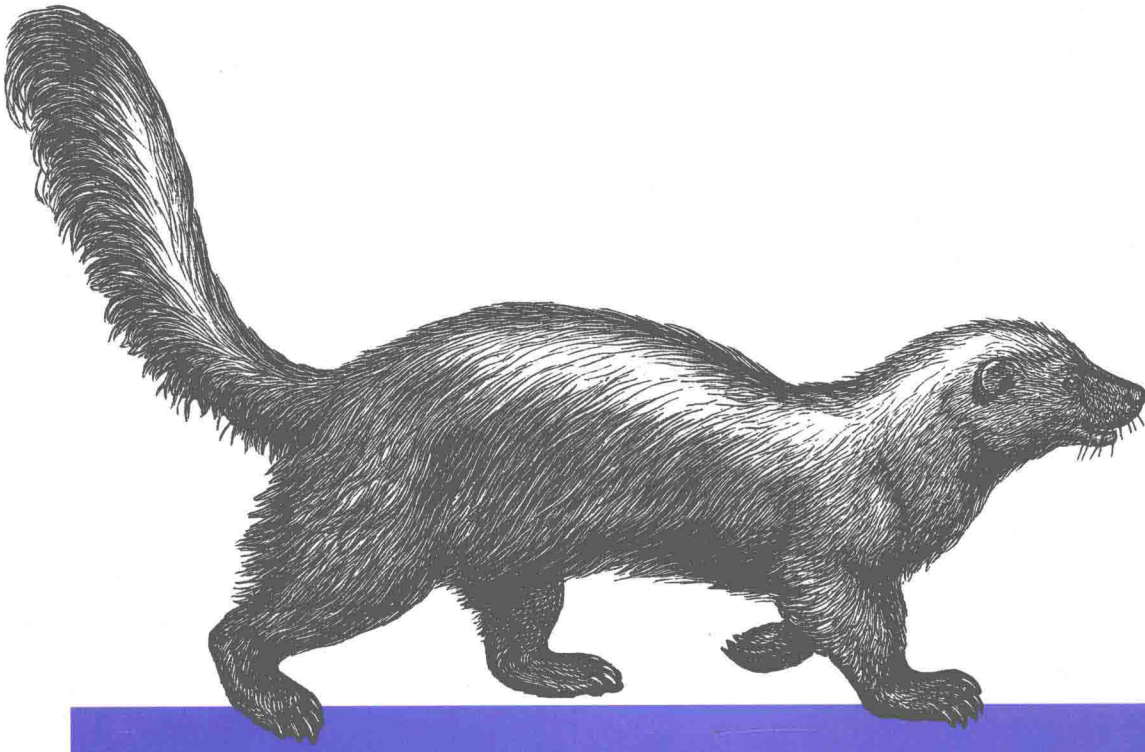
Hacking and Securing iOS Applications

"看过本书的朋友，能够将自己的iOS应用在安全方面的得分，从不及格提升到80分。"

——唐巧，《iOS开发进阶》作者



iOS应用安全攻防实战

[美] *Jonathan Zdziarski* 著

肖梓航 李俱顺 译

O'REILLY®

中国工信出版集团

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

iOS应用安全攻防实战

[美] Jonathan Zdziarski 著
肖梓航 李俱顺 译

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

内 容 简 介

数据被盗等安全问题已经不再是一件罕见的事情了。在这个信息化的时代里，数据就是价值，而且有越来越多的迹象表明，攻击者也正逐步将攻击目标转到移动端。如何保障自己的应用数据安全？本书将会提供一些用于防御常见攻击方法的方式。安全专家 Jonathan Zdziarski 将演示攻击者用来窃取数据、操控软件的许多技术，并向开发者介绍如何避免在软件中犯下各类常见的错误，以及避免软件被轻易地攻击。

版权贸易合同登记号 图字：01-2015-1605

图书在版编目（CIP）数据

iOS 应用安全攻防实战 /（美）斯的扎斯克（Zdziarski,J.）著；肖梓航，李俱顺译 . —北京：电子工业出版社，2015.7
书名原文：Hacking and Securing iOS Applications
ISBN 978-7-121-26074-2

