教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

# 物联网安全保障技术实现与应用

仇保利 主编 / 胡志昂 范红 邵华 副主编

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

# 物联网安全保障技术实现与应用

仇保利 主编
胡志昂 范红 邵华 副主编



清华大学出版社
北京

## 内 容 简 介

本书结合公安部第一研究所“物联网一体化安全检测专业化服务”项目的研究成果和作者的实践经验，系统阐述了物联网工程及产品安全检测的相关技术和方法。全书共10章。第1章介绍物联网体系结构、关键技术以及国内外物联网市场环境。第2、3章介绍我国物联网面临的安全威胁、安全需求以及国内外安全检测技术发展的最新动态。第4章从研究角度介绍物联网安全模型，包括物联网单层安全模型、物联网整体安全模型、物联网专项安全模型和云安全模型等。第5章介绍物联网安全保障体系架构，从法律法规、政策、标准、技术实施、检测与评估等方面进行阐述。第6～9章分别从物联网安全检测标准与指标、物联网产品检测、物联网工程/系统检测与检查、物联网风险评估等技术能力建设和实践进行了介绍。第10章根据已建成的检测平台，在智能感知类产品安全检测、接入传输类产品安全检测、业务应用类产品安全检测、系统安全检测/检查和风险评估等方面给出检测实例。

本书适合作为高等院校相关专业“物联网安全”课程的教材，同时可供从事物联网工程和产品研发及产品安全检测等工作的专业人员参考。



**图书在版编目(CIP)数据**

物联网安全保障技术实现与应用/仇保利主编. —北京：清华大学出版社，2017
(网络空间安全重点规划丛书)
ISBN 978-7-302-47611-5

Ⅰ. ①物… Ⅱ. ①仇… Ⅲ. ①互联网络－应用－安全技术 ②智能技术－应用－安全技术 Ⅳ. ①TP393.4 ②TP18

中国版本图书馆CIP数据核字(2017)第154217号

**责任编辑**：张　民　战晓雷
**封面设计**：常雪影
**责任校对**：焦丽丽
**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
**课件下载**：http://www.tup.com.cn，010-62795954
**印 刷 者**：北京富博印刷有限公司
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：29.75　　**字　　数**：683千字
**版　　次**：2017年10月第1版　　**印　　次**：2017年10月第1次印刷
**印　　数**：1～2000
**定　　价**：59.50元

产品编号：056209-01

网络空间安全重点规划丛书

# 编审委员会

# 出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006 年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007 年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时 5 年，制定出我国第一个信息安全专业指导性专业规范，于 2012 年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013 年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014 年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015 年 6 月，国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4 号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了“网络空间安全重点规划丛书”的工作，由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”“普通高等教育精品教材”“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn，联系人：张民。

“网络空间安全重点规划丛书”编审委员会

# 前言

物联网被看作是继计算机、互联网与移动通信网之后的又一次信息产业变革。我国已将物联网作为战略性新兴产业重点推进，特别是在2009年提出“感知中国”以来，物联网在我国快速发展，一大批物联网产业园和物联网产业集聚基地已经逐步发展和完善起来，正在显现出资源集聚效应和规模增值效应。

可以说物联网已将经济社会活动、战略性基础设施资源和人们生活全面架构在全球互联互通的网络上，所有活动和设施理论上都透明化了。一旦遭受攻击，安全和隐私将面临巨大威胁，极有可能在现实世界造成电力中断、金融瘫痪、社会混乱等严重危害公共安全的事件，甚至将危及国家安全，因此，保障物联网安全已变得越来越重要。

在近年的工作实践中，我们深刻认识到，面对国内日益发展的物联网市场，一方面急需出台物联网建设和产品研发的标准和规范，另一方面急需一批专业化检测服务队伍对各地物联网工程及产品进行安全性检测，为物联网发展保驾护航。为此，公安部第一研究所成功申请了国家发展与改革委员会信息安全专项“物联网一体化安全检测专业化服务”项目。笔者对项目研究成果和实践经验加以整理总结，编写了本书。全书共分为10章，主要内容如下。

