物联网安全体系思考与探讨

Consideration and Discussion on IoT Security Structure

朱常波，张曼君，马　铮（中国联通网络技术研究院，北京 100048）
Zhu Changbo，Zhang Manjun，Ma Zheng（China Unicom Network Technology Research Institute，Beijing 100048，China）

摘　要：
物联网作为战略性新兴产业的重要组成部分，在加快经济发展、促进产业转型升级、服务社会民生方面发挥着越来越重要的作用，是支撑整个产业和科技革命的重要基础设施。近年来，随着物联网连接和产业规模的快速增长，安全攻击范围和频度不断增长，带来了巨大的经济损失。基于物联网安全风险和管控难点，通过3T+1M物联网安全框架，从顶层设计到终端、网络、云端和智能运维，打造全方位安全能力，构建一体化的物联网安全保障体系。

关键词：
物联网；安全架构；端-管-云；产业合作
doi：10.12045/j.issn.1007-3043.2019.01.001
中图分类号：TN929.5
文献标识码：A
文章编号：1007-3043（2019）01-0001-04

Abstract：
As an integrated part of the strategic emerging industry，IoT plays an increasingly important role in accelerating economic development，promoting industry transformation and upgrade，and serving people's livelihood. It is a vital infrastructure that supports the entire industry and technology revolution. In recent years，with the rapid development of IoT connections and industry large-scale growth，The increasing scope and frequency of security attacks have brought huge economic losses. Based on security management and control difficulties，according to the 3T+1M IoT security architecture，it builds comprehensive security ability from top-level design to IoT device，network，cloud protection and intelligent O&M，and further constructs a whole IoT security assurance system.

Keywords：
IoT；Security structure；Terminal-network-colud；Industry cooperation

引用格式：朱常波，张曼君，马铮. 物联网安全体系思考与探讨[J]. 邮电设计技术，2019(1)：1-4.

0 引言

物联网的发展将人类社会带入到万物互联、万物智联时代，为所有行业带来了巨大的发展机遇。物联网将经济社会活动、战略性基础设施资源和人们生活全面架构在全球互联互通的网络上，所有活动和设施在理论上呈现透明化，一旦遭受攻击，安全和隐私将面临巨大威胁。GSMA的调研报告中指出，在所有决定物联网发展的要素中，安全占据最大的比重。根据Vanson Bourne research的调研显示，行业客户认为部署物联网的最大挑战是安全，即安全是业务正常上线运营的前提，安全可控是物联网产业能否成功的重要基础。

“万物互联，安全先行”。实现信息安全和网络安全是物联网大规模应用的必要条件，也是物联网应用系统成熟的重要标志。物联网安全需要足够多的重视，需要整个物联网行业持续的关注与跟进。

收稿日期：2018-11-30

1 物联网机遇和安全挑战

1.1 物联网发展现状

物联网（IoT）将海量的设备互联，以连接为基础，以数据为核心，以价值创造为突破，正在成为社会生活的一部分。物联网的本质是借助ICT技术对传统产业进行重构，通过物理世界和数字世界的融合，缩短

业务流程,提升生产效率,为客户提供更好的产品和服务,释放出产业创新的巨大潜能。

物联网驱动全球各行各业数字化、智能化,带来巨大的经济价值,已经成为全行业数字化转型的驱动力。各国公司、政府、组织和团体都在积极投入和研究这一仍处在发展中的技术,利用遍布各处的传感器,广泛收集和分析数据并应用,以更好地支撑各行各业的快速发展。图1为2009—2017年我国物联网产业规模的增长情况。

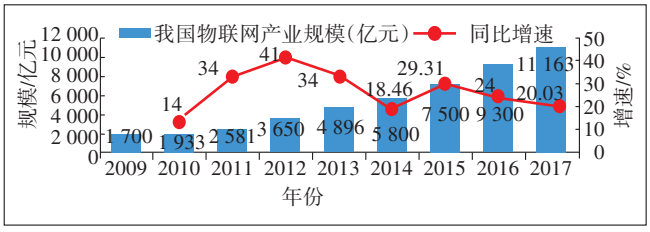

图1 2009—2017年物联网产业规模变化

根据华为GIV预测,随着万物感知和万物互联的升级,一切都将被带入万物智能的世界。到2025年,个人智能终端数将达400亿,全球连接总数达到1 000亿,这些连接将泛在于公用事业、交通、制造、医疗、农业、金融等各个领域,推动数字化转型,创造23万亿美金数字经济。伴随着感知、连接能力全面提升,IoT以连接为基础,以数据为核心,以价值创造为突破,正在成为我们社会生活的一部分。

