



# 2016 年度物联网安全 研究报告

北京匡恩网络科技有限责任公司  
2016 年 12 月

# 前言

信息技术的发展经历了几个飞跃性的阶段，被称为信息技术发展的几次浪潮。信息技术发展的第一次浪潮是计算机的出现，它为信息的处理提供了前所未有的技术手段，在很多方面解放了人的脑力劳动，也为信息的管理带来了方便；信息技术发展的第二次浪潮是互联网技术的出现，它使得计算机数据可以实现远程传输，进一步可实现全球范围内的信息共享，为电子商务电子政务提供了技术平台；物联网技术的出现可以被认为是信息技术发展的第三次浪潮，它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，实现物联网终端的互联、海量数据的融合等，将为信息技术的服务形式带来一次革命性的变化。

从物联网概念的提出，到物联网架构的探讨，到物联网产业的落地，物联网技术和产业的发展可以说是非常迅速的。随着物联网示范项目的增加和物联网产业的落地，人们逐步意识到物联网安全保护的重要性。目前，物联网产业还处在初级阶段，物联网安全保护还没有被产业界重视，但物联网安全问题引发的事件已经发生了。黑客通过入侵并控制安全防护不强的物联网设备，可以发起大规模拒绝服务攻击，在多个国家都造成不同程度的影响。这一事件也说明物联网安全的重要性。没有安全保障，物联网系统的建设将伴随着风险。

物联网经过几年的发展，已经进入多行业落地阶段，同时也开始进入物联网安全建设阶段。国家出台的一系列法律法规，标准规范，都会引导物联网产业健康发展。同传统信息系统和计算机网络安全一样，安全保护技术的目的不是完全杜绝攻击事件，也无法做到完全杜绝黑客攻击，但可以大大提高攻击成本。这就是安全防护的目的。

2016年11月7日，第十二届全国人大常委会第二十四次会议表决通过了《网络安全法》，并将于2017年6月1日起施行。这标志着我国已经进入依法治理网络，依法保护网络安全的时代。物联网技术作为网络时代的重大应用潮流，理应得到信息安全技术的重点保护。

在此情况下，我们整理了这份研究报告，在整体上对物联网安全技术进行描述，同时关注一些近年来发生的安全事件和相关技术的最新进展。希望这份研究报告能为同行提供一些有价值的信息。

北京匡恩网络科技有限公司保留对此报告的著作权和追究因滥用此文章内容引起的对北京匡恩网络科技有限公司名誉、利益损害等行为的法律责任。

北京匡恩网络科技有限公司

2016年12月

# 目 / 录

前 言	2
第一章 物联网安全架构	7
1.1 物联网的概念与内涵	8
1.1.1 物联网的基本概念	8
1.1.2 物联网发展历程	8
1.1.3 物联网的基本架构	10
1.2 国内外物联网产业发展现状及相关政策	11
1.2.1 国外物联网产业发展状况及相关政策	11
1.2.2 我国物联网产业发展现状及相关政策	12
1.3 物联网的安全架构	13
1.3.1 物联网安全整体架构	13
1.3.2 物联网感知层安全技术	14
1.3.3 物联网网络传输层的安全技术	15
1.3.4 物联网处理应用层安全技术	15
第二章 物联网安全现状	17
2.1 物联网相关产业发展情况	18
2.1.1 物联网相关产业及发展状况	18
2.1.2 智慧交通	19
2.1.3 智慧水利	24
2.1.4 智慧管网	25
2.1.5 智慧农业	28
2.1.6 智慧城市	30

<b>2.2</b>	<b>物联网安全典型事件分析</b>	<b>33</b>
2.2.1	物联网攻击导致 DDoS 攻击事件	35
2.2.2	方程式组织工具泄露事件分析观察	43
<b>2.3</b>	<b>物联网安全现状—从逻辑架构视角分析</b>	<b>49</b>
2.3.1	物联网感知层安全现状	49
2.3.2	物联网网络传输层安全现状	50
2.3.3	物联网处理应用层安全现状	50
<b>2.4</b>	<b>物联网安全相关法规与政策</b>	<b>52</b>
2.4.1	国际物联网安全法规与政策	53
2.4.2	国内物联网安全法规与政策	56
2.4.3	行业领域网络安全法规与政策	58
2.4.4	国家网络安全法	60
<b>第三章</b>	<b>工业物联网安全现状</b>	<b>63</b>
<b>3.1</b>	<b>工业物联网的系统架构</b>	<b>64</b>
3.1.1	什么是工业物联网	64
3.1.2	工业物联网与工业互联网的关系	64
3.1.3	什么是工业物联网安全	66
3.1.4	工业物联网系统的安全技术	68
3.1.5	物联网安全建设——工业物联网安全是重中之重	69
3.1.6	工业物联网系统安全建设方案—独立监控网	70
<b>3.2</b>	<b>工业物联网漏洞分析</b>	<b>71</b>
3.2.1	工业物联网漏洞分布	71
3.2.2	2016 年 top10 漏洞	73
<b>3.3</b>	<b>2016 年工业物联网方面大事记</b>	<b>76</b>

3.4	我国对工业物联网的安全相关法规与政策	78
3.4.1	我国工业控制系统安全法规与政策	78
3.4.2	行业领域工控网络安全法规与政策	81
<b>第四章</b>	<b>物联网安全保护技术</b>	<b>87</b>
4.1	物联网感知层安全保护技术	88
4.1.1	物联网感知层的构成	88
4.1.2	传感器网络安全保护技术	90
4.1.3	智能摄像头及其安全保护	92
4.1.4	智能网关节点的安全性	94
4.1.5	智能移动终端的安全性保护	95
4.2	物联网网络传输层安全保护技术	96
4.2.1	互联网安全保护技术	96
4.2.2	移动网络安全保护技术	97
4.2.3	物联网专用网络 LPWAN 安全保护技术	99
4.3	物联网处理应用层安全保护技术	104
4.3.1	物联网处理应用层概述	104
4.3.2	物联网处理应用层信息安全问题分析	105
4.3.3	物联网处理应用层的安全防护建议	107
4.3.4	物联网处理应用层安全态势感知	108
<b>第五章</b>	<b>物联网安全产业发展趋势</b>	<b>111</b>
5.1	物联网产业发展趋势	112
5.2	物联网安全技术和产业发展趋势	114
<b>第六章</b>	<b>物联网安全建设发展建议</b>	<b>117</b>

# 第一章 物联网安全架构

## 1.1 物联网的概念与内涵

### 1.1.1 物联网的基本概念

物联网不是什么新生事物，而是信息技术发展到一定阶段的产物。因此，物联网的概念不是定义一类新事物，而是对已有的一些技术的总结和提升。

物联网没有标准定义，但通过特征描述的形式可以给出了物联网内涵的刻画。目前人民普遍接受的对物联网系统的特征描述为：物联网是由感知层、网络传输层和处理应用层组成的系统。

从本质上说物联网是将传统网络虚拟空间与现实物理空间相结合的一种技术。虽然物联网从概念上看仅仅是传统网络（如互联网）往传感网络的延伸，但这种延伸具有本质性的技术飞跃，因为它从虚拟空间延伸到现实的物理空间。如果说计算机的发明解放了人们的脑力劳动，是信息技术的第一次浪潮，计算机的互联实现了信息的远距离实时共享，是信息技术的第二次浪潮，那么物联网的诞生可以说是信息技术的第三次浪潮，因为它可以将虚拟空间与现实世界有机结合。

### 1.1.2 物联网发展历程

电子计算机的诞生可以追溯到具体的日期，互联网的诞生也有最初的模型诞生，但物联网的诞生似乎很难找到具体日期。物联网的概念最早由 MIT 的 Kevin Ashton 在 1998 年演讲中提出：把射频识别标签与其它传感器应用于日常物品形成一个物联网。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并做出反应，触发动作和生成服务；物品通过与其它物品或环境互动来参与商业、信息和社会活动，已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。

2005 年 5 月，美国国会要求美国科学院评估美国的技术竞争力。2006 年 2 月发布的《美



国竞争力计划》则将信息物理系统 (Cyber Physics System, CPS) 列为重要的研究项目。该项目中定义的信息物理系统的实质就是物联网，其目的是在环境感知的基础上，深度融合计算、通信和控制能力的可控可信可扩展的网络化物理设备系统，通过计算进程和物理进程相互影响的反馈循环实现深度融合和实时交互来增加或扩展新的功能，以安全、可靠、高效和实时的方式检测或者控制一个物理实体。

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处理，为管理和控制提供决策依据，并在人类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。

从一个狭义角度理解，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撑下，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。

网络通信技术的进步和基础建设已经可以满足世界上数十亿人的通信和上网服务，更高的带宽、更廉价的通信成本已可以承受如视频、传感量等非通话信息的加载，通信运营商更是迫切希望为宽带通信附加新的增值服务热点，并已展开这方面的实际应用，为物质信息联入通信网络奠定了基础（物联网的神经网络）。

在信息处理领域，一方面云计算技术、超级计算技术、专家智能技术的进步使得对海量信息的处理能力大大增强，另一方面嵌入式技术、系统级芯片（SoC）技术的发展使得很多信息在终端即可进行压缩和预处理，这些为物质信息大量涌入通信网络后面临的海量信息处理问题提供了解决办法（物联网的大脑）。

随着人类社会的进步和发展，人类在能源、环境、交通、安全、居住等领域都面临着严峻的挑战，迫使人们不得不寻求更加高效、更加智能的资源利用和调配模式，而物联网正是实现人类资源感知、分配和利用的最有效途径，体现在物联网在能源电力、环境保护、市政管理、安防反恐等领域都存在巨大的应用潜力，并成为世界各国应对金融危机后产业升级的



首选方案（物联网的躯干）。

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，如对物联网的搜索引擎，物联网的网络工厂（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，所有这些必将极大的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。

### 1.1.3 物联网的基本架构

虽然物联网的概念已经提出多年了，但物联网的定义一直没有很合适的，甚至对物联网的内涵都没有完全确定。那么什么是物联网呢？一般地，当我们不能给出一个概念的确切定义时，可以通过特征描述的形式来介绍这个概念。因此物联网的概念还是通过特征描述的方式介绍比较合适。

物联网一般被认为是具有感知层、网络传输层、处理应用层的一个系统。感知层包括传感器节点、终端控制器节点、感知层网关节点、RFID 标签、RFID 读写器设备，以及短距离无线网络（如 Zigbee）等；网络传输层主要以远距离广域网通信服务为主；处理应用层主要以云计算服务平台为基础，包括云平台的各类服务和用户终端等。由于云计算可以同时提供对数据的智能处理和对终端用户的服务，因此物联网架构中的处理层包括应用服务。物联网的架构如图 1.1 所示。



图 1-1 物联网架构示意图

图 1-1 所示的架构不是唯一的表达物联网内涵的方式。从不同角度理解物联网，就能得到不同的架构。除上述架构外，还有两种不同的架构。一种是“海-网-云”架构（亦称为“端-管-云”架构），其中“海端”是所有物联网感知终端和用户终端的全体，“网络”即等同于网络传输层，“云端”即为处理层。这种“海-网-云”架构把应用隐含在云服务中了。另外一种架构是六个域的架构，包括“用户域”、“目标对象域”、“感知控制域”、“服务提供域”、“运维管控域”和“资源交换域”。这种架构是按业务性质进行划分的。不同的架构代表不同的视角，其所表示的物联网的本质不变。

## 1.2 国内外物联网产业发展现状及相关政策

### 1.2.1 国外物联网产业发展状况及相关政策

物联网概念提出初期，包括美国、欧盟、日本、韩国等许多国家都分别制定了具体的发展计划，并制定了相关政策。到 2016 年，物联网产业的发展已经超越国家边界，在很大程度上是一种全球行为了。例如，针对物联网数据传输的特点而设计的低功耗广域网（Low Power Wide Area Network, LPWAN）通信技术，在世界各地蓬勃发展。

据 IDC 测算，2020 年全球物联网有望影响的下游市场规模将突破 3 万亿美元，超过 250 亿台系统 / 装置联网，而同时使用因特网的用户总数达 44 亿人。麦肯锡 2015 年 7 月发布的最新报告则指出，全球物联网有望渗透的下游应用市场规模将在 2025 年以前成长达到 3.9-11.1 万亿美元，达到约 11% 的全球经济占有率，并与城市管理、生产制造、家庭事务、汽车驾驶、能源环保、物流运输、工作办公、消费结算、个人健康等重要领域结合形成 9 个千亿级规模以上的细分市场。

物联网市场庞大，发展迅速，但是物联网安全问题却是潜在的隐患。事实上，许多厂家都已经在物联网安全方面行动起来了。

2016 年 10 月，在拉斯维加斯在 Money20/20 大会上，英特尔和 Visa 宣布达成合作，将支付安全技术集成到英特尔芯片组。未来物联网社会，硬件设备厂商可以更好更安全的构建一个支付环境。据了解，英特尔将在芯片的硬件层面对 Visa 数据进行安全加密，使用 3D 安全认证，确保使用英特尔芯片的电脑、手机以及其他硬件设备支付数据的万无一失。此外英特尔还透露到，酷睿处理器也将兼容现有的 3D 安全认证协议以及 EMVCo 即将在年底发布的 2.0 版本。

2016 年 10 月，AllSeen 联盟与 OCF(Open Connectivity Foundation) 宣布合并，未来将以 OCF 为存续名称。这两大组织最知名的物联网框架分别为 AllJoyn 与 IoTivity，是

Google 与 Apple 生态圈外最大的两强，合并后将为尚处分散的物联网市场带来整合，互通互融的情境将更有机会实现。OCF 现将透过 Linux 基金会 (The Linux Foundation) 发起 IoTivity 和 AllJoyn 开源专案。这两项专案将合力支持统一部署 IoTivity 的未来版 OCF 规格，并将两种技术的精华整合于统一的解决方案中。目前运行于 AllJoyn 或 IoTivity 解决方案的装置将具备互通性且可向后相容。已根据其中任何一种技术开发物联网解决方案的企业可继续进行，因为其产品必将与统一的物联网标准相容，这也正是业界一直要求的。

据 2016 年 11 月的《物联网世界》报导，最近 ARM 推出了两款基于 ARMv8-M 架构的低成本 32 位 MCU Cortex-M23 和 Cortex-M33，它们可将久经市场验证的安全技术 TrustZone 拓展到要求最为严苛的 IOT 终端节点。

2016 年 11 月 15 日，美国国土安全部公布了《保障物联网安全战略原则》(STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS)。该准则对物联网安全建设提出了具体建议，包括如下条款：(1) 在设计阶段要将物联网安全考虑在内；(2) 提前进行安全更新和脆弱性管理；(3) 以实践安全为建设基础；(4) 根据潜在影响，优先安全度量；(5) 推进物联网全系统的透明性；(6) 连接网络时需小心谨慎。

赛门铁克近日发布了《2017 年安全预测报告》，预测报告称随着网络犯罪分子对入侵企业及用户数据方法的不断改进，针对云及联网设备的网络攻击数量或将在 2017 年会增加。

### 1.2.2 我国物联网产业发展现状及相关政策

我国在物联网领域的技术研发攻关和创新能力不断提升，在传感器、RFID、M2M。标识解析、工业控制等特定技术领域已经拥有一批具有自主知识产权的成果，形成了涵盖感知制造、网络制造、软件与信息处理、网络与应用服务等门类的相对齐全的物联网产业体系，产业规模不断扩大，物联网应用发展进入实质性推进阶段，理念和相关技术产品已广泛渗透到社会经济民生的各个领域，在越来越多的行业创新中发挥关键作用。

经过几年的发展，我国在物联网技术研发、标准研制、产业培育和行业应用等方面已具备一定基础，已初步形成环渤海、长三角、泛珠三角以及中西部地区四大区域集聚发展的空间格局。

据 2016 年 9 月 28 日第一财经日报报道，“物联网之父” Kevin Ashton 在哈佛大学的科技创新研讨会上对第一财经记者表示：“中国将引领本世纪物联网技术的发展，无人驾驶技术是物联网实现飞跃的重要因素。无人驾驶技术的实现将最早发生在中国”。这说明国外专家对国内在物联网领域发展的认可。

虽然国内近几年来在物联网领域的发展非常迅速，在某些方面已经在引领物联网技术的发展，但仍然存在一些制约物联网发展的深层次问题急需解决，其中包括物联网安全问题。

2016 年，低功耗广域网技术（LPWAN）在世界范围内跳跃式发展，可以解决物联网终端在对数据进行远距离传输时的功耗问题，也可以部分解决数据进行远距离传输过程中的数据安全问题，但对一个完整的物联网行业来说，离完整的信息安全解决方案还有很大距离。华为等企业也在推进 NB-IOT 技术的产业应用，目标应用包括智能抄表等领域。

为了推进物联网有序健康发展，我国政府加强了对物联网发展方向、重点的规范引导，不断优化物联网发展的环境。2016 年 10 月 17 日，工信部印发《工业控制系统信息安全防护指南》。这个指南虽然是针对工业控制系统的，但在智能制造和“中国制造 2025”等技术和政策推动下，工业领域的物联网逐步成为物联网行业的重点。该指南为工业控制系统的智能化发展提供了安全保护的政策指导。

2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议上表决通过了《中华人民共和国网络安全法》，该法自 2017 年 6 月 1 日起施行。这是一部具有历史意义的法律，标志着今后在网络安全方面的一些恶意行为可以有法可依地定性为违法行为。这对物联网安全保护具有重要意义。

### 1.3 物联网的安全架构

#### 1.3.1 物联网安全整体架构

针对物联网的架构，我们可以分别制定安全技术。因此物联网安全架构如图 1-2 所示。

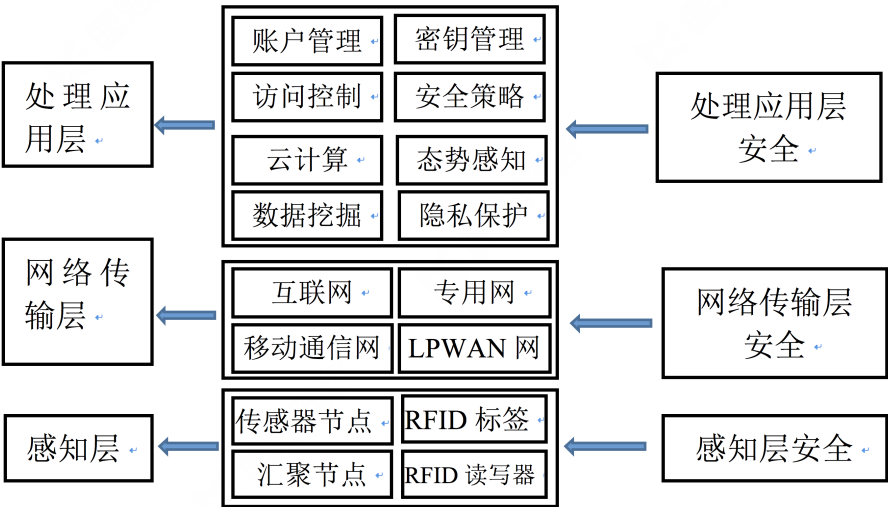


图 1-2 物联网安全架构示意图

值得注意的是，由于处理应用层中的处理功能和应用功能的安全技术可能有不同的开发



者和不同的用户，因此有些架构也将处理应用层的安全又细分为处理层安全和应用层安全，形成包括 4 个逻辑层的物联网安全架构，实际与分 3 个逻辑层的架构在本质上是一致的。

在图 1-2 所示的物联网安全架构中，感知层安全要保护的是数据在感知节点内部的处理安全（有没有恶意代码），和数据通信安全，包括传感器节点与汇聚节点之间的通信安全，和 RFID 标签与 RFID 读写器之间的通信安全。网络传输层安全主要是广域网通信过程的数据安全，包括通信节点之间的身份鉴别、数据机密性和数据完整性服务。对于物联网的网络传输层，还需要提供数据新鲜性保护，这是不同于传统通信网络的安全服务，重点用于对控制指令的保护。处理应用层安全主要包括处理服务，例如在云计算平台内的安全服务，包括系统安全、应用软件安全、数据存储安全、大数据处理安全等，和应用服务，例如对终端用户的身份鉴别、访问控制、密钥管理等一些列技术措施，实现云计算平台的数据在用户使用过程中应符合技术要求和策略。

### 1.3.2 物联网感知层安全技术

物联网的感知层可以包括各种传感器，大到视频监控，小到温湿度传感器等类型的传感器，其处理能力也千差万别。物联网感知层还包括 RFID 标签和读卡器，因此物联网感知层将包括处理能力及其受限的 RFID 标签。

在一个物联网系统中，我们需要明确感知层的边界，即哪些属于感知层。如果物联网的感知层是一个传感网，则传感网中的感知节点、路由节点、汇聚节点以及传感网所使用的网络（通常为短距离射频）都属于物联网的感知层。注意汇聚节点不是作为整个设备属于感知层，而仅仅是其汇聚功能属于感知层。因为在物联网系统中，作为感知层部分的汇聚节点除了完成与感知节点的通信外，还要负责将汇聚后的信息传送给上层处理中心，而其与上层通信的功能显然不再属于感知层。由于在物联网中，感知层的汇聚节点不仅具有汇聚的功能，还需要负责将所负责的传感节点的信息传递给处理中心，因此一般将感知层的汇聚节点称为感知层网关节点。因此，以传感网为物联网系统感知层的边界在传感网的网关节点，其汇聚功能到传感器节点部分是物联网的感知层。

在一个以 RFID 为主的物联网应用系统中，感知层将包括 RFID 标签和 RFID 读写器的通信功能。从 RFID 阅读器到后台数据库的部分将属于网络传输层。因此感知层的边界以 RFID 阅读器的功能为划分点。

感知层的安全技术包括如下内容：

(1) 设备安全，即传感器节点本身的安全，主要指传感器节点有足够的供电和正常的工作能力。更多的安全要求可能对传感器网络中的汇聚节点有意义。

(2) 计算安全，即传感器在处理数据时，处理器的执行环境安全性，包括操作系统（COS，

Android, Linux, Windows 等) 安全, 执行软件安全。

(3) 数据安全, 主要指重要数据的安全存储和调用接口, 如密钥信息, 通过外部接口直接读取这些数据应该受限。

(4) 通信安全, 即数据发送和接收时对数据的处理, 包括对数据的加密和解密能力, 完整性校验和验证能力, 对通信方的身份鉴别能力等。

### 1.3.3 物联网网络传输层的安全技术

物联网的网络传输层可以包括各种广域网。典型的广域网是互联网, 之后又有多种可以最终接入互联网的多种无线网络, 包括移动网络 (2G、3G、LTE、5G 等) 和近年来发展迅速的低功耗广域网 (Low Power Wide Area Network, LPWAN), 这些网络在物联网系统中都属于网络传输层。LPWAN 网络是专门为物联网业务而设计的, 具有低功耗的特点, 这对资源受限的物联网感知层节点是很重要的。

网络传输层安全的主要保护目标是网络本身和在网络上传输的数据。对网络本身的主要防护技术是抗 DDoS 攻击, 以保障网络的服务能力; 对数据的保护技术包括数据机密性技术、数据完整性技术、数据来源认证技术等。

### 1.3.4 物联网处理应用层安全技术

如果将物联网的处理应用层分处理子层和应用子层考虑的话, 物联网的处理子层主要指云计算平台, 其安全技术包括: (1) 云平台本身的环境安全; (2) 云平台的应用服务安全; (3) 云平台的数据安全。

云平台环境安全包括操作系统安全、虚拟隔离技术、用户安全管理技术、访问控制技术; 云平台的应用服务安全包括软件即服务 SAAS, 平台即服务 PAAS, 基础设施即服务 IAAS, 安全即服务 SecAAS 等; 云平台的数据安全包括数据处理安全和数据存储安全等。

物联网的应用子层对应的是具体的行业应用。对一些重要的业务数据, 如控制指令和配置参数等, 不应将安全服务依赖于通信服务商和平台商。为了提供行业内可控的全程数据安全, 需要有合理的密钥管理机制, 使得在物联网全流程内 (贯穿感知层、网络传输层和处理应用层) 具有安全保障。

在物联网系统建设过程中, 物联网安全保护机制应同时建设, 是否满足建设需求, 需要在建设初期进行评估, 建设过程中进行验证, 和建设后期进行测试。这就是安全评估和检测技术。

许多物联网的行业应用需要用到智能移动终端, 这些移动终端的安全性也是应用层安全的重要内容, 包括移动终端的操作系统安全、应用软件 (APP) 安全、用户口令安全等。





## 第二章

# 物联网安全现状

## 2.1 物联网相关产业发展情况

### 2.1.1 物联网相关产业及发展状况

物联网从概念的提出，到示范项目的落地，目前已经进入实际产业化阶段。物联网产业链结构已经比较完整了，从元器件到设备、从数据到安全服务、从软件产品到信息服务，都有系列产品和服务。一个完整的物联网产业链主要包括芯片与技术提供商、应用设备提供商、网络建设和运营服务商、软件与应用开发商、系统集成商、运营及服务提供商等环节。

今天，万物互联的物联网（IOT）时代正在“扑面而来”！BI Intelligence 在近日发布的《Internet of everything 2016》报告中预测，到 2020 年将有 340 亿台设备接入互联网，安装的物联网设备数量将达到 240 亿台，从 2015 年到 2020 年间，总共将有 6 万亿美元投资于物联网解决方案。在中国，根据工信部的权威数据，2015 年中国物联网产业规模已经达到 7500 亿元，同比增长 29.3%，媒体预测到 2020 年，中国物联网的整体规模将超过 1.8 万亿元。

普华永道在 11 月 29 日发布的《2017 年全球信息安全状况调查报告》报告显示，经过对中国内地和香港地区的审计，在过去 12 个月中，中国内地及香港企业检测到的各类信息安全事件平均数量为 2577 起，是去年同期的两倍，较 2014 年则飙升了 969%。Gartner 在另外一份安全报告中也对此预测：到 2020 年，针对企业的经确认安全性攻击中，有 25% 以上将涉及物联网。

物联网安全问题已经引起了各国政府的高度关注，就在美国这次的 DNS 服务商遭遇 DDoS 攻击事件之后，美国国土安全部在 11 月份旋即发布了《物联网安全指导原则》，向物联网设备和系统相关开发商、生产商、管理者及个人提供了一组安全规则建议；在欧洲，欧盟委员会目前正在起草新的网络安全标准，该标准主要针对物联网设备，欧盟委员会将会对市场上所有连接互联网的设备，推行新的安全标准，划分网络安全等级；在中国，就在刚刚召开的第三届世界互联网大会上，国家主席习近平在开幕主旨演讲上阐述关于网络空间治理理念，安全成为当中极其重要的内容。

物联网安全事件频发，既是挑战也同时蕴藏着巨大的商业机会。调查研究公司 MarketsandMarkets 预计称，2020 年全球物联网的安全市场将从 2015 年的 68.9 亿美元增长至 289 亿美元，即 2015 年至 2020 年的复合年增长率（CAGR）为 33.2%。

面对如此规模的“市场蛋糕”，吸引了产业链上下游大批市场玩家的“驻足”。既有传统的 IT 基础设施厂商（防火墙、VPN 等供应商）、互联网安全公司（更多从软件上提供安全防护、病毒查杀等）、也有专门瞄准物联网安全的新兴的创业公司。另外还有一类是产业

链上下游厂商在基于原有产品服务基础上，提供安全保护增值服务，如在芯片上增加高级安全设计。

但是，物联网安全是一个贯穿全产业链环节的系统工程，仅从硬件或者软件又或者网络传输单一层面进行检测、管理与安全防护，都很难从根本上杜绝安全隐患，尤其是涉及到国计民生等重大物联网项目，闭环安全生态的需求变得更为迫切，执行从底层芯片、软件系统、数据采集、数据存储、数据分析、网络传输到上层应用的全生态链安全变得非常关键。

从苹果 IOS 与谷歌 Android 两大移动互联网生态系统的构建对比上，我们也可以发现闭环生态模式在安全性等方面带来的价值胜过开放生态。苹果通过选择从芯片到软件系统、应用商店的闭环生态模式，应用可控性强、用户体验良好、安全性强，Android 选择开放的生态，版本碎片化严重、基于 Android 的各种厂商修改版本繁多、应用上线审核弱、安全性低。

另外，从商业模式上来看，若要求现有的物联网设备供应商来同时交付安全方案，站在市场客户的角度，这属于设备供应商的“分内事”、不应当为此额外支付费用，但对设备供应商来说，在不增加产品价格的同时还需要提供安全增值服务，意味着成本增加、利润缩水；从技术角度而言，物联网接入的设备数量与种类的海量与复杂性，不同设备供应商的安全方案由于各自采用的接口、标准协议的差异，在相互的兼容与对接上变得十分困难。

综合物联网安全市场的现状，迫切需求专业的、完整闭环安全生态模式的第三方安全解决方案提供商与服务商。

## 2.1.2 智慧交通

### 2.1.2.1 智慧交通定义

2010 年 IBM 提出“智慧的城市”愿景，引发了智慧城市建设的热潮。2012 年，我国城乡建设部正式发布了“关于开展国家智慧城市试点工作的通知”，同时印发了《国家智慧城市试点暂行管理办法》和《国家智慧城市（区、镇）试点指标体系（试行）》两个文件。至此，我国开启了智慧城市建设的篇章。随着智慧城市建设在我国的逐步展开，交通作为城市功能的重要载体也在进行从智能化到智慧化的改变。

智慧交通是将传感器技术、RFID 技术、无线通信技术、数据处理技术、网络技术、自动控制技术、视频检测识别技术、GPS、信息发布技术等运用于整个交通运输管理体系中，从而建立起实时的、准确的、高效的交通运输综合管理和控制系统。主要包括以下几个方面：先进的交通信息服务系统、先进的交通管理系统、先进的公共交通系统、先进的车辆控制系统、先进的运载工具操作辅助系统、先进的交通基础设施技术状况感知系统、货运管理系统、电子收费系统和紧急救援系统。显然，智能交通利用物联网技术、网络和设备来实现交通运输的智能化。

智慧交通是给予智能交通系统实现对交通运输体系中各种要素（包括人、车、路、环境）的全面感知、泛在互联、协同运行、高效服务和可持续发展；是集成物联网、大数据和云计算等新一代信息技术、结合人工智能、知识工程技术等市县具有一定自组织能力、判断能力和创新能力等更加高效和敏捷的交通运输系统。相比智能交通系统，智慧交通具有以下一些特征：

(1) 在提出背景方面，智慧交通是在智慧城市的大框架下提出的。

(2) 在架构方面，智慧交通是在智能交通的基础上展开的，但是不局限于智能交通系统的现有功能。

(3) 在功能应用方面，智能交通系统通过信息采集和分析，进行交通状态描述和面向出行群体的交通服务；智慧交通则试图找出隐藏在海量数据中的交通特征，挖掘有价值的信息，为交通管理者提供决策依据，实现交通管理的实时闭环控制，并通过人机交互等方式为出行者提供个性化的出行服务。

(4) 在技术基础方面，智能交通系统以计算机处理技术、互联网技术为基础展开。智慧交通则更多的使用物联网、大数据、云平台、数据挖掘等新技术、为交通系统可以更好的像人一样思考，决策。

#### 2.1.2.2 智慧交通关键技术

(1) 最短路径算法。最短路径算法是智慧交通系统中路径规划、网络分析的基础，其算法效率提升是智慧交通系统分析效率提升的关键。近年来，随着待处理的道路网络数据规模的增大，出现了一些较为成熟的加速技术可高效处理大规模道路网络数据的最短路径查询。这些方法以减少搜索空间为目标，最具代表的分别是 Reach 和 Hierarchy 两种类型。Reach 相关的 REAL 算法最具代表性，而 Hierarchy 算法最为代表的是压缩分层算法，该算法根据道路网络的拓扑特性在道路网络基础上压缩生成多层网络拓扑，进而提高查询效率。

(2) 轨迹数据挖掘。面对越来越多的轨迹数据，动辄上亿的数据量，传统的数据管理技术如关系数据库、空间数据库等都不能有效地解决轨迹数据的存储与查询问题，为了解决这类问题，产生了管理移动实体、提供移动对象的复杂查询支持为核心的移动对象数据库。移动轨迹数据就是一种典型的大数据，以北京市为例，北京市拥有机动车已经超过 500 万辆、出租车为 6.6 万辆，北京市交通信息采集平台的浮动车系统，仅一分钟的 GPS 打点间隔，每天累计的轨迹数据的轨迹点将近 1 亿，数据量多达十多 GB。将社交媒体、路况监测、城市摄像头、GPS 信息等综合起来，对多种异构数据进行管理和协同计算，通过轨迹数据的挖掘分析，从而可识别最佳驾车路径、推荐热点路径、实时动态拼车等智慧交通系统应用。