第1章对物联网体系结构、关键技术以及国内外物联网市场环境进行梳理。

第2、3章分别介绍我国物联网面临的安全威胁、安全需求以及国内外安全检测技术发展的最新动态。

第4章从研究的角度介绍物联网安全模型，包括物联网单层安全模型、物联网整体安全模型、物联网专项安全模型以及云安全模型等。

第5章介绍物联网安全保障体系架构，从法律法规、政策、标准、技术实施、检测与评估等方面进行阐述。

第6～9章分别从物联网安全检测标准与指标、物联网产品检测、物联网工程/系统检测与检查、物联网风险评估等技术能力建设和实践的角度进行介绍。

第10章根据已建设的检测平台，在智能感知类产品安全检测、接入传输类产品安全检测、业务应用类产品安全检测、系统安全检测/检查、风险评估等方面给出了实际检测示例。

本书由仇保利主编并负责全书的统稿工作。各章编写分工如下：仇保利编写了第1章和第5章，胡志昂编写了第2章、第10章，范红编写了第7～9章，邵华编写了第3章、第4章、第6章。

本书的编写得到公安部第一研究所“物联网一体化安全检测专业化服务”项目团队、清华大学公共安全研究院、上海交通大学的大力支持，作者在此一并表示感谢。

本书广泛收集了国内外的相关材料和数据，翻译了大量国外文献，凝聚了作者从事物联网安全保护的实践经验以及研究思考的成果。由于时间仓促，错误和纰漏之处在所难免，诚望广大读者批评指正。

作　者

2017年6月

# 目录

# 第1章 物联网概述

随着信息技术的快速发展，物联网(Internet of Things，IoT)被看作是继计算机、互联网与移动通信网之后的又一次信息产业变革。物联网对零售、物流、交通运输、医疗、家具等多行业信息化产生了深远的影响。比如，商场或超市中的商品，只要其在特定的地理范围内，那么相应的商品信息就可以自动地记录到信息系统当中，通过互联网实现自动传输、处理、存储、共享等过程。这种形式一方面可以帮助商家对货物的选购进行决策，另一方面可以掌握商品的流向，从而定制个性化服务，甚至可以有效地降低由于各种原因导致的商品丢失的几率。

## 1.1 什么是物联网

对于物联网的定义，可谓众说纷纭。简单来讲，物联网就是“物物相连的网络”。其核心和基础就是网络，是互联网在现实世界的延伸。物联网打破了以前的传统思维。过去一直是将物理基础设备和IT基础设施分开：一方面是汽车、商品、建筑物、家居，另一方面是机房、服务器、计算机、网络设备、网线等。而在物联网时代，所有的物品信息、基础设施、自然状态、人类属性都可以被感知，并在网络上自由地交换与共享。

物联网范畴包括物与物的连接、物与基础设施的连接、物与环境的连接以及物与人的连接。2005年，在突尼斯举行的信息社会世界峰会(World Summit on the Information Society，WSIS)上，国际电信联盟(ITU)就发布了《ITU互联网报告2005：物联网》，该报告描绘了物联网的蓝图：世界上所有的物体，从轮胎到牙刷，从房屋到纸巾，都可以通过互联网主动进行数据交换，如图1-1所示。

物联网起源于比尔·盖茨1995年《未来之路》一书。1998年，麻省理工学院提出了当时被称作EPC(Electronic Product Code，电子产品代码)系统的物联网构想。1999年，在物品编码和RFID(Radio Frequency Identification，射频识别)技术的基础上，Auto-ID公司提出了物联网的概念。下面列举比较常见的物联网定义。

国际电信联盟发布的ITU互联网报告，对物联网做了如下定义：“通过二维码识读设备、射频识别装置、红外感应器、全球定位系统和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相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。”

2012年发布的ITU-T Y.2060描述了物联网的定义：“物联网是信息社会的一个全球基础设施，它基于现有和未来可互操作的信息和通信技术，通过物理的和虚拟的物物相

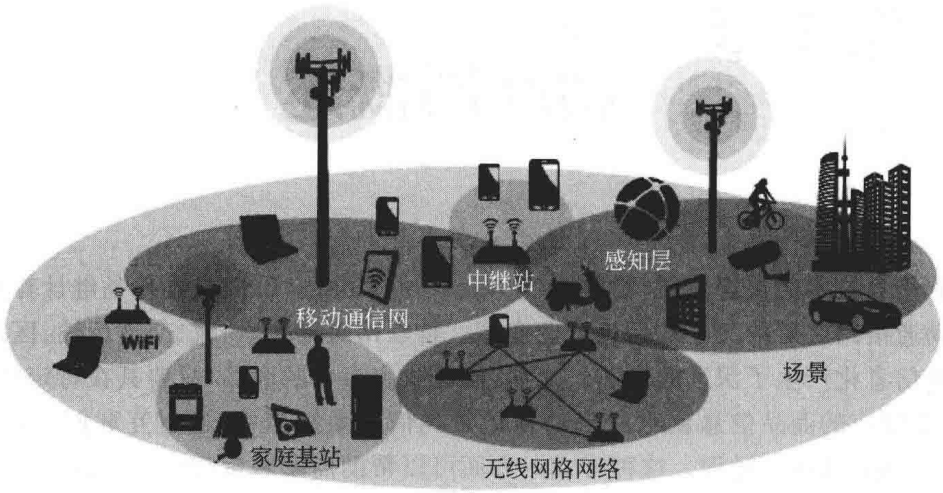


图 1-1　物联网蓝图

联来提供更好的服务。”