Ⅰ . ① i… Ⅱ . ①斯… ②肖… ③李… Ⅲ . ①移动终端－应用程序－程序设计 Ⅳ . ① TN929.53

中国版本图书馆 CIP 数据核字 (2015) 第 100983 号

策划编辑：刘 皎
责任编辑：李利健
封面设计：Karen Montgomery 张 健
印 刷：北京中新伟业印刷有限公司
装 订：三河市华成印务有限公司
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：24 字数：518千字
版 次：2015年7月第1版
印 次：2015年7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。

O'Reilly Media, Inc.介绍

O'Reilly Media通过图书、杂志、在线服务、调查研究和会议等方式传播创新知识。自1978年开始，O'Reilly一直都是前沿发展的见证者和推动者。超级极客们正在开创着未来，而我们关注真正重要的技术趋势——通过放大那些“细微的信号”来刺激社会对新科技的应用。作为技术社区中活跃的参与者，O'Reilly的发展充满了对创新的倡导、创造和发扬光大。

O'Reilly为软件开发人员带来革命性的“动物书”；创建第一个商业网站（GNN）；组织了影响深远的开放源代码峰会，以至于开源软件运动以此命名；创立了Make杂志，从而成为DIY革命的主要先锋；公司一如既往地通过多种形式缔结信息与人的纽带。O'Reilly的会议和峰会集聚了众多超级极客和高瞻远瞩的商业领袖，共同描绘出开创新产业的革命性思想。作为技术人士获取信息的选择，O'Reilly现在还将先锋专家的知识传递给普通的计算机用户。无论是通过书籍出版、在线服务或者面授课程，每一项O'Reilly的产品都反映了公司不可动摇的理念——信息是激发创新的力量。

业界评论

“O'Reilly Radar博客有口皆碑。”

——Wired

“O'Reilly凭借一系列（真希望当初我也想到了）非凡想法建立了数百万美元的业务。”

——Business 2.0

“O'Reilly Conference是聚集关键思想领袖的绝对典范。”

——CRN

“一本O'Reilly的书就代表一个有用、有前途、需要学习的主题。”

——Irish Times

“Tim是位特立独行的商人，他不光放眼于最长远、最广阔的视野并且切实地按照Yogi Berra的建议去做了：‘如果你在路上遇到岔路口，走小路（岔路）。’回顾过去Tim似乎每一次都选择了小路，而且有几次都是一闪即逝的机会，尽管大路也不错。”

——Linux Journal

推荐序

为你的 iOS 程序穿上安全的外衣

从有计算机程序开始，安全问题就一直存在，而互联网的流行使得安全问题被进一步放大，所以现在各大互联网公司对安全都非常重视。我曾经所在的网易公司就有专门的安全部门。安全部门的同事会扮演黑客的角色，对网易旗下的产品进行各种试探性的攻击，从而发现公司产品在安全方面的问题。

在移动互联网快速发展的今天，iOS 应用由于直接运行在用户的手机上，相比运行在服务器的后台服务，更有可能被黑客攻击。恶意的一些攻击手段包括劫持网络通信、窃取本地数据以及篡改程序行为。很多人把安全问题完全交给 iOS 系统自带的沙盒（Sandbox），但是仅仅靠沙盒是不够的。因为如果不做其他防护，一旦沙盒被攻破，程序的安全性就完全无法保障。

而在中国，这样的问题尤为突出，因为中国对软件的版权保护不力，使得盗版软件流行。而 iOS 应用如果需要安装盗版软件，越狱系统是最方便的方式（另一种方式是用企业签名）。越狱催生出一些 iOS 盗版应用市场，从而出现一些盗版的游戏、软件以及木马病毒的传播。

作为 iOS 应用的开发者，我们当然不希望自己的游戏被修改成无限道具和金币，自己的应用被修改成无须付费就使用应用内付费功能，更不希望黑客在我们的应用中植入木马，窃取受害用户的账号和密码等敏感信息。而这一切都是沙盒无法保护的。我们需要做更多的安全方面的工作，才能抬高应用被破解和修改的成本，使自己的应用更加安全。

