TURING 图灵原创

丰生强
邢俊杰 著

macOS 软件安全与逆向分析

macOS软件安全第一书

软件开发与安全人员案头必备的技术专著

全面分析macOS系统中最新的软件安全、逆向分析与加密解密技术

包含信息安全领域一线软件安全专家的多年实战经验，干货满满

获BAT、360等众多互联网公司一线软件安全专家一致认可和推荐

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

macOS 软件安全与逆向分析

丰生强　邢俊杰 | 著

人民邮电出版社

北京

图书在版编目（CIP）数据

macOS软件安全与逆向分析 / 丰生强，邢俊杰著. -- 北京 : 人民邮电出版社，2017.7
（图灵原创）
ISBN 978-7-115-46063-9

Ⅰ. ①m… Ⅱ. ①丰… ②邢… Ⅲ. ①软件开发－安全技术 Ⅳ. ①TP311.52

中国版本图书馆CIP数据核字(2017)第147374号

内 容 提 要

本书深入介绍 macOS 系统的软件安全、逆向分析与加密解密技术，主要包括 macOS 软件的开发基础、macOS 系统工作机制、macOS 软件调试接口与机制、二进制程序的格式、反汇编技术、逆向与动态调试技术、反破解技术以及系统安全与反病毒。本书包含了信息安全领域一线软件安全专家的多年实战经验，是安全人员与开发人员案头必备的技术专著。

本书适合所有 macOS 平台软件开发工程师、信息安全专业学生、信息安全专业从业人员阅读学习。

◆ 著　　丰生强　邢俊杰
责任编辑　张　霞
责任印制　彭志环
◆ 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
北京鑫正大印刷有限公司印刷
◆ 开本：800×1000　1/16
印张：29.5
字数：697千字　　2017年 7 月第 1 版
印数：1－3 500册　　2017年 7 月北京第 1 次印刷

定价：79.00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：京东工商广登字 20170147 号

丰生强，网名非虫，独立软件安全研究员，资深安全专家，ISC2016安全训练营独立讲师，有着丰富的软件安全实战经验。自2008年起，在知名安全杂志《黑客防线》上发表多篇技术文章，从此踏上软件安全道路，常年混迹于国内各大软件安全论坛。著有畅销安全图书《Android软件安全与逆向分析》。

邢俊杰，资深程序员，软件安全爱好者，C++ Web框架Cinatra开发者，对编译器与调试器开发有着深入的研究。现就职于国内某互联网公司。业余时间喜欢研究软件与系统的底层，热爱读书与动画。

微信连接

回复“安全”查看相关图书

微博连接

关注 @图灵教育每日分享IT好书

QQ连接

图灵读者官方群I：218139230
图灵读者官方群II：164939616

图灵社区
iTuring.cn

在线出版，电子书，《码农》杂志，图灵访谈

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

前　言

对于很多人来说，苹果系统的硬件设备都让人瞩目，尤其是高配置的 Macbook Pro 电脑，无论是在价格上还是在品质上，都是笔记本电脑行业的标杆。2016 年，苹果公司在硬件新品发布会上公开了全新设计带 Touch Bar 的 Macbook Pro，顶配 15 英寸的价格高达 32 888 元，这个价格足以让多数人望而却步。苹果的 macOS 只允许在自家的硬件设备上运行，不过，除了顶配的 Macbook Pro，还有一些入门级的硬件可供选择。在苹果硬件系列中，最便宜的应该是 Mac mini，不过你还得另外买台显示器。算下来，在 macOS 系统上无论是做开发、娱乐还是其他工作，都要比其他操作系统的成本高出不少。这也导致了 macOS 系统的关注度比其他操作系统低。

本书讨论的内容偏偏正是这样一个受众较少的操作系统上软件安全相关的话题，相信读者与我一样，能够感受到这些年 macOS 系统的安全形势与变化。随着苹果系统普及率的提高，安全问题将会慢慢凸显。