(3) 二三维一体化。地理信息系统正处在一个传统二维向二三维一体化的过渡阶段，



交通地理信息系统建设人员在发展过程中必然积累了大量二维数据，但是采用“一套二维系统外加一套三维系统”的“1+1”技术体系将使技术人员不得不放弃已有的资源而重新积累三维数据资源。为此采用二三维一体化的技术体系，最大程度保护了用户已有的数据资源，二维数据可以在三维场景中显示，三维数据也可以在二维地图中实现加载。利用其快捷的建模方式，可以快速地将二维数据转化为二维模型。国内的 GIS 平台厂商 SuperMap 基于二三维一体化技术体系，已开发出一系列产品，并已应用到交通领域的应用之中。

(4) 交通网络演化分析。随着交通网络数据规模剧增、交通路网逐渐复杂，交通网络的演化分析对智慧交通系统建设具有重要的意义。研究学者多从宏观、中观、微观尺度对交通网络进行演化和特征分析。针对不同的研究尺度，交通网络演化分析的结果不同，对于从宏观分析，道路网络具有绒泡菌特征；从中观角度分析，道路网络具备类似叶脉网络特征的网络模式；从微观角度分析，得到道路网络模式就具有血管网络特征。如何结合不同的尺度提出一种新的模型，结合社会统计数据、人口数据、土地利用数据等对现实交通网络的模拟，将是下个阶段的研究方向。

(5) 交通网络决策分析。智慧交通系统智慧的最大体现为交通网络智慧决策分析，根据动态交通情况，指导出行信息。通过监控、监测、交通流量分布优化等技术，进一步完善交警监控体系、公安系统和信息网络系统，实现交通信号灯的智慧控制，可通过“智能信号灯”设置，在地面对应的路面上设置感应线圈，其会根据车道上有无车辆反馈给信号灯，信号灯将自动选择红绿灯状态。在动态监测交通拥堵并提供疏堵方案中，交通网络决策分析需要结合道路数据库、历史道路数据（轨迹数据、历史气象数据、交通事件数据等）及其社会数据等提高交通系统的决策水平。

(6) 大数据技术。伴随城市的发展，交通设施的快速建设，机动车数量的急剧增加，交通拥堵、交通污染以及交通事故等问题亟待解决。为此，及时、准确地获取交通数据是智慧交通系统解决交通问题的前提，而该问题的解决需要依靠大数据 (BigData) 技术来解决。

### 2.1.2.3 智慧交通安全国外发展现状

据美国媒体 autoevolution 2016 年 8 月 3 日报道，Charlie Miller 和 Chris Valasek 是两位安全专家，他们曾成功入侵并控制一辆 2014 款 Jeep 自由光，导致菲亚特克莱斯勒汽车公司大规模召回汽车。这次他们发明了新的方法来侵入车辆系统。这次实验的对象还是去年用于入侵展示的 2014 款 Jeep 自由光。

这次的入侵并非通过无线进行的，而是需要进入车辆，将 OBD-II 接头连接到车辆诊断系统接口，这样就可以扰乱车辆的控制器局域网络 (CAN)。

虽然菲亚特克莱斯勒的召回使 140 万辆车免受黑客无线攻击，但这两位安全专家这次可

以在不干扰多媒体单元的情况下悄无声息地侵入汽车系统。

通过 CAN 总线向其发送大量不同指令和信号，车载电脑的安全阀就会过载，入侵者就可以完全控制转向、刹车和节气阀系统。

两位专家甚至在测试和展示时让车辆发生了碰撞，视频中显示手握方向盘的驾驶者并没有能控制转向系统，车辆被入侵者操控进行了大幅度的突然转向，最终驶进了水沟里。

两位安全专家已经向所有汽车厂商发出提示，要求他们为车辆的 OBD II 接口和 CAN 总线加装实体保护装置，这样黑客除非在车内放置控制器远程遥控，否则就无法侵入车辆。

根据美国权威汽车价值评估媒体 Kelley Blue Book 最新公布的汽车黑客攻击调查报告中指出鉴于近期被广泛讨论的 Jeep 汽车被黑事件车主已经真正开始关心车辆的网络安全问题。有 71% 的参与者表示知道 Jeep 汽车被黑事件；41% 的参与者表示在选购新汽车的时候会考量是否在近期存在被黑客攻击的新闻。

2016 年 10 月美国交通部最新颁布的汽车信息安全白皮书《现代汽车信息安全最佳实践》。美国交通部的 NHTSA 美国高速公路管理局历来需要肩负起驾驶员安全的责任，有义务来承担信息安全方面的责任。这些标准和指南旨在为车厂提供信息安全架构基础，并在此基础上各个车厂来定制自己信息安全测试流程。

然而，由于缺少规范的安全监管标准和流程，目前绝大多数厂商和供应商不能对其产品进行必要的安全性测试，结果很难按照信息安全标准实施测试。具体困难表现在业界没有成熟的信息安全测试设备把这些标准和汽车整个生产制造流程联系起来，造成车载系统，ECU 等设备在开发过程中和安全测试脱节。对于车厂，服务提供商，智能硬件厂商等而言，他们清楚地知道汽车存在被攻击的危险，但是却找不到安全产品服务商能帮助他们在产品开发过程中发现和解决安全漏洞。

#### 2.1.2.4 智慧交通安全国内发展现状

目前，工信部将“智慧交通”列为十大物联网示范工程之一。工信部提出的是“智慧”而不是“智能”，两者的本质区别在于“智慧交通”是利用现代化科技手段，实现人、车、路 and 环境的和谐协调的关系处理，使交通发展更加具有现代化的意识、更好的节约能源、减低环境污染、改善交通秩序和交通环境的全新交通发展形态，它是多个智能交通系统的集成。在国家的大力支持与推动下，国内各城市智能交通的发展速度较快。从对运输工具的监测到基础设施的信息化建设，在加大对交通违法行为检测的同时，通过信息化手段提升交通运输管理能力和服务水平，其中包括推进交通基础设施的数字化和智能化。比如随着车载导航装置的发展和手机的普及，在北京、上海、广东珠海等比较发达的城市已经出现了基于车载导航装置和手机的动态交通信息服务（如珠海的“安捷通”系统），这些发布方式必将随着城



市智能交通的发展进一步得到普及。在这个推进发展的过程中，国内智能交通发展已表现出以下几个特点：

(1) 电子警察、卡口、车辆识别系统、信号灯控制、GPS 车载导航系统、智能公共交通系统、停车场管理系统、行驶记录仪、交通收费设备、交通通信设备等产品 and 系统功能更趋完善。

(2) GPS、RFID 等一些新技术在智能交通领域得到更为广泛的应用。重庆、武汉、南京等城市，成功地将 RFID 技术应用于路桥不停车收费系统。上海世博会和深圳全运会均已使用 RFID 等新技术来解决交通管理问题。

(3) 智能交通已从简单的交通违规监测，如闯红灯、违章停车等，逐渐向为城市交通拥堵提供解决方案。

(4) 智能交通从单点检测，到线检测，再到区域检测，监测范围不断扩大，应用规模也不断增大。提升了对高速公路、国省道干线公路、城市道路的重要路段、大型桥梁、长大隧道、高风险水域、重要航段和港口等基础设施的监控。

(5) 智能交通从对交通工具的监管提升到对交通基础设施的建设，包括公路上数据信息的采集、传感器的安装、通信设施的完善以及路桥的自我检测等。

(6) 智能交通在安全管理和应急保障方面，通过重点建设路网监控、车辆监控、水上指挥、交通安全管理等系统，为应急指挥处置提供先进手段；在公众服务方面，围绕政务公开、网上办事、公众出行、客运售票，完善公众信息服务体系，进一步提升交通公共服务水平；在行政办公方面，通过开发应用各种政务信息系统，提升了行政效能。

鉴于智慧交通是多个智能交通系统的集成，我国各地在快速发展各智能交通系统的过程中，还存在以下主要问题：

(1) 认识和标准尚未同一。各地在启动智慧交通建设中，对智慧交通的内涵、边界、功能定位、技术路径、载体等尚未开展深入研究。目前很多城市的智能交通仍然是比较低层次的操作，还没有“大交通”的概念，一些相关的交通预测分析、决策服务、公共支持等仍然没有被很多城市的管理者和相关部门系统地理解，所谓的智能交通其实只是管控，多用来监测和拍摄那些违规的车辆牌照，前端探头所采集的相关数据，并没有与之对应的数据中心进行分析。同时行业标准体系缺乏，导致建设标准不统一的现象较为严重，从而使得信息资源的整合、互联共享以及系统功能的发挥等大打折扣。

(2) 关键技术有待突破。目前，智慧交通处于大规模建设阶段，如物联网技术与信息采集的融合、交通诱导、车辆身份识别、云计算与信息处理、网络信息安全等关键核心技术还有待研发和突破。传感器、网络技术和建设成本与智能交通的要求还不能互相适应；智

能交通产品和服务的用户满意度较低。

(3) 地方保护主义的存在。即在推行智慧交通建设中，各地还或多或少地存在地方保护主义的现象，即采用地方企业的产品或系统，由于不同企业的产品标准各不相同，势必会影响国家行业标准的统一，也会影响系统的运行效率和各系统间的兼容性以及提高系统运行的维护和再建设成本。

### 2.1.3 智慧水利

#### 2.1.3.1 智慧水利的定义

智慧水利是在水利信息化的基础上高度整合水利信息资源并加以开发利用，通过物联网技术、无线宽带、云计算等新兴技术与水利信息系统的结合，实现水利信息共享和智能管理，有效提升水利工程运用和管理的效率和效能。智慧水利涵盖了水文、水质、水资源、供水、排水、防汛防涝等各个方面。是通过各种信息传感设备，测量雨量、水位、水量、水质等水利要素，通过无线终端设备和互联网进行信息传递，以实现信息智能化识别、定位、跟踪、监控、计算、管理、模拟、预测和管理。

智慧水利的建设，是在物联网、无线宽带、云计算等新兴技术的支持下，充分利用现有的信息技术，协助水利管理达到“智慧”状态，使管理水利的管理、服务、决策工作更加精细、动态、智能。可以从三个维度来理解“智慧水利”。首先“智慧水利”是将物联网和互联网结合形成的水联网，从而成功的应用到水利事业当中。其次，“智慧水利”还是基础架构应用平台，应用集成平台构建了智慧水利各个业务系统的互联互通渠道，使其能够很好的融合。另外，智慧水利强调智慧应用，智慧应用实际上就是运用智能融合技术，通过数据来进行分析、计算和存储，为水利事业提供决策和咨询，使其流程得到优化。

#### 2.1.3.2 智慧水利发展现状

近年来，水利部陆续实施了一系列水利信息化建设战略，2012 年全国首个“水利部物联网技术应用示范基地”成立后，我国水利信息化建设正在以一个飞快的速度进行发展，江苏、浙江、福建、广东等地智慧水利项目纷纷上马。2013 年 10 月，广东省水利厅与广东联通签署战略合作协议，双方共建“智慧水利”无线应用平台。通过组建全省水利三防联通集群网，将水利门户、综合办公、三防决策、视频监控、会商调度、小水库监管等重点水利信息系统部署于智能手机终端上，实现水利业务信息随时随地移动查询处理和三防应急视频会商调度。

“智慧水利”项目加速发展，“智慧水利”项目加速发展，有效提高防汛抗旱、水资源优化配置、水利工程建设管理、水质监测等水利业务中信息技术应用的整体水平，带动水利现代化，更好地为社会经济发展提供保障。

虽然我国智慧水利的应用发展迅猛，但在建设和应用过程还存在许多问题。尤其是“重

硬件、轻软件”“重建设、轻应用”“重拥有，轻共享”等问题十分普遍。有不少省市为了“赶潮”，不惜重金配备高档设备搞智慧水利，但却不在平台上开发加以利用。即使有应用也是各单位之间各自为政，信息资源不能共享，形成一个个信息孤岛，对信息的综合应用几乎为零，造成非常大的浪费。而且许多项目建设后，内容服务更新跟不上，辅助决策类、统计分析类系统配备不足，专业人员培训普及跟不上，不能有效满足水利决策、应急管理的需求，使许多项目都成了摆设。

### 2.1.3.3 智慧水利关键技术

智慧水利涉及的关键技术主要集中在五个方面：一是基于水联网和 3S 技术的智能感知体系；二是高带宽的无线通信技术；三是异源异构数据集成分析技术；四基于互联网分布式计算机的云计算技术；五是具备一定的智能行为智能控制系统。概括而言，智慧水利就是使用了能自动采集信息的前端传感器，对雨量、水位、水量、水质等信息进行实时的采集，实现“实时感知”；通过先进的网络技术实现经济高效的综合信号传输；基于云计算功能，实现“智能处理”各类水务事件。

### 2.1.4 智慧管网

现代城市的地下铺设有各种不同的管道，包括自来水管、污水管、天然气管、石油管、各类通信电缆的管道等。这些管道因为具有网络形态而称之为管道网络，简称管网。管道可能由于各种原因出现故障，这是需要及时维修，例如石油管道和天然气管道出现问题时，及时维修就显得非常迫切。但是，在许多情况下，如何确定事故点是第一个遇到的问题。物联网技术应用于管网的管控，形成智慧管网系统，可以及时发现问题，精准定位故障点，预知事故性质，便于有效及时地对故障进行修复。

#### 2.1.4.1 智慧管网的定义

简单地说，智慧管网就是使用物联网技术，通过传感器等探测手段，能对管道网络的状态进行实施监督的一种系统。

传感器是人们对管网基础设施进行有效感知和探测的手段，把管网基础设施中的传感器组成网络，使大量的传感器等微型化计算设备自组织地连接在一起，并将普适计算模式从满足个人需要，进一步延伸到可以大规模推广的管网基础设施等生产和应用领域。可将信息基础设施推广到管网基础设施中形成管网基础设施的网络化、信息化，实现管网基础设施与信息基础设施的整合统一。

近年来中国各大城市相继出现了大规模的城市内涝问题，问题主要出现在城市管网建设的规划方面以及管网监控管理方面严重滞后。随着国家提出“智慧城市”发展战略，国务院也提出“5 年解决雨污分流、10 年解决城市内涝”的要求，同时提出完善应急机制、加强

管网日常管理、加大科技支撑力度，进一步加强城市降雨规律、排水影响评价、暴雨内涝风险等方面的研究；全面提升排水防涝数字化水平，积极应用地理信息、全球定位、遥感应用等技术系统。因此，市场呼唤出现一种方便监控和管理的智慧管网应用系统。

在过往的城市基础设施建设中，管网基础设施和信息基础设施的建设往往是分开进行的。一方面人们不断地建设和完善城市管网基础设施，另一方面，人们也在不遗余力地发展包含数据中心、个人计算机、宽带网络等的信息基础设施，但是两者之间往往互不相干。

随着现代经济的发展，主要依赖桌面型计算的主流网络计算模式，被倡导发展成更广泛地部署移动智能设备和微小计算设备的普适计算模式。从崇尚人围绕着计算机终端获取服务与支持，发展成计算机网络围绕着人主动提供服务与支持。

传感器是人们对管网基础设施进行有效感知和探测的手段，把管网基础设施中的传感器组成网络，使大量的传感器等微型化计算设备自组织地连接在一起，并将普适计算模式从满足个人需要，进一步延伸到可以大规模推广的管网基础设施等生产和应用领域。可将信息基础设施推广到管网基础设施中形成管网基础设施的网络化、信息化，实现管网基础设施与信息基础设施的整合统一。

#### 2.1.4.2 智慧管网发展现状

随着城市的快速发展，地下管线建设规模不足和管理水平不高等问题日益凸显，大雨内涝、管线泄漏爆炸、路面塌陷等事件屡见不鲜，使城市运行体系也频受重创，对人们的生活和生命财产安全也带来严重影响。此类地下管线问题已受到社会各界的持续关注，因此国家通过一系列的指导意见来规范和促进地下管线市场的健康发展。同时，随着技术水平的不断提高，使地下管线在铺设、运维、管理分析方面均取得明显改善。在智慧城市建设的大潮中，地上地下都是建设的范畴，这都为我国地下管线市场迎来蓬勃发展的机遇。国家对于地下管线的建设与管理方面提供了一些特许政策和投资支持，在为相关企业缓解经济压力的同时必然带动企业效率与业绩的提高，为所处行业带来推动作用，促进市场繁荣。并且国家鼓励在地下管线规划建设、运行维护及应急防灾等工作中广泛应用精确测控、示踪标识、无损探测与修复、非开挖、物联网监测和隐患事故预警等先进技术。相信国家的高度支持能促进我国开启庞大的地下管网市场发展，在规划建设、普查及信息化等领域为从事各类管线制造、铺设、勘测、管理分析的企业带来更多市场机遇。同时促使更多行业的管理者从中看到地下管线良好的市场前景，为其提供切入地下管网市场的机会。

据中国产业调研网发布的 2015 年版中国城市管网建设行业深度调研及市场前景分析报告显示，当前，各城市对于地下管线的建设已全面开展。其中广东珠海横琴综合管沟建设长度为迄今全国之最。其庞大的地下管沟系统全长约 32 公里，共同管沟净高 3.5 米、净宽 8.1 米，可将给水管、中水管、城市电力电缆、供热管、垃圾真空管一一收纳其中。而江苏也全



力打造“地下智慧南京”，设计方案覆盖了南京主城区，涉及电力、信息与通信、给水、排水、燃气、热力、工业、综合管沟等各类地下管线（沟），包括驻宁部队管线和过境的西气东输、川气东送等地下管线。预计到 2020 年我国城市管网市场规模将达到 6.7 万亿。

#### 2.1.4.3 智慧管网关键技术

智慧管网关键技术包括门户集成技术、Web 服务技术、数据仓库技术、数据采集和传感器技术、网络通讯技术以及软件智能技术。

(1) 门户集成技术：门户技术是建立管网门户平台，实现管网信息共享与集成应用的核心技术，建议采用 SOA 构架（图 2-1），通过网络对松散耦合的粗粒度或细颗粒的 SOA 应用服务组件进行分布式部署、组合和调度。SOA 组件（服务）之间通过简单、精确定义的接口进行通讯，不涉及底层编程接口和通讯模型，便于服务组件的挂接与卸载。

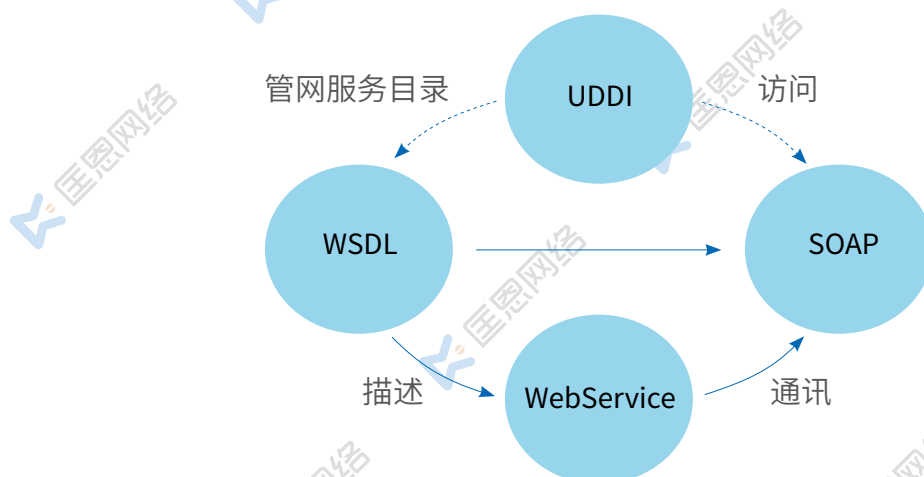


图 2-1 管网门户 SOA 的核心组件

(2) Web 服务技术：Web Service 是构建运行于门户平台中各种业务组件服务的主流技术，是一种新的 Web 应用程序分支，它向外界暴露能够通过 Web 进行调用的 API，是自包含、自描述、模块化的应用，可以在网络中被描述、发布、查找及调用。

(3) 数据仓库技术：针对管网信息的复杂性、海量性、不确定性、动态性以及多源、多精度、多时相、多尺度的特点，为统一管理和共享管网资源，使用数据仓库技术，建立面向主题的、集成的、不可更新的、随时间不断变化的管网数据集合，丰富管网数据模型、业务模型、分析模型，实现管网数据挖掘、支持管网智能分析与高级应用。

(4) 数据采集和传感器技术：主要指支持自动化和智能化的数据采集和通用适配器技术。包括感知、通信、自愈、抗干扰、误差补偿、分辨识别、信息融合和自控等传感器技术。智能传感器支持软件自动更新，保证传感器拥有最新的知识技能。通用适配器技术支持多种工业标准智能传感器的物联网接入。

(5) 网络通讯技术：网络承载各种管网信息和控制指令的高效、稳定和安全传输。网络分为有线网络和无线网络，涉及的主要技术有光传输技术、卫星通信技术、无线通信和移动电话、宽频数字技术、因特网技术。影响网络通讯质量的主要指标是带宽、传输距离、抗噪性和稳定性。

(6) 软件智能技术：计算机软件技术已从面向对象发展为面向服务，并正从面向服务向智能模型方向发展。软件智能体（software agent）是驻留在复杂动态环境中的计算机系统，它们自觉地感知环境并作用于环境，从而实现设定的目标或任务。城市管网智能体在管网分布式网络计算环境中感知并作用于管网环境，实现管网数据的智能获取、处理、存储、搜索、表现以及多重准则决策支持（Multiple Criteria Decision Making, MCDM）。管网智能体应具备利用空间知识进行推理和可进化两种基本能力。

## 2.1.5 智慧农业

### 2.1.5.1 智慧农业定义

为了发展现代农业和提高农业发展效益，解决现有农业生产中存在的各种供求矛盾，2014 年我国提出了“智慧农业”这一新概念。智慧农业是智能农业专家系统的简称，一般是指利用物联网技术、云计算技术和大数据等信息化技术实现“三农”产业的数字化、智能化、低碳化、生态化、集约化，从空间组织、管理整合现有农业基础设施、通信设备和信息化设施，使农业和谐发展实现“高效、聪明、智慧、精细”和可持续生态发展，是将科学技术融合在农业发展领域中的具体实践和应用。智慧农业是利用现代计算机技术和互联网手段与平台，通过专家经验和专家系统的指导，定量数字化模拟、加工与决策，使得农作物生长与产供销全过程智能化、数字化和信息化，实现农业信息采集、加工、处理和评价分析现代化、科学化和智能化的目标，是我国农业未来发展方向，是实现农业现代化重要举措之一。

智慧农业的主要目标是利用建成融数据采集、数字传输网络、数据分析处理、数控农业机械为一体的数字驱动的农业生产管理体系，在农业生产过程中对作物、土壤实施从宏观到微观的实时监测，以实现对农作物生长、发育状况、病虫害、水肥状况以及相应环境的定期信息获取，生成动态空间信息系统，对农业生产中的现象、过程进行模拟，达到合理利用资源、降低生产成本、改善生态环境、提高农作物产量和质量的目的。

从技术层面上讲，智慧农业是一门综合性的学科，涉及到土壤学、作物学、气象学和信息技术等科学领域，即可通过遥感技术、地理信息系统、全球定位系统、专家系统和农业模拟优化决策系统来实现其目标。

### 2.1.5.2 智慧农业发展现状

我国政府部门高度重视现代农业的发展，先后出台了《农业科技发展“十三五”规划》、《关



于加快推进农业科技创新持续增强农产品供给保障能力的若干意见》、《全国农垦农产品质量追溯体系建设发展规划（2011-2015）》等政策文件，全力支持“十三五”期间我国农业的发展。最新发布的《全国农业农村信息化发展“十三五”规划》指出，物联网等技术有望在农业部确定的 200 多个国家级现代农业示范区获得农业部和财政部资金补贴，并先行先试重点开展 3G、4G、物联网、传感网、机器人等现代信息技术在该区域的先行先试，推进资源管理、农情监测预警、农机调度及无人机监测等信息化的试验示范工作，完善运营机制与模式。按照“十三五”规划要求，今后 5 年，农业农村信息化总体水平将从现在的 35% 提高到 50% 基本完成农业农村信息化从起步阶段向快速推进阶段的过渡。具体指标包括：农业生产信息化整体水平翻两番，达到 12%；农业经营信息化整体水平翻两番，达到 24%；农业管理信息化整体水平达到 60；农业服务信息化整体水平达到 50% 以上等。

随着物联网技术的不断发展，越来越多的技术应用到农业生产中。目前，RFID 电子标签、远程监控系统、无线传感器监测、二维码等技术日趋成熟，并逐步应用到了智慧农业建设中，提高了农业生产的管理效率，提升了农产品的附加值，加快了我国智慧农业的建设步伐。运用智慧农业思想开发出来的计算机温室监测系统和生产技术，也被广泛应用到生产实际中。通过无线传感器，网络系统的构建，对作物的生长环境信息、生长状况进行实时的监测。随着物联网技术的蓬勃发展，农业生产的过程将会变得更加快捷、有效。

### 2.1.5.3 智慧农业关键技术

目前，发达国家采用高度自动化机械化精确生产的智慧农业生产模式，可以逐步脱离人的操纵，由系统自动操控，实现农业的产业化和信息决策自动化等。利用智慧农业技术，使得生产者可以远程监控各个田地的状况，从而减少多余劳动力的消耗和了解农产品生产安全性和质量好坏。

智慧农业是主要依靠“5S”技术[分别是遥感系统（RS）、全球定位系统（GPS）、地理信息系统（GIS）、专家系统（ES）、智慧化决策知识系统（IDSS）]、云计算技术、大数据技术及其他电子和信息技术，并与农业生产全过程结合的新发展体系和发展模式。这实际就是物联网技术在农业中的应用。智慧农业体系是运用“5S”技术快速进行土壤分析、作物长势监测，结合当时的气候、土壤情况进行分析，进而系统做出正确的决策，例如何时灌溉、灌溉多少，何时灭虫、施肥，何时收获，将农业生产活动、生产管理相结合，创造新型农业生产方式和经营出售新模式。

“5S”技术体系中，RS 技术模块遥感数据模块通过解译遥感数据源获取田地面积及其类型分布，进行实时监测，并以遥感反演参数作为数据输入源；GIS 模块在地理信息系统中整合遥感和气象数据，集成数据存储分析功能，利用地理信息系统建立农田、田地生态系统碳储量数据库，实现数据源的空间转换，并整合各类参数构建反演模型；GPS 模块将系统与

GPS 导航仪结合,得到农田、田地作物分布和生长情况绘制成图,根据这些信息制定相关的措施与决策;ES 模块智慧农业专家系统能够根据农田、田地作物分布特征,划分农作物产量贫瘠区与丰富区,得到农作物产量的等量图,为政府决策提供依据和支持;IDSS 模块智能化决策知识系统支持决策人员解决处于管理系统不同状态的某一领域中的决策问题。“5S”技术体系具有良好的人机接口,以便科学地使 IDSS 与决策管理人员对话,充分发挥决策者的知识、经验和判断能力的作用。

### 2.1.6 智慧城市

智慧城市不是一个产业,也不是一个行业,而是一个适合多种物联网行业发展的综合平台。智慧城市建设的目标是实现跨行业、跨领域的综合服务平台,通过多种行业数据和服务的智能交互,实现城市的有效综合治理,提高城市管理水平。

#### 2.1.6.1 智慧城市定义

智慧城市就是运用信息和通信技术手段感测、分析、整合城市运行核心系统的各项关键信息,从而对包括民生、环保、公共安全、城市服务、工商业活动在内的各种需求做出智能响应。其实质是利用先进的信息技术,实现城市智慧式管理和运行,进而为城市中的人创造更美好的生活,促进城市的和谐、可持续成长。

智慧城市是以互联网、物联网、电信网、广电网、无线宽带网等网络组合为基础,以智慧技术高度集成、智慧产业高端发展、智慧服务高效便民为主要特征的城市发展新模式。智慧化是继工业化、电气化、信息化之后,世界科技革命又一次新的突破。利用智慧技术,建设智慧城市,是当今世界城市发展的趋势和特征。

“智慧城市”的理念就是把城市本身看成一个生态系统,城市中的市民、交通、能源、商业、通信、水资源构成了一个个的子系统。这些子系统形成一个普遍联系、相互促进、彼此影响的整体。在过去的城市发展过程中,由于科技力量的不足,这些子系统之间的关系无法为城市发展提供整合的信息支持。而在未来,借助新一代的物联网、云计算、决策分析优化等信息技术,通过感知化、物联化、智能化的方式,可以将城市中的物理基础设施、信息基础设施、社会基础设施和商业基础设施连接起来,成为新一代的智慧化基础设施,使城市中各领域、各子系统之间的关系显现出来,就好像给城市装上网络神经系统,使之成为可以指挥决策、实时反应、协调运作的“系统之系统”。智慧的城市意味着在城市不同部门和系统之间实现信息共享和协同作业,更合理的利用资源、做出最好的城市发展和管理决策、及时预测和应对突发事件和灾害。

#### 2.1.6.2 智慧城市发展现状

目前,很多国家已经开始智慧的建设,主要集中分布在美国、欧洲的瑞典、爱尔兰、德国、

法国,以及亚洲的中国、新加坡、日本、韩国,大部分国家的智慧城市建设都处于有限规模、小范围探索阶段。韩国作为全球第四大电子产品制造国,物联网国际标准制定主导国之一,通过智慧城市建设培育新产业。美国将智慧城市建设上升到国家战略的高度,并在基础设施、智能电网等方面进行重点投资与建设。新加坡被公认为政府服务最好的国家,信息通信技术促进经济增长与社会进步方面都处于世界领先地位,智慧城市建设注重服务公众。

改革开放以来,我国城镇化发展迅速,据国家统计局统计,我国的城镇化率从2005年的42.99%上升至2015年的56.1%。据预测,到2030年中国城镇化率将达到65%左右,这意味着每年还将有1000多万人口进入城市。我国在城镇化过程中积累了一系列“城市病”,城市发展与人口、环境、资源的矛盾不断突出。如何解决城市发展的突出矛盾,实现有限资源的合理分配,并不断深化城市功能以提高利用效率成为城市管理者面临的重大难题,而城市信息化建设无疑是提升城市管理效率的重要方式。智慧城市是城市信息化的高级阶段,是信息化与城镇化结合的最佳模式,将充分发挥产业辐射作用,带动整个经济的转型。

我国智慧城市建设经历了两个阶段的发展:萌芽期和推进期。2010年是我国智慧城市建设的重要节点,在此之前我国智慧城市建设处于萌芽阶段。继2010年宁波市在政府的全面推动下实施智慧城市建设以来,其他城市纷纷效仿,智慧城市在我国的建设风生水起,不少城市提出了具体的建设目标和行动方案,甚至有些地区把智慧城市建设列入了“十二五”规划,如北京、上海、广州、天津、深圳、武汉、株洲、佛山等。截止2016年初,全国已经有597个智慧城市相关试点。

当前,我国正在通过“两化融合”、“五化并举”、“三网融合”等战略部署,积极利用物联网、云计算等最新技术,推进智慧城市建设。国内在建设智慧城市过程中,有些城市围绕创新推进智慧城市建设,提出了“智慧深圳”、“智慧南京”、“智慧佛山”等;而更多的城市则是围绕各自城市发展的战略需要,选择相应的突破重点,提出了“数字南昌”、“健康重庆”、“生态沈阳”等,从而实现智慧城市建设。

与发达国家相比,我国智慧城市建设在总体上尚处于起步时期和探索阶段,没有形成适合自身城市发展的机制体系和运营模式。我国有很大一部分城市的生产力水平和政府治理程度存在很大差距和差异,并且在相当长一段时期内将持续存在。因此,我国当前还不具备大规模开展智慧城市建设综合条件,只能支持先在具备基本条件的城市开展先行先试,示范带动,逐步扩散。

#### 2.1.6.3 智慧城市关键技术

(1) 物联网技术。物联网是通过互联网把植入城市物体的智能化传感器连接起来,形成物联网,实现对物体城市的全面感知,利用云计算等技术对感知信息进行智能处理和分析,实现网上“数字城市”与物联网的融合,并发出指令,对包括政务、民生、环境、公共安全、



城市服务、工商活动等在内的各种需求，作出智能化响应和智能化决策支持，使城市变为真正拥有智慧的城市。

(2) 3S (RS, GIS, GPS) 技术。3S 技术是遥感技术 (Remote Sensing, 简称 RS)、地理信息系统 (Geography Information System, 简称 GIS) 和全球定位系统 (Global Positioning System, 简称 GPS) 的统称，是空间技术、传感器技术、卫星定位与导航技术和计算机技术、通讯技术的结合，对多学科高度集成的空间信息进行采集、处理、管理、分析、表达、传播和应用的现代信息技术。

(3) 云计算技术。云计算技术是指基于互联网的超级计算机模式，即把存储于个人电脑、移动电话和其他设备上的大量信息和处理器资源集中在一起协调工作。在极大规模上可扩展信息技术的能力，并向外部客户作为服务来提供的一种计算方式。

(4) 宽带无线通信技术。宽带无线通信技术是利用电磁波信号在自由空间中传播进行信息交换的一种通信方式。目前使用较广泛的宽带无线通信技术包括无线局域网 802.11 (Wi-Fi)、3G 通信技术和 4G 通信技术。

