普通高等教育“物联网工程专业”规划教材

物联网安全导论

李联宁 编著

清华大学出版社

普通高等教育“物联网工程专业”规划教材

物联网安全导论

李联宁 编著

清华大学出版社
北京

内 容 简 介

本书详细介绍了物联网安全技术的基础理论和最新主流前沿技术，全书共分为6部分：物联网安全概述、物联网感知识别层安全、物联网网络构建层安全、物联网管理服务层安全、物联网综合应用层安全、物联网安全标准和安全体系规划设计。以12章的篇幅按互联网的网络结构分别讲述物联网安全需求分析、物联网安全技术架构、密码与身份认证技术、RFID系统安全与隐私、WSN无线传感器网络安全、无线通信网络安全、互联网网络安全、中间件与云计算安全、信息隐藏技术原理、位置信息与隐私保护、物联网信息安全标准以及安全体系结构规划与设计。每一章除了相关理论外，还讲解了最新前沿技术的原理。各章都附有习题以帮助读者学习理解理论知识和实际工程应用。为方便教师教学，附有全套教学PPT课件等。

本书主要作为高等院校物联网工程、信息安全、自动化、通信工程、计算机应用和电气信息类等专业高年级本科生和研究生教材，也可作为物联网安全技术的专业培训教材。对物联网安全和可靠应用领域的管理决策人员、从事物联网安全领域应用和设计开发的人员以及计算机网络工程技术人员都有学习参考价值。

图书在版编目（CIP）数据

物联网安全导论/李联宁编著．--北京：清华大学出版社，2013.4
普通高等教育“物联网工程专业”规划教材
ISBN 978-7-302-30377-0

Ⅰ．①物…　Ⅱ．①李…　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．①TP393.4　②TP18

中国版本图书馆CIP数据核字(2012)第242152号

责任编辑：白立军　战晓雷
封面设计：常雪影
责任校对：李建庄
责任印制：王静怡

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
课件下载：http://www.tup.com.cn,010-62795954

印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：23　　**字　　数**：575千字
版　　次：2013年4月第1版　　**印　　次**：2013年4月第1次印刷
印　　数：1～3000
定　　价：39.00元

产品编号：049180-01

前　言

随着物联网技术的飞速发展，物联网在中国受到了全社会极大的关注。与其他传统网络相比，物联网感知节点大都部署在无人监控的场景中，具有能力脆弱、资源受限等特点，这使得物联网安全问题比较突出，并且当国家重要基础行业和社会关键服务领域（如电力、金融、交通和医疗等）重要社会功能的实现即将依赖于物联网应用时，物联网安全问题已经上升到国家层面。

2010 年后，全国已有近 700 所高等院校向教育部提交了增设物联网等相关专业的申请，首批 37 所院校已获准开设物联网相关专业。目前符合大学物联网安全专业教学要求的教材十分稀缺，社会上对物联网安全技术书籍的需求数量也很大。本书试图在对物联网安全技术领域做详细介绍的基础上，给出实际工程案例及行业解决方案，以达到技术全面、案例教学及工程实用的目的。

本书主要分为 6 个部分，分别按物联网安全的技术架构分层次详细讲述涉及物联网安全的各类相关技术。

第一部分：物联网安全概述。简单介绍物联网信息安全的基本概念和主要技术，包括 3 章，内容为物联网安全需求分析、物联网安全技术架构和密码与身份认证技术。

第二部分：物联网感知识别层安全。介绍涉及物联网感知层安全的理论与技术，包括 2 章，内容为 RFID 系统安全与隐私和 WSN 无线传感器网络安全。

第三部分：物联网网络构建层安全。介绍涉及物联网网络层安全的理论与技术，包括 2 章，内容为无线通信网络安全和互联网网络安全。

第四部分：物联网管理服务层安全。介绍涉及物联网管理服务层安全的理论与技术，包括 1 章，内容为中间件与云计算安全。

第五部分：物联网综合应用层安全。介绍涉及物联网应用层安全的理论与技术，包括 2 章，内容为信息隐藏技术原理和位置信息与隐私保护。

第六部分：物联网安全标准和安全体系规划设计。简单介绍物联网安全标准和安全体系规划，包括 2 章，内容为物联网信息安全标准和安全体系结构规划与设计。

本书主要作为普通高等院校本科生和研究生教材，教材力争紧跟物联网安全技术的最新发展，使用大量的实际工程案例辅助教学，使学生在学习完成后能够具备实际工程能力。对专业从事物联网工作的领导干部、研究人员和工程技术人员也有学习参考价值。

