移动互联网安全丛书

移动终端安全

关键技术与应用分析

Mobile Security

Key Technology and Application Analysis

张 滨/赵 刚/袁 捷/胡入祯
邱 勤/徐 扬/董 航/唐 勇 编著

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

移动互联网安全丛书

移动终端安全
关键技术与应用分析

Mobile Security
Key Technology and Application Analysis

张 滨/赵 刚/袁 捷/胡入祯
邱 勤/徐 扬/董 航/唐 勇 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

移动终端安全关键技术与应用分析 / 张滨等编著
. -- 北京 : 人民邮电出版社, 2015.6
（移动互联网安全丛书）
ISBN 978-7-115-38359-4

Ⅰ. ①移… Ⅱ. ①张… Ⅲ. ①移动终端－安全技术
Ⅳ. ①TN929.53

中国版本图书馆CIP数据核字(2015)第021674号

内 容 提 要

本书全面介绍了移动终端安全技术，内容新颖，理论知识与实际案例并重。本书由浅入深、由概括到具体地讲解了移动终端的安全体系结构、安全防护技术与安全管理方案，涵盖终端安全基础知识、安全体系架构、操作系统安全机制、应用软件分析与保护技术，以及终端安全管理标准和工具等。

本书适合移动互联网从业人员、IT 技术人员、咨询分析师、科研人员以及其他对终端安全感兴趣的人士阅读。

◆ 编　　著　张　滨　赵　刚　袁　捷　胡入祯　邱　勤
　　徐　扬　董　航　唐　勇
责任编辑　代晓丽
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
固安县铭成印刷有限公司印刷
◆ 开本：700×1000　1/16
印张：11　　2015 年 6 月第 1 版
字数：215 千字　　2015 年 6 月河北第 1 次印刷

定价：55.00 元

读者服务热线：(010)81055488　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

前　言

在移动互联网高速发展的今天，通过智能终端呈现的丰富应用深刻地影响着人们衣食住行的方方面面。从出门查询交通路线，到理财、购物，再到运动、睡眠情况记录，移动终端应用给人们带来了巨大的便利。与此同时，终端安全问题也日益突出，成为社会关注的重点。

我国政府高度重视移动终端安全管理，已经出台“加强移动智能终端进网管理”“打击治理移动互联网恶意程序”“做好应用商店安全检查”等多项要求，取得了一定成效。但是近年来，移动终端安全事件仍呈高发态势。CNCERT 在 2014 年上半年新收录恶意程序 36.7 万个，较 2013 年同期增长 13%。2014 年“七夕”节当天，一条疯狂群发恶意程序链接的手机病毒“××神器”在安卓手机间通过短信大肆传播，不到一天时间感染上百万部手机，广大用户人心惶惶。2014 年 9 月，“好莱坞艳照门”震惊全球，相关报告指出，黑客利用苹果手机 Find My iPhone 的漏洞攻击了 iCloud 账户，从而成功盗取欧美女星存储在个人苹果手机上的照片、视频等内容。

移动终端安全关系到用户财产安全、个人信息安全、企业信息安全，甚至国家安全。移动终端安全的维护需要国家、行业、厂商和用户各个层面的共同努力。芯片、终端、操作系统、应用软件厂商提高技术安全标准能够从源头上减少终端安全威胁，政府部门立法和监管能够有效打击不法分子破坏终端安全的行为，电信运营企业在网络侧封堵恶意程序链接是截断病毒传播渠道的重要手段，用户提高安全使用意识则是终端安全的最后一道防线。

本书作者不仅参与了电信行业终端安全相关标准的制定、电信运营商对终端安全环境的治理，还承担了 SIM 卡防复制、手机不良信息治理、终端操作系统漏洞分析、应用软件测评加固、移动设备管理（MDM）等技术的研究和应用，在长期实践中形成了较全面的终端安全视角。本书理论知识与实际案例并重，详细分析了智能终端软/硬件层面的安全风险，并系统介绍了相关安全管理要求、行业标准和关键技术，希望能够帮助读者由浅入深地了解终端安全的技术现状和发展趋

势，同时为企业加强终端安全管理、做好终端安全防护提供帮助。

在本书的撰写过程中，中国移动信息安全管理与运行中心终端测评工作组、中国移动研究院张峰博士、中国移动设计院陈涛博士向作者提供了宝贵的数据素材，在此向他们致以诚挚的感谢!

