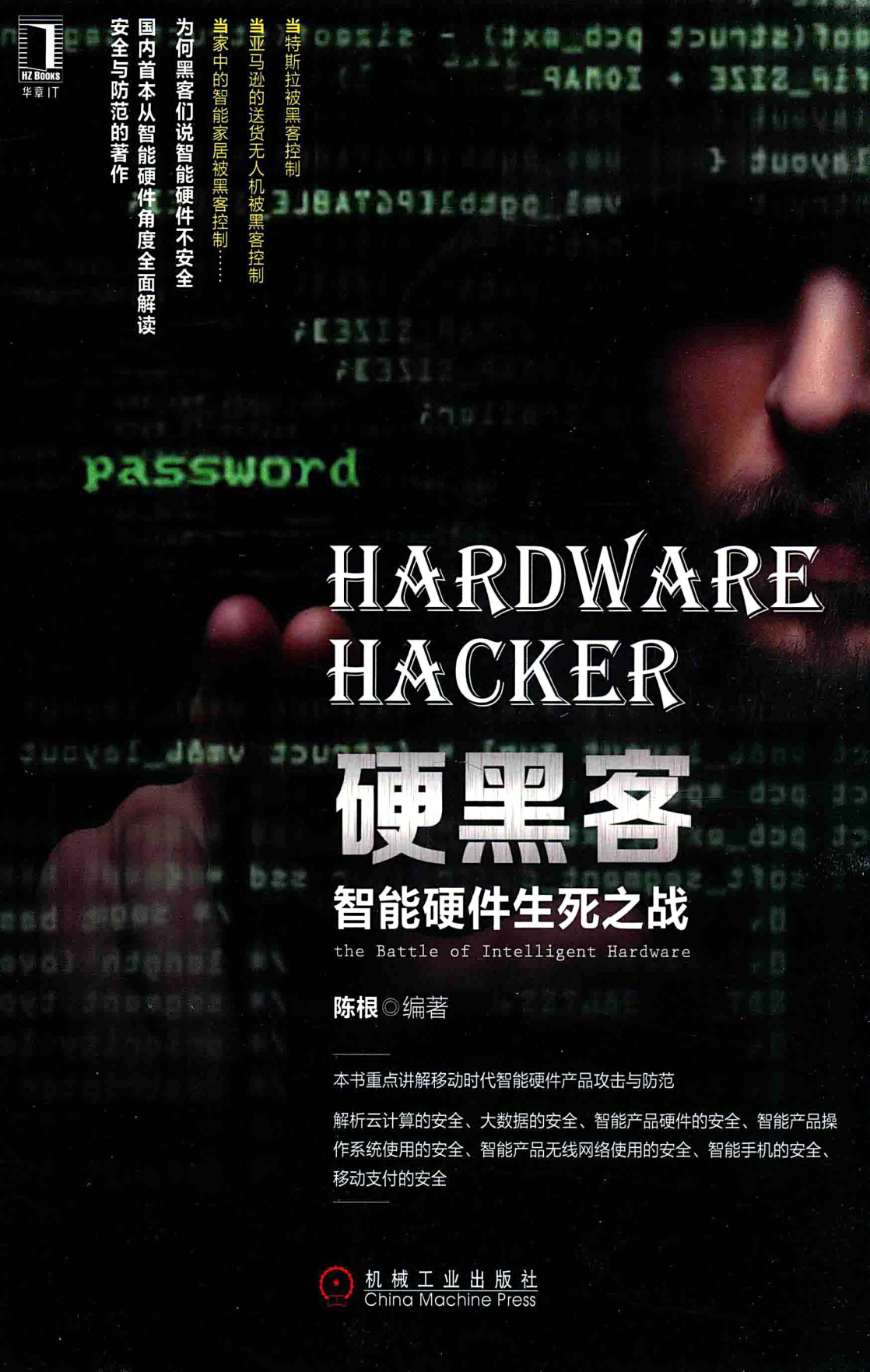

HZ BOOKS
华章IT
当特斯拉被黑客控制
当亚马逊的送货无人机被黑客控制
当家中的智能家居被黑客控制……
为何黑客们说智能硬件不安全
国内首本从智能硬件角度全面解读
安全与防范的著作
password
HARDWARE
HACKER
硬黑客
智能硬件生死之战
the Battle of Intelligent Hardware
陈根◎编著
本书重点讲解移动时代智能硬件产品攻击与防范
解析云计算的安全、大数据的安全、智能产品硬件的安全、智能产品操作系统使用的安全、智能产品无线网络使用的安全、智能手机的安全、移动支付的安全
机械工业出版社
China Machine Press

HARDWARE HACKER

the Battle of Intelligent Hardware

硬黑客

智能硬件生死之战

陈根◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

硬黑客：智能硬件生死之战 / 陈根编著 . —北京：机械工业出版社，2015.8

ISBN 978-7-111-51102-1

I. 硬… II. 陈… III. 智能技术－硬件－安全技术－研究 IV. TP18

中国版本图书馆 CIP 数据核字（2015）第 182959 号

硬黑客：智能硬件生死之战

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）

责任编辑：余 洁 责任校对：殷 虹

印 刷：藁城市京瑞印刷有限公司 版 次：2015 年 8 月第 1 版第 1 次印刷

开 本：170mm × 242mm 1/16 印 张：15.25

书 号：ISBN 978-7-111-51102-1 定 价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88379426 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

前　言

