HZ BOOKS
华章IT

[PACKT] PUBLISHING

· 网络空间安全技术丛书 ·

PRACTICAL INTERNET OF THINGS SECURITY

# 物联网安全

[美] 布莱恩·罗素 (Brian Russell) 德鲁·范·杜伦 (Drew Van Duren) 著
李伟 沈鑫 侯敬宜 王自亮 译

全面阐述物联网面临的安全挑战并提供有效解决方案

机械工业出版社
China Machine Press

# 物联网安全

PRACTICAL
INTERNET OF
THINGS SECURITY



[美] 布莱恩·罗素 德鲁·范·杜伦 著
(Brian Russell) (Drew Van Duren)

李伟 沈鑫 侯敬宜 王自亮 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

物联网安全 /（美）布莱恩·罗素（Brian Russell），（美）德鲁·范·杜伦（Drew Van Duren）著；李伟等译 . —北京：机械工业出版社，2018.8
（网络空间安全技术丛书）
书名原文：Practical Internet of Things Security

ISBN 978-7-111-60735-9

I. 物… II. ①布… ②德… ③李… III. ①互联网络－安全技术 ②智能技术－安全技术 IV. ① TP393.4 ② TP18

中国版本图书馆 CIP 数据核字（2018）第 194881 号

本书版权登记号：图字 01-2016-8643



# 物联网安全

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：赵亮宇 责任校对：李秋荣
印 刷：北京市荣盛彩色印刷有限公司 版 次：2018 年 9 月第 1 版第 1 次印刷
开 本：186mm×240mm 1/16 印 张：16.75
书 号：ISBN 978-7-111-60735-9 定 价：75.00 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

华章IT
HZBOOKS | Information Technology

# 译 者 序

简单来说，物联网（Internet of Things，IoT）就是“物与物相连的互联网”，它将互联网的用户端延伸和扩展到任何物品，是在互联网的基础上延伸和扩展的网络。

随着智能硬件技术的兴起，物联网发展呈现指数级增长态势。据 Gartner 预测，2020 年物联网设备数量将高达 260 亿件。美国等发达国家将物联网作为国家级战略新兴产业快速推进，我国也将物联网正式列为国家五大新兴战略之一，在“十三五”规划中明确提出“发展物联网技术和应用”，并将“物联网应用推广”列为国家八大信息化专项工程之一。万物互联的时代大幕已然开启，万物互联已成为技术发展和产业应用的必然趋势。

与此同时，全球物联网安全事件频发，破坏力极大，物联网安全也已经成为全球普遍关注的话题。2015 ～ 2016 年年底，乌克兰电网因遭遇多次攻击而出现的大规模停电事件引起全球对物联网安全的高度关注及警惕。2016 年 10 月，Mirai 僵尸网络控制大量物联网设备发起流量高达 620Gb/s 的 DDoS 攻击，导致美国大半个国家断网，成为物联网安全的标志性事件。

万物互联，安全先行。毫无疑问，物联网安全是物联网发展首先要解决的问题。2016 年年底，美国国土安全部（Department of Homeland Security，DHS）发布了“保障物联网安全的战略原则”，认为“物联网安全已演变成为国土安全问题”。很多国家都在加快制定物联网安全的技术规范和法律法规。我们认为，每一位网络安全或物联网行业的从业人员都应该正视安全问题，都有责任和义务为每一个物联网产品或方案贡献自己的力量。

物联网面临的安全挑战包括：规模巨大、分布广泛的设备，多种多样的通信协议以及需要对所有物联网设备和用户开放的云 / 数据中心。传统的网络驱动安全模式（网络侧集中部署设备，统一防护安全攻击）已经难以满足物联网安全的要求。

本书作者皆为业界翘楚，努力为构建安全的物联网世界提供一个切实可行的安全指南。本书首先从物联网所带来的改变开始，引出物联网中存在的漏洞、面临的攻击以及

可采取的对策，详细阐述了物联网安全工程、密码学基础、身份识别与访问控制、隐私管理、合规监控、云安全以及物联网安全事件响应等诸多方面的内容，既涵盖了物联网设备安全、设备之间的通信协议安全，也介绍了一些物联网安全的最佳实践。

历史经验告诉我们，每当新事物兴起时，总会伴随新技术的革新。在物联网的大潮澎湃激荡之际，物联网安全的各项研究和产业化也必将提上日程。希望本书能帮助各位读者全面认识物联网安全，为物联网开发者、运营者以及安全解决方案、安全政策制定人员的物联网安全事业助一臂之力。

本书主要由李伟、沈鑫、侯敬宜、王自亮完成翻译。我们力求做到技术术语准确，但限于水平，如有错误或疏漏，恳请广大读者朋友批评指正。

# 关于作者

Brian Russell，美国 Leidos 公司计算机安全解决方案的首席工程师。他重点研究物联网安全，指导安全解决方案的设计与开发，以及客户隐私与可信控制的实施。Brian 关注的领域包括无人机系统（Unmanned Aircraft Systems，UAS）、车联网的安全工程以及安全系统的开发，其中包括高可信密钥管理系统。他有 16 年的信息安全从业经历，是云安全联盟（Cloud Security Alliance，CSA）物联网工作组的主席，也是联邦通信委员会（Federal Communications Commission，FCC）技术咨询委员会网络安全工作组的成员。Brian 还是互联网安全中心（Center for Internet Security，CIS）20 个关键安全控制编辑小组的志愿者和安全智慧城市（Securing Smart Cities，SSC）的倡议者（http://securingsmartcities.org/）。