本书特点

- 循序渐进的学习路线。从本书开篇起，书中的知识与技术点无一不是由浅入深逐渐展开的。工具的使用与原理的讲解也都符合学习的思维。读者在阅读本书时，几乎不需要频繁切换章节。
- 实例分析。在讲解不同技术点时，为了让读者充分感受技术涉及的应用场景与实际的展示效果，书中会辅以大量实例。每个实例都是笔者精心编写、反复调试过的，并且都是开放源代码的，读者可以通过阅读这些实例的源代码来加深对技术的理解。
- 实用工具讲解。本书提倡读者多动手实践，其中实践的一部分内容就是掌握书中介绍的第三方工具。本书除了系统地介绍一些命令外，还使用到了八十多个第三方工具。这些工具大多是免费与开源的，掌握这些工具的使用，阅读理解它们的代码，了解背后的工作原理，才能更好地让实践与理论相结合。

如何学习本书

本书共 12 章，系统地讲解了软件安全相关的环境搭建、语言基础、文件格式、静态分析、动态调试、破解与防破解、游戏安全、恶意软件等多个主题。其中，环境搭建与语言基础是本书

最低的技术门槛，属于软件开发的范畴。这部分内容主要针对零基础 macOS 开发的读者；如果你从事过 iOS/macOS 软件开发，那么可以跳过。后面每一个技术点都是独立又相辅相成的，虽然可以跳过一些章节进行学习，但不鼓励这么做。

在讲解工具的使用上，对于命令行工具，本书会以终端命令展示与输出结果的形式讲解；对于有界面的 GUI 工具，本书会辅以图示来讲解操作步骤与展示效果。读者在实际动手时，可以按照书中的指引一步步地进行操作。

本书适用人群

本书主要讲解 macOS 平台软件安全相关的技术，在读者的定位上自然是离不开“软件”与“安全”这两个领域的。

软件方面，适合的读者有：

- 软件开发专业的高校学生；
- iOS/macOS 软件开发工程师。

安全方面，适合的读者有：

- 信息安全专业的高校学生；
- 软件汉化人员；
- 软件安全研究员；
- 系统底层开发人员；
- 逆向工程师；
- 病毒分析师。

阅读须知

本书的创作花费了笔者大量的时间与精力，它得以顺利出版，是无数个日日夜夜调试与写作的成果。因此，我不欢迎阅读本书盗版的读者，无论你通过什么渠道，出于什么目的，当你通过阅读盗版书看到这番话时，都是对笔者深深的伤害。

任何一种技术都有它的应用场景，任何一种知识都有更新与迭代期。本书创作时，恰遇 OS X 系统更名为 macOS，系统刚升级至 10.12，因此本书中讲解的工具与技术，是基于这个时期的系统版本，不能保证这些工具与技术在系统日后的版本上依旧能够适用。因此，本书不对日后版本系统上的可行性做任何担保，也不欢迎好事之徒对书中技术的可行性进行无端猜测。

本书是一本工具实践书，讲解了工具的使用与原理以及在实际分析过程中遇到的多数问题，但这并不代表本书能够帮你解决所有的问题。而且单纯通过阅读一本书并不足以完全了解逆向工程这一门深奥的学问。如果读者期待仅仅通过本书就完整地理解系统的安全机制与所有的软件攻

防手法，那么本书可能不适合你。

逆向工程是一门特殊的技术，它就像一把利刃，使用得当可以保护自己，使用不当就会伤害别人。本书中的技术只供用来做技术探讨，不得用于非法商业目的，任何企图通过本书技术从恶的读者，都请好自为之。

实例代码与勘误

本书中的实例代码全部托管到了 GitHub 上，读者可以到 https://github.com/feicong/macbook 页面下载。

本书在图灵社区本书主页和 GitHub 上均开设了勘误页面，如果细心的读者发现了书中的错误，可以提交 issue。

- 图灵社区：http://www.ituring.com.cn/book/1958
- GitHub：https://github.com/feicong/macbook_issues