但是，“猫和老鼠”的游戏每天都在上演，在我们不断增加防御手段的同时，黑客的攻击手段也在不断升级。所以，安全问题是一个永不过时的话题，没有绝对意义上的安全。

我们能做的就是不断地学习和研究，使得当前自己应用的安全水平已经能够防止大多数别有用心的黑客攻击。

那么国内 iOS 安全的现状是什么样呢？就我所知，几乎 99% 的 iOS 应用都没有做破解方面的防护。但是，如果你简单地做一些代码混淆、反动态库注入和反调试方面的工作，就可以将应用被破解的难度大大提高。另外，如果你使用 IDA 进行 iOS 代码反汇编，则可以看到你想看的所有应用的源码。我还记得在 2015 年春节前夕，微信在其应用中做了一个抢红包的功能，但这个功能还在测试中，所以被设置成永不开启。但是，我认识的一个做安全方面的朋友却用本书中介绍的 Cycript 工具，将该功能打开，结果造成相关功能被提前泄漏到网上。而一些破坏性更强的逆向攻击行为我都不敢将其公开，因为几乎所有的应用都在这些攻击方式下不能幸免。

那么我个人为什么对安全知识这么感兴趣呢？其实说来话长，我在高中时就开始学习编程，当时的梦想是当一名黑客。于是安全方面的学习就一直伴随着我的职业生涯。而我在学习 iOS 移动开发的时候，带着习惯，我也就开始学习 iOS 开发安全方面的知识。

还记得我学习 iOS 开发安全的时候，曾经看过本书的英文版，其内容同时包括攻击和防御相关的知识，非常适合 iOS 开发工程师学习，并且将其中的实践带到自己的应用中，以保护自己的应用不被攻击。我并不期望本书能够解决所有的安全问题，但是我相信，看过本书的朋友能够将自己的 iOS 应用在安全方面的得分从不及格提升到 80 分。

最后，感谢本书的作者、译者，以及电子工业出版社在 iOS 安全方面所做的贡献。

唐巧 《iOS 开发进阶》作者

2015 年 5 月于北京

译者序

未知攻 焉知防

这是一本介绍如何实现一个更安全的 iOS 应用的书。

在移动应用日趋丰富的今天，移动应用在日常生活中扮演了越来越重要的角色。随着移动互联网的普及，人们对移动应用安全性的要求也在不断提高。很多人认为 iOS 是坚不可催的系统，但是事实告诉我们，在 iOS 系统上也一样存在安全问题，这些安全问题可能最后对用户的个人信息、敏感数据甚至网络交易产生影响。这本书也是一个契机，让我们了解了加固 iOS 应用的一些方法，并尝试从不同的角度来让我们的应用更加安全。

安全技术的攻防，从某种角度上说是思维的攻防。正所谓，未知攻，焉知防。本书虽然页数不多，部分内容还受到年限的影响，但确实是一本不可多得的入门 iOS 应用安全的教程，它提供了一个全面了解和学习安全攻防的体系。从表面上看，本书用大量篇幅介绍了如何攻击一个 iOS 应用，但是实质上，读者通过对攻击方法的了解，就可以掌握攻防的思路，有针对性地来实现防御，让应用更加安全。

尽管 iOS 在版本上不断更新，但在攻防的思路上并没有发生变化，仅是在一些攻防的方法上有所演变。万变不离其宗，为了帮助读者更好地理解书中的思想，作为狗尾续貂，我在书的末尾（附录）添加了部分针对新系统特性的内容，介绍了一些新系统新变化带来的影响。希望读者在阅读本书时，能够尽可能少地受到版本更新的影响，也希望各位从中获益。由于个人能力有限，如果出现错误，希望不吝赐教。

当然，特别需要提醒的是：最佳的安全是一整个应用的安全体系，想让应用更加安全，要做的远不止书中的这些内容。

本书内容分为两部分，前半部分的攻击内容主要由肖梓航翻译，后半部分安全加固内容

由我翻译。特别感谢李利健编辑，她为审阅译文花费了大量的时间与精力，这种耐力和细心让我十分敬佩。感谢肖梓航的引荐，让我可以参与本书翻译，与大家一起努力使本书面世。感谢策划编辑刘皎在本书翻译过程中给予的极大理解和帮助。由于个人的严重拖延症，导致本书现在才能面世，对此，我们深表歉意。

