移动互联网时代的智能硬件安全探析

赵立新 著

中国财富出版社
CHINA FORTUNE PRESS

移动互联网时代的智能硬件安全探析

赵立新　著

中国财富出版社

图书在版编目（CIP）数据

移动互联网时代的智能硬件安全探析/赵立新著. —北京：中国财富出版社，2019.6

ISBN 978-7-5047-6922-0

Ⅰ.①移… Ⅱ.①赵… Ⅲ.①智能技术—硬件—计算机安全 Ⅳ.①TP303

中国版本图书馆CIP数据核字(2019)第102066号

策划编辑 李 丽 **责任编辑** 谷秀莉

责任印制 尚立业 **责任校对** 孙丽丽 **责任发行** 杨 江

出版发行 中国财富出版社

社 址 北京市丰台区南四环西路188号5区20楼 **邮政编码** 100070

电 话 010-52227588转2048/2028（发行部） 010-52227588转321（总编室）

010-68589540（读者服务部） 010-52227588转305（质检部）

网 址 http://www.cfpress.com.cn

经 销 新华书店

印 刷 天津雅泽印刷有限公司

书 号 ISBN 978-7-5047-6922-0/TP·0106

开 本 710mm×1000mm 1/16 **版 次** 2019年7月第1版

印 张 13 **印 次** 2019年7月第1次印刷

字 数 220千字 **定 价** 55.00元

作 者 简 介

赵立新，男（汉），河南镇平人，三门峡职业技术学院讲师，教务处实践教学科科长，工程硕士，2006年8月至今在三门峡职业技术学院任教。研究领域：无线传感网络、控制工程、程序开发等。参加工作以来，发表论文20余篇，主持参与省级科研课题、教改课题3项，校级课题5项，第四届“蓝桥杯”软件设计大赛河南赛区一等奖指导老师，荣获河南省国家教育考试优秀监考员、三门峡市优秀教师、三门峡职业技术学院优秀教师、教学质量优秀奖等荣誉称号。

内 容 简 介

随着移动互联网业务的日趋繁荣，智能硬件的水平也在不断提升，智能硬件的安全就成了不可忽视的问题。本书以智能硬件安全风险分析为研究框架，全方位介绍了有关智能硬件安全的攻击技术和防御思路，同时也分析了各硬件安全通路的研究思路和操作方法，提出了一些实用建议，对解决目前存在的智能硬件安全问题，有很好的借鉴意义。

目　录

第一章　走近智能硬件

第一节　智能硬件发展历程及优势

以智能手机为突破点，智能硬件彻底走进人们的生活。从2007年开始到2012年，智能硬件的发展主要围绕智能手机创新，触摸交互方式彻底革新了手机使用体验，商业模式则以硬件为入口和载体，以内容与应用服务为核心。

随着苹果手机的横空出世，触摸式交互硬件日渐普及。由于智能硬件贴近日常生活，交互方式的变革对于其使用影响极大。在诺基亚时代，触摸屏还未普及，人们与智能手机的交互方式更多的是键盘按键的方式，当时比较流行的黑莓手机拥有全按键键盘。2007年苹果公司推出iPhone后（于2009年进入中国市场），掀起了我国触摸式智能手机创新的浪潮。2009年2月，诺基亚发布其首款触摸屏手机5800XM，同年4月OPPO发布全触屏手机T9，同年10月华为发布触屏手机U8220。触摸交互的优势，在于其功能和表现力主要由应用程序来决定，其相较于键盘更具灵活性和亲和力。从市场竞争格局来看，头部稳定，但竞争激烈，2007—2012年，苹果智能手机出货量排名第一，2012年三星智能手机增长迅猛，2017—2018年，华为手机的出货量增长迅猛，整个智能手机市场不断上演着王者之争。智能硬件元器件供应平台开始崭露头角。

在市场发展初期，智能硬件厂商研发的新产品数量规模较小，对芯片的需求量也比较少，传统大型的集成电路供应商难以进行定制化生产。2010年，科通芯城成立，它是中国首家面向中小企业的集成电路元器件电商平台，科通芯城作为一个智能硬件创业者、集成电路等部件供应商的对接平台，帮助智能硬件创业者以更加便捷和廉价的方式获得元器件。

商业模式以内容与应用服务为核心。一种方式是将智能硬件作为服务的入口，智能硬件作为服务通常引入应用商店，在实现基本功能之上，用户可选择是否订购其他增值服务。该类型智能硬件的盈利模式，是在出售硬件时，回收全部的硬件成本并依附一定比例的利润。典型的硬件产品为智能手机、智能电视等。大多数早期的手机系统虽然都允许在手机上安装第三方应用，如诺基亚的Symbian（塞班系统）和微软的Windows CE系统，但需要事前在PC端上下载相应程序，之后与手机进行同步。而苹果iPhone搭载的第三方应用商店（App Store），提供了一种快速简便的方法来查找、购买和安装应用程序，用户可以直接订购App商店中的应用，这使得在手机中添加功能变得更为便捷。

