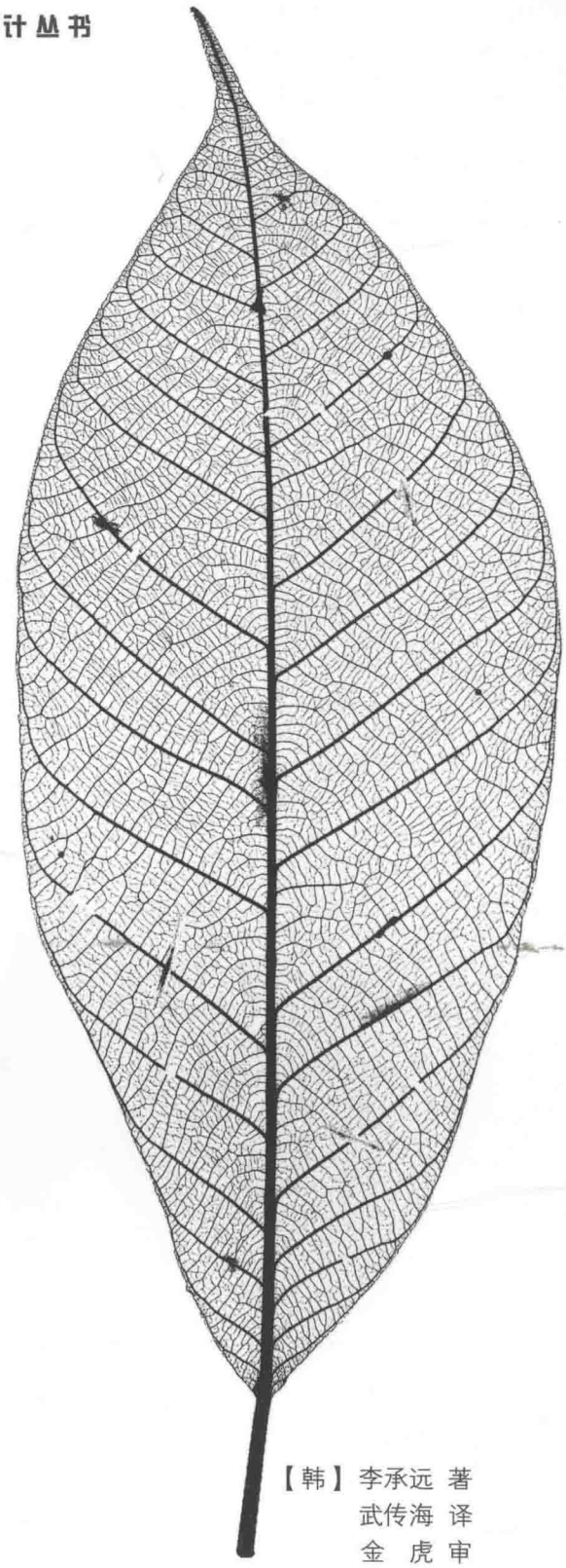
TURING 图灵程序设计丛书

인사이트 insight

逆向工程核心原理

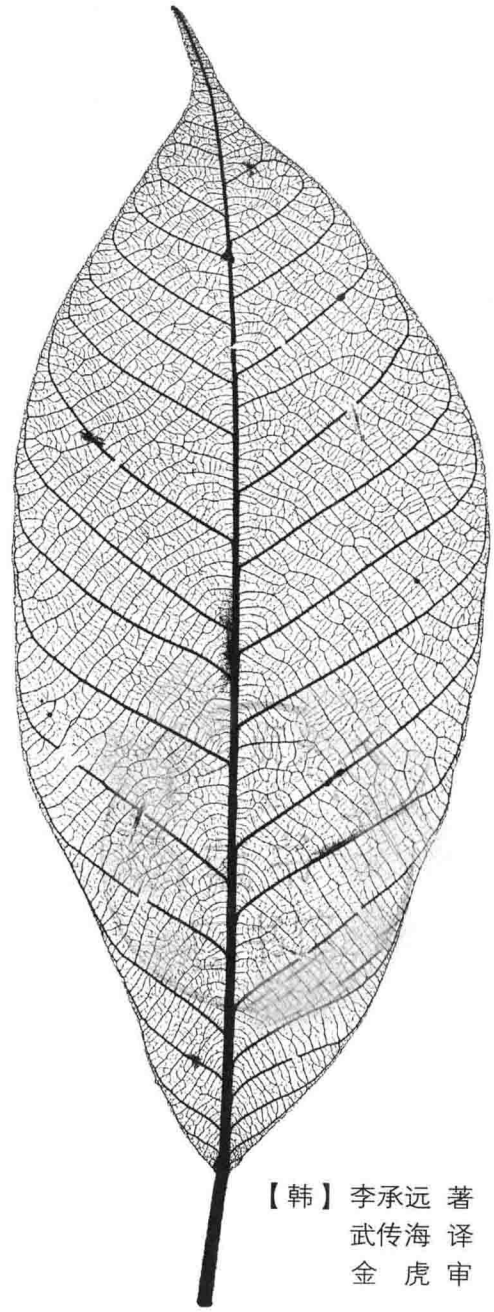


【韩】李承远 著
武传海 译
金 虎 审

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

逆向工程核心原理



【韩】李承远 著
武传海 译
金 虎 审

人民邮电出版社
北 京

图书在版编目（CIP）数据

逆向工程核心原理 /（韩）李承远著 ；武传海译.
-- 北京 ：人民邮电出版社，2014.5
（图灵程序设计丛书）
ISBN 978-7-115-35018-3

Ⅰ. ①逆… Ⅱ. ①李… ②武… Ⅲ. ①软件工程
Ⅳ. ①TP311.5

中国版本图书馆CIP数据核字(2014)第049919号

内 容 提 要

本书十分详尽地介绍了代码逆向分析的核心原理。作者在 Ahnlab 研究所工作多年，书中不仅包括其以此经验为基础亲自编写的大量代码，还包含了逆向工程研究人员必须了解的各种技术和技巧。彻底理解并切实掌握逆向工程这门技术，就能在众多 IT 相关领域进行拓展运用，这本书就是通向逆向工程大门的捷径。

想成为逆向工程研究员的读者或正在从事逆向开发工作的开发人员一定会通过本书获得很大帮助。同时，想成为安全领域专家的人也可从本书轻松起步。

◆ 著　[韩] 李承远
译　武传海
审　金　虎
责任编辑　傅志红
执行编辑　陈　曦
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路11号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：43.75
