INFORMATION SECURITY

nternet of Things

物联网信息安全

徐小涛 杨志红 主编
吴延林 夏启超 副主编

人民邮电出版社
POSTS & TELECOM PRESS

INFORMATION SECURITY

Internet of Things

物联网信息安全

徐小涛 杨志红 主编
吴延林 夏启超 副主编

人民邮电出版社
北京

图书在版编目（CIP）数据

物联网信息安全 / 徐小涛，杨志红主编. -- 北京 : 人民邮电出版社，2012.9
ISBN 978-7-115-28560-7

Ⅰ. ①物… Ⅱ. ①徐… ②杨… Ⅲ. ①互联网络－信息安全 Ⅳ. ①TP393.4

中国版本图书馆CIP数据核字(2012)第120165号

内 容 提 要

本书紧密跟踪物联网信息安全技术的最新发展，依据国内外物联网信息安全技术的最新标准，深入浅出地介绍了物联网信息安全的体系结构及关键技术；同时依据典型物联网信息安全领域的工程实践，介绍了物联网工程的信息安全管理机制。

本书内容包括物联网信息安全概述、物联网信息感知安全、物联网信息存储安全、物联网信息传输安全、物联网应用层信息安全、IPv6 信息安全、云计算安全以及物联网信息安全管理等物联网信息安全领域的关键环节。

本书内容力求科学性、先进性、系统性和实用性，可作为从事物联网信息安全工作的工程技术人员、管理人员、运营商和设备制造商的技术参考书或培训教材，也可作为高等工科通信专业和相关专业的高年级本科生的教材或参考资料。

物联网信息安全

◆ 主　　编　徐小涛　杨志红
副 主 编　吴延林　夏启超
责任编辑　李　静

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16.5　　2012 年 9 月第 1 版
字数：403 千字　　2012 年 9 月北京第 1 次印刷

ISBN 978-7-115-28560-7

定价：49.00 元

读者服务热线：(010)67119329　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着国内外对物联网技术重视程度的不断提高，物联网在社会的许多领域都获得了飞速的发展，成为现代社会信息化建设的重要推手。在网络攻击手段日趋多样的今天，信息安全成为制约物联网技术推广应用的瓶颈，解决物联网信息安全问题迫在眉睫。

为了适应物联网信息安全工作的发展需求，满足从事物联网技术研究、管理、服务、教学的工程技术人员了解物联网信息安全工作的发展情况，是作者编写《物联网信息安全》一书的根本目的。

全书共分为 9 章。第 1 章主要介绍了物联网信息安全的概念、基本属性、安全架构和信息安全基本策略，综述了物联网信息安全的服务内涵、安全机制以及信息安全设计原则和步骤。第 2 章主要介绍了物联网感知层面临的安全威胁，描述了物联网信息感知的安全特点，介绍了物联网感知层信息安全的关键技术和信息安全机制。第 3 章介绍了物联网信息存储安全的关键技术和主要手段，并对物联网系统的数据销毁、恢复以及灾难恢复技术进行了探讨。第 4 章结合物联网传输层的传输技术手段，介绍了物联网常用的信息传输技术的安全机制，并对异构网络的信息传输安全以及物联网的电磁泄漏防护进行了研究。第 5 章以物联网应用层的信息安全技术发展为基础，着力介绍了访问控制、数字签名、身份认证、数字水印和数字指纹等信息安全手段。第 6 章结合物联网的应用领域和面临的网络威胁形势，介绍了物联网应用过程中面临的主要攻击手段及防护技术。第 7 章以物联网关键技术 IPv6 的信息安全为着眼点，介绍了 IPv6 技术的信息安全协议和密钥管理机制。第 8 章以云计算在物联网中的应用为基础，介绍了云计算的信息安全形势、关键技术和信息服务机制。第 9 章以物联网的应用特征为基础，结合网络信息安全管理技术的发展，介绍了物联网信息安全风险评估、管理标准、管理体系以及效能评估。

本书由徐小涛、杨志红主编，吴延林、夏启超为副主编。本书得到了国防信息学院和江汉大学的大力支持，李建军主任、硕士研究生导师刘建中副教授、熊华副教授、马同兵副教授、郎为民副主任、胡东华讲师、王逢东讲师、张昆讲师、王会涛讲师对本书提出了宝贵的编写建议。李健讲师、朱元诚讲师、高泳洪讲师、项宏宇讲师完成了部分文档的处理，并更正了不少错误，在此向他们表示衷心的感谢。

