物联网安全标准及防护模型研究概述*

肖益珊[1,2]，张　尼[3]，刘廉如[1,2]，张忠平[1,2]
（1.宜通世纪科技股份有限公司，广东 广州 510630；
2.宜通世纪物联网研究院(广州)有限公司，广东 广州 510665；
3.中国电子信息产业集团有限公司第六研究所，北京 100083）

摘　要： 伴随物联网技术与各垂直行业加速融合渗透，物联网安全重要性日益凸显。首先对物联网安全挑战的新特点进行了总结，分析了物联网安全威胁，对国内外物联网安全政策法规、标准发展和安全模型进行了概述，最后对物联网安全趋势进行了总结和展望。

关键词： 物联网；安全威胁；安全标准；安全模型
中图分类号： TN929.5　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2020.11.001
引用格式： 肖益珊，张尼，刘廉如，等. 物联网安全标准及防护模型研究概述[J].信息技术与网络安全，2020，39(11)：1-7.

Survey of the research on security standard and protection model for Internet of Things

Xiao Yishan[1,2], Zhang Ni[3], Liu Lianru[1,2], Zhang Zhongping[1,2]
(1.Eastone Century Technology Co., Ltd., Guangzhou 510630, China;
2.Eastone Century IoT Research Institute(Guangzhou) Co., Ltd., Guangzhou 510665, China;
3.The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)

Abstract: With the accelerated integration and penetration of IoT technology and various vertical industries, the importance of IoT security becomes more prominent. The paper firstly summarizes the new characteristics of IoT security challenges, analyzes IoT security threats, outlines the domestic and international IoT security policies and regulations, standard development and security models, and finally prospects the IoT security trends.

Key words: Internet of Things; security threats; security standard; security protection model

0 引言

在物联网赋能千行百业，驱动传统行业数字化转型的过程中，大量的传统设备受限于计算能力、节能要求造成安全防护能力不匹配、不同步。终端形态多样化、接入方式泛在化、业务应用融合化、防护边缘模糊化，给物联网业务安全带来很多不确定性。新形势造就新需求，新特性导致新挑战，物联网面临的安全风险与挑战呈现复杂化、多元化、碎片化特点，具体挑战包括：传统行业安全防护起步晚，安全基础设施与安全意识薄弱；分散的终端设备易受攻击，物理保障难；IT和OT的融合，加之连接规模的快速增长，导致攻击面扩大，攻击危害易扩散；用户行为的多样与应用场景的复杂交织缠绕，加剧了威胁特征抽取与识别的难度，建模分析和模式识别应用效果不明显；物联网采集的数据种类多、范围广、类型杂，传统传输协议安全性设计存在缺陷，为用户数据隐私保护增加了难度；物联网业务涉及的合作伙伴多，产业链条长，存在安全

* 基金项目：广东省重点领域研发计划(2019B010109001)；科技部网络协同制造平台功能安全保障关键设备和系统项目(2019YFB1706001)；中国工程院重大咨询项目(2019-ZD-12)

责任边界模糊、界面划分不清的风险[1-3]。

1 安全威胁分析与建模

物联网安全威胁分析与建模对物联网安全需求的归纳总结、安全防护方案的制定至关重要。安全威胁建模的步骤包括：识别待保护的资产、创建物联网架构视图、识别威胁、记录威胁、对威胁进行评级。

常用的威胁识别技术包括威胁识别模型 STRIDE 和威胁评级模型 DREAD。STRIDE 模型用来识别常见的 6 种威胁，包括身份假冒(Spoofing)、篡改(Tampering)、抵赖(Repudiation)、信息泄露(Information Disclosure)、拒绝服务(Denial of Service)、权限提升(Elevation of Privilege)。DREAD 模型用来对威胁进行评级，包括潜在的损失(Damage Potential)、重现性(Reproducibility)、可利用性(Exploitability)、受影响用户(Affected users)、可发现性(Discoverability)。

