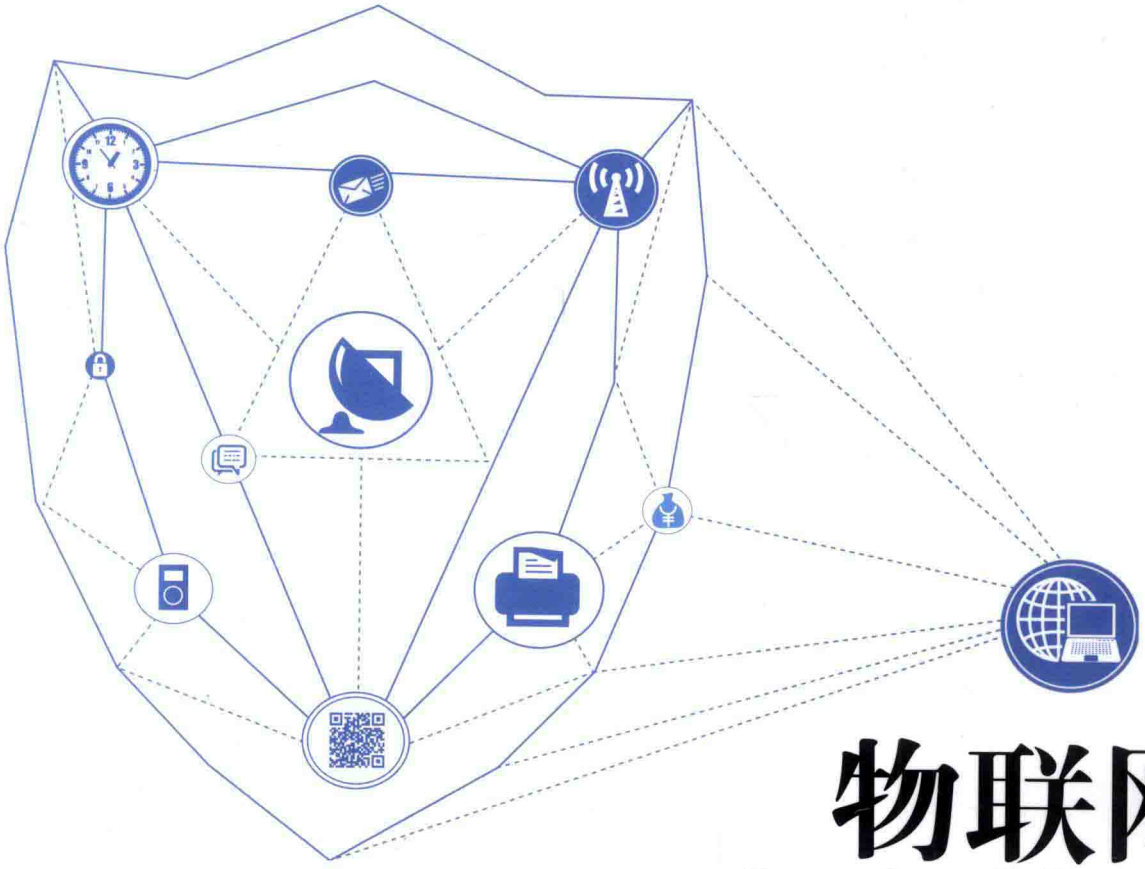
物联网工程专业系列教材



物联网安全基础

武传坤 等 编著

SECURITY FUNDAMENTALS FOR INTERNET OF THINGS

科学出版社

物联网工程专业系列教材

物联网安全基础

武传坤 等 编著

科学出版社
北京

内 容 简 介

本书共分13章，围绕物联网安全架构体系，分别介绍了物联网感知层安全、传输层安全、处理层安全、应用层安全和安全基础设施等内容及相关的一些解决方案。在第11 ~ 13章的行业应用部分，本书介绍了物联网主要存在哪些安全问题，对这些问题的学习可使读者认识信息安全的隐患存在于哪些方面。通过对本书的学习，读者将会认识到物联网行业应用对信息安全保护的不同需求，将能更好地理解和使用新兴的物联网行业信息安全解决方案和安全产品或系统。