人民邮电出版社的李静老师为本书的出版付出了辛勤的劳动，人民邮电出版社对本书的出版给予了大力的支持，在此一并表示感谢。

由于物联网信息安全技术仍在不断发展之中，新的技术标准和手段不断涌现，加之作者水平有限，编写时间仓促，本书难免存在不足之处，恳请各位专家和读者不吝指出。

编　者

2012 年 1 月

目　录

第1章 概 述

1.1 物联网和信息安全

1.1.1 物联网

物联网是一个新兴的网络技术。由于物联网概念出现的还不久，所以其内涵还在不断地发展，其信息安全机制也在不断完善。

1．物联网概念

目前，对于物联网的定义尚未在业内达成一致意见。物联网的定义主要是根据各标准化组织针对其产业化需要而制定的，主要有以下几个方面。

定义1：把所有物品通过射频识别（Radio Frequency IDentification,RFID）技术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。

定义1最早于1999年由麻省理工学院Auto-ID研究中心提出，实质是RFID技术和互联网的结合应用。RFID标签可谓是早期物联网最为关键的技术与产品环节，当时认为物联网最大规模、最有前景的应用就是在零售和物流领域。利用RFID技术，通过互联网实现物品（商品）的自动识别和信息的互联与共享。

定义2：2005年，国际电信联盟（International Telecommunication Union,ITU）在《The Internet of Things》报告中对物联网概念进行了扩展，提出任何时刻、任何地点、任意物体之间的互联，无所不在的网络和无所不在的计算的发展远景。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。

定义3：由具有标识、虚拟个性的物体/对象所组成的网络，这些标识和个性等信息在智能空间使用智慧的接口与用户、社会和环境进行通信。

定义3出自欧洲智能系统集成技术平台（the European Fechnology Platform on Smart Systems Integration,EPoss）在2008年5月27日发布的《Internet of Things in 2020》报告。该报告分析预测了未来物联网的发展，认为RFID和相关的识别技术是未来物联网的基石，因此更加侧重于RFID的应用及物体的智能化。

定义4：物联网是未来互联网的一个组成部分，可以被定义为基于标准的和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、物理属性和实质上的个性，使用智能接口实现与信息网络的无缝整合。

定义4来源于欧盟第7框架下RFID和物联网研究项目组在2009年9月15日发布的研究报告。该项目组的主要研究目的是便于欧洲内部不同RFID和物联网项目之间的组网；协调包括RFID的物联网研究活动；引导专业技术平衡发展，以使得研究效果最大化；在项目

之间建立协同机制。

从上述4种定义不难看出，“物联网”的内涵是起源于由RFID对客观物体进行标识并利用网络进行数据交换这一概念，并不断扩充、延展、完善而逐步形成的。

随着物联网技术的推广应用，我国的电信运营商也结合国内物联网的发展特点，给出了适合于中国物联网发展的定义。中国移动认为：物联网是指通过装置在各类物体上的电子标签、传感器、二维码等经过接口与无线网络相连，从而给物体赋予智能，可以实现人与物体的沟通和对话，也可以实现物体与物体间的沟通和对话，即对物体具有全面感知能力，对信息、具有可靠传送和智能处理能力的连接物体与物体的信息网络。

物联网定义的发展，打破了之前的传统思维，它将钢筋混凝土、电缆、芯片、网络整合为统一的基础设施。在此意义上，基础设施更像是一块新的地球工地，世界的运转就在它上面进行，其中包括经济管理、生产运行、社会管理乃至个人生活。物联网的大规模应用将有助于提高工作效率，降低生产运行成本，促进节能减排，实现人与自然和谐发展。

