Broadview
www.broadview.com.cn

腾讯GAD
游戏开发者平台
GAD游戏学院系列丛书

游戏安全

手游安全技术入门

腾讯游戏研发部游戏安全中心 编著

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

▶ GAD游戏学院系列丛书 ◀

游戏安全

手游安全技术入门

腾讯游戏研发部游戏安全中心　编著

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

内 容 简 介

本书是国内移动游戏安全领域的开山之作，填补了移动游戏安全书籍的空白，揭开了移动游戏外挂的神秘面纱。

随着移动互联网的日益普及，业内对移动安全领域的专业人才的需求逐年增加，而该领域的专业人才相对匮乏，很多开发人员和有志于从事相关行业的在校学生等一直缺少相关的参考资料和书籍。作为移动安全领域的入门书籍，本书以移动端（涵盖了 Android 和 iOS 两大平台）的游戏逆向分析和外挂技术为切入点，详细讲述了手游安全领域的诸多基础知识和技能，包括：移动端开发和调试环境搭建、典型的移动游戏特性、与外挂相关的安全开发技术、游戏和外挂的逆向分析方法、外挂开发实战演练、游戏引擎逆向分析等内容，书中的部分源代码可免费从网上下载。读者在掌握本书的内容之后，便可入门手游安全领域，同时可以很容易地将在本书中学到的知识扩展至移动端的其他领域，例如：安全方案开发、病毒分析、软件逆向及保护等。

本书可作为高等院校计算机安全相关专业的辅助教材，也可供移动端安全技术人员、游戏开发人员，以及有志于从事游戏安全相关工作的学生等参考。

图书在版编目（CIP）数据

游戏安全：手游安全技术入门 / 腾讯游戏研发部游戏安全中心编著. —北京：电子工业出版社，2016.6
（GAD 游戏学院系列丛书）
ISBN 978-7-121-28783-1

Ⅰ. ①游… Ⅱ. ①腾… Ⅲ. ①移动终端－应用程序－程序设计－安全技术 Ⅳ. ①TN929.53

中国版本图书馆 CIP 数据核字（2016）第 098642 号

策划编辑：张国霞
责任编辑：徐津平
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
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：720×1000　1/16　印张：24　字数：460 千字
版　　次：2016 年 6 月第 1 版
印　　次：2016 年 7 月第 2 次印刷
印　　数：3001～6000 册　　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）88254888，88258888。

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。

本书咨询联系方式：010-51260888-819　faq@phei.com.cn。

推荐语

“GAD 游戏学院系列丛书”的各位作者都是腾讯互娱的业务骨干。他们在这次丛书写作中把多年积累的干货倾囊相授，我们可以从书中感受到他们满满的诚意和认真、严谨的态度。希望“GAD 游戏学院系列丛书”能够真正帮助新人学习优秀的知识，让他们少走弯路；并能够为中国游戏行业的持续发展和人才培养贡献自己的力量。

——腾讯高级副总裁　马晓轶

软件安全行业从无到有，是随着安全对象的价值变化而逐步发展起来的。病毒和木马的肆意妄为、杀毒软件的兴盛、共享软件的蓬勃发展、壳等保护软件雨后春笋般的出现、端游的大行其道，以及游戏外挂与反外挂系统的流行，这些都让软件安全从业者大显身手。在手游开发技术迅猛发展的今天，手游的安全问题已是需要我们迫切解决的问题，本书的出版非常及时和必要。在游戏安全领域，从新手成长为高手的过程非常艰难，要坐得住冷板凳、耐得住寂寞，还要守得住本心和走正道。本书将会对你大有裨益，值得推荐！

——巨人网络奇点工作室负责人、安全专家　卫鹏飞（fly）

无论是出于好奇还是本着学习的态度去阅读本书，本书都不能算作一本通俗读物，而是一本充斥着大量的专业术语和专业知识的书籍。阅读本书，代表你对手游安全有专业的追求和期许，代表你对学习有自我驱动的渴望，因为在专业面前无论是新手还是老手、外行还是内行、跨界还是不跨界都不重要，重要的是做得好与不好、专业与不专业。任何时候，“专业”都是最具有说服力的武器，只有专业，才能成为专家，只有专家才能成为赢家。祝大家阅读愉快！

——《软件加密技术内幕》编委、暴风 TV CTO、安全专家　裴来隆（pll621）

推荐序一

十多年前我刚进入游戏行业时，国内做网络游戏的公司屈指可数，那时游戏行业还不被主流社会所接纳，被媒体妖魔化更是家常便饭。游戏的制作者们背负着巨大的舆论压力还能毅然、决然地去做游戏，正是因为他们都是被游戏本身的魅力所征服的资深玩家。只有我们自己知道，游戏是一种非常棒的体验，和看电影、听音乐一样是一种有益的娱乐形式。我知道有很多人不是为了寻求一份高薪工作，也不是看好游戏行业所谓的发展前景，只是出于自己对游戏的热爱，就不顾一切地进入了这个不被世人所理解的行业。