本书可供高等院校物联网相关专业用作物联网安全课程的教材，也可作为物联网安全研究人员的参考用书。

图书在版编目（CIP）数据

物联网安全基础/武传坤等编著. —北京：科学出版社，2013
（物联网工程专业系列教材）
ISBN 978-7-03-037267-3

Ⅰ. ①物… Ⅱ. ①武… Ⅲ. ①互联网络-应用-安全技术-高等学校-教材 ②智能技术-应用-安全技术-高等学校-教材
Ⅳ. ①TP393.408 ②TP18

中国版本图书馆CIP数据核字（2013）第069111号

责任编辑：赵丽欣 郭丽娜/责任校对：王万红
责任印制：吕春珉/封面设计：蒋宏工作室
版式设计：鑫联必升图文设计

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
双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2013年12月第 一 版 开本：889×1194 1/16
2013年12月第一次印刷 印张：24 1/2
字数：564 000
定价：49.00元

（如有印装质量问题，我社负责调换〈双青〉）
销售部电话 010-62134988 编辑部电话 010-62134021

前　言

信息技术的发展经历了几个革命性的进展。计算机的出现为信息的处理提供了前所未有的技术手段，也为信息处理技术带来了革命性的变化；Internet 的出现使得全球范围内的计算机互联成为可能，为电子商务、电子政务等以网络为基础的网络交易和工作流程提供了平台，为信息处理技术带来又一次革命性的变化；物联网的目标是将虚拟空间与现实空间相结合，使得现实空间中的物可以通过虚拟空间中的信息相互控制，实现海量终端的互联、海量数据的融合、异构网络的共同支撑、多种行业的数据共享等服务，而这将为信息技术的服务形式带来一次革命性的变化。

无论哪个阶段，对信息内容的安全保护都是非常重要的。在计算机时代，信息安全问题主要是防止非法用户盗取计算机内存储的内容，因此账户管理是信息安全保护的主要手段；在网络时代，出现了多种攻击手段，不仅仅是对信息的非法获取，还包括假冒、伪造、篡改、病毒、拒绝服务攻击等，有些攻击手段结合了多种技巧，使得用户防不胜防。在物联网时代，信息的价值会更高，对信息系统的攻击手段将会更复杂、多变，因此对信息系统的安全保护将面临空前的挑战。

然而，当前许多物联网示范系统中对信息安全的保护措施远不能满足信息安全保护的基本要求，随着这些示范系统规模的增大和在实际使用中发挥作用的重要性增强，信息安全问题将会逐渐显现。其他一些在建和拟建的物联网示范工程也需要更好地考虑信息安全保护措施。然而，物联网安全技术尚不成熟，缺少有关标准和规范予以指导，从而使得物联网行业应用中的信息安全解决方案还不够系统和规范。

为了在人才培养过程中培养信息安全意识，在物联网系统的建设和运营过程中更好地维护系统的信息安全，我们写了这本物联网安全方面的教材，希望提供一些最基本的物联网安全方面的知识，为物联网工程领域培养更全面的人才。同时，希望本书也为物联网行业的工程技术人员提供参考。

本书由中国科学院信息安全国家重点实验室组织编写，由多个作者合作完成。第 1 章和第 2 章由武传坤执笔完成，第 3 章由刘峰执笔完成，第 4 章由张锐执笔完成，第 5 章由徐静执笔完成，第 6 章由冯秀涛执笔完成，第 7 章由陈驰执笔完成，第 8 章由王雅哲执笔完成，第 9 章由翟黎和刘卓华执笔完成，第 10 章由张文涛执笔完成，第 11 章由滕济凯执笔完成，第 12 章由刘卓华执笔完成，第 13 章由皮兰执笔完成。另外，武传坤还负责本书的内容安排、写作风格统一、部分章节的内容调整和补充、部分章节的校对等工作。