IT技术、互联网的发展引领着产业的变革和跨界融合，随之而来的是，智能化的浪潮向家居、可穿戴设备、汽车、制造等领域快速延伸，这引起全世界高科技企业、投资机构的广泛关注，智能化浪潮也随即成为全球经济新的增长点。尽管物联网的概念提出已久，但它真正在产品上的表现则主要在最近两年内才实现。随着智能硬件产业的火爆发展，很多科技、IT、互联网、制造业巨头纷纷涌入这个产业。

2014年1月，谷歌32亿美元收购Nest；同年2月，美国可穿戴运动摄像机制造商GoPro向SEC递交IPO文件，并于6月正式登陆纳斯达克；2015年6月，被称为全球智能穿戴领域第一股的FitBit成功登陆美国资本市场，这一系列新科技与资本关系的演绎中出现的巨额变现能力让人们感知到这个市场的发展潜力巨大。百度、小米、乐视、京东、奇虎等一大批互联网企业积极布局智能硬件，聚焦技术和商业模式融合创新，推出了智能手机、智能电视、盒子、手环、路由器等一系列智能硬件产品，同时孵化培育了一批创新型企业，初步形成了良好的智能硬件产业生态圈。

智能产品的普及源于移动互联网技术的突破，借助于产品的智能化、互联网化，给人们的生活、工作、学习、社交、购物等方面带来便利。显然，智能产品的爆发得益于现代网络技术的高速发展，多种多样的数据传输方式和传输速度将一个大大的世界变成小小的地球村，时空实现了穿越和倒转；云计算带来社会计算资源利用率的提高和计算资源获得的便利，推动以互联网为基础的物联网迅速发展，更加有效地提升人类感知世界、认识世界的能力，促进经济发展和社会进步；大数据在众多领域掀起变革的巨浪，物联网、云计算、移动互联网、车联网、手机、平板电脑、PC以及遍布地球各个角落的各种各样的传感器，无一不是数据来源或者承载的方式，大数据的商业价值和市场需求成为推动信息产业持续增长的新引擎。

但是在2013年～2014年，虽然非常多的公司在试水智能硬件，但是几乎没有拿得上台面并且实现量产的产品。一是客观环境使然，软件及硬件、产业链等各种问题牵制了这些产品的量产，并且很难有很好的产品设计与体验。二是大部分的智能硬件都只是鸡肋，根本无法与之前的设想相比。无论是眼镜、手表、手环，还是音响、戒指，大部分功能只是围绕着手机的基础功能做延展，这些硬件多数无法形成新的需求，无法做到让人使用得如鱼得水，难以割舍。

