，才使IDA成为我最喜爱的软件。

最后，我要感谢Alison Law及No Starch出版社的所有工作人员，他们的辛苦劳动使得本书得以顺利出版。

前　言

撰写一本关于IDA Pro的书是一个充满挑战的任务。事实上，IDA是一款非常复杂的软件，它的功能特别强大，要在一本书中详细介绍所有这些功能，几乎是一项无法完成的任务。而且，IDA一直在不断推出新版本，因此，任何介绍IDA的图书在出版时都会落后一两个版本。在本书第1版即将出版时，IDA发布了版本5.3，但自本书第1版出版以来，IDA已发布了7个新版本（包括版本5.3）。IDA 6.0采用了一个新的、基于Qt[①]的图形用户界面，这促使我对本书进行更新，以介绍许多第1版并未介绍的功能。当然，和往常一样，IDA的另一个版本（6.1）也即将发布，[②]这确实让人非常兴奋。

我撰写这一版的目的是帮助更多用户了解IDA，并培养他们对逆向工程的兴趣（如果可能）。对于希望进入逆向工程领域的读者，我希望向你们强调掌握熟练的编程技巧的重要性。理想情况下，你们应热爱编程，甚至要时时刻刻都想着编程。如果你对编程感到畏惧，那么逆向工程可能并不适合你。你可能会认为，逆向工程根本不需要编程，因为这只需要分解其他人的程序，但如果无法开发出能帮助你自动完成各种任务的脚本和插件，你永远也不可能成为真正高效的逆向工程人员。对我而言，编程和逆向工程就像是《纽约时报》周日版的纵横字谜游戏，对此我乐在其中。

为保持一致性，这个版本保留了第1版的总体结构，并且更为详细地阐述了部分章节，同时增加了一些新内容。阅读本书的方式多种多样。对逆向工程知之甚少的用户可以从第1章和第2章开始，了解有关逆向工程和反汇编器的一些信息；对IDA了解不多、希望深入学习的读者可以从第3章开始，这一章主要介绍IDA的基本布局；第4章则描述如何启动IDA并加载文件进行分析；第5章到第7章介绍IDA的用户界面窗口和基本功能。

对IDA有一定了解的读者可以从第8章开始阅读，这一章讨论如何使用IDA处理复杂的数据结构，包括C++类；而第9章则介绍IDA交叉引用，它是IDA基于图形的显示（也在第9章介绍）的基础；第10章说明如何在非Windows平台上（Linux或OS X）运行IDA。

更加高级的IDA用户可能会发现，第11章到第14章是不错的起点，主要介绍IDA的高级用法及其配套工具。第11章简要说明IDA的一些配置选项；第12章描述IDA的FLIRT/FLAIR技术和相关工具，我们利用它们开发签名，并利用这些签名将库代码与应用程序代码区分开来；第13章讨论IDA类型库及如何扩展类型库；而第14章则回答一些常见的问题，说明IDA是否可用于修补二进制文件。

---

① Qt是诺基亚开发的一个跨平台的C++图形用户界面应用程序框架。——译者注

② 2011年4月发布了IDA 6.1，2011年10月发布了IDA 6.2。——编者注

IDA是一款即装即用的强大工具，可扩展性是它最大的优点之一，这些年来，用户利用这一优点让IDA完成了一些非常有趣的任务。IDA的可扩展性在第15章到第19章讨论。第15章介绍IDA的脚本功能（新增了IDAPython），并系统讨论IDA的SDK（软件开发工具包）提供的编程API；第16章全面介绍SDK；而第17章到第19章则讨论插件、文件加载器和处理器模块。

介绍完IDA的全部功能后，第20章至第23章转而讨论IDA在逆向工程方面更加实际的用法，分析各种编译器的区别（第20章），介绍如何使用IDA分析恶意软件中常见的模糊代码（第21章），以及如何利用IDA发现和分析漏洞（第22章）。第23章则介绍这些年来发布的一些有用的IDA扩展（插件）。

最后，第24章至第26章介绍IDA的内置调试器。第24章首先介绍调试器的基本功能；第25章讨论使用调试器分析模糊代码遇到的一些挑战，其中包括处理可能出现的反调试功能所带来的挑战；第26章则讨论IDA的远程调试功能，以及使用Bochs模拟器作为集成的调试平台，以此结束本书的讨论。