通常，物联网体系架构包括感知层、网络层、平台层和应用层，对各层主要安全威胁进行分析，可以进一步总结对应的安全需求[2,4-7]。

感知层的安全威胁主要包括物理攻击、终端缺乏更新机制导致的软件漏洞风险、病毒或恶意软件感染、恶意访问或操控、伪造或假冒攻击、信号泄露与干扰、资源耗尽攻击、敏感数据泄露威胁、服务中断风险等。

网络层的安全威胁主要包括网络安全协议漏洞和缺陷；异构网络融合引入的身份认证、密钥协商、数据机密性与完整性保护等问题；无线传输中数据被窃取、篡改或删除问题；非授权接入和访问网络；阻塞干扰、女巫攻击、洪泛攻击、选择转发攻击、非公平攻击、碰撞攻击、拒绝服务攻击、中间人攻击和假冒基站攻击；运营商网络侧批量应急管控风险等。

平台层的安全威胁主要包括隐私数据泄露、恶意代码攻击等安全攻击；虚拟机逃逸、虚拟机镜像文件泄露、虚拟网络攻击、虚拟化软件漏洞等虚拟化安全问题；平台组件、操作系统和服务程序漏洞和设计缺陷导致未授权访问、数据篡改和泄露等；篡改数据的重编程攻击、数据服务阻塞、错乱定位服务攻击、破坏隐藏位置目标攻击、破坏数据融合的攻击等。

应用层威胁主要包括病毒、蠕虫、木马、不受欢迎应用程序、远程攻击和人员威胁等。

2 政策与标准

2.1 政策法规

世界各国在物联网安全领域积极推动相关政策法规、技术规范制定和标准化工作[8]。

美国对物联网安全十分重视，从战略、政策、立法等维度协同推进物联网安全的落地实践。2016 年 12 月，美国国土安全部发布了《物联网安全策略原则》，制定了设计、制造和部署物联网设备的安全原则，包括：设计阶段需考虑的安全问题；漏洞管理、修复及安全更新；最佳安全实践及操作方法；基于风险管理优先级聚焦安全措施；提升供应链透明性；持续接入互联网，永久在线必要性的判定等。2017 年 8 月，美国两党议员向国会提交了一份关于物联网安全的法案《2017 物联网网络安全改进法》，旨在通过制定政府采购和使用物联网设备的行业安全标准来改善美政府所面临的物联网安全挑战。2018 年 1 月，美国商务部与国土安全部联合出台网络安全报告草案《提高互联网与通信生态系统对僵尸网络及其他自动分布式威胁的抵御能力》。2019 年 6 月，美国政府通过了《2019 年物联网网络安全改进法案》，该法案希望对联邦政府采购和使用的任何物联网设备设定最低的安全标准，以确保网络安全的基线。

欧盟对物联网安全的保障工作侧重在安全基线的设置及用户隐私数据的保护。2017 年 11 月，欧洲网络和信息安全管理局发布了《欧盟关键信息基础设施环境中的物联网安全基线指南》，梳理分析了物联网的安全需求、威胁态势、风险趋势，提出了物联网安全基线分析框架，旨在为欧盟在关键信息技术设施领域应用物联网提供部署指导和实践指南。2018 年 5 月 25 日正式生效的欧盟《通用数据保护条例》(General Data Protection Regulation，GDPR)，为保护欧盟用户个人数据提供了重要法律依据，在增强数据主体对于个人数据的控制能力同时，也对企业保障实现数据主体的权利提出了具体要求，如规定了企业对客户数据的搜集、存储、使用的规范和准则。

日本将终端设备安全保护作为对于物联网安全防护的核心和重点。2017 年 10 月，总务省基于内阁网络安全中心发表的《关于物联网系统安全的总体框架》出台了《物联网安全综合对策》，提前部署物联网安全对策。2019 年 2 月，总务省设立新规，

要求物联网设备必须具有防非法登录功能，并于2020年4月开始实行。

中国物联网安全战略定位清晰明确，采取顶层设计与应用推广相结合，技术手段和管理措施统筹兼顾的策略。2013年2月，国务院颁布了《关于推进物联网有序健康发展的指导意见》，指出了建立健全物联网安全测评、风险评估、安全防范、应急处置等机制。2016年12月，工信部发布了《信息通信行业发展规划物联网分册（2016－2020年）》，明确了要增强物联网基础设施、重大系统、重要信息等安全保障能力。2020年5月，工信部发布了《关于深入推进移动物联网全面发展的通知》，指出了要从移动物联网基础安全夯实、移动物联网安全防护和数据保护加强等方面建立健全移动物联网安全保障体系。