2. 物联网的基本特征

从通信对象和过程来看，物联网的核心是物与物以及人与物之间的信息交互。物联网的基本特征可概括为全面感知、可靠传送和智能处理。

全面感知，即利用射频识别、二维码、传感器等感知、捕获、测量技术随时随地对物体进行信息采集和获取。

可靠传送，即通过将物体接入信息网络，依托各种通信网络，随时随地进行可靠的信息交互和共享。

智能处理，即利用各种智能计算技术，对海量的感知数据和信息进行分析并处理，实现智能化的决策和控制。

为了更清晰地描述物联网的关键环节，按照信息科学的观点，围绕信息的流动过程，抽象出物联网的信息功能模型，如图1-1所示。

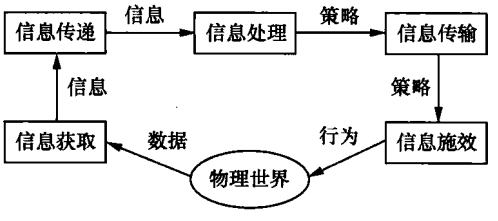

图1-1 物联网信息功能模块

（1）信息获取

信息获取包括信息的感知和信息的识别。信息感知是指对事物状态及其变化方式的敏感和知觉；信息识别是指能把所感受到的事物运动状态及其变化方式表示出来。

（2）信息传输

信息传输包括信息发送、传输和接收等环节，最终完成把事物状态及其变化方式从空间（或时间）上的一点传送到另一点的任务，这就是一般意义上的通信过程。

（3）信息处理

信息处理指对信息的加工过程，其目的是获取知识，实现对事物的认知以及利用已有的

信息产生新的信息，即制定决策的过程。

（4）信息施效

信息施效是指信息最终发挥效用的过程，具有很多不同的表现形式，其中最重要的就是通过调节对象事物的状态及其变换方式，使对象处于预期的运动状态。

1.1.2 信息安全

所谓信息安全是指保护信息资源，防止未经授权者或偶然因素对信息资源的破坏、改动、非法利用或恶意泄漏，以实现信息保密性、完整性与可用性的要求。在国际标准化组织的信息安全管理标准规范（ISO/IEC 17799）和其他一些权威机构的文献中，都定义了信息安全的基本特性，包括保密性、完整性、可用性、可控性、不可否认性等。

保密性就是对抗对手的被动攻击，保证信息不泄漏给未经授权的人，保证信息只允许授权用户访问。

完整性就是对抗对手主动攻击，防止信息被未经授权的人篡改，保证用户得到的信息及信息的处理方法是准确的、完备的。

可用性就是保证信息及信息系统确实为授权使用者所用，保证合法用户在需要时可以访问到所需信息和使用相关的资产。

可控性就是对信息及信息系统实施安全监控，对信息、信息处理过程及信息系统本身都可以实施合法的安全监控和检测。

不可否认性就是保证出现信息安全问题后可以有据可查，可以追踪责任到人或到事，又称信息的不可抗抵赖性。

我国国家信息安全重点实验室给出的定义是："信息安全涉及到信息的机密性、完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。"

英国 BS7799 信息安全管理标准给出的定义是："信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。"

美国国家安全局信息保障主任给出的定义是："因为术语'信息安全'一直仅表示信息的机密性，在国防部我们用'信息保障'来描述信息安全，也叫'IA'。它包含 5 种安全服务，包括机密性、完整性、可用性、真实性和不可抵赖性。"

纵观从不同的角度对信息安全的不同描述，可以看出 2 种描述风格。一种是从信息安全所涉及层面的角度进行描述，大体上涉及了实体（物理）安全、运行安全、数据（信息）安全；另一种是从信息安全所涉及的安全属性的角度进行描述，大体上涉及了机密性、完整性、可用性。信息系统安全的概念从经典模型上看，是要求系统无漏洞。这种系统的安全概念在于不断追求消灭漏洞，从概念上划分是静态的和基于空间的。这种模型的最大问题在于把系统漏洞看成是静态出现的，甚至完全没有考虑系统在运行中产生的"腐败"现象。而实际情况是系统漏洞是与系统运行状态相关的，并且是动态出现的。现代信息系统实用安全概念为：承认信息系统安全的脆弱性和可腐败性，正视信息系统安全的威胁，在尽可能地加强防护能力（消灭漏洞）的同时，要加强信息系统对自身漏洞和攻击的检测、管理、监控和处理能力，形成对信息系统安全事件的快速反应能力，强调信息系统安全基于时间的特性。