写作本书时，IDA的最新版本为6.1，本书在很大程度上以IDA 6.1为介绍对象。Hex-Rays公司非常慷慨，为用户提供了一个免费版本。IDA免费版是IDA 5.0的一个删减了部分功能的版本。本书讨论的大部分IDA功能也适用于免费版本，附录A简要介绍了用户在使用免费版本时可能遇到的一些不同之处。

首先学习IDA脚本功能，然后逐步学习如何创建编译插件，这似乎是一个自然的发展过程。因此，我们在附录B中全面介绍了每一个IDC函数及其对应的SDK操作。有时候，你可以在IDC函数与SDK函数之间建立起一一对应的关系（尽管这些函数的名称并不相同）；而有时候，实现单独一个IDC函数可能需要调用几个SDK函数。附录B回答了这个问题："我知道如何用IDC完成某个任务，但是，如何使用插件完成这个任务呢？"附录B中的信息通过逆向工程IDA内核获得，根据IDA的非传统许可协议，这样做完全合法。

在整本书中，我都尽量使用较短的代码说明问题。绝大多数的示例代码，以及许多用于生成示例的二进制文件，都可以在本书的官方网站上找到，其地址为http://www.idabook.com/。在那里，你还可以找到本书并未包含的一些示例，以及本书所使用的所有参考文献（如脚注中引用的URL的最新链接）。

目　录

第一部分　IDA 简介

第二部分　IDA 基本用法

第四部分 扩展 IDA 的功能

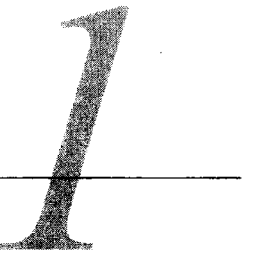
Part 1

第一部分

IDA 简介

本部分内容

第1章 反汇编简介



拿到一本专门介绍 IDA Pro 的书，你很可能急切地想知道书里会讲些什么。很明显，本书以 IDA 为中心，但我并不希望读者将其作为 IDA Pro 用户手册。相反，本书旨在将 IDA 作为推动逆向工程技术讨论的工具。你会发现，在分析各种软件（包括易受攻击的应用程序和恶意软件）时，这些技术非常有用。在适当的时候，我将提供在使用 IDA 时需要遵循的详细步骤，好让你执行与你手头的任务有关的特殊操作。因此，我将简略地介绍 IDA 的功能，包括最初分析文件时需要执行的基本任务，最后讨论 IDA 的高级用法和定制功能（用来解决更具挑战性的逆向工程问题）。我不会介绍 IDA 的所有功能。但是，你将发现，在应对逆向工程挑战时，本书介绍的功能极其有用，这也使得 IDA 成为你工具箱中最强大的武器。

在详细介绍 IDA 之前，了解反汇编过程的一些基础知识，以及其他一些对编译代码进行逆向工程的可用工具，会有一定好处。虽然这些工具的功能都不如 IDA 全面，但它们具备 IDA 的一部分功能，有助于我们了解 IDA 的某些功能。本章的剩余部分主要介绍反汇编过程。

1.1 反汇编理论

任何学过编程语言的人都知道，编程语言分为好几代，下面为那些上课不认真的读者简要总结一下。

- **第一代语言**。这些语言是最低级的语言，一般由 0 和 1 或某些简写编码（如十六进制码）组成。只有二进制超人才能读懂它们。由于数据和指令看起来都差不多，人们往往很难将它们区分开来，因此这种语言很容易造成混淆。第一代语言也称为*机器语言*，有时也叫做*字节码*，而机器语言程序常被称为*二进制文件*。
- **第二代语言**。第二代语言也叫*汇编语言*，它只是一种脱离了机器语言的表查找方式。通常，汇编语言会将具体的位模式或操作码，与短小且易于记忆的字符序列（即*助记符*）对应起来。有时候，这些助记符确实有助于程序员记住与它们有关的指令。*汇编器*是程序员用来将汇编语言程序转换成能够执行的机器语言的工具。
- **第三代语言**。这些语言引入了关键字和结构（它们是程序的构建块），因而其表达能力更接近于自然语言。通常，第三代语言不依赖于任何平台。但是，由于用第三代语言编写的程序使用了特定于操作系统的独特功能，它们便具有了平台依赖性。常见的第三代语