由于时间仓促，物联网安全方面可供参考的资料不多，不同执笔人的写作风格也不尽

相同，因此本书一定存在许多不足甚至错误之处，希望读者多提宝贵意见。我们也注意到，部分章节的内容可能有点深，我们也努力写得浅显易懂些，但许多概念和方法都需要介绍，因此这方面我们感觉做得还不够。如果有机会，希望再版时纠正错误，弥补存在的不足，也将根据物联网安全领域研究和行业发展等具体情况补充一些内容。

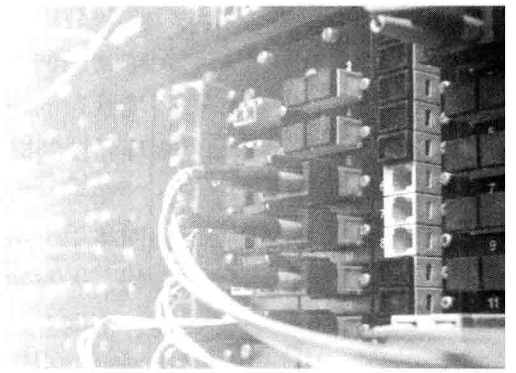
最后，感谢科学出版社为我们提供这么好的机会，让我们的一些初步研究成果、认知观点、技术方法等能早日与读者见面，我们也期待根据读者的宝贵意见不断改进，使其成为一本有用的教材和参考书。

在阅读本书过程中遇到的问题、发现的错误、对本书内容和结构方面的任何意见和建议，请发送至 ckwu@iie.ac.cn 或 chuankun.wu@gmail.com。如果本书的部分章节有更新，将通过网页 http://people.gucas.ac.cn/~ckwu 发布。

编著者

2013 年 3 月 8 日

目　录



第1章　物联网简介

1.1　引言

物联网概念最早由 MIT 的 Kevin Ashton 在 1998 年演讲中提出：把射频识别标签与其他传感器应用于日常物品形成一个物联网。Kevin Ashton 在第二年负责成立遍布四大洲七所大学联合组成的 Auto-ID 中心，把物联网的概念形象地描述为构建在互联网之上以射频识别标签等信息传感设备为核心的全球基础框架，跟踪从剃须刀、欧元纸币到汽车轮胎等数百万计的物品。

国际电信联盟（ITU）在 2005 年发布了针对物联网的年度报告“Internet of Things”，指出物联网时代即将来临，信息与通信技术的发展已经从任何时间、任何地点连接任何人，发展到连接任何物体的阶段，而万物的连接就形成了物联网。

在欧盟委员会资助下，欧洲物联网研究项目组 2009 年制订了物联网战略研究路线图，指出物联网是具有标识的物理或虚拟实体，基于标准的、可互操作的通信协议，通过接口无缝接入到信息网络，能够对感知物理世界的事件做出反应，触发动作和生成服务；物品通过与其他物品或环境互动来参与商业、信息和社会活动，以服务作为接口通过互联网来查询和改变物品状态，并考虑隐私与安全。

物联网已经不完全是纯学术的技术名词，逐渐地被应用到社会经济领域，而且上升到国家发展战略层面。美国 IBM 公司在 2008 年底提出了“智慧地球”的概念，其核心是将新一代信息技术融合到基础设施建设当中，把传感器嵌入和装备到全球每一个角落的电网、铁路、桥梁、隧道、公路等各种基础设施中，普遍连接形成物联网，其目的是利用新一代信息网络技术来改变政府、公司和人们相互交互的方式，以便政府、企业和市民可以做出更明智的决策。