目前，几乎所有的智能手机都搭载第三方应用商店，用户采用付费订购的模式从应用商店中订购App。根据IDC、IHS数据，2011年第三季度，搭载Android（安卓系统）的智能手机超过新增市场的50%。2015年1月，谷歌应用商店Google Play的应用数量首次超过了App Store，移动应用分发市场份额跃居世界第一。另一种方式是将硬件作为服务的载体。硬件本身不是收入的来源，也不是获得收入的入口，消费者在硬件框架下不断消费升级。典型的硬件产品为kindle等。2007年亚马逊推出kindle，之后不断更新，现已是第六代产品。kindle模式以阅读器、平板电脑等作为亚马逊产品或者服务的载体，以明显低于同类竞争对手的硬件价格，吸引用户购买亚马逊的硬件（如kindle Fire等），在此基础上，不断培养用户对亚马逊相关产品和服务的消费习惯，促使这些用户更多地购买亚马逊的音乐、视频、图书等产品。智能手机借力移动互联网，构建了庞大的信息经济，也为更

多类型智能硬件的出现奠定了基础，掀起了新的智能硬件创新浪潮。

从2012年开始，借助智能手机终端和云端支持，越来越多的智能穿戴设备出现在人们生活中。智能硬件产业生态趋于完整，云服务平台崛起，初创企业开始通过预售和众筹模式进行创业创新，产业充满活力。健康医疗类智能硬件快速增长。随着人们对生活品质追求的不断提高，对个人健康管理需求的日益旺盛，智能体脂秤、智能手环/手表等硬件设备成了采集个人健康数据的重要工具。智能手环、智能手表能够反映人们日常生活中的锻炼、睡眠、饮食等实时数据，让人们可以实时地、数据化地了解自身情况。2013年12月，咕咚网发布咕咚智能手环，该手环具有记录运动进程、睡眠质量、智能闹钟、定时提醒等功能。在智能手环领域，华为和小米两品牌的智能手环合计占市场份额的70%，斐讯、乐心则分别位居第三、第四位。2015年，有品推出智能体脂秤，之后小米、华为等企业进入这一市场。智能体脂秤可反馈人体信息数据，如体重、脂肪率、水分率、基础代谢率、肌肉量、骨盐量、蛋白质、BMI（身体质量指数）、身体得分、身体年龄等，将数据通过云端分析，在手机App中生成身体健康报告，并提供个性化的运动方案和饮食建议，使用户获得良好的健康服务体验。虚拟现实/增强现实技术的商业应用，日益广泛。

虚拟现实技术是融合三维显示技术、三维建模技术、传感测量技术和人机交互技术等多种前沿技术的综合技术，具有虚拟现实、增强现实和混合现实几种功能。虚拟现实技术和产品处于加速更新和升级阶段，目前的应用主要有三种模式：一是眼镜和手机配合使用模式，如三星Gear、谷歌Cardboard、暴风魔镜（2014年12月发布）等；二是头盔和游戏机配合模式，如Oculus CV、索尼PlayStation、HTC Vive等；三是一体机模式，如Sim Lens等。目前，眩晕感和交互性也有了较大改善。我国进入虚拟现实领域相对较晚，随着腾讯、阿里巴巴、百度、华为等企业的陆续进入，行业应用得以加速，市场需求逐步打开。比如，淘宝2016年推出的VR购物“Buy+”，可以让用户如同逛实体店一样网上购物，用户能360度视角观

看商品，并能够体验虚拟试穿服务等。从竞争格局来看，初步形成了两大领先集团，一是以谷歌和三星为首的移动 VR 集团，它们借助智能手机平台优势搭建移动 VR 平台抢占规模优势；二是以 HTC、Oculus、索尼为首的主机 VR 集团。智能硬件云服务平台崛起。

