高等学校物联网专业系列教材

物联网安全

刘建华◎主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

高等学校物联网专业系列教材

物联网安全

刘建华　主　编
孙韩林　副主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书介绍了信息安全和网络安全的基本概念及技术，并以四层物联网体系结构为基础，详细讨论了物联网应用中的安全问题。

全书分为 10 章：第 1 章介绍了物联网的基本概念及其安全问题；第 2 章介绍了物联网的体系结构及其关键技术；第 3 章介绍了信息安全加密的基础知识；第 4 章介绍了 PKI、数字签名、认证及访问控制等安全机制；第 5 章详细介绍了基本的网络安全技术；第 6 章介绍了典型物联网感知层技术的安全问题；第 7 章围绕无线接入技术介绍了物联网接入层安全；第 8 章介绍了物联网核心传输网的安全问题；第 9 章从数据存储和数据处理（云计算）角度介绍了物联网信息处理层的安全问题；最后，第 10 章以物联网在工业、节能环保、公共安全领域的应用为例，讨论了物联网应用中的安全考虑。各章均附有习题，供参考使用。

本书既可作为高等学校物联网专业本科生的教材，也可作为其他物联网相关专业的本科生及从事物联网相关工作人员的参考用书。

图书在版编目（CIP）数据

物联网安全 / 刘建华主编. — 北京：中国铁道出版社，2013.9

高等学校物联网专业系列教材

ISBN 978-7-113-13365-8

Ⅰ. ①物… Ⅱ. ①刘… Ⅲ. ①互联网络－安全技术－高等学校－教材②智能技术－安全技术－高等学校－教材

Ⅳ. ①TP393.4②TP18

中国版本图书馆 CIP 数据核字（2013）第 196127 号

书　　名：物联网安全

作　　者：刘建华　主编

策　　划：巨　凤　　**读者热线**：400-668-0820

责任编辑：徐盼欣

封面设计：一克米工作室

责任印制：李　佳

出版发行：中国铁道出版社（100054，北京市西城区右安门西街 8 号）

网　　址：http://www.51eds.com

印　　刷：北京海淀五色花印刷厂

版　　次：2013 年 9 月第 1 版　　2013 年 9 月第 1 次印刷

开　　本：787mm×1092mm　1/16　**印张**：17　**字数**：402 千

印　　数：1～3 000 册

书　　号：ISBN 978-7-113-13365-8

定　　价：35.00 元

高等学校物联网专业系列教材
编委会名单

总　序

物联网是继计算机、互联网和移动通信之后的又一次信息产业的革命性发展。目前物联网已被正式列为国家重点发展的战略性新兴产业之一。其涉及面广，从感知层、网络层，到应用层均有核心技术及产品支撑，以及众多技术、产品、系统、网络及应用间的融合和协同工作；物联网产业链长、应用面极广，可谓无处不在。

近年来，中国的互联网产业发展迅速，网民数量全球第一，这为物联网产业的发展奠定基础。当前，物联网行业的应用需求领域非常广泛，潜在市场规模巨大。物联网产业在发展的同时还将带动传感器、微电子、新一代通信、模式识别、视频处理、地理空间信息等一系列技术产业的同步发展，带来巨大的产业集群效应。因此，物联网产业是当前最具发展潜力的产业之一，是国家经济发展的又一新增长点，它将有力带动传统产业转型升级，引领战略性新兴产业发展，实现经济结构的战略性调整，引发社会生产和经济发展方式的深度变革，具有巨大的战略增长潜能，目前已经成为世界各国构建社会经济发展新模式和重塑国家长期竞争力的先导性技术。

物联网技术的发展和应用，不但缩短了地理空间的距离，也将国家与国家、民族与民族更紧密地联系起来，将人类与社会环境更紧密地联系起来，使人们更具全球意识，更具开阔眼界，更具环境感知能力。同时，带动了一些新行业的诞生和提高社会的就业率，使劳动就业结构向知识化、高技术化发展，进而提高社会的生产效益。显然，加快物联网的发展已经成为很多国家乃至中国的一项重要战略，这对中国培养高素质的创新型物联网人才提出了迫切的要求。