由于作者水平有限，书中不当之处恐难避免，敬请广大读者批评指正。终端安全技术发展日新月异，作者愿与广大读者深入交流、共同进步。

作　者

2014 年 10 月

目　录

第1章 背 景

移动终端具有隐私性、智能性、便携性、网络连通性，已成为我们日常工作、生活的重要工具。在移动终端推动移动互联网快速发展的同时，移动终端安全问题也日益严峻，引起社会的广泛关注。本章主要介绍移动互联网的发展现状、智能终端对移动互联网发展的影响以及移动智能终端面临的安全形势。

1.1 移动互联网的发展现状

移动互联网结合了移动通信随时随地的接入能力和互联网强大的创新业务能力，为移动用户提供移动接入方式和互联网服务。伴随着移动通信和互联网融合的扩大和深入，移动互联网为用户提供更具移动特性、更丰富多彩的应用服务。如图1-1 所示，从每天早晨的天气指数，到出行路上的交通路况，再到“吃货”必备的美食搜索，甚至是购物、理财……移动互联网应用对于个人生活已是无孔不入。

图 1-1 移动互联网应用于生活的方方面面

工业和信息化部发布的《2013 年通信运营业统计公报》[1]显示，2013 年，我国互联网网民数净增 5 358 万人，达 6.81 亿人，互联网普及率达到 45.8%，比 2012 年提高 3.7 个百分点。手机网民规模达到 5 亿人，比 2012 年增加 8 009 万人，网民中使用手机上网的人群占比由 2012 年的 74.5%提升至 81%，如图 1-2 所示。手机即时通信、手机搜索、手机视频和手机网络游戏用户规模比 2012 年分别增长 22.3%、25.3%、83.8%和 4.5%。电子商务应用在手机端应用发展迅速，手机在线支付用户在手机网民中占比由 2012 年年末的 13.2%上升至 25.1%。

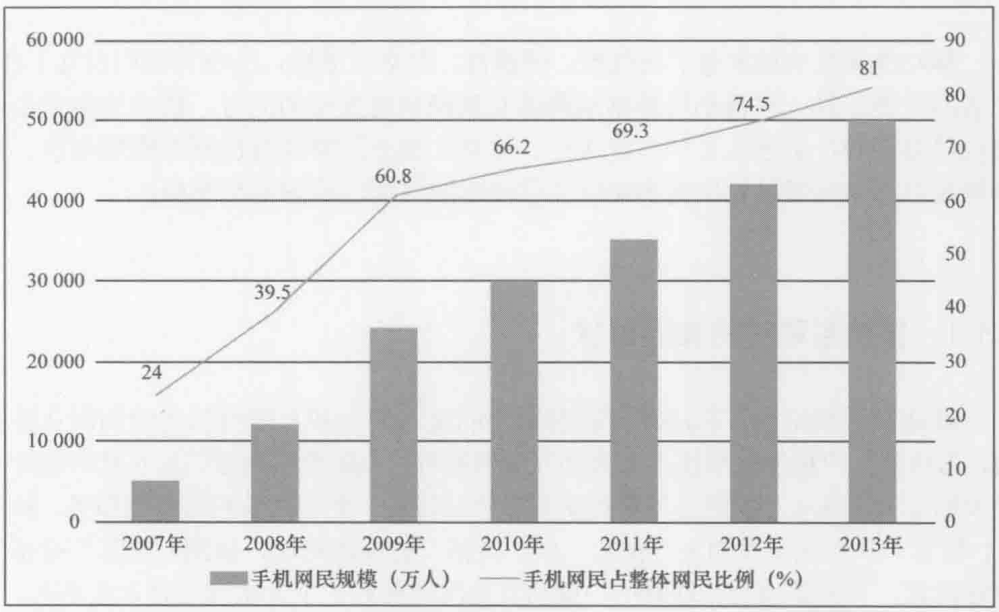

图 1-2　手机网民规模及比例变化情况（2007~2013 年）[1]