致谢

首先，感谢父母的养育之恩，是他们给予了我生命。他们是最可爱的人！

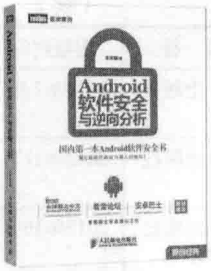
感谢老婆蓉对我工作的理解，由于工作的忙碌与截稿期的临近，我把本应该陪伴她的大量休息时间花在了伏案写作上（我不会在这里告诉你，我已经在为下一次的旅游计划做准备了）。

感谢图灵公司对本书的认可与支持，感谢策划编辑张霞对本书内容的跟进与督促，这才使得书稿能够顺利地完成。

感谢 Proteas 和熊猫正正在百忙之中抽出时间对本书进行了技术审校，他们的宝贵意见和建议使我受益匪浅。

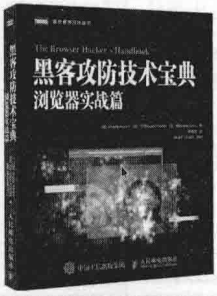
此外，在写作过程中，我得到了很多朋友与同行的帮助。熊猫正正一起构建了本书的写作框架，提供了丰富的 macOS 系统与逆向方面的学习资料，并审阅了初稿，这些都是宝贵且难得的；仙果提供了部分章节中逆向工具方面的演示效果；黄药师给出了游戏安全章节的有效建议；Claud Xiao 对目录的制定提供了建设性的建议；还有很多朋友在写作内容与审稿上给出了宝贵的意见，他们是：Proteas、听鬼哥说故事、怒吼①聲つ喵、人生无 NG（淡然出尘）（排名不分先后）……在这里向你们表示衷心的感谢。

推 荐 阅 读



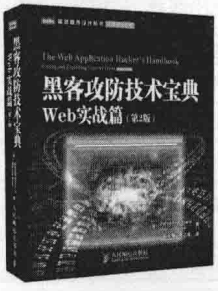
- 国内首本Android安全图书
- 各大网店同类图书销量榜首
- 深入讲解Android攻击与防范

书号：978-7-115-30815-3
定价：69.00 元



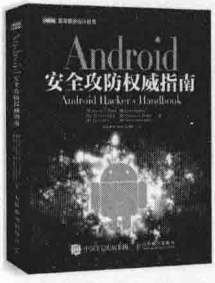
- 浏览器安全领域的先锋之作、浏览器攻击框架BeEF团队实战经验总结
- 涵盖所有主流浏览器以及移动浏览器
- 分三阶段、七大类讲解浏览器攻防方法

书号：978-7-115-43394-7
定价：109.00 元



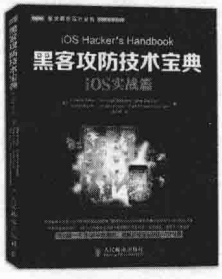
- 安全技术宝典全新升级
- 亚马逊书店五星赞誉
- 探索和研究Web应用程序安全漏洞的实践指南

书号：978-7-115-28392-4
定价：99.00 元



- Android安全第一书，专注于阐述设备root、逆向工程、漏洞研究和软件漏洞利用等技术细节
- 顶级白帽子原著 + 一线安全专家演绎
- tombkeeper、Flanker、dm557、非虫等知名白帽子鼎力推荐

书号：978-7-115-38570-3
定价：89.00 元



- 美国国家安全局全球网络漏洞攻击分析师、连续4年Pwn2Own黑客竞赛大奖得主Charlie Miller主笔
- 作者阵容超级豪华，6位均为信息安全领域大名鼎鼎的顶级专家，各有所长，且多有专著出版
- 国内唯一专注iOS平台漏洞、破解及安全攻防的中文专著

书号：978-7-115-32848-9
定价：69.00 元

目　录

第 1 章 如何分析macOS软件

万事开头难。许多希望学习逆向工程的朋友通常在网上翻看了许多相关的博客和教程之后仍会觉得无从下手，第1章将会带你从头开始搭建一个最简单的分析环境，引导你自己动手写一个简单的CrackMe并破解它。

