网络空间安全专业规划教材

总主编◎杨义先　　执行主编◎李小勇

移动应用安全分析

Mobile Application Security Analysis

王浩宇　徐国爱　郭　耀　著

北京邮电大学出版社
www.buptpress.com

网络空间安全专业规划教材

总主编　杨义先　　执行主编　李小勇

移动应用安全分析

王浩宇　徐国爱　郭　耀　著

北京邮电大学出版社
www.buptpress.com

内容简介

在移动智能终端和多样的移动应用给用户带来便利的同时，移动平台上各种新的安全与隐私问题也日益凸显。本书从多个维度对移动应用安全分析的相关技术进行全面系统的介绍，包括基本技术原理、工具使用、学术前沿成果、技术应用场景示例，以及研究挑战和未来方向等。第1章对移动安全领域所需掌握的研究背景知识进行简要概述；第2章介绍移动应用安全分析基础，包括常用的分析技术和分析工具；第3～6章主要介绍静态分析技术的原理和基本应用；第7章介绍移动应用动态分析技术，包括动态沙箱和自动化测试技术；第8章以移动应用广告安全分析为实例，介绍如何将静态分析技术与动态分析技术相结合来解决研究中的问题；第9章介绍如何结合移动应用分析以及系统优化来解决安全问题和防范隐私泄露；最后，第10章对移动应用安全分析领域的研究挑战与未来方向进行总结。

本书可作为计算机、网络与信息安全专业方向的高年级本科生及研究生的教材，或作为相关研究人员及爱好者的参考书。

图书在版编目(CIP)数据

移动应用安全分析 / 王浩宇，徐国爱，郭耀著. -- 北京 ：北京邮电大学出版社，2019.8
ISBN 978-7-5635-5796-7

Ⅰ. ①移… Ⅱ. ①王… ②徐… ③郭… 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(2019)第 161460 号

书　　名：移动应用安全分析
作　　者：王浩宇　徐国爱　郭　耀
责任编辑：毋燕燕
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京玺诚印务有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：10.5
字　　数：273 千字
版　　次：2019 年 8 月第 1 版　2019 年 8 月第 1 次印刷

ISBN 978-7-5635-5796-7　　定价：26.00 元

Prologue 序

Prologue

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战，促使我们必须以超常规手段来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下2014年规划该学科的相关情况，并结合现状，坦诚一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统（各种智能终端）、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全，研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科，下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等内容。

方向2，密码学及应用，为后三个方向（系统安全、网络安全和应用安全）提供密码机制；它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向3，系统安全，保证网络空间中单元计算系统的安全；它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向4，网络安全，保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全；它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等内容。

方向5，应用安全，保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用；它主要研究关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看，网络空间安全一级学科主要由五个模块组成：网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块1，网络空间安全基础知识模块，包括：数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块2，密码学基础理论知识模块，包括：对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块3，系统安全理论与技术知识模块，包括：芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块4，网络安全理论与技术知识模块，包括：通信网络安全、无线通信安全、IPv6安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块5，应用安全理论与技术知识模块，包括：Web安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业，至少应该平等地

包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我们当初只重点考虑了信息安全专业，所以，就留下了一些遗憾，甚至空白，比如，信息安全心理学、安全控制论、安全系统论等。不过值得庆幸的是，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平，从20世纪80年代初至今，已有30余年的全方位积累，而且，一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。本套系列教材主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据安全与隐私保护》《数字内容安全》《量子计算与后量子密码》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理(第3版)》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络空间安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科提供更有力的支撑。

杨义先

教授、长江学者

国家杰出青年科学基金获得者

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

前言

Foreword

Foreword

随着移动互联网时代的到来，移动智能终端快速发展。在移动智能终端和多样的移动应用给用户带来便利的同时，移动平台上各种新的安全与隐私问题也日益凸显。一方面，移动平台的恶意软件增长迅速，这些恶意软件会在用户不知情的情况下，从事恶意扣费、系统破坏、隐私窃取等恶意行为，给用户带来经济损失，造成隐私泄露风险等问题。另一方面，很多移动应用的行为与用户的隐私信息十分相关，由于智能手机上储存着用户的各种隐私信息（如联系人、银行账户、照片、地理位置信息等），这些信息很容易被移动应用所获取。因此，移动平台上的安全与隐私问题更为用户所关注。

本书对移动应用安全分析的相关技术进行全面系统的介绍，包括基本的技术原理、主流工具的使用、学术前沿成果、丰富的技术应用场景示例，以及研究挑战和未来方向。本书涵盖的研究内容包括移动应用隐私分析、第三方库检测和安全分析、应用重打包检测、基于元信息的安全分析、动态分析、广告安全分析和细粒度隐私保护等移动安全领域主流研究方向。

