Broadview
www.broadview.com.cn

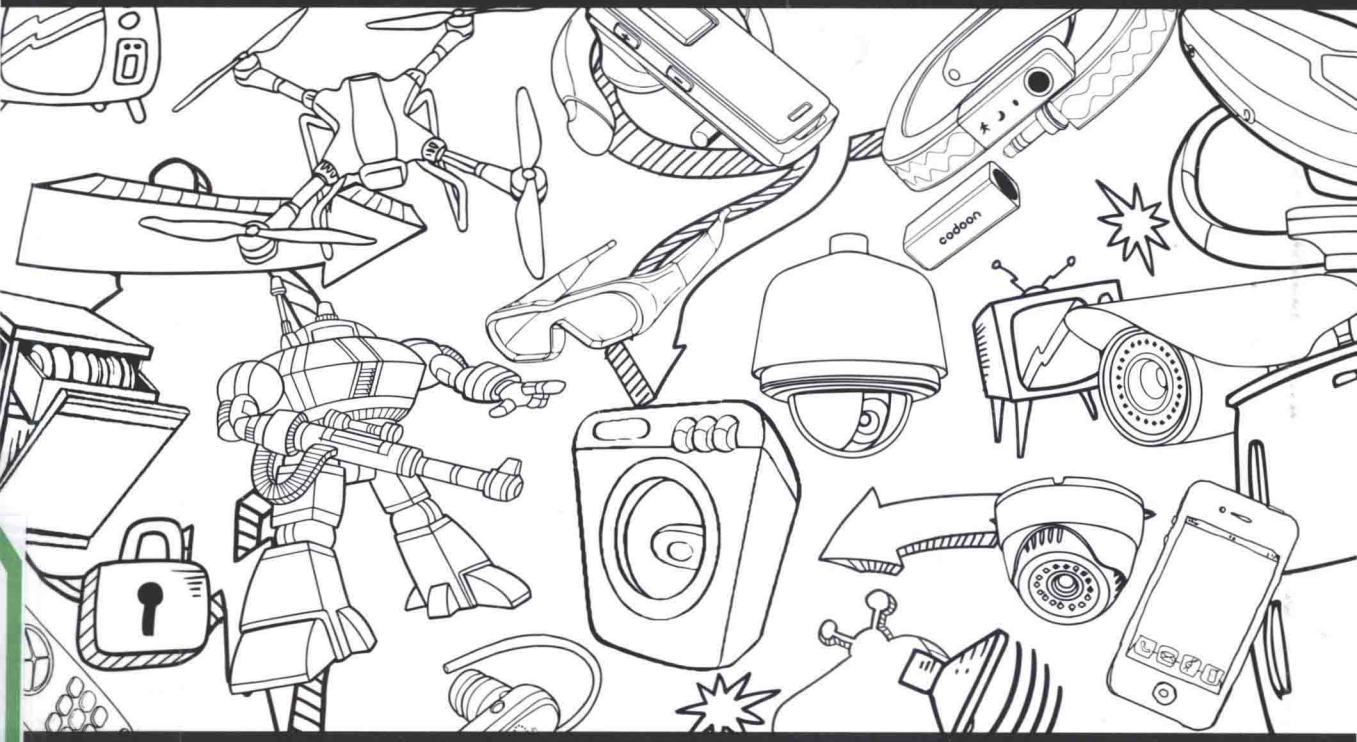
360 ADLAB

SKY-GO

安全技术大系

一本书掌握物联网安全核心技术

智能硬件安全



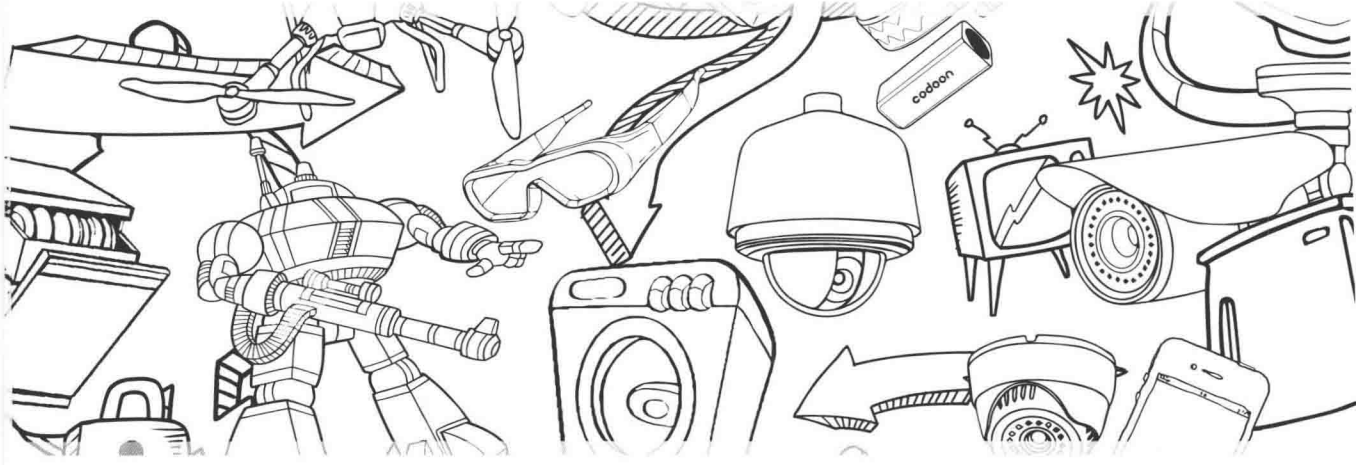
刘健皓　王奥博　等编著

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

安全技术大系

智能硬件安全



刘健皓　王奥博　贾文晓　严敏睿　编著

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

内 容 简 介

本书主要分为三部分：第一部分总体介绍为什么研究智能硬件安全，以及智能硬件安全风险分析和研究框架；第二部分介绍智能硬件信息安全研究的思路和具体操作方法；第三部分介绍智能硬件信息安全的分析思路。

本书适合硬件安全研究人员、智能硬件开发人员、网络安全人员，以及智能硬件爱好者阅读。

图书在版编目（CIP）数据

智能硬件安全 / 刘健皓等编著. —北京：电子工业出版社，2016.11
（安全技术大系）
ISBN 978-7-121-30103-2

Ⅰ. ①智… Ⅱ. ①刘… Ⅲ. ①硬件－安全 Ⅳ.①TP303

中国版本图书馆 CIP 数据核字(2016)第 246793 号

策划编辑：郑柳洁
责任编辑：郑柳洁
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
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：787×980　1/16　印张：14　字数：253.44 千字
版　　次：2016 年 11 月第 1 版
印　　次：2016 年 11 月第 1 次印刷
