计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.20220510
59(10):2190-2211,2022

物联网访问控制安全性综述

刘奇旭[1,2] 靳 泽[1,2] 陈灿华[1,2] 高新博[1,2] 郑宁军[1,2] 方仪伟[1,2] 冯 云[1]
[1](中国科学院信息工程研究所 北京 100093)
[2](中国科学院大学网络空间安全学院 北京 100049)
(liuqixu@iie.ac.cn)

Survey on Internet of Things Access Control Security

Liu Qixu[1,2], Jin Ze[1,2], Chen Canhua[1,2], Gao Xinbo[1,2], Zheng Ningjun[1,2], Fang Yiwei[1,2], and Feng Yun[1]
[1](*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)
[2](*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049)

Abstract In recent years, Internet of things (IoT) security incidents have occurred frequently. As an important security mechanism, IoT access control plays an important role. However, the existing Internet access control policies cannot be directly applied to the IoT scenarios because of the differences between IoT and Internet. At present, the IoT access control schemes have not paid attention to the security issues. Once the IoT access control is broken, it will cause serious consequences such as privacy data leakage and authority abuse. Thus, it is urgent to comprehensively study the security issues and solutions for access control of IoT. According to the complex architecture, the variety of devices, low storage and computing performance of IoT, the protection surface and trust relationship in IoT access control is combed, the trust chain is built and the risk transmission law in the trust chain is discussed. Around the protection surface and trust chain, we summarize the existing access control attack surface from the perception layer, network layer, and application layer, and analyze the existing security risks. In view of these security risks, we present the necessary access control security demand, including mechanism improvement, attack surface answer, multilevel authentication and authorization, and the combination with specific scenarios. Based on the requirements, the existing security solutions and targeted access control framework are summarized. Finally, we discuss the challenges faced in IoT access control and point out the future research direction that consists of an in-depth study on access control of the cloud platform of IoT, IoT cloud docking standardization, and the introduction of zero trust concept.

Key words Internet of things (IoT); access control; security; trust chain; attack surface

摘 要 近年来物联网安全事件频发,物联网访问控制作为重要的安全机制发挥着举足轻重的作用.但物联网与互联网存在诸多差异,无法直接应用互联网访问控制.现有的物联网访问控制方案并未重视其

收稿日期:2022-06-11;**修回日期**:2022-08-12
基金项目:中国科学院青年创新促进会(2019163);中国科学院战略性先导科技专项项目(XDC02040100);中国科学院网络测评技术重点实验室项目;网络安全防护技术北京市重点实验室项目
This work was supported by the Youth Innovation Promotion Association CAS (2019163), the Strategic Priority Research Program of Chinese Academy of Sciences (XDC02040100), the Project of CAS Key Laboratory of Network Assessment Technology, and the Project of Beijing Key Laboratory of Network Security and Protection Technology.
通信作者:冯云(fengyun@iie.ac.cn)

中的安全性问题,物联网访问控制一旦被打破,将造成隐私数据泄露、权限滥用等严重后果,亟需对物联网访问控制的安全性问题与解决方案进行综合研究.根据物联网架构复杂、设备多样且存储与计算性能较低的特性,梳理了物联网访问控制中的保护面和信任关系,形成信任链,并论述了信任链中的风险传递规律.围绕保护面和信任链,从感知层、网络层、应用层分别综述了现有的访问控制攻击面,分析了存在的安全风险.针对安全风险提出了应有的访问控制安全性要求,包括机制完善、应对攻击面、多级认证与授权、结合具体场景,基于这4个要求总结了现有的安全性解决方案和针对性的访问控制框架.最后讨论了物联网访问控制设计中所面临的挑战,指出了深入研究物联网云平台访问控制、物联网云对接标准化、引入零信任理念3个未来的研究方向.

关键词 物联网;访问控制;安全性;信任链;攻击面

中图法分类号 TP391

物联网(Internet of things, IoT)起源于20世纪90年代末期,最初的概念是建立一套无线射频识别(radio frequency identification, RFID)系统,以实现智能化的RFID管理[1].随着网络技术的发展,物联网已经从最初的几个设备互相连接的小型网络,发展成了人与物、物与物之间复杂而庞大的网络.到了今天我们的生活中的物联网设备已经随处可见,比如智能网关、智能监控、智能手表、智能台灯,涉及家具、医疗、交通、办公等各个领域.在2021年,全球的物联网市场增长了22%,达到了1 580亿美元,尽管受到了新冠疫情影响,但增长速度仍然十分迅猛.根据IoT Analytics的预测,"到2022年全球的物联网设备数量将达到145亿台"[2].在物联网产业飞速发展的同时,其所面临的安全问题日益剧增.根据Gartner在2020年1月发布的统计,有大约20%的组织和机构受到过基于物联网的攻击,绝大部分的组织和机构暴露在物联网的风险之下[3].

物联网秉承着"万物互联"的理念,深入渗透人类社会生产生活的方方面面,面临着多种多样的安全威胁.一方面,物联网承载了规模庞大的隐私数据,并且这些数据在物联网的终端、网络、云端之间传播,扩大了隐私数据的暴露面,增加了数据泄露风险;另一方面,物联网具备了一定的控制和操作权限,一旦被攻击者渗透并实施篡改或破坏,将对人类社会正常的生产生活造成严重威胁.

近年来发生了多起物联网相关的攻击事件,比如大众汽车的Polo被发现其信息娱乐系统存在安全漏洞,攻击者有可能获取大量的个人信息包括电话联系人和位置信息[4].而一些医疗用途的物联网设备的安全漏洞甚至会影响人们的生命安全,2017年就有报道指出一些植入式心脏起搏器或除颤器存在安全漏洞,攻击者利用这些安全漏洞可以使得设备无法正常工作[5].这些安全威胁不仅可以影响物联网设备的使用者,还可以通过控制这些物联网设备来攻击其他目标,比如2016年爆发的Mirai僵尸网络通过利用物联网设备进行了大规模的分布式拒绝服务攻击[6].物联网的安全风险是物联网发展中的巨大挑战,如果能成功缓解这些安全危机,物联网将给人们的生活带来极大的便利,否则,如果物联网漏洞被恶意的组织利用,那么对国家的安全、个人的隐私都会造成严重的威胁.因此,必须要加强物联网在数据、资源、权限等方面的安全研究,提升物联网资源请求、权限授予等访问控制的安全性.

本文将聚焦物联网的访问控制,从物联网的3个层次[7]:感知层、网络层、应用层,分别展开探讨.访问控制是计算机中关键的安全机制,它通过控制什么权限的主体可以访问什么类型的客体,来保证数据和资源免受未经授权的读取或修改,并且确保合法用户可以正常访问资源.访问控制作为信息安全的基石,有效地保证了网络空间的安全与秩序,一个完善的访问控制机制,可以为信息资源建立一个有效的屏障,以阻止其被非法地读取或修改,但在新型的物联网领域,相关的访问控制技术仍然不够完善.物联网有着相比于互联网更复杂的组织架构,涉及到应用、协议、硬件、云等一系列的访问控制参与环节,无法像传统的互联网应用的访问控制一样简单地控制用户与资源的关系.物联网在不同的场景下需要不同的访问控制策略,因此应当分层次、分场景地进行设计,才能有效地保证物联网访问控制的安全性[8].

目前,已经有学者就物联网安全性问题[9-10]、智能家居场景中的安全性[11-12]、物联网操作系统安全性[13]等方面的研究工作进行了综述,但还没有工作聚焦于物联网访问控制的安全性进行系统性梳理.

鉴于物联网访问控制安全性的重要意义,本文对近10年网络与信息安全领域四大顶级会议、期刊等来源的相关研究进行了广泛调研与梳理,从物联网访问控制的风险脆弱点入手,归纳可能的攻击面,从而提出应有的安全性要求,总结现有工作进展,为后续进一步的研究指明方向.本文的主要贡献总结为3个方面:

1) 分析了物联网3个层次间的数据流向与信任关系,提出了物联网访问控制信任链模型,围绕3个层次并结合信任链带来的风险传递,调研并总结了现有物联网访问控制的安全威胁研究,在物联网不同层次结构中分析了其安全问题和暴露出的攻击面;

2) 调研并总结了不同层次结构中针对不同的访问控制安全问题和攻击方法的解决方案以及应有的安全性设计要求;

3) 基于现有的研究基础,分析了物联网访问控制安全性研究的挑战与机遇,并给出了未来的研究方向.

1 研究背景

本节首先对相关的研究背景与基础知识进行介绍,明确物联网及访问控制领域的相关概念,并提出一个针对物联网复杂组织架构的"信任链"概念,从而探讨安全的物联网访问控制设计.

1.1 物联网基础知识

设备、网络协议、云平台和应用App之间的相互作用构成了物联网的体系大厦,学术界通常将物联网系统的体系架构分为感知层、网络层、应用层3个层次[10].感知层对应的是物联网各类设备,其上搭载了红外感应、射频识别等多种类型的传感器,主要负责识别和采集物理世界的数据;网络层对应的是各类通信协议,负责在感知层和应用层之间传递数据;应用层对应的云平台和应用App中的各类接口和服务,也是用户与物联网的接口,负责数据处理、计算以及智能决策.物联网业务的全生命周期的本质即数据的流转过程.网络协议存在于设备、云平台、应用App这3类实体之间,以及设备与设备之间、云平台与云平台之间,使得它们能够及时进行各类交互,在交互中传递数据,形成物联网数据链.通过物联网数据链,一个简单的物联网设备可以将自己的数据(如传感器数据)传递给用户App或云平台,而物联网用户或物联网的控制者也可以借助云平台,远程控制或监控自己的物联网设备.下面本文将针对4个简单的使用场景,对物联网数据流进行描述.值得注意的是,以下叙述的场景仅仅是相对流行的方案,现实中同样的使用场景可能出现完全不同的解决方案.

1) 远程控制设备

当用户远程使用App控制物联网设备时,App端将会与云平台建立通信,并将控制指令发送给云平台,云平台接收到控制指令,将会把用户的控制指令翻译为设备能够理解的控制信息,并发送给设备.

2) 远程监控设备

设备和云平台之间首先建立通信.设备将数据发送给云,云端会将这部分数据暂存.当用户打开App并查看设备状态时,云端将暂存的最新设备上报数据发送给用户.

3) 本地控制设备

本地控制设备一般依赖于近场通信协议或局域网通信.但对于以云通信为主的设备,需要设备先在云平台上进行注册.也就是说,本地控制设备在远程控制设备条件存在的情况下,通常是远程控制设备的一种简化.

4) 自动化编程控制设备

自动化编程控制设备是指在云平台上编写程序,通过触发器触发程序执行(例如当温度达到28摄氏度时打开空调),这种情况下需要用户将自己的程序上传到云平台.

1.2 访问控制基础知识

访问控制是一种通过对资源的访问、获取和操作进行身份验证和授权管理,使资源能够在合法范围内被使用或受限使用的技术,是维护网络安全、数据安全的重要措施.

