nnovative Research

中国联通研究院创新研究系列丛书

移动互联网时代的智能终端安全

李兴新 侯玉华 周晓龙 郭晓花 严斌峰 等 编著

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

nnovative Research

中国联通研究院创新研究系列丛书

移动互联网时代的智能终端安全

李兴新 侯玉华 周晓龙 郭晓花 严斌峰 等 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

移动互联网时代的智能终端安全 / 李兴新等编著
. -- 北京 : 人民邮电出版社, 2016.7
（中国联通研究院创新研究系列丛书）
ISBN 978-7-115-42290-3

Ⅰ. ①移… Ⅱ. ①李… Ⅲ. ①移动通信－互联网络－智能终端－安全技术 Ⅳ. ①TN929.5

中国版本图书馆CIP数据核字(2016)第083101号

内 容 提 要

本书从智能终端面临的安全威胁和安全需求说起，分层次地归纳了智能终端面临的安全威胁和安全需求，并分别讲述终端硬件、系统内核、国产智能终端操作系统、应用和应用商店等各个层面的安全技术和实施策略，最后，从终端、终端产品、云端、标准化工作等层面总结并提出终端信息安全解决参考方案。

本书内容涉及终端信息安全的各个方面，可以为终端安全产品规划部署提供有益参考，对构建和完善终端安全体系具有重要意义，适合安全行业人员、运营商及通信业内人士，以及希望了解更多终端信息安全知识的从业者参考阅读。

◆ 编　　著　李兴新　侯玉华　周晓龙　郭晓花　严斌峰　等
责任编辑　邢建春
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：10.75　　2016 年 7 月第 1 版
字数：196 千字　　2016 年 7 月河北第 1 次印刷

定价：49.00 元

读者服务热线：（010）81055488　印装质量热线：（010）81055316
反盗版热线：（010）81055315

丛书编委会

本书编写组

主编：李兴新　侯玉华　周晓龙　郭晓花　严斌峰

编著：旷　炜　吕文琪　邸青玥　齐　霄　张成岩

刘馨靖　张云勇　魏亚杰　姜　琳　赵　慧

陈　冰

序 言

随着移动互联网业务日益繁荣、智能终端硬件水平不断提升，移动智能终端市场前景空前广阔，2015年年底中国移动互联网智能终端设备活跃数已接近9亿。与传统通信终端相比，移动互联网时代，以个人为中心的移动互联网终端承载着大量个人日常工作和生活信息，其重要性日益凸显。而伴随而来的是越来越严重的信息安全威胁，各类病毒、木马、后门层出不穷，严重威胁了个人信息、隐私数据、金融财富甚至国家机密的安全。其中，终端安全作为应对信息安全威胁的核心环节，理应引起重视。

本书对移动智能终端信息安全做了系统化的描述。首先介绍了移动互联网和智能终端的技术和市场演进概括，进而分析了终端安全面临的威胁和现实需求，并着重介绍了终端安全所涉及的硬件、内核、操作系统、应用和应用商店几方面关键技术，最终对终端安全解决方案做分析和探讨。

终端信息安全是涵盖终端到云端、从硬件到软件的系统化需求，本书试图从市场和技术角度对终端安全问题进行分析，让读者系统性地了解移动互联网时代智能终端信息安全概念，对解决终端信息安全问题有一定的借鉴意义，可供消费者、安全行业人员、运营商及通信业内人士参考。

Preface 前 言

近几年，互联网技术快速发展，在国家大力实施创新驱动发展、“互联网+”、宽带中国及大众创业、万众创新战略下，中国互联网尤其是移动互联网发展迅猛。根据中国互联网络信息中心（CNNIC）发布的第 37 次《中国互联网络发展状况统计报告》统计，截至 2015 年 12 月，中国网民规模已达 6.88 亿，互联网普及率达 50.3%，半数中国人已接入互联网，同时，网民的上网设备正在向手机端集中，智能手机成为拉动网民规模增长的主要因素，同期我国手机网民规模达 6.20 亿，有 90.1%的网民通过手机上网。移动通信技术的发展、网络环境的日益完善和智能终端的进一步普及、网民数量的激增和旺盛的市场需求共同推动了移动互联网领域更广泛的应用发展热潮，移动互联网正在塑造全新的社会生活形态，基础应用、商务交易、网络金融、网络娱乐、公共服务等个人应用日益丰富。2015 年，手机网上支付用户规模达到 3.58 亿，增长率为 64.5%，使用手机网上支付的网民比例由 2014 年年底的 39.0%提升至 57.7%；通过互联网实现在线教育的用户规模达 1.10 亿；使用网络医疗的用户规模达 1.52 亿；使用网络约车的用户规模已达 1.18 亿。移动互联网由于其普惠、便捷、共享等特性，已经渗透到公共服务、企业经营和个人生活的各个领域，改变了人们的工作、学习和生活方式。智能终端作为移动互联网的入口，是移动互联网的基础组成部分，智能终端的发展是推动