物联网作为新兴的信息系统，其安全建设要在公共操作环境（Common Operating Environment,COE）网络信息平台的体系结构框架指导下实施 PDR（Protection、Detection.Response,

防护、检测、反应）方案建设。防护（P）的目的在于阻止侵入系统或延迟侵入物联网系统的时间，为检测和反应提供更多的时间；检测（D）和发现的目的在于作出反应；反应（R）是为了修复漏洞，避免损失或打击犯罪。物联网信息安全和其他信息系统安全一样，都具有定性和定量的双重特征。

1.2 物联网信息安全

1.2.1 物联网面临的信息安全问题

物联网的应用，可使人与物的交互更加方便，给人们带来诸多便利。在物联网的应用中，如果信息安全无保障，那么个人隐私、物品信息等随时都可能被泄漏，而且容易为黑客提供远程控制他人物品，甚至操纵重要物联网系统，夺取控制管理权限的可能性。总的来讲，物联网面临的信息安全问题主要包括感知节点安全、感知网络安全、自组网安全、传输网络安全、信息服务安全以及 RFID 安全等。

1. 感知节点安全

感知节点的数量庞大，并且分布在一个很大的区域内，缺少人的有效监控，攻击者可以轻易地接触到这些设备，从而对它们造成破坏，甚至通过本地操作更换设备的软硬件。

2. 感知网络安全

通常情况下，感知节点所有的操作都依靠自身所带的电池供电，它的计算能力、存储能力、通信能力受到节点自身所带能源的限制，无法设计复杂的安全协议，因而也就无法拥有复杂的安全保护能力。而感知节点不仅要进行数据传输，而且还要进行数据采集、融合和协同工作。同时，感知网络多种多样，从温度测量到水文监控，从道路导航到自动控制，它们的数据传输和消息也没有特定的标准，所以没法提供统一的安全保护体系。

3. 自组网安全

自组网作为物联网的末梢网，它拓扑的动态变化会导致节点间信任关系的不断变化，这给密钥管理带来很大的困难。同时，由于节点可以自由漫游，与邻近节点通信的关系在不断地改变，节点的加入或离开无需任何声明，这样就很难为节点建立信任关系，以保证 2 个节点之间的路径上不存在想要破坏网络的恶意节点。路由协议中的现有机制还不能处理这种恶意行为的破坏。

4. 传输网络安全

物联网的传输网络应当具有相对完整的安全保护能力，但是由于物联网中节点数量庞大，而且以集群方式存在，因此会导致在数据传输时，由于大量设备的数据发送而造成网络拥塞。而且现有通行网络是面向连接的工作方式，而物联网的广泛应用必须解决地址空间空缺和网络安全标准等问题，从目前的现状看物联网对其核心网络的要求，特别是在可信、可知、可管和可控等方面，远远高于目前的 IP 网所提供的能力，因此认为物联网必定会为其核心传输网络采用数据分组技术。

此外，现有的通信网络的安全架构均是从人的通信角度设计的，并不完全适用于设备间的通信，使用现有的互联网安全机制会割裂物联网设备间的逻辑关系。

5. 信息服务安全

由于物联网设备可能是先部署后连接网络，而物联网节点又无人看守，所以如何对物联网设备进行远程签约信息和业务信息配置就成了难题。另外，庞大且多样化的物联网平台必然需要一个强大而统一的安全管理平台，否则独立的平台会被各式各样的物联网应用所淹没。但是，对物联网设备的日志等安全信息进行管理成为新的问题，并且可能割裂网络与业务平台之间的信任关系，导致新的安全问题产生。

6. RFID 系统的安全问题

RFID 是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据，可识别高速运动物体并可同时识别多个标签，识别工作无需人工干预，操作起来也非常方便。RFID 系统同传统的互联网一样，容易受到各种攻击，这主要是由于标签和读写器之间的通信是通过电磁波的形式实现的，其过程中没有任何物理或者可视的接触，这种非接触方式和无线通信存在严重的安全隐患。RFID 的安全问题主要表现在以下三方面。

（1）RFID 标识访问安全

RFID 标识受本身的成本所限，很难具备足以自身保证安全的能力,这样就面临很大的问题。非法用户可以利用合法的读写器或者自制的一个读写器，直接与 RFID 标识进行通信，这样就可以很容易地获取 RFID 标识中的数据，并且还能够修改 RFID 标识中的数据。