在移动互联网行业中，与传统行业有较大区别的一点就是应用商店。随着移动互联网行业时代到来，作为用户进入移动互联网的重要入口之一，移动应用商店在移动互联网的产业链中占有举足轻重的位置。苹果 App Store 首创移动应用商店模式，无论从盈利方面还是从影响力方面来讲都获得了巨大的成功。此后的许多系统提供商、终端生产厂商和一些互联网公司纷纷加入移动应用商店的市场竞争[2]。从苹果发布 App Store 开始，到后来谷歌推出的 Android Market（后更名为 Google Play）和微软推出的 Windows Marketplace（后更名为 Windows Phone Store），移动互联网中的应用程序基本上是通过应用商店下载的，全球四大移动应用商店的特点对比见表 1-1。

表 1-1 四大移动应用商店对比[3~6]

应用商店	提 供 商	创建时间	应用收入分成	终端操作系统
Ovi Store	Nokia	2009 年 2 月	应用开发者 70%；其他 30%	控制终端操作系统 Symbian
App Store	Apple	2008 年 7 月	应用开发者 70%；Apple 30%	控制终端操作系统 iOS
Android Market	Google	2008 年 10 月	应用开发者 70%；手机服务运营商 30%	支持推动终端操作系统 Android 的发展，但无法控制
Windows Marketplace	Microsoft	2009 年 2 月	应用开发者 70%；其他 30%	控制终端操作系统 Windows Phone

当前移动市场上的主流操作系统 Android、iOS、Windows Phone 及 Symbian 均通过官方应用商店为终端用户提供应用程序分发服务，截至 2014 年 3 月，苹果 App Store、谷歌 Google Play 中的应用程序数量均已经突破百万[3, 4, 7]，微软 Windows Phone Store 和诺基亚 OVI 商店中的应用程序数量则分别达到 24 万[5]和 12 万[6]。在应用下载量上，App Store 下载量突破 600 亿，Google Play 已超过 750 亿，在移动平台应用程序中，Android 与 iOS 系统占据了明显的优势。

根据苹果 App Store、Google Play、App Annie、亚马逊 App Store 及 Windows Phone 应用商店截至 2014 年 8 月的公开数据统计，Facebook、WhatsApp、微信、Youtube、TED 等 66 个非游戏类应用正在全球范围内流行，持续时间都超过 1 年。这些应用涉及社交、视频、音乐、拍摄、咨询、出行、购物等类别，几乎同时满足人性多种底层的高频需求，包括但不限于满足提升存在感、成长、娱乐、人际沟通、节约时间、节约金钱、获取信息、安全需求等[2]。

1.2 移动互联网终端的发展现状

移动互联网环境下，终端出现了便携化、智能化的发展趋势。一方面，手机等便携式设备成为人们上网的主要工具，2013 年中国手机网民占整体网民的比例达 81%。另一方面，智能终端超过传统的非智能终端，成为手机的主流形式。根据美国市场研究公司 IDC 的报告，2013 年全球智能手机出货量达到 10.04 亿部，较 2012 年增长了 38.4%，而非移动智能终端出货量仅为 8.2 亿部，同比下滑了 22%。在中国，无论是增速还是市场占有率方面，智能终端已成为国内移动终端市场主体。2013 年 1～11 月，智能终端出货量为 3.47 亿部，同比增长 76.8%，占有率升至 72.7%，如图 1-3 所示。

图 1-3　2009～2013 年智能终端出货量及占比

移动终端的智能性主要体现在 4 个方面：其一是具备开放的操作系统平台，支持应用程序的灵活开发、安装及运行；其二是具备 PC 级的处理能力，可支持桌面互联网主流应用的移动化迁移；其三是具备高速数据网络接入能力；其四是具备丰富的人机交互界面，即在 3D 等未来显示技术和语音识别、图像识别等多模态交互技术的发展下，以人为核心的更智能的交互方式。

伴随着终端技术和移动通信技术的飞速发展，智能终端的形态和应用呈现多样化趋势。智能终端的产品形式从当初的 PDA 发展到今天，出现了智能手机、平板电脑、可穿戴设备等多类产品。与此同时，终端与应用整合迈向了新高度[8]，带来了空前的用户体验。从 iPhone 4S 智能语音识别 Siri 功能到可穿戴设备人体运动感应功能，都是软硬件一体化的典型案例。随着终端软硬件技术的进一步融合发展，应用程序能够更加自如地调用应用处理器、图像编解码芯片、显示屏、传感器、摄像头等在内的多类终端硬件能力，而增强现实及普适交互类新型应用正逐步走入我们的生活。

