TURING
图灵程序设计丛书

打开黑箱，感受底层世界的乐趣

- 如何防止软件被别人分析?
- 如何知道软件在运行时都干了什么?
- 如何防止攻击者利用漏洞夺取系统权限?

有趣的二进制

软件安全与逆向分析

[日] 爱甲健二 / 著　周自恒 / 译

中国工信出版集团　人民邮电出版社 POSTS & TELECOM PRESS

TURING
图灵程序
设计丛书

有趣的二进制

软件安全与逆向分析

[日] 爱甲健二 / 著　周自恒 / 译

人民邮电出版社
北　京

图书在版编目（CIP）数据

有趣的二进制：软件安全与逆向分析 /（日）爱甲健二著；周自恒译. -- 北京：人民邮电出版社，2015.10

（图灵程序设计丛书）

ISBN 978-7-115-40399-5

Ⅰ. ①有… Ⅱ. ①爱… ②周… Ⅲ. ①二进制运算 ②软件开发－安全技术 Ⅳ. ①TP301.6 ②TP311.52

中国版本图书馆CIP数据核字（2015）第227832号

内 容 提 要

本书通过逆向工程，揭开人们熟知的软件背后的机器语言的秘密，并教给读者读懂这些二进制代码的方法。理解了这些方法，技术人员就能有效地 Debug，防止软件受到恶意攻击和反编译。本书涵盖的技术包括：汇编与反汇编、调试与反调试、缓冲区溢出攻击与底层安全、钩子与注入、Metasploit 等安全工具。

本书适合对计算机原理、底层或计算机安全感兴趣的读者阅读。

◆ 著　　[日]爱甲健二
译　　周自恒
责任编辑　乐　馨
执行编辑　杜晓静
责任印制　杨林杰

◆ 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
北京隆昌伟业印刷有限公司印刷

◆ 开本：880×1230　1/32
印张：8.5
字数：260千字　　2015年10月第1版
印数：1-4 000册　　2015年10月北京第1次印刷

著作权合同登记号　图字：01-2014-4972号

定价：39.00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

译者序

这是一本讲“底层”知识的书，不过似乎现在大部分计算机用户都跟底层没多少缘分了。很多人说，写汇编语言的时候总得操心寄存器，写C语言的时候总得操心内存，而如今到了Web当道的时代，不但底层的事情完全用不着操心了，就连应用层的事情也有大把的框架来替你搞定。想想看，现在连大多数程序员都不怎么关心底层了，更不要说数量更多的一般用户了。当然，这其实是一件好事，这说明技术进步了，分工细化了，只需要一小部分人去研究底层，剩下大部分人都可以享受他们的伟大成果，把精力集中在距离解决实际问题更近的地方，这样才能解放出更多的生产力。

话说回来，底层到底指的是什么呢？现代数字计算机自问世以来已经过了将近60年，在这60年中，计算机的制造技术、性能、外观等都发生了翻天覆地的变化，然而其基本原理和结构依然还是1946年冯·诺依曼大神所描绘的那一套。冯·诺依曼结构的精髓在于，处理器按照顺序执行指令和操作数据，而无论指令还是数据，它们的本质并没有区别，都是一串二进制数字的序列。换句话说，“二进制”就是现代计算机的最底层。我们现在用计算机上网、聊天、看视频、玩游戏，根本不会去考虑二进制层面的问题，不过较早接触计算机的一代人，其实都曾经离底层很近，像这本书里面所讲的调试器、反汇编器、二进制编辑器、内存编辑器等，当初可都是必备的法宝，也给我们这一代人带来过很多乐趣。

在MS-DOS时代，很多人都用过一个叫debug的命令，这就是一个非常典型的调试器。准确地说，debug的功能已经超出了调试器的范畴，

除了调试之外，它还能够进行汇编、反汇编、内存转储，甚至直接修改磁盘扇区，俨然是那个年代的一把“瑞士军刀”。我上初中的时候，学校上计算机课用的电脑在BIOS里禁用了软驱，而且还设置了BIOS密码，于是我运行debug，写几条汇编指令，调用系统中断强行抹掉CMOS数据，重启之后显示CMOS数据异常，于是BIOS设置被恢复到默认状态，软驱也就可以用了，小伙伴们终于可以把游戏带来玩了。当然，学校老师后来还是找到我谈话，原因仅仅是因为我在信息学奥赛得过奖，他们觉得除了我以外不可能有别人干得出这种事了……

很多资历比较老的PC游戏玩家其实也都和二进制打过交道，比如说，大家应该还记得一个叫“整人专家FPE”的软件。如果你曾经用过“整人专家”，那么这本书第2章中讲的那个修改游戏得分的桥段你一定是再熟悉不过了。除了修改内存中的数据，很多玩家应该也用二进制编辑器修改过游戏存档，比如当年的《金庸群侠传》《仙剑奇侠传》，改金钱道具能力值那还是初级技巧，还有一些高级技巧，比如改各种游戏中的flag，这样错过开启隐藏分支的条件也不怕不怕啦。此外，各种破解游戏激活策略的补丁也是通过调试和反汇编研究出来的，我也曾经用SoftICE玩过一点逆向工程，找到判断是否注册激活的逻辑，然后用一个无条件跳转替换它，或者是跳过序列号的校验逻辑，不管输入什么序列号都能激活。

