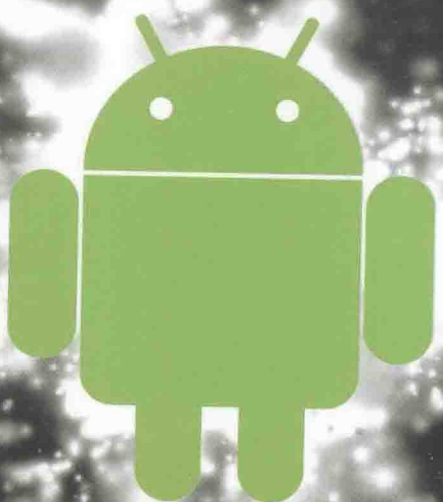
TURING 图灵程序设计丛书

Android
安全攻防权威指南
Android Hacker's Handbook

[美] Joshua J. Drake [美] Collin Mulliner
[西] Pau Oliva Fora [美] Stephen A. Ridley ◎著
[美] Zach Lanier [德] Georg Wicherski

诸葛建伟 杨坤 肖梓航 ◎译



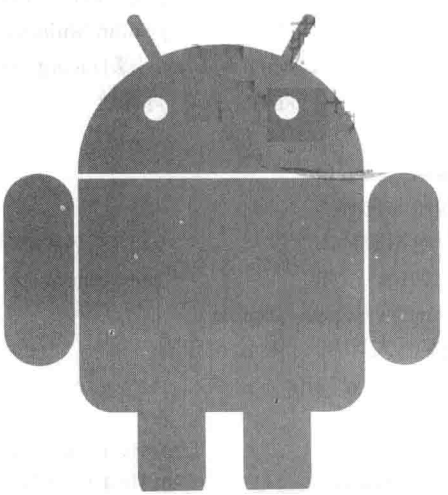
中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

Android
安全攻防权威指南
Android Hacker's Handbook

[美] Joshua J. Drake [美] Collin Mulliner
[西] Pau Oliva Fora [美] Stephen A. Ridley
[美] Zach Lanier [德] Georg Wincherski ◎著

诸葛建伟 杨坤 肖梓航 ◎译



人民邮电出版社
北 京

图书在版编目（CIP）数据

Android安全攻防权威指南 / (美) 德雷克(Drake, J. J.) 等著 ; 诸葛建伟, 杨坤, 肖梓航译. -- 北京 : 人民邮电出版社, 2015.4
(图灵程序设计丛书)
ISBN 978-7-115-38570-3

Ⅰ. ①A… Ⅱ. ①德… ②诸… ③杨… ④肖… Ⅲ. ①移动终端－应用程序－程序设计－安全技术－指南 Ⅳ. ①TN929.53-62

中国版本图书馆CIP数据核字(2015)第038666号

内 容 提 要

本书由世界顶尖级黑客打造，是目前最全面的一本 Android 系统安全手册。书中细致地介绍了 Android 系统中的漏洞挖掘、分析，并给出了大量利用工具，结合实例从白帽子角度分析了诸多系统问题，是一本难得的安全指南。

本书的目标读者为软件安全技术人员，操作系统及应用开发人员。

◆ 著 [美] Joshua J. Drake [西] Pau Oliva Fora
[美] Zach Lanier [美] Collin Mulliner
[美] Stephen A. Ridley [德] Georg Wincherski
译 诸葛建伟 杨 坤 肖梓航
责任编辑 朱 巍
执行编辑 杨 琳
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
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：25.5
字数：617千字 2015年4月第1版
印数：1-4 000册 2015年4月北京第1次印刷
著作权合同登记号 图字：01-2014-4711号

定价：89.00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

中文版序

“中国”和“Android”是一对独特的组合。近几年来，中国已经成为全球最大的手机市场，与此同时，Android 也成为最主流的智能手机操作系统。但是两者的联系并不仅仅体现在规模上。中国还拥有与众不同的手机产业环境，许多手机厂商专门为中国市场生产各种移动设备，而这些设备大都采用 Android 或者从 Android 原始代码衍生而来的操作系统。此外，中国还有着庞大的安全研究社区，并且产出了许多优秀的研究成果，尤其是在移动安全领域。我们希望 *Android Hacker's Handbook* 的这本中文版有助于中国的开发者和研究人员理解关于 Android 平台及其安全特性的必备知识。