本书第 1 章对移动应用生态系统中存在的安全和隐私问题进行简要综述，作为移动安全领域的研究背景。第 2 章作为移动应用分析的基础，对 Android 虚拟机、Android 安全机制、APK 的基本组成、移动应用的常用分析技术和分析工具进行了详细介绍。第 3～5 章主要介绍静态分析技术，其中第 3 章主要介绍 Android 平台上的权限问题以及权限机制优化的相关研究，第 4 章着重介绍了移动应用中第三方库的检测方法，第 5 章介绍了移动应用重打包检测的方法和工具使用。第 6 章对基于元信息的移动应用安全分析技术进行总结并介绍如何结合自然语言处理和程序分析技术进行安全检测。第 7 章介绍移动应用动态分析技术，包括动态沙箱和自动化测试技术。第 8 章以移动应用广告安全分析为实例，介绍如何将静态分析技术与动态分析技术相结合来解决研究中的问题。第 9 章介绍如何结合应用分析以及系统优化来解决移动应用中的安全漏洞和隐私泄露问题。最后，作者在第 10 章对移动应用安全分析领域的研究挑战与未来方向进行了总结。

读者通过本书的学习，可以了解移动安全前沿研究内容和方向，掌握移动应用分析基础，搭建自己的移动应用安全分析环境，实现和改进现有的分析技术，结合多种分析工具来解决实际的移动安全问题。

本书作为网络空间安全专业的教材，主要面向的读者包括计算机、网络与信息安全专业方向的高年级本科生及研究生。由于本书中引用了大量前沿的学术成果以及总结了相关研究问题和挑战，本书也适用于移动安全和软件分析等相关领域的研究者、从业人员及爱好者等学习参考。

本书在编写过程中参考和引用了大量的移动安全领域国内外专家和学者的研究成果，在此谨向所有专家、学者以及参考文献的编著者表示衷心的感谢！本书在编写过程中得到了很多专家和同行们的鼎力相助，感谢北京大学陈向群教授、北京邮电大学张森副教授等为本书提供的宝贵建议。本书中也包含了作者的很多研究成果，在此向所有的研究合作者包括陈向群教授、董枫博士、李承泽博士、李元春博士、马子昂、王靖瑜等表示感谢！最后，感谢董枫、杨昕雨、张程鹏、胡阳雨、刘天铭等同学对部分章节进行校对和帮助，加快了本书的顺利完成！

本书是作者多年来的成果以及集体智慧的结晶，本书已经尽力覆盖移动应用安全分析的方方面面，但书中内容还不尽成熟，难免有错漏之处，恳请读者批评指正。

目录

Contents

Contents

第 1 章

绪　论

近年来移动智能终端快速发展，智能手机已经融入人们的日常生活中。在移动智能终端和移动应用给用户带来便利的同时，移动平台上各种新的安全和隐私问题也日益凸显。一方面，移动平台的恶意软件(malware)增长迅速，这些恶意软件会在用户不知情的情况下，从事恶意扣费、系统破坏、隐私窃取等行为，给用户带来经济损失和隐私泄露问题。仅 2018 年 360 互联网安全中心就检测到超过 400 万个恶意应用，共感染 1.1 亿人次，大部分恶意应用存在资费消耗和恶意扣费等行为，恶意应用呈现家族化趋势。另一方面，虽然很多移动应用不属于恶意应用，但是其行为与用户的隐私信息十分相关，例如获取用户的联系人信息和地理位置信息用于定制化广告服务、第三方分析或者其他跟应用功能相关的服务等。智能手机上储存着用户的各种隐私信息(如联系人、银行账户、照片、地理位置信息等)，这些信息很容易被应用所获取，因此移动平台上的安全与隐私问题更为用户所关注。

本章将对移动应用生态系统中的安全和隐私问题进行简要综述，作为移动安全领域的研究背景。而在后续章节中会对部分安全问题进行展开介绍，主要从研究角度来讲述相关研究领域的发展现状、常用技术和工具使用。

1.1　移动应用生态系统

如图 1-1 所示，数十亿的移动应用用户，上千万的移动应用，数以百万计的移动应用开发者，上万种定制化手机和操作系统，以及数以千计的移动应用分发渠道，共同组成了庞大的移动应用生态系统。

图 1-1　移动应用生态系统的组成部分

(1) 移动终端用户:截至 2017 年,全球移动终端用户数量已经超过 50 亿,其中超过一半的用户是智能手机用户,这些用户是移动应用生态系统中的强大驱动力。

(2) 移动应用:移动应用发展飞速,目前 Google Play 和 iOS App Store 中均有超过两百万的移动应用。根据 App Annie 的报告,移动应用产业规模预计将在 2021 年达到 6.3 万亿美元的规模。