（2）信息传输信道安全

RFID 信息传输使用的是无线通信信道，这就给非法用户的攻击带来了方便。攻击者可以非法截取通信数据；可以通过发射干扰信号来堵塞通信链路，使得读写器过载，无法接收正常的标签数据，制造拒绝服务攻击；可以冒名顶替向 RFID 发送数据，篡改或伪造数据。

（3）RFID 读写器安全

RFID 读写器自身可以被伪造；RFID 读写器与主机之间的通信可以采用传统的攻击方法截获，所以 RFID 读写器自然也是攻击者要攻击的对象。由此可见，RFID 所遇到的安全问题要比通常的计算机网络安全问题复杂得多。

1.2.2 物联网信息安全关系

在面对物联网中的信息安全问题时，需要从社会、相关设备、安全技术等多个方面来综合考虑，重点需要处理好 6 个安全关系。

1. 物联网安全与现实社会的关系

我们知道，是生活在现实社会的人类创造了网络虚拟社会的繁荣，同时也是人类制造了网络虚拟社会的麻烦。现实世界中真善美的东西，网络的虚拟社会都会有；同样，现实社会中丑陋的东西，网络的虚拟社会一般也会有，只是表现形式不一样。互联网上如此之多的信息安全问题是人类自身制造的。同样，物联网的安全也是现实社会安全问题的反映。因此，我们在建设物联网的同时，需要拿出更大的精力去应对物联网所面临的更加复杂的信息安全问题。物联网安全是一个系统的社会工程，光靠技术来解决物联网安全问题是不可能的，它

必然要涉及技术、政策、道德与法律规范。

2. 物联网安全与计算机应用系统的关系

所有的物联网应用系统都是建立在互联网环境之中的，因此，物联网应用系统的安全都是建立在互联网安全的基础之上的。互联网包括端系统与网络核心交换 2 个部分。端系统包括计算机硬件、操作系统、数据库系统等，而运行物联网信息系统的大型服务器或服务器集群，及用户的个人计算机都是以固定或移动方式接入到互联网中的，它们是保证物联网应用系统正常运行的基础。任何一种物联网功能和服务的实现都需要通过网络核心交换在不同的计算机系统之间进行数据交互。病毒、木马、蠕虫、脚本攻击代码等恶意代码可以利用 E-mail、FTP 与 Web 系统进行传播，网络攻击、网络诱骗、信息窃取可以在互联网环境中进行。那么，它们同样会对物联网应用系统构成威胁。如果互联网核心交换部分不安全了，那么物联网信息安全的问题就无从谈起。因此，保证网络核心交换部分的安全，以及保证计算机系统的安全是保障物联网应用系统安全的基础。

3. 物联网应用系统建设与信息安全系统建设的关系

网络技术不是在真空之中，物联网是要提供给全世界的用户使用的，网络技术人员在研究和开发一种新的物联网应用技术与系统时，必然面对一个复杂的局面。成功的网络应用技术与成功的应用系统的标志是功能性与安全性的统一。不应该简单地把物联网安全问题看作是从事物联网安全技术工程师的事，而是每位信息技术领域的工程师与管理人员共同面对的问题。在规划一种物联网应用系统时，除了要规划出建设系统所需要的资金，还需要考虑拿出一定比例的经费用于安全系统的建设，这是一个系统设计方案成熟度的标志。物联网的建设涉及更为广阔的领域，因此物联网的安全问题应该引起我们更加高度的重视。

4. 物联网安全与信息保密的关系

信息保密技术是信息安全研究的重要工具，在网络安全中有很多重要的应用，物联网在用户身份认证、敏感数据传输的加密上都会使用到信息保密技术。但是物联网安全涵盖的问题远不止信息保密涉及的范围。信息保密技术是数学的一个分支，它涉及数字、公式与逻辑。数学是精确的和遵循逻辑规律的，而计算机网络、互联网、物联网的安全涉及的是人所知道的事、人与人之间的关系、人和物之间的关系，以及物与物之间的关系。物是有价值的，人是有欲望的，是不稳定的，甚至是难于理解的。因此，信息保密技术是研究物联网信息安全所必需的一个重要的工具与方法。