China and Android are a unique combination. Over the last couple of years China has become the world's largest mobile phone market while at the same time Android became the dominant smartphone operating system. But the combination of China and Android is not only about size. China has a unique mobile phone ecosystem with a number of mobile phone manufacturers that exclusively built devices for the Chinese market. Many of these devices run Android or operating systems that are derived from the original Android code. China also features a large security research community and is the source of a lot of good research, especially in the mobile space. With the Chinese translation of the *Android Hacker's Handbook* we hope to provide developers and researchers with essential and easy accessible knowledge about the Android platform and its security features.

Collin Mulliner

前　言

信息安全与大多数领域一样，都是从家庭式手工作坊开始萌芽的。经过自主发展，这一领域已经跨越了业余消遣式的初级阶段，逐渐成为一个健全的产业。如今的信息安全领域中，有顶着各种行政头衔的大佬们，也有从事一线研发工作的牛人们，还有来自学术圈的“眼线”们。这也是一块创新热土，能够让数论、密码学、自然语言处理、图论、算法、理论计算机科学等一系列看似冷僻的研究方向产生重大行业影响。对于这些令人神往的科学研究而言，信息安全行业正在发展进化成为它们的创新试验场，但与此同时，信息安全（特别是“漏洞研究”）仍然受信息技术领域整体发展的限制，并与信息技术领域的热点趋势保持一致。

正如我们每个人从个人生活中强烈感受到的那样，移动计算显然是信息技术领域近年来得到巨大发展的一个热点方向。现在，各种移动设备已经无时无刻不伴随在我们的左右，我们花在移动设备上的时间要比花在电脑上的时间多得多：办公用的电脑在下班后就会被我们遗弃在办公桌上，而家里的电脑在我们早上急匆匆去上班时甚至没有打开的机会，这种变化是前所未有的。与电脑不同的是，我们的移动设备始终是保持开机的，而且连接着工作与家庭这两个世界，因此也成为了坏人们眼中更具价值的攻击目标。

不幸的是，信息安全行业适应移动化趋势的脚步有些迟缓，近期才刚刚跨出了一小步。作为一个“保守派”占多数的行业，信息安全领域在移动与嵌入式安全研究开发上的行动在过去几年里过于缓慢（至少公开层面上是这样的），以至于移动安全在某种程度上仍然被认为是前沿研究，因为移动设备的消费者与用户最近才开始察觉并理解日常使用移动设备所面临的安全威胁。这些威胁也随之为移动安全研究与安全产品创造了市场前景。

对于信息安全领域研究者而言，移动平台就像是一块新大陆，等待着人们去探索，其中有着各种处理器架构、硬件外设、软件栈和操作系统所构成的多样化“地理结构”，它们共同构成了一个挖掘、利用和研究各类漏洞的生态系统。

根据 IDC 的统计，Android 在 2012 年第三季度的全球市场份额是 75%（以当季出货量计算），共出货一亿三千六百万部。苹果公司的 iOS 在当季的市场份额为 14.9%，黑莓与塞班则分别以 4.3%和 2.3%的市场份额被甩在后面。而到了 2013 年第三季度，Android 的市场份额上升到了 81%，iOS 下降至 12.9%，剩余的 6.1%则分散在其他移动操作系统中。在这样的市场份额分布格局下，Android 世界中有着一系列有趣的信息安全事件和研究工作，我们觉得一本能够描述该领域本质的书籍肯定是大家翘首以盼的。