物联网产业的快速增长推动产业布局的调整。电信运营商在物联网连接领域具备天然优势,利用用户规模的领先地位积极布局物联网产业生态,通过聚焦管道连接,对垂直行业应用进行探索。图2是全球运营商在物联网行业的布局。

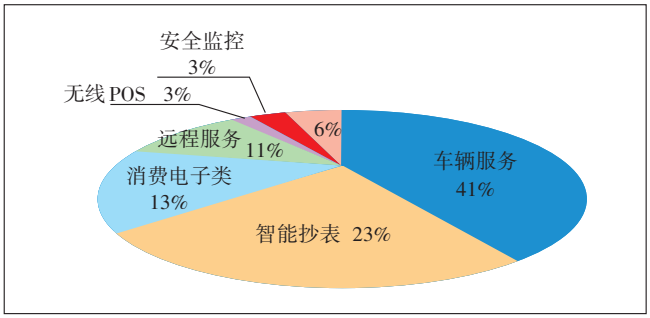

图2 全球运营商IoT业务连接情况

1.2 物联网安全问题

互联网技术革命,把人类带入了虚拟世界,物联网革命,将虚拟世界加载到现实社会中,虚拟和现实边界更加模糊,人们与物理世界的互动方式被彻底改变。泛在互联的应用场景为医疗、运输、制造等传统领域带来巨大好处,同时也催生出无所不在的安全问题。无论是信息泄露、系统被破坏或者被外部控制,都会导致严重的损失。近些年来物联网攻击频次和范围的大规模增长映射出物联网领域安全隐患严重,产品缺少安全机制和防护措施。

物联网属于新兴技术产业,大量传统设备在进行数字化改造时,几乎没有同步配置防护能力,影响了物联网的整体安全可靠性。同时由于物联网终端和应用的融合化、多样化,给物联网业务带来了更多的安全不确定性。正是由于不断增长的各类物联网互联设备为攻击者提供了巨大而广泛的网络攻击入口,导致物联网面临着大量问题和挑战。

a) 全面防护难。物联网终端整以每2年翻一番的速度增长,在规模上将远大于目前传统网络终端,且类型千差万别,无处不在,防护难度和成本非常大,难以进行全面监测和防护。一旦被利用,会对网络甚至整个物联网系统带来超大规模的安全攻击。

b) 全程监测难。大量物联网弱终端如水表、电表等,受限于成本和性能,无法集成安全防护软硬件,完全裸露在网络中,难以实现主动防护;同时受限于节能等需求,无法实时上报运行状态,做到端到端的全程监测和防护,因此容易受到非法入侵和破坏。

c) 分析建模难。物联网涉及行业众多,应用场景复杂,用户行为多种多样,威胁特征难以全面捕捉和识别,因此对威胁进行建模分析和信息挖掘难度大。

d) 数据保护难。在共享经济下,物联网数据需要更多的共享和交互场景,数据的交互涉及物物、人物、物云以及多个行业和部门之间的交互和共享,为数据隐私保护和安全传输带来巨大挑战。

e) 物理保障难。物联网终端分布范围广,很多应用场景是开放式部署,大量终端无人值守,自运行模式极易受外部攻击,同时难以及时发现。

f) 安全管理难。车联网、智慧医疗等应用场景直接涉及到用户生命安全,攻击破坏造成的损失也远远大于传统网络,但是由于用户对于物联网安全认识不够深刻,缺乏安全防护意识和制度保障,往往容易被攻击者利用实施各类攻击。

2 物联网安全架构

在万物互连互通的环境中,海量的物联网终端高并发的接入和生成、处理数据,对于网络和平台安全

而言都是巨大的挑战。运营商的网络为这些数据提供高并发的安全通信保障，云端和物联网平台支撑着丰富的物联网应用，这些支撑的系统和应用有可能沦为潜在恶意攻击的目标，同时物联网业务云化也给端到端的安全运维带来了更大的挑战。

因此基于物联网的安全威胁、应用场景和特定安全需求，要建立全局化的安全视角、体系化的安全架构，全方位涵盖端、管、云/平台、数据安全、隐私保护、端到端安全管控运维等，构建多道物联网安全防线，实现纵深化防御。

2.1 3T+1M框架

“3T+1M安全架构”聚焦端、管、云和平台安全特性的组合协同，应对物联网基础架构中的感知层、网络层和应用层的安全威胁，依托运营商通信网络安全保障能力优势，提供物联网整体安全态势的感知与分析能力（见图3）。

3T+1M物联网安全解决方案，核心在于基于物联网应用场景安全威胁，构建起终端防御、管道保障、云端保护3个物联网安全技术族（Technologies）以及安全运维与管理（Management），以此满足国家和区域法律法规、行业标准等合规要求，构建物联网安全端到端纵深防御体系，抵御威胁。