移动互联网发展的核心力量。

在移动互联网时代，终端安全形势也有了非常明显的变化。由于基础硬件平台的开放性、操作系统的智能化、移动互联网应用的不可控传播等使智能终端安全状况变得更复杂，也使整个移动互联网产业的安全风险不断增加。斯诺登“棱镜门事件”，曝光了美国政府的监控活动引发了全球对网络安全和个人隐私的担忧；Android、iOS 等操作系统存在诸多安全漏洞和隐藏后门，也严重威胁了用户个人隐私、商业机密、财富以及国家安全。政府、命脉行业以及商务人士对智能终端的安全需求日益增加。

国家和政府非常重视网络信息安全问题。2014 年 2 月 27 日，中央网络安全和信息化领导小组成立，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。智能终端安全作为网络信息安全的组成部分，将是移动互联网产业发展中不可回避的重要挑战。

本书以此为背景，从智能终端面临的安全威胁和安全需求说起，分层次地归纳了智能终端面临的安全威胁和安全需求，并分别讲述了终端硬件、系统内核、国产智能终端操作系统、应用和应用商店等各个层面的安全技术和实施策略，最后从终端、终端产品、云端、标准化工作等层面总结并提出终端信息安全解决参考方案。本书内容涉及终端信息安全的各个方面，可以为终端安全产品规划部署提供有益参考，对构建完善的终端安全体系具有重要意义。

全书共分为 7 章。第 1 章介绍了移动互联网和智能终端的发展历程，引出智能终端信息安全概念；第 2 章介绍了移动互联网背景下智能终端信息的安全威胁和安全需求，终端安全是分层面的系统化需求，在后续第 3~6 章分别分析了各层

面对应的安全技术；第 3 章介绍了终端硬件安全技术，重点介绍了主芯片、加密芯片、其他专用安全芯片等，提出终端硬件安全参考架构；第 4 章介绍了内核安全策略，主要是市场广泛使用的 SELinux 安全策略；第 5 章介绍了主流国产智能终端操作系统，包括沃 Phone OS、阿里 YunOS 等；第 6 章介绍了应用商店的安全分发机制和终端应用运行安全管理机制；第 7 章讨论了终端信息安全解决方案，包含公众用户、政企移动办公用户、高安全的终端安全解决方案，以及终端安全产品设计、云端安全管理方案等，并简单介绍了智能终端安全标准化研究工作。

本书适合于安全行业人员、运营商及通信业内人士，以及希望了解更多终端信息安全知识的从业者参考阅读。

本书在编撰过程中注重内容的完整性、通俗性和实用性。

完整性：本书涵盖了从硬件到软件、终端到云端的智能终端信息安全的各个层面，对相关核心技术、应用案例等方面都有论述。

通俗性：本书介绍了终端安全的基本知识，涵盖了终端安全的各个层面，相关技术介绍深入浅出，便于读者直观清晰地理解。

实用性：本书紧密结合实际，对终端信息安全的背景、需求、技术、部署和应用等各方面进行了分析和论述。

本书由中国联通研究院丛书委员会策划，李兴新统稿。第 1 章由侯玉华、严斌峰编写；第 2 章由郭晓花、齐霄、李兴新编写；第 3 章由邸青玥、旷炜、周晓龙编写；第 4 章由郭晓花、李兴新编写；第 5 章由吕文琪、周晓龙、李兴新编写；第 6 章由李兴新、旷炜编写；第 7 章由李兴新、邸青玥、周晓龙编写。