物联网概念从最初的产生到现在已经逐渐发展和演变。物联网的初始概念是在互联网基础上建立以射频识别标签等信息感知设备为核心的架构，实现对

全球物品的连接和跟踪；逐渐地，更多的传感器嵌入到物品中感知物品自身或环境状态的信息，物品越来越具有智能性，能够协同获取和处理感知信息，为管理和控制提供决策依据，并在人工直接干预或无需人工干预情况下进行联动。

在另一方面，物联网已经被应用到社会经济领域。随着大量物品不断连接到网络中，从人到人通信的移动通信网，机器到机器连接的互联网，发展到物与物、人与物连接互动的物联网，逐渐表现出“全面感知、无缝互联、高度智能、协同互动”新的物联网形态，使得人类的生产管理和社会生活更加高效，资源得到更加合理的利用，带来新的生产和服务模式，物联网产业的特征决定了它是推动我国实现经济增长方式转变和产业升级的战略性新兴产业。

从狭义角度理解，物联网就是具有感知和智能处理能力的可标识的亿万物品，基于标准的、可互操作的通信协议，在宽带移动通信、下一代网络和云计算平台等技术的支持下，智能处理物品或环境的状态信息，提供对其进行管理和控制的决策依据，甚至在人类直接干预或无需人工干预情况下实现联动，从而形成信息获取、物品管理和控制的全球性信息系统。

物联网产业覆盖人类生产生活的多个方面，它以信息感知获取为基础，以信息传输处理为纽带，以信息行业应用为平台，以信息增值业务为媒介，最终实现面向各个用户的信息服务产业链条。

物联网产业的诞生并不是一时兴起，而是随着纳米技术、新材料技术、微电子技术、网络通信技术、计算技术和自动化技术发展到一定阶段必然演变形成的新一轮信息化变革。

与互联网类似，物联网也具有巨大的产业拉动效应。基于人、物泛联世界的信息，是构成新的信息业务模式的源泉，众多面向政府、企业、群体和个人用户的信息服务将在此基础上诞生，如物联网上的 Google 搜索引擎，物联网上的网络工厂（代替互联网的网络商城），并可能有前所未有的创新应用诞生，所有这些必将极大地改变人类生产和生活方式，促成涉及领域更广阔、更深刻的，规模可达数万亿美元的庞大物联网产业诞生。

1.2 物联网系统的基本架构

物联网的核心可划分为三个逻辑层，分别为感知层、传输层和处理应用层。总体上，感知层的作用是获取原始数据，传输层的作用是将这些原始数据传输到远程的处理平台进行处理，而处理应用层的作用无疑是对来自不同感知节点的信息进行处理和应用。由于对数据的处理和对数据的应用无论从流程上和方法上都有很大区别，为了更清晰地描述完整的物联网架构，有时候将物联网的