(5) 虚拟现实技术。虚拟现实 (Virtual Reality, 简称 VR) 是利用电脑模拟产生一个三维空间的虚拟世界，提供使用者关于视觉、听觉、触觉等感官的模拟，让使用者如同身临其境一般，可以及时、没有限制地观察三度空间内的事物，它为实施智慧城市战略提供了三维描述方法和人机交互的虚拟城市环境，具有多维动态可视化和实时交互式操作的效果。

(6) 异源异构数据集成技术。异源异构数据集成技术存在于各自独立的信息系统中，由于软硬件平台及数据模型的不同，导致存取方式、结构和精确度都不同的数据，包括以关系表为代表的结构化数据、以 XML 为代表的半结构化数据和以文本文件为代表的无结构化数据。异构数据的集成是为了更好地利用分布在各处的数据资源，实现不同数据资源的合并和共享。可以通过网络建立跨部门、跨系统的数据交换平台，满足各信息管理系统之间的数据交换需要，为用户提供全方位的信息服务，并为管理者提供辅助决策的信息支持。

(7) 绿色节能技术。绿色的城市意味着污染全部控制、资源高效利用、人与自然和谐相处。绿色节能技术是指加强用能管理，采取技术上可行、经济上合理以及环境和社会可以承受的措施，从能源生产到消费的各个环节，降低消耗、减少损失和污染物排放，有效、合理地利用能源。如在建筑物中高度集成光伏建筑一体化、风力发电一体化等清洁能源技术和智能照明、空调群控等智能化管理技术，不仅能达到绿色节能的目的，还可对建筑物的温度和光线环境进行调控。通过步行交通、慢行系统、新能源汽车、纯电动公交和轨道交通组成的绿色交通运输体系，实现城市环境多元化及城市交通可持续发展的目的。通过这些措施以保持经济社会发展与资源环境承载能力相适应，创造人与自然和谐相处的环境。

(8) 移动互联网技术。移动互联网是一个全国性、以宽带 IP 为技术核心的,可同时提供话音、传真、数据、图像、多媒体等高品质电信服务的新一代开放的电信基础网络。它将移动通信和互联网二者结合起来,继承了移动随时随地随身和互联网分享、开放、互动的特点,逐渐渗透到人们生活、工作的各个领域。短信、铃图下载、移动音乐、手机游戏、视频应用、手机支付、位置服务等丰富多彩的移动互联网应用迅猛发展,正在深刻改变信息时代的社会生活。同时在互联网络基础设施完善以及 3G、移动寻址等技术成熟的推动下,移动互联网也将迎来发展高潮。

(9) 低碳减排技术。低碳减排技术是指以技术手段为契机减少污染物的排放,提高污染物的控制效率,发展新型高效节能、先进环保、资源循环利用激射装备以及减排环保服务业和再制造产业等领域。实现污染物减排,建设资源节约型、环境友好型社会,确保环境的安全。重点技术包括脱硫脱硝、污水处理、垃圾发电、可再生资源回收利用等。

(10) 智能控制技术。智能控制理论是控制理论发展的新阶段,主要用来解决那些用传统方法难以解决的复杂系统的控制问题。常用的智能技术包括模糊逻辑控制、神经网络控制、专家系统、学习控制、分层递阶控制、遗传算法等。以智能控制为核心的智能控制系统具备一定的智能行为,如:自学习、自适应、自组织等。

## 2.2 物联网安全典型事件分析

每年都有多起网络安全事件发生,而且在近年来呈上升趋势。随着物联网应用的落地,特别是工业物联网所涉及的工业系统和基础设施,物联网系统已经成为黑客攻击的重要目标。

2016 年发生的最具有代表性的物联网攻击事件,应该是前不久发生在美国的大规模分布式拒绝服务攻击 (DDoS) 事件了。我们将对此事件作详细分析。除此之外,2016 年发生的几个典型物联网安全事件如下:

### 【乌克兰最大机场遭网络攻击】

2016 年 1 月 20 日消息,在乌克兰首都基辅 (乌克兰共和国首都) 主要机场的电脑网络中,已经确认发现了恶意软件。

路透社的一份公开报告指出,位于基辅附近的鲍里斯波尔国际机场的电脑网络已经感染了恶意软件。根据报告中的内容,该电脑网络中存在一些敏感内容,包括机场的交通控制系统。

军方发言人声明中提到,恶意软件的命令与控制 (C&C) 服务器位于俄罗斯。因为该国最近频遭网络攻击,暂时还不能妄下结论,还不能够确定命令与控制服务器背后的控制者。

### 【以色列电力供应系统受历史最大规模网络攻击】

2016 年 1 月 26 日，以色列能源与水利基础设施部部长 Yuval Steinitz 已经披露称，该国电力供应系统受到重大网络攻击侵袭，且已经有多份报告表明勒索软件正是造成事故的直接原因。在 CyberTech 2016 大会上，Steinitz 谈到以色列的网络安全现状时指出“昨天（2016 年 1 月 25 日）我们确认了有史以来出现过的规模最大的网络攻击。”相关计算机设备已经关闭了两天，并于 1 月 26 号重新上线。

### 【德国核电站负责燃料装卸系统遭攻击】

2016 年 4 月，国外媒体报道称，4 月 24 日，正值切尔诺贝利核电站事故发生 30 周年之际，德国 Gundremmingen 核电站的计算机系统，在常规安全检测中发现了恶意程序。核电站的运营商 RWE 为防不测，关闭了发电厂，虽然仍然对外表示，并没有发生什么严重的问题。Gundremmingen 核电站官方发布的新闻稿称，此恶意程序是在核电站负责燃料装卸系统的 Block B IT 网络中发现的。

据说该恶意程序仅感染了计算机的 IT 系统，而没有涉及到与核燃料交互的 ICS/SCADA 设备。核电站表示，此设施的角色是装载和卸下核电站 Block B 的核燃料，随后将旧燃料转至存储池。

核电站还说，该 IT 系统并未连接至互联网，所以应该是有人通过 USB 驱动设备意外将恶意程序带进来的，可能是从家中，或者核电站内的计算机中。他们并没有公布该恶意程序的名字，只是说并不严重，并将整个事故分级为“N”（表示 Normal）。

当前，这家核电站正在进行全套的安全常规流程，员工检测全部的计算机系统，在核电站上线之前，进行各种常规检查。这家核电站是德国最老的核电站之一，预计 2021 年全面关闭，已经有 750 人联合在周末的时候抗议表示希望说服当局，能够在其寿终正寝之前就关闭剩余的两个反应堆。

卡巴斯基实验室创始人兼 CEO 的 Eugene Kaspersky 表示：“操作员和管理人员需要理解，这是一个每天有超过 31 万种新恶意程序出现的时代，其中有一些可能出乎我们的意料，能够破坏系统。对于这样的情况，尤其是那些有目的的直接攻击，我们都需要有所防范。”

### 【乌克兰再次因黑客攻击电力中断】

2016 年 12 月 17 日晚上，乌克兰国家能源公司遭受断电事故，受影响的区域包括乌克兰首都北部及周边地区。电网公司在断电后通过手工操作，大概在半小时左右恢复供电，并在 75 分钟后将供电系统恢复到正常状态。乌克兰能源公司主任说有迹象表明本次断电事故是外部入侵数据网络导致自动控制系统失效造成的。去年乌克兰电网就曾遭受很严重的网络



入侵导致断电事故，除此之外还成功拦截了多次猛烈攻击。

## 2.2.1 物联网攻击导致 DDoS 攻击事件

### 2.2.1.1 事件概述

2016 年 10 月 21 日，美国遭遇史上最严重分布式拒绝服务（DDoS）攻击，美国东海岸出现了大面积断网事件，造成包括 Twitter、Spotify、Netflix、Github、Airbnb、Visa、CNN、华尔街日报等上百家网站都无法访问。此次“断网”事件是由于美国最主要 DNS 服务商 Dyn 遭遇了大规模 DDoS 攻击所致。

调查分析认为，这是一次以物联网设备为主的 DDoS 攻击，攻击者来自超过一千万个 IP 来源，这些攻击来源被一种称为 Mirai 的病毒控制，成为发起攻击的“僵尸节点”。这些节点中大部分为路由器、DVR 或者 WebIP 摄像机、Linux 服务器以及运行有 Busybox 的物联网设备。当 Mirai 病毒扫描到一个物联网设备（比如网络摄像头、智能开关等）后就尝试使用默认密码进行登陆（一般为 admin/admin，Mirai 病毒自带 60 个通用密码），一旦登陆成功，这台物联网设备就成为被黑客操控用于攻击其他网络设备的工具。

据报道，一共有超过百万台物联网设备参与了此次 DDoS 攻击。其中，这些设备中有大量的 DVR（数字录像机，一般用来记录监控录像，用户可联网查看）和网络摄像头（通过 Wifi 来联网，用户可以使用 App 进行实时查看的摄像头）。安全研究公司 Flashpoint 调查部门负责人埃里森·尼克松（Allison Nixon）表示，这些涉事组件大多由一家名为 XiongMai Technologies 的中国公司生产，它们通常被用在其他品牌的设备上，包括出厂设置的硬编码设备上。而据安全公司的数据显示，参与本次 DDoS 攻击的设备中，主要来自于中国雄迈科技生产的设备。这家公司生产的摄像模组被许多网络摄像头、DVR 解决方案厂家采用，在美国大量销售。

Flashpoint 安全公司的专家说，“如果说用户可以轻松改密码就好了，但是模组中的密码被写入到了固件中，还没有工具可以修改这个模组的密码。更可怕的是，用户根本不知道还有这么一个密码的存在。”跟雄迈科技相似的公司还有很多，他们也开发摄像模组，也研发 DVR 解决方案。遗憾的是，相当一部分设备缺乏必要的安全保护举措，其中可能使用了硬编码密码等不安全机制，但制造商无法以远程方式向其推送更新补丁。

存在后门漏洞的物联网设备不仅仅来自中国的公司。SEC 信息安全咨询公司发现索尼摄像头也存在后门漏洞，摄像头的固件中存在一种硬编码的登录方式，可用来劫持设备并植入类似于 Mirai 的恶意软件。这些存在漏洞的摄像头均为 Sony Professional Ipela Engine IP 监控摄像头。该漏洞影响 80 款不同型号的索尼摄像头。索尼公司通过 SEC 信息安全咨询公司得知了该后门的详情，并已经针对受影响的型号发布了更新的固件。但是，更新固件只保

证那些尚未被 Mirai 病毒感染的设备不再被同样病毒感染，那些已经被感染的设备是否能清楚病毒尚不清楚，而且对抗升级版的病毒或其他病毒的能力，仍是一个未知数。

某个自称为 New World Hackers 的黑客组织宣称对此次攻击事件负责。他们指出，攻击只是对自身能力的测试，同时亦是一种消除安全漏洞并强制实施变革举措的推动性手段。但要找到证据证明谁是攻击者，目前还没这个能力，因为很难寻找攻击者留下的痕迹。

继美国的 DDoS 攻击之后，新加坡电信运营商星和（StarHub）遭受 DDoS 网络攻击，造成其部分家庭宽带用户在 10 月 22 日和 24 日断网。据星和介绍，他们遭受的两波攻击来自该公司自己用户的设备，因为这些设备遭到了病毒感染，成为了所谓的“僵尸节点”，被操控实施攻击。星和首席技术官 Mock Pak Lum 称，被感染的设备包括宽带路由器和网络摄像头。据有关研究人员进一步分析表明，设备种类还有火灾报警器、大楼控制系统、一些联网的家用电器、太阳能发电系统等 500 种以上。

这些事件说明针对物联网的攻击已经成为可能，物联网安全问题不是离我们很遥远，而是就在我们身边。

11 月 15 日，美国国土安全部专门制定了《保障物联网安全战略原则》，并表示，“物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉”。该战略原则指出，未在最初设计阶段构建安全并采取基本安全措施“可能会造成制造商的经济成本、声誉成本或产品召回成本损失。虽然还没有建立解决物联网问题的判例法体系，但传统的产品责任侵权原则可以适用。”

#### 2.2.1.2 关于 Mirai 病毒的分析

Mirai 是一种物联网僵尸网络病毒，在 9 月份参与发起了针对 KrebsOnSecurity 安全站点的大规模分布式 DDoS 攻击，新一类僵尸网络从各种容易被感染的物联网设备中发起攻击，流量巨大防不胜防。

Mirai 可以高效扫描物联网系统设备，感染采用出厂密码设置或弱密码加密的脆弱物联网设备，被病毒感染后，设备成为僵尸网络机器人后在黑客命令下发动高强度僵尸网络攻击。根据 KrebsOnSecurity 在 9 月份被攻击期间的记录，共计 620 Gbps 的 DDoS 巨大流量。

事实上，在 KrebsOnSecurity 被攻击之后不久，黑客论坛 Hackforums 就公布了这一名为 Mirai 的物联网僵尸网络病毒源代码。网名为 Anna-senpai 的黑客在论坛公布了源代码，称此次攻击发动是为了引起信息安全业界的注意，发布的源代码希望能够帮助安全业界提高。但是，攻击代码的公布并没有给物联网设备的安全防护带来实质性的改进，原因是许多物联网设备使用了出厂默认用户名和口令，而且一些弱口令被大量使用，有些登录口令甚至是固定的，不能动态修改，即使被检测到成为网络攻击的“僵尸”节点，也束手无策，除非更换

设备。但在更换设备前仍然是网络攻击的“僵尸”节点。

真正的威胁不是来自 Mirai 病毒本身，而是 Mirai 病毒提供的感染嵌入式设备的平台。因为嵌入式设备一般不进行安全检查，即使发现这些嵌入式设备遭受入侵，也可能束手无策。

这一情况也说明，一些物联网设备的安全意识较低，不认为攻击者会猜测到出厂默认用户名和口令，也没意识到攻击者入侵设备后会有哪些用途。这次美国“断网”事件没有涉及到攻击者的商业企图，但却给美国相关企业造成巨大经济损失。升级版的 Mirai 已经入侵了大量其他设备，包括数百万的路由器，随时可能带来再次的 DDoS 攻击。

### 2.2.1.3 匡恩网络对物联网设备漏洞的检查

我们分析发现，本次攻击事件利用了安防设备的弱口令漏洞。以雄迈的 NetSurveillance 和 CMS 系列为例，所有的 DVR / NVR CMS 固件，都开放了 telnet 服务且不能被禁用。固件内置的登录账号“root”有一个不可变的硬编码密码 xc3511。Mirai 病毒利用这个弱口令远程控制雄迈的安防设备。除了硬编码问题，雄迈许多产品的固件还有越权访问漏洞。因为没有对 DVR.htm 页面进行校验，攻击者可以绕过登录界面，直接访问 DVR.htm，导致视频信息泄漏。Mirai 病毒变种利用这个绕过漏洞远程控制雄迈的安防设备。

除了以上雄迈摄像头存在以上安全漏洞之外，我们发现，国内尚有大量安防监控设备存在类似问题。匡恩威胁态势感知平台在针对某市安防设备的安全检查过程中，扫描发现了 351 个摄像头暴露在公网，其中 96 个摄像头有漏洞，大概占比 28%。其中国内某较大品牌厂商的设备有漏洞 86 个，另一家常见品牌的设备也有 10 个漏洞。

存在问题的摄像头绝大部分都有默认口令，其中弱口令漏洞占比为 91.6%。例如某品牌摄像头的默认管理密码为 (admin/admin)。

经探测发现，虽然在公网环境中部分限制了对 80 端口的访问，但是可以通过配套的摄像机终端软件，通过 37777 端口访问摄像机内容，可以接入硬盘录像机批量控制多个摄像头，控制摄像角度等。

除弱口令漏洞外，我们还发现另一家摄像头厂商的漏洞集中在 onvif 协议身份认证缺失和弱口令，这些漏洞都能让黑客直接登录或绕开口令直接查看视频图像，这会对社会生活造成很大的安全隐患。

北京匡恩网络科技有限责任公司在得到授权后，对部分安防设备进行了深入测试，下面是几个所获得的控制实例：



- 某工厂：



图 2-2 某工厂视频远程渗透测试所获视频截图

- 某珠宝店：



图 2-3 某珠宝店视频远程渗透测试所获视频截图

- 某制造厂：



图 2-4 某制造厂视频远程渗透测试所获视频截图

安防监控产品本身作为维护国家公共安全的重要工具，遍布国家重要机构和群众生活的各个领域，里面存储的信息包含了从国家安全机密到普通百姓日常生活隐私的各个方面。一旦信息泄露，造成的损失和未来潜在的威胁难以估量。目前发现的安全隐患主要是由于设备生产厂商出厂预置的登陆口令在用户使用过程中未强制要求修改、使用者自身安全意识薄弱导致。

为了统计安防监控设备的漏洞分布情况，我们收录了各大漏洞库平台（涵盖了 CVE、CNVD 和 CNNVD 等漏洞库）中的 61 个安防监控设备漏洞，覆盖了超过 33 个厂商的网络摄像头和 DVR 设备。



设备厂商分布如下：

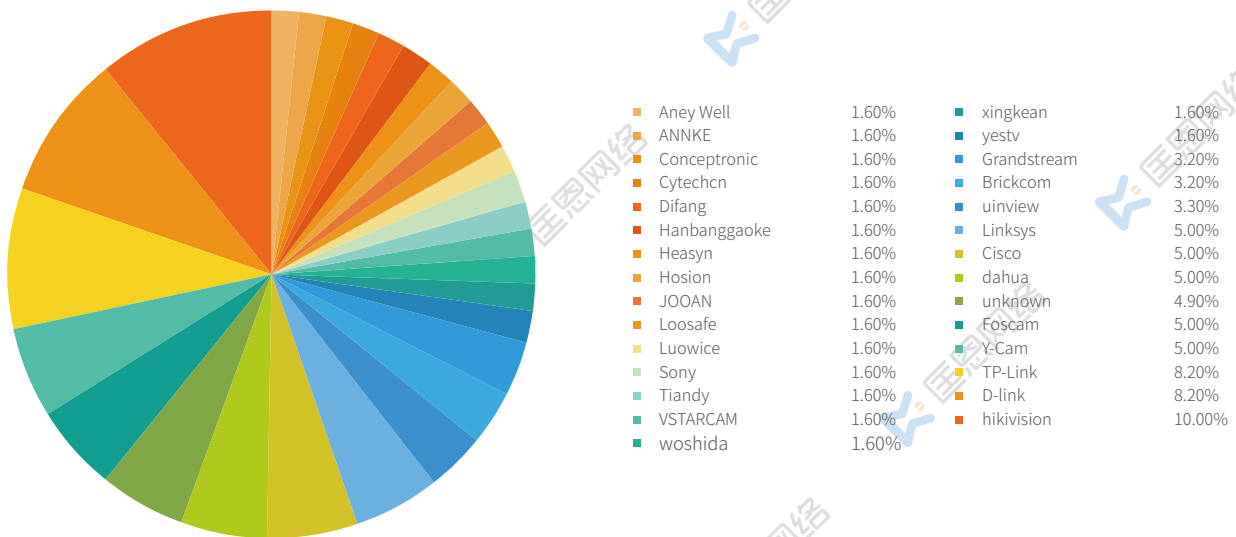


图 2-5 设备厂商分布图

从图2-5我们发现安防监控设备的漏洞主要集中于海康威视、大华、宇视、TP-Link、D-link、Airlive、Cisco 等知名厂商。上述厂商的安防监控设备在市场覆盖率方面较高，是安全研究人员的主要研究对象，不排除其他小厂商的设备有更多的安全隐患。

漏洞类型分布如下：

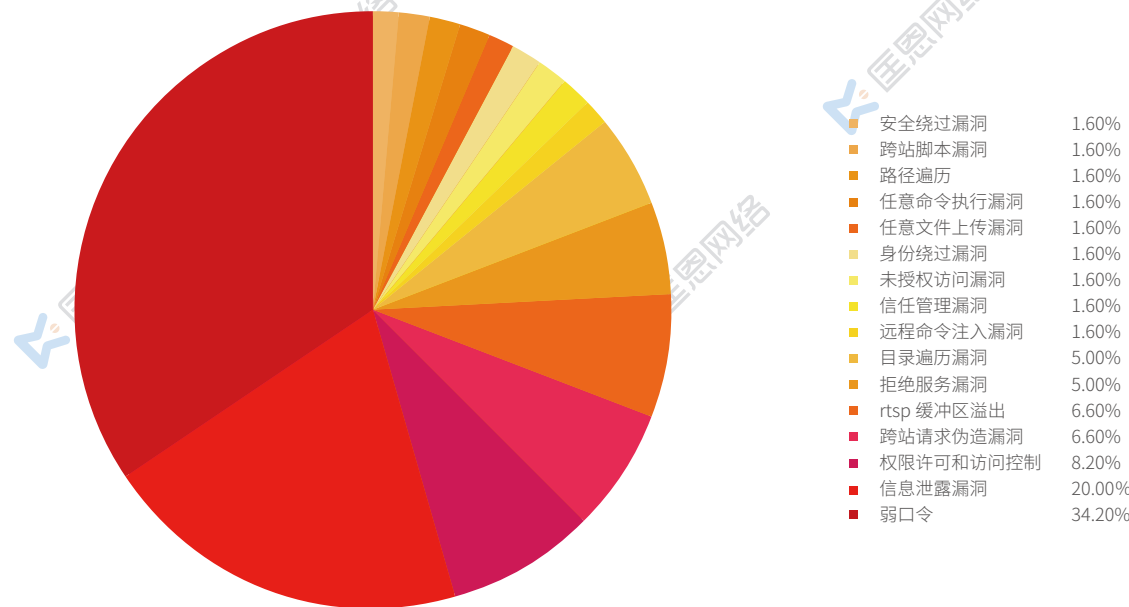


图 2-6 漏洞类型分布图

从图 2-6，我们发现安防监控设备的漏洞类型主要集中在弱口令、信息泄露漏洞、权限许可和访问控制、跨站请求伪造漏洞、RTSP 缓冲区溢出、目录遍历漏洞和拒绝服务漏洞。其中弱口令占有所有漏洞中的 34.40%，占比最高，而弱口令漏洞也是 Mirai 可以大范围感染物联网设备的主因。

为了探测北美 DDoS 事件中的 Mirai 恶意程序对国内安防监控设备的影响，匡恩威胁态势感知平台探测分析了国内近 18 万个安防监控设备，主要包含海康威视、大华、雄迈、宇视、华三等知名厂商。

我们探测发现 22488 个安防监控设备在线，共感知到 6060 个漏洞，主要包含弱口令、权限许可和访问控制等类型，其中 1110 个设备（占在线设备的 5%）存在 Telnet 弱口令漏洞，容易被 Mirai 恶意软件感染控制。

我们探测到的在线安防监控设备区域分布如下：

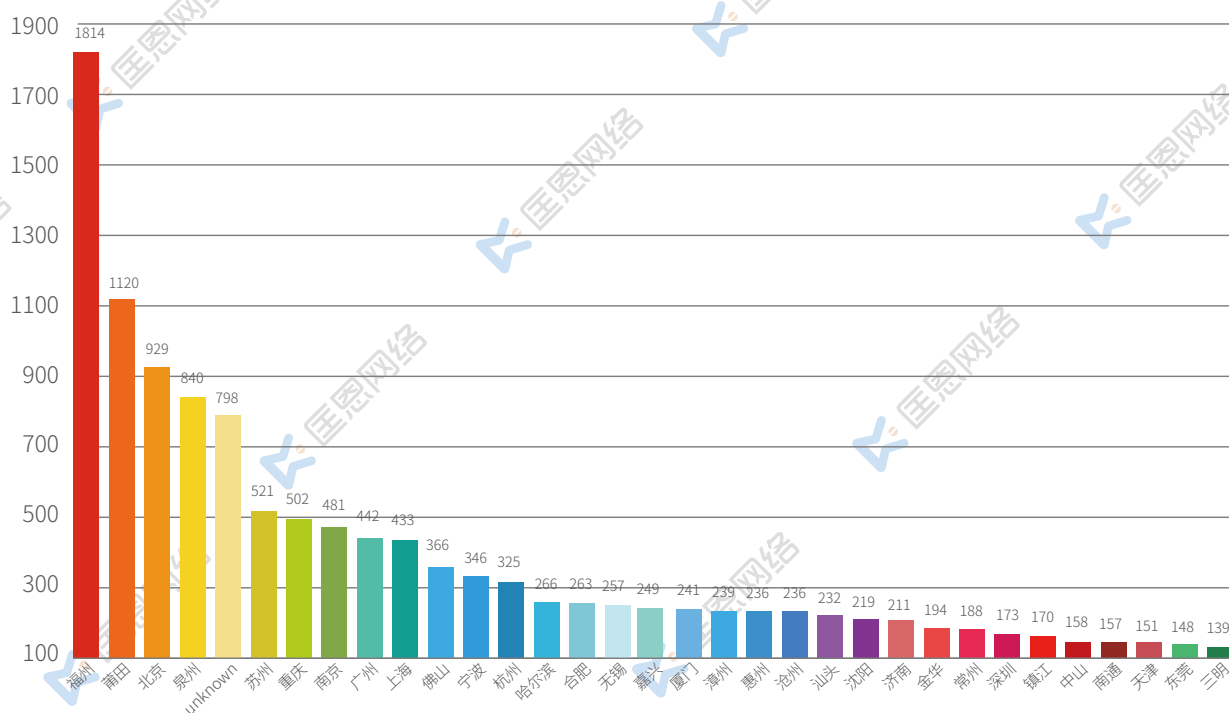


图 2-7 在线安防监控设备区域分布图

分析上图的数据，我们发现国内的安防监控设备主要分布在福建、江苏、浙江、北京、上海、重庆等经济较发达地区，其中福建省的联网安防监控设备数量最多。

根据我们监测结果发现的安防监控设备弱口令排名如下：

序号	登录用户名	登录密码	设备厂商	百分比
1	root	vi	Da	29.65%
2	guest	12	Unknown	9.46%
3	admin	me	Mo	4.97%
4	admin	pe	Unknown	4.49%
5	root	空密码	Vi	3.53%
6	root	Ztc	Z	3.37%
7	admin	12	Hi	2.40%
8	admin	54	Unknown	2.40%
9	admin	7ujMkc	De	2.40%
10	admin	1234	AC	2.24%

图 2-8 安防监控设备的弱口令排名

分析上表的数据，我们发现国内安防监控设备的 Telnet 用户名大多为 root、admin、guest 等常用字符，这些常用账号很容易被暴力猜测，建议更换为非常用字符；Telnet 密码多为安防监控厂商内置的默认密码，这些密码很容易被黑客收集到；使用这些设备的用户大多为普通人，很少会修改 Telnet 服务的默认密码。这些原因是 Mirai 等恶意软件可以轻易控制大量安防监控设备的主因。

为保证安防系统的安全性，匡恩网络作为物联网安全技术和设备专业提供商，对设备厂商和使用用户有如下建议：

- (1) IOT 设备（含安防监控设备）开发商应加强安全审核，避免出现弱口令或安全绕过漏洞，避免出现口令硬编码无法修改的漏洞。
- (2) 用户在使用时，应停止使用默认 / 通用密码，及时修改新的登录密码。
- (3) 使用时禁用对设备的所有远程（WAN）访问。（要验证设备是否未打开以进行远程访问，您可以使用工具扫描以下端口：SSH (22)，Telnet (23) 和 HTTP /HTTPS (80/443)）。
- (4) 使用时尽可能避免该摄像头在共网上可以直接访问，如果无法避免，使用路由器

或边界访问控制设备做限制公网用户直接访问摄像机或探测设备。

## 2.2.2 方程式组织工具泄露事件分析观察

### 2.2.2.1 事件概述

美国国家安全局（NSA）遭到了黑客的攻击。黑客团伙声称他们入侵了“Equation Group”（方程式组织），并将他们从该黑客组织的计算机系统中所获取到的大部分黑客工具全部泄漏在了互联网上。

黑客目前只提供了百分之六十的泄漏数据，剩下百分之四十的数据将会提供给拍卖竞价最高的人。该黑客组织表示，这些文件中包含有非常复杂的黑客工具，NSA 此前曾使用过这些来进行间谍活动。包含多个安全厂商的漏洞，这次泄露的工具全部是针对防火墙产品，包含的部分型号如下：Cisco ASA & PIX 系列、Juniper Netscreen & SSG 系列、Fortinet、Topsec、HUAWEI；而这只是文件中 60% 公开给大众的工具，还有 40% 的核心机密工具正在以高价拍卖。

### 2.2.2.2 泄漏工具简析

事件爆发之后可以下载的包含两部分文件，一个是公布出来的 PoC，另外一部分是加密的拍卖文件。

128M	7	25	10:49	eqgrp-auction-file.tar.xz.gpg	-- 拍卖资源，密钥未公布，无法解压
819B	8	1	06:20	eqgrp-auction-file.tar.xz.gpg.sig	
182M	7	25	10:50	eqgrp-free-file.tar.xz.gpg	-- PoC 文件，可解压
819B	8	1	06:20	eqgrp-free-file.tar.xz.gpg.sig	
3.0K	8	1	06:19	public.key.asc	
190B	7	25			
819B	8	1			

图 2-9 方程式组织被泄漏的工具包概况



目前可解压部分名字叫 eqgrp-free-file.tar.xz.gpg 解压后的目录结构如下。

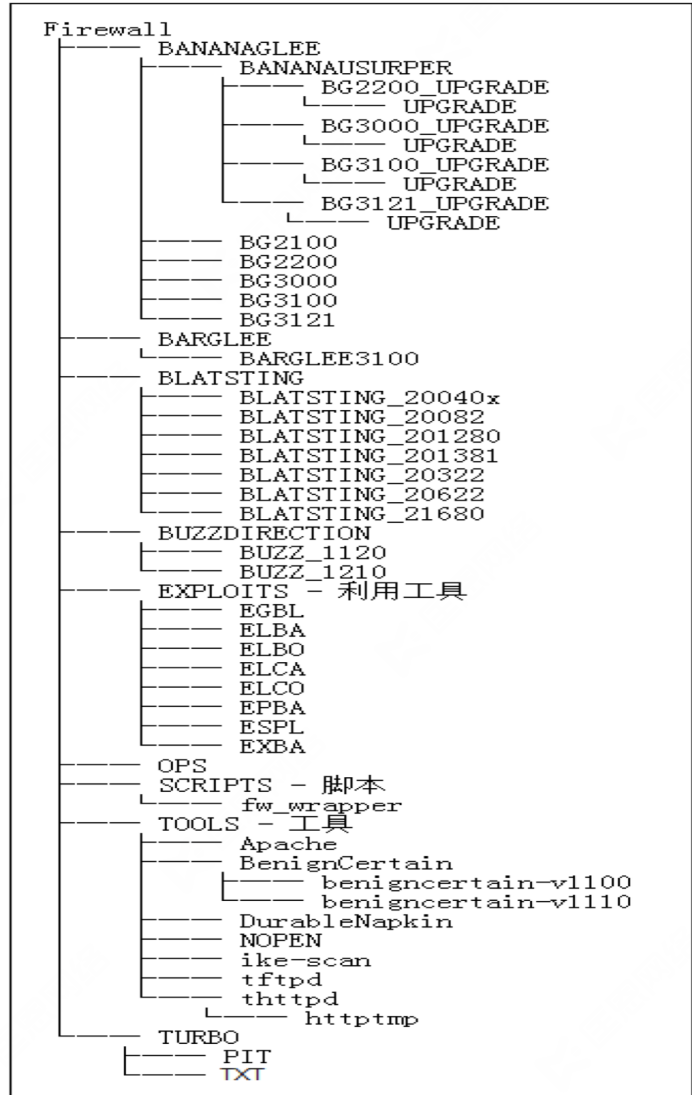


图 2-10 方程式组织被泄漏工具包的目录结构

目前泄漏出来的部分发现大部分是针对路由器、防火墙以及安全产品的攻击，大部分文件创建于 2010 年。

-rw-r--r--@	1	noname	staff	6.0K	8	16	12:35	.DS_Store
drwxr-xr-x	8	noname	staff	272B	4	10	2010	BANANAGLEE
drwxr-xr-x	3	noname	staff	102B	4	10	2010	BARGLEE
drwxr-xr-x	9	noname	staff	306B	4	10	2010	BLATSTING
drwxr-xr-x	4	noname	staff	136B	4	10	2010	BUZZDIRECTION
drwxr-xr-x	10	noname	staff	340B	4	10	2010	EXPLOITS
drwxr-xr-x	8	noname	staff	272B	8	16	12:35	OPS
drwxr-xr-x	35	noname	staff	1.2K	8	16	12:35	SCRIPTS
drwxr-xr-x	18	noname	staff	612B	8	16	12:36	TOOLS
drwxr-xr-x	4	noname	staff	136B	8	16	12:35	TURBO
-rw-r--r--	1	noname	staff	19M	4	10	2010	padding

图 2-11 利用方程式组织黑客工具部分信息

方程式黑客组织攻击工具目录简介如下：

```
OPS - 攻击操作控制工具包；
BANANAGLEE - Cisco & Juniper Devices；
BARGLEE - Juniper Netscreen Devices；
BLATSTING - 穷举爆破；
BUZZDIRECTION - 远控脚本，此文件夹内含两个相同功能、不同版本的脚本；
EXPLOITS - 各目标系统漏洞的利用代码；
SCRIPTS - 攻击脚本资源引用库；
TOOLS - 辅助工具包(编码转换、IP格式转换、加密解密装换等等)；
TURBO - 一些不同版本的二进制文件。
```