访问控制是主体根据策略对客体进行不同权限访问的过程,主要包括五大要素:主体、客体、认证、授权以及策略.

1) 主体.主体是能够访问客体的实体,包括人、进程或者设备等具有能够访问客体属性的实体,主体可以在系统中执行操作、在客体之间传递信息或者修改系统状态.

2) 客体.客体是系统中需要被保护的实体的集合,包括文件、记录、数据块等静态实体,也包括进程等可执行指令的实体.

3) 认证.认证是指访问控制客体对主体进行身份确认的过程,从而确保主体具有其所请求的权限.

4) 授权.授权是指授予某个主体对某资源的访

问权限的过程,强调的是某个主体可以对某资源进行哪些操作(读、写、执行等).

5) 策略.策略是指主体对客体访问的规则集合,规定了主体对客体可以实施读、写和执行等操作的行为,以及客体对主体的条件约束.策略体现的是一种授权行为,授予主体对客体何种类型的访问权限,这种权限应该被限制在规则集合中.

有效的访问控制保证只有经过授权的主体才能够在权限范围内访问客体,未经授权的主体禁止访问客体,能够很好地防止隐私信息的泄露和权限的滥用.

访问控制技术经过多年的演进,已经产生了多种类型的访问控制模型,包括自主访问控制(discretionary access control, DAC)[14]、强制访问控制(mandatory access control, MAC)[15]、基于角色的访问控制(role-based access control, RBAC)[16]、基于属性的访问控制(attributed based access control, ABAC)[17]、基于使用控制的访问控制(usage control, UCON)[18]、基于权能的访问控制(capability-based access control, CapBAC)[19]等.

1) 自主访问控制.自主访问控制的核心思想是自主授权,主体可以完全控制客体,并可以自己决定是否将对客体的访问权限或部分访问权限授予其他主体.这种访问控制方式权限管理分散,而且需要手动对权限进行管理,在面对庞大且复杂的物联网时,难以适应物联网的动态自发性、可操作性等特性.

2) 强制访问控制.强制访问控制的核心思想是系统强制主体服从访问控制策略,系统为主体和客体分配不同的安全标识,主体和客体不能够自行改变自身的安全标识,只能由系统或管理员强制分配,根据安全标识决定主体对客体的访问许可,本质是利用非循环单项信息流保证数据的机密性和完整性.

3) 基于角色的访问控制.基于角色的访问控制的核心思想是将访问权限与角色相关联,通过将权限分配给角色,再让用户成为适当的角色,从而使得用户得到这些角色的权限,根据用户的角色决定用户对资源的访问权限.这种访问控制方式在涉及大量角色的物联网环境中会存在角色爆炸问题,同时也难以满足物联网中细粒度、多层次的访问控制需求.

4) 基于属性的访问控制.基于属性的访问控制的核心思想是根据主体的属性授予访问权限,主体和客体都是通过与特征相关的属性进行识别,当用户发起访问请求时,根据他的属性授予相应的访问权限.这种访问控制方式由于其属性在访问过程中不可以改变,无法满足物联网中节点属性动态改变的需求,同时随着设备数量的增加,会增加策略管理的工作量和复杂性.

5) 基于使用控制的访问控制.基于使用控制的访问控制的核心思想是属性可变和持续检查,当主体发起访问请求时,授权元素检查主体和客体的安全属性以决定是否允许访问,这种检查持续伴随着整个访问过程,在访问过程中,一旦主体或者客体的安全属性发生改变,授权将相应地改变,撤销授权或支持继续访问.

6) 基于权能的访问控制.基于权能的访问控制的核心思想是根据权能(密钥、令牌等)授予用户相对应的访问权限,一种权能拥有对某些资源的访问权限,系统仅允许权能拥有者对这些资源的访问,拒绝其他访问.此外,主体可以将其全部或部分访问权限通过委托机制授予其他主体,同时支持主体撤销其所授予的权能,这使得 CapBAC 具有分布式、细粒度等优点.

随着云计算、物联网等新技术和新场景的不断涌现,引发了源源不断的新威胁、新风险.尤其是面对复杂多变的物联网环境,传统的访问控制模型的灵活性和扩展性不足,难以适应规模庞大、数据激增、变化迅速的物联网环境;固化的访问控制策略难以应对物联网中访问控制参与对象类型多样的特性.

1.3 物联网访问控制

物联网访问控制即物联网场景下的访问控制技术,用于保障设备、用户、云端之间资源请求与权限授予过程的安全合规.相较于互联网访问控制,其区别主要在于 4 点:

1) 计算与存储能力不同.物联网中存在大量的各类轻量级感知层设备,通常设备容量低,不支持复杂的运算、数据存储,难以参照互联网设备建立较强的安全边界,也因此成为攻击者的重点目标.

2) 体系架构不同.由于设备的性能较低,物联网中的运算、决策主要依靠云平台来实施、对接并下发,无法复用互联网中心化的访问控制架构.同时物联网架构导致数据的传输和交互更加频繁,扩大了风险暴露面.

3) 通信协议不同.在互联网中,有线通信协议更加普及,而物联网中由于大量设备的存在,无线通信协议更加常用,因此无线通信协议的安全性更加重要.物联网设备的异构性也提高了对通信协议的要求.在协议模型方面,互联网中“请求/响应”模型的通信协议更加普及,而物联网由于大量设备存在,

并且通信存在大量不稳定因素,引入了很多“发布/订阅”模型的通信协议.

4) 业务场景不同.互联网访问控制的业务场景主要是控制数据资源的访问,而物联网的业务场景更加多样化、与物理世界更加密切相关,包含家居、医疗、工业控制等,不同场景中的设备性能、具体架构、安全需求都有所区别,需要具体问题具体分析.

因此,物联网访问控制与互联网访问控制不尽相同.真实世界中发生的安全威胁虽然只是由某一个物联网实体(设备、云等)的安全缺陷触发,但危害却可以通过物联网数据链传递到其他实体,而物联网数据链构建的基础是实体之间的信任关系,也就是访问控制信任链.

如图 1 所示,用户 App、云平台、设备都有各自独立的访问控制模型.对于云平台,云平台作为访问控制客体,设备和用户作为访问控制主体,云平台需要对设备和用户进行认证,在接入层面需要验证设备和用户是否有权接入云平台,在交互层面需要验证用户是否有权访问设备;对于用户 App,App 作为访问控制客体,设备和云平台作为访问控制主体,App 需要首先验证云平台的真实性,防止中间人攻击;对于设备,设备作为客体,云平台和用户 App 作为主体,设备要对云平台进行认证.这样,用户 App、云平台、设备之间通过各自独立的访问控制模型形成一个相互的信任关系,产生访问控制信任链.

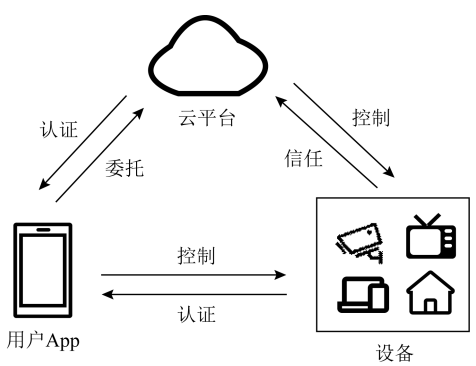

Fig. 1 Trust chain of IoT access control

图 1 物联网访问控制信任链

对于访问控制信任链,存在 3 个攻击面:1)攻击者可以直接绕过物联网设备对用户的认证,从而直接控制设备;2)攻击者通过中间人攻击等手段劫持物联网设备与云平台的连接,从而注入或窃取数据;3)攻击者绕过云平台对用户的认证,从而通过云平台间接地控制物联网设备.因此,在物联网场景下,信任链中的一环出现访问控制失效,恶意的控制流和数据流就会沿着信任链传递,造成难以预估的危害.

本文在 1.1 节中简单介绍了 4 种控制设备的场景,这些场景在信任链中可能存在 3 种风险传递模式.

1) 设备端风险传递

利用设备对云平台或用户的访问控制漏洞,可以近距离接触设备并对云平台进行控制或导致数据泄露.通过访问控制信任链,设备端的安全问题可能传递到云平台和用户端,造成更严重的安全问题.需要注意的是,设备对云平台也需要进行访问控制,设备需要首先确认云平台的身份,也需要确认来自云平台消息的完整性,防止诸如 DNS 污染等问题.设备端产生的风险,一方面直接作用于设备;另一方面,借助云平台的信任,设备端风险可以传递到用户侧,例如 1.1 节中介绍的远程监控设备,设备端的数据如果受到篡改,用户会通过云平台接收到假的设备状态而导致严重后果,如虚假的火灾警报.

2) 云平台风险传递

云平台作为数据的传输中转站,一旦出现安全风险,可能对大量的设备和用户造成影响.攻击者可以利用远场通信协议的安全漏洞[20]或云平台处理逻辑的安全问题,对连接在云平台上的设备进行控制或监听或对连接在云平台上的用户 App 进行欺骗.由于访问控制信任链中,设备和用户 App 对云平台的信任,这种攻击的隐蔽性强,受害者很难发现.另外,我们在 1.1 节中介绍了云平台自动化编程控制设备的新模式.从数据链的角度分析,云平台应用发起的控制指令,仍然是由云平台发起的,数据的传递基于设备端对云平台的信任链,一旦云平台应用出现安全问题,可以造成难以估量的后果.因此,云平台应用程序的复杂安全威胁也是目前研究的重点之一.

值得注意的是,即使是 1.1 节中提到的本地控制设备场景,在当今智能家居等行业的发展背景下,云平台也会在设备绑定、客户端鉴权等方面扮演非常重要的角色.即使用户 App 和设备在同一个局域网下,云平台也有可能在绑定设备的过程中扮演必不可少的角色.

3) 客户端风险传递

客户端安全风险主要是用户移动端 App 的安全问题.由于移动端 App 的安全问题很难通过信任链将恶意数据传递到其他物联网实体,因此目前对物联网移动端 App 的研究相对较少.

2 物联网访问控制现有研究

物联网与传统互联网存在着巨大差异,尤其是物联网架构不同于互联网的架构,而且物联网设备具有容量低、计算能力低等特性[21],这些特性也给物联网访问控制提出了更高的要求,导致物联网无法简单复用互联网的访问控制系统和相关基础设施.作为物联网安全性保障的重要环节之一,有很多学者在物联网访问控制领域开展了相关研究,总结了物联网访问控制应该遵循的原则,并提出了诸多类型的模型与架构设计.

2.1 物联网访问控制原则

Ouaddah 等人在文献[22]中结合物联网的特性总结了物联网访问控制应该遵循的 8 个原则:

1) 协同性.物联网环境下可能存在多个不可信的个人或者组织进行协同,访问控制系统必须允许各个主体制定自己的政策,且能与其他组织的政策兼容合作.

2) 自适应策略.由于各个主体的动作是动态、不可预测的,必须允许访问控制的策略可以针对上下文进行动态调整更新来适应不同的需求.

