HZ BOOKS
华章IT

[PACKT]
PUBLISHING

· 网络空间安全技术丛书 ·

工业物联网安全

[美] 斯拉瓦尼·巴塔查尔吉 著 马金鑫 崔宝江 李伟 译
(Sravani Bhattacharjee)

- 工业互联网联盟首席技术官斯蒂芬·J. 梅勒鼎力推荐，全方位阐释工业物联网安全实践
- 涵盖用来设计基于风险的安全控制方案的各种实用工具
- 讨论多层防御技术相关的实用技能，包括 IAM、端点安全、互联技术以及基于边界和云环境的应用

机械工业出版社
China Machine Press

工业物联网安全

PRACTICAL
INDUSTRIAL INTERNET
OF
THINGS SECURITY

[美] 斯拉瓦尼 · 巴塔查尔吉 著
(Sravani Bhattacharjee)
马金鑫 崔宝江 李伟 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

工业物联网安全 /（美）斯拉瓦尼·巴塔查尔吉著；马金鑫，崔宝江，李伟译 . —北京：机械工业出版社，2019.5
（网络空间安全技术丛书）
书名原文：Practical Industrial Internet of Things Security

ISBN 978-7-111-62569-8

I. 工… II. ①斯… ②马… ③崔… ④李… III. 计算机网络－网络安全 IV. TP393.08

中国版本图书馆 CIP 数据核字（2019）第 077788 号

本书版权登记号：图字 01-2018-7388

工业物联网安全

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：张志铭
责任校对：殷 虹
印 刷：北京瑞德印刷有限公司
版 次：2019 年 5 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16
印 张：15.25
书 号：ISBN 978-7-111-62569-8
定 价：79.00 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
购书热线：（010）68326294
投稿热线：（010）88379604
读者信箱：hzit@hzbook.com

译 者 序

本书指出了工业物联网的安全边界及安全问题，通过实例提供了一系列解决方案，可作为工业物联网安全从业人员的指导用书。正如工业互联网联盟的斯蒂芬·J. 梅勒先生所说的，本书填补了工业物联网安全的概念框架和实践之间的空白，实用性较强，对于安全从业人员非常有益，值得细读。

本书的翻译在不偏离原意的前提下尽可能保证语句顺畅，使读者读起来不至于太生硬。对于其中翻译不到位的地方，还请读者见谅。

感谢对本书翻译工作付出辛勤劳动的北京邮电大学的陈晨、徐涵、张政、姚敏等，他们在相关专业术语的翻译方面提出了很多宝贵的建议。

本书的译者之一李伟博士在新婚燕尔之际抽出身来完成翻译工作，借本书祝愿他们夫妇百年好合。

感谢中国信息安全测评中心对本书的支持与帮助。

马金鑫

序　言

在大约 40 年前互联网刚刚出现时，没有人担心是否安全，甚至没有人考虑这方面的问题，因为没有必要——当时所设计的应用程序的主要用途是，在欧洲核子研究组织（CERN）的各个实验室之间共享非涉密的文件；而当时的互联网工作模式，主要是具有共享意愿的私人在进行交互。

作为一项重要的发明，统一资源定位符（URL）目前主要用于个人与业务的交互。通过互联网，我们可以使用网上银行、预订航班机票和酒店，以及提供信用卡信息等。由于互联网不再是一个简单的文件共享方案，因此安全就成为一个重要的问题。此外，健康档案通常都是在线保存的，并且我们（有时在不经意间）会通过社交媒体和提供特定服务（比如约会相亲）的网站来泄露大量的个人数据。我们希望这些数据能够作为秘密进行保存。因而，个人隐私理所当然地成为一个引人关注的问题。

如今，我们正在将各种实体连接到互联网。我们可以控制现实世界中的物理设备，互联网逐渐变成业务与实体进行交互的工作模式。因此，物理安全成了一个问题。此外，以无人驾驶汽车为例，不仅需要在安全气囊等物理层面实现安全配置，而且还需要在无人驾驶技术方面做到稳定可靠，从而保证不会在时速 65 英里[⊖]的情况下突然发生故障。它们需要具有足够的弹性，从而在汽车真正发生故障时，仍然能够平稳降速。