欢迎加入云安全联盟物联网工作组：

@https://cloudsecurityalliance.org/group/internet-of-things/#_join

可通过如下网址与 Brian 联系：https://www.linkedin.com/in/brian-russell-65a4991。

---

非常感谢我的妻子——Charmae，以及孩子们——Trinity 和 Ethan。在写作本书期间，他们给予我的鼓励和爱是无价的。同时还要感谢云安全联盟物联网工作组所有伟大的志愿者和成员们，在过去的几年里，他们与我一起工作，使我能够更好地理解并提出物联网安全解决方案。最后，感谢我的父母，没有他们的鼓励我也难以完成本书。

---

Drew Van Duren，美国 Leidos 公司的高级密码学和网络安全工程师，有 15 年出色的从业经历，从事商业领域、美国国防部、交通部等安全系统的安全防护工作。最初，他是一名航空工程师，逐步涉足网络物理（交通系统）风险管理、安全加密通信工程，并为高可信度 DoD 系统设计安全网络协议。Drew 为联邦航空管理局的无人机系统集成部门

提供了很多安全意见，支撑 RTCA 标准，该标准用于在美国国家空域系统中飞行的无人机加密保护开发。此外，他还从事美国交通部联邦高速公路总署（FHWA）和汽车工业方面的工作，包括车联网通信设计的威胁建模和安全分析管理、安全系统、地面交通系统、通过已连接的车辆安全证书管理系统（SCMS）进行的密码认证操作。在进入交通工业领域工作前，Drew 是一名技术总监，负责管理两个最大的（FIPS 140-2）加密测试实验室，经常为多种国家安全程序的密钥管理和加密协议提供专家意见。他具有商业领航和操纵无人机系统的执照，还是 Responsible Robotics 有限公司的联合创始人，该公司致力于使无人机安全而负责任地飞行。

可通过如下网址与 Drew 联系：https://www.linkedin.com/in/drew-van-duren-33a7b54。

---

首先，非常感谢我的妻子——Robin，以及孩子们——Jakob 和 Lindsey。在写作本书期间，他们无边无际的爱、幽默和耐心一直陪伴着我。在我需要的时候，他们总是及时陪我娱乐。还要感谢我的父母，他们持续不断的爱、训导以及鼓励在我个性形成时期培养了我的多种爱好——建模、工程、航空、音乐。最重要的是，大提琴演奏使得我的生活更为丰富，需求更为集中。最后，要感谢我已去世的外祖父母，特别是我的外祖父——Arthur Glenn Foster，他对科学和工程的好奇心似乎永无止境，对我早年的成长影响巨大。

---

# 关于技术审校人员

Aaron Guzman 是洛杉矶区域著名的渗透测试人员，擅长应用程序安全、移动渗透测试、Web 渗透测试、物联网入侵以及网络渗透测试。之前他供职于诸如 Belkin、Symantec 以及 Dell 之类的技术公司，入侵代码，构建基础设施。凭借多年的经验，Aaron 曾在多个会议上做过报告，包括 Defcon、OWASP AppSecUSA 以及美国开发者代码训练营。他曾参与多个物联网安全指导手册的编写和应用程序安全相关开源社区项目的开发。此外，Aaron 还是南加州洛杉矶开放式 Web 应用程序安全项目（Open Web Application Security Project，OWASP）、云安全联盟 SoCal（CSA SoCal）以及高科技犯罪调查协会（HTCIA SoCal）小组组长。如需了解 Aaron 的最新研究进展，可关注其 Twitter 账号 @scriptingxss。

# 前言

很少会有人置疑物联网的出现带来了安全问题，包括信息安全、物理安全和私密性相关的问题。鉴于物联网的迅速产业化和受众多样化，在决定写作本书时我们所面临的一个主要挑战和目标是，如何以一种尽可能实用而又与具体行业无关的方式，来识别并提取核心的物联网安全原理。同样重要的是，我们需要平衡实际应用和背景理论知识，尤其是考虑到当前以及即将出现数量无法估计的物联网产品、系统和应用程序时。为此，本书包含一些基本的信息安全（以及物理安全）主题，并按照足够充分而又最小化范围的原则涵盖这些内容，因为我们需要在有意义的安全讨论中以它们作为参考点。在这些安全主题中，一些适用于设备（终端），一些适用于设备之间的通信连接，而剩下的则是针对更大型的组织。

本书的另一个目标是，在讲解安全指导内容的过程中，不再重复罗列当前网络、主机、操作系统、软件等对象中所应用的现有的大量网络安全知识，尽管我们知道其中某些内容对于物联网安全的讨论是有意义的。由于无意像售卖产品的产业或公司那样，因此我们致力于充分对实用安全技术进行创造并裁剪，这些技术中包含代表物联网和传统网络安全之间不同点和共通点的特性及差别。