这是不是像极了硅谷创业传奇故事的开头？一群充满激情、创意并且有想法的年轻人执着地、不计回报地做着被世人视为异端的事情。当然，其结局和硅谷创业的结局一样美好。十多年过去了，在这群偏执狂的努力下，我国的游戏行业不论是产业规模还是技术能力，都已经在全世界举足轻重，并且拥有了像腾讯、网易这样能位列整个行业前茅的游戏公司，而游戏也已经上升为国家的战略文化产业。不论在资本、市场还是政策层面，当年人见人躲的“丑小鸭”，如今已通过自己的努力成为阳光下耀眼的“白天鹅”。

腾讯公司在游戏行业耕耘多年，有得也有失，经验和教训都不少。作为行业的龙头老大，腾讯除了自身的发展经营，也肩负着行业责任和社会义务。这套“GAD 游戏学院系列丛书”的编纂，汇集了来自腾讯各个不同项目、工作室和部门的顶尖游戏制作者的智慧和经验。我们将这些智慧和经验和盘托出，希望能为游戏行业策划新人的成长和能力提高尽到自己的一份力。

现在是最好的时代，信息大爆炸与互联网的高速发展极大地消灭了特权，知识的获取高效而简单，为所有人史无前例地创造了一个公平的世界。大家站到了同一个起

跑线上，每个有理想的年轻人都有弯道超车的机会，在互联网这条伟大的航路上，游戏行业绝对是你值得上的船！

我们在一个最好的时代，任何足够优秀的产品都会被足够多的人热爱！

腾讯公司副总裁

姚晓光

推荐序二

早高峰的地铁上，一名上班族虽然被人群挤压着，可还是艰难地举着手来玩游戏；校园的一个寝室里，室友们大呼小叫，联机到深夜，也在玩游戏；现在，3 岁的孩子都会趁大人不玩手机的间隙，熟练地解锁手机来玩手机游戏；甚至与你相隔千里、上了年纪的爸爸妈妈，打电话给你就是为了问他们玩游戏时遇到的问题……游戏已经无差别地进入无数人的生活中，就像吃饭、睡觉一样，每日必做，不可或缺。

随着这些年来游戏政策的解禁、游戏舆论的改变及游戏玩家的成长，从各种意义上讲，玩游戏都成为一种再正常不过的全民娱乐方式了。相应地，从事游戏行业也不再是不务正业，这不仅是一份正经工作，更是一份可以为别人创造快乐和回忆、为自己实现理想和价值的创意性职业。

作为较早入行的游戏人，我非常欣喜地看到有这么多年轻人热爱游戏，想把做游戏作为自己的职业。这些年轻的准游戏人，比我们当年有更多的玩游戏经验，比我们当年有更扎实的游戏科班知识，比我们当年有更广阔的眼界与冲劲。当他们成长为游戏行业的中坚力量时，一定会创造出更多、更有趣、更天马行空和更令人惊叹的作品。未来的游戏是什么样子的，在什么硬件平台上玩，用什么交互方式操作，我无法预测。现在行业里最新潮的 VR、AR 游戏，在游戏历史的长河中，也许只是一个片断。游戏的未来充满了未知的机会和无限的可能。

腾讯游戏的诸位资深专家，毫无保留地贡献了自己的工作经验，编写了这套“GAD 游戏学院系列丛书”，希望这套丛书能帮助各位准游戏人打开游戏世界的大门。游戏的新世界，由你们来创造！

腾讯公司副总裁

陈宇

前　言

随着电子游戏的快速发展，特别是网络游戏的兴起，游戏虚拟社交、PVP 系统、团队协作及高价值的游戏经济系统让游戏真正成为一个虚拟世界。为了不让这个虚拟世界成为法外之地，我们需要建立一套完整的游戏安全体系来解决其中可能面临的安全问题。例如：游戏外挂带来的游戏公平性问题、盗号木马引发的密码泄露和游戏虚拟财产损失、打金工作室对游戏经济系统的冲击等。游戏越流行，对安全的需求就越强烈。通过在《地下城与勇士》《穿越火线》《天天酷跑》等游戏中长期积累的安全运营实战对抗经验，腾讯游戏安全团队不断完善游戏安全系统，并希望通过编写一系列游戏安全书籍（本书是其中之一）来沉淀和分享我们的经验。

游戏外挂是最突出、最难以解决的游戏安全问题。游戏设计上的安全缺陷、服务器校验的缺失及特定的游戏玩法等都可能引入容易被外挂利用的游戏安全漏洞。对于外挂问题，我们几乎不可能通过一套安全系统彻底解决，往往需要长期的持续运营，对于代理的海外游戏更是如此。除了反外挂系统的开发，在游戏研发中如何提升游戏的基础安全性，在运营中如何建立高效的外挂监控、打击流程，如何训练检测模型并结合各种处罚手段来提高使用外挂的门槛，等等，这些都是我们在实际运营中必须要考虑的问题。