图 2-12 方程式黑客组织攻击工具目录简介

进一步解析 EXPLOITS 文件夹，得到如下信息：



图 2-13 EXPLOITS 文件夹中的工具

其中的工具分别如下：

- EGBL = EGREGIOUS BLUNDER (Fortigate 防火墙 + HTTPD exploit (apparently 2006 CVE)：

基于 web 的利用，目标是 Fortigate 防火墙。涉及到 60，60M，80C，200A，300A，400A，500A，620B，800，5000，1000A，3600，3600A 等版本的飞塔防火墙。目前有安全研究人员认为这个就是 Avast 发现的 CVE-2006-6493，基于 OpenLDAP 漏洞的攻击

- ELBA = ELIGIBLE BACHELOR：

目标是 3.2.100.010, 3.3.001.050, 3.3.002.021 and 3.3.002.030 等版本的天融信防火墙。该 exp 基于第三方库展开攻击。

- ELBO = ELIGIBLE BOMBSHELL:

目标是天融信防火墙 3.3.005.057.1 到 3.3.010.024.1 版本, 从 payload 的时间来看在 2009 年已经被开发, 并且有各自不同的代号。WOBBLYLLAMA, FLOCKFORWARD, HIDDENTEMPLE, CONTAINMENTGRID, GOTHAMKNIGHT 等代号, 在代码中有“FOR DEVELOPERS ONLY”的标注字样。

- ELCA = ELIGIBLE CANDIDATE:

针对天融信防火墙 3.3.005.057.1 到 3.3.010.024.1. 的 EXP, 攻击的切入点应该是 /cgi/maincgi.cgi 模块。

- ELCO = ELIGIBLE CONTESTANT:

针对天融信防火墙 3.3 版本之前的 EXP, 攻击的切入点也是 /cgi/maincgi.cgi 模块, 代码被作者加有注释, 只能登录之后使用。

- EPBA = EPIC BANANA:

主要是对 Cisco PIX 防火墙和 Cisco Adaptive Security Appliance (ASA) 设备中的某些模块展开攻击。代码中有包含安全研究员 NoahSpurrier 写过的某些 pexpect.py 的 python 模块, 并包含了用于辅助开发的模块分支。从目录结构来看思科的 ASA 设备的下列型号 711, 712, 721, 722, 723, 724, 80432, 804, 805, 822, 823, 824, 825, 831, and 832 和思科 Pix 防火墙的下列型号 711, 712, 721, 722, 723, 724, 804 可被该 EXP 攻击。

- ESPL = ESCALATE PLOWMAN:

权限提升的 exp, 影响 watchguard 的防火墙, 版本不明, 应该是通过 ifconfig 命令注入代码。

- EXBA = EXTRA BACON (Cisco Adaptive Security Appliance v8.0 to v8.4):

一个远程代码执行的 EXP, 影响思科的 ASA 设备的 802, 803, 804, 805, 821, 822, 823, 824, 825, 831, 832, 841, 842, 843, 844 型号, 通过 SNMP 协议来获知目标的在线和软件的版本号以此来使用该 exp 进行攻击。

额外的各文件夹内都是具体的利用脚本, 里面说明了各脚本支持的攻击目标版本。而所有的攻击手法和利用方法, 都还需进一步研究。

- BANANAGLEE 和 BARGLEE 目录：

主要包含了对 Cisco ASA/Pix 防火墙和 Juniper NetScreen 防火墙的固件植入软件，同时包含了大量的防火墙的 bin 文件供刷入。该目录下面的 Install 文件夹下，都有一个 LP 文件夹，里面都是针对各防火墙型号的攻击脚本，有 pl、py、sh 和其他可执行文件几种类型。具体的利用方法还需要进一步研究。

```
start_redirector.pl creates and uploads PacketDropper filter files and/or starts a
local listener to perform encryption and redirection.


Usage: start_redirector.pl --clr_tunnel_ip <ip> --enc_tunnel_ip <ip> --enc_redir_ip
<ip>
--target_ip <ip> --orig_src_ip <ip> --local_ip --enc_tunnel_pt <port>
--enc_redir_pt <port> --clr_redir_ip <ip> --enc_key <encryption key file>
[--proto <protocol>] [--redir_to_target_dest_pt <port>]
[--redir_to_target_src_pt <port>] [--tunnel_to_attacker_dest_pt <port>]
[--tunnel_to_attacker_src_pt <port>] [--restart] [--logdir <logdir>]

--clr_tunnel_ip <ip>
    IP address that packets will be sent to for encryption and redirection

--enc_tunnel_ip <ip>
    Source IP address of encrypted packets when they reach the redirector
```

BLATSTING 和 BUZZDIRECTION 目录则包含了用于天融信和 Fortigate 的固件植入软件。

另外一个 Tools 文件夹中是一些常见的工具，如 apache 的 linux 安装包，tftp 等用于搭建文件传输的工具



- Apache
- BenignCertain
- DurableNapkin
- ike-scan
- NOPEN
- tftpd
- thttpd
- 1212.pl
- dehex.pl
- false.exe
- installdate.pl
- morel.exe
- teflondoor.exe
- teflonhandle.exe
- xtractpleasing

图 2-14 方程式黑客组 Tools 文件夹中的工具信息



### 2.2.2.3 事件简要总结和启示

在方程式组织工具泄露事件中更吸引我们的是该组织的政府背景，我们简要回顾一下美国在网络战中的一系列准备和政策。

首先是 1998 年发布的第 63 号总统令 (PDD63)《克林顿政府对关键基础设施保护的政策》，紧接着 2000 年发布了《信息系统保护国家计划 v1.0》。布什政府在 2001 年 911 事件后马上发布的第 13231 号行政令《信息时代的关键基础设施保护》，并宣布成立“总统关键基础设施保护委员会”，由其代表政府全面负责国家的网络空间安全工作。并研究起草国家战略，于 2003 年 2 月正式发布《保护网络空间的国家战略》，又于 2008 年发布机密级的第 54 号国家安全总统令，设立“综合性国家网络安全计划”，该计划以“曼哈顿”（二战研制原子弹）命名，具体内容以“爱因斯坦”一、二、三组成，目的是全面建设联邦政府和主要信息系统的防护工程，建立全国统一的安全态势信息共享和指挥系统。

2008 年 4 月，布什总统发布了《提交第 44 届总统的保护网络空间安全的报告》，建议美国下一届政府如何加强网络空间安全。

2009 年 2 月，奥巴马政府经过全面论证后，公布了《网络空间政策评估——保障可信和强健的信息和通信基础设施》报告，将网络空间安全威胁定位为“举国面临的最严重的国家经济和国家挑战之一”，并宣布“数字基础设施将被视为国家战略资产，保护这一基础设施将成为国家安全的优先事项”，全面规划了保卫网络空间的战略措施。

2009 年 6 月，美国国防部长罗伯特·盖茨正式发布命令建立美国“网络空间司令部”以统一协调保障美军网络安全和开展网络战等军事行动。该司令部隶属于美国战略司令部，编制近千人，2010 年 5 月，美国网络司令部正式启动工作。

2011 年 5 月，美国白宫网络安全协调员施密特发布了美国《网络空间国际战略》，其战略意图明显，即确立霸主，制定规则，谋求优势，控制世界；同年 7 月，美国国防部发布《网络空间行动战略》，提出 5 大战略措施，用于捍卫美国在网络空间的利益，使得美国及其盟国和国际合作伙伴可以继续从信息时代的创新中获益。

2012 年 10 月，奥巴马签署《美国网络行动政策》(PDD21)，在法律上赋予美军具有进行非传统作战权力，明确从网络中心战扩展到网络空间作战行动等。

2013 年 2 月，奥巴马发布第 13636 号行政命令《增强关键基础设施网络安全》，明确指出该政策作用为提升国家关键基础设施并维护环境安全与恢复能力。

2013 年 4 月，奥巴马向国会提交《2014 财年国防预算优先项和选择》提出至 2016 年整编成 133 支网络部队，其中国家任务部队 68 支，作战任务部队 25 支，网络防御部队 40 支。

2014 年 2 月，美国国家标准与技术研究所针对《增强关键基础设施网络安全》提出《美国增强关键基础设施网络安全框架》（V1.0），强调利用业务驱动指导网络安全行动，并为四个等级，组织风险管理进程。按网络安全风险程度不同分

2015 年 4 月 23 日，美国五角大楼发布新版网络安全战略概要，首次公开要把网络战作为今后军事冲突的战术选项之一，明确提出要提高美军在网络空间的威慑和进攻能力。

不仅美国紧锣密鼓执行网络空间国际和战争战略，最近颁布的北约网络空间安全框架表明，目前世界上有一百多个国家具备一定的网络战能力，公开发表网络安全战略的国家达 56 家之多。

由此可见，网络空间已经成为继陆、海、空、天之后的第五大主权领域空间，也是国际战略在军事领域的演进，这对我国网络安全提出了严峻的挑战，我们更应积极应对，加快建设我国网络安全保障体系，捍卫我国网络安全国家主权。

## 2.3 物联网安全现状—从逻辑架构视角分析

物联网安全方案不是按照逻辑层分别建设的，而是一个系统化的整体。目前，除了在网络传输和数据平台处理阶段采用了一些常规信息系统所使用的安全方案外，针对物联网设备和物联网系统的安全解决方案非常缺乏。就安全保护技术而言，针对每个物联网的逻辑层，有一些有侧重的安全技术。这里分别进行讨论。

### 2.3.1 物联网感知层安全现状

物联网的感知层主要涉及到传感器节点、网关节点和短距离无线通信技术。在这些节点中进行的通信，目前仅依赖于无线通信技术本身所提供的安全服务，如 Zigbee 网络的安全机制，Wifi 网络的安全机制等。有许多应用在实际中甚至连这些基本的安全机制都没有，例如使用了 Zigbee 网络，但是没有启动其中的安全机制，甚至在所使用的网络中根本没有实现应有的安全功能。

但是，由于感知层目前还处在比较分散的状态，除了一些工业物联网系统外，攻击者通过网络进入感知层设备的动机很小，因此感知层的安全保护目前处在松散状态，很少有针对感知层专门设计的安全产品。

今年 9 月份被发现的 Mirai 病毒，针对物联网终端设备已经展开了大规模入侵，感染了全球 130 万台以上的物联网设备，然后将这些物联网终端设备作为“僵尸网络”节点，发起多次大规模拒绝访问（DDoS）攻击。科学家认为，导致这一现象的原因是物联网设备在出

厂之前没有做好安全检查。

目前这种入侵行为还在继续，升级后的 Mirai 病毒将感染更多的设备，包括物联网终端设备和物联网网关设备等多种基于嵌入式系统的网络设备，后续类似的攻击随时都有可能。这一事件已经引起人们的重视，一些安全性不强的设备已经进行了系统或软件升级，但一些没有安全意识的厂商生产的设备，没有给安全升级提供可能，因此短时间内还找不到有效的解决办法。

随着物联网规模的增大，由于多数的感知层设备不能直接连接互联网，而是通过网关（或汇聚）的设备占主要，感知层安全问题将成为物联网安全的重点。

### 2.3.2 物联网网络传输层安全现状

传统通信主要靠互联网传递大量信息，而物联网的网络传输层则更多使用无线网络，因为无线网络具有可移动、易安装等特点。因此影响物联网发展的关键网络传输技术是具有安全功能的无线通信技术。为了解决这一问题，许多不同的技术方案被提出。近年来得到快速发展的低功耗广域网（LPWAN）通信技术，将在很大程度上解决这一问题，从而形成支撑物联网产业发展的完整技术链，催生物联网产业的爆发式增长。

由于物联网网络传输层一般使用标准的通信协议，无论使用互联网连接，还是使用移动网络连接，都有一些标准安全协议可以使用。当使用无线连接时，从第二代移动网络（2G）就有了加密和身份鉴别国际标准算法，从第三代移动网络（3G）之后，对这些安全算法进行了升级，提供从网络到终端的双向鉴别机制。近几年发展起来的 LPWAN 网络技术，也各自都有不同的安全保护方案。因此，物联网在网络传输层的安全，基本在执行国际标准或行业标准，在数据安全保护和数据来源鉴别方面，没有太多的问题。

但是，网络资源的非法使用仍是个难以解决的问题，即使对非法使用网络的节点能及时发现并拒绝接入，面对大规模分布式攻击，在发现和拒绝之前已经占用了网络资源，因此容易造成拒绝服务（DDoS）攻击。今年发生在美国的大面积断网事件，就是黑客通过控制大量物联网设备发起的拒绝服务攻击造成的。

### 2.3.3 物联网处理应用层安全现状

如果把互联网比作一张无形的网，那么物联网就是一个触手可及的世界。互联网曾经深刻地改变了商业市场，为社会经济注入了不同于传统经济形态的新血脉，而物联网则因与世界万物相伴相生的能力，将作为一种强大的内生力量，引发远远超越商业变革的革命，史无前例。

毫不夸张地说，世界有多大，物联网就有多广，任何行业、任何企业、任何个人都可以

与物联网发生千丝万缕的联系。目前比较火的智能可穿戴设备、车联网、AR/VR、人工智能等，只是物联网一角。

物联网的处理应用层主要体现在云计算平台和行业应用。目前，物联网产业发展蒸蒸日上，但物联网安全机制尚不完善，特别在处理应用层，各个平台运营商都有自己的安全防护机制，但大多数是传统的用户管理、访问控制、入侵检测、审计分析、数据备份和恢复等。在用户终端的安全防护更缺乏，移动用户终端面临的威胁十分严重，几乎每个移动用户终端都在用户不知情的情况下，自己的信息被传送到许多应用平台。这样现象有待政策引导和技术规范。下面我们列举 2016 年发生的一些网络信息泄漏事件，这些事件也是从网上得到的，可以从侧面反映作为物联网处理层的数据处理中心，在信息泄漏方面不可推卸的责任。

2016 年 1 月，机锋被曝泄露 2300 万用户信息。据知情人士称，机锋论坛泄露的 2300 万用户数据包括用户名、注册邮箱、加密后的密码等信息，由于机构数据库对用户密码仅使用了简单的 md5( 计算机安全领域广泛使用的一种散列函数 ) 加密，黑客能够快速破解出绝大部分明文密码。对此，机锋方面通过微博回应称，技术部门已展开深入调查，“目前初步判断是 2013 年泄露的老数据”，并强调，“机锋所有用户密码均为多次加密的非明文转换码，网上泄露的用户信息并不能破解密码并盗取用户账号”。

2016 年 2 月，十大酒店泄露大量房客开房信息。据漏洞盒子白帽子提交的报告显示，知名连锁酒店桔子、锦江之星、速八、布丁。高端酒店万豪 ( 丽思卡尔顿酒店 等 )、喜达屋 ( 喜来登、艾美酒店等 )、洲际 ( 假日酒店等 ) 网站存在高危漏洞，黑客可轻松获取到千万级的酒店顾客的订单信息，包括顾客姓名、身份证、手机号、房间号、房型、开房时间、退房时间、家庭住址、信用卡后四位、信用卡截止日期、邮件等等大量敏感信息。

2016 年 4 月，超 30 省市的数千万社保用户敏感信息或遭泄露。据报道，包括重庆、上海、山西、沈阳、贵州、河南等超 30 个省市卫生和社保系统出现大量高危漏洞，数千万用户的社保信息可能因此被泄露。

2016 年 8 月，约 10 万条高考生信息泄露。据知情人士介绍，高考生信息在网上被肆意出售。10 万条信息标价 1 万元，平均每一条信息价格为 0.1 元。这些信息被一些不法分子购买后用来进行招生诈骗，目前，武汉警方已将此案两名主要嫌疑人控制。但是，不少考生遭受精准诈骗，损失重大，社会影响恶劣。

2016 年 9 月，内蒙古 19 万高考考生信息遭遇泄露，这些信息中包括考生的姓名、身份证号码及其父母姓名、电话，名单覆盖了内蒙古自治区的 12 个盟市，数量最多的地方达 4 万多条。

9 月 14 日，据国家级网络安全应急机构——国家互联网应急中心报告显示，“开发者



使用非苹果公司官方渠道的工具 xcode 开发苹果应用程序 (苹果 app) 时, 会向正常的苹果 app 中植入恶意代码。被植入恶意程序的苹果 app 可以在 appstore 正常下载并安装使用。该恶意代码具有信息窃取行为, 并具有进行恶意远程控制的功能。”

苹果系统程序编写软件 xcode 曝出被黑客植入恶意代码, 已有微信、滴滴打车、高德地图、网易云音乐等近 350 款 app 被感染, 可致用户私密信息泄露, 腾讯发布报告称受影响用户可能超过 1 亿。苹果公司已经将相关软件下架。

2016 年 10 月, 网易邮箱过亿用户敏感信息遭泄露, 影响到网易 163、126 邮箱过亿数据, 泄露信息包括用户名、密码、密码密保信息、登录 ip 以及用户生日等。

2016 年 11 月, 伟易达集团 500 万个家长和超过 20 万个小童的数据资料泄露。据伟易达集团报道, 11 月 14 日黑客入侵了 learning lodge 的客户资料库。国外媒体 motherboard 表示, 他收到黑客入侵 vtech 的客户资料, 当中有大约 500 万个家长和超过 20 万个小童的资料, 包括姓名、电邮地址、密码和个人住址。

2016 年 12 月 10 日晚间, 京东被曝数据外泄。据称, 此次有一个 12G 的数据包外泄, 数据包括用户名、密码、邮箱、QQ 号、电话号码、身份证等多个维度, 数据多达数千万条。京东在 12 月 11 日凌晨发表声明, 称该数据源于 2013 年 Struts 2 的安全漏洞。

2016 年 12 月 15 日, 据外媒报道, 老牌互联网巨头雅虎虽然已经卖给了 Verizon, 但网络安全事件依然不断。继今年 9 月份被曝泄漏 5 亿用户数据后, 它们又出现了更加严重的安全问题。该公司称它们发现了新的安全漏洞, 该漏洞可追溯至 2013 年 8 月, 该漏洞造成至少 10 亿用户的姓名、电邮和密码被盗。这就意味着在短短 3 个月内, 雅虎用户数据泄露总数已经达到 15 亿人次。

这些触目惊心的数字说明物联网处理应用层的安全问题非常严重, 一方面是用户和数据平台运营商对安全问题不够重视, 另一方面我们也看到目前缺少规范性的政策的引导和技术规范。这不是一部《网络安全法》所能解决的问题。

## 2.4 物联网安全相关法规与政策

为了保障物联网产业的健康发展, 国内外政府和相关产业联盟都出台了一系列相关标准和法律法规。有些法规是针对一般网络信息系统的, 包括物联网在内, 有些法规则明确是针对物联网而制定的。

### 2.4.1 国际物联网安全法规与政策

物联网安全的标准和政策对物联网行业的健康发展非常重要。没有这些法规与政策的指引，物联网行业的安全保障容易出现混乱而不成体系的局面。

#### 2.4.1.1 美国发布《保障物联网安全战略原则》

随着物联网产业的兴起，产业内对物联网安全方面的支出一路上升。根据，Gartner 公司在 2016 年 4 月份的一份报告中表示，2016 年，全球物联网安全方面的支出将达到 3.48 亿美元，比 2015 年的支出：2.815 亿美元增长 24%。而到 2018 年，物联网安全支出预计会达到 5.47 亿美元。2016 年，继多起物联网安全事件的爆出，美国从物联网安全的角度制定了相应的政策与标准。首先，2016 年，奥巴马政府新增 140 亿美元的网络安全发展预算；其次，更新并新增了多项网络安全政策，包括《保障物联网安全战略原则》、《网络安全研发战略规划》、《网络安全国家行动计划》以及《制造业与工业控制系统安全保障能力评估》草案；除此之外，还设立了专门的网络安全管理机构，并建立网络安全部队。

2016 年 11 月 15 日，美国国土安全部（DHS）发布《保障物联网安全战略原则》，是美国致力于物联网安全规划的第一步。在此 1.0 版本中，美国国土安全部（DHS）表示，物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉。若未在最初设计阶段构建安全并采取基本安全措施，可能会造成制造商的经济成本、声誉成本或产品召回成本损失。虽然还没有建立解决物联网问题的判例法体系，但传统的产品责任侵权原则可以适用。

以下为物联网安全战略原则的部分总结内容：

在设计阶段结合安全：企业将设备推入市场时必须考虑安全设计，以避免给恶意攻击者创造大量机会操控联网设备。

启用安全更新和漏洞管理：产品部署后，应实时对产品进行安全监测，及时发现漏洞，并通过补丁、安全更新和漏洞管理等策略缓解。

建立在可靠的安全最佳实践之上：传统网络安全中许多经过验证的实践可以作为提升物联网安全的出发点。

根据影响优先考虑安全措施：数据泄露的风险和后果大不相同，这取决于联网设备。因此，专注破坏、泄露或恶意活动的潜在后果对决定物联网生态系统的安全方向尤为重要。

提升透明度：在可能的情况下，开发人员和制造商需要了解供应链，以方便识别软件和硬件组件，并了解任何相关漏洞。增强意识以帮助制造商和工业消费者识别安全措施应用的位置和具体方法。

连接需仔细谨慎：考虑物联网的使用和物联网被破坏的相关风险，物联网消费者，尤其工业企业应该仔细谨慎的对企业联网问题进行考虑。

在此战略原则中，DHS 定义了联邦机构需要执行的四项物联网安全事项：

- 协调其它联邦部门和机构与物联网制造商、网络连接提供商和其它行业利益相关者合作。随着进一步细化和理解最佳实践和方法，会进一步集中更新和应用所发布的战略原则。
- 在所有利益相关者中构建与物联网有关的风险意识。DHS 将与其它机构、私有部门和国际行业伙伴合作，制定培训计划，深化安全教育，增强公众意识。
- 识别并推进激励措施，保障物联网设备和网络安全。目前物联网面临的情况是网络安全责任人不明确，且安全问题所带来的风险通常不由增强安全的人承担。因此，在将来的物联网安全规则制定中，会综合考虑侵权责任、网络保险、立法、监管、自愿认证管理、标准设定举措、自愿行业级计划等一系列因素。今后，DHS 将召集合作伙伴讨论这些重大事项、并收集意见和反馈。
- 为物联网国际标准发展进程做贡献。美国的物联网设备是全球生态系统的一部分，国家组织也正在全力应对物联网安全问题。美国将于国际合作伙伴和私营部门合作，支持国家标准的发展。物联网安全战略原则强调，物联网的相关活动应制定一致的标准和规则，以便整个物联网市场的有序、安全发展。

### 2.4.1.2 美国发布《数字经济的安全保护与发展》报告

2016 年 12 月 1 日，美国国家网络空间安全促进委员会 发布题为《数字经济的安全保护与发展》的报告，为下届政府提供关于加强网络空间安全的建议，其中部分建议须在特朗普当权 100 天之内开始实施。鉴于本届政府任期将在 2017 年 1 月 20 日结束，奥巴马敦促委员会尽快向特朗普过渡政府宣贯。奥巴马称，下届政府和国会将受益于委员会的见解，并使用委员会的建议作为导向。

报告强调改善物联网安全的重要性。报告涵盖网络空间安全的方方面面，包括分布式拒绝服务攻击、认证与身份管理、关键基础设施、中小企业安全、物联网威胁、网络安全研发、

---

2016 年 2 月，美国总统奥巴马发布了《网络安全国家行动规划》，旨在通过一系列长期与短期举措改善美国的网络空间安全态势。奥巴马同时签署了一项行政命令，成立“国家网络空间安全促进委员会”，由来自企业届及学术界的重要思想领袖组成，负责提出建议以帮助国家在未来十年内强化公共与私营部门的网络空间安全水平，最终促进隐私保护、公众安全保障、经济与国家安全防御以及引导美国民众更好地保护数字化财产。

---

消费者安全意识培养、人力缺口、联邦机构的企业风险管理、安全事件响应、国际协约及行为规范。其中，报告首次将物联网安全提升为一个举国需要重点关注领域，并给出了具体的发展建议。

一是建议司法部评估联网设备安全责任的法律。司法部应带头与商务部、国土安全部、联邦贸易委员会、消费者产品安全委员会以及感兴趣的私有行业展开跨机构研究，评估物联网安全相关法律的完备情况，并在 180 天内提出建议。

二是为物联网设备建立基于风险的标准、指导方针和最佳实践。下届总统应在就职后 60 天内颁布行政命令，指导国家标准与技术研究院和业界合作，识别现有标准、最佳实践，迅速达成一套基于风险的综合安全标准。

三是加强公众的网络空间安全意识。物联网设备已经成为公众生活中不可或缺的一部分，因此必须加强对公众的教育和宣传，并鼓励民众的积极参与。

四是在研发阶段降低产品互联性的风险。互联设备的经销商必须确保其供应商注重组件和子部件的安全，在产品开发的过程就已经过安全验证。美国政府、公共和私营部门一向重视研发中的创新。尽管对网络空间研发的整体投资非常可观，但在技术、产品、系统和环境固有安全方面的投资相对较少。因此，应加强网络空间基础研究，促进系统固有安全性、防御性和弹性的形成。

五是提高政府和私营部门的合作。随着目前网络技术的发展，国家关键基础设施与其他民用设施乃至私营网络设施之间的界限日益模糊，深化公私合作将更好保护关键基础设施以应对网络攻击。

#### 2.4.1.3 云安全联盟发布《物联网安全指南》

云安全联盟于今年 10 月 7 日发布的长达 80 页的《物联网安全指南》，指出物联网安全的必要性。

随着关键国家基础设施逐渐依赖物联网，汽车联网趋势盛起，而物联网能被用来发起 DDoS 攻击。此外，无人机正“迈入”主流地位，并被作为侦察平台，物联网产品一般会“影响隐私”。

云安全联盟在新的物联网建议中指出，以安全开发方法起步是关键。这就意味着开发人员必须从一开始就满足联网设备的安全要求和过程。其次，物联网不应物理暴露在不完全的环境中，这也意味着不应只在通信层面实现物联网安全。因为，设备会被物理窃取，例如，共享密钥被解除等。另外，物联网设备价格低廉、嵌入式系统的资源限制了对安全性的考虑等问题，也应在将来的物联网安全考虑因素之中。



### 2.4.1.4 工业互联网联盟发布《工业物联网安全框架》

2016 年 9 月，工业互联网联盟发布了一份旨在解决工业物联网 (IIOT) 及全球工业操作运行系统相关安全问题的文件——《工业物联网安全框架》。该框架集中在 5 个方面来解决问题：安全保障性、隐私性、安全性、可靠性和适应性，同时，这也是该联盟所定义的工业系统 5 大特征。该框架设计了各种风险、评估、威胁和性能指标供产业经理用来保护各自的公司企业。

工业物联网安全框架旨在从多个方面解决安全问题，包括业务、功能与实现。公司经理可用该安全框架基于风险评估做出更明智的决策。其安全评估由各种不同模块构成，比如终端、通信、监视和配置。每一块都将提供方案实现的最佳实践，以解决整个系统的可信度问题。

该框架从工业物联网的 3 个角色对安全进行构建：

- 打造硬件和软件的供应商；
- 使用硬件和软件来构建解决方案的系统集成方；
- 使用解决方案和系统的业主方。

工业物联网安全问题涉及各方各面，从工业过程和应用，到安全和可靠性需求，而且安全问题不能孤立解决。如今很多工业系统都还不具备完善的安全措施。工业互联网的安全水平远远不能满足工业互联网的安全需求。因此，我们必须向工业系统中添加更高标准的安全需求，必须以“可靠性”这一基本要求为前提。

《工业物联网安全框架》描述了整合不同安全域的结果，提供了如何选择和达成安全目标的指南，并讲述了如何利用工业物联网技术解决网络破坏和网络间谍的方法。

### 2.4.1.5 欧洲将制定新物联网安全规范

继 Mirai 病毒网络攻击事件之后，欧盟委员会也宣布将制定新物联网设备安全规范，新规将是欧盟电信法改革计划的一部分。欧盟提出这一提案，旨在通过更严厉的监管规范解决安全问题。英国财政部在 11 月的一份声明中称，英国计划在 5 年内投入 19 亿英镑用于互联网安全防御。英国政府还将设立一个新的“网络安全研究所” (CSRI)，将来自各大学的技术与切尔滕纳姆 (Cheltenham) 创新中心的技术相结合，帮助发展网络安全创业公司。

## 2.4.2 国内物联网安全法规与政策

2009 年 8 月，时任国务院总理温家宝在无锡视察时提出感知中国的概念，将物联网产业发展上升到战略性新兴产业的高度，与此同时，相关部门也发现，物联网关键技术，尤其是安全技术，是物联网产业健康发展的瓶颈。2011 年，工业和信息化部发布《物联网“十二五”

发展规划》指出，要大力攻克核心技术，加快构建标准体系，加强信息安全保障。特别需要说明的是，《规划》将信息安全保障作为一个专门任务予以重视，其内容包括加强物联网安全技术研发，建立并完善物联网安全保障体系，加强网络基础设施安全防护建设。国家“十三五”规划指出，要实施网络强国战略，加快构建高速、移动、安全、泛在的新一代信息基础设施。支持智慧城市的建设，提高网络安全等方面风险防控能力。

物联网安全技术目前还没有统一的国际标准，国家标准也正在制定中，主要原因是物联网是个特别大的系统，包括的行业非常多，因此在信息安全保护方面制定统一的标准有一定难度。其实，物联网安全问题主要是物联网感知层的安全问题，因为在网络传输层和处理应用层，可以采用传统信息系统的信息安全保护技术，而感知层的设备种类繁多，性能差异大，从高性能的视频监控设备，到无人值守的传感器模块，在信息安全保护技术方面都有着很大的区别。最具有技术挑战的，是资源受限设备的信息安全保护，例如小型传感器和 RFID 标签等。

如果说在传感器等设备方面，我们落后的技术可以通过采购国外技术和设备来弥补的话，那么在物联网安全方面，特别是物联网感知层的信息安全保护方面，很难通过直接购买国外技术改进，因为物联网感知层的安全技术一般与硬件产品融为一体，购买国外的安全技术就等于购买国外的产品。而且安全技术不仅仅限于产品本身，而是要渗入数据处理中心，因为信息安全是一个系统，而不是一个独立的模块。因此，无论国外在物联网感知层方面有什么信息安全保护技术，我们都需要研发自己的技术并应用于自己的产品，这样才能实现“可控性”，这也是信息安全体系的重要指标。

综上所述，物联网安全技术的挑战重点在于对感知层资源受限设备的轻量级安全保护，包括轻量级安全算法和轻量级安全协议。轻量级安全算法具有通用性，而轻量级安全协议只能做到在小范围内具有一定的通用性。

近年来，国家在物联网安全方面给予了很多政策支持和一定的资金支持，例如在“十二五”期间，科技部设立了国家 863 项目“物联网安全感知关键技术及仿真验证平台”，在“十三五”的规划中，又设立了工控安全专项，这些都说明国家对物联网安全领域的重视和支持。但是，物联网系统建设中对信息安全的防护投入却远远不够。有关分析表明，我国在信息安全领域的投资占整个 IT 投资比例不足 1%，和美国（3.6%）及日本（6%）等成熟市场差距依然明显。对信息安全防护意识的程度、对信息安全防护体系的检查以及对信息安全问题所造成的损失的正确评估和责任追溯，是决定信息安全投入的主要原因。

考虑到物联网安全问题关系到行业应用的安危，甚至在一定程度上会关系到国家的安全，国家应该提前进行部署，而不能等到亡羊补牢。因此，物联网安全方面的基础研究应该由国家设立资金予以支持，并在研究成果产业化后进一步给予一定补助，这样会提高面向产业应

用研究的动力。

物联网是一种新型产业方向，是信息技术发展的一个新阶段。物联网安全问题还没有在物联网行业应用中得到广泛关注，甚至还没有引起社会的足够重视。目前的矛盾是，行业界认为物联网安全问题没有这么严重，而学术界认为物联网安全方面的研究不能产生创新性理论成果。这种情况导致从事信息安全研究的学者不愿意研究物联网安全问题，而从事物联网产业建设的团队又很少有信息安全领域的专家，这种矛盾导致了物联网安全需求仍然停留在口号上。如何鼓励从事信息安全研究的科研人员投入到物联网安全方面的研究，推动国家物联网产业的信息安全建设，保障物联网产业的健康发展，是一个值得思考的问题。市场引导人们的行为，政策引导市场的走向，因此制定一个合适的政策可以更好地引导物联网行业应用与信息安全科学研究的结合，提高物联网系统的安全保护。

### 2.4.3 行业领域网络安全法规与政策

#### 2.4.3.1 车载信息安全产业联盟发布《车载信息安全技术要求白皮书》

2016 年 10 月 13 日，车载信息安全产业联盟成立，车载信息安全产业联盟由在国内外从事信息安全、汽车、汽车电子等行业的知名企业，国内信息安全认证、测评机构等自愿组成，旨在营建健康有序、可持续的产业经济环境，提升车载信息安全产业的市场影响力。该组织将通过开展技术交流、完善业内技术标准、提高行业整体能力，提升车载信息安全产业在国际市场的总体竞争力。