字数：1 202千字　2014年5月第1版
印数：1－4 000册　2014年5月河北第1次印刷
著作权合同登记号　图字：01-2013-8251 号

定价：109.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第 0021 号

推 荐 语

向安全技术专家迈出第一步的必选书！

最近，越来越多的人开始关心信息技术安全，但是相关领域的安全技术专家仍然十分匮乏。主要有两方面原因导致这种现象形成：一方面是因为必须做大量准备，努力学习；另一方面是因为市面上缺乏系统讲解这类内容的专业书籍。

信息技术安全领域的图书很少有讲解恶意代码分析的，本书恰好填补了这一空白。无论是刚开始学习恶意代码分析的朋友，还是从事恶意代码分析的专家，都会为本书面世而激动。

虽然读者阅读本书时需要具有基本的汇编语言知识，但是本书内容讲解非常细致，涵盖了从恶意代码分析基础知识到高级技术的全部内容，系统而有条理，语言简洁，通俗易懂，并在讲解中选配了恰当的示例程序，使内容更易理解。对于最近出现的恶意代码中的各种常用技术，本书都做了详细讲解，无论你是初学者还是分析专家，都能从中获益。

信息安全技术涉及各领域，需要知识渊博、经验丰富的专家。本书将帮你轻松迈出成为安全技术专家的第一步。

——韩昌奎，ASEC 中心主任

如果此刻你手上正捧着这本书，说明你已经被代码逆向分析的魅力深深吸引了！

对于刚开始学习代码逆向分析技术的人而言，需要学习的内容很多，这容易让人心生畏惧、止步不前。其实不需担心，本书在学习过程中给出了大量提示，各位借助这些提示可以更好地理解所讲的内容。