Wiley 出版社已经出版了 Shellcoder's、Mac、Database、Web Application、iOS 和 Browser 等“黑

试读结束：需要全本请在线购买：　www.ertongbook.com

客攻防技术宝典”系列图书[①]。《Android 安全攻防权威指南》是这一系列的最新图书，充分借助了整个系列的一些基础信息。

本书及相关技术概述

我们决定写这本书的主要原因是，当前移动安全研究领域的知识图谱过于稀疏，仅有的参考资源和技术资料互相孤立，甚至是相互冲突的。虽然已经有了不少专注于 Android 的优秀论文和其他出版物，但其中很大一部分所涵盖的内容都非常狭窄，仅仅关注 Android 安全的某个特定方向，或者只是在讨论移动或嵌入式设备的某个安全问题时将 Android 作为一个辅助例子予以提及。此外，Android 相关的已公开漏洞信息非常稀缺，虽然现在已经有超过 1000 个已公开的漏洞会影响到 Android 设备，但通过常见漏洞信息渠道报告的只有不到 100 个。我们相信，本书所介绍的相关技术、概念、工具、技巧和案例，可以帮助你迈上改善 Android 安全产业态势的漫漫长路。

本书的结构

本书应该按照章节顺序进行阅读，但是对于正在钻研 Android 或者进行 Android 设备安全研究的读者来说，也可以将本书作为一本参考资料。本书一共分为 13 章，几乎涵盖了安全研究人员第一次接触 Android 所需要了解的所有内容。这些章节通过图表、截图、代码片段和反汇编代码等来介绍 Android 的软硬件环境，进而讨论在 Android 上进行软件漏洞利用和逆向工程的不同之处。全书的大致结构是，从一些宽泛的话题开始，以深度的技术细节收尾。这些章节逐步具体化，最终将讨论一些安全研究的高级话题，如发现、分析和攻击 Android 设备。本书尽可能地引用来自外部的各类详细文档，从而专注于阐述设备 root、逆向工程、漏洞研究和软件漏洞利用等技术细节。

- 第 1 章介绍 Android 移动设备的生态系统。首先回顾 Android 系统发展的历史，然后介绍通用软件的构成、Android 设备的市场流通情况以及供应链当中的各大关键角色，最后从较高层面上总结和讨论 Android 生态系统发展遭遇的挑战以及安全研究面临的困难。
- 第 2 章阐述 Android 系统的基础知识。首先引入系统安全机制的基础核心概念，然后深入关键安全组件的内部机制。
- 第 3 章介绍获取 Android 设备完全控制权的动机与方法。首先讲授适用于众多设备的通用技术，而后逐一详细分析十几个公开的漏洞利用。
- 第 4 章涉及 Android 应用相关的安全概念和技术。讨论了 Android 应用开发过程中常见的安全错误，并介绍如何使用正确的工具和流程来找到这些问题。
- 第 5 章讨论移动设备可能遭受攻击的形式，并解释用来描述这些攻击的关键术语。

① 其中《黑客攻防技术宝典：系统实战篇》《黑客攻防技术宝典：Web 实战篇》《黑客攻防技术宝典：iOS 实战篇》已由人民邮电出版社出版，《黑客攻防技术宝典：浏览器实战篇》亦将于 2015 年面世。——编者注

- 第 6 章讲述如何使用模糊测试技术来发现 Android 系统中的软件漏洞。从介绍模糊测试宏观流程入手，重点描述如何使用这些流程更好地帮助我们发现 Android 系统中的安全问题。
- 第 7 章介绍如何分析在 Android 系统中发现的缺陷和安全漏洞。本章涵盖了 Android 系统中不同类型与层次代码的调试技术，最后以基于 WebKit 引擎的浏览器中一个未修补的安全问题为案例进行深入分析。
- 第 8 章关注如何利用 Android 设备中发现的内存破坏漏洞，涵盖了编译器和操作系统的内部机理，例如堆的实现、ARM 体系架构规范等。章节最后详细分析了几个公开的漏洞利用。
- 第 9 章介绍高级利用技术 ROP（Return Oriented Programming）。进一步讲述 ARM 体系架构，并解释为何、如何使用 ROP 技术，最后对一个独特的漏洞利用作了更为细致的分析。
- 第 10 章深入 Android 操作系统内核的内部工作原理，涵盖如何从黑客的角度来对内核进行开发和调试，本章最后还会教会你如何利用若干已公开的内核漏洞。
- 第 11 章将带你返回用户空间，来讨论一个特殊且重要的 Android 智能手机组件——无线接口层（RIL）。在阐明 RIL 的架构细节之后，教你如何通过与 RIL 组件的交互，对 Android 系统中处理短消息的模块进行模糊测试。
- 第 12 章关注目前存在于 Android 系统中的安全保护机制，介绍了这些保护机制是何时被发明并引入 Android 系统，以及是如何运作的，最后总结绕过这些保护机制的方法。
- 第 13 章深入探索通过硬件层面来攻击 Android 和其他嵌入式设备的方法。首先介绍如何识别、监视和拦截各种总线级别的通信，并展示如何利用这些方法来攻击那些难以触及的系统组件。最后给出了如何避免遭受这些常见硬件攻击的诀窍。