此外，该联盟的成立，还将有助于推动政府制定有利于产业发展的重大政策，切实促进车载信息安全产业的健康、有序发展。车联网市场发展得如火如荼，加快安全系统的构建也是迫在眉睫。为此，在成立大会上，联盟就发布了《车载信息安全技术要求白皮书》，以推动车载信息安全类技术标准的发展。

《白皮书》认为，车载电子信息系统攻击手段及方式通常包括以下四种：

（一）网络攻击：在网络传输层篡改消息、伪造服务、窃听等，典型的攻击方式如重放攻击、中间人攻击、TCP 注入攻击；

（二）软件漏洞：通过对车载系统软件的恶意修改进行攻击威胁，典型方式如植入木马、后门、二次打包应用程序；

（三）数据篡改：通过对车载系统软件以及存储的敏感数据进行恶意分析，从而获取用户的敏感信息以及软件的漏洞信息；

（四）异常行为：通过对车载系统软件的安全漏洞进行利用，实现对车载设备的攻击威胁。

因此,《白皮书》提出,车载电子信息系统的安全需求,应包括抵御网络攻击、检测扫描软件漏洞、防止数据篡改、实时监测异常行为等基本需求,以及车辆行驶安全保证、车辆信息交互功能保证、隐私信息安全保证等特殊需求。

《白皮书》同时还提出了车载信息安全产品架构模型、车载信息安全产品标准化框架、标准化发展规划等。联盟希望,《白皮书》提出的框架模型后续能够成为行业标准。

#### 2.4.3.2 GSMA 协会发布《GSMA 物联网安全指南》

全球移动通信系统协会(GSMA)代表全球移动运营商的共同权益。GSMA 在更广泛的全球移动生态系统中连结着近 800 家移动运营商,250 多家企业,其中包括手机与设备制造商,软件公司,设备供应商,互联网企业,以及相关行业组织。GSMA 还是业界领先活动的主办方,如世界移动通信大会、世界移动大会 - 上海,以及移动 360 系列会议等等。

为了促进日益增长的物联网(IoT)市场的服务安全发展和部署,GSMA 协会通过对移动产业咨询后,于今年 2 月 24 日发布了《GSMA 物联网安全指南》(The GSMA IoT Security Guidelines)。该文就如何应对常见网络安全威胁以及与物联网服务相关的数据隐私问题,为物联网服务提供商和实用物联网生态系统具有重要参考价值。

该项目得到了移动产业的大力支持,包括移动运营商 AT&T、中国电信、阿联酋电信(Etisalat)、KDDI、NTT DOCOMO、Orange、西班牙电信(Telefónica)、挪威电信(Telenor)和威瑞森(Verizon),以及供应商和基础设施合作伙伴 7Layers、爱立信(Ericsson)、金雅拓(Gemalto)、泰利特(Telit)和 u-blox。

GSMA 的物联网安全指南为物联网生态系统中的所有参与者而设计,包括物联网服务提供商、物联网设备制造商和开发者。它们概述了应对潜在威胁所采用的技术和方法及其执行方式,从而将帮助服务提供商构建安全的服务。此外,它们还提出了对物联网服务的所有组件进行风险评估的必要性,以确保这些组件能够安全地采集、存储和交换数据,同时成功地减少网络安全攻击。

《GSMA 物联网安全指南》是围绕 GSMA 互联生活计划而编制。该计划旨在帮助运营商在机器对机器(M2M)市场加快交付新型互联设备和服务。它致力于推动行业合作,促进适当监管,优化网络,从而在不久的将来为 M2M 以及长期为物联网的发展提供支持。

#### 2.4.3.3 消费者技术协会发布《物联网安全》白皮书

2016 年 11 月,美国消费者技术协会(Consumer Technology Association, CTA)发布《物联网安全》白皮书。白皮书表示,相比监管措施,自愿性最佳实践能更好确保数十亿联网设备的网络安全,并呼吁行业与政府共筑物联网安全。



白皮书指出，“决策者应避免宽泛、不规范的监管措施。因为这类措施可能会阻碍或延迟新物联网应用的发展，并扼杀创新（例如可以控制清洁剂的远程健康监测设备）产品的经济和社会利益。相反，自我调节和其它共识的行业能力将允许利益相关者以实际灵活的方式解决零散的具体问题”，“零散或不一致的监管方法潜在破坏物联网发展，并会让消费者困惑。美国食品和药物管理局的 24 个独立联邦机构，包括联邦贸易和通信委员会、国家公路交通安全管理等——在物联网某些方面设有监管当局”，“2020 年，物联网发展需要的网络容量至少是如今的 1000 倍”。

白皮书解释道，“适用于特定物联网设备或应用的具体法律、法规和监管体系并不总是明晰，物联网这个复杂的网络对小型企业而言特别困难，因为小型企业无力承担”。

消费者技术协会会长 Gary Shapiro 表示，标准制定和监管过程不应该是美国联邦机构某一个组织的责任。Shapiro 敦促下一任总统特朗普倾力推动互联网创新，确保联邦机构腾出足够的频谱，确保企业具备所需资源缔造物联网的辉煌未来。

#### 2.4.4 国家网络安全法

2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》，并将之在中国人大网公布，向社会公开征求意见。

2016 年 11 月 7 日上午，十二届全国人大常委会第二十四次会议经表决，通过了《中华人民共和国网络安全法》。这是我国网络领域的基础性法律，明确加强对个人信息保护，打击网络诈骗。该法自 2017 年 6 月 1 日起施行。

网络安全法的指导思想是：坚持以总体国家安全观为指导，全面落实党的十八大和十八届三中、四中全会决策部署，坚持积极利用、科学发展、依法管理、确保安全的方针，充分发挥立法的引领和推动作用，针对当前我国网络安全领域的突出问题，以制度建设提高国家网络安全保障能力，掌握网络空间治理和规则制定方面的主动权，切实维护国家网络空间主权、安全和发展利益。

网络安全法共有 7 章 79 条，内容上有 6 方面突出亮点：第一，明确了网络空间主权的原则；第二，明确了网络产品和服务提供者的安全义务；第三，明确了网络运营者的安全义务；第四，进一步完善了个人信息保护规则；第五，建立了关键信息基础设施安全保护制度；第六，确立了关键信息基础设施重要数据跨境传输的规则。


对当前我国网络安全方面存在的热点难点问题，该法都有明确规定。针对个人信息泄露问题，网络安全法规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。并规

定了相应法律责任。

针对网络诈骗多发态势，网络安全法规定，任何个人和组织不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。并规定了相应法律责任。

此外，网络安全法在关键信息基础设施的运行安全、建立网络安全监测预警与应急处置制度等方面都作出了明确规定。

国家网络安全法作为建设网络强国的法制保障，为工业控制系统安全既带来了机遇，也带来了挑战。机遇方面，随着国家网络安全法草案公开征求意见及后续将要开展的进一步工作，工业控制系统安全行业将更加有序、更加有章可循，相关工作也会更加规范地开展和实施。所涉及的相关组织机构、人员等的重视程度、意识形态也将得到明显的改善和提升；挑战方面，也正是因为相关工作需要更加有序、规范地进行，要求相关组织机构、人员等必须不断完善工作制度，不断提升工作要求，依章、依规、依法开展工业控制系统安全工作。



# 第三章

## 工业物联网 安全现状

## 3.1 工业物联网的系统架构

工业物联网是一种特殊的物联网系统，既有一般物联网的共性，又有行业特色所带来的一些典型的特征。不是每一个物联网行业都像工业物联网一样特殊。由于工业物联网在物联网系统中的重要地位，本章着重针对工业物联网进行分析研究。

### 3.1.1 什么是工业物联网

物联网的概念已经在几年前就提出了，但工业物联网的概念还没有专门的描述。很明显，工业物联网是物联网的一个子集，一种特殊情况，因此可以说是工业领域的物联网。

正如前面所描述的，物联网没有严格的定义，通常物联网的概念通过特征描述来说明。一般来说，物联网包括感知层，网络传输层和处理应用层。感知层包括数据采集设备、RFID 标签和读写器、数字开关设备、传感网关节点设备、监控设备、GPS 设备等，以及这些设备组成的局域网；网络传输层一般指互联网、移动通信网和无线广域网；处理应用层一般指云计算平台及其所提供的各类服务。

那么什么是工业物联网呢？工业物联网也离不开物联网的一般架构，其感知层主要是工业数据的采集，网络传输层也是互联网、移动通信网和无线广域网，处理应用层是工业云平台及其所提供的服务。

物联网是所有物联网相关行业的统称。工业物联网也是所有工业物联网相关行业的统称，包括生产系统物联网、运输系统物联网、监控和管理系统的物联网等。因此，工业物联网是物联网技术与工业生产、加工、运输过程的高度融合，将工业生产系统、工业监控系统、工业管理系统、物资运输系统、消费反馈系统等融为一体，通过数据中心的智能处理，可以提高工业生产效率，实现多品种少批量，提高产品质量和用户满意度，使工业生产效率更高、费用更低、产品质量更高、客户满意度更高。

### 3.1.2 工业物联网与工业互联网的关系

在工业物联网的概念被提出之前，工业互联网的概念就已经存在了，而且国外一些企业早在 2014 年就成立了“工业互联网联盟”（Industrial Internet Consortium）。相应地，国内成立了“工业互联网产业联盟”（Alliance of Industrial Internet）。在工业互联网产业联盟 2016 年关于《工业互联网体系架构》的研究报告中指出：“工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。其本质是以机器、原材料、控制系统、信息系统、产品以及人之间的网络互连为基础，通过对工业数据的全面深度感知、实时传输交换、快速计算处理和高级建模分析，实现智能控制、运营优化和生产组织方式变革”，并指出工业互联网包括“网络”、



“数据”和“安全”三个方面。

不难看出，工业互联网的主要内容是工业物联网的网络通信资源、应用数据和安全服务。相比之下，工业物联网在工业互联网基础上，还包括工业生产设备、网络通信设备以及用户终端设备等。工业互联网不包括这些设备的物理实体，只关注这些设备所处理的信息。从这个意义上说，工业互联网是工业物联网的网络支撑系统，而工业物联网是工业互联网的扩展。

那么，工业互联网与互联网的关系如何呢？根据我们的分析，无论工业互联网如何定义，它都是一种服务于工业领域的以互联网架构为主的网络。如果这个网络连接互联网，那么它就是互联网的一部分；如果这个网络与互联网分开，只要通过 IP 协议进行网络传输，我们仍然可以看作是互联网的一种。注意不能把互联网理解为一张网，即不能认为不接入这张大网的都不是互联网。

根据这些观察和上面的分析，我们可以大概给出几种概念之间的逻辑关系，如下图。

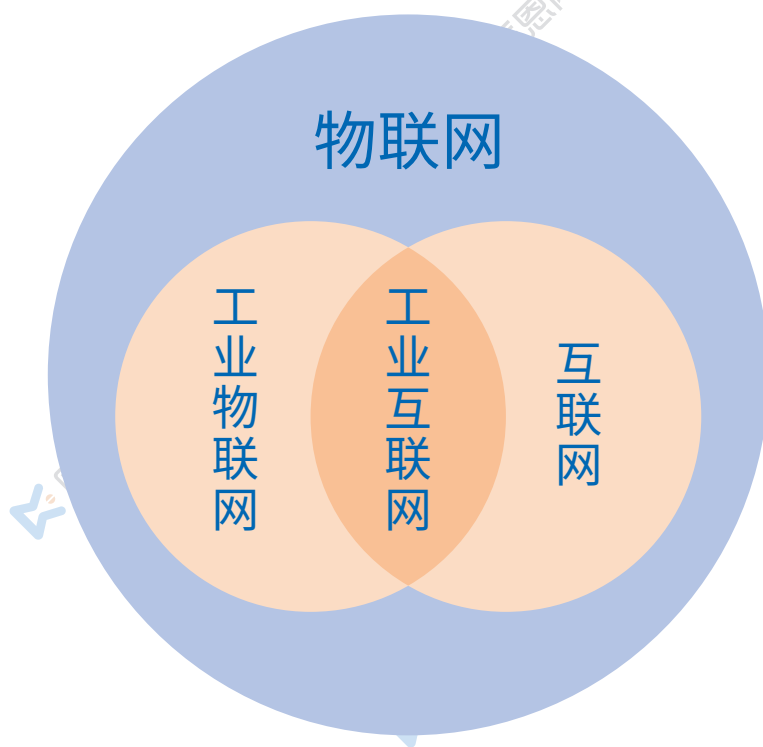


图 3-1 有关物联网的几种概念之间的关系示意图

除了上述几种概念外，还有一种概念是“互联网+”，它与“互联网”之间是什么关系呢。很明显，“互联网+”是基于互联网的一些扩展服务。我们可以简单列出几种类型的服务：

- 互联网+工业生产：结果是工业物联网的一个子类；

- 互联网 + 物资运输：结果是智慧物流和产品溯源；
- 互联网 + 销售消费：结果是电子商务、电子消费；
- 互联网 + 车辆信息：结果是智能交通、路况导航；

“互联网 +”所能涵盖的服务是无边界的，是一个动态的过程，随着所服务对象的变化而变化。因此“互联网 +”不是一种特殊的网络，也不是互联网的延伸，而是一种基于互联网、移动互联网的服务模式。

### 3.1.3 什么是工业物联网安全

物联网的架构分为三个逻辑层，即感知层、网络传输层和处理应用层。在工业物联网中，感知层的数据主要来自于工业生产，这类数据包括感知数据、设备运行参数、监控数据等。为此，工业物联网的感知层数据，不能仅仅理解为传感器数据，而是多种类型的数据。为了更好地反映这种情况，我们把工业物联网系统中的感知层称为数据采集层。为了名称上的一致性，我们把工业物联网系统中的网络传输层称为数据传输层。考虑到工业物联网系统中数据处理后一般不是为终端客户提供应用，而是反馈给工业生产，处理过程为主，而应用过程相对要简单，因此我们把工业物联网系统中的处理应用层称为数据处理层。这样，我们就形成了在各个逻辑层的名称上与传统物联网略有不同的架构。工业物联网架构中的几个逻辑层与一般物联网的架构对应如下图所示：

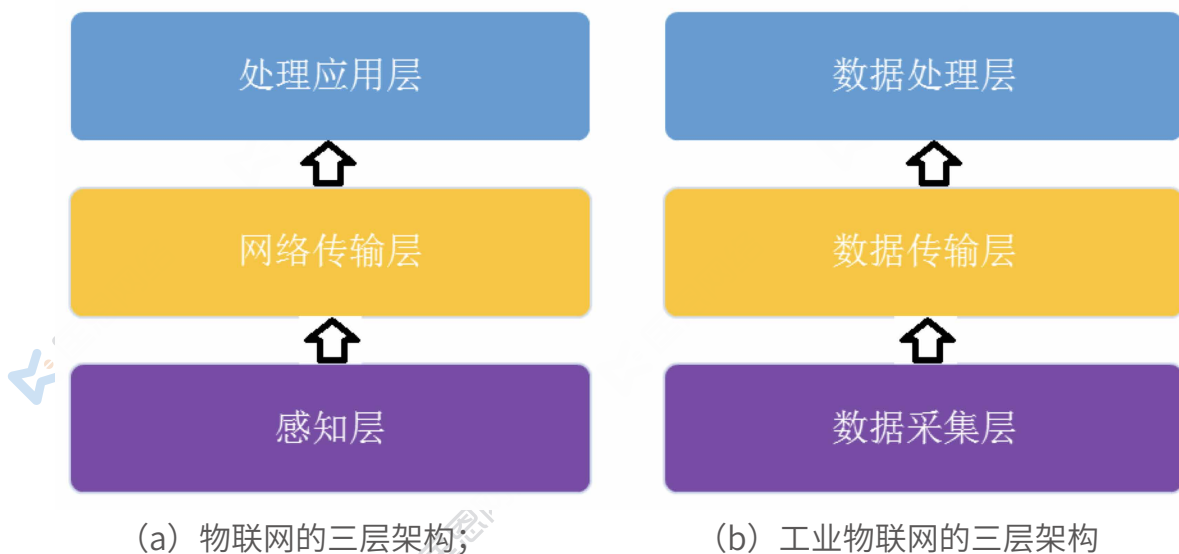


图 3-2 工业物联网架构图

### 3.1.3.1 工业物联网系统的数据采集层

根据图 3-2 所示的工业物联网架构，工业物联网的数据采集层就是采集工业生产过程中需要进一步分析处理的数据，这些数据可能来自工业生产的不同阶段。C 参照工业控制安全等级保护设计要求的国家标准草案，工业物联网系统从业务功能上的分层如下图所示：

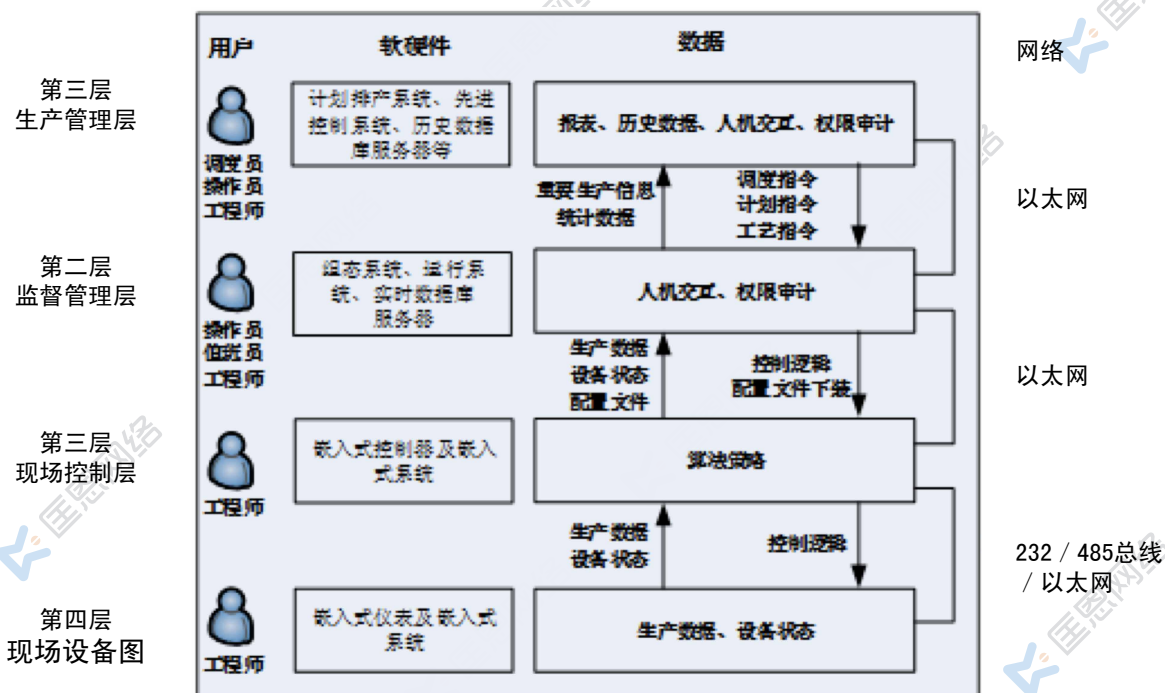


图 3-3 工业物联网系统的业务功能及安全防护

从图 3-3 可以看出，工业物联网系统中的数据采集层包括现场设备层和现场控制层所有用于数据采集的设备和内部网络（如现场总线）。但由于数据采集设备与其他工业生产设备之间相互关联，为简单起见，一般将整个工业现场设备层和现场控制层都看做数据采集层。那么监督控制层和生产管理层是否也属于数据采集层呢？虽然没有严格的划分，而且不同的工业在架构上也不同，但一般来说，监督控制已经不属于工业生产过程中的实时控制了，而且控制指令可以通过广域网络传输，因此可以看作数据处理层。图 3-3 中的生产管理层就属于数据处理层。

在数据采集层中，有生产现场的设备和控制设备，这些设备由上位机进行控制。上位机根据生产设备反馈的数据进行实时控制反馈，实现对生产设备的实时控制和调整。在这个小循环中，上位机的安全性是至关重要的。入侵者如果能控制上位机，就可以破坏其所控制的受控设备。震网病毒对伊朗核电站的破坏就是通过入侵到上位机中实施的。最近发现存在一种不需要通过上位机而能直接入侵 PLC 控制器的病毒，可以不需要通过上位机而直接进行传播感染，这一事件又给应对工业物联网系统的安全威胁带来更为严重的挑战。

### 3.1.3.2 工业物联网系统的数据传输层

工业物联网系统中的数据传输层与一般物联网的数据传输层是一致的。从工业物联网的架构（图 3-2）来看，在数据采集层之上是数据传输层。但数据传输层采用的一般是按照国际标准或行业标准搭建的通信网络，如互联网，3G 或 4G 移动网络。近年来，针对物联网这一特殊应用的低功耗广域网（Low Power Wide Area Network, LPWAN）技术发展迅速，一些技术已经产品化并已规模生产，但其安全问题还没有得到充分论证分析。5G 移动通信技术也在快速发展中，其应用目标也包括物联网相关产业。根据工业系统对数据实时性要求较高的特点，5G 移动通信技术或许更适合工业物联网系统。同样，5G 移动通信中的安全技术仍然处在研究阶段，其安全程度需要经过研究人员的充分分析和产品的市场验证后才有结论。

### 3.1.3.3 工业物联网系统的数据处理层

工业物联网系统的数据处理层，从物理形态来看，与其他物联网行业的数据处理中心没有区别，也是一个云计算平台。但针对工业应用，这个云平台应该拥有一些工业系统专用的处理过程和应用软件。例如许多工业应用对数据的完整性和对身份的鉴别能力要求很高，因为不希望控制指令得到伪造和篡改，而对数据机密性方面则要求没那么高，反而要求要快速，而且一般不需要很复杂的隐私保护技术，因为工业云平台一般不处理复杂的个人隐私信息，可能会涉及到用户的姓名、地址、联系方式等，对这类数据的隐私保护处理还是比较容易的。

据《中国智能制造网》报道，西门子面向市场推出了“MindSphere—西门子工业云平台”。MindSphere 被设计为一个开放的生态系统，工业企业可将其作为数字化服务平台。MindSphere 还为西门子的工厂数字化服务奠定坚实的基础，譬如对数控机床以及驱动链的预防性维护。

与其他云计算平台相比，工业云平台面临的安全威胁更为严重，因为工业系统的价值高，影响大。造成工业云平台安全威胁的，除了云平台本身的系统和应用软件可能存在漏洞外，云平台与数据采集层之间的通信协议也可能带来安全问题。广泛服务于网络通信安全的 OpenSSL 协议，在 2014 年被发现有严重的实现漏洞，被称之为“heart bleed”（心脏出血），黑客通过这一漏洞，可以入侵控制通过 OpenSSL 进行“安全通信”的终端设备。

### 3.1.4 工业物联网系统的安全技术

工业物联网的安全技术覆盖工业物联网的各个逻辑层。工业物联网的数据采集层是一个庞大的工业生产系统，对这一系统的入侵可以造成非常严重的影响。目前工业物联网的规模还不小，多数工业控制系统还没有形成工业物联网的形态，个别已经形成工业物联网形态的系统，数据处理中心也是一个业务范围有限的私有云平台。因此，工业物联网的安全威胁主



要来自于数据采集层。继德国政府提出“工业 4.0”这个高科技战略计划之后，我国政府提出了“中国制造 2025”行动计划，该行动计划将推动“智能制造”工业的发展，推动信息化与工业化的高度融合，推动工业物联网的规模化发展。随着工业物联网的发展，数据处理层的安全问题，表现为工业控制系统的安全问题，仍然是整个工业物联网系统安全保护的重点。

事实上，在工业物联网系统的不同逻辑层，安全技术所保护的目标是不同的。下面我们分别进行描述。

#### (1) 数据采集层的安全技术。

数据采集层安全保护的目标是工业生产设施的安全，数据传输层安全保护的目标是网络服务功能的安全，数据处理层安全保护的目标是主要是工业数据。

目前，数据采集层的安全威胁主要是一些工业控制系统的专用蠕虫病毒，针对工业控制系统和组态软件的安全漏洞进行感染和传播，达到有针对性地进行破坏的目的。匡恩网络在这方面具有领先技术，对工业物联网的数据采集层实施了“4+1”安全防护策略，研发了相应的技术和产品，实现了包括“结构安全”、“本体安全”、“行为安全”和“基因安全”的全生命周期安全保护。

#### (2) 数据传输层的安全技术。

在工业物联网的数据传输层，目前采用的是网络基础设施所拥有的安全保护技术，如 3G 和 4G 移动网络中的标准安全技术。新发展是 LPWAN 技术和 5G 移动通信所采用的安全技术，也可以为工业物联网的数据传输层提供不同程度的安全保护。

#### (3) 数据处理层的安全技术。

在工业物联网的数据处理层，目前的安全保护技术正在研究开发中。匡恩网络研发的大数据平台态势感知技术，可以为数据处理层的安全保护添砖加瓦。

### 3.1.5 物联网安全建设——工业物联网安全是重中之重

工业物联网是一种特殊的物联网，也是物联网的核心。这是因为：（1）工业领域对信息化的需求较其他领域更强烈，而且也有更多可以投入的资金。事实上，在物联网的概念被提出之前，在工业领域已经有实际使用的工业物联网系统了。特别是在电力行业，物联网技术的使用从很早就开始了，因为需要在远程监控环境参数，控制发电、输电等设备。（2）在物联网安全事件中，多数属于工业控制领域，虽然有些工业控制领域的物联网程度还不是很很高。在工业领域之外的其他行业的物联网系统在近几年才开始建设，而且主要是示范应用，其重要程度比不上工业物联网。有人说，一个信息系统遭受威胁的程度，不仅仅依赖其所采

取的安全保护程度，更取决于受敌手关注的程度。物联网应用示范系统受敌手关注程度不高，因此发生的安全事故也不多，即使发生这样的安全事故，由于重要程度不高，其所造成的影响也小。

但是，工业物联网系统如果遭受入侵攻击，所造成的损失会更大。2010 年震网病毒对伊朗核电站入侵造成的损失，2015 年乌克兰核电站入侵事件的影响，都大于这次 DDoS 攻击事件。可能有人会说伊朗核电站不是工业物联网系统，但这并不影响工业物联网系统对攻击者的吸引力。因为对入侵者来说，入侵工业物联网系统，比入侵其他行业的物联网系统，能引起更大的关注，或者获得更多利益。随着智能制造技术的推进，德国“工业 4.0”战略的实施，和“中国制造 2025”政策的落实，越来越多的工业企业会选择使用工业物联网系统，用最新技术迎接新时代先进工业生产的竞争。

因此，保护工业物联网系统的安全，是物联网安全目标的重中之重。

### 3.1.6 工业物联网系统安全建设方案—独立监控网

毋庸置疑，不同的工业物联网系统会采取不同的安全防护措施，但安全体系有共同之处。基本的安全防护体系包括预防（防止非法入侵）、检测（万一预防失败，则在系统内检测是否有非法入侵行为）、响应（如果查到入侵，应采取什么行动）、恢复（对受破坏的数据和系统，如何尽快恢复）等阶段。

但是，一些高级入侵可能会完全控制系统，是系统失去自我检测能力，更不用说响应和恢复了。当然，有时候恢复过程是在入侵破坏行为发生后通过人工干预方式来完成。但检测和响应就需要系统本身的能力了。对于一些关键系统，需要额外的力量来辅助其完成检测与响应。许多工业物联网系统就是这样的关键系统，因此我们建议使用辅助检测系统，一个独立于工业物联网系统之外的检测或监控系统，通过对工业物联网系统的数据进行分析，判断系统是否遭受入侵。在这种情况下，即使工业物联网系统本身在入侵控制下失去自我检测能力，外部的检测系统也可以独立工作。这是工业物联网系统和其他重要物联网系统特有的需求，我们称之为独立监控网络。独立监控网络的主要工作是“检测”，如果需要“控制”功能的话，建议在人工干预（即人工确认）情况下开启。

这种独立监控网络的工作目标单一，一般无需联网，因此其本身遭受网络攻击的可能性非常小。监控网络所使用的设备可以及时更新系统，特别是更新最新发现的漏洞信息，从而比工业物联网系统本身具有更高的防护能力。可以使用在线更新（如果联网的话）或离线更新（工作人员现场操作）的方式进行，不影响工业物联网系统的正常运转，只影响检测网络设备本身在更新过程中的工作状态。

## 3.2 工业物联网漏洞分析

随着工业物联网的快速发展，工业物联网漏洞逐步成为网络空间的关注重点之一。工业物联网漏洞也呈现出了较快的增长趋势。根据 ICS-CERT 上的漏洞统计，从 2011 年~2015 年是工业物联网暴露漏洞快速增长的阶段。其中 2014 到 2015 年工业物联网暴露的漏洞从 249 迅速增加到了 371，增长率为 49%。而 2016 年前 2 个季度美国报告的工业物联网关键基础设施漏洞超过 600 个，工业物联网漏洞增长了 60% 以上。

### 3.2.1 工业物联网漏洞分布

#### 3.2.1.1 按威胁类型

按照漏洞造成的危害，我们将工业物联网漏洞分为越权执行、越权写入、越权读取、拒绝服务四大类威胁。

(1) 越权执行，指的是缓冲区溢出、命令执行、SQL 注入等可以直接对系统造成较大程度控制的漏洞。

(2) 越权写入，指的是能以某种方式在系统上写入文件、修改用户密码和系统配置等，但无法直接执行代码的漏洞。

(3) 越权读取，指的是能读取指定或任意文件、内存信息等的漏洞。

(4) 拒绝服务，指的是可导致进程崩溃、死锁等，使系统无法正常工作的漏洞。

根据我们对工业物联网漏洞按威胁类型的分析结果，危害最严重的越权执行类漏洞数量是最多的。

而通过对越权执行类漏洞的详细分析发现，这类漏洞又以缓冲区溢出类漏洞最多，占该类漏洞的一半以上。从 PC 软件上看，近年来缓冲区溢出类漏洞无论是绝对数量还是相对比例都呈下降趋势，而在工业物联网控制系统领域却出现较多缓冲区溢出类漏洞的现象，其主要原因可能是因为以前研究者对此类漏洞关注较少，所以很多软件中累积了大量此类漏洞，而当研究者们开始对这些软件进行检查时，积累多年的漏洞就暴露了出来。

另外 web 方面，很多软件为了实现通过浏览器控制管理的功能，自己实现了 WEB 服务器。我们发现这些自己实现的 WEB 服务器几乎都存在安全漏洞。

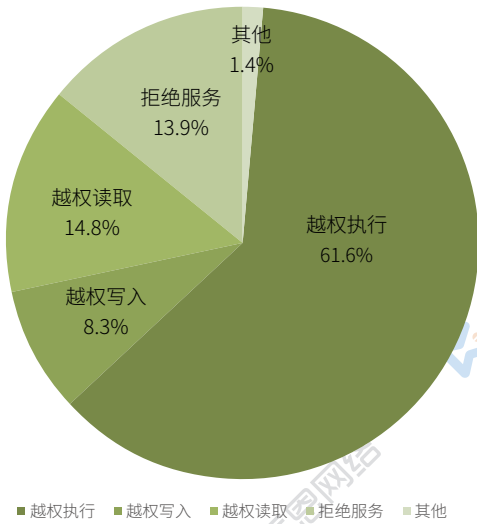


图 3-4 公开漏洞威胁类型分布图

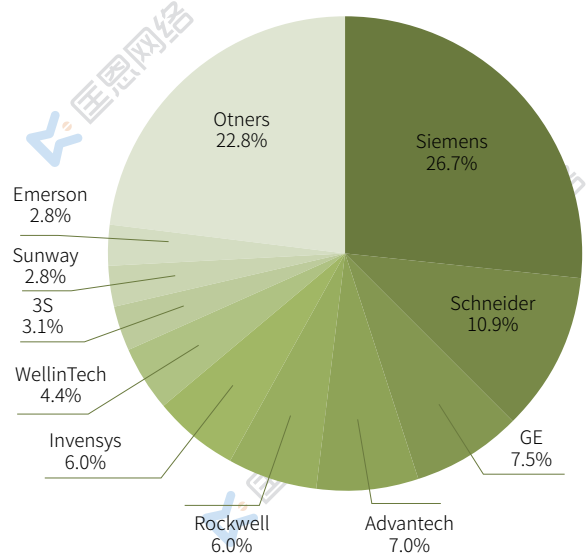


图 3-5 根据厂商的漏洞分布图

### 3.2.1.2 按设备厂商

工业物联网漏洞所涉及的工业控制系统厂商主要是国际著名的工业控制系统厂商。但国内也有两家工业控制系统厂商进入到了前十的行列，其中北京亚控科技发展有限公司（亚控科技，WellinTech）公布有 17 个漏洞，其中被 CVE 收录 14 个，北京三维力控科技有限公司搜集到 11 个相关漏洞，其中被 CVE 收录 2 个。厂商漏洞饼状图 3-5。