2010 年 5 月，国家教育部已经批准了 42 余所本科院校开设物联网工程专业，在校学生人数已经达到万人以上。按照教育部关于物联网工程专业的培养方案，确定了培养目标和培养要求。其培养目标为：能够系统地掌握物联网的相关理论、方法和技能，具备通信技术、网络技术、传感技术等信息领域宽广的专业知识的高级工程技术人才；其培养要求为：学生要具有较好的数学和物理基础，掌握物联网的相关理论和应用设计方法，具有较强的计算机技术和电子信息技术的能力，掌握文献检索、资料查询的基本方法，能顺利地阅读本专业的外文资料，具有听、说、读、写的能力。

物联网工程专业是以工学多种技术融合形成的综合性、复合型学科，它培养的是适应现代社会需要的复合型技术人才，但是我国物联网的建设和发展任务绝不仅仅是物联网工程技术所能解决的，物联网产业发展更多的需要是规划、组织、决策、管理、集成和实施的人才，因此物联网学科建设必须要得到经济学、管理学和法学等学科的合力支

撑，因此我们也期待着诸如物联网管理之类的专业面世。物联网工程专业的主干学科与课程包括：信息与通信工程、电子科学技术、计算机科学与技术、物联网概论、电路分析基础、信号与系统、模拟电子技术、数字电路与逻辑设计、微机原理与接口技术、工程电磁场、通信原理、计算机网络、现代通信网、传感器原理、嵌入式系统设计、无线通信原理、无线传感器网络、近距无线传输技术、二维条码技术、数据采集与处理、物联网安全技术、物联网组网技术等。

物联网专业教育和相应技术内容最直接地体现在相应教材上，科学性、前瞻性、实用性、综合性、开放性应该是物联网专业教材的五大特点。为此，我们与相关高校物联网专业教学单位的专家、学者联合组织了本系列教材“高等学校物联网专业系列教材”，为急需物联网相关知识的学生提供一整套体系完整、层次清晰、技术先进、数据充分、通俗易懂的物联网教学用书，出版一批符合国家物联网发展方向和有利于提高国民信息技术应用能力，造就信息化人才队伍的创新教材。

本系列教材在内容编排上努力将理论与实际相结合，尽可能反映物联网的最新发展，以及国际上对物联网的最新释义；在内容表达上力求由浅入深、通俗易懂；在知识体系上参照教育部物联网教学指导机构最新知识体系，按主干课程设置，其对应教材主要包括物联网概论、物联网经济学、物联网产业、物联网管理、物联网通信技术、物联网组网技术、物联网传感技术、物联网识别技术、物联网智能技术、物联网实验、物联网安全、物联网应用、物联网标准、物联网法学等相应分册。

本系列教材突出了“理论联系实际、基础推动创新、现在放眼未来、科学结合人文”的特色，对基本概念、基本知识、基本理论给予准确的表述，树立严谨求是的学术作风，注意与国内外的对应及对相关概念、术语的正确理解和表达；从实践到理论，再从理论到实践，把抽象的理论与生动的实践有机地结合起来，使读者在理论与实践的交融中对物联网有全面和深入的理解和掌握；对物联网的理论、研究、技术、实践等多方面的发展状况给出发展前沿和趋势介绍，拓展读者的视野；在内容逻辑和形式体例上力求科学、合理，严密和完整，使之系统化和实用化。

自物联网专业系列教材编写工作启动以来，在该领域众多领导、专家、学者的关心和支持下，在中国铁道出版社的帮助下，在本系列教材各位主编、副主编和全体参编人员的参与和辛勤劳动下，在各位高校教师和研究生的帮助下，即将陆续面世。在此，我们向他们表示衷心的感谢并表示深切的敬意！

虽然我们对本系列教材的组织和编写竭尽全力，但鉴于时间、知识和能力的局限，书中难免会存在各种问题，离国家物联网教育的要求和我们的目标仍然有距离，因此恳请各位专家、学者以及全体读者不吝赐教，及时反映本套教材存在的不足，以使我们能不断改进出新，使之真正满足社会对物联网人才的需求。