我们在翻译过程中力求将内容尽量还原，行文尽量流畅。但是受限于译者水平，书中的纰漏难免，恳请广大读者批评、指正。关于本书的任何意见和想法，欢迎发送邮件至 cmd4shell@gmail.com，也欢迎关注我的新浪微博 @s1mbily，一起探讨。

最后希望各位能够让自己的 iOS 应用更加安全。

李俱顺

2015 年 4 月于杭州

前言

数据被盗了，这并不是一件罕见的事。在这个信息化的时代，窃取数据成为一件非常有利可图的事情。无论是钓鱼还是大规模的数据泄露，罪犯都可以从电子犯罪中大量获利，并且其收益远超因此承担的风险。当我说这件事并不罕见时，不是在表示不屑，而是在向你发出警告。你的企业中所使用的应用软件里存在可攻击漏洞的可能性非常高。恶意攻击者使用已有军火库中的一系列工具可以对应用软件进行逆向工程、跟踪和操纵，而这些是绝大部分程序员所没有意识到的，甚至许多加密实现都非常脆弱，一个训练有素的攻击者可以从这样或者那样的角度渗透进入，许多次都凸显出软件开发者对安全的错误认识。

攻击者可以采用已经被广泛所知的关于安全漏洞的知识，将其用于长期连接到公共网络的设备、用于可以从你口袋里窃取出来的设备、用于经常被遗忘在吧台上的设备。攻击者只需要花几分钟的时间就可以复制出设备中的文件，或者恶意地注入间谍件或 rootkit，从而轻松地获得设备中的企业应用软件及其保护的数据——这一切甚至可以在你去别处喝了一杯返回吧台前完成。攻击者可以通过各种各样的方法窃取到移动平台的应用软件和数据，之后再悠闲地进行攻击，有时设备所有者压根就不会知道，甚至有时都不需要物理地接触到设备。

本书将演示黑帽子用来窃取数据、操纵软件的许多技术，以及向开发者介绍如何避免在软件中犯下各类常见的错误，避免软件被轻易地攻击。这些攻击并不仅限于从设备上窃取数据，还可能导致更多邪恶的攻击。本书中，你将看到一个示例说明如何攻破一些信用卡支付处理软件，这个问题不仅将存储在设备上的信用卡数据暴露给了攻击者，还可以通过操纵该软件将商户的巨额信用卡资金用于退还给其并没有实际进行过的交易，从而直接从该商户的账户上窃取资金。你还会看到其他许多示例，对这些漏洞进行利用不仅会导致那些移动应用软件的数据产生风险，还让使用这些软件的人陷入危机。读者还

会了解到这些攻击是如何执行的，并看到许多示例和演示说明如何编写更安全的代码使应用软件不会受到这些攻击。

本书读者

本书适合给 iOS 开发人员用于学习设计安全的应用软件，不仅针对政府或金融类软件，还包括所有开发者希望保护其中的数据或功能的软件。为了理解本书中的大部分内容，你需要对 iOS 的 Objective-C 开发有一定的基础。如果对 C 或汇编语言有了解会更好，但并不是必需的。

虽然本书主要针对 iOS，但许多材料都可以直接用于 Mac OS X 计算机。因为这两个环境都是 Objective-C 环境，并且有许多相同的工具，因此，从本书中你还会发现许多内容可以用于从 Mac OS X 的软件中找到漏洞。

全书结构

本书分为两部分。第 1 篇讨论 iOS 和 iOS 软件中存在的许多漏洞及其攻击方法，第 2 篇介绍如何开发更安全的软件。

第 1 章介绍移动安全的核心问题，并且列举出常见的误解，以及许多开发人员对安全的错误的思维方式。

第 2 章向读者介绍许多攻击 iOS 设备的技术，包括越狱。读者会学到如何构建一份定制的代码，并通过流行的越狱技术和定制 RAM 磁盘将其注入到 iOS 设备中。

第 3 章介绍了如何在几分钟内窃取到 iOS 设备的文件系统，以及为什么开发者不能仅仅依赖于设备厂商所提供的磁盘加密功能。你还会学到如何通过一些常见的社会工程学方法接触到一台设备而不让其所有者察觉。