在智能硬件领域，用户流量是核心关键资源，社交关系有助于形成产品的口碑传播，而这决定了智能硬件创业者后期商业模式的转化。不少智能硬件创业者选择依靠腾讯、京东等互联网公司大平台。2014 年 7 月，腾讯推出微信智能硬件平台，通过公众服务号接入的智能硬件，用微信来同步、管理不同智能硬件的数据，并将这些数据与微信社交关系连接，提供朋友圈分享等功能。2014 年 10 月，腾讯发布 QQ 物联智能硬件平台，在流量、服务、核心技术、云资源、大数据计算以及硬件创新服务体系等各方面，实施全方位的能力开放，这有助于降低云端、App 端等研发成本，并能提升用户黏性。2017 年 6 月，京东推出智能服务平台 Alpha，通过开放 Alpha Open API，以云端接入或定制化开发的方式，为冰箱、电视、音箱、汽车、机器人等多种硬件设备终端开放赋能，并支持第三方开发者的能力接入。虽然智能硬件创业者选择接入腾讯、京东等平台，能够获得平台在流量服务、社交传播等方面的支持，但是对智能硬件的创业者而言，也意味着丧失了智能硬件的部分控制权，一些创业者甚至认为依赖大平台 App 易于沦为单纯的硬件制造商，进而陷入低毛利率怪圈。

智能硬件初创企业借力预售和众筹电商平台。这一模式的典型企业是点名时间、京东众筹等，其也在这一阶段发展成熟。点名时间在 2011 年 5 月成立，最初主要做股权众筹，2014 年 7 月抛弃了众筹模式，转型为智能硬件首发平台和预售电商。在首发平台方面，点名时间集合国内外、线上线下销售渠道，帮助企业进行采购预订。在预售电商方面，在预售期内，渠道商家通过点名时间可以获得 3 ~ 5 折的市场价，早期用户可获得 5 ~ 7 折的抢先体验价。2014 年 7 月，京东众筹成立，它借助于京东的电商平台，为智能硬件创业者提供筹资与孵化平台。根据京东众筹提供的数据，截至

2017 年 6 月底，京东众筹累计筹资额超过 44 亿元，共呈现出 10000 多个创新众筹项目，其中，千万元级项目 80 多个，百万元级项目近 800 个，众筹项目成功率超过 90%。众筹模式的优势：在智能硬件的迭代研发或初试阶段，智能硬件创业者通过众筹平台可以获得有效的市场反馈及启动资金，利于早期的用户积累、品牌传播，并能解决资金问题。

2015 年以后，随着智能硬件在技术、功能和模式上的不断更新迭代，语音交互、体感交互等成为提升用户体验的重要方向，智能家居、智能家电、服务机器人等纷纷出现，试图占领更多生活场景，与此同时，行业市场规模不断扩大。具备语音交互功能的智能硬件，成为智能家居的重要产品。触摸技术实现了交互方式从一维向二维平面的拓展，但其局限性在于手指必须接触屏幕表面，这限制了用户使用范围，因此，智能语音交互成为未来提升用户体验的重要方向之一。2015 年，科大讯飞与京东共同出资成立的灵隆科技推出京东叮咚，京东叮咚搭载了科大讯飞的人工智能语音交互界面，优势在于依托 AIUI 功能，语音识别能力较好，且支持接入多个第三方应用平台。2017 年 7 月，阿里巴巴推出了天猫精灵，天猫精灵搭载了阿里巴巴 AI Labs 的人机智能交互系统 Ali Genie，其优势在于拥有较为安全的声波支付功能，绑定支付宝后可以进行语音购物。2018 年 3 月，小米推出的小爱智能音箱，搭载小米的水滴平台（现升级为小爱开放平台）。用户通过说某个特定的词来唤醒智能音箱，之后便可以与音箱进行语音交互，进而实现零触控的交互体验。这些智能音箱大都搭载了自主学习算法，可以分析并学习用户的偏好、行为与习惯。小爱智能音箱的优势在于价格相对低廉，可以控制小米旗下的电视、扫地机器人、空气净化器、电饭煲等电器，并借助于米家智能插座、智能插线板、墙壁开关，对其他品牌的电器进行智能控制。在智能家居领域，小米生态链具有绝对优势，占据了智能家居市场份额前十名中的五位。随着语音交互、视觉图像交互、动作交互等技术的不断升级，服务机器人正在变得越来越贴合人类需求，如可借助深度摄像头识别面部表情，借助语音识别模块判断情绪，并可接入 IBM Watson

（沃森）平台，提升自主判断与决策能力等。

3D 摄像技术的日渐成熟，助推三维体感交互。语音交互虽然能够解放人类双手，但仍有一定的局限性（如距离限制），对于远程拍照（航拍）、车载、游戏等领域，语音交互往往难以满足人们需求。目前一种可行的解决方法是采用三维摄像技术，它有助于实现视觉交互从二维平面向三维立体空间的拓展，可用于识别手势动作、人脸、虹膜等生物特征，提升生物识别的安全度。2017 年，高通推出了前置 iris 生物识别模组及高端计算机视觉摄像头模组。iris 生物识别模组主要用于虹膜识别，具有 40ms 的低延时，并能够支持活体检测。高端计算机视觉摄像头模组通过红外发光器发射出光束，IR 摄像头读取该光斑图案，对点状图在物体上发生的扭曲以及点与点之间的距离进行计算，进而与 RGB 图像进行复合，最后形成 3D 模型。这意味着搭载高通下一代处理器的智能终端能够实现 3D 人脸识别、虹膜识别功能。