2.2 安全标准

在标准制定方面，ISO/IEC、ITU－T、ETSI、全国信息安全标准化技术委员会（SAC/TC260）、中国通信标准化协会（CCSA）等国内外标准组织积极推进物联网安全标准化工作。

ISO/IEC JTC1/SC27（信息技术委员会/安全技术分委员会）、SC41（物联网及相关技术分委员会）、SC25（信息技术设备互联分委员会）分别围绕着信息安全、物联网技术、智能家居、家庭网关等领域制定相关标准，如安全体系架构、轻量级加密、认证鉴权、隐私控制与保护等安全技术。

ITU－T SG17（安全研究组）负责物联网通信安全研究和标准制定工作，SG20/Q6（物联网和智慧城市研究组/安全、隐私保护、信任和识别课题组）侧重于物联网和智慧城市的安全标准。SG17围绕安全框架、加密规程、窄带物联网安全要求、物联网安全事件操作日志格式、安全控制措施、设备和网关安全要求、平台安全要求与框架等方面规划了物联网安全系列标准。

ETSI（欧洲电信标准化协会）网络安全技术委员会于2019年2月发布了《消费类物联网安全》，旨在提供联网消费类物联网设备的安全基线，为物联网的认证授权、安全威胁评估、安全机制分析等领域奠定基础。

针对物联网安全问题，我国也在积极布局和推进物联网安全标准制定工作。以全国信息安全标准化技术委员会（SAC/TC260）、中国通信标准化协会（CCSA）、车载信息服务产业应用联盟（TIAA）、工业互联网产业联盟（AII）为代表的国内相关标准化机构、产业联盟纷纷启动开展了物联网安全相关标准体系的建设工作。图1所示为物联网安全标准主题。

全国信息安全标准化技术委员会（SAC/TC260）在2018年12月28日正式发布了27项国家标准，

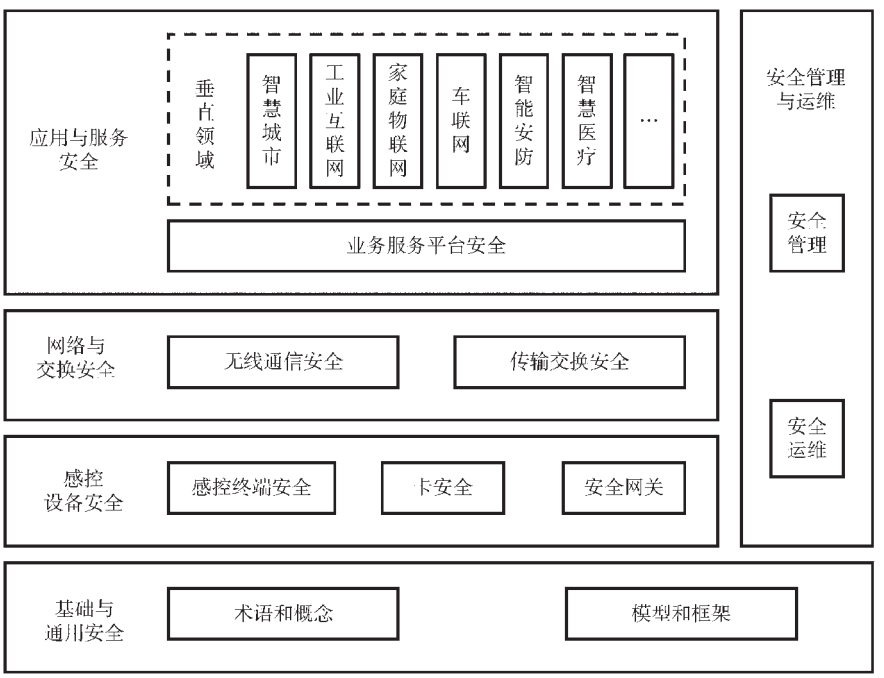

图1 物联网安全标准主题

其中涉及物联网安全的有《信息安全技术物联网安全参考模型及通用要求》《信息安全技术物联网感知终端应用安全技术要求》《信息安全技术物联网感知层网关安全技术要求》《信息安全技术物联网感知层接入通信网的安全要求》《信息安全技术物联网数据传输安全技术要求》5 个标准，已于 2019 年 7 月 1 日正式施行。