参加研究和写作的成员还有：张成岩、刘馨靖、张云勇、魏亚杰、姜琳、赵慧、陈冰。

本书凝聚了作者长期的智能终端安全实践经验以及研究思考的成果。作者广

泛收集了国内外相关材料，参考了一些安全论著，并结合了终端产业的最新发展情况，部分相关材料在本书编写过程中有引用，在此表示感谢。人民邮电出版社的邢建春编辑、研究院信息室范云杰编辑为此书倾注了大量心血，在此致以诚挚的谢意。

本书受国家“核心电子器件、高端通用芯片及基础软件产品”（核高基）科技重大专项课题“移动智能终端操作系统开发 2012ZX01039002-003”基金资助。

本书是作者的积极探索和思考的成果，仅代表个人观点，与任何机构的立场无关。我们希望通过大家的共同努力，理清智能终端安全的发展思路，在移动互联网大环境中创造安全可靠的终端应用环境，为网络信息安全创新发展贡献一份力量。由于信息安全概念外延广阔，作者水平有限，加之时间仓促，书中难免有错误或不当之处，恳请广大专家学者不吝批评指教。

作者

2016 年 3 月于北京

目录 Contents

第1章 Chapter 1 绪 论

1.1 移动互联网发展概述

1.1.1 移动互联网发展历程

移动互联网起源于移动通信网络与互联网（Internet）的结合。互联网的开创始于 1969 年美国国防部的 ARPAnet 网络，ARPAnet 网络最初服务于美国国防部的军事系统，从技术上不具备推广的条件，随着 TCP/IP、WWW 等技术的研发，并入网络的电脑主机和局域网逐渐增加，从而诞生了真正的 Internet 网络。20 世纪 90 年代后，Internet 商业化服务提供商的出现，商业机构逐渐发现 Internet 在通信、资料检索、客户服务等方面的巨大潜力。于是，其势一发不可收拾，世界各地无数的企业及个人纷纷涌入 Internet，从而带来 Internet 发展史上一个新的飞跃。1994 年 4 月，中国正式加入 Internet，成为真正拥有全功能 Internet 的第 77 个国家。Internet 目前已有超过 200 个国家和地区加入，截止到 2014 年底，全球活跃互联网用户突破 30 亿人。

移动通信技术在过去的十多年中发生了巨大的变化。20 世纪 80 年代开始提出第 1 代移动通信技术（1G，The 1st Generation），第 1 代移动通信网络采用模拟语音调制技术，其业务量小、质量差、安全性差、速度低，传输速度约为 2.4 kbit/s，如美国推出的 AMPS（Advanced Mobile Phone Service，高级移动电话业务）、英国推出的 TACS（Total Access Communication System，全接入通信系统）、北欧的 NMT（Nordic Mobile Telephone，北欧移动电话系统）。但是不同的网络采用不同的技术，相互之间无法漫游，也无法开展数据承载的业务。20 世纪 80 年代中期欧洲等发达国家开始研制第 2 代移动通信技术（2G，The 2nd Generation），欧洲国家主导的 GSM（Global System for Mobile Communication，全球移动通信系统）系统于 1991 年正式运行。为了满足数据业务的需求，GPRS（General Packet Radio Service，通用分组无线业务）技术顺势而生，其数据速率可达 115 kbit/s，使移动通信与 Internet 结合在一起，提供移动互联网浏览、收发邮件等业务，开始真正意义上的移动互联网业务。在向第 3 代移动通信技术（3G，The 3rd Generation）的演进过程中，又推出了增强型数据速率 GSM 演进（EDGE, Enhanced Data Rate for GSM Evolution）技术，EDGE 技术有效地提高了 GPRS 信道编码效率及其高速移动数据标准，其数据业务传输速率达到 384 kbit/s。伴随着用户对数据带宽的需求不断提升，国际电信联盟（ITU, International Telecommunication Union）提出发展 IMT-2000 第 3 代移动通信技术，主要的技术标准包括 WCDMA（Wideband CDMA，宽带码分多址）、cdma2000 和 TD-SCDMA。TD-SCDMA 支持的峰值下行速率达 2.8 Mbit/s，CDMA 网络在高速移动状态可提供 384 kbit/s 的传输速率，在低速移动或室内环境下，可提供 2 Mbit/s 的传输速率。IMT-2000 家族中各种标准存在相互兼容的问题，同时还存在频谱利用率低、速率不够高等问题，因此需持续向第 4 代移动通信（4G，The 4th Generation）标准演进，其主要标准包括