5. 物联网安全与国家信息安全战略的关系

物联网在互联网的基础上进一步发展了人与物、物与物之间的交互，它将越来越多地应用于现代社会的政治、经济、文化、教育、科学研究与社会生活的各个领域，物联网安全必然会成为影响社会稳定、国家安全的重要因素之一。因此，信息安全问题已成为信息化社会的一个焦点问题。每个国家只有立足于本国，研究信息安全体系，培养专门人才，发展信息安全产业，才能构筑本国的信息安全防范体系。如果哪个国家不重视物联网信息安全，那么他们必将在未来的物联网国际竞争中处于被动和危险的境地。

6. 物联网安全与信息安全共性技术的关系

对于物联网安全来说，它既包括互联网中存在的安全问题（传统意义上的网络环境中信息安全共性技术），也有它自身特有的安全问题（物联网环境中信息安全的个性技术）。物联网信息安全的个性化问题主要包括无线传感器网络的安全性与 RFID 的安全性问题。

1.2.3 物联网信息安全的特征

安全是基于网络的各个系统运行的重要基础，物联网的开放性、包容性和匿名性也决定了不可避免地存在信息安全隐患，物联网的推广应用需要在物联网基本特征的基础上深入研究物联网信息安全。

从网络信息安全的角度来看，物联网作为一个多网的异构融合网络，不仅存在与传感器网络、移动通信网络和互联网同样的安全问题，同时还有其特殊性，如隐私保护问题、异构网络的认证与访问控制问题、信息的存储与管理等。

信息与网络安全的目标是要达到被保护信息的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。在互联网的早期阶段，人们更关注基础理论和应用研究，随着网络和服务规模的不断增大，安全问题得以特显，引起了人们的高度重视，相继推出了一些安全技术，如入侵检测系统、防火墙、PKI 等。目前物联网的研究与应用还处于初级阶段，很多的理论与关键技术有待突破，特别是与互联网和移动通信网相比，还没有展示出令人信服的实际应用。在物联网的推广应用过程中，应该借鉴互联网的发展经验来探讨物联网的安全问题。

从物联网的信息处理过程来看，感知信息经过采集、汇聚、融合、传输、决策与控制等过程。整个信息处理的过程体现了物联网安全的特征与要求，也揭示了所面临的安全问题。

一是感知网络的信息采集、传输与信息安全问题。感知节点呈现多源异构性，感知节点通常情况下功能简单（如自动温度计）、携带能量少（使用电池），使得它们无法拥有复杂的安全保护能力；而感知网络多种多样，从温度测量到水文监控，从道路导航到自动控制，它们的数据传输和消息也没有特定的标准，所以没法提供统一的安全保护体系。

二是核心网络的传输与信息安全问题。核心网络具有相对完整的安全保护能力，但是由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量设备的数据发送使网络拥塞，产生拒绝服务攻击。此外，现有通信网络的安全架构都是从人通信的角度设计的，对以物为主体的物联网，要建立适合于感知信息传输与应用的安全架构。

三是物联网业务的安全问题。支撑物联网业务的平台有着不同的安全策略，如云计算、分布式系统、海量信息处理等，这些支撑平台要为上层服务管理和大规模行业应用建立起一个高效、可靠和可信的系统，而大规模、多平台、多业务类型使物联网业务层次的安全面临新的挑战。

从物联网的安全特征来看，信息隐私是物联网信息机密性的直接体现，如感知终端的位置信息是物联网的重要信息资源之一，也是需要保护的敏感信息。另外在数据处理过程中同样存在隐私保护问题，如基于数据挖掘的行为分析等。要建立访问控制机制，控制物联网中信息采集、传递和查询等操作，不会由于个人隐私或机构秘密的泄漏而造成对个人或机构的伤害。信息的加密是实现机密性的重要手段，物联网的多源异构性，使密钥管理显得更为困难，特别是对感知网络的密钥管理是制约物联网信息机密性的瓶颈。

物联网的信息完整性和可用性贯穿物联网数据流的全过程，网络入侵、拒绝攻击服务、Sybil 攻击、路由攻击等都可能使信息的完整性和可用性受到破坏。