安全技术经典译丛

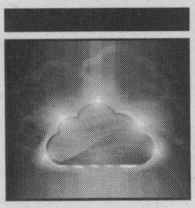
物联网安全

Securing the Internet of Things

[美] 李善仓(Shancang Li) 著
许立达(Li Da Xu)
梆梆安全研究院 译

ELSEVIER
清华大学出版社

安全技术经典译丛



物联网安全

[美] 李善仓(Shancang Li) 著
许立达(Li Da Xu) 著
梆梆安全研究院 译

清华大学出版社
北 京

北京市版权局著作权合同登记号 图字：01-2018-0457

图书在版编目(CIP)数据

物联网安全 / (美)李善仓(Shancang Li)，(美)许立达(Li Da Xu)著；梆梆安全研究院 译. —北京：清华大学出版社，2018
(安全技术经典译丛)
书名原文：Securing the Internet of Things
ISBN 978-7-302-50719-2

Ⅰ. ①物… Ⅱ. ①李… ②许… ③梆… Ⅲ. ①互联网络－应用－安全技术 ②智能技术－应用－安全技术 Ⅳ. ①TP393.4②TP18

中国版本图书馆 CIP 数据核字(2018)第 170756 号

责任编辑：王　军　韩宏志
封面设计：孔祥峰
版式设计：思创景点
责任校对：牛艳敏
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市国英印务有限公司
经　　销：全国新华书店
开　　本：148mm×210mm　　印　　张：4.875　　字　　数：135 千字
版　　次：2018 年 10 月第 1 版　　印　　次：2018 年 10 月第 1 次印刷
定　　价：49.80 元

产品编号：077462-01

Elsevier (Singapore) Pte Ltd.
3 Killiney Road, #08-01 Winsland House I, Singapore 239519
Tel: (65) 6349-0200; Fax: (65) 6733-1817

Securing the Internet of Things
Shancang Li, Li Da Xu

ISBN-13: 9780128044582

This translation of Securing the Internet of Things by Shancang Li, Li Da Xu was undertaken by Tsinghua University Press and is published by arrangement with Elsevier (Singapore) Pte Ltd.

Securing the Internet of Things by Shancang Li, Li Da Xu 由清华大学出版社进行翻译，并根据清华大学出版社与爱思唯尔(新加坡)私人有限公司的协议约定出版。

物联网安全　(梆梆安全研究院译)
ISBN：978-7-302-50719-2

作者简介

李善仓(Shancang Li)是西英格兰大学计算机科学与创新技术系的高级讲师。Shancang 曾在爱丁堡龙比亚大学任教，并在布里斯托大学的密码学小组任安全研究员，从事多个行业和技术领域的移动/数字取证工作。他在安全研究领域的背景包括网络渗透测试、无线安全、移动安全和数字取证。

许立达(Li Da Xu)，IEEE 院士和俄罗斯工程院院士，美国弗吉尼亚州诺福克奥多明尼昂大学信息技术和决策科学系杰出教授，2016 年入选汤森路透的“高被引用科学家(HCR)”名录。据汤森路透称：“2016 年度的高被引用科学家代表了世界上一些最具影响力的科学头脑。”

许立达是 IFIP TC8 WG8.9 的创始人；IEEE SMC 社会技术委员会信息系统的创始人；*Journal of Industrial Information Integration* (Elsevier BV)、*Journal of Industrial Integration and Management* (World Scientific)、*Enterprise Information Systems* (Taylor & Francis)的创始主编；*Frontiers of Engineering Management* (Higher Education Press)和 *Journal of Management Analytics* (Taylor & Francis)的联合创始主编。

除这些显著成就外，许立达博士还是中国教育部授予的“长江学者”讲座教授。许立达博士的合作单位包括中国科学院计算技术研究所、中国科学技术大学、上海交通大学、中国国务院发展研究中心和美国弗吉尼亚州奥多明尼昂大学。

他参加了系统科学与工程学科的早期研究和教育学术活动。许立达博士与 West Churchman、John Warfield、钱学森等知名学者进行过广泛的合作与交流。此外，他领导了早在 20 世纪 80 年代初开始的以信息系统和企业系统为主题的早期研究和教育学术活动。

许多人认为他是产业信息集成工程这一新兴学科的创始人之一。他是《企业集成与信息体系架构》的作者，也是《系统科学方法论》一书的合著者。包括钱学森在内的许多知名学者都在他们的重要研究中引用了他的著作。