1.3　智能终端对移动互联网发展的影响

伴随着移动互联网的飞速发展，网络通信、应用服务、终端设备及其商业模式等均发生了颠覆性的变革，移动智能终端业已成为整个产业竞争的战略制高点和核心平台，对产业发展产生了深远影响。移动智能终端引领了信息通信产业几乎所有关键要素的发展，是移动互联网业务的实现载体，也是用户使用运营商业务的最终环节，更是引领运营商业务和用户发展的关键手段。同时，移动智能终端也成为影响运营商市场竞争的首要因素[9]。

国内手机市场已迈入“智能时代”，不仅终端产业本身发生巨变，移动智能终端也引发了整个 ICT 产业的颠覆性变革：互联网式开源、免费的终端系统软件制

造方式、变革性的终端应用软件传播模式、超乎想象的移动交互体验、爆发性的应用、流量和模式创新颠覆了业界对移动终端原有的认知。移动终端引领的制造与服务的一体化创新和跨界融合正深刻地冲击着整个信息通信产业[8]。

智能终端是移动互联网应用的载体，而应用创新引领ICT产业发展新图景。智能终端的发展推动应用趋向多元化繁荣、广范围延伸，在任何时间、任何地点、利用任何终端享有全媒体的信息服务成为业界努力的方向。应用形态多样化扩展，多屏合一、多屏互动等新型业态批量涌现；应用模式不断变革，高价值信息和能力的持续引入，模糊着虚拟与现实的界限，扩展着应用场景和空间，极大地激励了应用创新的发展；移动互联网与物联网融合进一步深化，推动信息技术应用深入到生产、生活的各个领域，影响范围不断扩大。回顾过去，借力快速普及、规模空前的移动智能终端发展浪潮，电子商务、行业应用已成为移动互联网应用的热点。展望未来，二维码、NFC等技术的普及将推动移动支付逐步走向成熟，随着产业规模迅速扩大，移动电子商务将成为今后一个时期整个ICT领域发展的焦点。

1.4 移动智能终端安全形势

在移动智能终端及移动互联网应用高速多元化发展的同时，移动终端安全问题也日益突出，不少安全事件甚至给用户的合法权益造成了严重损害。根据美国安全公司McAfee的数据，2013年全球新增移动恶意程序样本247万个，样本总数较2012年年底增长197%，如图1-4所示，这些恶意程序的传播途径多种多样，包括APP下载、恶意网站访问、垃圾邮件、诱骗短信和含毒广告等[10]。

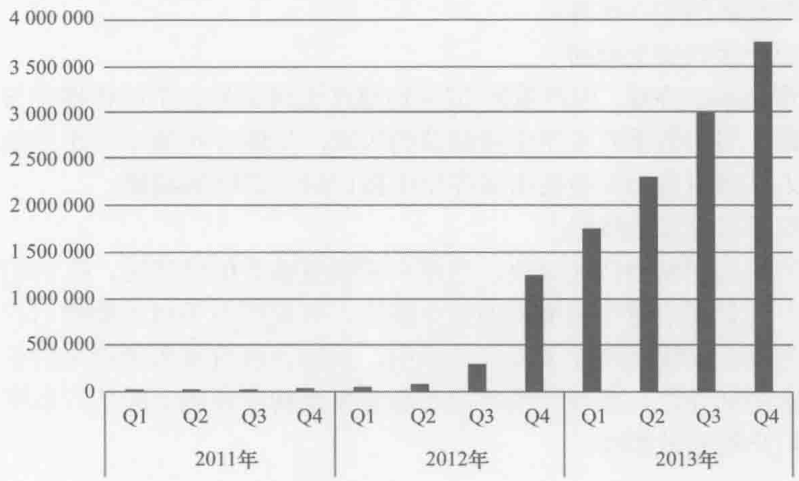

图1-4 全球移动恶意应用数量变化（2011～2013年）[10]