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。

推荐序一

几乎没有人怀疑未来会是一个万物互联的物联网时代，在过去的 3 年中各种物联网智能硬件层出不穷，但当大量的互联网企业开始设计、制造智能硬件，当家电企业忙着让自己的家电“联网”“智能”的时候，人们并没有意识到这些智能硬件会成为黑客们的新玩具，于是路由器被入侵、洗衣机被入侵、电视机被入侵、家用摄像头被入侵、专业的安防摄像头也被入侵，直到连智能网联汽车也被成功入侵并可以被远程控制！

人们终于意识到物联网在给我们的生活带来巨大便利的同时，也带来了个人信息泄露的风险，甚至可能会因为信息安全问题而威胁到我们的人身安全，发现物联网的技术平台竟然有那么多的风险存在：从芯片、电路板到固件，从无线通信协议到控制智能硬件用的手机 APP，都存在被攻击、被利用、被破解的可能，而物联网安全的研究工作才刚刚起步。

360 网络攻防实验室、360 独角兽团队是国内比较早意识到智能硬件安全性问题的团队，对大量的智能硬件设备做了安全研究，也是国际上最早成功破解特斯拉电动汽车的团队。本书从固件、网络安全、无线通信协议安全、控制 APP 安全等角度，以智能摄像头、智能网联汽车、智能电视盒子、智能家电、可穿戴设备、智能机器人为实际案例分析了物联网的安全问题，比较适合作为一本物联网安全的入门读物。

谭晓生

北京奇虎科技有限公司副总裁 首席隐私官

推荐序二

万物互联时代的核心是各类智能硬件产品。这些智能硬件的出现，一方面为人类的生活带来了极大的便利，提升了人们生活的品质，另一方面其在各个维度可能存在的安全隐患问题也让用户心存担忧。相对于互联网安全，智能硬件安全在国内尚缺少相关书籍进行全面而系统的介绍。刘健皓带领的 360 网络攻防实验室合力编著的这本《智能硬件安全》正是在这个大背景下非常及时地填补了这个领域的空白。