目　录

第 1 章

简介：物联网安全

1.1 引言

新兴的物联网(Internet of Things，IoT)被认为是下一代的互联网。由于物联网中数十亿设备互相连通，它也将成为对黑客极有吸引力的目标(Roman et al.，2011)。物联网中的每个物理对象都能够在没有人干预的情况下进行交互(Bi et al.，2014)。近年来，物联网在各种基础设施中的应用都已得到发展，如物流、制造业、医疗保健、工业监控等(ITU，2013；Pretz，2013)。许多尖端技术(如智能传感器、无线通信、网络、数据分析技术、云计算等)都已被研发出来以帮助物联网在不同智能系统中充分发挥潜力(Bi et al.，2014；Tan et al.，2014)。然而，物联网技术仍处于初级阶段，还有许多与物联网相关的技术难题需要攻克(Li et al.，2014c)。物联网中最显著的一个技术障碍是安全(Li et al.，2014c)，它涉及基础设施安全性、通信

网络安全性、应用安全性和一般系统安全性的感知(Keoh et al.，2014)。为了解决物联网中的安全挑战，我们将基于四层架构分析物联网中的安全问题。

1.1.1 概述

物联网的概念在1999年被首次提出(Li et al.，2014c)，而其确切定义仍随着不同视角的变化而改变(Hepp et al.，2007；ITU，2013；Li et al.，2014c；Pretz，2013)。物联网被认为是未来新一代的互联网；它集成了不同范围的技术，包括传感、通信、网络、面向服务的体系结构(Service-oriented Architecture，SoA)和智能信息处理技术(Council，2008；Li et al.，2014c；Lim et al.，2013)。然而，它也带来了一系列严峻挑战，比如安全性、混合网络、智能传感技术等。其中安全性是最主要的，它从根本上保护着物联网免受攻击和发生故障(Roman et al.，2011)。传统意义上，安全意味着密码学、安全通信和隐私保护。然而，物联网安全囊括更广泛的任务，包括数据机密性、服务可用性、完整性、反恶意软件、信息完整性、隐私保护、访问控制等(Keoh et al.，2014)。

作为一个开放的生态系统，物联网安全与其他研究领域有很多交集。物联网的多样性使其非常容易受到针对可用性、服务完整性、安全性和隐私的攻击。在物联网底层(感知层)，传感设备/技术的计算能力和电源供应都非常有限，不能提供很好的安全保护；在中间层(如网络层、服务层)，物联网非常依赖网络和通信，易于遭受窃听、拦截和拒绝服务(Denial of Service，DoS)的攻击。例如，在网络层中，没有集中控制的自组织拓扑容易受到节点复制、节点抑制、节点假冒等身份认证攻击。而在上层(如应用层)，数据聚合和加密对改善所有各层的可扩展性和脆弱性问题非常有用。为了构建值得信赖的物联网，我们需要一个系统级安全分析和自适应安全策略框架。

1.1.2　前沿进展

物联网是互联网的延伸，通过整合移动网络、互联网、社交网络和智能设备为用户提供更好的服务或应用(Cai et al.，2014；Gu et al.，2014；Hoyland et al.，2014；Kang et al.，2014；Keoh et al.，2014；Li et al.，2014a；Li et al.，2014b；Tao et al.，2014；Xiao et al.，2014；Xu et al.，2014a；Xu et al.，2014b；Yuan Jie et al.，2014)。物联网的成功取决于各级安全的标准化，它在全球范围内提供安全的互操作性、兼容性、可靠性和有效性(Li et al.，2014c)。如今，物联网已被许多国家认定为国家战略的重中之重。欧洲物联网研究项目组(IoT European Research Cluster，IERC)赞助了许多物联网基础研究项目：IoT-A 为物联网设计了参考模型和体系结构，而正在进行的 RERUM 项目则着眼于物联网安全(Floerkemeier et al.，2007；Gama et al.，2012；Welbourne et al.，2009)。日本政府提出了“u-Japan”和“i-Japan”的战略，以推进可持续的信息、通信和技术(Information Communication and Technology，ICT)社会(Ning，2013)。在美国，信息技术和创新基金会(Information Technology and Innovation Foundation，ITIF)则着重于新的物联网信息和通信技术(He and Xu，2012；Xu，2011)。韩国则推出了 RFID / USN 和“新 IT 战略”项目，以推进物联网基础设施的发展(Xu，2011)。中国政府于 2010 年正式启动了“感知中国”计划(Bi et al.，2014)。