本书面向的读者

任何想要加深对 Android 安全认识的人都可以阅读本书，不管是软件开发者、嵌入式系统设计师、安全架构师，还是安全研究人员，本书都会帮助你拓宽对 Android 安全的理解。

致　谢

“感谢我的家人，特别是我的妻子和儿子，他们在图书撰写过程中不知疲倦地给予我支持与付出。我要向业界和学术界的合作伙伴们致以谢意，他们的努力研究拓展了公共知识的边界。我还要感谢：令人尊敬的合作作者们对本书的贡献和坦率的交流；拥有宽松氛围的 Accuvant 公司支持我撰写本书并从事其他研究工作；Wiley 出版社在整个过程中对作者撰写工作的激励和引导。最后要感谢的是#droidsec、Android 安全团队和高通安全团队的成员们，你们推动了 Android 安全的发展。”

——Joshua J. Drake

“我要感谢 Iolanda Vilar 鼓励我参与本书的撰写，并在我远离她守在电脑前的所有时刻里，一如既往地支持我。感谢 Ricard 和 Elena 在我的孩提时代允许我追逐自己的梦想。感谢 Wiley 出版社和本书的所有合作作者，我们在这本书上共同工作了无数个日日夜夜，特别要感谢 Joshua Drake 给我烂到家的英语提供的所有帮助。还要感谢 viaForensics 公司的同事们，我们在一起作出了许多非常棒的技术研究。最后感谢#droidsec IRC 频道的所有伙伴们，以及 G+上的 Android 安全社区、Nopcode、48bits 以及我在 Twitter 上关注的所有人，如果没有你们，我不可能跟得上移动安全领域所有的最新技术发展。”

——Pau Oliva

“我要感谢 Sally，我生命中的挚爱，感谢她能够包容我。感谢我的家庭一直以来给我的鼓励。感谢 Wiley 出版社的编辑 Carol 和 Ed 提供了这个机会，感谢我的合作作者们与我分享了这段虽然艰难但令人难忘的旅程。感谢 Ben Nell、Craig Ingram、Kelly Lum、Chris Valasek、Jon Oberheide、Loukas K.、John Cran 和 Patrick Schulz 的支持和反馈，以及一路支持和帮助过我的其他朋友。”

——Zach Lanier

“我要感谢我的女朋友 Amity，我的家人、朋友和同事们的鼎力支持。此外，我要感谢我的顾问为这本书的写作付出了大量时间。特别要感谢 Joshua 让这本书成功面世。”

——Collin Mulliner

“没有人比我的父亲 Hiram O. Russell，母亲 Imani Russell，还有两个弟弟妹妹 Gabriel Russell 和 Mecca Russell 更值得我感谢。我之所以能成为现在的我，离不开家人的支持和厚爱。我父母都给予了我无限的鼓励，而我的弟弟和妹妹也不断地以他们的智慧、成就与品质打动我。你们是我生命中最最重要的。我还要感谢我美丽的妻子 Kimberly Ann Hartson，能够一直包容我并在我的生命中充当这样一个充满爱心和平静的力量。最后，我想感谢信息安全社区。信息安全社区是非常奇怪的圈子，但它是我的‘成长’家园 。同事和研究人员（包括我的合著者）是我永恒的灵感之源，为我提供了获取新闻、八卦与理想目标的常规渠道，并让我对这方面的工作更感兴趣。我很荣幸有机会能够合作编撰本书。”