高等学校物联网专业系列教材编委会

2011 年 10 月 1 日

前　言

2005 年 11 月 17 日，在突尼斯举行的信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布了“ITU INTERNET REPORTS 2005 EXECUTIVE SUMMARY：The Internet of Things”（ITU 互联网报告 2005：物联网），提出了“The Internet of things”的概念。我国翻译为“物联网”。顾名思义，“物联网就是物物相连的互联网”。物联网是新一代信息技术的重要组成部分，其本质还是互联网，只是其用户端延伸和扩展到了任何物品与物品之间进行信息交换和通信的网络。物联网通过智能感知、识别技术与普适计算、泛在网络的融合应用，被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。物联网是互联网的应用拓展，与其说物联网是网络，不如说物联网是业务和应用。

目前，物联网是全球研究的热点问题，国内外都把它的发展提高到国家级的战略。我国政府特别重视物联网的发展和应用。2009 年国务院总理温家宝“感知中国”的讲话把我国物联网领域的研究和应用开发推向了高潮，物联网被正式列为国家五大新兴战略性产业之一，写入了“政府工作报告”，受到了全社会极大的关注。为了更进一步促进我国物联网的发展，全国已经有数十所院校开设了物联网专业。物联网专业的人才培养要求很高，是个交叉学科，涉及电子通信技术、传感技术、RFID 技术、嵌入式系统技术、网络技术等多项知识。

互联网是一个多元的、开放的网络，对当前社会的政治、经济、文化和人们的生活有着巨大的影响，已经深入人心，成为人们生活的重要组成部分。随着互联网的发展，也带来了网络的安全问题，例如网络攻击、病毒侵袭、垃圾邮件等各类安全问题层出不穷。物联网作为互联的在“物”上的延伸，也会存在各种安全问题。本书在总结基础安全理论、技术和解决方法的基础上，针对物联网的安全特点进行总结、整理和分析，旨在为物联网专业的本科生提供一本有特色的、有针对性的学习资料。

全书共分为 10 章，其中第 1～5 章为基础部分，主要讲述了物联网的基本概念、面临的安全问题、物联网体系结构和关键技术，以及信息安全基础理论（包括密码体制、安全机制、安全服务和网络安全技术）；第 6～9 章为物联网安全部分，按照物联网的感知层、网络层（分为接入网和核心网）和应用层的层次结构，分层讲述了各层关键技术的安全问题分析、解决方法及发展趋势；第 10 章以当前典型的物联网应用为例，讨论了

物联网应用中的安全考虑。

本书由刘建华任主编，由孙韩林任副主编，其中第 1～5 章由刘建华执笔，第 6～10 章由孙韩林执笔，全书由刘建华统编定稿。

本书在编写过程中得到研究生的大力帮助，他们是梁俊杰、崔丹、石珮珊、王筱蕾、屈飞、咎林萍、王倩。他们完成了为全书绘制插图、部分文稿翻译、资料搜集以及格式整理等工作，在此对他们的贡献表示感谢！同时也感谢我的同事屈军锁等的支持和帮助！感谢中国铁道出版社巨凤等编辑的大力支持和帮助！

本书在编写过程中参考了大量的图书资料，这些资料也凝结了作者的辛勤劳动和智慧，在此一并表示感谢！

物联网技术和应用发展迅速，限于编者的知识水平和能力，书中的疏漏甚至错误之处在所难免，恳请各位专家、学者和广大读者批评指正。

编者

2013 年 7 月

目　录

第1章 物联网发展及其安全问题

学习重点

1．理解物联网的定义，了解物联网存在的问题。

2．理解信息安全定义，明确物联网存在的安全问题。

1.1　物联网的概念

1.1.1　背景知识

1．信息及信息系统

目前人们处在信息时代，信息化是这个时代的特征之一。那么，什么是信息？信息如何获取？如何处理信息？信息能帮助人们做些什么？这些问题都是应该深刻思考的。

关于信息的严格定义目前说法不一，其中，最有影响的是美国科学家香农所提出的。香农通过对信息通信问题的研究，提出了著名的信息论，他认为信息在通信中就是消除信号的不确定性。

信息传播三大要素是信源、信宿和信道。信息传播过程可简单地描述为：信源→信道→信宿。

① 信源：符号、文字、声音、图像等。

② 信道：载体，光、电等电磁信号。

③ 信宿：从载体中抽取信息。

信息可以用消息、信号等形式来表达。

2．信息获取

人们发出信息的方式可以是声音、眼光、手势、文字等，人们获取信息可以通过眼睛、声音、感觉等方式，但这些都是不够的，人的自身感觉的准确性、敏感性、快速性等是有限的。因此，人们研究了传感器，用于帮助对客观世界的不断深入了解。传感器有各种类型，如温度的、压力的、图像的、声音的、速度的等。