从技术上说，多种多样的网络和通信技术都可被应用于物联网，例如 Wi-Fi、ZigBee(IEEE 802.15.4)、低能耗蓝牙(Low Energy Bluetooth，BLE)、ANT 等。更具体地说，互联网工程任务组(Internet Engineering Task Force，IETF)已经将基于 IPv6 的低功耗无线个域网(IPv6 over Low-Power Wireless Personal Area Networks，6LoWPAN)、低功耗路由算法(Routing over Low-power and Lossy-networks，ROLL)和受限应用协议(Constrained Application Protocol，CoAP)标准化以应用于资源受限的设备(Cai et al.，2014；Chen et al. 2014；Esad-Djou，2014；Gu et al.，2014；Hoyland et al.，2014；HP Company，2014；

Kang et al.，2014；Keoh et al.，2014；Li and Xiong，2013；Li et al.，2014a；Oppliger，2011；Raza et al.，2013；Roe，2014；Tan et al.，2014；Wang and Wu，2010；Xiao et al.，2014；Xu et al.，2014a，b；Yao et al.，2013)。对软件真实性和知识产权保护的担忧产生了各种各样的软件验证和证明技术，通常称为可信启动(Trusted Boot)或可测启动(Measured Boot)。数据的机密性始终是一个主要问题。目前，相关安全控制机制已被开发，以确保无线通信和移动通信中数据传输的安全性，例如 802.11i(WPA2)或 802.1AE(MACsec)。最近，Raza et al. (2012)中报道了 RFID 市场的安全标准。对于 RFID 应用，欧盟委员会(European Commission，EC)已经发布了一些建议，以合法、道德、社会可接受的方式概述以下安全问题(Di Pietro et al.，2014；Esad-Djou，2014；Furnell，2007；Gaur，2013；HP Company，2014；Raza et al.，2012；Roe，2014；Roman et al.，2013；Weber，2013)：

- 衡量 RFID 应用的部署，以确保国家立法符合欧盟数据保护指令(EU Data Protection Directive)95/46、99/5 和 2002/58。
- 提出评估隐私和数据保护影响的框架(PIA；No.4)。
- 评估个人资料和隐私保护申请实施的影响(No.5)。
- 识别可能引发信息安全威胁的任何应用程序。
- 检查信息。
- 发布有关隐私信息的建议和 RFID 使用的透明度。

但对于物联网来说，安全问题仍然是一个具有挑战性的领域。物联网中可能连接数十亿台设备，我们仍需要精心设计安全架构来充分保护信息并使数据在物联网上安全共享。

物联网应用层出不穷，而这将带来新的安全挑战。例如：

- 产业安全问题。包括智能传感器、嵌入式可编程逻辑控制器(Programmable Logic Controller，PLC)、机器人系统等，而它们通常会与物联网基础设施集成在一起。物联网产业基础设施的安全控制是一个大问题。
- 混合系统安全控制。物联网可能涉及很多混合系统，如何提供跨系统的安全保护对于物联网的成功至关重要。

- 对于在物联网中创建的新业务流程，需要保护业务信息和数据。
- 物联网终端节点的安全性。如何使终端节点及时接收软件更新或安全补丁，而不影响功能安全性是一个挑战。

1.1.3　安全需求

在物联网中，每个连接的设备都可能成为物联网基础设施或个人数据的潜在入口(HP 公司，2014；Roe，2014)。数据安全和隐私问题非常重要，但由于互操作性、混搭和自主决策性导致了系统的复杂性、安全漏洞和潜在漏洞，与物联网相关的潜在风险也因而达到一个新的级别。因为复杂系统可能会造成更多与服务有关的漏洞，隐私风险也将在物联网中出现。在物联网中，许多信息与我们的个人信息有关，如出生日期、地点、预算等。这是大数据挑战的一个方面，安全专家需要确保他们能考虑到整个数据集的潜在隐私风险。物联网应以合法、道德、社会可接受的方式实施，同时考虑到法律挑战、系统方法、技术挑战和业务挑战。本章重点介绍安全物联网架构的技术实现设计。在整个物联网生命周期中，从初始设计到运行服务都必须解决安全问题。如图 1-1 所示，物联网场景中的主要研究挑战包括数据机密性、隐私性和信任(Di Pietro et al.，2014；Furnell，2007；Gaur，2013；Miorandi et al.，2012；Roman et al.，2013；Weber，2013)。