当前，大量的传统产业（比如家电制造商、玩具制造商、汽车业等）和创业技术公司正在以惊人的速度创造和销售互联设备与服务。不幸的是，大部分都非常不安全——一些安全研究人员已经严肃地指出这一事实，他们常常带着一种真正的担忧。尽管他们的批评很多是有理有据的，但不幸的是，其中一些批评带有一定程度的傲慢自大。

然而有趣的是，一些传统产业在高可信度的物理安全和容错设计方面很先进。这些产业广泛利用一些核心的工程规范（机械、电器、工业、航天和控制工程）和高可信度的物理安全设计来规划产品和复杂系统，非常安全。很多网络安全工程师对这些规范及其对物理安全和容错设计的重要作用完全不了解。因此，我们在实现物联网安全目标的

过程中遇到了一个重大障碍：物理安全性、功能性和需要针对所定义的“信息物理系统”（Cyber-Physical System，CPS）进行设计并部署的安全工程规范，这三者之间无法协调。CPS 以多种方式将物理和数字工程规范整合在一起，学院课程和企业工程部门很少会处理这些规范。我们希望，传统产业工程师、安全工程师和其他技术管理人员能够学会更好地协调物理安全需求和可信信息安全目标之间的关系。

在从物联网中受益的同时，必须最大限度地阻止当前和未来物联网可能造成的伤害。要做到这一点，需要对其进行合理而又安全的保护。我们期望读者能够从本书中受益，找到有用的信息来保护自己的物联网。

## 本书所涵盖的内容

第 1 章，危险的新世界，介绍了物联网的基本概念，包括定义、使用，具体应用和实现方法等。

第 2 章，漏洞、攻击及对策，概述了将要学习的多种威胁以及相应的对抗方法。

第 3 章，物联网开发中的安全工程，讲解了物联网安全生命周期中的多个阶段。

第 4 章，物联网安全生命周期，详细介绍了物联网安全生命周期操作运行方面的内容。

第 5 章，物联网安全工程中的密码学基础，对所应用的密码学知识进行了介绍。

第 6 章，物联网身份识别和访问管理解决方案，深入挖掘研究了物联网的身份与访问管理机制。

第 7 章，解决物联网隐私问题，研究了物联网的私密性相关问题。同时，本章也试图帮助读者理解如何缓解这类问题。

第 8 章，为物联网建立合规监测程序，帮助读者探索如何创建一个物联网合规程序。

第 9 章，物联网云安全，对物联网相关的云安全概念进行了讲解。

第 10 章，物联网事件响应，介绍了物联网的事件管理和取证。

## 本书所需的基本环境

需要 4.3 版本的 SecurITree 软件，一个通用的台式或笔记本电脑，以及运行 Java 8 环境的 Windows、Mac 或 Linux 系统平台环境。

## 本书所针对的目标读者

本书以想要保障联通物联网机构的数据安全的IT安全专业人员（包括渗透测试人员、安全架构师以及白帽黑客）为目标读者。同时，商业分析人员和管理人员也能够从本书获益。

## 排版约定

警告或重要提示使用该图标显示。

# 目　录

# 第1章

# 危险的新世界

“当变革之风吹起时，一些人筑起围墙，另一些人则建造风车。”

——中国谚语

物联网正在改变一切。然而不幸的是，很多企业、消费者、商用技术设备所有者以及基础设施运营商很快会发现他们正身处于安全问题的险境之中。使所有设备变得“智能”，这个过程为网络罪犯、极端民族主义者创造了一大波疯狂的机会，也为安全研究人员带来了挑战。这些威胁将随着它们对经济、企业、商业贸易、个人隐私和物理安全的潜在影响而不断增多。塔吉特公司、索尼影业、普里梅拉蓝十字的保险公司，甚至白宫的人事管理部门（Office of Personnel and Management，OPM）都曝出了大量关于传统网络安全领域内的主要漏洞和安全事件，这些事件的曝光生动鲜活而又不那么令人愉快。一些漏洞使得公司及其CEO蒙羞或者垮台，而最重要的是对公民个体造成了重大损害。可见过去的网络安全技术已被证明是不合格的。现在看一下物联网世界，其中包括了诸如使用Linux嵌入式系统的智能电冰箱、联网洗衣机、汽车、可穿戴设备、植入式医疗设备、工厂机器人系统等设备，或者包括任何刚接入网络的设备。过去，很多这类企业从未认真考虑过信息安全方面的问题，然而随着企业之间竞争加剧及层出不穷的新产品、新功能，现在他们发现自己正处于不知道如何进行开发、部署和安全操作的危险境地。

在技术方面取得进步的同时，一直有一些人有意或无意地试图对这些先进技术展开攻击。如上所述，我们正处于安全噩梦的险境之中。通过这个论断想要说明什么？首先，物联网的技术创新发展与物联网的安全知识和安全意识觉醒急剧脱节。十年前难以想象