其中漏洞数排名前 10 的厂家漏洞情况如下。

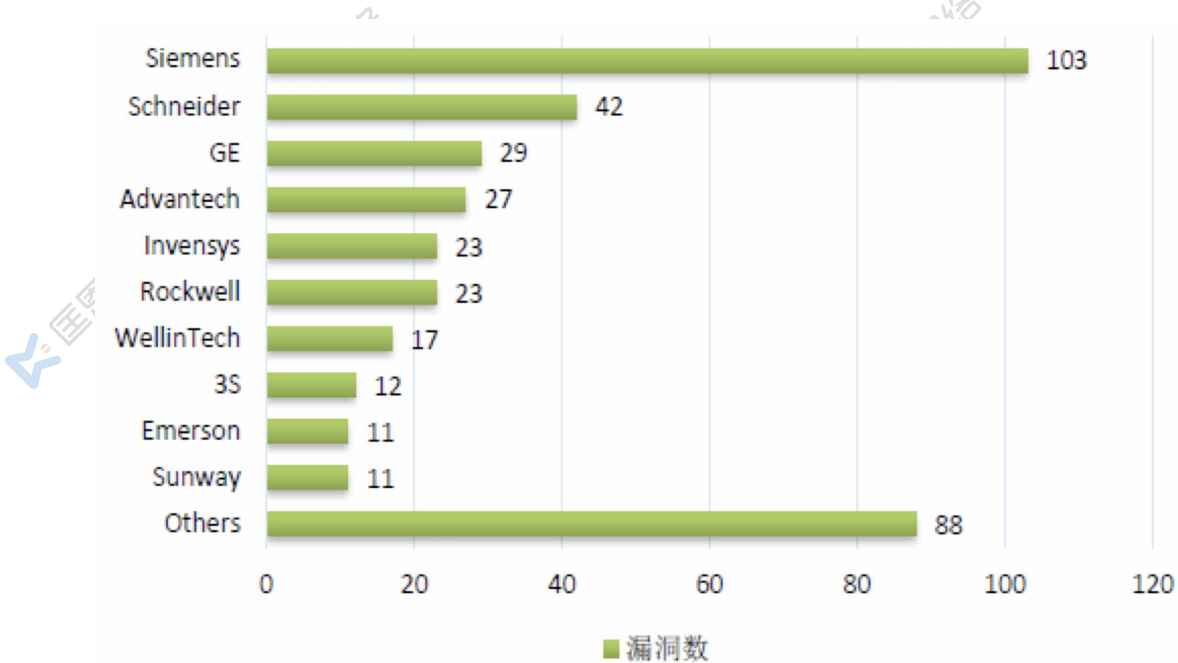


图 3-6 工业控制系统厂商漏洞数量 Top10



### 3.2.1.3 按工控组件类型

工业物联网按工控组件分为：scada、PLC、HMI、工业网络设备、RTU、组态软件等部分。按工业物联网组件类型的漏洞统计显示 scada、PLC、工控组态软件、工业网络设备漏洞是工业物联网上漏洞的重灾区。而其他漏洞部分包括了操作系统漏洞。

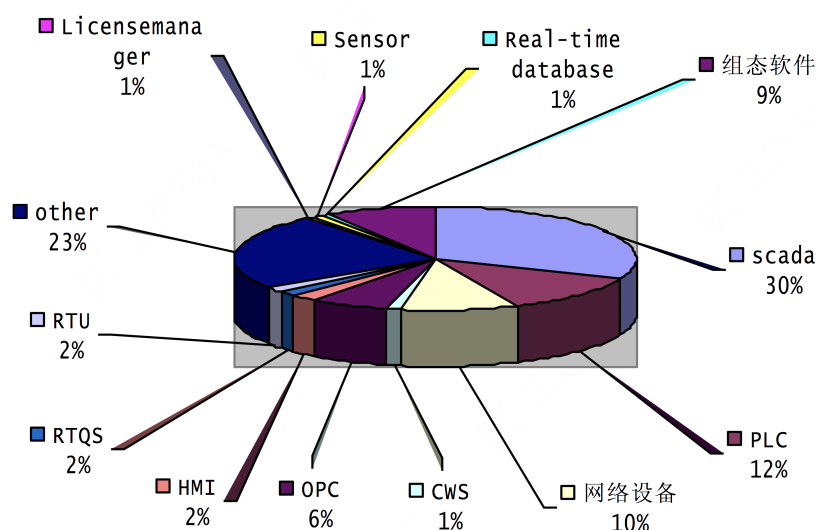


图 3-7 不同类型工控组件的分布情况

### 3.2.2 2016 年 top10 漏洞

在 2016 年所发现的漏洞中，根据漏洞危害程度的大小，我们选取了前 10 位介绍如下。

#### 1. Tcp 侧信道漏洞，漏洞编号：CVE-2016-5696。

▶ 漏洞描述：采用侧信道攻击方式，攻击者无需处在通讯路径中，同时被攻击的服务器和客户端不需要植入任何恶意程序。黑客利用漏洞可劫持未加密 web 流量。

▶ 推荐理由：攻击方式较为新奇，漏洞的发现者之一曹越，曾因为重现黑客凯文米特尼克的 tcp 劫持，获得“最大脑洞奖”。

▶ 参考链接：<http://www.freebuf.com/vuls/111943.html>

#### 2. Linux 远程利用漏洞。漏洞编号：CVE-2016-4484。

▶ 漏洞描述：攻击者通过长按 enter 键 70 秒或输入 93 次空白密码，就可获得访问根 initramfs shell 的权限。

▶ 推荐理由：攻击方式独特

▶ 参考链接：<https://www.newdefend.com/news/detail/205>

3. Linux 内核提权漏洞。漏洞编号：CVE-2016-5195。

▶ 漏洞描述：Linux 内核的内存子系统在处理写时拷贝（Copy-on-Write）时存在条件竞争漏洞，导致可以破坏私有只读内存映射。一个低权限的本地用户能够利用此漏洞获取其他只读内存映射的写权限，从而进一步导致提权漏洞。

▶ 推荐理由：一个潜藏长达九年之久的 linux 内核漏洞，影响范围广。

▶ 参考链接：<http://m.bobao.360.cn/learning/detail/3123.html>

4. 用户特权提升漏洞。漏洞编号：CVE-2016-8869& CVE-2016-8870

▶ 漏洞描述：利用这两个漏洞，攻击者可以在网站关闭注册的情况下注册并提升为特权用户

▶ 推荐理由：Joomla! 是全球排名第二的 CMS，影响范围颇大，且在中国以高校和政府为主要使用者。

▶ 参考链接：<https://bbs.aliyun.com/read/297832.html?spm=5176.2020520154.sas.146.7qFgVW>

5. 三星 smartthings 平台漏洞。漏洞编号：无 CVE 编号

▶ 漏洞描述：通过平台上的多个设计缺陷，利用软件漏洞可以解锁车门，未经主人允许可以设置新的虚拟按键，通过虚假的信息设置打开了智能锁，甚至还可以通过发送虚假信息触发火灾报警器以及关闭度假模式（主人离开后自动调节照明和安全的设置）等

▶ 推荐理由：2016 年典型的物联网安全漏洞之一

▶ 参考链接：<http://www.freebuf.com/news/103348.html>

6. Intel 芯片中的 BTB 组件漏洞。漏洞编号：无 CVE 编号

▶ 漏洞描述：Intel 芯片中的 BTB 组件漏洞：通过采取碰撞攻击，绕过 ASLR，60 毫秒实现系统攻击

▶ 推荐理由：攻击方式较为新奇

▶ 参考链接：<https://www.newdefend.com/news/detail/199>

7. 高通 “Quadrooter” 漏洞。漏洞编号：CVE-2016-2503, CVE-2016-2504, CVE-2016-2059, CVE-2016-5340

▶ 漏洞描述：黑客可以欺骗用户安装恶意应用，在应用安装后，黑客可以获得根权限，随后完全控制受影响的 Android 设备，包括数据和硬件。此外，“Quadrooter”还允许攻击者将应用程序的级别从 user-level（用户级别）升级到 root-level（root 级别），授予攻击者访问任意手机功能的权限。

▶ 推荐理由：影响全球超过 9 亿部安卓手机和平板电脑，黑客在入侵成功后，可以获得根权限，随之完全控制被入侵设备。

▶ 参考链接：<http://www.cnvd.org.cn/webinfo/show/3909>

8. 海康威视远程系统 XXE 漏洞。漏洞编号：无 CVE 编号。

▶ 漏洞描述：漏洞是在对非安全的外部实体数据进行行处理时引发的安全问题。

▶ 推荐理由：2016 年曝出的具有代表性的物联网安全漏洞之一。

▶ 参考链接：<http://www.freebuf.com/vuls/116613.html>

9. 思科 ASA 系列防火墙漏洞。漏洞编号：CVE-2016-6415

▶ 漏洞描述：存在于思科 IOS、思科 IOS XE 和思科 IOS XR 软件中的 IKEv1 数据包处理代码中，未经身份验证的远程攻击者可以利用这个漏洞获取到目标设备内存中的数据内容，同时意味着，该漏洞能够通过远程发送数据包来提取出思科 VPN 密钥。漏洞产生的原因主要是因为软件中负责处理 IKEv1 安全会话请求的那部分代码没有进行足够有效的条件审查。有超过 84 万思科设备受影响。

▶ 推荐理由：利用此漏洞，方程式组织开发利用工具“BENIGNCERTAIN”，而这只是方程式组织诸多利用工具之一。

▶ 参考链接：<http://www.freebuf.com/vuls/115207.html>

10. “BadTunnel”漏洞。漏洞编号：CVE-2016-3213

▶ 漏洞描述：该漏洞主要是一系列各自单独设计的协议和特性协同工作所导致。一个成功的漏洞利用需要伪造 NetBIOS（最初由 IBM 开发）连接，使不同设备上的软件通过局域网进行通信。即使攻击者不在目标网络中，仍然可以绕过防火墙和 NAT 设备，通过猜出正确的网络设备标识符，在网络中建立可信的交互，将网络流量全部重定向到攻击者的计算机。

▶ 推荐理由：Windows 历史上影响最广泛的漏洞，从 win95 到 win10 都受影响。

▶ 参考链接：<http://www.freebuf.com/vuls/106877.html>

### 3.3 2016 年工业物联网方面大事记

由于大部分工业物联网安全事件的相关报道和曝光程度较低，我们简要对 2016 年工业物联网的方面相关的重大事件和事故汇总如下。

事件名称	事件描述	事件总结
中国网络安全法发布	2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》。《网络安全法》草案于 2015 年 7 月 6 日至 2015 年 8 月 5 日在中国人大网上全文公布，并向社会公开征求意见。2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议表决通过了《中华人民共和国网络安全法》。	该法案 1.服务于国家网络安全战略和网络强国建设 2.助力网络空间治理，护航“互联网+” 3.构建我国首部网络空间管辖基本法 4.提供维护国家网络主权的法律依据 5.在网络空间领域贯彻落实依法治国精神。 标志着中国网络空间安全进入了法制化轨道，网络空间不再是无主之地。
工信部发布《工业控制系统信息安全防护指南》	11 月 11 日，为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28 号），保障工业企业工业控制系统信息安全，工信部近日制定并印发了《工业控制系统信息安全防护指南》（简称《指南》）。	工业控制系统信息安全防护指南意义重大，它对工业控制系统应用企业以及从事工业控制系统工作的企业起到了很好的指导作用，解决了大家面临的很多困惑和难题，并提供了很好的针对工业控制系统面临的网络安全问题的解决思路和落地技术手段，主要体现在： (1) 管理要求的精准化 (2) 技术要求的全面化 (3) 技术实现的具体化 (4) 业务兼容的可操作性 指南的印发，从全局考虑，以新的高度对工业企业的安全防护方案提出指导，将全面提升国内工业控制系统信息安全的整体防护水平。
美国发布《保障物联网安全战略原则》	11 月 15 日，在发布的“保障物联网安全的战略原则，版本 1.0”中，美国国土安全部（DHS）表示，物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉。该战略原则指出，未在最初设计阶段构建安全并采取基本安全措施“可能会造成制造商的经济成本、声誉成本或产品召回成本损失。虽然还没有建立解决物联网问题的判例法体系，但传统的产品责任侵权原则可以适用。”	物联网安全部分高级原则： 在设计阶段结合安全 启用安全更新和漏洞管理 建立在可靠的安全最佳实践之上 根据影响优先考虑安全措施 提升透明度 连接需仔细谨慎 物联网存在的许多漏洞能通过公认的安全最佳实践得到缓解。美国无法承担不安全物联网设备带来的影响，战略原则考虑到对关键基础设施、个人隐私和经济的潜在损害，为物联网安全标准发展做共享。
物联网恶意软件 Mirai	“Mirai”恶意软件造成美国网络大面积瘫痪，并且感染了高达 177 个国家的物联网设备，并且，这次事件也与美国总统大选有关。	信息安全正成为对一个国家的政治、经济等国家命脉产生影响的新武器。



PLC 蠕虫病毒	此蠕虫病毒是一个概念性 POC，适用于多个厂家的 PLC 设备，并且可以在一定规则范围内相互进行传播。	在工控安全甚至物联网安全领域，具有划时代意义，以往的病毒感染均需借助上位机，而 plc 病毒仅通过 plc 之间进行互相传播，且无法检测。
超 3200 万 Twitter 账号密码泄露	8 月 5 日，俄罗斯社交网站 VK.com 遭入侵，1.71 亿用户帐号信息泄露，泄露这些信息的黑客名为 Tessa88。而 Twitter 这次泄露的数据信息同样来自此人：超过 3200 万 Twitter 用户的登录信息正在暗网黑市出售，价格为 10 比特币（超过人民币 38000 元）。	社交网络个人信息泄露并被贩卖，人们的隐私权受到极大的侵犯，并存在进一步侵犯的风险。
曝苹果 App Store 逾千应用存漏洞或泄露用户隐私	2 月 1 日，据国外网站 Ibtimes 报道，知名网络安全公司 FireEye 日前警告称，由于一款名为“JSPatch”、可帮助开发者修改应用程序的软件上存在安全漏洞，导致苹果应用商店内 1000 多款使用了该框架的 iOS 应用处于黑客攻击危险之中。	移动设备是攻击者比较青睐的攻击目标，因为相对于笔记本和台式电脑而言，它们缺乏安全防护。因此应对移动设备更多的关注。
Operation GHOU (食尸鬼) 行动	卡巴斯基于 2016 年 6 月监测到了 Operation Ghoul (食尸鬼行动) 网络攻击，Operation Ghoul 针对 30 多个国家的工业、制造业和工程管理机构发起了定向渗透入侵。目前，卡巴斯基发现，有 130 多个机构已被确认为这类攻击的受害者。	从受害机构行业类型分布可以看出，攻击者主要以制造业和工业设备生产机构为主要渗透入侵目标。在此次攻击涉及行业多，攻击范围广的跨国攻击，国民的生活和财产受到极大影响。
乌克兰“电力门”分析报告	乌克兰攻击事件实际发生于 2015 年 12 月底，而针对乌克兰“电力门”事件的主要报道及分析结果则出现于 2016 年第一季度。2016 年 1 月 4 日，ESET 公司就发表文章称，乌克兰境内的多家配电公司设备中监测到的 KillDisk，由此怀疑使用了 BlackEnergy 后门，攻击者能够利用它来远程访问并控制电力控制系统。由于此事件是针对电力设备的攻击，对于国家关键基础设施的安全性具有非同寻常的意义，故存在巨大的风险。	针对此次乌克兰电网攻击事件，得出如下教训： 1. 安全防护体系存在漏洞，网络隔离不足。 2. 网络安全监测不力。 3. 网络和信息安全意识淡薄。 4. 不间断电源 (UPS) 同样需要安全防护。 5. 警惕不断涌现的攻击新技术。
伊朗黑客攻击美国大坝事件	2016 年 3 月 24 日，美国司法部公开指责 7 名伊朗黑客入侵了纽约鲍曼水坝的一个小型防洪控制系统。这些伊朗黑客可能为伊朗伊斯兰革命卫队服务，他们还涉嫌攻击了包括摩根大通、美国银行、纽约证券交易所在内的 46 家金融机构。	鲍曼大坝事件被旧事重提，这说明下一个惊动人们的坏消息很有可能是黑客可以控制工业系统并且掌控开关了。关于国内网络安全，当局（和安监局）不用在意潜在威胁，而是应该更加关注现有安全，例如如何正确维护基础设施系统。

工业物联网控制系统设计之初是为了完成各种实时控制功能，并没有考虑到安全防护方面的问题，通过网络互联将他们暴露在互联网上，无疑将给他们所控制的关键基础设施、重要系统等都带来巨大的安全风险和隐患。从近几年网络攻击的发展趋势来看，目前工业控制系统遭受的网络攻击已经成为各国政府所面临的严重的国家安全挑战之一。

## 3.4 我国对工业物联网的安全相关法规与政策

广义的工业物联网系统包括工业控制系统（以工业生产系统为主）、工业监控系统和工业管理系统等。由于工业物联网的特殊性，一些安全政策的制定是专门针对工业物联网系统的，也有一些政策是针对包括工业物联网系统在内的，或为物联网提供基础服务的网络系统而制定的。

### 3.4.1 我国工业控制系统安全法规与政策

2016 年，我国的网络安全基础工作进一步深化，政策环境明显改善，关键基础设施风险评估和安全保障、新兴信息技术安全预警工作取得了突破性的进展。国家信息通报机制得到进一步完善，积极开展了专题研究和技术检测工作。

为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》文件精神，应对新时期工控安全形势，提升工业企业工控安全防护水平，2016 年 10 月，工业和信息化部印发《工业控制系统信息安全防护指南》，指导工业企业开展工控安全防护工作。

《指南》坚持“安全是发展的前提，发展是安全的保障”，以当前我国工业控制系统面临的安全问题为出发点，注重防护要求的可执行性，从管理、技术两方面明确工业企业工控安全防护要求。编制思路如下：

(1) 落实《国家网络安全法》要求：《指南》所列 11 项要求充分体现了《国家网络安全法》中网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置等法规在工控安全领域的要求，是《国家网络安全法》在工业领域的具体应用。

(2) 突出工业企业主体责任：《指南》根据我国工控安全管理工作实践经验，面向工业企业提出工控安全防护要求，确立企业作为工控安全责任主体，要求企业明确工控安全管理责任人，落实工控安全责任制。

(3) 考虑我国工控安全现状：《指南》编制以近五年我部工控安全检查工作掌握的有关情况为基础，充分考虑当前工控安全防护意识不到位、管理责任不明晰、访问控制策略不完善等问题，明确了《指南》的各项要求。

(4) 借鉴发达国家工控安全防护经验：《指南》参考了美国、欧盟、日本等发达国家工控安全相关政策、标准和最佳实践做法，对安全软件选择与管理、配置与补丁管理、边界安全防护等措施进行了论证，提高了《指南》的科学性、合理性和可操作性。

(5) 强调工业控制系统全生命周期安全防护：《指南》涵盖工业控制系统设计、选型、建设、测试、运行、检修、废弃各阶段防护工作要求，从安全软件选型、访问控制策略构建、数据安全保护、资产配置管理等方面提出了具体实施细则。

《指南》坚持企业的主体责任及政府的监管、服务职责，聚焦系统防护、安全管理等安全保障重点，提出了 11 项防护要求，具体如下：

#### (1) 安全软件选择与管理

- 在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。
- 建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。

#### (2) 配置和补丁管理

- 做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计。
- 对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。
- 密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证。

#### (3) 边界安全防护

- 分离工业控制系统的开发、测试和生产环境。
- 通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。
- 通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

#### (4) 物理和环境安全防护

- 对重要工程师站、数据库、服务器等核心工业控制软硬件所在区域采取访问控制、视频监控、专人值守等物理安全防护措施。

- 拆除或封闭工业主机上不必要的 USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

### (5) 身份认证

- 在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理。对于关键设备、系统和平台的访问采用多因素认证。

- 合理分类设置账户权限，以最小特权原则分配账户权限。
- 强化工业控制设备、SCADA 软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令，定期更新口令。
- 加强对身份认证证书信息保护力度，禁止在不同系统和网络环境下共享。

### (6) 远程访问安全

- 原则上严格禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务。

- 确需远程访问的，采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略。

- 确需远程维护的，采用虚拟专用网络（VPN）等远程接入方式进行。
- 保留工业控制系统的相关访问日志，并对操作过程进行安全审计。

### (7) 安全监测和应急预案演练

- 在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。
- 在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。
- 制定工控安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。

- 定期对工业控制系统的应急响应预案进行演练，必要时对应急响应预案进行修订。

### (8) 资产安全

- 建设工业控制系统资产清单，明确资产责任人，以及资产使用及处置规则。



- 对关键主机设备、网络设备、控制组件等进行冗余配置。

#### (9) 数据安全

• 对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评估结果对数据信息进行分级分类管理。

- 定期备份关键业务数据。
- 对测试数据进行保护。

#### (10) 供应链管理

• 在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。

- 以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。

#### (11) 落实责任

• 通过建立工控安全管理机制、成立信息安全协调小组等方式，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。

### 3.4.2 行业领域工控网络安全法规与政策

各行业密切跟踪网络安全发展动态，紧密围绕国家信息化和信息安全发展战略，实施了一系列安全措施和举措，逐步提升了信息安全防护水平。

#### (1) 电力行业

国内电力行业是工控网络安全工作的先行者，开展了一系列的安全防护工作，首先体现在法规的制定完善以及设备安全隐患排查及漏洞的整改上。

- 2005 年 5 号令《电力二次系统安全防护规定》；
- 2007 年 34 号文《关于开展电力行业信息系统安全等级保护定级工作的通知》；
- 2007 年 44 号文《电力行业信息系统等级保护定级工作指导意见》；
- 2012 年 62 号文《电力行业信息系统安全等级保护基本要求》；
- 2013 年国能综安全〔2013〕387 号文《关于开展电力工控 PLC 设备信息安全隐患排查及漏洞整改工作的通知》；

- 2014 年，国家发改委第 14 号令颁布《电力监控系统安全防护规定》；
- 2015 年，国家能源局下发 36 号文《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》。

电监会 5 号令是专门针对电力二次系统安全防护的指导性文件，并且电监会（现电监会职能已经并入能源局）是定期对电力企业进行安全检查，对于严重违背电监会 5 号令精神的企业要求限期整改，并从调度侧严格规范电力企业执行电监会 5 号令，如果出现限期整改仍然无法达标的企业，要限制上网，所以，从电力企业自身的业务需求出发，二次系统安全防护非常重要，并且必须遵照 5 号令的要求来执行。电监会于 2007 年发布关于开展电力行业管理信息安全等级保护定级工作的通知，要求在电力企业中开展等级保护，要求按照电力行业定义的不同等级的系统进行定级工作。从发电企业实际的情况看，大部分的重点电厂已经完成了等保定级和相关的安全建设。

从国家出台的针对工控安全的政策开始，各个发电集团已经开始考虑如何来有效的开展工控安全的建设。受国家能源局委托华能在 2012 年和 2013 年陆续对一些电厂的控制设备进行了漏洞整改，从整改的过程中也积累了大量的工控系统安全建设的经验。利用已有的工控安全建设的经验，通过与现有的工控安全技术进行有效结合，来加强在工控安全方面的建设，现阶段是华能和各个发电集团在未来工控安全建设方面的一个重要的方向。各个发电集团在日常的安全考核中，已经把工控安全列入到日常的安全考核项目中。一些发电集团已经开始着手针对工控安全从整个集团的角度来考虑如何构建起一套行之有效的管控措施。一些省级电力公司已经开始在一些电厂尝试引入一些新的方法和思路来构建工业控制系统安全，如在 SIS 系统的边界处，通过监听等方式结合数据分析平台，制定相关的工控系统安全考核基线，形成一整套针对工控系统的安全预警机制。

2015 年 4 月国家能源局发布了《电力企业网络与信息安全专项监管报告》。报告显示，电力企业网络与信息安全形势保持了持续稳定态势，保证了电力行业重要信息基础设施安全、稳定、高效运行。

## （2）石油 / 煤化工行业

石油 / 煤化工行业信息化经过多年的持续建设，已经行成覆盖其上中下游全部企业、一体化的网络系统以及配套的信息化基础设施平台，信息系统已经成为其生产运营和经营管理的“中枢神经系统”。

早在 1999 年，国家石油和化学工业局在广泛调查研究的基础上，总结了石油化工厂的设计经验，吸收了国外标准的有关内容，编制发布了《石油化工分散控制系统设计规范》（SH/T3092-1999），对 DCS 系统的软硬件配置、应用软件组态及有关安装方面提出了技术规定。

2011 年,工业和信息化部发布《关于加强工业控制系统信息安全管理的通知》(工信部协[2011]451 号),对选择工业控制系统设备使用及相应安全防护措施提出明确要求。2012 年,国务院发布《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》(国发〔2012〕23 号),要求确保能源、交通等涉及国计民生的重要信息系统和基础信息网络安全,保障电力、水力、石油石化、油气管网等重要领域工控系统安全。2013 年,石化行业相应制定了《石油化工安全仪表系统设计规范》(GB/T 50770-2013),对石油化工企业安全仪表系统的工程设计、制造和操作维等进行了规定。2014 年 12 月,工控系统信息安全国家标准 GB/T30976-2014 首次发布,基本满足工业控制系统的用户、系统集成商、设备生产商等各方面的使用。国家标准的发布,极大地促进了工控系统信息安全的发展。目前,国家正在对工业控制系统测量和控制、专用防火墙、测控终端、通信网络和信息安全验收等内容编制通用技术标准,这些标准的发布和实施,将为我国能源行业工控系统信息安全提供有力的技术支撑。

目前,煤化工企业普遍采用基于 ERP/SCM、MES 和 PCS 三层架构的管控一体化信息模型,MES 处于企业信息系统 ERP/SCM 和过程控制系统的中间位置。MES 系统在整个信息系统中主要担当了两个方面的作用:一是数据双向通道的作用。即通过 MES 系统的实施,可以有效弥补企业 PCS 层及 ERP/SCM 层之间的数据间隙,由下至上,通过对底层 PCS 层数据的搜集、存储及校正,建立过程控制数据层次上的数字化工厂,结合生产调度层次上的调度事件信息数据等,为上层 ERP/SCM 计划管理层提供准确统一的生产数据;由上至下,通过对实时生产数据的总结,上层 ERP/SCM 层可以根据未来订单及现阶段生产状况调整生产计划,下发 MES 层进行计划的分解及产生调度指令,有效指导企业生产活动。因此,MES 系统在数据层面上,起到了沟通 PCS 层和 ERP/SCM 层的桥梁作用,并保证了生产数据、调度事件等信息的一致性及准确性。企业出口由于对通讯速率及带宽的需求,采用 IT 防火墙进行网络边界防护,通过策略制定,保障企业办公网络用户对互联网资源的合法访问,以及阻止来自互联网未经授权对企业办公网络的非法访问。

在产品方面,包括煤化工在内的国内能源与制造行业工控安全市场处在刚起步的前期阶段,国家发改委、工信部等主管部委也通过设立专项基金,以资助国内科研院所、企业的工控安全技术与产品研发及产业化,并力争在工控安全技术与装备领域加快缩短与国外的差距,最终逐步摆脱对国外产品的依赖。

部分国内骨干石化企业,根据国家的相关政策和要求,以及自控应用的经验,也制定摸索出了一系列行之有效的企业制度与标准。如中石化针对工控系统,先后制定了《中国石化仪表设备管理规定》、《中国石化过程控制系统病毒防治管理办法》、《联锁保护系统管理规定》、《分散型控制系统(DCS)技术规定》、《安全仪表系统(SIS)技术规定》、《仪表检维修规程》等等,这些制度、标准规范的制定,为石化企业工控系统的安全保护起到了至

关重要的作用。同时，根据功能安全标准的要求，中石化还对炼化装置的安全仪表系统进行 SIL 评估，根据评估的结果对系统进行完善，并与合肥通用机械研究院合作，共同研究石化仪表设备的全生命周期问题。相信这些措施的实施，将为完善我国化工行业工控系统管理标准体系作出积极贡献。

此外，我国石化行业围绕工控系统的安全保护的宣传教育，定期组织仪表技术竞赛，开展仪表管理制度及技术规范、控制网络技术培训、防雷及抗干扰技术培训、功能安全技术、以及有针对性的系统维护与系统组态等技术培训，不断强化工控系统操作人员和维护人员的安全意识和专业技能。

### (3) 制造业

2016 年 11 月，美国国家标准与技术研究所（NIST）发布《制造业与工业控制系统安全保障能力评估》草案。这份草案的评估工作为其规划的思想实施流程中的第一部分——其中每项流程都将产生一份名为《设计参考》的实践性指南——旨在帮助制造商们利用各类商业化网络安全工具以安全方式设置自身系统。

其中将涵盖的四大议题包括：

- 行为异常检测——用于监控计算机网络，查找其中的异常流量或者其它可疑现象；
- ICS 应用程序白名单——仅允许经过授权的应用程序在 ICS 系统之上运行；
- 恶意软件检测与缓解——发现并阻止恶意程序；
- ICS 数据完整性——确保由 ICS 设备生成的数据能够准确反映机器内部的实际情况。

### (4) 煤炭行业

中国煤炭信息协会信息化分会组织有关单位和大型煤炭企业编制了《煤炭信息化十二五发展规划》中第四条提出：


“根据国家网络与信息安全法律法规，建立煤炭行业信息安全标准体系和认证认可体系，在大型企业推广实施信息安全等级保护、风险评估等制度。推进煤炭行业安全可控关键软硬件应用推广，加强企业信息网络安全监测、管控能力建设，确保基础信息网络安全和重点信息系统安全。推进行业信息安全保密基础设施建设，重点企业构建信息安全保密防护体系。加强行业、企业门户网站安全管理，确保网络与信息安全。”

2016 年版的《煤矿安全规格》中第四百八十九条规定提出：“监控网络应当通过网络安全设备与其他网络互通互联。”



### (5) 铁路行业

在安全管理规范方面，2013 年 7 月 24 日国务院第 18 次常务会议通过《铁路安全管理条例》，自 2014 年 1 月 1 日起施行。该管理条例第七十三条规定：铁路管理信息系统及其设施的建设和使用，应当符合法律法规和国家其他有关规定的安全技术要求。铁路运输企业应当建立网络与信息安全应急保障体系，并配备相应的专业技术人员负责网络和信息系统的安管理工作。同时，2016 年 2 月开始执行的《中国铁路总公司网络安全管理办法》，对网络安全防护方面给出了具体的规范和执行办法，该规范分别从运维安全管理、访问授权管理、数据安全、终端安全管理、信息资产安全管理、人员安全管理、网络安全信息通报、检查与考核等方面给出具体的管理和执行方法，将网络安全提升到一个新的高度。



# 第四章

## 物联网安全 保护技术

## 4.1 物联网感知层安全保护技术

### 4.1.1 物联网感知层的构成

物联网感知层的主要功能是实现对信息的采集、识别和控制。感知层从设备功能上又可以分为感知设备子层和通信设备子层。感知设备子层通过传感器、RFID 读写器、摄像头、GPS 等模块实现温度、湿度、风向、标签、道路拥塞等信息的感知和获取。感知设备子层主要涉及传感器、条形码、RFID、音视频编解码、GPS 等技术。通信设备子层通过 IEEE802.15.4、3G、RF 等无线模块或 xDSL、FTTX 等有线模块实现信息的采集和传输。通信设备子层主要涉及 ZigBee、GSM/TD-SCDMA 等技术。

由于通信设备子层使用的技术都基于现有成熟的通讯网络技术，将不做进一步的介绍。下面重点介绍几种感知设备子层的技术。

#### (1) 传感器

中华人民共和国国家标准 GB/T 7665—2005 对传感器 (Transducer/Sensor) 的定义是：能感受规定的被测量并按照一定的规律转换成可用输出信号的器件或者装置，通常由敏感元件和转换元件组成。传感器的分类一般有按工作原理分类、按被测量分类、按敏感材料分类、按能量关系分类、按应用范围分类。传感器是物联网感知层的主要信息感知设备，近二十年来，传感器的发展非常迅速，目前全球传感器的种类已超过 2 万余种，常见的有温度、压力、湿度、光电、霍尔磁性传感器等。温度传感器基于物质的各种物理性质随温度变化的规律，把温度变化转换为电信号。压力传感器在受到外部压力时会产生一定的内部结构的变形或位移，进而转化为电特性的改变，产生相应的电信号。湿度传感器主要包括电阻式和电容式两个类别。电阻式湿度传感器也成为湿敏电阻，利用氯化锂、碳、陶瓷等材料的电阻率的湿度敏感性来探测湿度。电容式湿度传感器也称为湿敏电容，利用材料的介电系数的湿度敏感性来探测湿度。光传感器可以分为光敏电阻以及光电传感器两大类。光敏电阻主要利用各种材料的电阻率的光敏感性来进行光探测。光电传感器主要包括光敏二极管和光敏三极管，这两种器件都是利用半导体器件对光照的敏感性。霍尔传感器是利用霍尔效应制成的一种磁性传感器。霍尔传感器结合不同的结构，能够间接测量电流、振动、位移、速度、加速度、转速等等，具有广泛的应用价值。随着新材料、新工艺、微细加工技术的发展使传感器逐步向微型化、多功能、智能化、集成化、多融合、网络化的方向发展。