3．信息传递

因为要对获取的信息进行传递，即信息通信，人们建立了各种网络，如电话网用于传递声音信息，电视网用于传递图像信息，计算机网络用于传递计算机处理后的各种多媒体信息等。因特网是目前世界上最大的计算机网络，传递信息的能力最强。

4．信息处理

当前，人们所能获取的信息很多，琳琅满目，但人们处理信息的能力很有限，因此，需要通过计算机快速、准确、有效地对信息进行处理。智能化信息处理是信息处理的新境界，即计算机处理信息能像人一样灵活、准确、迅速。

5．信息服务

不同的人，想要做的事情不同，对信息的需求也不同，因此按照人们的不同要求，把信息处理像商品一样服务于大众，已经为人们所接受。云计算就是这样一个提供信息服务的概念。

1.1.2　什么是物联网

提出“物联网”（The Internet of Things）这个概念的被认为是比尔·盖茨，他在著作《未来之路》中首次提到了“物联网”。但到目前为止，总体上物联网还处于一个概念和研发的阶段。关于物联网的定义还比较混乱，物联网的一些重大共性问题（如架构、标识编码、安全及标准等）也未得到很好的解决，并未在全球达成共识。

定义 1：把所有物品通过射频识别（RFID）和条码等信息传感设备与互联网连接起来，实现智能化识别和管理。

早在 1999 年，这个概念即由美国麻省理工学院的 Auto-ID 研究中心提出。RFID 可谓早期物联网最为关键的技术和产品环节，当时认为物联网最大规模、最有前景的应用是在物流领域，利用 RFID 技术，通过互联网实现物品的自动识别、信息互联和共享。

定义 2：2005 年国际电信联盟（ITU）在“The Internet of Things”报告中对物联网的概念进行了扩展，提出任何时刻、任何地点、任何物体之间的互联，无所不在的网络和无所不在的计算的发展愿景，除 RFID 技术外，传感器技术、纳米技术、智能终端等技术将得到更加广泛的应用。严格意义上讲，这不是物联网的定义，而是关于物联网的一个描述，如图 1-1 所示。

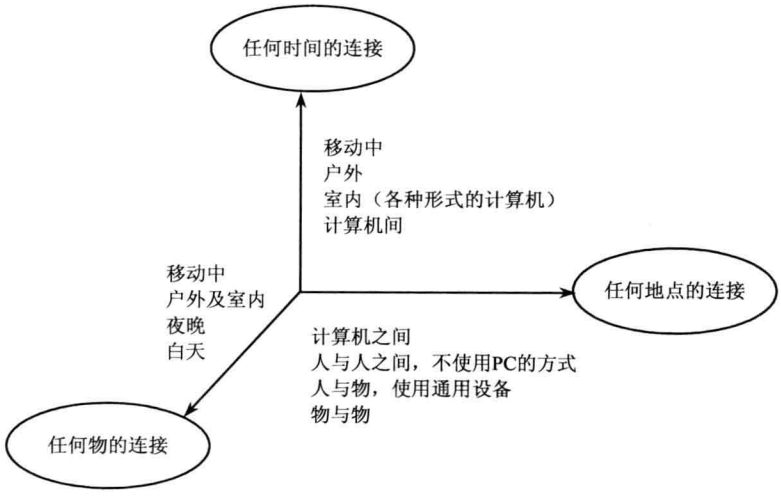

图 1-1　物联网

定义 3：物联网是未来 Internet 的一个组成部分，可以被定义为基于标准的可互操作的通信协议且具有自配置能力的、动态的全球网络基础架构。物联网中的“物”都具有标识、物理属性和实质的个性，使用智能接口，实现与信息网络的无缝整合。

这个定义来自欧盟的第七框架下的 RFID 和物联网研究项目的一个报告“The Internet of Things Strategic Research Roadmap”（2009.09.15）研究报告。该报告研究的目的在于 RFID 和物联网的组网和协调各类资源。

定义 4：由具有标识、虚拟个性的物体/对象所组成的网络，这些标识和个性运行在