中国通信标准化协会(CCSA)在物联网安全的标准化工作主要聚焦在通信网络和系统，由 TC5(无线通信技术委员会)和 TC8(网络与信息安全技术委员会)负责标准制定，规划和完成的代表性标准包括《物联网管理平台安全防护要求》《物联网标识解析安全技术要求》《基于 SIM 卡的物联网安全服务技术要求》《物联网类终端通用安全技术要求和测试方法》《物联网安全态势感知技术要求》《基于信任根的物联网设备系统安全技术要求》《物联网感知层协议安全技术要求》《物联网终端嵌入式操作系统安全技术要求》《物联网安全分级分类管理技术要求》等。

国内外的相关标准组织围绕着物联网的基础与通用安全、感知设备安全、网络与交换安全、应用与服务安全、数据安全、安全管理与运维等方面开展全面的标准制定工作。在政策引导和标准牵引下，产业界围绕安全技术、安全产品、安全解决方案和安全服务等领域构建健康的安全生态，驱动物联网与各行各业相互渗透，为构建自主安全、开放协同、融合共享的产业环境，共同构筑物联网安全的防护网。

3 安全模型

3.1 SerIoT 物联网安全参考模型

SerIoT 项目旨在通过集成认知路由的 SDN、雾计算、物联网蜜罐、区块链、可视化分析、决策支持和基于硬件启动的物联网设备认证等技术提供架构驱动的安全解决方案，以解决广泛的物联网网络安全威胁[9]。

综合考虑物联网端到端系统视图的全面性和社区的开放性与活跃度，SerIoT 物联网安全参考模型选择基于 ISO/IEC 30141 物联网参考体系架构。ISO/IEC 30141 物联网参考架构的域视图如图 2 所示，包括物理实体域(Physical Entity Domain，PED)、