租赁商业模式开启。一些智能硬件公司采用租赁模式来获得收益，这类典型硬件产品为共享单车、车载电子系统等。销售或者租赁这类智能硬件设备给用户，采用软件许可费、按时计费或按使用里程数计费等计费形式获得收益。

硬件为租赁服务的模式，往往需要持续拓展用户规模，优化用户使用体验。很多采用租赁模式的智能硬件企业并未抓住“提流速、强体验”这一核心，本质上仍是传统租赁模式在规模上的扩张。未来全景式智慧生活智能音箱将成为智能家居的重要入口。在智能家居场景，语音交互是比触摸交互更加自然的方式。智能音箱有望成为室内交互的智能终端。智能音箱可以通过接入开放平台，实现传统的听音乐、听书、操作家电等功能，还能够实现诸如网络购物、叫外卖、呼叫专车等日常服务。加上日益成熟的声纹识别技术，语音支付的安全性大幅提高。数据表明，2016 年智能音箱全球出货量达到 590 万台，预计到 2022 年全球出货量将增长 10 倍，市场规模达 55 亿美元。“运动跟踪 + 手势识别”将成为主流交互模式之一。

未来的智能硬件将不再有键盘和鼠标，用户不必再用手指接触屏幕，远距离就能够操作界面，人机交互体验将变得更自然。

随着三维摄像模块在移动芯片上的集成，具有运动跟踪和手势识别功能的硬件将越来越多。手势识别配合人工智能技术，能够很好地预判用户行为意图。比如，用户只要做出一个抓取的手势，便能够打开和放大用户所指向的某个虚拟物体。个人健康数据追踪将衍生新的商机。通过智能定位系统可以获得个人的全方位扫描信息，例如，人的位置、动作甚至是迟疑行为等，都可能被传感器捕捉与记录下来，进而通过数据分析精准预测个人的想法和行为。通过健康数据追踪，可以实时获取心跳频率、生物活动程度，从而帮助我们更深入地了解自身身体状况，借助健康大数据分析，进行个性化诊疗、推荐个性化的医药，未来甚至可以根据个体基因、生活方式，进行更高级的健康定制化服务。

5G 网络将大幅提升智能硬件的用户体验质量。与 4G 网络相比，5G 的数据吞吐量增加了 10 倍，通信容量增加了 100 倍，而延迟是此前的 1/10，这对于改善虚拟现实、增强现实等硬件设备的用户体验质量至关重要。5G 技术带来的低功耗，还将提升智能硬件设备的续航时间。云平台将给智能硬件营运提供敏捷化服务。云端提供了高可靠性计算、极快的速度及扩展弹性，而使用者却无须承担任何负担。云端的一个核心优势在于，其变得越强大，终端设备就会变得越来越小巧。云端负责所有的工作，而终端只是提供对接云端工作的窗口。在云端里，智能硬件运营商可以轻易地将诸如语音识别、图像识别等功能拓展到硬件上。智能硬件正在向智能家居、智能车载、智能可穿戴、健康医疗、无人机等领域不断拓展，并且新技术、新模式不断涌现，未来或将开启全景式智慧生活，这给人们以无限的想象空间。

第二节　智能硬件的发展趋势

智能硬件通过软硬件结合的方式，对传统设备进行改造，进而让其拥有智能化的功能。智能化之后，硬件具备连接的能力，可实现互联网服务的加载，形成“云 + 端”的典型架构，具备了大数据等附加价值。

从行业层面来看，智能硬件的整个市场规模仍在高速增长。2015 年，智能硬件热门品类的销量已经破千万，并在智能家居、可穿戴设备等的带动下持续增长。同时，企业将不断整合核心能力，构建完整的智能生态链。

互联互通与交互方式的优化，将成为智能硬件产品发展的重点，而智能家居将继续成为热点发展领域。智能类产品的用户黏性与其实用性息息相关，简单、多样化的交互方式更能满足消费者需求。当前已经推广应用的场景化模式，可以让用户通过简单的触控或者语音操作直接触发智能家电的一系列预置动作，迅速、便捷地享受完整的智能生活。这种设备间的互联互通以及交互方式的变化，已经不再是单一智能产品可以完成的，带给用户的体验也是完全不同的。