工业物联网（Industrial Internet of Things，IIoT）是由机器、计算机和人等各种实体组成的互联网，它将彻底改变经济和社会形态，但前提是它要有可信度。

可信度（可信赖性）是由**信息技术**（Information Technology，IT）和**运维技术**（Operational Technology，OT）两个领域中的信息安全性（它不再仅仅指网络中的安全）、私密性、物理安全性、可靠性和稳定性共同组合而成的概念。这个集合中包含了来自很多不同区域、使用不同术语（“安全”一词对于 IT 专家和工厂经理而言具有不同的含义），并且拥有不

⊖ 1 英里 = 1609.344 米。——编辑注

同时间线（在我们谈论的时候，IT 行业正在为我的手机更新换代，而一个化学工厂则需要进行大量的合规性检验）的人。这就要求我们对文化、进程、价值和重点进行仔细的思考和调整。

因此，可信度是一个复杂而昂贵的主题，其中包含了多个方面的内容和原则。它要求相关人员掌握全面的基础知识，从而提升安全意识、专业技能和实践能力。它直接关系到全世界经济和社会中的安全性、环境破坏以及伦理道德。然而，企业利益相关者和技术专家（包括系统开发人员、集成商和制造商）对于可信度还是缺乏全面的理解。想要使用 IIoT 的工业用户需要综合性的指导。

本书包含了 IIC 的相关工作、现有标准以及最佳实践，并将它们整合成一本安全从业人员的指导手册。它广泛适用于多个垂直领域，其目标读者主要是解决方案架构师以及任何负责 IIoT 安全的人员，旨在通过简短的篇幅来帮助他们理解 IIoT 所涉及的安全问题。本书将这些框架无缝结合在一起，展示了它们对于多种 IIoT 实例的实用性。

当今的工业界十分需要这样的资源。本书填补了概念框架和实践之间的空白，着重介绍了贯穿于生命周期的安全角色和责任，从业务实例和需求定义到开发和集成阶段，一直到部署与现场操作。除了 IIC 资源，读者还将发现其他一些有用的工业参考资料，包括 IEEE、IEC、OMG、云安全联盟、NIST 以及一些研究组织和学院等的研究成果。而就本书而言，我们将主要介绍 IIC 的关注内容和新方案。

本书并不是对 IIoT 安全的总结陈述，而更像是一段旅程的起点，读者可以从这里开始认识一个数字互联的世界，并且一起完善它，从而应对在可预见的将来可能会出现的安全挑战。

斯蒂芬·J. 梅勒

工业互联网联盟首席技术官

2018 年 6 月 27 日于美国加利福尼亚州拉荷亚

前　言

工业物联网（IIoT）正在为我们带来巨大的社会和经济机遇。它开启了一个自主机器和智能过程的崭新时代。然而，互联互通会带来一个不可避免的副作用，即我们将暴露于网络入侵的威胁之中。因此，安全性也就成为 IIoT 部署过程中人们最关注的问题。IIoT 安全性与物理系统的可靠性，以及人与环境的物理安全性等有着错综复杂的联系。

本书为读者提供了针对 IIoT 安全各个方面的内容，以及用来构建和部署安全 IIoT 解决方案的实践技术。在本书中，我们将从专业视角为读者介绍 IIoT 安全的基本原则、威胁模型、参考架构，以及现实生活中的案例分析。

本书涵盖了用来设计基于风险的安全控制方案的各种实用工具，并且深入讨论了多层防御相关技术，包括 IAM、端点安全、互联技术以及基于边界和云环境的应用，如此读者才能牢固掌握重要的安全规程。除了开发人员、架构师、生产经理、制造商和业务经理之外，很多相关人员都应该关注对 IIoT 生命周期中的流程、标准化操作、治理所进行的安全加固，以及对新兴技术（例如，区块链、AI/ 机器学习、TSN 以及量子计算）可用性所进行的评估，从而大规模地实现稳定且具有社会效益的互联系统。

本书读者对象

本书的目标读者是 IIoT 从业者，包括 IIoT 研究人员、安全专家、架构师、开发人员以及业务利益相关者。任何需要深入理解工业设施互联所带来的独特物理安全和信息安全挑战，以及需要学习实用方法来保护工业资产的人，都可以从本书中获益。