3) 细粒度.因为物联网系统中的各种设备会受到各种环境因素的影响而被触发,访问控制也应该同样考虑到这些环境因素,将环境信息引入到系统中进行更细粒度的决策(例如,根据当前的时间、位置、目标设备等信息决定是否允许操作).

4) 易用性.访问控制应该易于管理和修改,以方便缺少相关技术的普通用户使用.

5) 分布式自治系统.每个实体的访问控制策略的实施和管理应由其自己的规则来控制,以适应物联网环境下分布式安装的智能设备.

6) 异构性.由于物联网设备之间存在各种物理上的差异,在进行管理时应存在一个统一的虚拟接口,来方便控制管理存在不同特性的设备.

7) 轻量性.访问控制系统应保证轻量来节省各种物联网设备本就不富裕的计算能力和能源消耗.

8) 可扩展性.访问控制系统应可以随时扩展,以应对当前越来越多的物联网设备、应用和用户.

2.2 现有研究

当前物联网访问控制相关研究主要集中在访问控制架构、机制流程、模型 3 个方面.

在架构方面,由于物联网场景通常由多种类型的设备组合连接而成,访问控制不再是传统互联网中的少量几个系统之间的互相授权,而是大量设备之间的权限管理,因此互联网场景下常用的中心化访问控制架构难以适用.此外,这些设备一般互为异构且计算能力弱,难以处理加解密、智能策略生成等复杂算法,更无法将传统互联网中的访问控制系统直接进行移植,需要探索适用于物联网场景的访问控制系统,重点满足轻量性、异构性等原则.在较早的研究中,有学者就中心化的物联网访问控制进行研究[23-25],而随着物联网架构的进一步演进,现有研究出于将计算负载分散化和增加容灾能力的目的,主要探索去中心化、分布式架构的设计.区块链是如今非常流行的去中心化技术,众多研究提出了将区块链、智能合约等技术引入到系统中,利用区块链技术的分布式、可验证等特性来实现可扩展、分布式、可协作的访问控制.文献[26-28]均提出了基于区块链的物联网分布式体系架构,并在其中整合了智能合约来实现在物联网环境下对设备基于属性的域内和跨域访问控制,并达到了灵活、动态、自动化的目标.雾计算和边缘计算是通过将计算需求迁移到其他设备来提高计算性能和架构扩展性的技术,也已经有研究[29]提出将雾计算和边缘计算运用到物联网访问控制的架构设计中.

在机制流程方面,当前研究主要针对访问控制系统中的各种交互协议与数据格式,由于物联网设备的特殊性,通常无法采用有线连接,而是使用移动网络、蓝牙、ZigBee 等无线方式与服务器连接.无线连接与有线连接相比存在延迟高、带宽小、抗干扰能力弱等特点,无法直接使用互联网中复杂的交互协议与框架,当前研究主要是将轻量级的协议与框架引入物联网访问控制系统当中.在交互协议方面,研究人员围绕 MQTT,CoAP 等物联网通信协议进行访问控制相关设计[30-32].在数据格式方面,研究人员倾向于结合 JSON(javascript object notation),XACML(extensible access control markup language),SAML(security assertion markup language)等数据格式灵活、简单的优点,提出了物联网授权框架,使得资源受限的物联网设备也能进行细粒度和灵活的访问控制[33-35].这些研究能够降低物联网访问控制流程中的流量、内存、性能损耗,且同时能保证访问控制系统的正常运行.

在模型方面,当前研究主要是将互联网中已有的 RBAC,ABAC,UCON,CapBAC 等访问控制模型进行移植.进行移植的原因之一是这些传统模型

已经在互联网的悠久历史中证明了其可靠性和实用性,只需要针对物联网环境下的分布式等特性进行少量修改就可以直接使用.Gusmeroli 等人[19]和 Zhang 等人[36]分别将 CapBAC 和 UCON 等访问控制模型移植到物联网环境下,使其适应分布式系统.另一原因是直接移植模型可以使得现有的互联网系统可以方便地与物联网设备进行对接交互,让原有的互联网用户可以无缝地接入物联网中来实现 WoT(Web of things),从而减少企业开发程序上的人力成本.Jia 等人[37]和 Barka 等人[38]将 RBAC 模型进行了移植并集成到系统中,而 Bai 等人[39]则将 UCON 模型进行了移植,这使得互联网系统与物联网设备之间的访问控制成为现实.

从现有相关研究来看,当前物联网访问控制研究更注重功能性,主要针对物联网环境下由于架构不同和资源受限带来的计算能力低、带宽小等问题,需对互联网下访问控制所用的方法进行修改后移植到物联网场景中.具体来说,在访问控制架构上,从中心化的架构逐渐转向分布式架构,借助区块链等先进的分布式技术进行设计;在机制流程上,则围绕适用于物联网的通信协议和轻量级数据格式进行研究;在模型上,主要研究将成熟的互联网访问控制模型向物联网移植并适配.

但现有研究并未重视物联网环境下访问控制系统的安全性.一方面,当前的物联网由于设备类型多样、业务需求多样,其体系结构非常复杂且处在持续的演进中.另一方面,物联网中的设备通常与用户物理相邻,它可以是身边的摄像头、烟雾报警器,也可以是工控系统中的水闸电闸,这些设备能够以多种形式影响到用户本身,所以,直接使用从互联网移植现有访问控制技术的系统架构、机制流程、权限模型而不对安全性进行额外的验证和适配是不充分的,可能引发安全上的隐患与风险,导致敏感数据泄露,危害到工业生产安全、人身安全甚至是国家安全.因此,本文聚焦物联网访问控制的安全性,调研并综述相关研究进展.

2.3 物联网访问控制安全性

物联网访问控制是保护用户数据、保障设备合法操作指令的安全技术,而要使访问控制真正生效,则需要保障访问控制自身的安全性,包括主体、客体、机制策略、身份认证、权限授予等方面的安全.由于物联网体系架构的复杂性和业务场景的多样性,物联网难以建立传统的安全边界,其访问控制系统难以实现端到端的设计.为实现安全的访问控制,需要围绕物联网数据链、信任链和业务场景,研究从哪些层面入手保障访问控制安全性,即物联网访问控制保护面.

1) 设备安全

设备上搭载的传感器所采集的指纹、声纹是物联网进行用户身份认证的重要数据来源,关系到用户的身份信息是否独立、安全,若该类数据被伪造或窃取,将产生身份冒用风险,导致访问控制失效.

2) 流量安全

物联网在感知层、网络层、应用层之间的数据传输依赖网络流量,对于访问控制场景,则需要在 3 个层次之间进行身份认证信息、授权指令等的传输.因此,流量的安全性至关重要,需要在该层面防范数据窃取、中间人攻击等风险,增强网络协议的安全性对于流量安全的保障.

3) 应用安全

根据物联网的数据链与访问控制信任链,应用是用户与设备、设备与云平台的接口,向上传递身份认证信息,向下传达授权决策与操作指令,因此需要在应用 App 层面保障安全.

4) 云安全

云平台承担着复杂的数据计算、处理与存储任务,在更多的访问控制场景中负责授权策略管理,并且,物联网中既存在云平台与设备、应用的交互,也存在云平台与云平台之间的交互,因此,云安全是保障安全的物联网访问控制生效的重要着力点.

5) 接口安全

物联网多个层次之间以及各个层次内部的数据流转都依赖接口,不安全的接口存在信息泄露、篡改的风险.

接下来,本文基于上述保护面和物联网,围绕物联网体系架构的 3 个层次进行访问控制攻击面的分析,并归纳相应的安全解决方案研究.如图 2 所示,本文结合 IoT 云平台、用户、设备构成的信任链端点,主要以信任链上的 3 个物联网层次(应用层、网络层、感知层)为基础进行阐述,包括对每个层次的主要内容和应用场景的攻击面总结和解决方案总结.其中,应用层主要有云应用、云对接、设备绑定 3 个方面;网络层主要有近场通信和远程通信 2 方面;感知层主要有传感器和设备软硬件 2 方面.最终再根据不同的互联网安全维度进行保护面总结,保护面包含设备安全、流量安全、云安全、应用安全和接口安全 5 个维度.

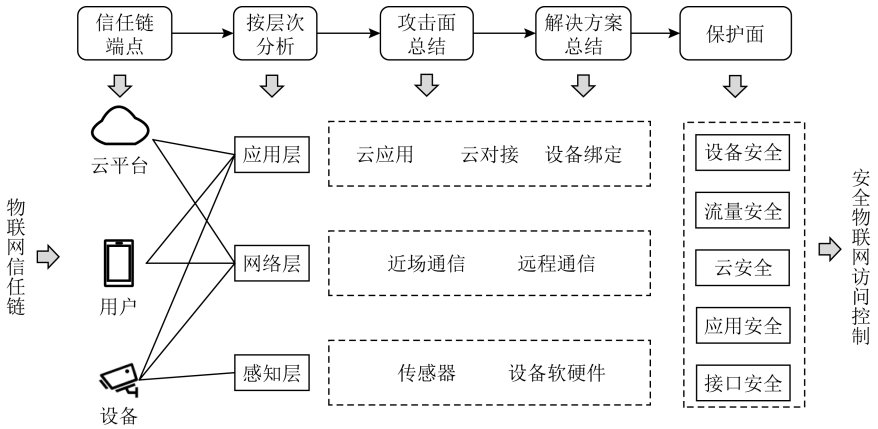

Fig. 2 Research on security of IoT access control

图 2 物联网访问控制安全性研究

3 物联网访问控制攻击面

2.3 节结合物联网数据链与信任链传递的特点阐述了物联网访问控制安全性的内涵与保护面,而与保护面相对应的就是攻击面,为保障安全性,需要对可能存在的风险进行研究与把握.物联网访问控制主要是多个实体的访问控制模型相互连接、相互交互、互为主客体.在本节中,我们以 3 个物联网层次作为切入点,介绍针对物联网访问控制的主要攻击面.

3.1 感知层攻击面

感知层是物联网架构中最基础的层次,负责向上层提供数据支持,是一个具有物理设备的实体,感知层分为传感器和设备软硬件 2 个层次.传感器负责收集外界信息,设备软硬件负责驱动传感器工作,并与上层建立连接.感知层的访问控制模型主要有 2 方面:一方面设备传感器作为主体,采集外界信息;另一方面设备作为客体,与多种主体(如 App 和云)进行交互.在现有的针对感知层的研究中,主要考虑传感器数据的可靠性以及感知层软硬件的设计与实现.

3.1.1 感知层传感器安全问题

对于感知层传感器而言,有研究[40-41]表明现有的安全方案和访问控制系统无法为传感器提供足够的安全防护,产生了漏洞:伪造传感器所收集的数据,使得传感器无法获取相应的外部信息.在现有的研究中存在很多伪造传感器数据的攻击案例,这种攻击可能导致应用层基于错误的传感器数据产生错误的判断,由于应用层的访问控制模型无法涉及到感知层的细节,应用层的访问控制模型会被完全欺骗.