第 4 章介绍如何对操作系统中遗留的数据进行取证分析，以及攻击者可以从窃取到的设备中获得哪些信息。

第 5 章介绍如何攻击 iOS 的钥匙链加密和数据保护加密机制，以及这些机制的内在问题。

第 6 章演示如何通过 HFS 的日志系统获得已删除的文件，并给出如何安全地删除文件使其无法被恢复的示例。

第 7 章介绍一些用于侦查和操纵运行时环境的工具，并演示攻击者可以如何操纵应用软件中的对象、变量和方法来绕过各类安全保护。

第 8 章介绍许多工具和方法，可以用于反汇编和调试软件、注入恶意代码，以及开展其他底层攻击。

第 9 章介绍用于劫持 SSL 会话的一些工具，并说明如何防止自己的软件陷入这类攻击中。

第 10 章详细介绍多种安全机制和方法，以及如何用恰当的加密技术来保护数据。

第 11 章介绍如何将软件设计为残留更少的跟踪信息，从而避免数据被取证分析而泄露。

第 12 章介绍用于让攻击软件变得更复杂和困难的许多实践方法。

第 13 章给出了一些技术，软件可以用它们来检测是否运行在一台越狱后的设备中，以及是否存在一些流行的越狱工具。

第 14 章总结全书，说明理解问题并制定战略的重要性。

本书约定

本书中使用下列字体约定：

斜体（Italic）
: 用于表示网址（URL）、邮箱地址、文件名和文件扩展名等。

楷体
: 用于表示新的术语。

`等宽字体（Constant width）`
: 用于列举代码，以及对变量名、函数名、数据库、数据类型、环境变量、声明语句、关键词等代码元素的行内引用。

`等宽加粗字体（Constant width bold）`
: 用于显示要输入的命令，或者其他应该引起读者注意的文本。

`等宽斜体（Constant width italic）`
: 用于说明这部分文本应该由读者根据上下文提供新的值来替换。

这类标注通常是一个技巧、建议或者一般性标注。

这类标注用于警告或提醒。

使用示例代码

本书就是为了帮助你完成手头工作的，因此，一般情况下，你可以将本书中的代码直接用于你的程序或文档中。你不需要再次联系我们获得授权，除非你一次性复制其中的绝大部分代码。例如，在编写的程序中使用了来自本书的多个代码块是不需要授权的，但是将 O'Reilly 公司图书的示例代码作为 CD-ROM 形式销售或者分发必须经过授权许可。引用这本书来回答一个问题或者引用其中的示例代码并不需要授权，但是在你产品的文档中一次性使用大量来自本书的示例代码必须经过授权许可。

我们感谢你引用本书，但并不强行要求这么做。引用通常包括书名、作者、出版社和 ISBN。例如："*Hacking and Securing iOS Applications* by Jonathan Zdziarski. Copyright 2012 Jonathan Zdziarski, (ISBN 9781449318741)."如果你觉得自己使用代码的方式超出了合理使用或者上述权限的范围，请与我们联系：*permissions@oreilly.com*。

法律免责申明

本书中所讨论的技术、技术和内容所有者对使用技术的限制，以及限制使用这些技术的相关法律在不断地变化。因此，本书中所述的一些攻击方法可能已经无法正常工作，可能导致对它们所作用的设备或系统的意外损坏，或者违反相关法律与用户协议。你在使用这些技术时需要自己承担风险，O'Reilly Media, Inc. 对造成的任何损坏以及使用这些技术导致的损失不承担任何责任。任何情况下，你应该注意使用这些技术可能导致违反一些法律，包括版权法。

Safari® Books Online

Safari Books Online 是一个按需数字化图书馆，你可以在这里找到 7500 本技术和创造类图书或视频，快速找到你想要的答案。

通过订阅，你可以从我们的在线图书馆中阅读任何页面或者观看任何视频，通过移动设备阅读数据，在书籍还未正式印刷之前访问到，特别是能访问到作者撰写中的手稿并且发送反馈，复制和粘贴代码示例，组织收藏夹，下载章节，设置关键内容的书签，创建笔记，打印页面等一系列节省时间的功能。