2.2 物联网终端防御技术（1T）

构建终端安全体系是保证物联网安全的第1道防线。由于物联网应用行业多，需要针对不同场景、不同类型的终端进行设计，根据终端环境和处理能力进行区分，匹配与其计算资源和应用相适应的安全技术。

对于成本和性能受限的弱终端，需满足基本安全能力，如双向认证、加密传输、远程升级等；对于能力较强，要求较高的强终端，需要提供更加丰富的安全能力，如安全证书管理、防病毒、入侵检测等。对于快速响应处理场景下的终端，对时延要求较高，传统的加解密、审计分析等安全操作可能会影响业务体验，需要研究更加高效、轻量级的安全算法，兼顾安全和效率。此外，终端与网络、终端与平台之间需要建立安全协同的防御体系，对威胁进行多维度感知和防护。

2.3 物联网网络保障技术族（1T）

网络是物联网安全的第2道防线。物联网终端由于自身防护能力较弱，可以考虑如何在网络和平台侧海量的终端和数据中，对恶意行为进行快速检测，并迅速做出判断和相应，进行报警和隔离处置。利用运营商的网络能力，在网络侧提供安全监控服务，是运营复杂度最低、建设成本最低、对业务影响最小同时也是最实际有效的防护方案。

借助多网运营经验，运营商提供基于网络侧的异常行为检测，对实时流量通过规则匹配、大数据分析、

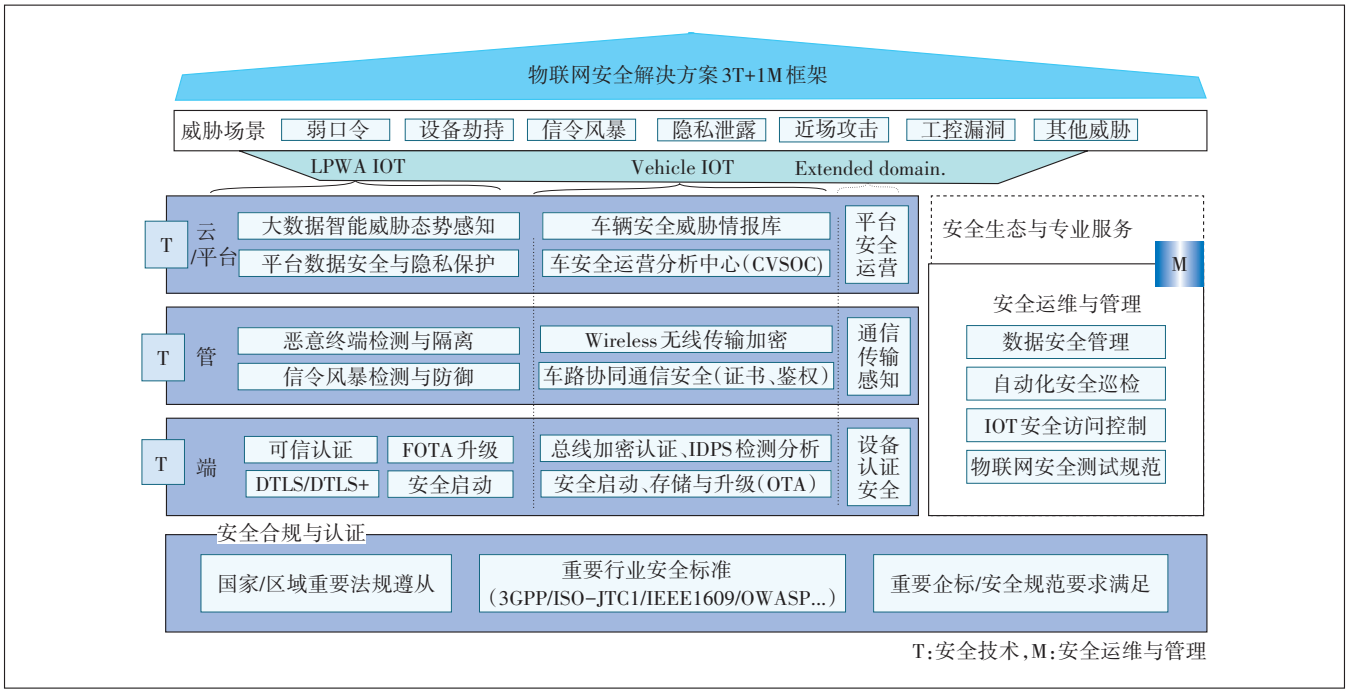

图3　物联网安全3T+1M架构

深度机器学习等检测方法进行异常分析,从而发现各种行为威胁和攻击威胁;除此之外,还可以结合互联网、移动网的数据,进行联合分析,形成更为全面的恶意软件特征库和行为模型库,提供更好的态势感知和威胁预警能力。运营商通过终端用户的策略定制业务,根据威胁的不同类型,向用户提供多种符合终端和网络安全需求的威胁处置服务。