维基百科给出的定义是：“物联网是一个基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。”

中国工业和信息化部对物联网的最新定义是：物联网是互联网和通信网的网络延伸与应用拓展，具有整合感知识别、传输互联和计算处理等功能，是对新一代信息技术的高度集成和综合运用。物联网通过信息共享和业务协同，将人与人之间的信息交互沟通向人与物、物与物扩展延伸，它的应用为优化资源配置、加强科学管理、缓解资源能源约束提供了可能，拓宽了道路。

不管如何定义，从物联网本质上讲，物联网是人类对现实世界更透彻地感知、更深入地洞察的需求，是现代信息技术发展到一定阶段后出现的一种聚合性应用与技术提升。

从推动经济发展的角度来讲，物联网有望成为后金融危机时代经济增长的引擎。物联网把新一代 IT 技术充分运用在各行各业之中，具体来说，就是把感应器嵌入和装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道等各个物体中，然后将物联网与现有的互联网有机整合起来，实现人类社会与物体的整合，在这个整合的网络中，存在能力超级强大的中心计算机群，能够对整合网络内的人员、机器、设备和基础设施实施实时的管理和控制，在此基础上，人类可以用更加精细和动态的方式管理生产和生活，达到“智慧”状态，提高资源利用率和生产力水平，改善人与自然的关系。

## 1.2　物联网体系结构

物联网作为一种聚合性的综合网络系统，涉及信息技术自上而下的每一个层面，将各类信息技术协同起来，则需要体系结构支撑，因此，在物联网应用过程中，出现了若干物联网的体系结构。

### 1. 物品万维网

物品万维网(Web of Things,WoT)是从技术实现的角度来描述物联网。WoT 是指利用 Web 的设计理念和技术,将物联网网络环境中的设备抽象为资源和服务能力连接到 Web 空间,搭建基于异构网络和分布式终端的泛在应用开发环境,使得物联网上的嵌入式设备和业务更容易接入与访问。WoT 是 IoT 的一种实现模式。它将那些嵌入智能设备的日常用品或者计算机都集成到 Web。不像其他 IoT 系统那样,WoT 利用了 Web 的标准,将互联网的整个生态系统扩展到日用智能设备。目前在 WoT 里比较广泛接受的标准有 URI、HTTP、REST、RSS 等。

WoT 技术特点如下:

(1) HTTP 作为应用层协议而不像 Web Services 那样作为传输协议。

(2) 用 REST 接口将智能设备的同步能力开放,并且适用于整个 ROA(Resource Oriented Architectures,面向资源的架构)。

(3) 利用 Web 标准(Atom)或者服务器推送机制(Comet)将智能设备的异步能力开放。

利用这些特点,使得智能设备的服务的耦合性降低,同时也提供了一个统一的接口让开发者更容易运用。

WoT 可以真正释放设备联网的潜能,物联网的目标是为所有被束缚在智能设备内部的信息提供 URI(Uniform Resource Identifier,统一资源标识符),使用标准的 MIME(Multipurpose Internet Mail Extension,多用途因特网邮件扩充)来编码这些信息,并且通过 HTTP 来传输这些信息。

目前 IoT 系统多数都是垂直化的系统,开放性很差,彼此的互通性存在问题,资源的共享性差,升级困难,成本很高。WoT 系统提供了一种开放的方式,有利于资源的重用和跨平台的协作等,这是 WoT 的独有优势。

理论上 WoT 独特的使用场景似乎不存在。WoT 能做的,IoT 都能做。但谈及开放性和成本的时候,有些就只有 WoT 能做了。WoT 更适合于面向弱安全性和弱实时性要求、跨平台需要比较高、开放性高的应用场景。如果成本方面有压力,而对于业务的丰富性有要求,则 WoT 将比 IoT 有更加良好的表现。

2015 年 1 月,W3C 宣布新设立 WoT 计划(Web of Things Initiative),开发支持基于互联传感器及作动器(控制器)等为代表的物联网资源、基于 Web 数据的应用和服务及其开放市场以及所需的开放 Web 标准。