本书比较重视代码逆向分析者的心态引导与培养，在内容讲解上也与其他书籍不同，并不是单纯的技巧罗列，而是深刻讲解了相关技术的深层含义、技术的工作原理以及内部实现结构，这也是本书的重点所在。同时配合丰富示例，让内容变得更具体形象、更易理解，作者的良苦用心可见一斑。

你想成为代码逆向分析员吗？如果你感到困惑："我是开发人员，难道也需要读它吗？"不妨试试，它将成为你最好的同伴。

——郑官真，CISCO 高级研究员

前　言

本书将指引你进入美妙又刺激的代码逆向分析世界，开启一段神奇之旅！

软件逆向工程（代码逆向分析）是一种探究应用程序内部组成结构及工作原理的技术。欢迎各位来到代码逆向分析世界，经历各种神奇的冒险，迎接各种富有趣味的挑战。

不论是我们自己编写的程序，还是其他人编写的无源码程序，只要运用逆向分析技术，我们就能轻松窥探程序内部结构、掌握工作原理。灵活运用逆向分析技术可以在程序的开发与测试阶段发现 Bug 和漏洞，并直接修改程序文件或内存解决这些隐含的问题。而且，我们还可以借助逆向分析技术为程序添加新功能，使程序更强大。这就像是一种魔法，魅力无限。

学习逆向分析技术前并不需要准备太多。下面给各位讲讲我的经历。几年来，我一直维护着一个逆向分析技术学习博客，访客们问得最多的问题是："究竟该怎样学习逆向分析技术？"我结合自身经验并分析了一些学习失败的案例后发现，失败的最大原因并不是学习本身的难度与要学内容的数量，而是对学习逆向技术的恐惧与忧虑——"我连 C 语言还不懂呢"、"一定要掌握汇编语言吗"、"OS 架构我还没搞明白"、"不知道怎么用调试器"、"学完这么多内容才能真正开始学逆向分析技术啊"，以上这些担心正是迫使学习者们中途放弃的主要原因。其实，学习逆向分析技术与学习 C 语言、汇编语言、OS 架构、调试器用法等内容是一样的。将这些内容全部掌握的人已经是专家了，当然不需要这个入门过程。

你仍对逆向分析技术一无所知？没关系，不必沮丧，这反而是件好事。因为你会在以后的学习过程中学到很多东西，会变得更聪明、更有价值，谁说这不是件好事呢？

如果你梦想成为逆向分析工程师，但不知如何入门；如果你是一名程序开发者，又对逆向分析技术非常感兴趣，那么本书将非常适合阅读。学习逆向分析技术并不像公式一样背下来就可以了，死记硬背的结果是你会不知道如何灵活运用。学习某些知识技术时，不仅要掌握其本身，还要知道它们的内部机制与工作原理，既知其然又知其所以然，这才是最重要的。所以，本书讲解相关知识与技术时，将讲解重点放在对其工作原理的分析与说明上，这将更有利于各位真正掌握它们。为什么本书非常适合作为逆向分析技术的入门书呢？以下是我的几点理由。

第一，开发与分析的经验。一名逆向分析工程师不仅要具备专业的逆向分析技术，还要具有一定的程序开发能力。我以前从事网络应用程序开发，后来开始做恶意代码分析工作，慢慢就对逆向分析技术熟悉起来。可以说，我是从程序开发者转变为逆向分析员的为数不多的人之一。程序开发与逆向分析这两项技术相辅相成、互为补充、共同发展，形成相得益彰的效果。日常工作中，它们就像一双翅膀应用于各类业务。分析程序时，人们自然就会从程序开发与逆向分析这两个角度着手。书中用到的几乎所有示例都基于我在逆向分析实践中获得的知识与经验，是我亲自

开发的程序，紧扣各章主题，绝无累赘。

第二，培训与演讲的经验。我在公司慢慢有了资历，随之而来的培训、研讨会、演讲也逐渐多起来。我进行逆向分析技术培训时，面对的学员大都是初学者，这些机会非常有利于我了解他们遇到的困难与想知道的东西。所以，我一直在用心思考，如何用更易理解的方式传授要讲解的知识，这样就慢慢形成了自己特有的讲解技巧与风格。编写本书时，我又将这些培训经验应用到本书的组织结构、内容讲解、示例选择等各方面，以求将较为难懂的技术以更易懂的方式呈现给各位。