本书的内容总体分成三个板块。第一个板块总体介绍了为什么要研究智能硬件安全，智能硬件的安全风险和研究方法框架及思路。第二个板块全面介绍了智能硬件安全的几类具体研究方法。第三个板块介绍了一些常见的智能硬件的安全分析及破解案例，并且提出安全建议。

基于对车辆安全问题（车辆驾驶安全和车辆信息安全）的共同爱好和兴趣，我和刘健皓及其团队在过去一年有非常频繁而深入的交流。刘健皓是一位顶尖的安全技术专家，2014 年他的团队利用曾经存在的漏洞，破解过特斯拉汽车，能够实现远程控制；2015 年他的团队又利用曾经存在的漏洞，破解过比亚迪汽车，能够实现对汽车的远程攻击。

本书可以作为物联网安全实例教程，为国内智能硬件安全研究人员提供基本方法指引，从而提高国内智能硬件安全厂家的整体安全水平。同时，本书的部分内容也可以作为科普读物，帮助最终用户提高使用智能硬件时的安全意识。相信本书将会有效地提升生产厂商和用户对智能硬件安全问题的认识，从而促进万物互联在安全层面的发展。

颜水成

奇虎 360 首席科学家，360 人工智能研究院院长

推荐序三

万物互联的时代即将到来，智慧城市、智能家居、智能机器人、智能出行逐渐走入人们的日常生活，智能硬件将成为人们生活中不可或缺的一部分。目前，智能硬件的安全问题并未得到人们的广泛关注，实际上，智能硬件安全问题造成的危害甚至比信息安全问题更严重，直接影响到人身安全、社会安全和国家安全。安全无小事，智能硬件安全必须引起高度重视。

本书是国内第一本介绍智能硬件安全的书籍，介绍了智能硬件的安全风险和研究方法，并附有实战分析及破解案例。希望通过阅读本书，能提高智能硬件生产厂家的安全意识，为智能硬件安全研究人员提供方法和指引，让更多的人参与到智能硬件安全生态体系中，为整体安全能力提升做出贡献。

谈剑峰

上海市信息安全行业协会会长

名家点评

这几年物联网正在飞速发展，人类正在从工业文明大步迈进信息文明，正在用一些新方法解决一些老问题，这些方法用的不是钢筋、水泥和电线，而是云、软件和数据。在即将开启的万物互联的时代，人们在享受智能带来的生活便利与舒适的同时，智能设备的安全问题也已经成为衡量一款智能设备质量的重要指标，物联网的安全问题正在受到关注与重视。

作者通过基础综述、技能方法指导、分类总结等方式，以实例讲解为线索编纂了本书，系统且全面，读者可以按照作者的思路循序渐进地学习。对智能设备安全比较陌生，希望今后在这个领域有所发展的读者，可以在了解物联网安全研究分析基础之后，从手机 APK 分析、固件分析、网络协议分析这三章入手，学习后会对智能硬件安全分析的主要技能方法有一定掌握。如果对无线电和硬件系统知识掌握得比较少，可以暂时跳过软件定义无线电分析方法章节，直接进入后面的实例讲解章节，将每章的实例和前面讲的技法结合起来学习，应该能够基本掌握智能设备安全研究分析方法。而后应该尽可能多地做分析练习，将已经学习到的知识通过实践进行巩固，从而提高自己的独立分析能力。当对智能设备有了一定安全分析能力后，再回过头来了解如何通过软件无线电来分析无线电信号，智能汽车可能存在什么样的安全问题，智能机器人又会面临什么样的安全威胁等章节的内容。至此，对智能设备领域已经有了比较立体的认识，可以独立阅读更多智能设备安全相关资料，并判断选择自己将来的研究方向，也可以向更深层次、更专业的某个方向深入研究。

本书从基础介绍、威胁分析到各种类型的智能设备安全问题分析、漏洞实例分析，深入浅出地对智能设备安全做了全面讲解，通过实例分析帮助读者更形象深入地学习理解智能设备安全研究分析技术并为每类产品安全问题提出相应的安全建议。不论你是智能设备安全的技术爱好者，还是智能设备的开发人员，或者希望将来成为一位智能设备安全问题的挖掘者，都可以从本书中获得你想要的东西。