Tukur 等人[42]进行了一项研究,模拟了内部攻击者对物联网系统中的传感器实施的数据伪造,证明了篡改感知层的物理环境对整个物联网系统的数据完整性造成直接的负面影响.这种伪造数据的攻击可以在 GPS 传感器、光线传感器、麦克风、摄像头上实施.与传统的访问控制不同的是,传感器获取的客体数据大多来自于真实的物理世界,导致传感器的访问控制几乎无法使用现有的技术,只能在一定程度上针对每一种数据来源的真实性进行判断.而一旦传感器的判断错误,上层的其他访问控制模型也会无条件相信传感器的错误数据,导致信任链的底层出现疏漏.

比较典型的案例是针对 GPS 信号接收器的信号伪造,Tippenhauer 等人[43]分析了欺骗 GPS 传感器的可能性,他们使用 GPS 信号模拟器尝试干扰了 Atmel 公司的 ATR0600 GPS 芯片,其实验结果证实了 GPS 信号接收器可以很容易地被欺骗到任意一个位置.Park 等人[44]提出了一种针对医用输液泵中红外液滴传感器的数据伪造攻击,该文作者发现红外液滴传感器没有持续地对饱和输入进行检测,因此可以通过使用额外的红外线发射器来干扰传感器,可以实现对输液速度的控制.

对传感器的欺骗同样也会发生在指纹、声纹等直接用于身份认证的传感器.指纹识别技术现在已经十分成熟,但也存在着简单有效的指纹欺骗方法,比如使用塑料制作指纹模型,在文献[45]中对指纹传感器的欺骗进行了全面的综述.相比于指纹识别技术,声纹识别技术起步较晚,声纹识别依赖音频中的音色、韵律和语言内容,攻击者可以通过模仿、重放、语音合成、语音转换等手段欺骗声纹识别,在文

献[46-47]中综述了这 4 种欺骗手法以及相应的对策.同时也存在一些针对语音控制系统的攻击,Zhang 等人[48]设计了一种人类无法听到但智能语音助手可以正常识别的攻击方法 DolphinAttack,并在 Siri,Google Now 等平台上进行了概念验证,成功完成了在 iPhone 上发起 FaceTime 通话、使用 Google Now 将手机切换到飞行模式等命令攻击.传感器还可能受到拒绝服务的攻击,破坏其数据的可用性.有一项研究证实了可以通过噪音干扰 MEMS 陀螺仪工作,并在实验中成功使得配备有 MEMS 陀螺仪的无人机坠毁[49].

3.1.2 感知层设备安全问题

感知层设备作为访问控制的客体,被多种主体访问.感知层设备主要分为软件和硬件 2 个层面,软件涉及操作系统和上层的应用程序[13].感知层设备的访问控制的失效可能发生在非法的控制端或恶意用户获取了设备的信息或对设备进行了修改.

在感知层设备的软件层面,访问控制攻击面主要包括:弱口令、访问控制失效的通信接口、缺乏认证的更新机制.一些感知层设备可能提供了远程访问的功能,比如通过 FTP 查看文件、使用 Telnet 或 SSH 与设备进行交互.Kumar 等人[50]进行了一项调查,使用弱口令字典扫描物联网设备的 FTP 和 Telnet 服务,发现有 17.4%的 FTP 服务和 2.1%的 Telnet 服务使用了弱口令.很多物联网设备使用 Web 服务或蓝牙等无线协议与上层应用进行通信,这些服务提供了一些数据接口供上层服务调用,如果这些数据接口未能实现鉴权功能或存在越权访问等逻辑漏洞,可能导致传感器数据泄露或执行非法指令等后果.在 Rapid7 公司的一项调查中列举了一些关于婴儿摄像头的漏洞,其中 CVE-2015-2882 是相机设备中运行的 Web 服务存在硬编码的账号“admin”和密码“M100-4674448”,攻击者可以在相机设备所处的本地局域网中访问其 Web 操作界面[51].一些感知层设备在提供固件升级时,缺少对固件的完整性认证,从而导致攻击者可以将恶意的固件写入到设备中.Ronen 等人[52]通过相关功率分析(correlation power analysis, CPA)[53]的侧信道方法推测出 Philips 灯泡用于加密和验证固件更新的密钥,他们利用推测出的更新密钥刷新灯泡固件从而实现了完全控制,并且实现了蠕虫攻击,即利用一个灯泡来攻击另一个灯泡.

在感知层设备硬件层面,针对设备客体访问控制的攻击面包括了针对硬件的侧信道攻击和调试接口暴露.利用侧信道和密码学分析可以泄露 CPU 中的状态信息[54],比如,Gnad 等人[55]提出,利用模数转换器(analog-to-digital converter, ADC)可以推断系统中 CPU 的活动,并成功进行了 AES 密钥恢复攻击.而 Ronen 等人[52]实施了一种未知明文选择差分 CPA 攻击来推测 Philips 灯泡固件更新时的 AES-CCM(advanced encryption standard-counter with cipher lock chaining message authentication code)算法的验证密钥.对于某些感知层设备可能保留有调试用的硬件接口,具有物理接触这些设备的攻击者可以绕过软件层面的认证服务,直接获取系统内的信息,甚至获取操作系统交互权限.一些物联网设备在出厂后仍然保留了调试接口,这使得某些能够物理接触设备的人员可以通过调试接口获取硬件上的信息(比如加密密钥),导出固件代码,甚至可以向设备中写入恶意代码[56].

当设备的软硬件的访问控制模型被打破时,其危害可能被信任链传递到其他层次.例如,云平台的访问控制模型会无条件接受设备传递的数据,因为云平台已经没有任何办法验证设备是否已经被攻击者控制,进而也会被应用层的访问控制模型认可,影响应用层逻辑.但针对感知层设备的攻击需要攻击者接触设备,利用条件较苛刻.

3.1.3 小 结

感知层攻击面总结如表 1 所示.感知层作为主要的信息收集层,其最常见的访问控制安全风险在

Table 1 Perception Layer Access Control Attack Surface

表 1 感知层访问控制攻击面

缺陷	威胁存在位置	说明	相关文献
数据伪造	传感器	伪造身份信息导致访问控制验证错误	[42-48]
接口失效	设备软件	接口未能实现鉴权等访问控制功能,或存在越权访问等逻辑漏洞	[50-51]
缺乏认证更新机制	设备软件	缺乏完整性验证,导致设备植入恶意固件,从而打破原有的访问控制	[52-53]
侧信道	设备硬件	利用侧信道绕过访问控制,窃取数据	[52,55]
调试接口暴露	设备硬件	通过调试接口绕过认证服务	[56]

于:作为访问控制主体,身份认证信息存在采集和上传中的伪造问题;而同时感知层在执行操作的客体角色中,存在着由设备容量小、计算能力低等因素所导致的认证机制不完善的攻击面.设备自身的漏洞也是明显的攻击面.

3.2 网络层攻击面

网络层是位于物联网架构中间的层次,主要支撑感知层和应用层之间,以及位于感知层的设备之间和位于应用层的云平台与应用 App 之间的通信,是由不同的通信协议组成的一个层次,网络层的访问控制威胁也主要分布在各种不同的通信协议中.按照设备的近场性,可以将网络层分为近场通信层和远场通信层.近场通信层主要涉及设备配对、设备间近距离通信、设备和 App 之间近距离通信等;远场通信主要涉及设备和云服务器之间、云服务器和 App 之间的通信等.

网络层向上对接云平台和应用层的访问控制模型,向下对接感知层设备的访问控制模型.

3.2.1 网络层近场通信安全威胁

IoT 近场通信协议主要有 BLE(bluetooth low energy),ZigBee,Z-Wave,6LoWPAN 等.近场通信协议的设计问题和漏洞能够破坏客体设备的访问控制模型,也包括用户设备(手机),主要漏洞是设备未授权访问、用户隐私泄露、设备劫持等.近场通信协议的安全问题能够绕过设备的访问控制模型,进而通过信任链传递到云或其他主体,并且这些安全问题的避免难度较大,目前主流研究集中在对协议的漏洞进行研究,并改进协议,进行安全加固.

BLE 是由传统蓝牙发展而来的,为物联网的设备间近场通信提供了一种低功耗、低成本的通信协议,由 BLE 引入的安全威胁是当前研究的热点之一.Fawaz 等人[57]对 BLE 隐私保护规范中的地址随机化在现实世界的部署中是否真正能够保护用户隐私的问题进行了探究,收集并分析了 214 种不同类型 BLE 设备的广播,发现由于开发者和制造商没有正确执行 BLE 隐私保护规范、地址弱随机化、地址长时间不改变等原因导致了地址随机化失效,泄露了大量的信息.Celosia 等人[58]利用 BLE 中的 GATT (generic attribute)配置文件创建了一个指纹,成功规避了 BLE 隐私保护规范的反跟踪特性(即 MAC 地址随机化),利用该指纹可以跟踪用户、推断用户敏感信息等.Zuo 等人[59]从配套的移动应用程序中提取具有静态 UUID(universally unique identifier)的 BLE 设备指纹,对 BLE 设备进行指纹识别,侵犯用户隐私;该文作者还发现许多 BLE 设备采用 Just Works 配对,允许攻击者在不需要认证的情况下主动连接这些设备,造成未授权访问攻击,使用 UUID 指纹定位这些设备,配合 Just Works 配对或弱认证,攻击者可以完全控制这些设备.Sivakumaran 等人[60]成功实施了针对 BLE 的应用共存攻击,即当手机中有一个应用程序已经与 BLE 设备建立连接时,手机中另一个恶意的应用程序能够未授权访问受保护的 BLE 设备中的敏感数据.Wen 等人[61]设计实现了 FirmXRay 自动静态二进制分析工具,用于 BLE 链路层漏洞检测,还收集了 793 个独特的固件来评估 FirmXRay,实验结果表明,98.1%的设备配置了随机静态 MAC 地址,71.5%的设备配置了 Just Works 配对,98.5%的设备配置了不安全密钥交换.这些漏洞会导致用户的敏感信息泄露、设备的未授权访问等安全问题.Wu 等人[62]研究了 BLE 链路层的安全性,聚焦 BLE 设备重新连接的场景,发现了其认证机制的 2 个设计缺陷(可选认证和认证绕过),利用设计缺陷该文作者提出了 BLESA(BLE spoofing attacks),即 BLE 欺骗攻击,攻击者模拟 BLE 服务器设备,向之前配对的 BLE 客户端设备发送欺骗数据,成功欺骗了 BLE 客户端设备.Ludant 等人[63]发现了蓝牙芯片设计中的链接漏洞,将 BLE 广播链接到了经典蓝牙帧(BTC),该文作者利用该漏洞将 BLE 广播与全球唯一标识符(globally unique identifier, GUID)链接,利用 BDADDR 标识符可以跟踪 BLE 用户,从 BLE 广播中窃取用户敏感信息.