这一章不会介绍复杂的IDE，也不会使用各种“酷炫”的逆向工具，一切删繁就简，只使用命令行工具和简单的命令，来完成我们第一次Mac平台的逆向之旅，让你对逆向的过程有一个初步的认识。虽然目前在这个分析环境中只有几个命令行工具，但在后面的章节我们会不断地扩充。另外，Mac平台上的分析工具目前还不像Windows上那样种类繁多，所以我们还会自己开发一些实用的工具，添加到我们的分析环境中，使它变得更为充实。

1.1 分析环境搭建

首先，我们需要一个编译器来编译代码，目前在macOS系统上最流行的编译器自然是大名鼎鼎的Clang。

1.1.1 安装 Clang

如果你安装过Xcode，那说明你已经安装了Clang编译器，就可以先跳过本节。

Clang隶属于苹果公司的开源项目LLVM，是LLVM的一个前端，LLVM的官网为http://llvm.org，如图1-1所示。

你可以直接到LLVM官网下载编译好的Clang，但是这样下载Clang缺少一些必要的工具，使用起来很不方便，这些工具大部分跟Clang一样，包含在苹果的开发工具包中，这个工具包可以直接从App Store上下载。但是，还有更简便的方法。

首先打开一个终端，点击Launchpad→其他→终端，在终端中输入clang并回车，系统会自动检测到我们有没有安装Clang编译器，然后会提示我们是否下载并安装命令行开发者工具，如图1-2所示。

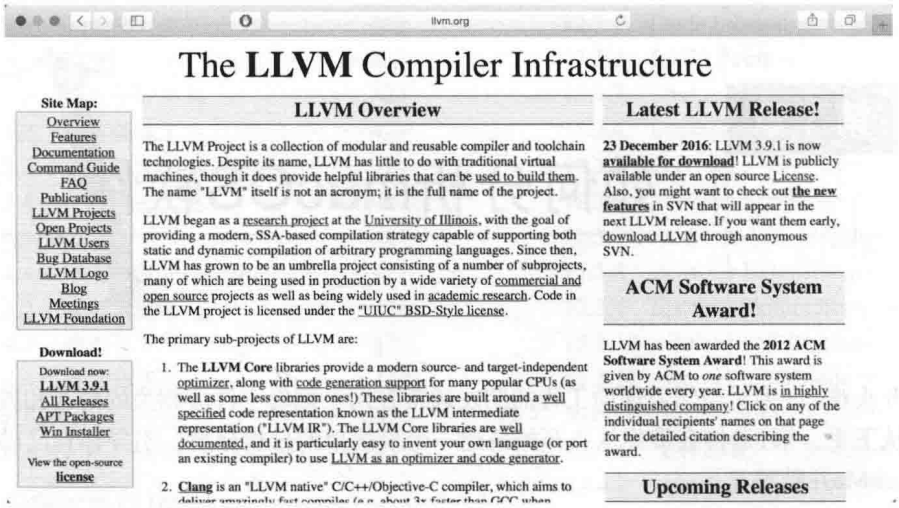


图1-1　LLVM官网

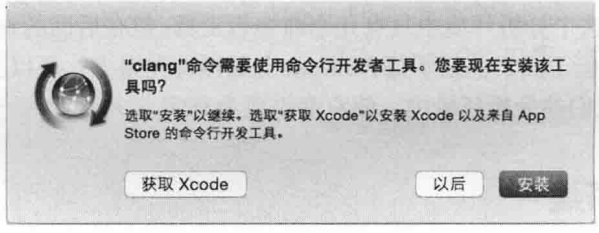


图1-2　安装命令行开发者工具提示

选择“安装”，就会出现安装协议，同意安装协议，过一会儿Clang编译器就会下载并安装到系统中了，一起安装的还有make等常用的命令行编译工具。我们可以执行clang -v查看Clang是否安装正确。

```
$ clang -v
Apple LLVM version 7.0.0 (clang-700.1.76)
Target: x86_64-apple-darwin14.5.0
Thread model: posix
```