本书主要内容

第 1 章介绍基本的 IIoT 概念、定义，以及保护 ICS/SCADA/DCS 系统所面临的独特

挑战。本章还就一些典型 IIoT 用例的安全评估工作进行了深入研讨。

第 2 章帮助读者深入理解工业应用中的数据流、参考架构以及 IIoT 的风险管理方法。最后，本章基于**工业互联网安全框架**（Industrial Internet Security Framework，IISF），建立了一个端到端的 IIoT 安全架构。

第 3 章全面介绍用于保护 IIoT 架构的身份与访问控制技术及其演化发展。

第 4 章介绍端点安全的重要主题，帮助读者真正理解保护 IIoT 端点的重要性、挑战以及解决方案。

第 5 章介绍**工业互联网连接框架**（Industrial Internet Connectivity Framework，IICF），同时从深度与广度两方面探讨 IIoT 连接技术和架构，从而帮助读者深入洞察其安全态势。

第 6 章利用现实中的 IoT 系统云环境示例，讲解从边界到云端保护 IIoT 应用的安全技术。

第 7 章讨论 IIoT 安全在管理与治理方面的重要角色，目的是为业务经理和业内人士提供一些指导意见。

第 8 章帮助读者理解众多的新兴技术，并在保护联网的工业用例方面对其进行评估。

第 9 章涉及本书讨论的 IIoT 安全的各个方面，并且结合实例进行讲解。

第 10 章对本书提到的技术发现进行简要总结，并对下一步要做什么进行了总结陈述与展望。

如何使用本书

为满足具有 IT 或业务背景的技术专业人员以及组织的业务经理的需求，本书进行了精心编排。第 3 ～ 6 章都包含了一些高级内容，因此要求读者具有一定的 IT 背景，并具有一些工业方面的基础知识。其余章节则为具备技术和业务背景的 IIoT 从业人员提供了至关重要的知识。

下载本书彩图

本书中所用的截图和样图，可以从 http://www.packtpub.com 通过个人账号下载，也可以访问华章图书官网 http://www.hzbook.com，通过注册并登录个人账号下载。

本书约定

警告或重要的注意事项。

小建议或小窍门。

作者简介

Sravani Bhattacharjee 是一名数据通信技术专家，拥有 20 多年的从业经历。2014 年以前，她作为思科（Cisco）公司技术主管领导主持了针对多家企业的云端 / 数据中心解决方案的架构设计和安全评估工作。作为 Irecamedia 公司的负责人，她目前致力于与工业物联网创新团体合作，通过制订行业白皮书以及发表各种评论和技术营销内容来推动相关认识和商业决策的进步。她是一名 IEEE 物联网小组成员、一位作者以及一位演说家，她拥有电子工程专业硕士学位。

我真诚地感谢行业同仁为本书所提出的意见、所付出的宝贵时间以及所给予的支持。特别感谢微软公司的 Arjmand Samuel、RTI 公司的 Stan Schneider、Mocana 公司的 Dean Weber、IIC（工业互联网联盟）的 Stephen Mellor、思科公司的 Paul Didier 和通用电气公司的 Rebecca Lawson。RTI 公司的 Rajive Joshi 和 Infineon 公司的 Steve Hanna 的主动帮助与支持令我感动。感谢我所有的家庭成员和朋友们，在我完成本书的过程中不断地提供关心与帮助。

评审者简介

Sven Schrecker 是 Intel 公司物联网安全解决方案小组的首席架构师。他主要负责设计开放且基于标准的平台与策略来实现跨传统和新型技术的端到端物联网安全，并利用硬件和软件解决方案来显著提高嵌入式与工业部署方面的安全性。同时，他还是 IIC 安全工作组主席，致力于提高 IIoT 的整体安全能力。他发明了 40 余项与安全相关的专利，这些专利或处于申请阶段，或已经获得专利权。

免责声明

本书中的所有内容仅可在合乎道德的前提下使用。如果你未获得设备所有者的书面许可，则请勿使用本书中的任何信息。如果你采取非法行动，则可能会受到法律范围内的拘捕或起诉。如果你滥用本书中的任何信息，那么出版社不承担任何责任。此书中的信息只能在适当人员书面授权的测试环境下使用。

目　录