ZigBee 也是最常使用的物联网近场通信协议之一,由 ZigBee 协议引入的安全威胁也受到了学术界广泛的关注.Morgner 等人[64]利用 ZigBee3.0 新增加的 touchlink 调试功能对 ZigBee 发起攻击,并且在 touchlink 预配置的链接密钥泄露的场景下成功获取了 ZigBee 网络中所有节点控制权.Akestoridis 等人[65]研究了当集中式 ZigBee 网络中禁用 MAC 层安全的设计选择的后果发现,攻击者可以从 ZigBee 流量的被动检查中获得有价值的信息,包括识别某些加密的 NWK 命令,然后使用这些命令开发选择性干扰和欺骗攻击,以迫使最终用户重置目标设备,并最终暴露网络密钥,造成敏感信息泄露.

近场通信协议的安全问题主要打破设备的访问控制模型,进而通过信任链影响到云端访问控制模型、应用层访问控制模型,由于通信协议的漏洞相对较难避免,因此具有很强的隐蔽性.但利用近场通信

协议需要攻击者在较近的物理距离内发起攻击,影响面相对较小.

3.2.2 网络层远场通信安全威胁

网络层远场通信主要聚焦于各种物联网流行的通信协议上,目前使用较为广泛的协议包括 MQTT(Message Queuing Telemetry Transport),CoAP(Constrained Application Protocol),AMQP(Advanced Message Queuing Protocol),HTTP(Hyper Text Transfer Protocol),XMPP(Extensible Messaging and Presence Protocol),DDS(Data Distribution Service for Real-time Systems).远场通信协议的安全疏忽能够打破云平台或云端数据的访问控制体系,远场通信协议对于访问控制模型的挑战,成为了目前学术界的关注重点之一.

网络层远场通信协议大多在设计之初就缺乏对适用物联网的安全性设计,对于保密性,通常都是由 TLS 协议(Transport Layer Security)或 DTLS 协议(Datagram Transport Layer Security)保证的.Al Fardan 等人[66]基于对 TLS 和 DTLS 协议中解密处理的精确时间分析,利用明文恢复攻击窃取了敏感信息.对于协议本身的安全问题与协议适用物联网时协议对接云平台和云端数据的访问控制模型时存在的安全问题,目前的研究较少.Jia 等人[20]通过对 MQTT 通信机制的安全分析发现了 MQTT 协议在物联网场景下产生的多个漏洞,例如不安全的 MQTT 消息管理、不安全的 MQTT 会话管理、未授权的 MQTT 身份等.

由于云平台和协议特性之间的安全鸿沟,云平台很难利用现有的访问控制技术去限制物联网协议,攻击者可以利用协议的特性,打破云平台的访问控制模型,进而欺骗云平台去修改云端设备元数据,并成功控制受害者设备,窃取用户敏感信息.Wang 等人[67]提出了 MPInspector 框架,实现了自动化分析远场通信消息传递协议的安全性,在 9 个广泛使用的物联网平台上对 MQTT,CoAP,AMQP 协议进行分析,并且使用 MPInspector 框架评估这些协议的安全性,发现了针对物联网远场通信协议的 11 种类型的攻击方式,其中包括客户端身份劫持攻击、恶意主题订阅、未经授权的消息响应等.这些攻击方式可以在协议的层面突破云平台甚至云端数据的访问控制模型,并通过信任链将危害传递到大量物联网设备.

远场通信协议主要通过打破云平台的访问控制模型或应用层的访问控制模型来修改云端数据,并通过信任链将危害传递到设备和用户 App,远场通信协议因为可以修改云端数据,其安全问题具有影响面大、破坏性大的特点,在极端情况下,一个攻击者甚至可以利用远场通信协议和访问控制模型之间的安全鸿沟,对整个云上连接的设备进行低成本的大规模攻击.

3.2.3 小 结

网络层攻击面总结如表 2 所示.网络层在访问控制中主要负责身份认证信息和授权策略的传输,场景包括近场通信和远场通信,其安全性由各类通信协议、加密协议来保障,而攻击面也存在于尚不完善的通信协议的认证机制、加解密、粒度等性能方面.

Table 2 Network Layer Access Control Attack Surface

表 2 网络层访问控制攻击面

缺陷	威胁存在位置	说明	相关文献
地址随机化失效	近场通信协议	由地址随机化失效导致攻击者可以跟踪用户,推断用户敏感信息等	[57-58]
配对机制缺陷	近场通信协议	由配对机制缺陷而造成的设备未授权访问	[59,61]
应用共存攻击	近场通信协议	缺少对 BLE 协议主体的细粒度访问控制模型,导致客户端 App 可非法占用物联网 App 的通信信道.	[60]
不安全的密钥交换	近场通信协议	近场通信时不安全的密钥交换,可能造成未授权访问	[61]
认证机制的设计缺陷	近场通信协议	攻击者可以利用客户端设备认证机制的设计缺陷,用假数据对其进行欺骗	[62]
流量嗅探	近场通信协议	通过从协议流量中获取有价值的信息,利用这些信息获取网络密钥和敏感信息	[64-65]
针对 TLS 和 DTLS 的攻击	远场通信协议	TLS 和 DTLS 协议缺陷/配置错误导致的敏感信息被窃取,具有潜在的影响身份认证的风险	[66-67]
不安全的身份管理	远场通信协议	由通信协议的身份验证缺陷导致恶意攻击者可以欺骗云平台访问控制模型,进行重放攻击或客户端劫持等	[20,67]
不安全的消息管理	远场通信协议	攻击者可以利用云平台缺失或不完善的访问控制的协议特性,非法注入消息,进而控制或监控设备	[20,67]

3.3 应用层攻击面

在当前的IoT架构中,应用层一般是物联网顶层设计的逻辑,如在智能家居场景下的用户、家庭等概念均运行在应用层之上.物联网应用层是一个抽象层,应用层之上一般只是数据和访问控制逻辑.正因如此,一旦应用层访问控制出现问题,运行在其他层次的安全手段(如网络层的安全防护)难以发现.另外,由于云平台需要存储几乎所有的应用层数据,一旦云平台的应用层访问控制逻辑出现问题,借助1.3节中提到的信任链,可能导致大量IoT设备沦陷.

应用层的主要载体是物联网管理者或用户的IoT App,以及各种IoT云平台.目前相当多的IoT设备都拥有连接WiFi或者通过BLE,ZigBee连接智能网关从而访问互联网的能力.如1.1节中的4种常见场景,物联网的合法用户通过IoT App修改应用层数据,云平台或者软件自身自动地将应用层数据翻译为设备可读的指令.

而现有的IoT云平台根据其功能可以分为2类:

第1类是IoT设备厂商自身的云平台.例如小米米家、涂鸦智能等,一般可以与本厂商的IoT设备进行连接,通过网页/手机App控制IoT设备,并提供接口可以与其他云平台或者Trigger Action平台进行对接,部分平台例如SmartThings,甚至允许用户上传自己的程序在云平台上,允许用户自己编程控制IoT设备.云应用大大拓展了物联网的使用范围,但也使得应用层访问控制变得极为复杂,大大增加了安全的不确定性.

第2类是自动化流程平台.例如IFTTT,Zapier等,除了可以与第1类的厂商云平台进行对接,还可以与推特、Dropbox等非IoT厂商的云平台对接.以此提供除了IoT设备之外的触发和应用能力,例如通过发送短信操控IoT设备,或者由IoT设备触发短信的发送.而少部分IoT设备,例如门锁、牙刷、医疗设备、摄像头等,可能厂商并没有建设云平台,或者这个设备本身并不具备连接互联网的能力,实际上是直接通过局域网或者BLE连接用户手机App,并以此被用户所控制.

对于直接受到IoT平台操控的设备,攻击威胁主要来自云平台的访问控制失效;而受App近场通信直接操控的IoT设备,攻击威胁主要来自手机App本身和设备端不完善的访问控制的联合作用.

3.3.1 云平台中的云应用产生的漏洞

当前的云平台一般都会允许用户创建一些简单的规则或者应用,以方便用户满足自己的一些特殊需求.其中一些平台,例如IFTTT与SmartThings,还允许用户发布自己的云应用并共享给其他人使用.而大量创建的应用不可能做到每个都被人工审计过,导致其中会存在难以对云平台应用程序访问控制的基本问题,从平台的接口盗取用户隐私数据,甚至控制用户的IoT设备.

Fernandes等人[68]对SmartThings平台进行了安全评估,发现其事件子系统存在安全缺陷,且由于其访问控制设计的精细度不足,即使应用只申请了设备的有限访问,但实际上也获得了设备的完全控制权.将这些缺陷结合起来,使得攻击者可以通过恶意的SmartApp来实现窃取锁密码、引发假火警等操作.而Surbatovich[69]与Cobb等人[70]则对IFTTT进行了分析,发现约有一半左右的云应用可能不安全,这些应用可能会破坏用户信息的机密性和完整性,例如:当用户家地下室门打开后发送消息的云应用存在泄露用户活动行为的隐患.

除了恶意应用,还有不少应用本身并不是恶意的.单一应用不会产生安全风险,但是多个应用之间的物理或者非物理上的意外组合或交互,导致在应用层构建了一条逻辑上的、云平台未曾预料到的数据链和信任链,引发访问控制漏洞.例如,根据Balliu等人[71]的研究,如果一个应用的功能为无人在家时打开恒温器,而另一个应用的功能为室温过高时打开窗户,当一个用户同时使用这2种应用时,则可能出现屋子主人出门办事,恒温器启动后却自动触发了打开窗户的云应用,为入室盗窃创造了条件.

3.3.2 云平台与云平台对接时产生的漏洞

目前,云平台的互相连接非常常见,尤其是在消费级物联网云平台,这便于消费者将多个厂商的物联网设备或者非物联网服务进行联动和管理.比如,一个智能安防和智能家居的开发者可以通过IFTTT将某个品牌的智能门锁与另一个品牌的智能灯进行联动,在门打开时亮起灯光.IFTTT作为顶层云平台,需要与2个其他厂商的云平台进行对接,以方便接受门的开启信息和发出开灯的命令.云平台之间的交互显著加长了物联网数据链,使访问控制安全的攻击面延伸,云平台之间对接的协议也没有标准化方案.

目前厂商的主要做法是使用OAuth(open authorization)协议来进行平台之间的授权和鉴权[72],但OAuth本身为一个集中式的权限管理协议,这种集中式的服务会使得攻击者在攻陷一个系统后就可以

利用系统中保存的令牌同时获得当前系统中所有用户的物联网设备权限.另外,由于 OAuth 协议中缺少对被授权主体的验证,在云平台与云平台对接授权后,设备主人通过云平台将设备共享给其他用户(例如:授予短期住宿的客人开门权限),如果云平台的实现不当,不慎将 OAuth 令牌泄露给用户,会导致用户意外获得这个门锁的完全控制权,即使主人在平台上撤回权限也无法真正回收权限.

此外,由于目前各个平台的对接标准不统一,各个平台都存在特有的格式和要求,导致对接时的信息可能会被另一方错误使用,导致访问控制漏洞.例如:Yuan 等人[73]发现 Google Home 与 SmartThings 对接时,SmartThings 会向 Google Home 传递设备 Device ID,对于 SmartThings 平台来说,这是一个需要保密的信息,但是 Google Home 却认为其是一个可以公开的普通字段,因此 Google Home 在授权给其他用户时会将 Device ID 传递给其他用户,导致恶意用户可以伪造设备的触发事件.