第三，丰富的沟通经验。我几年前就开设了一个逆向技术学习博客并运营至今。刚开始的想法非常简单，就是想归纳整理自己学到的逆向分析技术。后来访客越来越多，留下的问题也多起来。我感到很惊讶，之前一直以为韩国是逆向分析技术的“不毛之地”，结果关注逆向分析技术的人比我想得要多，并且他们关注的范围也非常广泛。这大大拓宽了我的视野，于是我开始访问其他逆向分析技术学习博客，接触到了更多文章与问题，慢慢了解了他们关注的部分。我在此过程中逐渐认识到，初学者们想知道的是逆向分析技术的系统的学习方法。他们入门之后迫切要学习的是专业的逆向分析技术与内部工作原理。有感于此，我就萌生了写一本系统学习逆向分析技术书的想法，就这样，在逆向分析与开发、培训、演讲、交流等经验基础上，这本逆向分析技术学习入门书诞生了。

那么，读者应该如何使用本书学习逆向分析技术呢？对此，我给出如下几点建议，供各位参考。

第一，技术书不是装饰书架的道具，它们是提高各位技术水平的工具。所以阅读时要勾画出重要部分，在书页空白处写下自己的想法与心得等。阅读时，在书页上记录相关技术、注意事项、技术优缺点、与作者的不同见解等，让它成为只属于你的书。读完这样一本逆向分析技术书后，不知不觉间就构建出自己独特的逆向分析世界，最终成为代码逆向分析专家。

第二，拥有积极乐观的心态。逆向分析是一项深奥的技术，会涉及 OS 底层知识。要学的内容很多，并且大部分内容需要亲自测试并确认才能最终理解。必须用积极乐观的心态对待这一过程，学习逆向技术无关聪明与否，只跟投入时间的多少有关。学习时，不要太急躁，请保持轻松的心态。

第三，不断挑战。逆向分析不尽如人意时，不要停下来，要尝试其他方法，不断挑战。要相信一定会有解决的方法，可能几年前早已有人成功过了。搜索相关资料并不断尝试，不仅能提高自身技术水平，解决问题后，心里还能感受到一种成就感。这样的成功经验一点点积累起来，自信心就会大大增强，自身的逆向分析水平也会得到明显提高。这种从经验中获得的自信会不知不觉地对逆向分析过程产生积极影响，让逆向分析往更好的方向发展。

希望本书能够帮助各位把“心愿表”上的愿望一一实现，也希望各位把本书讲解的知识、技术广泛应用到逆向分析过程中，发挥更大的作用。谢谢。

感谢

动笔容易写完难。我只身一人是无法完成本书的，写作过程中得到了很多人的关心、支持与

鼓励，没有他们就不会有本书。借此机会，我向所有给予帮助的人表示最诚挚的谢意。

首先，感谢爱妻素英，谢谢你一直以来相信我、默默支持我，你的微笑是我的能量之源。还要感谢我的两个宝贝儿子浩俊、姜宪，你们的陪伴让疲劳烟消云散，让我心里始终充满幸福。还有我的父母，你们总是关心着我和我的工作。正是你们给了我战胜一切困难的勇气，衷心感谢你们。

其次，要感谢崔景哲先生，您的称赞与鼓励一直激励着我写完全书。还要感谢韩昌圭先生与郑宽镇先生，两位前辈写的推荐词使本书增色不少。我早在动笔时就嘱托二位为本书写推荐语了。请一定允许我为两位的新书写推荐词。

再次，向 Insight 出版社的韩基晟社长以及所有员工，特别是赵岩熹编辑表示最诚挚的谢意。他将一块粗糙的原石打磨成了珍贵的宝石，我以后写书也会无条件请他负责。

最后，对关注本书的同事、公司实习生，以及博客访客们表示感谢。你们总是热心地询问："什么时候出书啊？"你们的关心最终促成我写完全书。还要感谢购买本书的读者们，你们的梦想与热情一直鼓舞着我。

李承远
www.reversecore.com
reverscore@gmail.com

目　录

第一部分　代码逆向技术基础

第四部分　API 钩取