#### (2) 图形码

图形码是一种信息的图形化表示方法，可以把信息制作成条形码或二维码，然后用相应的扫描设备把其中的信息输入到计算机中。二维码的优点是信息容量大，译码可靠性高，纠

错能力强，制作成本低，保密与防伪性能好。作为一种比较廉价实用的技术，图形码在今后一段时间内还会在物联网的各个行业中得到应用。

### (3) RFID

射频识别 (RFID: Radio Frequency Identification) 作为物联网标志性的感知设备之一，俗称电子标签。RFID 射频识别是一种非接触式的自动识别技术，主要用来为各种物品建立唯一的身份标识，是物联网的重要支持技术。RFID 的系统组成包括：电子标签、读写器 (阅读器)，以及作为服务器的计算机。其中，电子标签中包含 RFID 芯片和天线。每个 RFID 芯片中都有一个全球唯一的编码；在为物品贴上 RFID 标签后，需要在系统服务器中建立该物品的相关描述信息，与 RFID 编码相对应。当用户使用 RFID 阅读器对物品上的标签进行操作时，阅读器天线向标签发出电磁信号，与标签进行通信对话，标签中的 RFID 编码被传输回阅读器，阅读器再与系统服务器进行交互，根据编码查询该物品的描述信息。

### (4) 多媒体采集器

多媒体采集器作为未来物联网感知层常用的感知设备之一，泛指音频、视频、图像等信息的采集装置，如：摄像头、话筒、微型照相机等。随着物联网多媒体业务的逐步开展，多媒体采集器的作用日益明显。各种实体的采集器以数字化信号的方式，对一种或者多种多媒体信息，进行实时或准实时的获取和采集。

### (5) GPS

全球定位系统 (GPS: Global Positioning System) 技术具有全天候、高精度和自动测量等特征，被广泛的应用于物联网的位置定位之中。尤其对于网关节点和其他关键节点，使用 GPS 定位进行精确的地理定位是感知层的必然选择。

感知层在物联网中起着信息来源的关键作用，感知层设备的质量将直接影响物联网的可靠性和高效性，下文将针对感知层设备的测试进行进一步的研究。

### (6) ZigBee 协议

ZigBee 协议是基于 IEEE802.15.4 标准的低功耗局域网协议。根据国际标准规定，ZigBee 协议是一种短距离、低功耗的无线通信技术。其特点是近距离、低复杂度、自组织、低功耗、低数据速率。主要适合用于自动控制和远程控制领域，可以嵌入各种设备。简而言之，ZigBee 协议就是一种便宜的，低功耗的近距离无线组网通讯技术。ZigBee 协议从下到上分别为物理层 (PHY)、媒体访问控制层 (MAC)、传输层 (TL)、网络层 (NWK)、应用层 (APL) 等。其中物理层和媒体访问控制层遵循 IEEE 802.15.4 标准的规定。

#### 4.1.2 传感器网络安全保护技术

随着通讯技术和计算机技术的飞速发展，人类社会已经进入了网络时代。智能传感器的开发和大量使用，导致分布式控制系统对传感信息的交换提出了新的要求，单独的传感器数据采集已经不能适应现代控制技术和检测技术的发展，取而代之的是由分布式数据采集系统组成的传感器网络。传感器网络是由一组传感器以一定的方式构成的有线或无线网络，其目的是协作地感知、采集和处理网络覆盖区中感知对象的信息，它综合了传感器技术、嵌入式技术、分布式信息处理技术和通信（有线 / 无线）技术。

传感器单独适用的场合越来越少，更多的传感器系统是将传感器与网络紧密结合在一起成为传感器网络。网络传感器的发展方向是从有线形式发展到无线形式，从现场总线形式发展到无线传感器网络形式，最终融入互联网，形成物联网。

第一代传感器网络出现在 20 世纪 70 年代，是由传统的传感器组成的测控系统，采用点对点传输的接口规范。例如，工业控制系统开始统一使用二线制 4~20mA 电流和 1~5V 电压标准进行信号传输。

第二代传感器网络是基于智能传感器的测控网络。到 20 世纪 80 年代，微处理器的发展和与传感器的结合，使传感器具有了计算能力，随着节点智能化的不断提高，现场采集的信息量不断增加，传统的通讯方式已成为智能传感器发展的瓶颈。在分布控制系统中，数据通信标准 RS232、RS422、RS485 等开始采用。但是智能传感器与控制设备之间仍然采用传统的模拟电压或电流信号进行通信，没有从根本上解决布线复杂和抗干扰差的问题。

第三代传感器网络是基于现场总线的智能传感器网络。20 世纪 80 年代末到 90 年代初，现场总线技术的推出，将智能传感器的通讯技术提升到一个新的阶段。现场总线是连接智能化现场设备和主控系统之间全数字、开放式、双向通信网络。现场总线技术利用数字通讯代替了传统的模拟信号，有效降低了系统的成本和复杂度，分层的体系结构实现了分布式智能。现场总线的种类较多，例如 CAN、Lonworks、Profibus、HART、FF 等，它们各有特点和不同领域的应用价值。但是，每种现场总线都有自己的通讯标准，互不兼容，这给系统的扩展和维护带来了不利影响。现场总线控制系统可认为是一个局部控制网络，基于现场总线的智能传感器只实现了某种现场总线的通讯协议，还没有实现真正意义上的网络通讯协议，并且总线协议在局部网络中明文传输，一旦受到攻击能够直接控制传感器设备。

第四代传感器网络是无线传感器网络（Wireless Sensor Network, WSN）。它的定义是：由大量、静止或移动的传感器节点，以自组织和多跳的方式构成的无线网络，目的是以协作的方式感知、采集、处理和传输在网络覆盖区域内被感知对象的信息，并把这些信息发送给用户。无线传感器网络系统通常包括传感器节点（sensor node）、汇聚节点（sink node）和管理节点。从网络节点来看，大量传感器节点随机部署在监测区域内部或附近，能够通过



自组织方式构成网络。传感器节点监测的数据沿着其他传感器节点逐跳地进行传输，在传输过程中监测数据可能被多个节点处理，经过多跳后路由到汇聚节点，最后通过互联网或卫星到达管理节点。

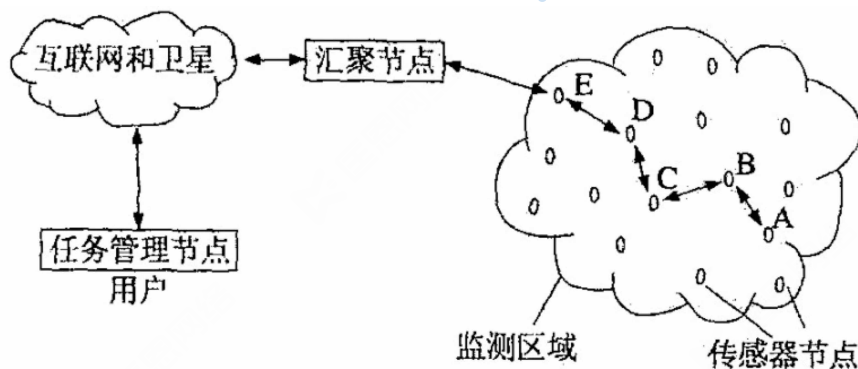


图 4-1 传感网与互联网连接时的信息传输

由于无线传感器网络是无线通信，攻击者可轻易在该网络的任务域里监听信道，向信道里注射比特流，重放以前监听到的数据包。传感器是随机部署在无人值守的外部空间，攻击者可轻易捕获该节点，重写内存，或者用自己的传感器来替代该节点，通过冒充以获得数据信息。由于每个传感器处理能力、存储能力和通信能力都相对较弱，并且无线收发器的接受距离短，可轻易受到资源强大的攻击点的破坏。该类攻击点可以利用信号发送距离远的特点，在全网范围内实施攻击，监听整个无线传感器网络的数据传输。同时利用其强大的功率和数据发送能力，频繁向任务域里发送数据包，阻塞传感器使其失效。攻击点能够利用自身资源性能方面的优势，伪装成无线传感器网络的基站，或者改变传感器的路由使自身成为蠕虫洞。传感器由于受到攻击点的破坏或者自身耗尽能量退出该网络时，该网络的路由和密钥管理机制也会发生相应的变化。

下面通过图示给出一些实例。



图 4-2 北京某校门的信息重放攻击

Sector	Block	Code
0	0	FB918F7FAA0804006263646566676869
0	1	00000000000000000000000000000000
0	2	00000000000000000000000000000000
0	3	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
1	0	00000000000000000000000000000000
1	1	00000000000000000000000000000000
1	2	00000000000000000000000000000000
1	3	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
2	0	000010001507100710180300FFFFFFFF94
2	1	00003000075483000010000080000D9
2	2	000040000744970000100000070000C6
2	3	64492185218608778F69907CEC41CA14
3	0	00000000000000000000000000000000
3	1	00000000000000000000000000000000
3	2	00000000000000000000000000000000
3	3	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF

图 4-3 北京某学校校园卡记录信息

Hex	Flight	Altitude	Speed	Lat	Lon	Track	Messages	Seen
ad67bb		11800	0	0,000	0.000	0	34	1
ada521	HAL15	9825	283	0,000	0,000	265	6	9
a77a4f		36000	379	34.199	-119.246	275	81	14
a9bb70		28625	0	0,000	0,000	0	37	3
a8bcf0		0	0	0,000	0,000	0	43	2
a8c45e		0	0	0,000	0,000	0	3	24
a70b4d		6825	0	0,000	0,000	0	22	27
a8b939		0	0	0,000	0,000	0	295	1
aa4199	456	19525	0	0,000	0,000	0	14	23
a4ce21	AAR202	7300	254	34.012	-118.444	83	923	0
71bc18		9825	273	34.030	-118.647	95	395	0
a8da40		0	0	0,000	0,000	0	71	34
a3dbe7		5425	0	0,000	0,000	0	41	1
a379af		0	0	0,000	0,000	0	61	0
a89216		36000	0	0,000	0,000	0	64	3

图 4-4 飞机 ADS-B 截获数据 (AM 131.550MHz 带宽 5kHz-8kHz)

#### 4.1.3 智能摄像头及其安全保护

网络摄像头简称 WEBCAM，英文全称为 WEB CAMERA，是一种结合传统摄像机与网络技术所产生的新一代摄像机，它可以将影像透过网络传至地球另一端，且远端的浏览者不需用任何专业软件，只要标准的网络浏览器（如 Microsoft IE 或 Netscape），即可监视其影像。

网络摄像头是传统摄像机与网络视频技术相结合的新一代产品，除了具备一般传统摄像机所有的图像捕捉功能外，机内还内置了数字化压缩控制器和基于 WEB 的操作系统，使得视频数据经压缩加密后，通过局域网，internet 或无线网络送至终端用户。而远端用户可在 PC 上使用标准的网络浏览器，根据网络摄像机的 IP 地址，对网络摄像机进行访问，实时监控目标现场的情况，并可对图像资料实时编辑和存储，同时还可以控制摄像机的云台和镜头，进行全方位地监控。网络摄像头国外品牌包括 AXIS、SONY、松下、IQinvision、三星、GE、霍尼韦尔、博世、Arecont Vision、ACTI、彩富、Brickcom；国内品牌包括海康、大华、朗池、黄河、艾普视达、帝视尼、蓝色星际、景阳、金三立、恒业国际等。

网络摄像头，也是网络空间中的一个节点。通过不同网络摄像头的特征进行搜索，就可以找到这些连接到网络空间的摄像头。再或者通过搜索引擎都是都可以找到这些设备的。因为这些网络设备是接入互联网的，这就导致了爬虫可以爬到他的一些管理页面等。

通过口令破解或者直接利用漏洞可以获得密码。利用摄像头的固件漏洞，直接编写exp，然后可以直接获得登陆所需的帐号和密码，甚至可以替换摄像头的画面。对于某些品牌的摄像头，黑客还能够通过交叉编译使其变成网络资源并占用。



图 4-5 北京某学校网络摄像头

常见的智能摄像头安全防护方法：

- (1) 更改设备初始密码，并采用复杂的数字与字母组合；
- (2) 确保网络防火墙打开，并及时更新安全软件；
- (3) 摄像头固件及时升级；
- (4) 修改智能摄像头网络信息，避免爬虫定位摄像头 IP；

对于智能摄像头厂商来说，需要对设备固件进行仔细的安全测试与漏洞挖掘，确保设备本身安全。

#### 4.1.4 智能网关节点的安全性

##### (1) Nest 及其安全分析。

Nest 成立于 2010 年，于 2011 年推出其第一代 Nest 智慧温控器，获得《华尔街日报》科技创新能源类大奖，最初在 Lowe's 及 Apple 的实体商店贩卖，而后于 2012 年开始与美国电力公司 Reliant Energy 合作，推出节约能源的方案，透过拓展不同的销售对象，Nest 的销售量快速成长，每月的销售量可达约 4-5 万台，可看作为智慧温控器的市场领导产品。

Nest 承袭 Apple 的设计理念，重新塑造温度控制器的外型，提供简易的操作接口，此外 Nest 重新定义温控器的功能，将原本仅是做为控制空调的设备，转变为帮助消费者进行能源管理的智慧家庭设备。

针对消费者，Nest 透过环境侦测、连网查询、学习机制等，以提供使用者各种节能的功能。包含 Auto-Schedule：根据用户的生活习惯调整温度；Auto-Away：当传感器侦测到无人在家时，自动调整空调；Nest Leaf：当温度达到能源效率时会出现绿叶图案，进一步引导鼓励节约能源；Airwave：透过风扇传播冷空气，以降低冷气压缩机的运行。透过以上模式协助用户节省家中空调所使用的能源。

此外，Nest 亦与电力公司合作，对于电力公司来说，用电量的淡旺季差异过大，对于电力的调配是很大的问题，因此 Nest 针对电力公司，并非以节约能源为目的提供服务，而是协助降低用电高峰期的电力使用量，透过其主要的演算技术 Auto-tune Technology，提供 Rush Hour Rewards 的服务，协助电力公司能在用电量较大的时段进行终端用户的用电调整，以达到降低电量尖峰期用电负荷的问题，维持供电量的稳定。



图 4-6 Nest 智慧温控器组件图



Nest 智慧温控器可以连接 Wi-Fi，然后将通过各种传感器收集到的数据自动整理并且生成报告传送到服务器中。该设备可以储存 2GB 的数据，通过内置的充电电池为由 Texas Instruments 生产的 Cortex M3 处理器提供动力。同时 Nest 还有两个运动传感器，能够第一时间检测到家中是否有人活动。与所有的硬件产品一样，Nest 智慧温控器也存在漏洞。黑客通过 USB 与 Nest 设备连接，并且能够进入到开发者模式，上传恶意代码，修改用户数据，甚至可以获得设备最高权限。

目前 gtvhacker 组织在 GitHub 上已经发布了针对 Nest 设备的漏洞攻击脚本。

#### 4.1.5 智能移动终端的安全性保护

近年来，智能移动设备在数量上呈现出爆发式的增长态势，在性能上得到迅速发展。从智能手机到智能 PAD 等设备，在物联网系统的应用中起到重要作用，成为物联网系统中用户的智能移动终端。

智能移动终端是实现人机信息交互的核心部件。目前智能移动设备的操作系统主要有：Symbian，Android，iOS，Windows Mobile 等。根据市场占有情况，以 Android 系统为主。

Android 是由 Google 发布应用智能手机的操作系统，与 Symbian 和 Windows Mobile 类似，不同的是它完全开源，并且 Google 不断投入人力进行该系统的维护和升级。开发人员利用该系统平台可以很方便的进行二次开发应用。Android 应用程序开发是 Android 开发中最上面的一个层次，这些应用程序是完全的 Java 程序，他们构建在 Android 系统提供的 API 之上。Android 应用程序可以基于两种环境来开发，AndroidSDK 和 Android 源代码。Android 的进程沙箱隔离机制、应用程序签名机制、权限声明机制、访问控制机制、进程通信机制、内存管理机制能够满足应用程序对安全的需求。

对于企业用户来说，他们所关注的是一个能够彻底解决移动领域安全问题的方案。但是 Android 的安全问题很严重。如下列举了 Android 系统存在的几个安全问题：

- 成为恶意软件的首要目标。

据研究分析，高达 97% 的移动恶意软件将 Android 设备列为攻击目标，这也就意味着其他平台遭到恶意软件攻击的几率是相当低的，所以 Android 的安全性已经到了不得不改善的地步。

- 严重的碎片化问题。

“碎片化”是 Android 由来已久的问题，而这个问题到目前仍未得到解决。目前 Jelly Bean 是安装量最大的 Android 版本，占到了三分之二左右，但是还有不少设备在运行着 Android 2.2 Froyo、Android 2.3 Gingerbread 和 Android 4.0 Ice Cream Sandwich，而这



些老版本的系统并不具备新版本中的安全功能，所以将会有大量用户的设备存在遭受恶意软件骚扰和网络攻击的风险。

- 发生在 Windows 上的事情正在重演。

Android 生态系统中恶意软件的增长态势与早期的 Windows 非常相像。当年那些恶意的黑客就是看到有越来越多的人开始使用 Windows 操作系统时，就把注意力几乎全部转移到了 Windows 平台上。而目前在移动操作系统占据主导地位的 Android 自然会成为他们的首要攻击目标。

- 非授权应用商店存在隐患。

让人感到意外的是，谷歌旗下的 Play 应用商店并没有对 Android 设备的安全造成威胁，数据显示在 Play 应用商店中发现的恶意软件仅占到全部恶意软件的 0.1%。但是，当用户从非授权的应用商店下载应用之后，各种问题就出现了。针对这种情况，F-Secure 建议用户应该在非授权的应用商店下载应用。

- 恶意软件数量仍将增长。

虽然 Android 系统在不断升级更新，但安全问题似乎没有降低。相反，随着 Android 终端数量的增加，出现的针对 Android 的恶意软件数量仍在增加。

## 4.2 物联网网络传输层安全保护技术

物联网的网络传输层主要指具有广域网传输能力的网络，包括传统的互联网，移动通信网，以及近年来发展起来的低功耗广域网（LPWAN）。

### 4.2.1 互联网安全保护技术

互联网所使用的具有代表性的安全技术是 IP 层的安全协议 IPSec，传输层的安全协议 SSL、TLS，以及应用层安全协议（如 https，pgp，ssh 等）。

IPSec 和 TLS 加密技术在互联网中应用广泛，IPSec 提供了以下安全机制：认证头 AH、封装安全载荷 ESP 和密钥管理协议 IKE。认证机制使 IP 通信的数据接收和发送方确认真实身份，数据在传输过程中是否遭篡改。加密机制通过对数据进行编码来保证数据的 CIA 属性，主要应用端到端的传输以防数据在传输过程中被窃听。

传输层安全协议 TLS，以及其前身安全套接层 SSL 是一种安全协议，目的是为互联网通信，提供安全及数据完整性保障。采用 RSA 等非对称加密算法在浏览器、电子邮件、网上金融、

即时通信、VoIP、网络传真等应用程序中。

除上述两种安全加密协议外还是其它协议，如 SSH、PGP、SFTP 等协议，主要应用于安全配置管理和个人数据加密等场景。

互联网安全技术面临的挑战，如：OpenSSL 心脏出血、DROWN 等已知、未知漏洞威胁着互联网已有的安全技术。

#### 4.2.2 移动网络安全保护技术

移动通信网络主要包括 2G、3G、4G（LTE）以及正在发展中的 5G 技术。由于第一代移动通信网络主要用于语音模拟信号的传输，不具有数字信息处理能力，因此在物联网技术中不考虑。

##### 4.2.2.1 2G 网络安全

移动无线通信特点既容易让用户接入，也容易被窃听，所以安全性和移动通信密切相关。2G 网络是指第二代无线蜂窝电话通讯协议，是以无线通讯数字化为代表，能够进行窄带数据通讯。GSM 系统存在的安全隐患：

- (1) 单向认证，只有网络对用户的认证，没有用户对网络的认证，因此存在安全漏洞。
- (2) 非端到端加密，只在无线信道部分加密（即在 MS 和 BTS 之间），而固定网中采用明文传输。
- (3) 移动台和网络间信令信息高度敏感，需要完整性保护。在 GSM 网络中，没有考虑数据完整性问题，如果数据在传输的过程中被篡改也难以发现。
- (4) GSM 中使用的加密密钥长度是 64 bit，随着计算机的快速发展，可以在较短时间内被破解。

##### 4.2.2.2 3G 网络安全

第三代移动通信系统，即 3G 网络，相对于 2G 网络来说主要是采用了 CDMA 技术，扩展了频谱，增加了频谱利用率，提升了速率，更加利于 internet 业务，针对 GSM 存在的安全问题，3G 网络主要进行了如下改进：

- (1) 实现了双向认证。提供基站对 MS 的认证，也提供了 MS 对基站的认证，有效防止伪基站攻击。
- (2) 提供了接入链路信令数据的完整性保护（f9 算法）。
- (3) 密钥长度增加为 128 bit，改进了算法（f8 算法）。

(4) 3GPP 接入链路数据加密延伸至无线接入控制器 (RNC)。

(5) 3G 的安全机制还具有可拓展性, 为将来引入新业务提供安全保护措施。

(6) 3G 能向用户提供安全可视性操作, 用户可随时查看自己所用的安全模式及安全级别。

#### 4.2.2.3 4G(LTE) 网络安全

第四代移动通信系统, 即 4G 网络, 也称 LTE 网络, 是按照长期演进型架构设计的。虽然在功能上借鉴了 3G 网络的安全机制, 但还是有许多独特的方面。首先它不像 2G 和 3G 服务那样使用 TDM 和 ATM 回程, LTE 使用基于 IP 的回程。大量的基于 IP 的通信进入移动基础设施, 使它变得更易受到来自外部的攻击。LTE 网络的全 IP 架构带来了更多的安全风险。攻击者可以访问未加密的用户流量或网络控制信令。

随着公共接入微蜂窝基站部署的增加, LTE 网络面临更多的安全风险, 这些公共接入微蜂窝基站的部署主要购物、办公等公共服务的本地容量。这些安置在公共区域的小型设备面向大众, 无法得到像传统基站物理保护措施, 让攻击者更容易找到突破点来攻击网络。

LTE 网络架构和分组核心还面临其他安全挑战, 包括 SCTP 与 Diameter 传输和应用协议的封锁, 以及移动网络上来自不同网元的分布式拒绝服务攻击 (DDoS)。数据信令网关、移动包核心 (Mobile Packet Core) 和无线接入网络基础设施都有潜在的漏洞。

#### 4.2.2.4 5G 网络安全

随着第四代移动通信技术 LTE 的商业化应用, 对于下一代通信技术 (5G) 的研究也已经悄然展开。相较于 4G 网络, 5G 移动网络将带来更高的峰值速率体验、高密集用户连接的优质服务、泛在网络互联互通、更优质的用户访问体验以及实时而可靠的网络连接。5G 网络将带来更高的峰值 10G 带宽的极速体验、高密集用户连接的优质服务、泛在网络互联互通、更优质的用户访问体验以及实时而可靠的网络连接。但是 5G 网络的安全问题仍然处在研究阶段。

5G 网络技术相较于 4G 拥有更多的创新技术, 促进网络功能和拓扑结构的出现。4G 网络是对 3G 网络技术的扩展和演化, 通过 LTE/LTE-A 等技术的使用, 提高了网络带宽的利用率, 从而增强了网络的传输速度和用户体验, 并使传统的蜂窝数据网络 2G、3G 全面适应 IP 综合业务网络。但实质上, 4G 依然依赖传统网络通信为基础。5G 网络以功能为核心, 使用 SDN 软件定义网络、NFV 网络功能虚拟化及云计算等技术, 5G 网络在使用中通过接口可以实现软件定义、可编程、高动态扩展和极度灵活的特点。

5G 网络目前面临的安全威胁主要有以下几个方面:

- (1) NN 网络的动态性和兼容性, 在其它网络域中移动时可能被劫持和控制。
- (2) D2D 在发现机制和通信方法上, 可能存在身份认证及非法接入风险。
- (3) 接入设备的非唯一身份引发的安全问题。
- (4) 超高密度用户接入引发的其它安全威胁。
- (5) SDN 软件定义网络的相关安全性问题。
- (6) 信道租用引入的安全问题。
- (7) 异构融合引入的跨域安全性问题。

今年 11 月中旬, 华为在 3GPP RAN1 87 次会议上 5G 短码方案的讨论中, 战胜了高通主推的 LDPC 和法国主推 Turbo2.0, 凭借 Polar Code(极化码) 成为了 5G 控制信道 eMBB 场景的官方指定编码方案, 同时也是中国企业在无线信道标准制定中的一次突破性胜利。可以预见, 明年将在 5G 网络技术的研究方面取得快速发展。

#### 4.2.3 物联网专用网络 LPWAN 安全保护技术

低功耗广域网 (Low Power Wide Area Network, LPWAN) 技术是一种适合长距离无线通信的技术, 因为面向物联网应用而设计的, 因此具有低功耗特征。通过星型网络覆盖的, 支持单节点最大覆盖可通 100 公里的蜂窝汇聚网关的远程无线网络通讯技术。为实现此目标, 必须牺牲数据传输速率的性能指标, 这在物联网应用中是满足条件的, 因为物联网系统中所传输的数据一般都是小量数据。

该技术在将引领物联网在全球快速推广和应用, 具有远距离、低功耗、低维护成本等优点, 与短距离通信 WIFI、蓝牙、ZigBee、Z-wave 等现有技术相比, LPWAN 真正实现广域物联网低成本的时代。目前 LPWAN 技术没有形成统一的规范标准, Sigfox、LoRa、Telensa、PTC 等都是比较典型的 LPWAN 技术。LPWAN 本身是相对于以往 2G/3G/4G 等 WWAN 而言。目前在低功耗广域网领域, LoRa 和 NB-IoT 最为热门的两种技术, LoRa 技术由 Semtech 公司于 2013 年发布的一种全新无线技术, 相对于其它无线技术发展更快速, 完成了商业化推广。NB-IoT 是 3GPP 在 2014 年 9 月 RAN#65 会议中提出成立新的 SI 研究, 其主要基于 Cat.0 的基础上进一步研究更低成本、低功耗、更强覆盖的 LTE-MTC 技术, 即 NB-IoT。

在安全性方面由于 LoRa 只是作为一种低功耗远距离通信芯片技术, 由于使用的是免费 ISM 频段, 在安全方面继续使用现有的无线安全机制, 首先静态密钥的可靠性问题, 共享同一套 WEP 密钥存在密钥漏洞的安全隐患。其次, 缺乏集中控制手段, 通常密钥通过预定义共享方式进行。



NB-IoT 使用了授权频段，有三种部署方式：独立部署、保护带部署、带内部署。全球主流频段 800MHz 和 900MHz。由于 NB-IoT 使用许可频段网络，因此拥有更强的安全性和抗干扰能力。

### 4.2.3.1 Sigfox 简介

继 2015 年年初从几个重量级投资者处获得 1 亿欧元的融资之后，法国创业公司 Sigfox 计划打造全球性新网络，使得洗衣机、智能仪表等诸多设备连接到互联网。Sigfox 是一家位于法国图卢兹的初创公司，该公司在美国将首先针对 10 个主要城市，包括波士顿，洛杉矶，芝加哥，休斯敦，亚特兰大和达拉斯在 2016 年第一季度之前实现物联网连接。

该公司首先的目标是在美国部署其网络，致力于在美国的物联网发展。SigFox 公司计划在 2016 年 4 月以前在美国的十大城市部署物联网（包括纽约和旧金山）。Sigfox 是提供一种低速网络连接，即通信运营商所谓的“机器对机器”，声称已经涵盖了法国，西班牙，英国和荷兰，目前，它正在爱尔兰，葡萄牙，丹麦和捷克共和国推出。SigFox 计划在美国兼顾“大工业和创业公司生态系统”，鼓励他们设计的产品和服务，或者使用其技术。

投资 Sigfox 的公司均为全球知名企业与电信业者，包括日本 NTT Docomo、南韩 SK Telecom、法国工业集团 Engie 与 Air Liquide、西班牙电信运营商 Telefonica、卫星运营商 Eutelsat 公司、以及美国创投基金 Elliott Management 等。

### 4.2.3.2 Lora 简介

2013 年 8 月，Semtech 公司向业界发布了一种新型的，基于 1GHz 以下的超长距低功耗数据传输技术（简称 LoRa）的芯片。其接受灵敏度达到 -148dbm，与业界其他先进水平的 sub-GHz 芯片相比，最高的接收灵敏度改善了 20db 以上，其低具有功耗极且成本低廉而引起了极大的关注。由于该产品使用一种特殊的扩频技术，这使得不同扩频序列的终端即使使用相同的频率同时发送也不会相互干扰。在此基础上研发的集中器/网关 (Concentrator/Gateway) 能够并行接收并处理多个节点的数据，大大扩展了系统容量。基于该技术的测距和定位功能将会推动它在物联网领域的大规模应用。

2015 年 1 月 LoRa 联盟成立，该联盟成员包括思科、IBM、Kerlink、Semtech 和微芯，另外还有许多电信营运商，如 Bouygues、KPN 等。

2016 年 1 月中兴通讯与 Semtech 公司在深圳总部签署了战略合作协议，双方在 LoRa 技术及应用方面进行深入合作，促进 LPWAN 产业链的发展。其中中兴通讯与近 20 家合作厂商共同发起建立中国 LoRa 应用联盟 (China Lora Application Alliance, 简称 CLAA)，该联盟由各行业物联网合作伙伴组成，旨在推动 LoRa 产业链在中国的应用和发展，建设多业务共享、低成本、广覆盖、可运营的 LoRa 物联网。



#### 4.2.3.3 NB-IOT 简介

2013 年初，华为与业内有共识的运营商、设备厂商、芯片厂商一起开展了广泛而深入的需求和技术研讨，旨在研发一套基于现有蜂窝移动通信基础设施的低功耗广域网通信技术，并迅速达成了推动窄带蜂窝物联网产业发展的共识，NB-IoT 研究正式开始。当时，大家为这个窄带蜂窝物联网起名叫 LTE-M，全称为 LTE for Machine to Machine，名字蕴含的期望是基于 LTE 产生一种革命性的新空口技术，该技术既能做到终端低成本低功耗，又能够和 LTE 网络共同部署。LTE-M 确定了窄带蜂窝物联网的关键目标：覆盖率需要达到 99.9%，链路预算至少比 GSM 高 20dB 以上；终端功耗越低越好；终端的模组成本希望低于 5 美金。

在 LTE-M 的技术方案选择上，当时主要有两种思路：一种是基于现有 GSM 演进思路；另一种是华为提出的新空口思路，当时名称为 NB-M2M。在 2014 年 5 月份，由沃达丰，中国移动，Orange，Telecom Italy，华为，诺基亚等公司支持的 SI “Cellular System Support for UltraLow Complexity and Low Throughput Internet of Things” 在 3GPP GERAN 工作组立项，这两种思路都被包含在内，LTE-M 的名字演变为 Cellular IoT，简称 CIoT。由于绝大多数运营商更加关心新空口方案，因此，在相当长的一段时间内，NB-M2M 成为了运营商热议的一个话题。

2016 年 6 月 16 日，NB-IoT (Narrow Band Internet of Things, 窄带蜂窝物联网) 作为 3GPP R13 一项重要课题，其对应的 3GPP 协议相关内容获得了 RAN 全会批准，正式宣告了这项受无线产业广泛支持的 NB-IoT 标准核心协议历经 2 年多的研究终于经全部完成。

众多行业分析机构的研究都认为中国将成为全球最大的物联网市场。与 3GPP 标准化节奏保持同步，国内也开始了 NB-IoT 相关标准的制定工作。在 2015 年 11 月份的中国通信标准化协会 CCSATC5 WG9#74 次会议上，通过了《面向物联网的蜂窝窄带无线接入总体技术要求》的立项，标志着国内 NB-IoT 标准化工作正式启动。在 2016 年 6 月初 CCSA TC5 WG9#77 次会议上通过了 NB-IoT 系列行标（包含核心网，接入网和终端）的立项工作。

NB-IoT 系列行标计划发布时间为 2016 年年底。这标志着在中国，NB-IoT 已经具备了在 2017 年年初规模商用的基本条件。NB-IoT 构建于蜂窝网络，只消耗大约 180KHz 的频段，可直接部署于 GSM 网络、UMTS 网络或 LTE 网络，以降低部署成本、实现平滑升级。2016 年随着 NB-IoT Forum 的成立来自全球的企业加入 GSMA 联合华为，沃达丰，爱立信，中国移动，中国联通，AT&T，德国电信，Etisalat，GTI，英特尔，KDDI，KT，LG Uplus，Mediatek，诺基亚，Oberthur Technologies，高通，意大利电信等势必将迎来 NB-IoT 的时代。