O'Reilly Media 已经将这本书上传到 Safari Books Online 服务。要获得对这本书的完整电子版访问权限，或者阅读其他来自 O'Reilly 或其他出版社的类似主题的书籍，可以到 *http://my.safaribooksonline.com* 免费注册。

联系我们

请将本书相关的评论和问题寄到下列地址：

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

北京市西城区西直门南大街 2 号成铭大厦 C 座 807 室（100035）
奥莱利技术咨询（北京）有限公司

我们为本书设置了一个网页，在该网页中列出了勘误表、示例和所有附加的信息，你可以从以下网址访问该页面：

http://www.oreilly.com/catalog/9781449318741

如果要留言或者提交关于本书的技术问题的反馈，请发邮件至：

bookquestions@oreilly.com

本书的更多信息、资源、参考文献和新闻，请登录出版社官方网址：*http://www.oreilly.com*。

我们的 Facebook: *http://facebook.com/oreilly*
我们的 Twitter: *http://twitter.com/oreillymedia*
我们的 YouTube 视频：*http://www.youtube.com/oreillymedia*

目录

前言 xv

第 1 章　你所知道的一切都是错的 1

单一化方案的误解 2
iOS 安全模型 4
　iOS 安全模型的组件 4
钥匙和锁存在一起 7
密码等于弱安全 8
数字取证击败加密 9
外部数据同样也有风险 10
劫持流量 10
　数据可能很快就被偷走 11
谁都不要信，包括你的应用软件 12
物理访问并非必需的 13
总结 14

第 1 篇　攻击

第 2 章　iOS 攻击基础 17

为什么要学习如何破解一台设备 17

越狱解析 18
开发者工具 18
终端用户越狱 20
越狱一台 iPhone 21
DFU 模式 22
不完美越狱和完美越狱 24
攻破设备并注入代码 24
构建定制代码 25
分析你的二进制程序 27
测试你的二进制程序 29
代码守护化 31
以 tar 归档包的形式部署恶意代码 35
以 RAM 磁盘形式部署恶意代码 36
练习 50
总结 50

第 3 章 窃取文件系统 53

全盘加密 53
固态 NAND 53
磁盘加密 54
iOS 硬盘加密会让你在哪里失败 55
复制实时文件系统 56
DataTheft 载荷 56
定制 launchd 66
准备 RAM 磁盘 72
创建文件系统镜像 73
复制原始文件系统 75
RawTheft 载荷 75
定制 launchd 80
准备 RAM 磁盘 81
创建文件系统镜像 82
练习 83
社会工程学的作用 83

无法正常使用的诱饵设备 84
未激活的诱饵设备 85
包含恶意代码的诱饵 86
密码工程学软件 86
总结 87

第 4 章　取证跟踪和数据泄露 89

提取照片的地理标签 90
被合并到一起的 GPS 缓存 91
SQLite 数据库 93
连接到一个数据库 93
SQLite 内建命令 94
执行 SQL 查询 95
重要的数据库文件 95
联系人地址簿 95
地址簿头像 97
Google 地图数据 99
日历事件 105
通话记录 105
电子邮件数据库 106
笔记 107
照片元数据 108
短信 108
Safari 书签 109
短信 spotlight 缓存 109
Safari Web 缓存 110
Web 应用缓存 110
WebKit 存储 110
语音邮件 110
对残余的数据库记录进行逆向 111
短信草稿 113
属性列表 113
重要的属性列表文件 114

其他重要的文件 119
总结 121

第 5 章 对抗加密 123

Sogeti 数据保护工具 123
安装数据保护工具 124
构建暴力破解器 125
构建需要的 Python 库 126
提取加密密钥 126
KeyTheft 载荷 126
定制 launchd 127
准备 RAM 磁盘 128
准备内核 129
执行暴力破解 130
解密钥匙链 133
解密原始磁盘 135
解密 iTunes 备份文件 137
通过间谍件对抗加密 137
SpyTheft 载荷 138
将 spyd 守护化 143
定制 launchd 144
准备 RAM 磁盘 145
执行载荷 145
练习 146
总结 146

第 6 章 无法销毁的文件 147

刮取 HFS 日志 148
还原闲置空间 150
常被还原出来的数据 150
应用软件屏幕截图 150
已删除的属性列表 152