

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

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问：北京大成律师事务所 韩光 / 邹晓东

# 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

## 前言

## 第 1 章 智能产品与安全现状 / 1

### 1.1 智能产品概述 / 1

1.1.1 手表手环 / 1

1.1.2 智能电视 / 2

1.1.3 智能汽车 / 2

1.1.4 家庭安防 / 3

1.1.5 虚拟现实 / 5

### 1.2 安全是永恒的主题 / 6

1.2.1 2014 年十大木马——不可不知 / 6

1.2.2 2014 年五大软件漏洞——不可不防 / 11

1.2.3 2015 年主要信息安全行业发展趋势 / 15

1.2.4 大数据、云计算和移动决胜网络安全 / 17

### 1.3 2015 年网络安全威胁预测 / 19

1.3.1 针对医疗行业的数据窃取攻击活动将会增加 / 20

1.3.2 物联网攻击将主要针对企业而非消费产品 / 20

1.3.3 信用卡盗窃犯将变身为信息掮客 / 20

1.3.4 移动威胁的目标是凭证信息而非设备上的数据 / 21

1.3.5 针对沿用数十年的源代码中的漏洞进行攻击 / 21

1.3.6 电子邮件威胁的复杂程度和规避能力将会大幅增加 / 21

1.3.7 全球网络攻击战场上将出现更多新的参与者 / 21

### 1.4 构筑安全屏障从何入手 / 22

## 第 2 章 云计算安全 / 23

- 2.1 云计算概述 / 23
  - 2.1.1 云计算定义 / 23
  - 2.1.2 云计算特征 / 24
- 2.2 2014 年云计算安全事件 / 24
  - 2.2.1 Dropbox / 25
  - 2.2.2 三星 / 25
  - 2.2.3 Internap / 25
  - 2.2.4 微软 Lync、Exchange / 26
  - 2.2.5 Verizon Wireless / 26
  - 2.2.6 No-IP.com 恶意中断 / 26
  - 2.2.7 微软 Azure / 26
  - 2.2.8 Amazon Web Services 的 CloudFront DNS / 27
  - 2.2.9 Xen 漏洞重启 / 27
- 2.3 云计算安全威胁 / 27
  - 2.3.1 数据丢失和泄露 / 27
  - 2.3.2 网络攻击 / 30
  - 2.3.3 不安全的接口 / 31
  - 2.3.4 恶意的内部行为 / 32
  - 2.3.5 云计算服务滥用或误用 / 33
  - 2.3.6 管理或审查不足 / 33
  - 2.3.7 共享技术存在漏洞 / 36
  - 2.3.8 未知的安全风险 / 37
  - 2.3.9 法律风险 / 37
- 2.4 云计算的关键技术 / 38
  - 2.4.1 虚拟化技术 / 38
  - 2.4.2 分布式海量数据存储 / 38
  - 2.4.3 海量数据管理技术 / 38
  - 2.4.4 编程方式 / 39
  - 2.4.5 云计算平台管理技术 / 39



## 2.5 云安全发展趋势 / 39

- 2.5.1 私有云的演变 / 40
- 2.5.2 云数据“监管”将影响管辖权法律 / 40
- 2.5.3 企业必须部署可行的云安全协议 / 40
- 2.5.4 确保移动设备以及云计算中企业数据安全成为企业关注的重心 / 40
- 2.5.5 灵活性将成为云计算部署的主要驱动力 / 40
- 2.5.6 云计算部署和不断变化的 CASB 解决方案将重绘 IT 安全线 / 41
- 2.5.7 泄露事故保险将成为常态 / 41

## 第 3 章 大数据安全 / 42

### 3.1 大数据概述 / 42

- 3.1.1 大数据的定义 / 42
- 3.1.2 大数据的特征 / 42
- 3.1.3 大数据产业现状 / 43
- 3.1.4 大数据面临的挑战 / 44

### 3.2 2014 年典型大数据事件 / 46

- 3.2.1 国科大开设大数据技术与应用专业 / 47
- 3.2.2 世界杯的大数据狂欢 / 47
- 3.2.3 支付宝首提数据分享四原则为大数据“立规矩” / 47
- 3.2.4 苹果承认可提取 iPhone 用户数据 / 48
- 3.2.5 影业纷纷引进大数据 / 48
- 3.2.6 日本构建海上“大数据路标” / 49
- 3.2.7 联合国与百度共建大数据联合实验室 / 49
- 3.2.8 美国海军将云计算和大数据技术用于远征作战 / 49
- 3.2.9 大数据剑指金融业 / 49
- 3.2.10 淘宝大数据打击假货 / 50