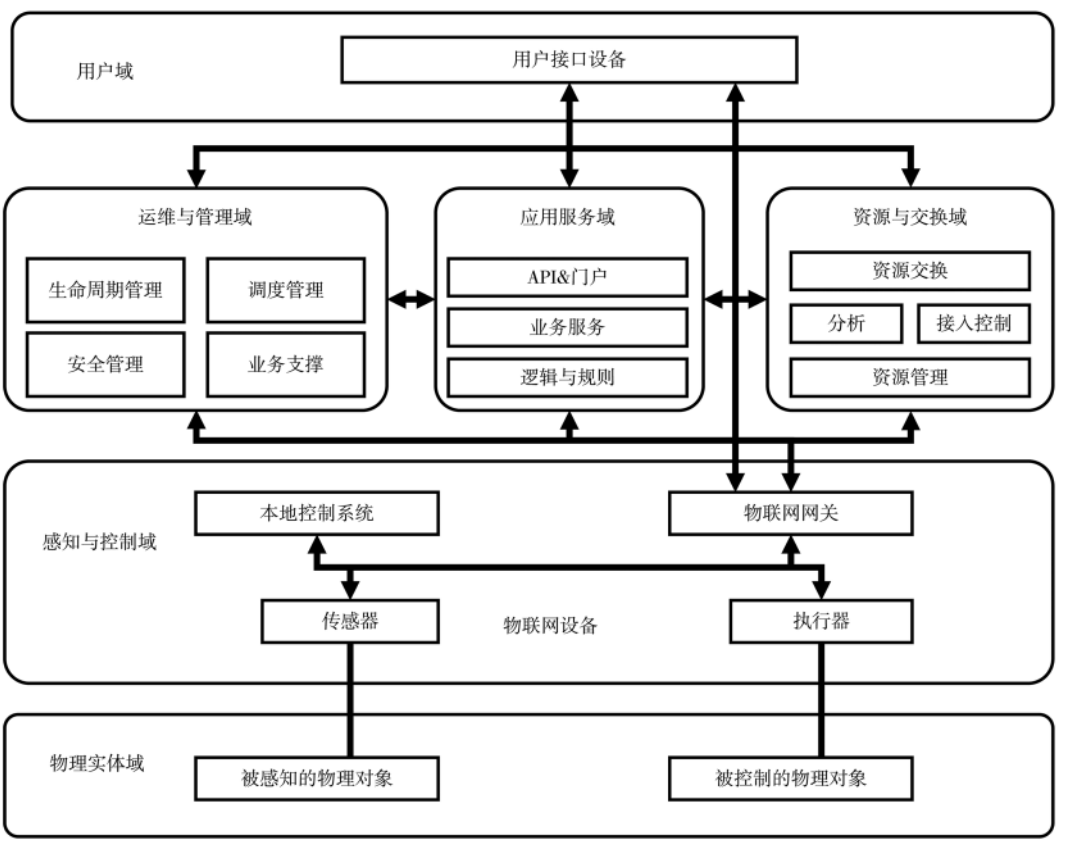

图 2 ISO/IEC 30141 物联网参考架构域视图

传感与控制域(Sensing&Controlling Domain, SCD)、运营和管理域(Operation&Management Domain, OMD)、资源与交换域(Resource&Interchange Domain, RID)、应用服务域(Application Service Domain, ASD)和用户域(User Domain, UD)。

SerIoT 物联网安全参考模型由 SerIoT 管理功能和 SerIoT 网络基础架构两部分组成。SerIoT 管理功能解决物联网网络管理,物联网监控、异常检测与决策支持, 物联网设备安全与隐私保护;SerIoT 网络架构以 SDN 基础设施、物联网蜜罐和雾节点/边缘节点为基础。模型架构如图 3 所示。

SerIoT 管理域支持传感与控制域、应用服务域、资源与交换域之间的安全网络通信,并在决策支持和可视化分析的上下文为 SerIoT 用户域提供管理接口,以实现人为应对安全风险和实施安全对策。

SerIoT SDN 基础设施通过边缘转发器和核心转发器实现使能物联网网络通信,SerIoT 路由引擎是网络管理功能的核心,SDN 控制器在边缘和核心转发器上执行路由决策。

SerIoT 雾计算协调基板(Fog Computing Coordination Substrate)负责在边缘侧提供计算和存储资源,实现资源和服务的分层管理和编排,能够通过专用的、靠近边缘的雾节点向物联网设备提供高效透明的服务分发。SerIoT 雾管理和网络编排(Fog MANO)负责在网络层级和雾节点管理和控制雾基板。

SerIoT 蜜罐是模拟物联网设备、网关或路由器,实现数据采集、恶意流量和恶意软件分析的二层虚拟环境。

SerIoT 模型通过基于策略的框架和物联网设备启动服务,定义物联网设备的安全和隐私保护的特定方案,并且利用区块链技术实现物联网设备状态和重要事件的可信上报。

3.2 GB/T 37044 物联网安全参考模型

GB/T 37004-2018《信息安全技术 物联网安全参考模型及通用要求》从物联网系统参考安全分区、系统生存周期和基本安全防护措施三个维度描述了物联网安全参考模型[10],如图 4 所示。

物联网参考安全分区从物联网系统的逻辑空间维度出发,基于物联网参考体系架构,依据每一个域及其子域的主要安全风险和威胁,归纳相应的安全防护需求,形成感知安全区、网络安全区、应用安全区和运维安全区等安全责任逻辑分区。