### 2. 物联网的自主体系结构

物联网的自主体系结构(Autonomic-oriented Architecture for the Internet of Things)是为了适应异构的物联网无线通信环境而设计的体系结构。该自主体系结构采用自主通信技术。自主通信是以自主件为核心的通信,自主件在端到端层次以及中间节点执行网络控制中已知的或者新出现的任务。自主件可以确保通信系统的可进化特性。

物联网的自主体系结构如图 1-2 所示,包括数据面、控制面、知识面和管理面。数据面主要用于数据分组的传递;控制面通过数据面发送配置报文,优化数据面的吞吐量以及

可靠性；知识面提供整个网络信息的完整视图，并且提炼成为网络系统的知识，用于指导控制面的适应性控制；管理面协调和管理数据面、控制面和知识面的交互，提供物联网的自主能力。

这里，自主特征主要是由 STP/SP 协议栈和智能层取代传统的 TCP/IP 协议栈。如图 1-3 所示，STP 和 SP 分别表示智能传送协议(Smart Transport Protocol)和智能协议(Smart Protocol)，物联网节点的智能层主要用于协商交互节点之间 STP/SP 的选择，用于优化无线链路上的通信和数据传送，满足异构物联网设备之间的联网的需求。

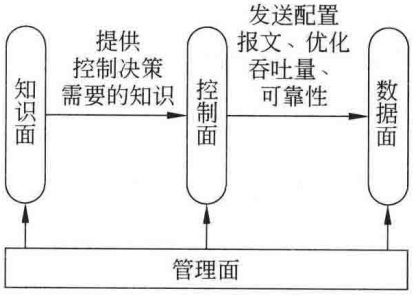


图 1-2　物联网自主体系结构

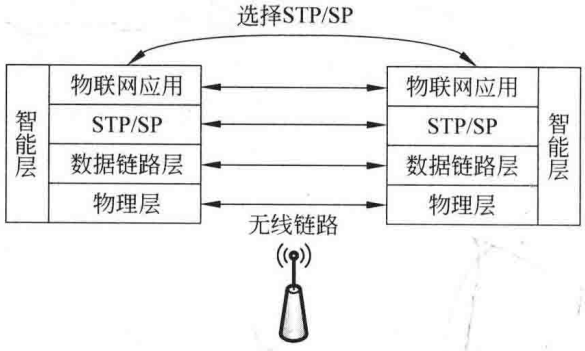


图 1-3　物联网自主体系结构的协议栈

这种面向物联网的自主体系结构涉及的协议栈较为复杂，只适用于计算资源较为富裕的物联网节点。

### 3. UID 技术体系结构

日本在电子标签方面的发展始于 20 世纪 80 年代中期的实时嵌入式系统 TRON，T-Engine 是其中核心的体系架构。在 T-Engine 论坛领导下，泛在 ID(Ubiquitous ID，UID)中心于 2003 年 3 月成立，设立在东京大学，并得到日本政府经产省、总务省以及大企业的支持，其成员包括微软、索尼、三菱、日立、日电、东芝、夏普、富士通、NTT、DoCoMo、KDDI、J-Phone、伊藤忠、大日本印刷、凸版印刷、理光等重量级企业。UID 中心建立的目的是为了建立和普及自动识别物品所需的基础技术，最终实现“计算无处不在”的理想环境。2004 年 4 月，UID 中国中心成立，标志着中国向“计算无处不在”的时代迈进了一大步，使中国在泛在技术的应用领域与世界最先进的水平同步发展。2010 年，福州大学成立“福州大学 UID 物联网联合研发中心”，从事 UID 软件的开发工作和推广工作。

UID 技术体系架构由泛在识别码(Ucode Tag)、Ucode 信息服务器(Ucode information server)、泛在通信器(ubiquitous communicator)和 Ucode 解析数据库(Ucode relation database)4 部分组成，其系统结构如图 1-4 所示。

其应用流程是泛在通信器读取物体上的 Ucode 基本信息，并将 Ucode 基本信息上报给 Ucode 解析数据库进行解析，与此同时也可以将 Ucode 信息进行注册，若成功解析，返回一个 URL 地址，访问 Ucode 信息服务器，泛在通信器访问 Ucode 信息服务器即可使用相关服务，包括读取更详细的数据或控制物体等。

考虑到安全要素，UID 技术体系架构增加了 eTRON 认证中心，如图 1-5 所示。

Ucode 是识别对象所必需的要素，ID 则是识别对象身份的基础。Ucode 是在大规模