一般来说，智能硬件产品的发展阶段分为监测、控制、“优化和自主”三个阶段。也就是说，智能硬件的发展，是从监测用户身体或家居指标，到控制家庭设备，最终到优化用户体验和实现自动执行命令的过程。目前，整个智能产品的发展，仍处于第二阶段，智能硬件不智能，要下载一堆 App，难以互联互通的问题依然突出，这阻碍了产品的进一步普及。

据相关研究数据显示，在已经使用智能设备的用户当中，有超过 35% 的用户“非常依赖”他们的设备。对于可穿戴硬件等产品而言，这一数字远未到理想程度。比如，用户原以为手环类产品可以帮助其调整作息甚至减肥，但最终发现手环只能监测数据，不能精细化监测，也不能基于数据

提供足够有用的健身计划。此时，数据实用性则成了一个新的问题。

同时，随着技术发展带来的智能化水平提升，智能硬件将逐渐趋于丰富多元化、渠道公开化、人性智能化和垂直细分化。丰富多元化主要指随着智能硬件的火爆，满足多样化需求的智能硬件产品层出不穷。渠道公开化主要是从线上、线下渠道融合角度来谈的。当前，线上渠道不再是初创硬件厂商更倾向的渠道选择，线下体验 +B 端渠道开拓更受重视，部分创新型企业甚至在设立之初就直接成立渠道拓展部。人性智能化主要表现为智能硬件不再创造需求，而是开始落地考察大众的真正需求，提供人性化的智能解决方案。垂直细分化则是面临当前智能硬件发展瓶颈时硬件厂商的解决之道，即在垂直细分领域开始探索解决方法，摸索适合细分领域受众人群的真正需求。

不过，智能硬件的发展已经成为一种必然趋势，随着平台、生态的逐步成型，以及像 VR 这样的新技术的不断发展与应用，智能硬件的未来更值得期待。随之而来的，将是越来越多消费者生活习惯的改变，以及智能生活时代的到来。

第三节　智能产品在各领域的应用

经历了技术驱动和数据驱动阶段，智能产品现在已经进入场景驱动阶段，并深入各个行业去解决不同场景的问题。此类行业实践应用也反过来持续优化着智能产品的核心算法，形成正向发展的态势。目前，智能产品主要在制造、家居、金融、零售、交通、安防、医疗、教育、物流等行业有广泛的应用。

一、制造

随着工业制造 4.0 时代的推进，传统制造业对智能产品的需求开始爆发，

众多提供智能工业解决方案的企业应势而生。智能产品在制造业的应用可以分为产品研发阶段、生产阶段、销售阶段、售后服务阶段几个阶段。

在产品研发阶段，欧特克、西门子、PTC（美国参数技术公司）、达索等工业设计软件厂商都推出了创成式设计（Generative Design，GD）解决方案，本方案融合了人工智能及机器学习技术，设计者可定义特定的材料、设计空间、允许的载荷和约束及目标权重，该软件可自动计算几何解法，自行对产品进行尺寸、形状及拓扑优化，生成多种可选方案，让研发人员从中找出最优方案。通过创成式设计，研发人员可以专注于产品性能，减少重复工作。

在生产阶段，智能产品主要应用在视觉检测、无序分拣、柔性打磨等方面。

视觉检测：智能产品的应用可以帮助企业实现自动化检测，通过对产品进行拍照并建立模型，让机器在大量的照片中分辨怎样的照片是良品，怎样的照片是不良品，经多次训练后，机器可以自行对照片进行快速判断。这种方式可以将工程师的经验转化为深度学习算法，使之得到推广和应用。

无序分拣：融入智能产品之后，机器能够自行学习如何抓取不规则摆放的零件。通过机器视觉对物体进行识别定位，采用学习算法并经多次训练后，机器人可以判断在杂乱摆放的零件中应该先抓取哪一个，抓取哪个位置能够使抓取的成功概率最大。

柔性打磨：打磨零件需要很大的柔性，智能产品需要在打磨的过程中不断适应并调整打磨的力度和角度，从而建立力与机器末端轨迹的关系。通常，先采取不同的方式来示教打磨过程，然后根据示教过程中的传感器数据建立学习模型，最后将学习模型与智能产品的具体控制算法相结合，就能在机器上快速实现柔性打磨。

在销售阶段，基于机器学习模型对用户的购买习惯以及产品的属性进行深度学习，可以形成全面的知识图谱，在此基础上向用户进行个性化推荐，向销售商提供相关的生产与营销建议，这项技术的应用可以帮助企业提升