### 3.3 大数据的安全问题 / 50

- 3.3.1 大数据系统面临的安全威胁 / 50

- 3.3.2 大数据带来隐私安全问题 / 54
- 3.3.3 2014 年国内外数据泄密事件盘点 / 59
- 3.4 大数据安全保障技术 / 62
  - 3.4.1 数据信息的安全防护 / 62
  - 3.4.2 防范 APT 攻击 / 63
- 3.5 大数据安全发展趋势 / 73
  - 3.5.1 数据安全成为新一代信息安全体系的主要特征 / 73
  - 3.5.2 加密技术作为数据安全基础技术得到用户广泛接受 / 73
  - 3.5.3 数据安全建设成为助推信息安全与应用系统融合的发动机 / 73
  - 3.5.4 数据安全纳入主流行业信息安全标准体系 / 74
  - 3.5.5 数据安全品牌集中度显著提高 / 74

## 第 4 章 智能产品的硬件安全 / 75

- 4.1 对硬件的物理访问：形同虚设的“门” / 75
  - 4.1.1 撞锁技术及其防范对策 / 75
  - 4.1.2 复制门禁卡及其防范对策 / 76
- 4.2 对设备进行黑客攻击：“矛”与“盾”的较量 / 78
  - 4.2.1 绕过 ATA 口令安全措施及其防范对策 / 78
  - 4.2.2 针对 USB U3 的黑客攻击及其防范对策 / 79
- 4.3 默认配置所面临的危险：“敌人”在暗，你在明 / 80
  - 4.3.1 标准口令面临的危险 / 81
  - 4.3.2 蓝牙设备面临的危险 / 81
- 4.4 对硬件的逆向工程攻击：出手于无形 / 81
  - 4.4.1 获取设备的元器件电路图 / 81
  - 4.4.2 嗅探总线上的数据 / 83
  - 4.4.3 嗅探无线接口的数据 / 85
  - 4.4.4 对固件进行逆向工程攻击 / 85
  - 4.4.5 ICE 工具 / 87
- 4.5 智能硬件安全保障 / 89

- 4.5.1 移动终端安全防护 / 89
- 4.5.2 数据加密技术 / 95
- 4.6 2015 年智能硬件产业预测 / 97
  - 4.6.1 第三边界产业掀起新一轮商业浪潮 / 97
  - 4.6.2 2015 年智能硬件产业发展趋势 / 99
  - 4.6.3 2015 年将走进大众生活的智能硬件技术 / 101
  - 4.6.4 扩展阅读 / 103

## 第 5 章 智能产品操作系统使用安全 / 104

- 5.1 iOS 操作系统的安全 / 104
  - 5.1.1 iOS 概述 / 104
  - 5.1.2 iOS 8 / 105
  - 5.1.3 iOS 越狱 / 108
  - 5.1.4 iPhone 基本安全机制 / 109
  - 5.1.5 iOS “后门”事件 / 114
- 5.2 Android 操作系统的安全 / 115
  - 5.2.1 Android 基础架构 / 116
  - 5.2.2 Android 5.0 的三大安全特性 / 119
  - 5.2.3 Android 攻防 / 121
- 5.3 Windows Phone 操作系统的安全 / 127
  - 5.3.1 Windows Phone 概述 / 127
  - 5.3.2 破解 Windows Phone——铜墙铁壁不再 / 130
  - 5.3.3 Windows Phone 安全特性 / 131
- 5.4 智能硬件操作系统的发展新趋势——自成一家，多向进发 / 135
  - 5.4.1 Firefox：消除智能硬件隔阂，推进 Firefox 平台系统 / 135
  - 5.4.2 三星：欲借智能电视发展自家 Tizen 操作系统 / 136
  - 5.4.3 LG：下一代智能手表或放弃谷歌 Android Wear 系统 / 137
  - 5.4.4 微软、黑莓、Linux、谷歌、苹果：五大生态系统圈地汽车行业 / 138

