信息科学技术学术著作丛书

物联网安全

胡向东　魏琴芳　向　敏　等　著

科学出版社

信息科学技术学术著作丛书

物联网安全

胡向东　魏琴芳　向　敏　等　著

科学出版社
北京

内 容 简 介

本书是作者从事多年物联网安全相关科研工作实践的结晶。本书较全面、系统、深入地论述了物联网安全的基本理论、专门技术和最新发展。全书共14章，内容包括绪论、物联网安全的密码理论、无线传感器网络安全概述、密钥管理、非正常节点的识别、入侵检测、认证、安全成簇、安全数据融合、安全路由、安全定位、物联网中的抗干扰、射频识别的隐私与安全、物联网嵌入式系统的安全设计。

本书可供从事物联网安全和可靠应用的管理决策人员、与物联网安全相关领域应用和设计开发的研究人员、工程技术人员参考，也可作为高等院校物联网工程、信息安全、测控技术与仪器、自动化、通信工程、计算机应用等专业高年级本科生和研究生教材。

图书在版编目(CIP)数据

物联网安全/胡向东等著. —北京：科学出版社，2012
（信息科学技术学术著作丛书）
ISBN 978-7-03-033913-3

Ⅰ.物… Ⅱ.胡… Ⅲ.①互联网络-应用-物流②互联网络-安全技术
Ⅳ.①TP393.4②F253.9

中国版本图书馆CIP数据核字(2012)第053334号

责任编辑：张艳芬 / 责任校对：包志虹
责任印制：赵 博 / 封面设计：陈 敬

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2012年4月第 一 版 开本：B5(720×1000)
2012年4月第一次印刷 印张：22 3/4
字数：436 000

定价：72.00元

（如有印装质量问题，我社负责调换）

作者简介

胡向东(1971—),博士,教授,中国计算机学会计算机安全专业委员会委员、教育部“工程应用型自动化专业课程体系研究与教材建设委员会”委员,重庆市第二届学术技术带头人,“传感器与自动检测技术”国家精品课程负责人。

主要从事网络化测控及其信息安全、复杂系统建模、仿真与优化等方向的研究工作。作为项目负责人承担国家高新技术研究计划(“863”计划)项目、国家科技重大专项、国家自然科学基金项目等20余项,主持重庆市重点教改研究课题等10项;在国际、国内重要期刊和会议上发表学术论文50余篇,其中30余篇被三大检索系统收录;主编普通高等教育“十一五”国家级规划教材《应用密码学》、《应用密码学(第2版)》,撰写《传感技术》、《传感器与检测技术》、《智能检测技术与系统》、《物联网安全》等著作8部;获重庆市科技进步奖一等奖、三等奖各1项,获国家级教学成果奖二等奖1项、重庆市高等教育教学成果奖二等奖1项;指导学生获全国计算机仿真大赛全国二等奖2项、全国大学生“飞思卡尔”杯智能汽车竞赛全国总决赛二等奖1项。

《信息科学技术学术著作丛书》序

21世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的新动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术，超级计算机、软件和信息存储技术，数据知识化和基于知识处理的未来信息服务业，低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性；体现出科学出版社“高层次、高质量、高水平”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国科学院计算技术研究所所长

李国杰

前　言

为加快转变经济发展方式、促进经济结构的战略性调整，引领经济社会走上创新驱动、内生增长、科学发展的轨道，我国正在大力培育和发展战略性新兴产业。战略性新兴产业体现了新兴科技和新兴产业的深度融合，既代表科技创新的重要方向，也代表产业发展的重要方向，具有市场前景广阔、经济技术效益好、带动性强的突出特点。随着“工业化与信息化融合”、“智慧地球”、“传感中国”等理念的提出，物联网作为战略性新兴产业的重要代表性领域，掀起了第三次信息技术浪潮。不断发展的信息技术正在快速地改变着人们的工作模式、生活习惯和思维方式，越来越多的信息安全问题如影随形，物联网的安全和隐私保护问题亟待解决。

物联网作为一个大的产业链，是一个多学科交叉的综合应用领域。尽管科技界、产业界、政府部门以及广大普通民众基于各自不同的背景对物联网有不同的理解和体会，但有一点是共同期待和永恒坚持的，即“没有安全就没有应用，没有应用就没有发展”，在越来越强调生命尊严和生活质量的今天，与人们的生产、生活息息相关的物联网的安全尤其重要！