系统生存周期从物联网系统存续时间维度出发,将物联网系统划分为规划设计、开发建设、运维管理、废弃退出四个阶段,并定义各阶段的安全任务目标和安全防护需求。

基本安全防护措施从物理安全、网络安全、系统安全、应用安全、运维安全和安全管理等方面,采取技术手段和管理手段并重的措施。

3.3 3T+1M 安全架构

提出的“3T+1M 安全架构”旨在应对物联网基础架构中感知层、网络层和应用层的安全风险和威

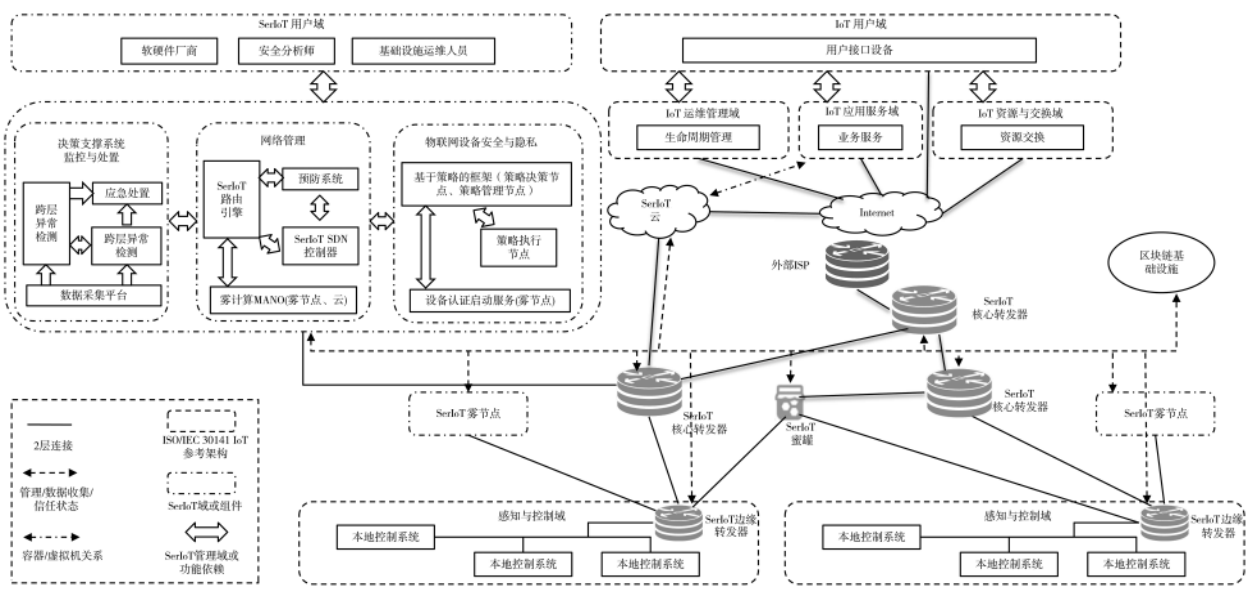

图 3 SerIoT 物联网安全参考模型

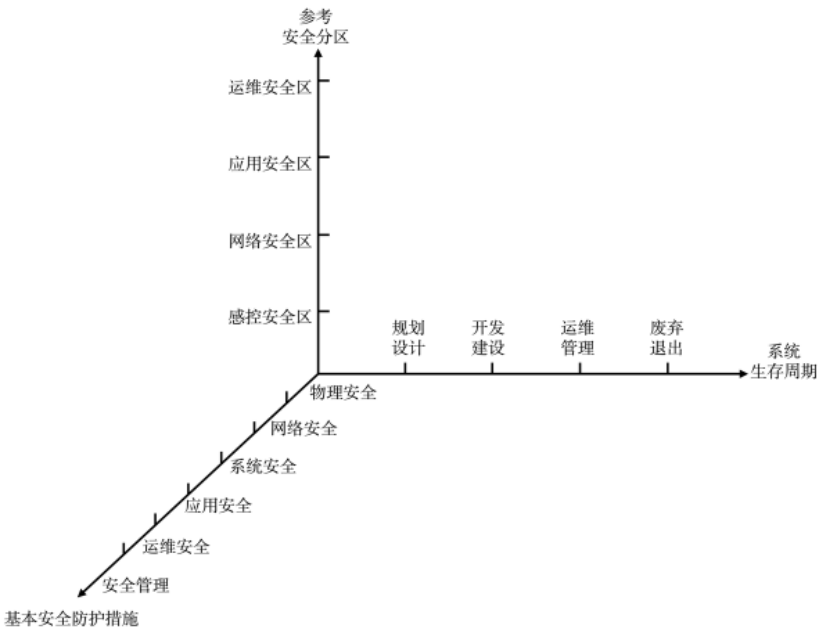

图 4 GB/T 37004 物联网安全参考模型

网安全防线，实现纵深防御[3，11－12]。

3T+1M 物联网安全架构如图 5 所示，其核心在于终端防御、网络保障和平台保护 3 个物联网安全技术族(Technologies)和 1 个安全运维与管理(Management)，以应对多样化的物联网应用和业务安全威胁，构建物联网端到端安全防御体系。