——Stephen A. Ridley

“我衷心感谢我的妻子 Eva 和儿子 Jonathan，能够容忍我花时间写书，而不是去照顾他们。我爱你们。感谢 Joshua 能够将我们聚在一起让本书面世。”

——Georg Wicherski

关于作者

Joshua J. Drake 是 Accuvant LABS 公司研究部门总监，集中精力于逆向工程以及安全漏洞分析、挖掘与利用等领域的原创性研究。他在信息安全领域拥有十多年的研究经验：1994 年开始研究 Linux 安全，2009 年开始研究 Android 安全，并于 2012 年开始为 Android 主流 OEM 提供咨询服务。之前，他曾供职于 Metasploit 团队和 VeriSign 公司的 iDefense 实验室。在 BlackHat USA 2012 大会上，Georg 和 Joshua 成功演示了通过 NFC（Near Field Communication，近场通信）攻破 Android 4.0.1 浏览器。Joshua 曾在 REcon、CanSecWest、RSA、Ruxcon/Breakpoint、Toorcon 和 DerbyCon 等黑客会议上发表演讲。他在 2013 年赢得了 Pwn2Own 黑客大赛，并于 2010 年随 ACME Pharm 团队获得 Defcon 18 CTF 决赛冠军。

Pau Oliva Fora 是 viaForensics 公司的移动安全工程师，此前在一家无线设备厂商中担任研发工程师。自从 2008 年 10 月 Android 操作系统随 T-Mobile G1 登台之后，他便开始活跃于研究 Android 安全问题。他对智能手机安全的研究热情不仅仅表现在开发了大量漏洞利用代码和工具上，同时还表现在其他许多方面，例如他甚至在 Android 出现之前就担任了人气 XDA 开发者论坛的版主。他的工作是为一些主流的 Android OEM 提供咨询服务。对移动安全社区的亲身参与和近距离观察，让他特别兴奋地参与到撰写这本描述移动安全本质的著作当中。

Zach Lanier 是 Duo Security 公司的资深安全研究员，在信息安全的不同领域中有十多年的工作经验。他从 2009 年开始进行移动与嵌入式安全研究，范围覆盖应用安全，平台安全（特别是 Android）以及设备、网络与运营商安全。他的研究兴趣还包括攻击、防御和隐私增强技术。他曾在多个公开和内部的业界会议上发表过演讲，包括 BlackHat、DEFCON、ShmooCon、RSA、Intel 安全会议、Amazon ZonCon 等。

Collin Mulliner 是美国东北大学的博士后研究员，主要研究兴趣是移动和嵌入式系统的安全和隐私，重点关注移动智能手机。他在该领域中的早期工作可追溯至 1997 年，当时他在为 Palm OS 开发应用。Collin 以在彩信（MMS）和短信（SMS）安全方面的工作而闻名。之前，他对漏洞分析和攻击技术更感兴趣，但是最近他将关注点转移到了防御方向上，研究开发攻击缓解与应对措施。Collin 在德国柏林科技大学获得计算机博士学位，之前分别在加州大学圣巴巴拉分校和达姆施塔特应用科技大学获得硕士和学士学位。

Ridley（他的伙伴们是这么称呼他的）是一位安全研究员与技术作者，在软件开发、软件安全和逆向工程领域有十几年的经验。在最近几年中，Stephen 在除了南极洲的每个大陆上都演讲并展示过他在逆向工程和软件安全方面的研究工作。之前，Stephen 曾经是新型在线银行 Simple.com 的首席信息安全官，Matasano Security 公司的资深研究员，一家美国国防部承办商的安全任务保障组创始成员，他精于安全漏洞研究、逆向工程和“攻击软件”，对美国国防部和情报部门提供技术支撑。现在，Stephen 是 Xipiter（一家开发新型低能耗智能传感器设备的信息安全研发公司）的首席科学家。Stephen 最近的工作获得了 NPR、NBC 等电视台以及《连线》《华盛顿邮报》《快公司》、VentureBeat、Slashdot、The Register 等媒体的专题报道。