但经过近两年的摸索、尝试、创新，以及产业链技术的不断成熟，可以说物联网时代的关键终端载体，也就是智能硬件将步入正轨，并呈现新一轮的爆发增长，一切的终端、产品、设施都将智能化，并借助于互联网、移动互联网技术实现万物互联的物联网时代。随之而来，智能硬件的安全将会成为一个新的危机点。过去由于互联网的快速发展，基于互联网的系统、网络、PC等环节的安全困扰着使用者，也由此每年给各种组织、机构、用户带来了巨大的损失；而进入移动互联网时代之后，各种安全问题伴随着互联网技术向移动互联网技术转移而转移，显然，当前基于智能手机的移动互联网安全成为用户、企业、黑客的焦点。

随着移动互联网向物联网转移，这些物联网时代的关键载体，也就是这些硬件终端将成为黑客的下一个关注焦点。可以说，物联网时代的安全问题更为复杂，终端智能硬件产品本身、通信传输环节、系统平台、大数据平台、云服务平台等任何一个环节都可能成为黑客攻击的对象。本书正是基于即将爆发的智能硬件安全问题进行探讨，之所以取名为“硬黑客”，也正是基于过去在软环境中所存在的安全隐患将伴随着物理实体的智能硬件出现而转移，由过去的软系统层面向当前的硬产品层面转移。智能硬件能否一路顺利地发展，并且真正造福人类，其中一个关键的要素就是智能产品本身的使用安全性，可以说，硬件安全将会是智能硬件接下来的一场生死之战。

智能产品是继智能手机之后的一个科技概念，是通过软硬件结合的方式，对传统的设备进行改造，进而让其拥有智能化的功能。改造的对象可能是电子设备，例如手表、电视和其他电器；也可能是以前没有电子化的设备，例如门锁、茶杯、汽车，甚至房子。智能化之后，硬件具备连接的能力，实现互联网服务的加载，形成“云＋端”的典型架构，具备大数据等附加价值。

智能硬件已经从智能手机、可穿戴设备延伸到智能电视、智能家居、智能汽车、医疗健康、智能玩具、机器人等领域。比较典型的智能硬件包括Google

Glass、三星 Gear、FitBit、麦开水杯、咕咚手环、Tesla、乐视电视等。

2014 年，移动互联、大数据、云计算、物联网等技术为个人生活带来了便利，为企业发展提供了技术上的支持。但是“水能载舟，亦能覆舟”，在过去的一年全球互联网安全也摊上不少大事：“Heartbleed”和“Bash”漏洞震惊全球，数据泄露事故似乎已经成为家常便饭，ATP 攻击事件层出不穷，DDoS 黑客活动的频率与手法不断升级，甚至出现了史上流量最大的攻击。安全是智能产品永恒的主题，无论是对开发者、生产者还是使用者。智能产品的设计、生产、销售、使用、销毁，每一个环节都存在安全隐患。如何构筑智能产品的安全屏障，考虑到与智能产品安全的相关程度，我认为应该关注以下几个方面，并从这几个方面做出实际的安全工作：

- 云计算的安全、大数据的安全。
- 智能产品硬件的安全、智能产品操作系统使用的安全、智能产品无线网络使用的安全。
- 智能手机的安全、移动支付的安全。

新技术、新攻击令人眼花缭乱，企业如何能在这场日益复杂并且不断变化的“战争”中领先一步，是时候拨开云雾，一探未来安全趋势，从而有的放矢了。

而写这本书的目的便是试图站在智能产品产业链的各个关键环节来揭秘智能产品这一科技宠儿的安全大事。

目　录

第 1 章

智能产品与安全现状

1.1 智能产品概述

通常情况下，人们习惯性称呼的智能产品又叫智能硬件。智能硬件是继智能手机之后的一个科技概念，是通过软硬件结合的方式，对传统的设备进行改造，进而让其拥有智能化的功能。改造的对象可能是电子设备，如手表、电视和其他电器；也可能是以前没有电子化的设备，如门锁、茶杯、汽车甚至房子。智能化之后，硬件具备连接的能力，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。