物联网终端防御技术(1T)从保障贯穿物联网终端全生命周期的安全角度出发，采用系统分域隔离防御、远程升级修复以及设置终端之间的多重微边界安全防线等技术手段，实现可信认证的终端接入安全，以及海量终端可视化统一安全管控。

物联网网络保障技术(1T)从网络角度来补充物联网终端防御的不足，从终端数据中挖掘和识别恶意行为的特征，基于恶意软件特征库和恶意行为模型库实现行为威胁和攻击威胁的快速检测、决策和处置。

胁，侧重端、管、云/平台的安全协同，提供物联网全局化安全态势感知和分析检测能力，全方位构建物联

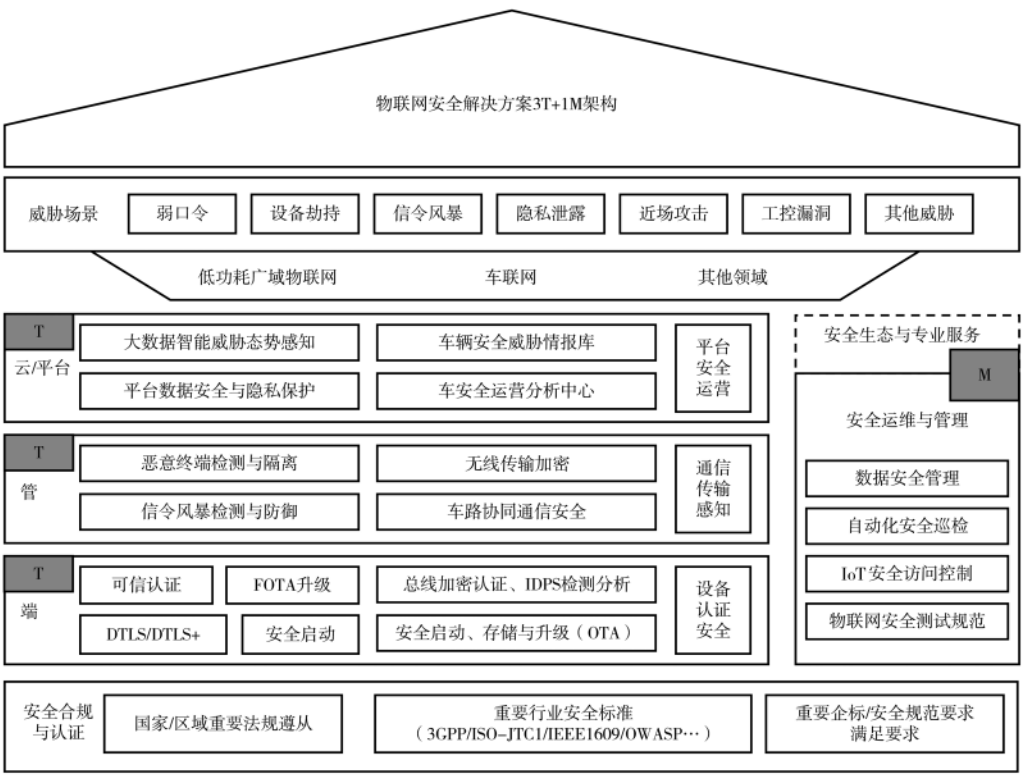

图 5 物联网安全 3T+1M 架构

物联网平台保护技术(1T)从平台和数据角度为物联网安全筑起第三道防线,聚焦物联网平台的安全态势感知、数据安全与隐私保护,保障物联网平台的基础环境安全、系统可用性、接入安全、数据安全和 API 安全等。