处理应用层分为处理层和应用层，形成四个逻辑层的架构，如图 1.1 所示。但两种架构的内涵是一样的。

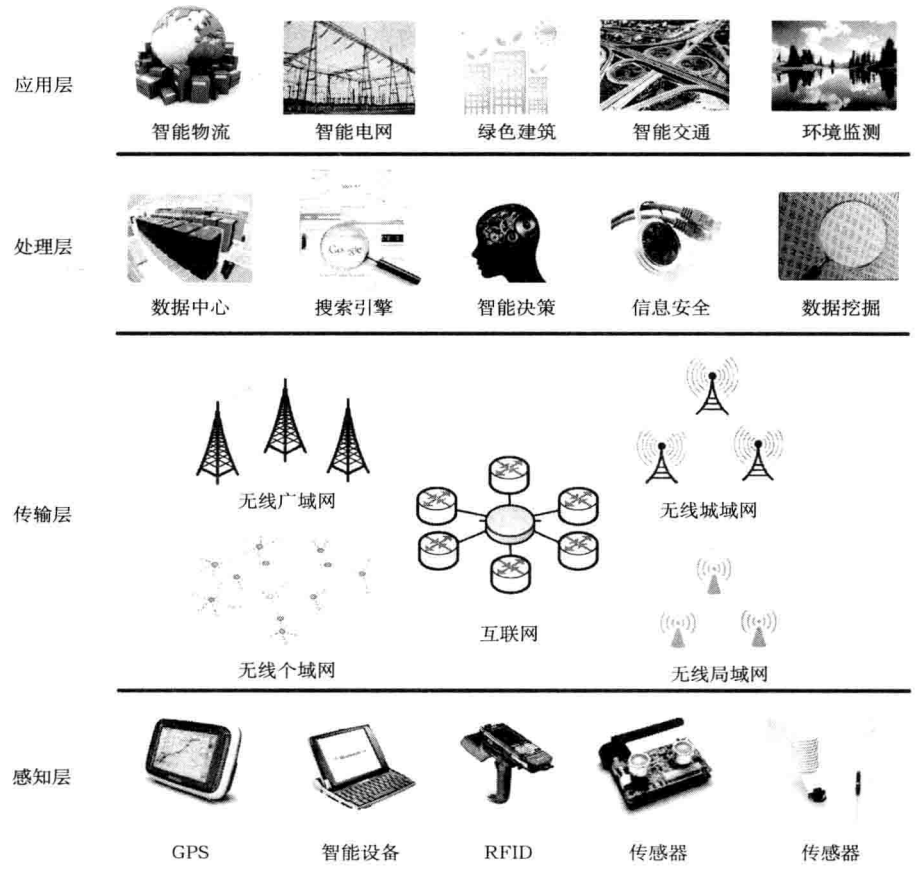


图1.1
物联网架构及其应用示意图

对物联网系统的架构还有另外一种划分，即“海－网－云”架构。在这种架构中，所有终端设备被划分为一层。由于物联网系统的终端数量是巨大的，可以用海量来形容，因此将此类设备形象地称为“海”。数据传输的基础网络设施被称为“网”，很明显这个“网”不是单一的网，而是多种异构网络的统称，包括局域网、互联网、移动网等。物联网系统的数据处理将面对庞大数据，人们由此提出了“大数据”的概念。所谓大数据，是指那些使用传统单机模式无法处理的数据，这里数据的处理需要一定规模的处理平台，而用户只需要知道跟处理平台的逻辑关系，无需知道自己的数据是在哪台计算机或者处理器处理的，也无需知道自己的数据存储在哪里，只关心当自己需要的时候可以从数据处理中心得到数据，这样的数据处理中心被形象地描述成“云”。这样，就形成了物联网的“海－网－云”逻辑架构。物联网的这种架构与图 1.1 所示的四层架构之间的关系是：“海”包括图 1.1 中的感知终端（即感知层中的终端

设备）和应用终端（应用层中的用户终端），“网”包括图 1.1 中感知层的传输网络和传输层，“云”相当于图 1.1 中的处理层。因此物联网的“海－网－云”架构是以设备、通信和处理进行划分的。无论哪种架构，都基于可见的东西，而一些保证物联网系统运转的不可见的东西，包括信息处理技术、信息传输通信协议、信息处理软件和管理等，都至关重要且相当复杂。

事实上，在物联网概念提出之前，已经有许多成熟的信息感知技术、信息传输技术和信息处理技术，但物联网对这些技术提出了更高的要求。在信息感知方面，物联网局部范围内物品间能够协同感知位置、物品或环境状态，实现感知信息的全面获取，而且感知层所获取的感知信息不是原始数据，而是经过初步处理后的数据；在网络传输方面，物联网涉及各种物品的异构接入网络、公共传输网络及企业专用网络，实现物品的无缝接入与互联；在信息处理方面，智能化的信息处理渗透到整个物联网的各个层面，从底层感知信息的预处理、网络传输过程中的信息融合和决策判断，到各种行业应用的服务处理。但物联网架构上的处理一般针对感知信息的集中、智能化处理，最有代表意义的感知层是云计算平台，目前已有多种云计算服务平台可供使用；在全面的感知信息获取和可靠的网络传输基础上，利用智能化的信息处理技术，根据社会生产、管理和人们生活需求，物联网能够形成各种各样的应用和服务。因此，物联网系统的基本架构是为行业应用服务的，离开行业应用的物联网只是一种概念，很难落实到实际系统。