(3) 移动应用开发者:目前有超过 12 00 万名移动应用开发者,其中超过一半的开发者关注于 Android 生态系统,包括正常的开发者和恶意开发者。

(4) 手机和操作系统:移动平台主要包括 iOS 和 Android 两大生态系统。iOS 作为封闭的操作系统,在系统更新、安全防护方面具有优势。而 Android 作为一个开放的平台,各种手机厂商和开发者都可以对系统进行定制化,因此系统版本众多,碎片化严重。

(5) 移动应用分发渠道:移动应用有着多种分发渠道。对于 iOS 应用,用户主要从 iOS App Store 进行应用下载和安装,由于应用市场有着较强的应用审查机制,因此恶意应用较难进入 iOS 应用市场来感染用户。而对于 Android 应用,除了 Google Play 官方市场,用户还可以从各种第三方市场和论坛网站等分发渠道进行应用的下载。据不完全统计,Android 应用至少有数千种不同的分发渠道,而这些分发渠道也带来很多安全隐患。此外,很多应用可以通过移动广告渠道进行传播。

整个移动应用生态系统庞大且复杂,存在大量的安全漏洞和隐私泄露问题亟待解决。因此,近些年来移动应用安全问题广泛受到学术界的关注。

从终端用户角度出发,由于大部分的安全问题都是由于终端用户没有安全意识造成的,因此很多研究关注于如何帮助终端用户更好地理解应用的隐私行为(如分析隐私信息使用意图以及对应用进行隐私评级),如何鉴别危险应用和区分可靠的应用分发渠道,以及如何避免安全漏洞带来的风险。

从移动应用角度出发,海量应用中存在各种安全威胁,包括恶意应用、盗版应用、欺诈行为、安全漏洞和隐私风险等,如何发现并检测新的安全威胁一直是学术界研究的热点。

从应用开发者角度出发,由于大部分安全和隐私问题都能够追溯到开发者,因此如何帮助开发者构建更安全的移动应用,以及如何检测恶意及垃圾开发者是很多研究关注的内容。

从手机和操作系统角度考虑,系统碎片化现象导致了严重的安全漏洞和兼容性问题,很多研究关注于如何对系统进行优化来解决这些问题。此外,如何在智能终端运行不可靠的应用以及对应用行为进行细粒度的访问控制限制,也是移动安全领域研究的重点。

从应用分发渠道考虑,由于应用市场中具有海量应用,如何对应用市场进行安全风险评估,以及如何对海量应用进行快速分析和检测,也是研究的重点。

本书主要关注于 Android 平台的安全和隐私问题,原因如下:(1)Android 是一个开放并且被广泛使用的操作系统平台。截止到 2018 年,Android 拥有移动市场超过 88%的占有率。同时,由于 Android 系统的开源性,研究者可以在 Android 平台上修改代码或构建原型系统进行实验验证,而且 Android 应用比较容易下载及分析。(2) Android 平台的安全和隐私问题相对严峻。移动平台上超过 97%的恶意软件都是针对 Android 平台,同时 Android 平台上权限滥用以及隐私泄露的情况普遍存在。因此,本书在后续章节进行介绍时,不加特殊说明的情况下,移动应用及应用均指 Android 移动应用。但本书中所涉及的安全分析技术较为通用,其相关原理和思想也可用于 iOS 平台移动应用的安全分析场合。

1.2 移动应用生态系统中的安全和隐私威胁

移动应用生态系统中的安全和隐私威胁总体来看主要包括三部分：安全漏洞、恶意软件和隐私泄露。

1.2.1 安全漏洞

移动平台的安全漏洞可以划分为系统级漏洞(内核漏洞)和应用级漏洞。

1. 系统级漏洞

由于 Android 系统的开放性，在系统的演化过程中不断被曝出很多严重的安全漏洞。从 CVE 统计上来看，2017 年和 2018 年发现漏洞最多的前五款软件产品如表 1-1 所示。可以看到，Android 系统一直属于存在漏洞最多的系统之一。系统级漏洞给智能终端带来巨大的安全威胁。

一方面，很多系统级漏洞属于 Root 提权漏洞，能够被恶意利用获得高风险的权限，进行控制手机。在 Android 系统的发展中，出现过很多知名的提权漏洞，包括 CVE-2009-2692(由 sock_sendpage 方法的空指针解引用造成)，CVE-2011-3874(由 libsysutils.so 中的栈溢出问题造成)，CVE-2012-0056，CVE-2011-1823，CVE-2012-4220，CVE-2013-6282，CVE-2014-3153，CVE-2015-3636 等，感兴趣的读者可以深入了解。