本书是作者从事多年的物联网安全相关科研工作实践的结晶。本书从提出写作构想、准备资料、总结研究成果，到最终完稿，经历了四年多的艰苦努力与再三凝练，同时深刻见证了物联网技术与产业的快速进步，以及对物联网安全快速增长的需求与期待。基于物联网特有的分布、技术和物权等属性，物联网对攻击者展现出前所未有的吸引力，并暴露出明显的安全脆弱性。与传统信息安全问题不同的是：一方面，传统的信息安全技术难以直接应用于物联网并保证其安全目标的实现；另一方面，物联网安全与国家安全、人身安全、隐私保护等密切相关，涉及物理上实实在在的财物与生命安全，不再仅仅是信息安全问题，而且我国在物联网的关键软硬件国产化方面还有很多工作要做，因此物联网的安全备受关注。物联网既是多学科交叉综合应用的产物，又处于技术和产业成熟前的快速发展期，物联网的安全解决方案正处于积极的研究探索阶段，其安全目标的实现任重而道远，目前还没有完全成熟、定型、系统的物联网安全解决方案。本书是当前物联网相关安全方案的系统总结，多角度展示了物联网安全不同专题、不同方向的研究成果，作者希望借此抛砖引玉，启发并催生出更多创新性研究成果，推动物联网安全解决方案尽快走向成熟、趋于完善，早日实现物联网科技惠及民生的美好愿景。

本书由重庆邮电大学胡向东教授组织撰写，第 2 章由魏琴芳撰写，第 5 章由胡向东、余朋琴撰写，第 7 章由胡向东、丰睿撰写，第 9 章由胡向东、唐贤伦、冯志宇撰

写，第 12 章由向敏、胡向东撰写，胡向东负责其余章节的撰写和全书的统稿。特别感谢参考文献中所列各位作者，包括未能在参考文献中一一列出资料的作者，正是因为他们在各自领域的独到见解和特别的贡献为作者提供了宝贵的参考资料、研究视角和丰富的写作源泉，使作者能够在系统总结本领域科研工作成果的基础上，汲取各家之长，及时形成本书。

参加本书资料搜集整理、仿真实验的还包括王泉、罗志勇博士和万天翔、张力、王雪、赵代娜、崔鹏、尚可、韩恺敏、许宏如、张玉函、白润资、汤其为等研究生；刘宴兵教授为本书的撰写提供了富有建设性的指导和建议。在此对他们付出的辛勤劳动表示由衷的感谢。本书的出版受到重庆邮电大学出版基金资助，并得到国家自然科学基金项目（61170219）、重庆市科委自然科学基金项目（CQ CSTC2009BB2278，CSTC2011jjA40028）、重庆市教委研究项目（113029）、2011 重庆市高等学校优秀人才支持计划项目和重庆邮电大学自然科学基金项目（A2011-15、A2011-17）的资助。

物联网安全的内涵丰富、多学科交叉特征明显、技术发展迅速、应用需求多样，对本书的撰写是作者在此领域的一次努力尝试，限于作者的水平和学识，书中难免存在疏漏和错误之处，诚望读者不吝赐教，以利修正，让更多的读者获益（huxd@cqupt. edu. cn）。

作　者

2011 年 9 月

目　录

第1章 绪 论

1.1 物联网概念的形成

随着当代生产力的快速发展，多学科科学技术交叉融合的推动，以及不断增长的应用需求的递进牵引，以“智能化”为核心的物联网应运而生。物联网就是“物品的互联网”(the Internet of things，IoT)，可以认为是传统的物流信息化工作的进一步深化与综合，也是传统互联网的使用对象由人及物在应用范围上的延伸和扩展，将互联网的用户终端由个人电脑延伸到任何需要实时管理的物品，其目的是让没有生命、为人服务的物品也能“开口说话”，通过网络实现互联互通，允许人和物在任何时间(anytime)、任何地点(anywhere)，使用任何的路径或网络(any path/any network)、任何的服务或业务(any service/any business)，与任何的事物或设备(anything/any device)、任何人(anyone)无缝地联系，将聚合(convergence)、内容(content)、知识库(collections)、计算(computing)、通信(communication)和连接(connectivity)等元素集成在一起形成一个有机的整体(见图 1.1)，从而加强人与