物联网是传统传感网发展的高级阶段，是传感网与互联网、云计算等技术深度渗透所形成的一种新型网络为基础的行业应用系统。传感网（包括 RFID）是实现全面感知的基础，互联网是物联网信息的主要传输载体，云计算技术是物联网智能处理的支持技术。尽管物联网的应用 / 产业特征更为明显，但在技术的深度渗透过程中，物联网形成了自己独特的关键技术特征。

1.3 物联网关键技术

在物联网重点技术领域，攻克制约物联网产业发展和应用推广的核心关键技术，加强共性技术、支撑技术以及推动未来一段时间内的物联网技术发展的基础理论的研究和应用工作，从技术创新方面加快形成产业创新集群，这些都是提升产业发展水平的基本要求。物联网关键技术包括以下几方面。

1. 物联网基础资源管理与服务

物联网基础资源包括物联网的名称和地址，其中，名称指物的名字与标识，

地址指物的网络地址与资源地址。这些资源支撑着各类物联网应用的开展和网间互联互通。核心技术包括可信、可管、具有隐私保护机制的物联网基础资源管理技术及其系统集成；高性能、安全的物联网基础资源服务技术及其服务系统；物联网基础资源服务发现、信息分类和检索技术、安全监控、攻击防范、数据关联分析和舆情预警技术。

2．物联网信息获取与识别技术

新型标签、传感技术、芯片与信息预处理技术和微能源管理技术是物联网中信息获取与识别的关键。核心技术包括新型标签技术、微纳传感器及其加工与封装、低功耗多处理器片上系统与片上网、识别定位芯片、低功耗射频电路芯片、片上天线技术。支撑技术包括敏感材料、微能源与储能技术、能量采集技术等。

3．物联网组网与传输技术

研究不同应用场景下节点通信与组网技术。核心技术包括大规模自组网与可靠信息交互、多感知信息的分布式融合技术，面向国家安全与特定行业应用的网络隔离技术、保密、抗干扰、分级信息传输技术等，实现节点之间有效、安全的信息交互与协同处理。支撑技术包括服务管理与资源发现、物联网管理技术、多网互联技术。

4．物联网信息处理技术

研究物联网海量信息的情报提炼与态势判断、动态数据管理与检索。重点研究以信息感知和融合为基础、以情报生成为中心的物联网多源数据的协同交互和数据融合，形成从信息感知、模式识别、情报处理和决策与处置的安全感知体系架构、标准和技术解决方案，建立物联网流数据的存储与查询的数据库系统，挖掘海量物体信息关系链。

5．物联网安全技术

物联网实现虚拟世界与物理世界的互联互通，需要新的安全体系和技术。核心技术包括物联网安全架构，跨网络架构的实体认证技术，对物联网中实体的远程控制和操作，海量感知终端的身份安全管理和识别，资源受限环境的信息保密与认证技术，信息安全基础支撑平台的建设，云计算与云存储安全的关键技术，物联网安全技术的系统集成等。

6．物联网系统集成技术

结合微纳传感与 MEMS 传感等技术进步，研制集感知、传输、预处理等功能于一体的物联网节点设备，构建面向不同行业和公众应用的物联网集成应用

系统；加快物联网系统级软件开发，重点发展信息处理、智能控制、数据库软件、中间件等基础性软件；针对多业务、多应用融合需求，加大应用管理和服务软件以及信息服务平台技术的开发力度，推动物联网应用的快速发展。