另一方面，系统级漏洞也对移动应用本身带来很多安全问题，即使应用本身并不存在恶意行为。例如，Android 系统中的签名漏洞不断被曝出，包括早期的三个 Master Key 漏洞、FAKE ID 漏洞和后来的 Janus 漏洞等。这些漏洞会导致使用 Android V1 签名机制(本书第 2 章会对签名机制详述)的应用出现严重的安全隐患，能够被攻击者恶意修改而不影响应用本身签名。

表 1-1 漏洞最多的软件系统①

2017 年出现漏洞最多的软件系统(基于 CVE 统计)			
软件系统	厂商名称	类型	漏洞数目
Android	Google	操作系统	842
Linux Kernel	Linux	操作系统	454
iPhone OS	Apple	操作系统	387
Imagemagick	Imagemagick	应用	357
Mac OS X	Apple	操作系统	299
2018 年出现漏洞最多的软件系统(基于 CVE 统计)			
Debian Linux	Debian	操作系统	950
Android	Google	操作系统	611
Ubuntu Linux	Canonical	操作系统	494
Enterprise Linux Server	Redhat	操作系统	394
Enterprise Linux Workstation	Redhat	操作系统	378

① https://www.cvedetails.com/top-50-products.php?year=2017

2. 应用级漏洞

即移动应用本身存在的安全漏洞，一方面包括通用的加密漏洞、随机数漏洞、SQL 注入漏洞等，另一方面也包括 Android 应用所特有的组件交互漏洞和 WebView 远程代码执行漏洞等。由于移动终端进行漏洞利用的特殊性，近年来也出现很多组合攻击漏洞，例如“应用克隆”漏洞。近年来移动应用的安全事件中，超过一半都是由于应用本身的缺陷和漏洞造成的。

应用级漏洞可以由应用本身代码引入，也可以由应用嵌入的第三方库引入。Android 应用开发者绝大多数都是小型公司和独立开发者，往往缺少大公司常备的代码审计和代码安全规范检查，也缺乏足够的安全编程意识，使得 Android 应用的安全隐患尤为严重。此外，即使一些大公司开发的应用和 SDK 中也经常存在高危安全漏洞。例如，百度 MOPLUS 第三方 SDK 中的高危漏洞“虫洞”(Wormhole)影响了上万个流行应用以及数百万用户，该漏洞允许 APP 在未经用户授权情况下安装运行其他 APP、推送页面通知、访问修改联系人、得到位置信息、发送仿冒短信等。Facebook 和 Dropbox 等应用也都曾被发现存在严重的安全漏洞。因此，移动平台的漏洞风险影响很大，漏洞检测和验证的研究至关重要。大量研究工作提出通过静态分析、模糊测试、深度学习等技术进行自动化程序漏洞挖掘，但自动化漏洞检测的误报率相对较高，需要大量人工进一步进行漏洞机理分析。

1.2.2 恶意软件(恶意应用)

近年来，移动平台恶意应用增长飞速，并且不断出现新型恶意应用和攻击手段。根据《移动互联网恶意代码描述规范》定义，移动应用的主要恶意行为包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈、流氓行为八大类，如表 1-2 所示。除了传统的恶意载荷(malicious payload)以外，移动平台也出现了各种新型恶意应用。例如，勒索应用在近年来成爆发趋势，挖矿木马随着区块链的兴起也逐渐增多，各种仿冒应用和克隆应用源源不断。

恶意应用传播的主要方式是应用重打包，即通过反编译合法应用，植入恶意代码，重新编译并打包应用的方式。研究表明，超过 80%的恶意应用都是通过重打包方式传播。此外，很多恶意应用家族通过应用更新时传播。即在安装之后，应用通知用户有新的版本，当用户安装更新后，新的版本包含恶意功能。著名的 DroidKungFu 恶意应用家族即通过这种方式传播。因此，Google Play 要求其市场中的应用在发布之后，只能通过 Google Play 升级应用，而不能通过应用的本地服务器进行更新。但国内市场中的大部分应用还是可以通过本地更新。此外，还有很多恶意应用通过偷渡式下载(drive-by download)方式传播，即很多正常应用中可能嵌入恶意的广告来传播恶意应用。

近年来，大量的研究工作针对移动平台恶意应用进行检测，提出了包括基于静态行为特征、动态信息流分析、机器学习等各种方法的检测技术。然而，恶意应用也存在大量的对抗手段，包括字符串混淆、API 反射、攻击代码动态加载、攻击方式本地化(隐藏于 native 代码)、应用加壳、反调试等各种方式，给恶意应用的检测增大了难度。