精通二进制的人还懂得如何压榨出每一个比特的能量。说到这一点，不得不提鼎鼎大名的64k-intro大赛。所谓64k-intro，就是指用一段程序来产生包含图像和声音的演示动画，而这段程序（可执行文件）的大小被限制为64KB（65536字节）。想想看，用iPhone随便拍一张照片就得差不多2MB大小，相当于64KB的32倍，然而大神们却能在64KB的空间里塞下长达十几分钟的3D动画和音乐，着实令人惊叹不已。我第一次看到64k-intro作品是在上初中的时候，当时某一期《大众软件》杂志对此做了介绍，光盘里还附带了相应的程序文件。当我在自己的电脑上亲自运行，看到美轮美奂的3D动画时，瞬间就被二进制的

奇妙感动了。

二进制的乐趣不胜枚举，其实最大的乐趣莫过于“打开黑箱”所带来的那种抽丝剥茧的快感。夸张点说，这和物理学家们探求“大统一理论”，不断逼近宇宙终极规律的过程中所体验到的那种快感颇有异曲同工之妙。诚然，二进制的可能性是无穷无尽的，这本书所涉及的也只是其中很小的一方面，但正如作者在前言中所说的那样，希望大家能够借此体会到底层技术所特有的快乐。*烫烫*

周自恒

2015 年 8 月于上海

免责声明

本书的内容以提供信息为目的，在使用本书的过程中，读者需要自己做出判断并承担相应的责任。对于读者因使用本书中的信息所造成的任何后果，作者、技术评论社、译者、人民邮电出版社恕不负责。

本书中的内容基于2013年7月12日的最新信息编写，在读者实际阅读时可能已经发生变化。

此外，软件方面由于其版本的更新，可能会与本书中所描述的功能和画面存在差异。在购买本书之前，请务必确认您所使用的软件版本。

各位读者在阅读本书之前，请同意并遵守上述注意事项。如果没有阅读上述事项，那么对于由此产生的问题，出版社和作译者可能也无法解决，敬请各位读者理解。

关于商标和注册商标

本书中所涉及的产品名称，一般皆为相应公司的商标或者注册商标，在本书正文中已省略™、® 等标记。

前言

如今，计算机已经深入千家万户，为我们的生活带来了很多方便。但与此同时，计算机系统也变得越来越复杂，技术人员需要学习的知识也与日俱增。和过去相比，计算机技术中难以理解的黑箱也越来越多了。

- **操作系统到底是干什么的？**
- **CPU 和内存到底是干什么的？**
- **软件为什么能够运行？**
- **为什么会存在安全漏洞？**
- **为什么攻击者能够运行任意代码？**

要想回答上面这些问题，我们需要用到以汇编为代表的二进制层面的知识。

尽管现在正是 Web 应用如日中天的时候，但二进制层面的知识依然能够在关键时刻发挥作用。例如：

“用 C/C++ 开发的程序出现了不明原因的 bug，看了源代码还是找不到原因。”

在这样的情况下，即便不会编写汇编代码，只要能看懂一些汇编语言，就可以通过调试器立刻锁定发生 bug 的位置，迅速应对。

此外，如果别人编写的库里有 bug，那么即便看不到源代码，我们也能够对其内部结构进行分析，并找到避开问题的方法，也可以为库的开发者提供更有帮助的信息。

再举个例子。学习汇编能够更好地理解 CPU 的工作原理，从而能

够处理系统内核、驱动程序这一类近乎于黑箱的底层问题，对于实际的底层开发工作也非常有帮助。

不过，说实在的，“有没有帮助”“流不流行”这些都不重要，从个人经验来看，因为感觉“好像有用”“好像有帮助”而开始学习的东西，最后基本上都没有真正掌握（笑）。当然，也许是因为我天资愚钝，不过我们在上学的时候，老师天天教导我们要好好学习，可是实际上有几个人真的好好学习了呢？虽然我没做过统计，但从感觉来看，整个日本也许还不到 1% 吧。

那么问题来了，要想真正学会一件事，到底需要什么呢？

我是从初中时代开始学习编程的，尽管当时完全没有想过将来要当程序员，靠技术吃饭，但我依然痴迷于计算机，每天编程到深更半夜，甚至影响了学习成绩，令父母担忧。

为什么当时的我如此痴迷于计算机而无法自拔呢？那是因为“编程太有趣了”。自己编写的代码能够按照设想运行起来，或者是没有按照设想运行起来，再去查找原因，这些事情都为我带来了莫大的乐趣。

我编写这本书，也是为了让大家对技术感到“有趣”，并且“想了解得更多”。而在编写这本书的过程中，我再一次感到，在不计其数的编程语言中，汇编语言是最“有趣”的一种。

如果你突然觉得“讲底层问题的书好像挺有意思的”而买了这本书，那么我相信，这本书一定能够为你带来超出预期的价值。

希望大家能够通过这本书，感受到二进制世界的乐趣。

目录

第1章
通过逆向工程学习如何读懂二进制代码