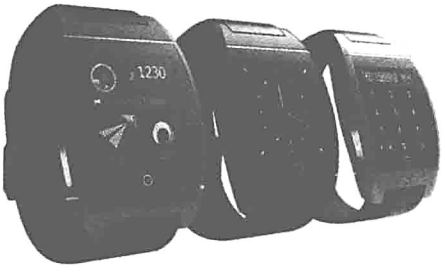
智能硬件已经从智能手机、可穿戴设备延伸到智能电视、智能家居、智能汽车、医疗健康、智能玩具、机器人等领域。比较典型的智能硬件包括 Google Glass、三星 Gear、FitBit、麦开水杯、咕咚手环、Tesla、乐视电视等。

1.1.1 手表手环

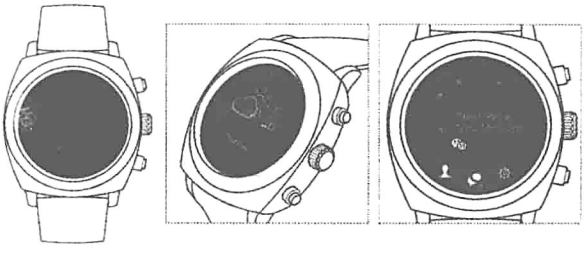
智能手表、智能手环仍然没有在这一拨热潮中降温。三星、LG、Sony 等厂商继续迭代智能手表产品。新产品苹果的 Apple Watch 等推出。

Apple Watch

在国内市场，Inwatch、土曼、果壳电子的智能手表也在继续迭代，思路也更加成熟，比如果壳电子开始重新定义产品的设计，改为圆形表盘。



Inwatch



果壳电子圆形表盘智能手表

1.1.2 智能电视

智能电视是具有智能操作系统的开放式平台，通过互联网连接，不仅可实现一般电视的播放功能，更可自行下载、安装、卸载各类应用软件，持续对功能进行升级和扩充。

智能电视

1.1.3 智能汽车

智能汽车就是在普通汽车的基础上增加了先进的传感器（雷达、摄像）、

控制器、执行器等装置，通过车载传感系统和信息终端实现与人、车、路等的智能信息交换，使汽车具备智能的环境感知能力，能够自动分析汽车行驶的安全及危险状态，并使汽车按照人的意愿到达目的地，最终实现替代人来操作的目的。

在汽车智能化仍然在逐渐推进的过程中，一批用于汽车的“智能穿戴”开始涌现出来，成为汽车全面智能化的过渡产物。

此类产品主要有两类，一种是车机类，主要是基于 Android 平台的汽车车机越来越多，在深圳有不少第三方团队在做此类产品研发，用于汽车后装市场；另一类是通过 OBD 通用数据接口，获得汽车的油耗、速度等常规数据，同时加入 GPS 模块，不仅可让汽车通过一个小配件进行 GPS 轨迹的记录，同时可以对司机驾驶习惯等进行大数据分析。

智能汽车

1.1.4　家庭安防

2014 年 1 月谷歌宣布 32 亿美元收购 Nest 之后，围绕家庭空间的智能设备就开始受到更多创业者和投资者的关注。

比如关注入户安全问题的“丁丁门磁”，让门的开关在手机掌握中。再比如欧瑞博因为推出了一款燃气报警器，开始受到小米的觊觎并抛出橄榄枝；传统家电厂商海尔在推出其 uHome 智能家居平台时，安防即是其重要一环。常见的安防类产品就是摄像头，如小米、360 家庭卫士、联想看家宝等。