物联网安全运维和管理(1M)的关键在于制定安全运维的操作指南和应急流程规范,构建完善安全运维工具,提升物联网事前预防、事中监控和事后处置的安全闭环管理能力。

根据上述物联网安全模型和架构分析可见,基本思路是构建分区分域分阶段的端到端安全纵深防御体系。利用安全态势感知、多域分层入侵检测、轻量级安全协议、恶意终端隔离、软件定义安全边界、协同防御等关键技术实现“云-管-端”协同联动的闭环安全管理体系。

4 结论

“万物互联,安全先行”。物联网的多源异构性、开放性、泛在性使其面临巨大的安全威胁,加之物联网终端和应用的多样性和复杂性,物联网安全问题面临更为严峻的挑战。

物联网安全发展经历了单一产品安全、端到端解决方案安全,正在向整体架构安全演进,以满足不同垂直领域应用场景的个性化安全需求。软件定义边界、计算资源受限的终端节点轻量化安全协议(认证加密、密钥管理、安全认证、密钥协商等)、去中心化可信认证、边缘计算安全、跨域设备身份可信认证、安全态势感知、安全可视化、虚拟化等新技术不断涌现,物联网安全产品在产业(工业互联网、泛在电力物联网等)和技术(大数据、人工智能、区块链等)的融合驱动下持续创新升级。

针对物联网发展可能面临的网络安全新形势、新需求和新特性,需要从健全物联网安全技术标准、构建适应物联网环境的安全防护机制、搭建物联网全生命周期立体防御体系、探索新技术在物联网安全领域新应用等方面,联合物联网产业链各方力量,共同打造物联网安全生态,促进物联网产业健康良性发展。

参考文献

[1] 中国电信网络与信息安全研究院,绿盟科技.2019 物联网安全年报[R].北京:中国电信网络与信息安全研究院,2019.

[2] 中国信息通信研究院,中国移动信息安全管理与运行中心.物联网安全白皮书(2018 年)[R].北京:中国信息通信研究院,2018.

[3] 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.

[4] 信息安全与通信保密杂志社,梆梆安全研究院.2016 物联网安全白皮书[R].北京:信息安全与通信保密杂志社,2017.

[5] 中国电信安全帮,绿盟科技.2017 物联网安全研究报告[R].北京:中国电信,2017.

[6] 王和,杨华,高福兵.物联网安全[J].四川兵工学报,2011(11):90-91,109.

[7] 武传坤.物联网安全关键技术与挑战[J].密码学报,2015,2(1):40-53.

[8] 全国信息安全标准化技术委员会通信安全标准工作组.物联网安全标准化白皮书(2019 版)[R].北京:全国信息安全标准化技术委员会,2019.

[9] SERIOT.Reference architecture for secure and safe Internet of Things by the seriot project[EB/OL].(2019-01-14)[2020-09-04].https://seriot-project.eu/2019/01/14/reference-architecture-for-secure-and-safe-internet-of-things-by-the-seriot-project/.

[10] GB/T 37044-2018 信息安全技术 物联网安全参考模型及通用要求[S].2018.

[11] 中国联通,华为.物联网安全技术白皮书(2018)[R].北京:中国联通,2018.

[12] 张曼君,马铮,高枫,等.物联网安全技术架构及应用研究[J].信息技术与网络安全,2019,38(2):4-7.

(收稿日期:2020-09-07)

作者简介:

肖益珊(1976-),男,工程师,主要研究方向:物联网、5G、工业互联网。

张尼(1979-),男,博士后,教授级高级工程师,主要研究方向:信息安全、大数据、工控安全等。

张忠平(1965-),通信作者,男,教授级高级工程师,主要研究方向:物联网、5G、工业互联网。E-mail:zhangzhongping@etonetech.com。