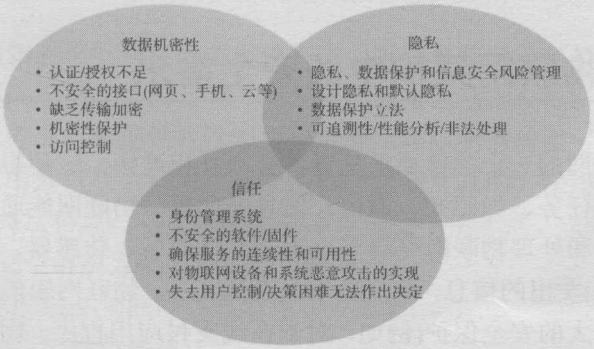


图 1-1　物联网中的安全问题

为更好地说明物联网的安全需求，我们将物联网建模为四层体系结构：感知层、网络层、服务层和应用接口层。每一层都能够提供相应的安全控制，如访问控制、设备认证、数据完整性和传输机密性、可用性以及防病毒或攻击的能力。在表 1-1 中，我们总结了物联网中最重要的安全问题。

表 1-1　物联网中最脆弱的十大环节

安全问题	应用接口层	服务层	网络层	感知层
不安全的 Web 接口	√	√	√	
认证/授权不充分	√	√	√	√
不安全的网络服务		√	√	
缺少传输加密		√	√	
隐私问题		√	√	√
不安全的云接口	√			
不安全的移动接口	√		√	√
不安全的安全配置	√	√	√	
不安全的软件/固件	√		√	
物理安全性差			√	√

安全需求取决于每个具体的感知技术、网络和层级，下面会逐一讨论。

1.2　物联网架构中的安全需求

物联网的一个关键要求是设备必须互相连接，这使得它能够执行特定的任务，如感知、通信、信息处理等。物联网能通过网络获取、传输和处理物联网终端节点(如 RFID 设备、传感器、网关、智能设备等)发出的信息，完成高度复杂的任务。物联网应能为应用程序提供强大的安全保护(例如，对于在线支付应用程序，物联网应能

保护支付信息的完整性)。

物联网系统架构必须能为物联网提供运营保障，成为物理设备和虚拟世界之间的桥梁。在设计物联网框架时，应考虑以下因素：

(1) 技术因素，如传感技术、通信方式、网络技术等；

(2) 安全保护，如信息的机密性、传输的安全性、隐私保护等；

(3) 业务问题，如业务模型、业务流程等。

目前，面向服务的体系结构(SoA)已经成功应用于物联网设计，应用正朝面向服务的集成技术发展。在商业领域，各种服务之间的复杂应用已经出现。这些服务位于物联网的不同层面，如感知层、网络层、服务层和应用接口层。基于服务的应用将很大程度上取决于物联网的架构。图 1-2 描绘了一个通用的物联网 SoA，它由四层组成。

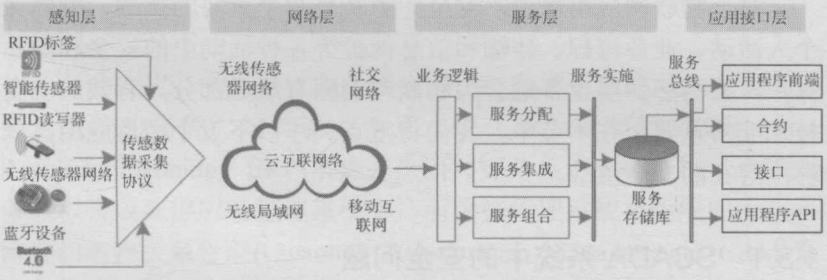


图 1-2　物联网 SoA 架构(Bi et al.，2014)

- **感知层**与物联网终端组件集成，感知和获取设备信息。
- **网络层**是支持设备间无线或有线连接的基础设施。
- **服务层**用来提供并管理用户或应用程序所需的服务。
- **应用接口层**由与用户或应用程序之间交互的方法组成。

基于每层特点，各层的安全需求可能会有所不同。一般来说，物联网的安全解决方案应考虑以下需求：

(1) 感知层和物联网终端节点安全需求；

(2) 网络层安全需求；