3.3.3 IoT 设备绑定存在漏洞

设备绑定漏洞主要存在于智能家居领域.当云平台设备进行绑定时,需要用户手机 App、云平台、IoT 设备三方共同协作完成,最后才能将 IoT 设备绑定到用户手机 App 的账号中.而如果在云平台中进行设备绑定的状态模型出现问题,则可能导致设备被敌手重绑定、解绑定等.Zhou[74]与 Chen 等人[75]展示了多种状态模型漏洞的利用方法,他们发现目前云平台绑定 IoT 设备时用到的均为类似设备 ID、设备网卡地址、设备型号等公开或者容易被嗅探出来的信息,使得攻击者在获得这些信息后可以伪造出一个"幻影"设备,将真正的设备绑定到攻击者的帐号下,或者将"幻影"设备绑定在原有帐号下伪造各种数据,这种攻击方式本质上利用的是云平台对设备接入的访问控制逻辑错误,利用物联网数据链,使有害信息传递到用户 App.

3.3.4 App 与设备端应用层漏洞

与手机 App 有关的访问控制漏洞,主要发生在本文 1.1 节中提到的本地控制设备,或控制一些不支持云平台的 IoT 设备上.在这种情况下,IoT 设备受到手机 App 的直接操作,由于 App 与 IoT 之间的交互通常使用局域网、蓝牙等本地通信方式,使得攻击者如果在本地或者已经取得手机部分权限的情况下,可以利用物联网设备访问控制模型的安全问题进行攻击.例如 Sivakumaran 等人[60]发现,在安卓系统中手机 App 与 IoT 设备配对完成后,如果设备上装有攻击者的 App 且有蓝牙权限,可以与此 IoT 设备的蓝牙连接,如果设备没有实现额外的通信加密,将会导致恶意 App 也可以控制 IoT 设备.

设备端应用层的访问控制漏洞比较复杂,主要发生于设备端允许多种控制主体的情况下.值得注意的是,设备端应用层漏洞与设备端感知层漏洞具有显著区别,感知层漏洞主要是设备软硬件本身的安全漏洞,而设备端应用层漏洞则主要利用设备状态机模型和控制逻辑的问题.例如,Jia 等人[76]发现,一台设备可能被多个控制主体同时控制,如 Apple HomeKit 和设备厂商的云服务,这 2 种控制方式的状态机完全独立,当设备主人没有占用 Apple HomeKit 的控制通道,一个潜在的攻击者可以悄无声息地占用这条控制通道.借助于这种多通道控制,一个设备可以在应用层对应多个主人.

3.3.5 小 结

应用层攻击面总结如表 3 所示.应用层在物联网架构中具有最高的计算和存储能力,因而在访问

Table 3 Application Layer Access Control Attack Surface

表 3 应用层访问控制攻击面

缺陷	威胁存在位置	说明	相关文献
应用访问控制系统绕过	云应用	云平台缺少云应用访问控制系统或者其存在缺陷,使得云应用可以非法窃取用户隐私或者控制设备	[68-71]
中心化的权限管理系统	云平台	中心化的权限管理系统使得在一个云平台被攻陷后,其上泄露的所有凭据都可以直接被攻击者所使用	[72]
未统一的对接协议	云平台	云平台与其他云平台进行对接时缺少一个统一的对接协议,使得敏感信息缺少访问控制	[73]
未验证的设备绑定状态模型	云平台	在 IoT 设备绑定至用户的过程中所使用的状态模型如果存在缺陷,攻击者可以利用漏洞控制其他用户的设备	[74-75]
存在缺陷的系统 API	手机应用	应用使用存在访问控制缺陷的系统 API,导致其他恶意手机 App 可以控制手机上绑定的 IoT 设备	[60]
多重控制通道	物联网设备	利用物联网设备集成的多重控制通道,使设备在应用层对应多个访问控制主体,攻击者占用一个通道便可以合法控制设备	[76]

控制中也主要承担策略的维护和权限的下发.由于物联网信任链的风险传递,存在逻辑缺陷或机制不对等的云、应用、设备或接口成为了访问控制安全性的短板,引发访问控制机制与协议缺陷、系统漏洞等攻击面.

4 物联网访问控制安全性解决方案

如2.2节所述,已经有相关工作提出了物联网访问控制框架的特性与原则,但并未针对安全性问题进行细致的研究探索.为了实现安全的物联网访问控制,需要结合物联网的特性,满足4点要求:

1) 机制完善

物联网结构与数据流转复杂,因此,需要更加细致、完善的访问控制机制与流程.

2) 应对攻击面

安全的访问控制除了在机制上要完善,还应该在具体的技术建设层面解决脆弱点与攻击面带来的安全风险.

3) 多级认证与授权

由于物联网的数据流转在多个层次之间进行流转,存在信任链条的传递,在每一个环节都可能存在不同类型的风险,因此,安全的物联网访问控制应该向着多级认证、逐级授权的细粒度方向演进.

4) 结合具体场景

物联网与人类社会的生产生活息息相关,其业务场景包括了智能家居、智慧医疗、工业控制、车联网等,不同场景的数据敏感程度与被控风险程度有所不同,在具体建立访问控制时需要结合具体场景进行设计规划.

本节围绕访问控制在物联网架构各个层次中的攻击面以及各个层次在访问控制中的角色,对现有的访问控制安全性解决方案的相关研究进行归纳总结.

4.1 感知层访问控制安全性解决方案

感知层主要包含设备及设备上搭载的传感器.在访问控制场景中,一方面作为主体,负责收集数据作为身份认证信息;另一方面负责执行云端通过认证与授权后下发的指令.

4.1.1 传感器层面

传感器在物联网系统中广泛存在,其形式多样、种类丰富,在物联网架构中扮演着收集信息的角色,其主要的访问控制安全威胁在于收集到的有关身份认证的信息(如指纹、声纹等)可能被篡改、被伪造,因此,很多研究工作从信息防伪造的角度着手,强化传感器层面的访问控制安全.

在传感器层面,大多数的访问控制解决方案需要针对特定传感器的特定攻击方法来实施,比如较为常见的指纹和声纹伪造2种场景.针对指纹传感器欺骗检测的方法一般分为2类[45]:基于硬件的检测和基于软件的检测.

对于硬件检测,可以通过增加传感器设备来收集生命特征,比如温度、血压、导电率等,这种硬件检测方法准确度较高但增加了设备的成本,且无法应用于旧设备中.

软件检测仅通过增强对图像的识别来区分真实指纹和伪造的指纹[77].目前基于机器学习的软件图像检测方法较为流行,比如Xia等人[78]提出了一种新的韦伯局部二值描述符(Weber local binary descriptor,WLBD)用于指纹活性检测,他们在原有的韦伯局部描述符的基础上进行了改进,并在公共数据库中取得了更好的准确性.而对于声纹伪造的识别,可以从不同的角度进行分析,比如口腔运动、咽部震动、磁场、声场分析.Yan等人[79]通过声音在空气中传播产生的声能物理场来区分人类和扬声器,实现了一种与文本无关的人声验证方法CaField,在多种语音输入的测试中实现了99.16%的检测准确率.

4.1.2 设备层面

设备感知层的访问控制模型较简单,攻击面与传统的嵌入式设备攻击面大致相同,主要的薄弱点为设备软硬件漏洞,因此设备层面的安全防御主要是漏洞的发现和修复以及可信计算加固,防止潜在的漏洞利用等.

文献[80]提出了一种针对物联网设备的自动模糊测试框架IoTFuzzer,它可以在不获取固件的情况下发现物联网设备中的内存安全漏洞,通过分析可以操作物联网设备的移动App的代码来生成测试样例,再使用API钩子对目标物联网设备进行测试.在文献[80]的作者给出的测试结果中,IoTFuzzer成功识别到17台物联网设备中的15个内存安全漏洞.而Zheng等人[81]实现的FIRM-AFL框架可以用于物联网设备固件的灰盒测试.与文献[80]不同的是,FIRM-AFL需要对物联网设备固件进行仿真运行,文献[81]提出了一种增强过程仿真的技术,结合了全系统仿真和用户态仿真,提升了仿真的运行效率.文献[81]的评估表明,FIRM-AFL可以发现现实物联网设备固件中的漏洞,并且平均吞吐量可以达到全系统仿真的8.2倍.除了使用自动模糊测试

的手段及时发现漏洞外,还可以通过可信执行环境、控制流保护、数据执行保护等手段防御漏洞攻击.在物联网设备中提供可信执行环境可以隔离可信应用和普通应用,在一定程度上缓解了远程漏洞攻击影响,保证了可信应用的安全,同时也可以避免具有物理权限的攻击者提取敏感信息.

文献[82]中对比了2种目前可用于物联网设备的可信执行环境,即ARM TrustZone和安全控制器(security controller, SC),发现ARM TrustZone更加灵活高效,但安全控制器能更有效地抵抗物理入侵.而物联网设备的控制流保护也可以在一定程度增加漏洞攻击的利用难度,避免攻击者利用漏洞控制物联网设备,从而直接打破访问控制体系.文献[83]中提出了一个名为Silhouette的编译器执行流保护技术,可以用于常见的嵌入式设备中,该技术可以有效地保护返回地址的完整性,缓解了控制流执行攻击.感知层设备作为物联网系统的数据来源,任何的漏洞攻击都会导致整个系统的访问控制失效,因此设备中的软件和硬件都应实施一定程度上的漏洞防御机制才能保护整个物联网系统的安全.

4.2 网络层访问控制安全性解决方案

网络层在物联网中主要负责数据的传输,为了更安全地访问控制,需要保障数据传输过程中的安全,通过完善加密算法、传输协议等避免访问控制场景中的身份认证信息、授权信息被窃取或篡改.

4.2.1 网络层近场通信

面对网络层近场通信的安全威胁通常有2种解决方案:

1) 设计全新的安全通信协议,使其不仅适用物联网的低功耗、低成本的需求特性,并且尽可能保障通信的安全,安全的设计贴合物联网的复杂架构.Luo等人[84]提出了一种适用于异构物联网环境的轻量级近场通信协议,基于对称密钥和混沌系统实现了设备间的安全通信.

2) 在原有协议的基础上进行扩展或者改进,利用扩展部分保障原有通信协议的安全或者改进原有协议以便消除威胁.Fawaz等人[57]针对由于BLE设备广播的访问控制失效引起的安全威胁提出了BLE-Guardian系统,用于保护BLE设备、物联网用户、环境的隐私.Alshahrani等人[85]基于ZigBee提出了一种新的协议,实现了物联网设备间的相互认证,并且使得认证具备匿名性,同时多角度评估验证了协议的安全性.Wang等人[86]提出了一种新的无证书ZigBee加入协议,解决了由ZigBee预共享密钥泄露导致的访问控制失效问题.Wu等人[87]提出了LIGHTBLUE工具,该工具应用控制流和数据流分析的组合来删除BLE主机中未使用的代码,最大限度地减少了攻击面,减少了由于访问控制失效等导致的各种安全威胁.