书中各章都附有习题，以帮助读者学习理解和实际工程应用。同时，可以从清华大学出版社网站（www. tup. com. cn）下载配套的教学课件（PowerPoint 演示文件）以便教学使用。

本书由李联宁教授编著，在本书编写过程中，编者参考了国内外大量的物联网及计算机网络书刊及文献资料，在此对有关文献的作者表示感谢。对于本书中的错误或不妥之处，恳请广大读者不吝赐教。

编者

2012 年 12 月

目　录

第一部分　物联网安全概述

第二部分 物联网感知识别层安全

第五部分 物联网综合应用层安全

第一部分　物联网安全概述

第 1 章　物联网安全需求分析

第 2 章　物联网安全技术框架

第 3 章　密码与身份认证技术

第1章　物联网安全需求分析

根据国际电信联盟的定义，物联网（Internet of Things，IOT）主要解决物品到物品（Thing to Thing，T2T）、人到物品（Human to Thing，H2T）、人到人（Human to Human，H2H）之间的互联。核心共性技术、网络与信息安全以及关键应用是当前的物联网研究的重点。

与其他传统网络相比，物联网感知节点大都部署在无人监控的场景中，具有能力脆弱、资源受限等特点，这些都导致很难直接将传统计算机网络的安全算法和协议应用于物联网。这使得物联网安全问题相对比较突出，并且将来当国家重要基础行业和社会关键服务领域（如电力、金融、交通和医疗等）重要社会功能的实现都依赖于物联网及感知型业务应用时，物联网安全问题必然上升到国家层面。

考虑到当前的物联网安全研究尚未形成体系，主要研究集中在单个技术，如感知前端技术（如RFID、传感技术）和个体隐私保护等方面，下面首先给出物联网安全安全性与层次结构分析；随后对层次结构涉及的物联网关键技术以及安全问题进行分析和论述。

1.1　物联网安全性要求

1.1.1　物联网安全涉及范围

在未来的物联网之中，每一个物品都会被连接到一个全球统一的网络平台之上，并且这些物品又时刻地与其他物品之间进行着各式各样的交互行为，这无疑会给未来的物联网带来形式各异的安全性和保密性挑战。比如，物品之间可视性和相互交换数据过程中所带来的数据保密性、真实性以及完整性问题等。

要想让消费者全面地投入未来的物联网的怀抱，要想让用户充分体验未来的物联网所带来的巨大潜在优势，要想让未来物联网的参与者尽可能避免通用性网络基础平台所带来的各种安全性与隐私性风险，物联网就必须实现这样一种特殊的工作方式，可以简便而安全地完成各种用户控制行为，也就是要求未来的物联网的技术研究工作充分考虑安全性和隐私性等内容。

传统意义上的隐私是针对于“人”而言的。但是在物联网的环境中，人与物的隐私需要得到同等地位的保护，以防止未经授权的识别行为以及追踪行为的干扰。而且随着“物品”自动化能力以及自主智慧的不断增加，像物品的识别问题、物品的身份问题、物品的隐私问题以及物品在扮演的角色中的责任问题将成为我们重点考虑的内容。

同时，通过将海量的具有数据处理能力的“物品”置于一个全球统一的信息平台和全球通用的数据空间之中，未来的物联网将会给传统的分布式数据库技术带来翻天覆地的变化。在这样的背景下，现实世界中对于信息的兴趣将分布并且覆盖数以亿万计的“物品”，其中将