#### 4.2.3.4 几种方案的分析比较

三种技术方案不同，实际上提供了三种不同的商业模式：

【Sigfox】 Sigfox 旨在成为全球物联网运营商，模块可以从多个供应商处获得，因此批量生产后硬件成本下降不是问题。但是 Sigfox 的期望值很高，他们希望成为全球 IOT 运营商。他们与运营商合作，获得数据，然后将数据转给设备所属的公司。

优点：世界各地的服务都是一样，标准化程度高，跨地球跨国界的数据交换无需格式转换；已经规模化建设。

缺点：物联网服务的对象不是个人，主要是企业数据。许多企业数据不愿意放在运营商的数据平台，因此成为全球运营商是一个不切实际的想法，很难得到大客户的支持。

【LoRa】 LoRa 提供一种技术，让其他公司的业务在全球范围内组成自己的物联网。LoRaWAN 协议定义了设备之间如何通讯，数据如何传输给设备。LoRa 与 Sigfox 最大的不同之处在于谁都可以运行设备，LoRa 联盟也鼓励运营商部署 LoRa 网络，但是任何人都可以购买 LoRa 基站，并且自主组网。很多公司称之为私有网络。个人也可以这样做，The Things Network 是一个自发组织，很多个人在上面开发 LoRaWAN 硬件。相对于全国的部署，LoRa 更适合区域性的部署。如果 LoRaWAN 设备提供商提供服务，我们可以自己建立基站，来延续这种服务。

优点：开放程度高，便于开发应用协议；自控程度高，适合大型企业自己运营；已有应用案例。

缺点：初期的基础设施（基站）需要大量投资，企业自行运维的经验不足可能导致很多问题；如果发现有安全漏洞，及时进行系统更新有困难。

【NB-IOT】 NB-IOT 技术则基于现有的蜂窝移动通信基础设施，建造成本低，从而可为网络运营商谋取更多的利益。

优点：基于现有移动网络，规模化程度高，得到运营商的重视，容易得到运营商的投资；有国内自主核心知识产权，会得到国内企业的青睐；

缺点：起步较晚，受行业标准和牌照的限制。

#### 4.2.3.5 LoRa 与 NB-IOT 的技术性能比较

SigFox 是商用化速度较快的一个 LPWAN 网络技术，它采用超窄带技术，使得网络设备消耗 50 微瓦的功率为双向单向通信或 100 微瓦。这一协议由 SigFox 公司拥有，其创始人是法国企业家 Ludovic Le Moan，主要打造低功耗、低成本的无线物联网专用网络。除此之外，

我们没见到 Sigfox 的其他性能描述。

NB-IoT 与 LoRa 是最有发展前景的两个低功耗广域网通信技术，LoRa 技术的诞生较早于 NB-IoT 的出现，它主要使用线性调频扩频调制技术，即保持调制相同低功耗特性，又增加通信距离，还提高了网络效率免干扰，在此基础上研发的集中器 / 网关能够并行接收并处理多个节点的数据，大大扩展了系统容量。

NB-IoT 技术推广才刚起步，而 LoRa 相对 NB-IoT 已经有很多成熟的商用案例。两大阵营的应用可能会有高度重叠，但 NB-IoT 毕竟是由运营商来主导其它外围各厂家配合，在这点上 NB-IoT 有明显优势，同时现有基础设施可以重复利用，但在信息的隐私问题上存在挑战，数据先到运营商平台的网络企业是否愿意把自己的数据或客户的数据进行共享此事有待商榷，所以目前而言说哪方更有优势为时尚早，只能说在某领域或行业谁做的更专。

LoRa 和 NB-IOT 的部分性能比较可由下表给出。

功能	网络名称	NB-IoT	LoRa
技术特点		蜂窝	线性扩频
网络部署		与现有蜂窝基站复用	独立建网
网络拓扑		星型	星型
频段		运营商频段	非授权频段
传输距离		远距离	远距离 (1-20KM)
速率		<100kbps	0.3-50kbps
连接数量		200k/cell	200k-300k/cell
安全措施		支持	128 位 AES
终端电池工作时间		约 3~10 年	约 3~10 年
成本 (模块)		3-5 美元	5 美元

## 4.3 物联网处理应用层安全保护技术

### 4.3.1 物联网处理应用层概述

提到物联网的处理应用层，我们一定会联想到“智慧”或“智能”，智慧城市、智能电网、智能交通、智能家居等都离不开物联网，这些智慧应用系统，大都建立在物联网处理应用层。我们还可以做一个比喻，如果把物联网比喻成人体，传感器是我们的眼耳鼻舌等感觉器官，传输网络相当于我们的传导神经，而物联网的应用层核心则相当于我们的大脑，该层需要汇集和接收物联网中所有信息，进行分析运算，实现物联网的智慧应用，最终实现人、物、系统的万物智慧互联。

物联网处理应用层涉及国家、政治、经济、民生、个人隐私等各个方面，建设安全防护体系已经成为物联网成功的关键因素之一，为了更好的分析物联网处理应用层的安全问题，建立安全防护体系，我们首先需要对物联网处理应用层的技术组成有一个基本的认知。

物联网处理应用层的技术架构需要融合更多的先进技术，包括互联网、云计算、大数据、人工智能等，以满足对整个庞大的物联网进行信息运算和交互的需求，以下列出了物联网和当前的主要先进技术间的关系：

(1) 互联网：物联网将互联网进行了延伸（包含传统互联网和移动互联网），形成更大的智慧网络，而物联网的服务可以在互联网平台上实现服务（浏览器或 APP）交付；

(2) 云计算：物联网处理应用层需要一个大规模分布式弹性的高性能计算平台，云计算（私有云、公有云或混合云）平台成为物联网应用系统的理想平台，通过云计算，实现高效存储、海量运算和便捷的服务交付；

(3) 大数据：物联网处理应用层所接收的数据，是不折不扣的大数据，物联网数据具有海量异构、结构化数据和非结构化数据混合、数据体量巨大等特点，具备所有大数据的特征（Volume（大量）、Velocity（高速）、Variety（多样）、Value（价值），简称 4V），需要大数据技术进行分布式数据存储和挖掘，以 Hadoop 等大数据架构为代表的先进架构在物联网中被广泛使用；

(4) 人工智能（AI）：人工智能代表着人类进化新的里程碑，通过深度学习，人工智能系统可以建立大量的感知模型，形成相互关联的人工智能知识库，实现基于海量数据的智慧分析结果，在物联网应用中真正充当超级大脑；

(5) APP：随着移动技术的发展，手机、平板电脑的数量远超桌面计算机，成为人和网络交互的主要途径，运行在这些手机、PAD 上的 APP 被广泛接受，在物联网中，手机、PAD 上的 APP 同样会成为物联网人机交互的主要途径之一，我们可以通过 APP 获取物联网



的具体应用，享受便捷服务。

#### 4.3.2 物联网处理应用层信息安全问题分析

物联网的安全风险必须予以重视，黑客入侵智慧电力系统可能导致城市供电瘫痪；入侵智能家居系统可能导致整个家庭变得危险；入侵智慧医疗系统，会直接危及病人的健康；入侵智慧交通系统，会导致交通瘫痪；入侵车联网，会导致车辆失控。物联网处理应用层作为整个物联网的窗口和纽带，通过物联网网络传输层与传感器相联，同时亦通过服务接口向互联网（含传统的互联网和移动互联网）、组织内部网络发布具体的物联网应用服务，或与其他智慧信息系统进行交互，系统安全边界广泛而模糊，威胁面巨大，讨论物联网处理应用层的安全问题，我们可以从物联网处理应用层的黑客动机、威胁和脆弱性三个方面入手进行分析：

##### 4.3.2.1 攻击动机

黑客攻击物联网处理应用层的动机包括如下几个方面：

(1) 经济利益：物联网处理应用层承载着丰富的应用，经济利益广泛，资金窃取、勒索、钓鱼、诈骗等传统互联网出现的问题，都可能在物联网处理应用层出现，无论从涉及的财富价值还是数据价值，物联网对黑产世界都具有足够的吸引力；

(2) 政治：近年来国家和政治对抗已经延伸到网络空间，物联网相比互联网连接的范围更广，甚至会与国家基础设施形成连接，一旦被攻击后果更为严重，物联网可能成为各国网络部队重要的攻击目标，物联网安全已经被各国政府重视；

(3) 隐私窥探：物联网应用承载的个人和组织的隐私信息非常丰富，海量的注册信息、监控信息、行为信息等无所不包，尤其是智慧家居、智慧医疗，直接会涉及到隐私问题，之前就发生过某品牌的云摄像头把家中女主人换衣场景泄露到网络的事件，通过对物联网进行隐私窥探是黑客所期望的；

(4) 敏感数据窃取：物联网覆盖范围广，数据资源丰富，一些数据在小范围时属于开放数据，一旦形成大范围的汇集，会成为敏感数据，甚至是涉密数据，黑客，尤其是国家级别的攻击者会非常关注这些数据，采用黑客手段获取；

(5) 轰动效应：物联网作为先进技术的代表之一，攻击事件非常吸引眼球，例如破解特斯拉（貌似白帽子和黑帽子都十分感兴趣），很快就成为了公众热点；

##### 4.3.2.2 威胁来源

物联网处理应用层可能面临的威胁面很广泛，基本上互联网、云计算、大数据等平台等



物联网处理应用层所采用技术的威胁面都会被物联网处理应用层系统继承，这里列出了一些可能的威胁（但不限于这些威胁）供参考：

(1) 服务阻断：以 DDoS 为代表的拒绝服务攻击构成物联网处理应用层的重要威胁，近年来，DDoS 攻击呈大幅上升趋势，物联网处理应用层不仅面临着来自互联网的 DDoS 攻击（僵尸网络），也会面临被黑客利用物联网本身庞大的传感器网络的攻击，今年 10 月份美国发生的利用物联网设备对美国最主要的 DNS 服务商 Dyn 遭遇大规模 DDoS 攻击，导致 Twitter、Spotify、Netflix、AirBnb、CNN、华尔街日报等数百家网站无法访问的安全事件，同样为物联网处理应用层敲响了警钟；

(2) APT 攻击：APT 攻击具有高隐蔽性和潜伏性，一旦成功渗透，会将恶意软件（蠕虫等）快速传播，APT 攻击是当前物联网处理应用层需要防护的主要攻击之一；

(3) 恶意代码：物联网更容易成为恶意代码的温床，恶意代码（病毒、蠕虫等）仍然会成为物联网应用的常见威胁；

(4) WEB 安全威胁：物联网处理应用层的 APP 服务端、WEB 服务器直接暴露在公网上，互联网上的数据安全威胁同样威胁着物联网，包括 SQL 注入、跨站脚本攻击等同样会威胁到物联网的应用系统；

(5) 计算资源窃取：物联网处理应用层投入了大量的计算资源，包括云计算、大数据平台，一旦物联网应用系统被攻破，就可以将这些计算资源用于黑客期望的非法用途；

(6) 跳板：物联网应用系统与大量的物联网传感器相连（存在信任关系），一旦物联网处理应用层被攻破，可能变成黑客的跳板，向传感器渗透，实施远程控制；

(7) 冒用：攻击者可能冒用合法用户的身份、或者被信任的传感器、或者与物联网应用系统有信任关系的其他系统，进入物联网应用系统，形成渗透；

(8) 云穿透：从云平台的角度，物联网应用系统相当于云平台的租户，一旦云平台被黑客攻击，可能直接穿透虚拟化机制，产生针对物联网应用系统的渗透，或者直接获取物联网应用系统存储在云平台上的数据；

(9) 数据污染：黑客可能向物联网的大数据平台注入脏数据，导致系统误判，产生非预期影响；

### 4.3.2.3 物联网处理应用层脆弱性。

物联网处理应用层的应用系统融合了互联网、云计算、大数据、人工智能等先进技术，且分布式部署，具有高复杂性，这些先进技术平台可能存在的安全漏洞会被物联网应用系统继承，存在漏洞是大概率事件，我们归纳了一些可能的脆弱性：

(1) 平台漏洞：物联网应用系统平台本身的漏洞，例如云平台的漏洞、大数据平台的漏洞等；

(2) 组件漏洞：物联网应用系统会采用很多的组件，如数据库、中间件、WEB 服务器、缓存、安全软件、设备等，这些组件可能会存在漏洞，导致互联网应用层存在漏洞；

(3) 应用系统漏洞：物联网应用系统可能存在代码级别的漏洞；

(4) 逻辑漏洞：物联网处理应用层在流程方面可能会存在逻辑漏洞，导致特殊输入产生绕过动作，使系统面临威胁；

#### 4.3.3 物联网处理应用层的安全防护建议

物联网应用系统的安全防护体系，应当从系统工程的角度，采取多维视角，继承和发扬深度防御思路，结合云计算、大数据、人工智能等新技术的特点，从技术、管理、人等三要素构建立体安全防护体系，这里提出一些防护体系架构参考意见：

(1) 基于生命周期的风险评估：应当从物联网应用系统生命周期的维度，在系统规划、分析、设计、开发、建设、验收、运营和维护、系统废弃的每一个阶段进行信息安全管理，在系统设计和分析阶段就进行安全目标、安全体系、防护蓝图等顶层设计，并将安全防护设计与系统设计相融合；在系统开发阶段，进行代码安全评估，测试阶段同期进行安全测试；在建设阶段进行安全管理；在验收阶段同时进行风险评估和测评，保障安全防护的有效性和合规性，在运营和维护阶段同时进行安全运营，并周期进行风险评估，跟踪威胁情报，持续改进安全管理和安全防范措施，在系统废弃阶段做好残余信息的消除等，保障系统保障全生命周期的系统安全；

(2) 构建深度防御体系：应当从组织、技术、管理的维度构建多层次的深度防御体系，合理划分安全域，从机密性、完整性、保密性的安全目标出发，结合国家政策标准的合规要求（如等级保护），设计整体安全解决方案，保障系统安全；

(3) 建立动态的风险评估机制：应当建立物联网应用系统的信息安全统一管理和态势感知系统，结合专家周期性风险评估，实现系统动态安全；

(4) 实施专项威胁防控，针对物联网处理应用层突出的安全问题，如 APT 攻击、DDoS 攻击、数据库脱敏与加密、漏洞管理、设备与系统、系统与系统、人与系统的双向认证机制等问题，评估和设计专项防护，加强防护；

(5) 对于大型物联网的应用系统，应当建立与之同步的测试系统和攻防演练环境，进行广泛的研究工作；

- (6) 建设物联网应用系统的审计系统，实现信息安全关键信息的审计；
- (7) 建设安全运维系统，设计体系化的制度、流程，保障运维安全；
- (8) 建设异地备份容灾体系，保障系统在特殊时期的连续运营；
- (9) 建立应急响应体系，并加强应急演练，保障应急演练的有效性和可操作性。

#### 4.3.4 物联网处理应用层安全态势感知

物联网处理应用层应用系统多采用分布部署，涉及的平台、系统、中间件、应用软件、网络设备、安全设备众多，需要部署平台化的云安全态势感知系统。云安全态势感知系统具备层次化的多维数据（安全状态、事件、威胁情报、安全知识等）的汇集、大数据关联分析、动态风险评估及安全态势可视化，结合专家互动分析，实现统一的物联网安全展示、监控、运维、应急体系，从而构建企业级、区域级或行业级的涵盖人员、技术、流程的整体安全保障体系，如图 4-7 所示。

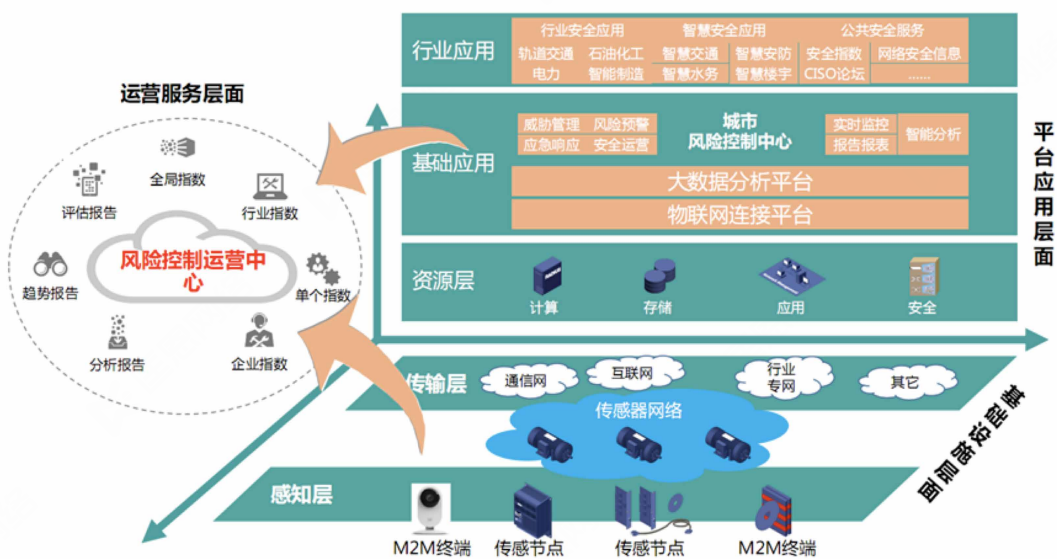


图 4-7 物联网安全态势感知系统架构图

- 数据采集，数据传输

数据采集通过主动或被动式的数据采集方式，用分布式任务调度引擎，自动采集相关安全数据，通过基于缓存的分布式消息队列进行实时处理，根据规则引擎、以及决策引擎针对安全数据进行识别、转换、处理和传输。

- 网络探测，情报利用

通过主动探测方式，及时获得网络上设备、系统和应用的运行状态以及资产信息，既能够时刻知晓最新的安全防护范围，有效调整安全防护策略，更可以结合外部的威胁情报，对网络安全趋势有第一时间的分析和判断。

- 关联分析，态势感知

采用安全模型和算法对多源异构数据从时间、空间、协议等多个方面进行关联和识别，通过大数据平台能力，对网络安全状况进行综合分析与评估，形成网络安全综合态势图，借助态势可以精确定位网络脆弱部位并进行威胁评估，发现潜在攻击、预测未知风险，提高全局网络安全防御能力和反击能力。

- 人工智能，模式学习

使用机器学习和数据挖掘技术，基于各种安全数据实现对网络行为、主机行为、应用行为的特征学习，通过大数据构建出网络环境中的各种行为模型，从而识别出正常和异常、趋势和对比等信息，实现自动学习、自动适应和自动规则生成，降低人员操作失误风险，提高安全响应速度。

- 风险评估，量化指标


对物联网、信息网络上的恶意代码、漏洞、攻击方法等进行搜集、整理和分析，并对探测的漏洞与权威漏洞库进行关联评测，根据漏洞严重性、影响范围等综合因素给出量化评估，并结合网络中实际产生的攻击数据，按照科学的指标体系开展全面的风险度量。

- 事件预警，应急响应

基于深度学习的专家分析和准确及时的威胁情报支持，将严重安全事件、高危安全威胁、重大损失等进行预判，通过安全通告、实时信息推送等方式提供安全警报，并提醒用户采取相应的防范应对措施。

- 合规检查，评估报告

将标准合规、安全检查、风险评估、安全报警、应急响应等日常安全工作有机地融为一体，实现安全制度和 workflows 的平台化、自动化、标准化，明确安全工作考核和衡量方式，落实安全工作责任和工作内容，通过还可以满足相关安全标准和监管检查的管理要求。



# 第五章

## 物联网安全产业发展趋势



## 5.1 物联网产业发展趋势

物联网的发展已经从 2009 年的概念阶段，到今天的快速发展阶段，今后还将加速增长。IHS 预测全球物联网设备的安装基数将从 2015 年的 154 亿增长到 2020 年的 307 亿。2025 年，这一数字更将达到 754 亿。

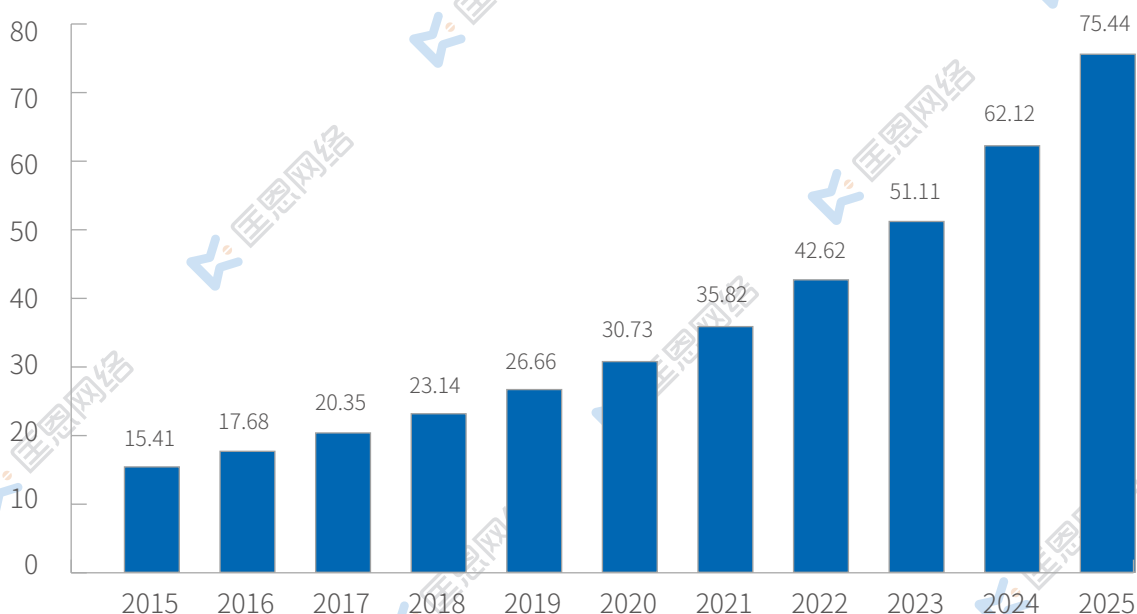


图 5-1 IHS 对物联网市场的预测图（数据来源：IHS）

福布斯（Forrester）预测，交通运输、政府部门的安保与监控零售和库存管理以及初级制造业的工业资产管理将是未来物联网增长的热门领域。相比小公司，大企业更有可能使用物联网。调查中 23% 的大型受访企业在使用物联网，中小企业中，这个比例只有 14%。

麦肯锡估计，物联网市场总规模在 2020 年将达 37 亿美元，达到 32.6% 的年复合增长率。2025 年之前，物联网的潜在经济影响力为 2.7 ~ 6.2 万亿美元。

据贝恩咨询公司预测，到 2020 年，出售硬件、软件和综合解决方案的物联网服务供应商年收入可达 4700 亿美元，可用利润达 600 亿美元。同时贝恩预测云服务提供商、分析和基础设施软件供应商将对物联网交易产生重要影响。

Gartner 预测 2016 年全球物联网设备数目达到 64 亿，比 2015 年增长 30%。2020 年这个数字将达到 208 亿。

IDC 预测全球物联网收入将从 2015 年的 27.12 亿美元增加到 2020 年的 70.65 亿美元，复合年增长率（CAGR）达到 21.11%。同时，IDC 还预测物联网设备的安装基数将以 17.5% 的年复合增长率在 2020 年增加到 281 亿。



图 5-2 工业应用物联网发展分布图（数据来源：Forrester）

物联网设备从 2015 年到 2021 年以 23% 的复合年增长率（CAGR）增长，到 2018 年将超过手机成为最大的互联设备类别。Ericsson 预计到 2021 年，全球联网设备将达 280 亿，其中 160 亿与物联网相关。

IndustryARC 预测工业物联网到 2021 年市场将达 1238.9 亿美元。通用电气预测在未来 15 年中，工业物联网（IIoT）领域的投资最高可达 60 万亿美元。埃森哲预计工业互联网到 2030 年能够为全球经济带来 14.2 万亿美元的经济增长。

## 5.2 物联网安全技术和产业发展趋势

近年来，随着物联网相关技术的成熟落地，一些物联网相关产业也在持续发展。受国家有关政策的影响，这些产业对物联网安全也非常重视。一些表面上对安全性要求不高的行业，如智慧农业，也认识到对物联网系统安全保护的重要性。

在物联网迅猛发展的同时，物联网安全成了产业痛点。美国已经领会到了物联网安全漏洞被利用的滋味。今年 10 月 21 日，美国上千家网站遭受大规模 DDoS 攻击，攻击源头大批是被入侵的物联网设备，造成这些设备成为“僵尸”攻击节点。有关专家也指出：物联网产业越大，安全问题就越多，风险也越大。因此物联网产业界应该把信息安全问题放到规划阶段来考虑，而不是到了中后期出现问题了才进行弥补，这对于产业长远的发展来说，所付出的代价将是最小的。

2016 年是物联网安全的建设年，产业界对物联网数据的处理层（云平台）安全和终端安全都给与高度重视。在物联网的网络传输层，低功耗广域网 LPWAN 技术将逐步占据主要市场，成为物联网网络传输层的主流产品，其安全技术将直接影响到物联网网络传输层的数据保护。据华为公司提供的数据，到 2020 年，全球 70 亿物联网终端设备中，约有 30 亿会使用蜂窝无线通信网络，其中 LPWAN 将占主导地位。另外 40 亿物联网终端呢？这些物联网终端将不直接连接广域网，而是通过一个网关节点将数据通过广域网传输到后台数据处理中心。另据研究机构 Gartner 预计，到 2020 年物联网设备将增至 200 亿台，这些物联网设备的大多数是组成一个传感器局域网的终端节点，在这些物联网终端节点与网关节点之间的传输，一般采用短距离无线传输方式。目前，短距离无线传输的安全性还不够高，不足以支持物联网产业的需求。因此，为物联网感知层数据提供安全保护，以及为物联网整体系统提供安全解决方案，将成为物联网安全产业的另一战略要地。

今后，物联网安全方面的投入比例会逐步提高，因此物联网安全产业规模的发展速度将快于物联网产业的整体发展速度。

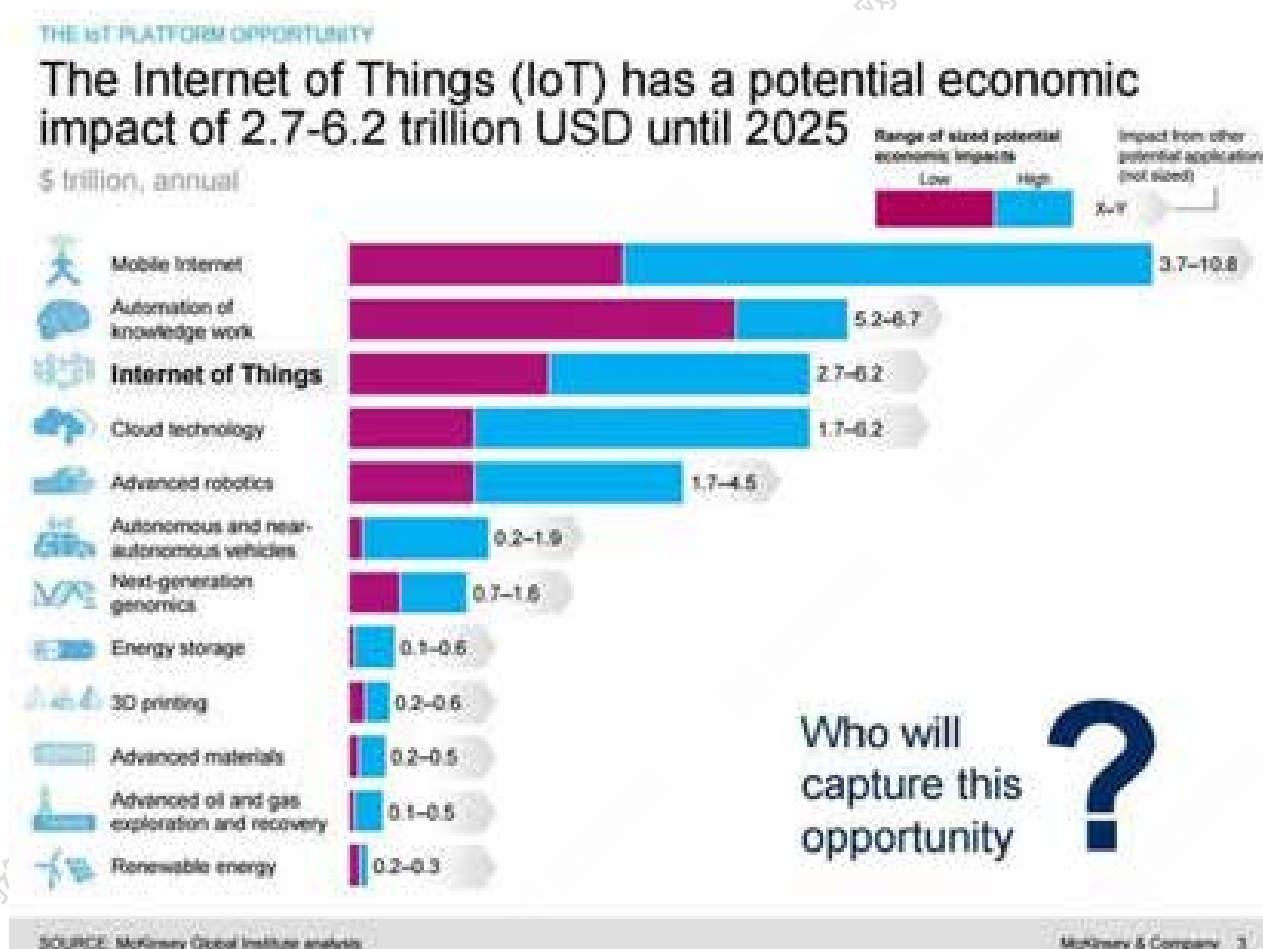


图5-3 工业应用物联网发展分布图 (数据来源: 麦肯锡)



# 第六章

## 物联网安全建设 发展建议



2016 年 12 月，美国宽带互联网技术咨询组 (BITAG) 发布报告提出建立物联网安全供应链。报告指出，物联网设备供应链中，应明确安全和隐私保护策略；应允许设备参数的重置功能；厂商应及时发布漏洞信息和应对措施；应建立安全软件供应链；应建立物联网设备整个生命周期的安全保护；应提供制造商的应急联系方式。

除此之外，为了物联网产业的健康发展，我们就物联网安全建设补充几条建议。

(1) 物联网安全体系需要与物联网应用系统同时建设，因为后期增加额外的安全防护系统，不但会有一系列限制（硬件环境、软件环境、接口等），而且费用也会更高。物联网设备和系统的安全防护是生产商 / 建设商 / 运营商的责任，而不能仅仅依赖现有的法律法规和行业标准等。

(2) 物联网安全的建设不能仅仅停留在网络传输层和应用层，还要建设感知层的安全防护，我们称此为物联网系统“最后一公里”的安全问题。在物联网感知层，仅依赖于短距离无线通信自身的安全机制（如 Zigbee 的安全功能），对物联网系统是远远不够的。目前来看安全需求不大的物联网感知层，到 2020 年当终端数量达到数百亿时，安全需求将变得很明显。

(3) 黑客对物联网设备攻击的目标根据轻重程度分为：控制设备（如开关设备）、将入侵设备当作“僵尸”节点对其他设备发起 DDoS 攻击（如美国的断网事件）、发送假数据（假冒攻击、伪造攻击）、获取节点信息。有些攻击不需要入侵到设备内部。因此所有物联网设备最少应提供指令控制和成为“僵尸”节点的防护机制。

(4) 物联网安全的最终解决方案应该在业务数据（包括指令、配置类数据）的安全，而不是仅依赖网络传输层安全（即信道传输安全）和处理层安全（即云计算安全），因为对用户来说，只有业务数据安全方案才是可控的。安全方案可以由第三方设计和建设，但系统运营应该保证自己的可控性。

(5) 工业物联网的发展是必然趋势，但许多工业系统担心暴露在互联网上会有很大的安全风险。为了解决网络所带来的风险和网络所提供的技术便利之间的矛盾，应该把联网系统理解为一种能力，而不是时时刻刻连接网络。例如，在一分钟内开放网络端口一秒钟，然后再关闭，这样既可以满足网络连接需求，又在很大程度上（98% 以上的时间）处于“离线”状态。

(6) 物联网安全应关注隐私信息保护。感知层数据即使采取了认证性、机密性和完整性等保护手段，也容易泄露隐私信息，例如数据多少本身就泄露信息，相当于网络环境的流量分析攻击；隐私信息的泄漏在数据处理层更显得突出，通过大数据分析手段，一些碎片的、单独不泄漏用户隐私信息的数据，通过关联融合，就可能泄漏用户隐私信息。但隐私保护同时也是具有挑战性的技术，因为隐私信息的范围不好定义，隐私信息的泄漏的途径千奇百怪。



[www.kuangn.com](http://www.kuangn.com)

### 北京匡恩网络科技有限公司

北京市海淀区知春路 7 号致真大厦 D 楼 13 层

电话: 400-068-0583

传真: 010-59512799

邮箱: [info@acorn-net.com](mailto:info@acorn-net.com)