4.2.2 网络层远场通信

网络层远场通信的安全威胁解决方案与近场通信的解决方案类似,通常有2种方案:1)设计新的适用于物联网远场通信并有安全通信保障的新协议;2)在原有协议基础上进行扩展或改进.Kumar等人[88]设计实现了物联网端对端加密协议JEDI(Joining Encryption and Delegation for IoT),可以用于解耦多对多通信,具有对数据的细粒度访问和支持密钥过期等各种适用于物联网远场通信的特性,特别是低成本、低功耗特性;JEDI协议还允许主体将密钥委托给其他主体,从而授予对数据的访问权限,并以可扩展的分布式方式管理访问控制.Jia等人[20]提出了新的控制关键协议实体的设计原则和增强访问模型MOUCON(message-oriented usage control model),以解决MQTT缺乏协议内实体保护和原始的MQTT协议的安全模型不支持身份、消息、会话状态等保护导致的安全威胁.Lohachab[89]基于椭圆曲线密码体制和MQTT协议提出了一种适用于分布式物联网环境的轻量级认证和授权框架.

4.3 应用层访问控制安全性解决方案

应用层包含云平台和用户App,其中存在云平台与用户的交互、云平台与设备的交互、云平台与云平台之间的交互等,在各种类型的交互中都存在着访问控制过程.而应用层在物联网架构中作为具备高性能运算与存储的层次,需要建立更完善的访问控制模型、更安全的认证与授权机制.

4.3.1 基于云平台上云应用行为的访问控制

目前,云平台中云应用所广泛运用的访问控制系统均基于权限,多项研究[90-92]已经证明基于权限的访问控制系统因其控制粒度不足,无法控制应用获得权限后的使用方式,使其仍不能阻止云应用的恶意行为.当前的学者为了解决这个问题,主要通过不同方式收集当前应用的行为,直接对应用行为进行安全审计,从而构建拥有更加细致的控制粒度的访问控制系统,这让应用即使拥有权限也无法做出恶意的行为.

目前的研究方向有3种,分别通过静态分析、动态插桩和监听流量来收集应用行为.

1) 静态分析.直接对应用的代码进行行为分析,判断应用是否存在恶意的行为.例如:SOTERIA[92]和 SAINT[93]均通过静态分析来识别应用的行为.其中,SAINT 主要跟踪应用中的信息流,避免用户敏感信息的泄露;而 SOTERIA 则主要分析应用中对 IoT 设备的控制,构建设备的状态机并分析安全性,防止恶意应用控制 IoT 设备,从而危害用户的生命财产安全.

2) 动态插桩.通过在已有的代码中手动或者自动的方式插入用于审计的代码,从而直接限制数据的流向或者在运行时收集上下文信息并分析出当前应用的行为.其中 FlowFence[94]通过开发人员在当前应用代码上增加、修改代码来控制数据的流向从而实现动态插桩,使得敏感数据只能流向预期的目标.ContexIoT[90], Tyche[91], ProvThings[95], IoTGuard[96], SmartAuth[97]均实现了自动插桩,不需要额外消耗开发人员的时间,能够自动跟踪数据的流向并分析程序操控 IoT 设备的行为.例如 ContexIoT,ProvThings 等还实现了用户界面,允许向用户警告程序的危险行为,让用户决定是否放行;而 SmartAuth 还额外有一套基于自然语言处理(natural language processing, NLP)的分析系统,可以自动获得程序正常的行为,从而减少向用户告警的次数.

3) 监听流量.这个方面最具有代表性的解决方案是 Homonit[98],其通过解析捕捉到 ZigBee 或者 Z-wave 等无线协议的流量,然后将这些流量中的特征进行分析从而得出应用是否存在不当行为.这种方式相对来说限制较小,不需要应用的源代码也可以对应用的行为进行检测,但是也最容易受到干扰导致误报.

4.3.2 统一且去中心化的云平台对接授权协议

在当前的云平台与云平台对接中,主要沿用了互联网中的 OAuth 协议,其作为一个集中式的权限管理协议,容易导致系统被攻陷后凭据被攻击者获取从而使得其破坏访问控制,因此授权协议应该是去中心化的.对于这个问题,已经有 Andersen 等人[72]和 Fernandes 等人[99]给出了 WAVE 和 XToken 的解决方案,他们都使用了基于密码学的方法,将集中式的权限模型变为分布式的权限模型,这使得即使一方权限被攻陷,攻击者也无法完全控制其所拥有的权限.另外,由于 OAuth 并非为 IoT 场景所设计,对接时往往需要传递额外的信息,比如设备、用户相关的资料,而这些信息本身可能是需要保密的,却可能被对接方错误地泄露出去,导致访问控制问题.为了解决这个问题,需要目前的云平台联合起来,基于 XToken,WAVE 等去中心化协议,共同商议出一套统一的对接授权协议.

4.3.3 云平台设备绑定

目前发现的设备绑定时漏洞的成因主要来自于在更改绑定状态模型时没有验证绑定状态转换的合法性和认证时使用静态设备身份认证信息.为此,应研究动态生成的设备绑定信息和经过验证的绑定状态模型.IoT 设备的设备 ID 等信息应在注册时由云平台通过算法生成后下发,而不是在出厂时硬编码进芯片中,并且生成算法中应包含用户 ID、随机数等难以被攻击者猜测、枚举出的信息.同时,为了防止攻击者进行恶意的绑定状态转换,云平台在对绑定状态进行转换时,应验证状态转换请求的发送用户的绑定状态、目标绑定的设备状态和请求消息中的认证信息,避免状态的非法转换[74].

4.4 小 结

当前物联网访问控制安全性解决方案总结如表 4 所示.总结当前的物联网访问控制安全性解决方案相关研究,漏洞的检测是各个层次都重点关注

Table 4 Security Solution of IoT Access Control

表 4 物联网访问控制安全性解决方案

物联网层次	针对攻击面	解决方案	相关文献
感知层	认证信息伪造	增加特征数量、多源认证,增加伪造难度	[45]
	设备漏洞	增强认证识别算法	[77-79]
		研究漏洞发现与修复技术	[80-83]
网络层	通信协议在认证机制、加解密、粒度等性能方面存在缺陷	设计新的安全通信协议	[20,84,88]
		在原有协议基础上扩展或改进	[57,85-87,89]
应用层	访问控制机制与协议缺陷	设计更合理的对接授权协议	[72,99]
	系统漏洞	应用行为细粒度审计	[90-98]
		增强设备绑定时验证,缓解设备绑定漏洞	[74]

的研究方向.而根据访问控制业务功能的区别,各层次的安全性解决方案也有所侧重.其中,感知层侧重认证信息伪造的规避;网络层侧重通信协议的安全加固;应用层侧重认证与授权机制以及协议的设计和完善.

根据当前的相关研究,物联网访问控制侧重架构与机制的设计、移植和应对攻击面的安全解决方案研究,在架构与安全性整体化设计方面还有所欠缺.

5 挑战与机遇

本节针对当前安全的物联网访问控制所面临的困难与挑战进行了总结.

1) 物联网设备种类规模巨大在当前环境下,物联网已经广泛渗透到各行各业中,在智能家居、智慧城市、工业 4.0 等各种场景中,都可以看到大量物联网设备的影子.规模如此巨大的物联网设备对访问控制系统的性能和架构提出了巨大的挑战.除了规模巨大,物联网设备由于在不同场景下的广泛运用,其种类也同样繁多,这些设备往往都针对特定场景进行了特殊的设计,导致不同设备之间存在巨大差异,包括计算能力、处理器架构、操作系统等多个方面,这使得访问控制系统不仅需要覆盖到所有场景下不同的设备类型,还要协调拥有不同特性的设备遵守其控制.为解决这些问题,需要研究让访问控制系统在拥有强大性能的同时还拥有良好的安全性和兼容性的方法.

2) 物联网安全架构复杂

物联网设备由于其天生的“万物互联”特性,一般采用分布式部署,物联网设备之间会直接进行通信而不依赖额外的中心服务器进行中转.但同时由于物联网设备需要提供给用户使用,一般仍然会存在一个中心的服务用于对用户提供接入、下发用户的命令或者接受来自设备的信息.这种复杂的中心化与去中心化混合的架构对访问控制系统提出了巨大的挑战,系统需要同时满足设备、用户、云端服务三者之间的访问控制,使得安全架构非常复杂,难以保证安全性.然而,当前的访问控制系统通常只着力于两者之间的访问控制,例如用户和设备之间的访问控制,而忽略云端,目前需要一种新的访问控制系统能够同时满足三者之间的安全访问控制,但同时保证系统能够适应物联网的特殊环境而不会变得过于复杂.

3) 解决方案以点为主缺乏统一

目前现有的物联网系统为了保证安全性,一般都会存在访问控制系统,但由于缺少类似互联网 Web 中的 OAuth,XACML 等统一的访问控制框架和协议,使得各个物联网系统均为“点”,需要通过自己编写实现的系统进行访问控制.这些系统往往缺少相关安全性测试,无法保证用户和设备的安全,且这些系统也无法互相对接,让“点”无法连成“线”和“面”,导致各个系统之间无法在保证安全的情况下方便地共享数据,与“万物互联”的理念相违背.因此,需要研究人员和当前广大的物联网设备公司进行合作,开发出一套统一而具有通用性的访问控制系统.

6 未来研究方向

为了实现更安全、更高效的物联网访问控制,本节提出了 3 个未来研究方向.

1) 深入研究物联网云平台访问控制

云平台作为物联网的数据中心和控制中心,其中接入了大量的设备并存储了大量的数据,一旦访问控制失效,将造成严重危害.然而,目前云平台的访问控制问题是物联网访问控制问题中的重灾区,包括云平台内部访问控制问题、云平台间的访问控制问题,以及云平台与设备、手机 App 等交互时的访问控制问题.由于云平台内部的复杂性、云平台中应用和设备的多样性、不同云平台厂商间的封闭性,以及云和设备、协议之间的安全鸿沟,目前难以找到统一适用的访问控制模型解决云平台的访问控制问题.深入研究物联网云平台访问控制,是未来亟需研究的方向之一.

2) 研究物联网云对接标准化

当前物联网云平台厂商各自都有自己的对接标准和访问控制机制,这些对接标准和访问控制机制能够很好地适配本厂商生产的设备,然而面对其他厂商生产的设备接入,或者本厂商生产的设备接入其他云平台时,就会引发访问控制失效问题.由于物联网具有分布式、灵活、动态接入的特性,很多厂商不仅允许与本厂商的 IoT 设备进行连接,还允许与其他厂商的云平台进行连接,甚至允许与自建云平台进行连接,这些连接过程由于不同的厂商有不同的标准规范,对连接后的平台和设备的访问控制安全性造成了极大的冲击.为延续物联网分布式、灵活、动态接入的特性,并使得对接入后的平台和设备

的安全性得到保证,本文认为标准化这些对接过程是非常必要的.