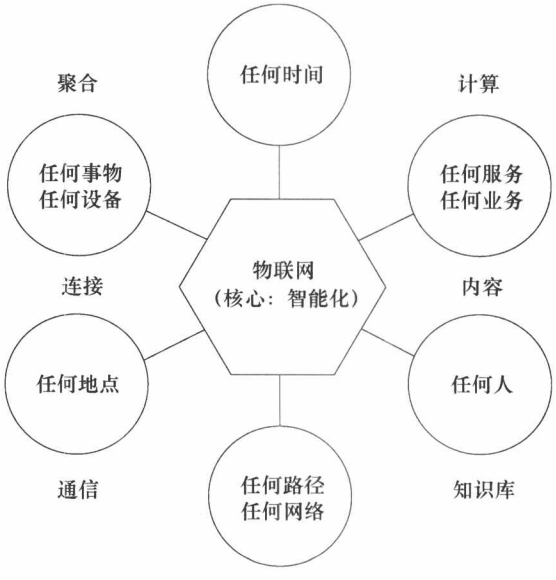

图 1.1 物联网的基本内涵

物、物与物等的信息交流，实现更高的工作效率，节省操作成本，体现“服务的智能化”和“科技惠及民生”的本质[1]。

物联网中的“物”是时空范围内存在的、可以被标识和识读的实际（物理）的或数字（虚拟）的实体，它们通常可通过分配的身份（identity，ID）号、名称或位置地址来识别。应用创新是物联网技术的发展核心，国际电信联盟（ITU）于 2005 年在一份报告中曾描绘“物联网”时代的图景：当司机出现操作失误时汽车会自动报警；公文包会提醒主人忘带了什么东西；回家前先发条短信，浴缸就能自动放好洗澡水等[2]。

物联网的概念大致起源于 1999 年美国麻省理工学院自动识别中心（MIT AutoID Center）给出的“物联网”理念，即在计算机互联网基础上，利用射频识别（radio frequency identification，RFID）、无线数据通信等技术，构造一个覆盖世界上万事万物的网络，以实现物品的自动识别和信息的互联共享；同年，在美国召开的“移动计算和网络国际会议”上还提出“传感网是下一个世纪人类面临的又一个发展机遇”[3,4]；2003 年，美国《技术评论》将传感网络技术列为未来改变人们生活的十大技术之首；也有人认为，早在 1995 年比尔·盖茨的《未来之路》一书中已提及物联网的相关概念；2005 年，在突尼斯举行的“信息社会世界峰会”（WSIS）上，ITU 发布了《ITU 互联网报告 2005：物联网》[2]，正式提出了“物联网”的概念；2009 年，IBM 公司提出“智慧地球”的概念，在世界范围内掀起了物联网的热潮，发展物联网技术被多个国家列为重大信息发展战略。

物联网从提出至今只有十余年时间，其内涵尚处于快速发展变化过程中，还没有一个统一的定义。目前，较为大家所接受的物联网的基本含义是：通过 RFID、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理[5]。物联网的核心概念在于“基于网络对物品信息的按需、自动、及时、可靠感知”。一般认为物联网应具备三个基本特性：①及时感知信息，即利用各种可用的感知手段，能实现对物体动态信息的实时采集；②可靠传输信息，即通过各种信息网络与互联网的融合，将感知的信息准确可靠地传递出去；③智能处理信息，即利用云计算等智能计算技术对海量的数据和信息进行分析和处理，以便按需、自动地获取到有用信息并对其进行利用。物联网的本质是通过能够获取物体信息的传感器来进行信息采集，通过网络进行信息传输与交换，通过信息处理系统进行信息加工及决策。

物联网在国内是一个得到广泛认同的概念，并将传感网、物联网和泛在网（ubiquitous network）三者看做是一个递进的包容拓展关系，但国际上习惯将物联网称为泛在网，大概强调的是物联网发展的最终形态。从英文的角度理解，物联网就是物品的互联网，到目前为止，不同领域的专家学者对物联网与互联网的关系有