如果能正确输出版本信息，则说明已经成功安装了Clang，接下来就可以使用它来编译程序了。

1.1.2　HT Editor

HT Editor是一个开源跨平台的十六进制编辑器，但它的功能可远远不止十六进制编辑器这么简单，它还有强大的反汇编/汇编功能，支持x86、x64、ARM、Power等多种处理器，并支持Windows平台上的PE文件格式、Linux上的ELF格式以及macOS的Mach-O文件格式。我们在这里要用它来破解CrackMe。

HT Editor的官网为http://hte.sourceforge.net/，如图1-3所示（打开该网站可能需要国外的代理）。

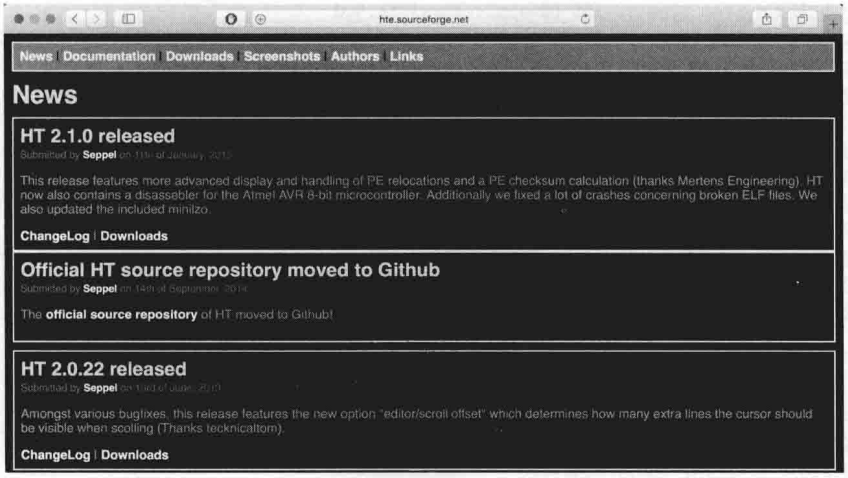


图1-3 HT Editor官网

HT Editor官网只提供了Windows版本的二进制文件，在Mac上我们需要自己动手编译来生成它。不过不要担心，这并不是什么难事，在macOS上编译大多数开源项目跟在UNIX系统是一样的，基本上只需要“./configure && make”就可以了。

首先，点击Downloads超链接，下载最新版本的源代码，如图1-4所示。

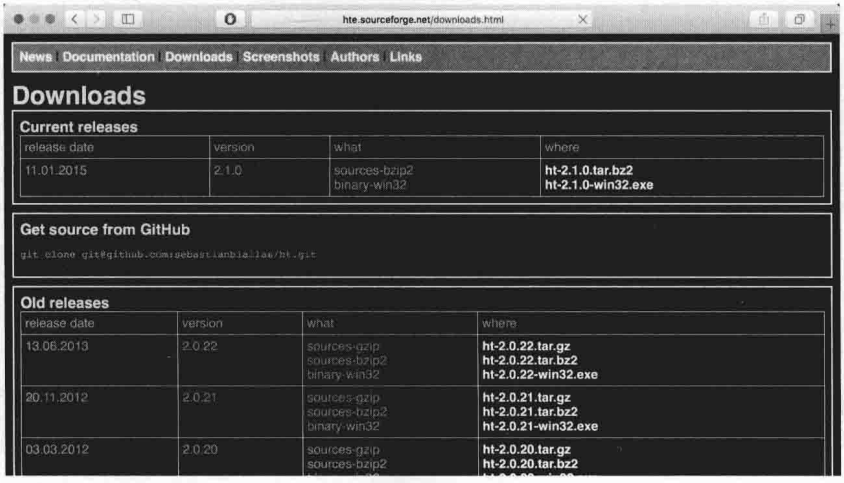


图1-4 HT Editor官网

在写作本书时，HT的最新版本是2.1.0。点击“ht-2.1.0.tar.bz2”超链接下载源代码并将其解压缩到一个合适的目录，我将其解压到用户目录下的Project目录中。然后打开一个终端，使用cd命令切换到源代码所在的目录，然后在终端中执行./configure并回车，会看到大量的“checking”：