7．共性支撑技术

重点研究可编程、测试、环境建模等共性技术，研发物联网节点专用操作系统和综合软件开发环境，建立标准测试验证平台、物联网应用技术规范和系统测试平台，加强现代信息通信、计算机及网络、新材料、新能源等基础支撑技术的研究与应用。

1.4 物联网的技术标准

经济全球化的背景下，“技术专利化，专利标准化，标准国际化”已成为市场竞争的重要特征。目前，国际上有多个与物联网相关的技术制定组织及所制定的多个技术标准，各国间难以互联互通和加强合作。为促进全球物联网产业发展，需要各国组成权威的技术制定组织，尽快统一技术标准。

但各个国家都希望在技术标准这一关系到物联网产业发展主导权的领域抢得先机。发达国家往往通过控制国际标准的制定来抢占发展的制高点，跨国公司则通过技术专利演变成事实标准，来保持其在市场竞争中的优势地位，以获得高额、稳定的收益。如果发展中国家不迅速在关键核心技术方面取得突破，在国际标准制定方面掌握一定的主动权，不排除发达国家依靠技术上的优势结成“物联网标准俱乐部”的可能。

传感器、芯片、关键设备制造、智能交通高端市场 70% 以上被国外企业抢占，元器件、芯片、软件的一些高端产品缺乏新产品和品牌的生成机制，系统集成能力还非常薄弱。例如，传感器产业与国际水平存在明显差距，特别是超高频 RFID 技术国内发展较晚，技术相对欠缺，从事超高频 RFID 产品生产的企业很少，更缺少具有自主知识产权的创新型企业；应用层技术研发起步更晚，大部分分散于低端层次，尚处于跟踪阶段，缺乏核心技术，整体解决方案能力不足；对应用技术的标准化和知识产权保护等问题，也还没有引起足够的重视，绝大部分知识产权和技术标准由国外企业掌控，一些核心技术、产品和装备依赖进口。这些将严重制约我国物联网产业实现跨越发展。

造成这种现状的原因是多方面的，主要体现在技术研发目前更多停留在国家科研机构层面，尚未形成有序的研发层次，技术转化没有形成有序机制和有效平台；研发力量比较分散，政府投入严重不足，研发重点不突出，有限的资

金投入面太广，难于形成技术突破；国内企业技术研发跟进不力，在核心技术研发方面投入的资金、人力相对国外企业也存在明显差距等方面。

我国物联网技术标准体系也亟待统一和完善。物联网是跨技术、跨行业、跨领域的应用，各行各业应用特点和用户需求不同，亟需统一标准体系，尤其是实现核心技术的专利化和标准化。虽然目前我国已开展物联网相关标准的制定，但整体来看，相关主要标准尚未出台，距离建立完整标准体系的要求还比较远。现有标准的零散、缺失和不统一，导致物联网市场分割，制造和服务成本偏高，容易使产业发展走弯路，不利于物联网产业发展。另外，我国与国际标准融合存在较大差距，技术标准上话语权还相对有限，造成我国物联网开发、集成、部署和维护的高成本，制约物联网业务的大规模应用。

1.5　物联网的信息安全和隐私保护问题

信息安全和隐私保护是互联网时代的关键问题，而在物联网时代，信息安全和隐私保护问题将变得更加重要。如果说互联网的主要服务是为人与机器的远程连接提供了一种平台的话，那么物联网将为物与物的远程连接和控制提供技术手段。如果没有更为可靠的信息安全技术，物联网环境下的信息安全和隐私的泄露将遭受更大的威胁，其结果也将更严重。

对信息安全性保护的需求不局限于对数据内容机密性保护。事实上，物联网应用系统中对信息安全的要求更多的是认证性，即对数据来源和数据完整性的确认、对通信端（人或机器）身份的确认，和对认证后将进行的数据机密性保护所需要的会话密钥的建立技术。