同时,针对不同应用场景,增强物联网管道安全能力,比如针对NB-IoT场景增强防DDoS攻击和防信令风暴能力,针对车联网重点构建车路网协同通信可信能力等。

2.4 物联网平台保护技术族(1T)

平台和数据是物联网安全的第3道防线,云端平台及数据的防护包括平台安全、数据存储、处理、传输、开放环节中的安全与隐私保护等。对于云平台本身的保护采用WAF、防火墙、HIDS等手段抵抗恶意攻击,针对物联网数据保护的特殊要求进行防护加强,比如视频数据加密存储,同时要满足各国对于物联网数据隐私的相关要求。

除此之外,在物联网平台和云端可以建立端云协同的防御体系,在云端对于终端的安全状态进行感知、监测和升级,同时采取相对应的安全防护措施。

2.5 物联网安全运维和管理(1M)

物联网安全运维的核心是制定运维人员操作规范和建立安全运维系统工具,从而提升物联网体系事前防范、事中监控、事后处置的安全闭环管理能力。

一方面从端、管、云分层运维管理角度协同处理,具备端到端的全网可视化安全态势感知能力,提供安全评估及运维安全报告、智能化安全检测工具和安全巡检系统工具;另一方面,为物联网运维管理人员提供安全运维指导,在运维操作层面提供安全防御的标准操作流程,从而使能运维人员和决策者的业务管理能力。

在构建3T+1M物联网安全防御体系的过程中,关键技术能力的建设需要通过端、管、云和运维管理的相互协同,才能构筑整个安全防御体系。

3 物联网安全产业合作探讨

物联网产业的健康发展离不开安全保障,物联网安全是一个端到端、全生命周期的体系化工程,在安全生态和标准推动上刚刚起步,需要上下游产业链一起秉承开放合作的理念,群策群力,通力合作,共同推动物联网安全体系的建设。

首先需要整个产业界一起推动物联网安全架构落地应用和不断完善,加快相关国际国内标准的制定,为产业健康发展提供战略指引;其次需要网络运营商和终端、芯片厂家一起加大关键技术的研发投入和应用推广,做到核心技术、加密算法的自主可控;同时,需要应用开发厂家在设计阶段开始考虑安全需求,并且在产品上线后开展安全漏洞管理,快速响应安全威胁;最后,需要整个产业界高度重视用户的数据安全,因为随着可穿戴设备、智能交通、电子医疗等物联网业务的发展,物联网中交互的数据更加重要、更加隐私,甚至关乎用户生命安全,需要终端、网络、应用每个环节都做好数据安全保障,实现合规运营。

万物互联,安全先行。物联网产业安全、健康发展需要产业各方一起,加强行业内和行业间的协同合作,共同打造安全可控的物联网生态体系,迈向万物感知、万物互联、万物智能的全新时代。

参考文献:

[1] IoT Security Guidelines overview document[S/OL]. [2018-08-22]. www.gsma.com/connectedliving.
[2] IoT Security Guidelines for IoT Service Ecosystem[S/OL]. [2018-08-22]. www.gsma.com/connectedliving.
[3] IoT Security Guidelines for IoT EndpointEcosystem[S/OL]. [2018-08-22]. www.gsma.com/connectedliving.
[4] IoT Security Guidelines for Network Operators[S/OL]. [2018-08-22]. www.gsma.com/connectedliving.
[5] 中国联通. 物联网安全技术白皮书[R]. 北京:中国联通,2018.
[6] 中国联通. 5G网络安全白皮书[R]. 深圳:华为技术有限公司,2018.
[7] 张曼君,马铮,张小梅,等. 运营商的物联网安全业务[J]. 中国新通信,2017(1).
[8] 张曼君,马铮,张小梅,等. 物联网环境下的身份认证方案[J]. 邮电设计技术,2017(8).
[9] Vanson Bourne. 2017年全球物联网调研报告[EB/OL]. [2018-10-25]. http://www.199it.com/archives/568269.html.
[10] 施荣华,杨政宇. 物联网安全技术[M]. 北京:电子工业出版社,2013.
[11] 雷吉成. 物联网安全技术[M]. 北京:电子工业出版,2012.

作者简介:
朱常波,中讯邮电咨询设计院有限公司、中国联通网络技术研究院副总经理,高级经济师,博士,主要从事总师技术支撑及科研管理工作;张曼君,高级工程师,博士,主要从事网络与信息安全相关工作;马铮,高级工程师,博士,主要从事网络与信息安全相关工作。