## 第6章 智能产品无线网络使用安全 / 143

- 6.1 无线网络技术 / 143
  - 6.1.1 无线网络概述 / 143
  - 6.1.2 无线网络的类型 / 143
  - 6.1.3 无线网络的功能 / 144
- 6.2 无线通信技术——NFC / 145
  - 6.2.1 NFC 技术概述 / 145
  - 6.2.2 NFC 技术发展现状 / 152
- 6.3 无线通信技术——蓝牙 / 157
  - 6.3.1 蓝牙技术概述 / 157
  - 6.3.2 蓝牙技术的应用 / 162
  - 6.3.3 蓝牙技术应用的安全威胁及应对措施 / 167
- 6.4 无线通信技术——Wi-Fi / 170
  - 6.4.1 Wi-Fi 概述 / 170
  - 6.4.2 Wi-Fi 的应用 / 172
  - 6.4.3 Wi-Fi 应用的安全问题 / 173
- 6.5 无线网络的安全威胁 / 176
  - 6.5.1 被动侦听 / 流量分析 / 176
  - 6.5.2 主动侦听 / 消息注入 / 176
  - 6.5.3 消息删除和拦截 / 177
  - 6.5.4 伪装和恶意的 AP / 177
  - 6.5.5 会话劫持 / 177
  - 6.5.6 中间人攻击 / 178
  - 6.5.7 拒绝服务攻击 / 178
- 6.6 无线网络的安全技术 / 178
  - 6.6.1 安全认证技术 / 178
  - 6.6.2 数据加密技术 / 181

## 第7章 智能手机的安全 / 183

- 7.1 智能手机安全现状 / 183

- 7.1.1 手机安全环境日渐恶化 / 183
- 7.1.2 移动安全关乎个人、企业 and 国家 / 184
- 7.1.3 移动安全风险涉及产业链各环节 / 184
- 7.1.4 移动安全病毒危害不断 / 185
- 7.1.5 移动安全威胁渠道多样 / 186
- 7.1.6 移动互联网黑色利益链 / 186
- 7.1.7 厂商扎堆发力安全手机领域 / 187
- 7.1.8 运营商结盟厂商布局安全手机 / 188
- 7.2 2014 年智能手机安全事件 / 189
  - 7.2.1 iCloud 安全漏洞泄露名人裸照 / 189
  - 7.2.2 窃听大盗系列木马上演——现实版“窃听风云” / 189
  - 7.2.3 酷派安全漏洞事件 / 189
- 7.3 智能手机终端用户的安保 / 190
  - 7.3.1 如何安全使用 Wi-Fi / 190
  - 7.3.2 如何安全使用智能手机 / 190
  - 7.3.3 如何防范“伪基站”的危害 / 191
  - 7.3.4 如何防范骚扰电话、电话诈骗、垃圾短信 / 191
  - 7.3.5 出差在外，如何确保移动终端的隐私安全 / 192

## 第 8 章 移动支付的安全 / 193

- 8.1 移动支付概述 / 193
  - 8.1.1 移动支付的概念 / 193
  - 8.1.2 移动支付的基本要素 / 194
  - 8.1.3 移动支付的特征 / 197
  - 8.1.4 移动支付的发展现状 / 197
- 8.2 移动支付的安全现状 / 200
  - 8.2.1 移动支付技术的安全性比较 / 201
  - 8.2.2 近年移动支付安全事件 / 212
- 8.3 移动支付安全相关技术 / 214
  - 8.3.1 移动支付安全总体目标 / 214

- 8.3.2 移动支付安全技术方案 / 215
- 8.3.3 安全的手机支付 / 220
- 8.4 2015 年移动支付发展趋势 / 225
  - 8.4.1 从 Beacon 到移动支付 / 225
  - 8.4.2 新的支付方式 / 226
  - 8.4.3 无卡交易和有卡交易 / 226
  - 8.4.4 社交支付将找到盈利方式 / 227

# 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。

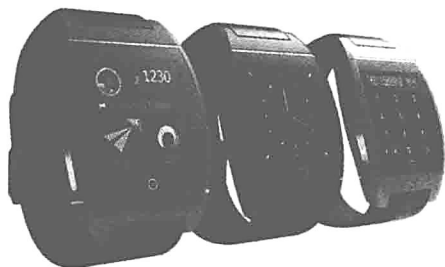
### 1.1.1 手表手环

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。

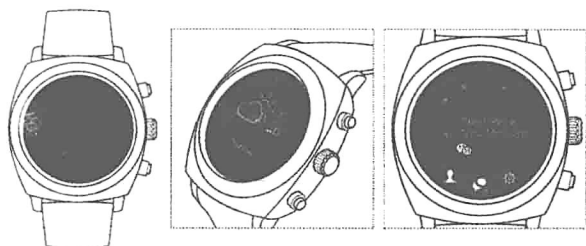


Apple Watch

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。