本书作者刘健皓在智能硬件设备安全技术研究方面起步较早，具有丰富的实践经验，技术扎实全面，发现过不少智能设备的安全问题，还发现过汽车电子系统的安全问题，我们经常互相学习交流，他是一名非常棒的安全技术研究员。非常高兴健皓能邀请我为本书写序，我也很愿意将本书推荐给对智能设备安全感兴趣的你，本书一定可以帮到你。希望大家未来在智能设备安全研究领域也像健皓一样成绩卓越，能够帮助人们更好、更安全地享受物联网带来的伟大进步。

祝大家阅读愉快！

王英键

XCon 创始人，资深安全研究员

前　言

目前智能硬件行业正处于飞速发展阶段，智能硬件通过传感器和互联网的巧妙结合给用户带来优质的产品，提高了用户的生活质量。但与此同时，也出现了一些因智能硬件信息安全问题给用户带来的经济与财产的损失。所以智能硬件信息安全问题将比传统信息安全更重要，但因为智能硬件技术是一种多项技术混合应用的体系，更难以做到全面防范。为了提高国内智能硬件信息安全能力水平，帮助信息安全研究人员、智能硬件开发设计人员更好地理解信息安全技术，我们团队共同编著了本书。

智能硬件安全技术是一把双刃剑，既能感受到智能硬件安全研究过程中的乐趣与兴奋，也能利用智能硬件的安全问题给用户造成损失。在此希望大家抱着学习的态度来阅读此书，而不是为了寻找破解智能硬件的方法，利用智能硬件漏洞去做不好的事情。

同时希望本书可以给智能硬件安全研究人员、开发人员、设计人员、物联网专业学生，以及生活中的极客提供指导和参考。

本书架构

本书深入浅出地介绍了智能硬件信息安全的基本概念，同时对几种安全研究方法做了具体的介绍，最后结合一些实际破解案例进行分析（这些破解案例所涉及的智能硬件的漏洞都已经修复）。通过一层一层的递进学习，能够将一位基本了解计算机信息安全技术的读者培养成能够上手进行智能硬件安全研究的从业人员。

第 1 章介绍了智能硬件信息安全的一些基本概念、技术架构、风险分析、研究框架等内容。这些内容来自于刘健皓的经验总结。

第 2~5 章介绍了主流的智能硬件安全研究方法，包括 APK 逆向分析、固件分析、网络活动分析和无线电分析。通过这些分析方法可以发现智能硬件的整体安全风险。

这部分内容由汽车信息安全团队（Sky-GO）安全研究员王奥博、贾文晓编著。

第 6~12 章针对市面上的智能硬件进行分类，按照不同种类和不同的使用需求对应进行安全分析。主要包括对智能电视盒子、智能汽车、智能安防、智能摄像头、智能家电、智能穿戴娱乐、智能机器人这些智能硬件破解案例的分析。通过案例分析可以很好地印证第 2~5 章介绍的分析方法，前后呼应，帮助读者理解。这部分由整个汽车信息安全团队（刘健皓、严敏睿、王奥博、贾文晓）共同编著。

致　　谢

首先，感谢我的老婆及家人。老婆怀孕的时候还鼓励我完成本书的编著工作，并给予我极大支持。

感谢 360 公司的周鸿祎、齐向东给团队提供了优质的研究条件和得天独厚的研究平台。

感谢 360 公司的谭晓生。感谢谭校长对汽车信息安全团队的悉心教导与栽培。

感谢 360 信息安全部全体成员对我工作的支持与理解。

感谢 360 核心安全与企业安全公关市场部的韩笑、尹乃萧、许传朝、马利娜、徐粲然、陈晨、苑一时、景义哲、裴志勇、胡晓、耿陆力等同事为团队的研究成果进行传播等工作。

感谢 360 移动安全研究院的蒋旭宪、周亚金等同事对团队的工作支持。

感谢 360 人工智能研究院的颜水成、韩玉刚、陈强对团队的工作支持。

特别感谢 360 网络攻防实验室的老领导林伟老师，是他为我规划了智能硬件和车联网两个研究方向，并支持鼓励我一直研究下去，才有了本书。

刘健皓

360 汽车安全实验室负责人

目　录