而在我国，CNCERT 于 2013 年捕获移动互联网恶意程序 70.3 万个，是 2012 年的 3.3 倍。2013 年，我国境内感染移动互联网恶意程序的用户数量已超过 200 万。从恶意程序的行为特征上看，恶意扣费类恶意程序数量占 72%，排名第一，其次是资费消耗类、系统破坏类和隐私窃取类，如图 1-5 所示。

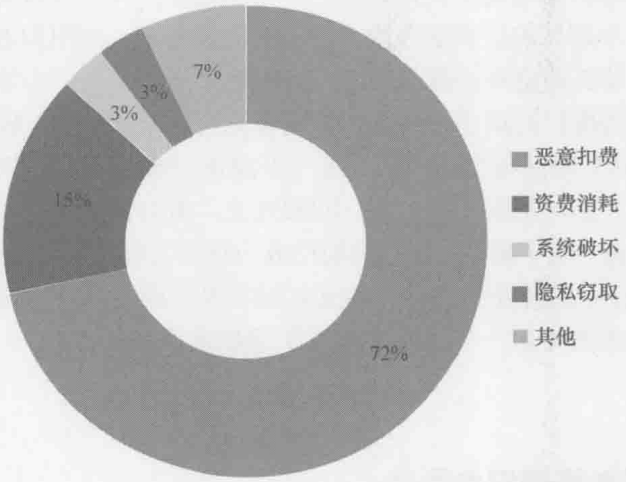

图 1-5　CNCERT 统计 2013 年移动恶意程序行为特征分布[11]

移动恶意程序只是移动智能终端面临的安全威胁之一。移动智能终端不仅承载了传统移动终端的无线通信能力，还具有通用操作系统、接近普通 PC 的强大处理能力、相对固定的 IP 地址、存储大量个人隐私数据、无处不在的移动接入、开放业务平台、海量的应用等特点，可能被不法分子进行信令攻击、数据攻击、数据窃取、资源滥用、计费欺骗等多种渠道的攻击。综合来看，以下 8 个方面的安全风险需要我们加以重视。

（1）空中接口安全威胁

对于移动通信终端，用户数据/信令均通过无线信号在空间传播并与基站进行通信，因此，用户数据有在空中被截获的风险，如图 1-6 所示。用户的通话、短消息等个人私密内容均有被攻击者在空中接口进行窃听的威胁。

（2）信息存储安全威胁

智能终端的更新换代比较快，当用户需要更换智能终端时，在旧的智能终端中存储的个人私密信息有被泄露的安全威胁。目前很多手机在删除用户电话簿、短消息等信息时仅仅是删除了文件的索引，实际并没有覆盖掉原来的信息，当智能终端流落到别处时，就存在被攻击者恶意恢复智能终端上的所有私密信息的风险，导致用户隐私被泄露。

图 1-6 空中接口安全威胁

另外，用户在暂时离开智能终端时，如开会放在会场、上班放在办公桌上，智能终端上的信息（电话簿、短信、日程安排等）就存在被泄露的风险，这可能导致一些商务机密被泄露，从而造成巨大的损失。因此，我们需要研究如何安全存储机密信息，如何控制智能终端内信息不被非法访问。

（3）终端丢失安全威胁

由于智能终端体积较小且一般随身携带，容易丢失或被盗。智能终端中存储的个人私密信息很多，如果被他人获得并利用，则会给用户造成很大的损失。因此需要研究相应的安全机制来保护智能终端在丢失、被盗的情况下个人信息的安全。

（4）数据接入安全威胁

随着技术的不断发展，智能终端接入网络的速度越来越快，这也给智能终端带来巨大的安全威胁。一方面，用户使用各种上网业务越来越便捷、高效，另一方面，通过网络传播病毒的可能性也大大增加。

移动智能终端通过无线网络连接访问互联网络可能访问到携带病毒的网页；玩网络游戏、下载应用程序，都可能造成病毒感染；还有一些业务应用，如彩信等，也可能给智能终端引入病毒。

（5）外围接口安全威胁

很多智能终端具有丰富的外围接口，无线接口有蓝牙、Wi-Fi、红外等，有线接口有 USB 接口等，这些外围接口给智能终端带来了很大的安全威胁。无线接口可能在用户不知情的情况下被非法连通，并进行非法的数据访问和传送，不但造成私密信息的泄露，还可能造成病毒的传播。