随着网络和通信技术的发展，越来越多的信息需要受到安全技术的保护，越来越多的信息会成为隐私保护技术服务的对象。当我们的交往范围比较小时（如一个村落内），我们的个人信息几乎没有什么可以保护的，也无需保护；当我们的交往范围大一些时（如城市的外来人员），一些信息就成为个人隐私信息，如收入、家庭财产、子女情况等，这些信息不希望陌生人得知；当我们的交往范围更大一些时（如网络交友），更多的信息会成为隐私信息，包括个人姓名、职业等；当我们走进虚拟世界或受物联网的约束时，更多的一些信息会成为隐私信息，包括使用设备的代号（如手机 IMSI 码）、地理位置，甚至生活习惯（如行走路线和不同地点停留时间）等。

安全性和隐私性是关系到物联网系统健康和可持续发展的关键技术。一些小微规模的物联网示范应用系统可能无需信息安全保护措施，或者只需要非常简单的信息安全保护机制（如简单的数据加密），而在实际中也没有发现信息

安全方面问题，不是因为这些系统不需要信息安全保护或者信息安全措施已经足够，而是不值得攻击者去实施攻击。但是，随着这些系统的规模化发展，简单的信息安全保护技术将不能满足需求，将会面临越来越严重的敌手攻击，如果这些物联网系统应用于重要行业，由于信息安全机制的脆弱所带来的经济损失和社会影响将是无法估量的。

生活中，人们对信息安全所面临的威胁认识不足，所采用的技术手段也比较简单落后。试想一想，有多少泄密事件在我们没有感觉的情况下发生了，有多少信息的泄露让我们感到不可思议的困难但却实实在在地发生了。维基解密所披露的一些秘密信息，让世人震惊：这些秘密信息在严格管控和最高技术保护中是如何泄露出去的呢？其实，维基解密也许还有一些尚未披露的秘密信息，其他机构和个人也可能获取到某些核心秘密信息，只不过这些信息尚未公布于众，也许永远不会公布于众，那么这些泄露的信息中又有多少是我们认为尚在安全保护之下的呢？

通过互联网公布的信息我们看到，2011 年 12 月 21 日，国内最大的程序员社区 CSDN 上 600 万用户资料被公开，同时黑客公布的文件中包含用户的邮箱账号和密码；2011 年 12 月 22 日，人人、开心、多玩、7k7k、178 游戏、嘟嘟牛等网站用户信息被黑客公布，涉及用户资料近 5000 万份；12 月 24 日，天涯全面沦陷，泄露多达 900 万账户信息；12 月 24 日，网易土木在线也沦陷，数据量惊人；12 月 25 日，百度疑因账号开放平台泄露账户信息；网络泄密事件还在不同程度地继续着……

2011 年末发生的一系列网络泄密事件警示我们，许多系统的安全保护措施远远不够，我们不能总是亡羊补牢，甚至一些系统可能已经亡羊了，因为没有意识到，所以还没有考虑到要补牢。许多从事密码算法和信息安全的研究人员都知道，在信息安全的保护方面不能有丝毫的侥幸心理，敌手的攻击能力和获取信息的能力比我们想象的要强得多，一些信息系统看似没有遭到敌手的攻击，一方面可能尚未引起敌手注意，或敌手认为不值得去攻击；另一方面，或许该系统已经被敌手攻破了，只是用户没有察觉到而已。

信息安全作为一种关键技术，在物联网的感知层、传输层、处理层和应用层都具有非常重要的应用，不同逻辑层对信息安全的需求不同，需要的信息安全技术也不同。因此信息安全作为一种第三方服务产业将得到实质性地发展，包括公钥证书管理中心、电子产品知识产权认证和管理中心、身份管理系统和平台、信息安全检测与评估平台等。但不同于其他产品的是，信息安全类产品一般由可信机构（如政府）负责或参与管理，以降低信息安全领域人为欺骗的因素。

除作为第三方服务类型提供的信息安全产品外，物联网相关产品也将具有