腾讯游戏安全团队从 2013 年开始，随着微信、手 Q 游戏平台的建立，启动了筹备移动游戏反外挂的方案。早期上线的休闲类游戏虽然通过外挂获取的收益不高，但由于用户群庞大，而且早期游戏的基础安全性不高，所以热门游戏还是经历了一波外挂的强烈攻势。从最原始的内存修改器发展到专用外挂、内含外挂逻辑的重打包游戏安装包，虽然外挂的使用量已经回落到很低的水平，但是对抗仍然在持续。现在，外挂反对抗的手段不断复杂化，表现出直接对抗安全方案的特点，未来可能趋向于 PC 端的更加复杂的外挂对抗形式。随着移动游戏玩法不断重度化的发展趋势，游戏领域

势必会引入更多的 PVP 玩法及更自由的游戏虚拟财产交易模式，移动游戏反外挂对抗任重道远。

知己知彼，百战不殆。反外挂系统具备很强的实战性，为了更深入地理解反外挂系统，我们首先要充分了解外挂的开发流程和工作原理。作为游戏安全领域的入门书籍，本书介绍了移动游戏平台的外挂开发所需要的工具和技能，并梳理了必要的知识框架。希望本书能够为对客户端安全技术、游戏安全技术感兴趣的在校学生及初学者打开游戏安全技术的大门，也欢迎大家通过 GSLAB.qq.com 平台来交流和分享关于游戏安全攻防相关的经验和心得。

本书内容导读

本书以深入浅出的方式讲解了手游安全领域涉及的移动端安全技术，重点讲解手游外挂技术，并提供部分源代码给读者使用，源代码的下载地址为 http://gad.qq.com/article/detail/7158994。本书分为 6 篇，共计 21 章，以下是对各篇内容的简要介绍。

第 1 篇　概述篇（第 1 ~ 3 章）

概述篇首先介绍了手游面临的安全风险；然后讲解了什么是外挂，并对常见的外挂进行分类和介绍；最后汇总了手游外挂涉及的安全技术。

第 2 篇　环境搭建篇（第 4 ~ 6 章）

环境搭建篇首先介绍了移动端开发环境的搭建过程，包括：Android 平台开发环境搭建、iOS 平台非越狱和越狱开发环境搭建；然后介绍了调试环境的搭建过程，包括：Android 平台 IDA 调试环境搭建、iOS 平台 32 位 GDB 调试环境搭建、iOS 平台 64 位 lldb 调试环境搭建；最后介绍了手游安全领域中常用工具的基本使用方法。

第 3 篇　游戏基础篇（第 7 ~ 9 章）

游戏基础篇讲解了入门手游安全所需掌握的游戏基础知识，包括：游戏开发基础知识、引擎的概念、常见引擎简介、游戏漏洞概述及不同游戏类型的漏洞风险分类。

第 4 篇　逆向篇（第 10 ~ 11 章）

逆向篇从静态分析和动态分析两方面展开：静态分析介绍了 ARM 汇编的基础知

识、Android 平台的 ELF 文件格式、iOS 平台的 Mach-O 文件格式及 IDA 静态分析；动态分析介绍了 Android 平台的 IDA 动态调试、iOS 平台的 GDB 和 lldb 动态调试。

第 5 篇　开发篇（第 12 ~ 17 章）

开发篇剖析了在手游外挂开发过程中涉及的安全技术的实现原理，并提供代码配合讲解，干货十足。其中剖析的安全技术包括：注入、Hook、内存篡改、进程信息获取及反调试。

第 6 篇　实战篇（第 18 ~ 21 章）

实战篇首先讲解了不同类型的游戏的分析和破解方法，并且通过实例剖析了各种类型的游戏的分析方法；其次通过实例讲解了手游外挂的分析过程；然后以《2048》游戏为实例，对游戏通关功能进行了分析，并对快速通关的作弊功能进行了实现；最后讲解了 Unity 3D 引擎的逆向分析，包括：Unity 3D 引擎在 iOS 和 Android 平台下逻辑代码的编译处理原理、Unity 3D 引擎的 AssetBundle 机制的实现原理及《天天来战》游戏的 AB 包破解过程。

致谢

感谢 GAD 游戏学院组织并提供了这样一个写作平台，感谢电子工业出版社博文视点提供了优质的出版平台，感谢所有在本书撰写过程中给予我们帮助和指导的小伙伴们，感谢腾讯互娱的各位领导对这次图书写作工作的重视和支持。

腾讯游戏研发部游戏安全中心

目 录