Georg Wicherski 是 CrowdStrike 公司的资深安全研究员，特殊癖好是对计算机安全底层进行探索和修补，手工调试私人定制的 Shellcode，以及修改漏洞利用代码使其变得足够稳定与可靠。在加入 CrowdStrike 公司之前，Georg 曾在卡巴斯基和迈克菲公司工作。在 BlackHat USA 2012 大会上，Georg 和 Joshua 成功演示了通过 NFC 攻破 Android 4.0.1 浏览器。他曾在 REcon、SyScan、BlackHat USA、BlackHat Japan、26C3、ph-Neutral、INBOT 等会议上发表演讲。0ldEur0pe 是他的本地 CTF 战队，他们参加过无数黑客竞赛，并多次赢得冠军。

试读结束：需要全本请在线购买：　www.ertongbook.com

版权声明

All Rights Reserved. This translation published under license. Authorized translation from the English language edition, entitled *Android Hacker's Handbook*, ISBN 9781118608647, by Joshua J. Drake, Pau Oliva Fora, Zach Lanier, Collin Mulliner, Stephen A. Ridley, Georg Wicherski, Published by John Wiley & Sons. No part of this book may be reproduced in any form without the written permission of the original copyrights holder.

Simplified Chinese translation edition published by POSTS & TELECOM PRESS Copyright © 2015.

本书简体中文版由John Wiley & Sons, Inc.授权人民邮电出版社独家出版。

本书封底贴有John Wiley & Sons, Inc.激光防伪标签，无标签者不得销售。

版权所有，侵权必究。

目　录

第 1 章 纵观 Android 生态圈

尽管 Android 这个词仍然可以用来指代人形机器人，但如今其含义已经远比十年前丰富，可以用于许多种场景中。在移动领域中，它既可以指公司、操作系统，也可以指开源项目和开发者社区。一些人甚至把移动设备称为 Android。总之，现在围绕着这个非常流行的移动操作系统，已经形成了一个完整的生态圈。

本章将仔细审视 Android 生态圈的构成与健康状态。首先介绍 Android 是如何发展成目前的状态的，然后将这个生态圈的利益相关者进行分组，帮助读者理解他们的角色与动机。最后本章讨论生态圈中一些复杂的关联关系，它们会造成影响安全性的几个重要问题。

1.1 了解 Android 的根源

Android 并不是一夜之间就成为世界上最流行的移动操作系统的。过去十年，Android 走过了一段漫长而颠簸的旅程。本节讲述 Android 是如何成为现在的样子，并开始探究到底是什么孕育了 Android 生态圈。

1.1.1 公司历史

Android 是从一家名为 Android 的公司开始的，这家公司于 2003 年 10 月由 Andy Rubin、Chris White、Nick Sears 和 Rich Miner 创立。他们专注于创造能够考虑位置信息和用户偏好的移动设备。在成功调查市场需求并克服资金困难之后，谷歌公司在 2005 年 8 月收购了 Android 公司。在接下来的一段时间里，谷歌开始与硬件、软件和电信企业建立伙伴关系，意图进军移动市场。

2007 年 11 月，开放手机联盟（OHA）宣告成立。这个企业联盟包括了以谷歌为首的 34 家创始会员公司，共同秉承着对开放性的承诺。此外，联盟的目的是加速移动平台上的创新，为消费者提供更丰富、更便宜和更好用的移动体验。在本书出版时，OHA 会员已经增至 84 个。联盟会员包含了移动生态圈的所有重要环节，包括移动运营商、手机制造商、芯片制造商和软件厂商等。你可以在 OHA 的网站上找到联盟会员的完整列表：www.openhandsetalliance.com/oha_members.html。

OHA 成立后，谷歌宣布了他们的第一款移动产品：Android。但谷歌仍然没有向市场发布任何一款运行 Android 的设备。最终经过 5 年之后，在 2008 年 10 月，Android 终于开始进入大众市场，第一款 Android 手机 HTC G1 的公开发布，标志着一个新时代的开始。

试读结束：需要全本请在线购买： www.ertongbook.com