3) 在物联网访问控制中引入零信任理念

在应对物联网场景中的应用安全、网络安全、数据安全方面,仅在传统安全方案的基础上做边界加固和单点增强,难以系统性地缓解各类安全威胁,而零信任是一个新兴的模型,作为一种可以支撑未来发展的安全防护方式正逐渐受到越来越多的关注.零信任模型并非全盘否定,而是秉承网络始终存在内部和外部威胁,所有的设备、用户和流量在验证前不存在固有信任的原则,坚持持续验证、最小权限.因此,访问控制作为物联网场景中数据安全和网络安全防护的重要关口,需要引入零信任模型的理念进行物联网场景的适配和流程架构的设计,从而实现动态、实时、持续、精准、安全的访问控制.

7 总 结

近年来物联网安全事件频发,物联网安全越来越得到重视.而访问控制作为保护资源和信息的关键机制,在物联网生态中发挥着重要作用.本文针对物联网访问控制的安全性进行了充分的调研梳理,从物联网的3个层次分别展开,分析了每个层次中存在的风险脆弱点以及对应的攻击面,总结了近年来针对这些攻击面的防御理论和方法,并提出了物联网访问控制安全性设计要求.基于现有的理论研究基础,分析了安全的物联网访问控制中存在的挑战,最后给出了未来的研究热点.

作者贡献声明:刘奇旭负责论文的总体规划、指导与论文的撰写工作;靳泽负责论文主要内容的调研和撰写;陈灿华、高新博、郑宁军分层次负责相关工作的调研和梳理;方仪伟负责相关文献的整理和内容校对工作;冯云负责论文内容和结构的梳理.

参 考 文 献

[1] Sun Qibo, Liu Jie, Li Shan, et al. Internet of things: Summarize on concepts, architecture and key technology problem [J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(3): 1-9 (in Chinese)
(孙其博, 刘杰, 黎羴, 等. 物联网: 概念、架构与关键技术研究综述[J]. 北京邮电大学学报, 2010, 33(3): 1-9)

[2] Wegner P. Global IoT market size grew 22% in 2021—these 16 factors affect the growth trajectory to 2027 [EB/OL]. [2022-03-30]. https://iot-analytics.com/iot-market-size/

[3] Gartner. IoT Security primer: Challenges and emerging practices [EB/OL]. [2020-01-06]. https://www.gartner.com/en/doc/iot-security-primer-challenges-and-emerging-practices

[4] Which? Press Office. Popular connected cars from Ford and Volkswagen could put your security, privacy and safety at risk, Which? finds [EB/OL]. [2020-04-09]. https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds/

[5] Larson S. FDA confirms that St. Jude's cardiac devices can behacked [EB/OL]. [2017-01-09]. https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/

[6] Antonakakis M, April T, Bailey M, et al. Understanding the Mirai botnet [C] //Proc of the 26th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2017: 1093-1110

[7] Yaqoob I, Ahmed E, Hashem I A T, et al. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges [J]. IEEE Wireless Communications, 2017, 24(3): 10-16

[8] Ravidas S, Lekidis A, Paci F, et al. Access control in Internet-of-things: A survey [J]. Journal of Network and Computer Applications, 2019, 144: 79-101

[9] Zhang Yuqing, Zhou Wei, Peng Anni. Survey of Internet of things security [J]. Journal of Computer Research and Development, 2017, 54(10): 2130-2143 (in Chinese)
(张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10): 2130-2143)

[10] Yang YiYu, Zhou Wei, Zhao Shangru, et al. Survey of IoT security research: Threats, detection and defense [J]. Journal on Communications, 2021, 42(8): 188-205 (in Chinese)
(杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述: 威胁、检测与防御[J]. 通信学报, 2021, 42(8): 188-205)

[11] Yan Han, Peng Guojun, Luo Yuan, et al. Survey on smart home attack and defense methods [J]. Journal of Cyber Security, 2021, 6(4): 1-27 (in Chinese)
(严寒, 彭国军, 罗元, 等. 智能家居攻击与防御方法综述[J]. 信息安全学报, 2021, 6(4): 1-27)

[12] Wang Jice, Li Yilian, Jia Yan, et al. Survey of smart home security [J]. Journal of Computer Research and Development, 2018, 55(10): 2111-2124 (in Chinese)
(王基策, 李意莲, 贾岩, 等. 智能家居安全综述[J]. 计算机研究与发展, 2018, 55(10): 2111-2124)

[13] Peng Anni, Zhou Wei, Jia Yan, et al. Survey of the Internet of things operating system security [J]. Journal on Communications, 2018, 39(3): 22-34 (in Chinese)
(彭安妮, 周威, 贾岩, 等. 物联网操作系统安全研究综述[J]. 通信学报, 2018, 39(3): 22-34)

[14] Graham G S, Denning P J. Protection: Principles and practice [C] //Proc of the Spring Joint Computer Conf. New York: ACM, 1972: 417-429

[15] Bell D E, LaPadula L J. Secure computer systems: Mathematical foundations [R]. Bedford, MA: MITRE Corp, 1973

[16] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models [J]. Computer, 1996, 29(2): 38-47

[17] Yuan E, Tong Jin. Attributed based access control (ABAC) for Web services [C] //Proc of IEEE Int Conf on Web Services (ICWS). Piscataway, NJ: IEEE, 2005. DOI: 10.1109/ICWS.2005.25

[18] Park J, Sandhu R. The UCONABC usage control model [J]. ACM Transactions on Information and System Security, 2004, 7(1): 128-174

[19] Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of things [J]. Mathematical and Computer Modelling, 2013, 58(5-6): 1189-1205

[20] Jia Yan, Xing Luyi, Mao Yuhang, et al. Burglars' IoT paradise: Understanding and mitigating security risks of general messaging protocols on IoT clouds [C] //Proc of 2020 IEEE Symp on Security and Privacy (S&P). Piscataway, NJ: IEEE, 2020: 465-481

[21] Sethi P, Sarangi S R. Internet of things: Architectures, protocols, and applications [J]. Journal of Electrical and Computer Engineering, 2017(1): 1-25

[22] Ouaddah A, Bouij-Pasquier I, Abou A, et al. Security analysis and proposal of new access control model in the Internet of thing [C] //Proc of 2015 Int Conf on Electrical and Information Technologies (ICEIT). Piscataway, NJ: IEEE, 2015: 30-35

[23] Neisse R, Steri G, Baldini G. Enforcement of security policy rules for the Internet of things [C] //Proc of the 10th Int Conf on Wireless and Mobile Computing, Networking and Communications (WiMob). Piscataway, NJ: IEEE, 2014: 165-172

[24] Kim J E, Boulos G, Yackovich J, et al. Seamless integration of heterogeneous devices and access control in smart homes [C] //Proc of the 8th Int Conf on Intelligent Environments (IE). Piscataway, NJ: IEEE, 2012: 206-213

[25] Rivera D, Cruz-Piris L, Lopez-Civera G, et al. Applying an unified access control for IoT-based intelligent agent systems [C] //Proc of the 8th Int Conf on Service-oriented Computing and Applications (SOCA). Piscataway, NJ: IEEE, 2015: 247-251

[26] Liu Han, Han Dezhi, Li Dun. Fabric-IoT: A blockchain-based access control system in IoT [J]. IEEE Access, 2020, 8: 18207-18218

[27] Du Ruizhong, Liu Yan, Tian Junfeng. An access control method using smart contract for Internet of things [J]. Journal of Computer Research and Development, 2019, 56(10): 2287-2298 (in Chinese)
(杜瑞忠, 刘妍, 田俊峰. 物联网中基于智能合约的访问控制方法[J]. 计算机研究与发展, 2019, 56(10): 2287-2298)

[28] Dramé-Maigné S, Laurent M, Castillo L. Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts [C] //Proc of the 15th Int Wireless Communications & Mobile Computing Conf (IWCMC). Piscataway, NJ: IEEE, 2019: 1582-1587

[29] Alnefaie S, Cherif A, Alshehri S. Adistributed fog-based access control architecture for IoT [J]. KSII Transactions on Internet and Information Systems, 2021, 15(12): 4545-4566

[30] Cirani S, Picone M. Effective authorization for the Web of things [C] //Proc of 2015 IEEE World Forum on Internet of Things (WF-IoT). Piscataway, NJ: IEEE Computer Society, 2015: 316-320

[31] Hernández-Ramos J L, Jara A J, Marin L, et al. Distributed capability-based access control for the Internet of things [J]. Journal of Internet Services and Information Security, 2013, 3(3/4): 1-16

[32] Cirani S, Picone M, Gonizzi P, et al. IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios [J]. IEEE Sensors Journal, 2014, 15(2): 1224-1234

[33] Hernandez-Ramos J L, Pawlowski M P, Jara A J, et al. Toward a lightweight authentication and authorization framework for smart objects [J]. IEEE Journal on Selected Areas in Communications, 2015, 33(4): 690-702

[34] Seitz L, Selander G, Gehrmann C. Authorization framework for the Internet-of-things [C] //Proc of the 14th Int Symp on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). Piscataway, NJ: IEEE, 2013: 1-6

[35] Fremantle P, Aziz B, Kopecký J, et al. Federated identity and access management for the Internet of things [C] //Proc of 2014 Int Workshop on Secure Internet of Things (SIoT). Piscataway, NJ: IEEE, 2014: 10-17

[36] Zhang Guoping, Gong Wentao. The research of access control based on UCON in the Internet of things [J]. Journal of Software, 2011, 6(4): 724-731

[37] Jia Jindou, Qiu Xiaofeng, Cheng Cheng. Access control method for Web of things based on role and SNS [C] //Proc of the 12th Int Conf on Computer and Information Technology (CIT). Piscataway, NJ: IEEE, 2012: 316-321

[38] Barka E, Mathew S S, Atif Y. Securing the Web of things with role-based access control [C] //Proc of 2015 Int Conf on Codes, Cryptology, and Information Security (C2SI). Switzerland: Springer, Cham, 2015: 14-26

[39] Bai Guangdong, Yan Lin, Gu Liang, et al. Context-aware usage control for Web of things [J]. Security and Communication Networks, 2014, 7(12): 2696-2712

[40] Sikder A K, Petracca G, Aksu H, et al. A survey on sensor-based threats and attacks to smart devices and applications [J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1125-1159

[41] Sikder A K, Aksu H, Uluagac A S. 6thSense: A context-aware sensor-based attack detector for smart devices [C] //Proc of the 26th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2017: 397-414

[42] Tukur Y M, Ali Y S. Demonstrating the effect of insider attacks on perception layer of Internet of things (IoT) systems [C] //Proc of the 15th Int Conf on Electronics, Computer and Computation (ICECCO). Piscataway, NJ: IEEE, 2019: 1-6

[43] Tippenhauer N O, Pöpper C, Rasmussen K B, et al. On the requirements for successful GPS spoofing attacks [C] //Proc of the 18th ACM Conf on Computer and Communications Security (CCS). New York: ACM, 2011: 75-86

[44] Park Y, Son Y, Shin H, et al. This ain't your dose: Sensor spoofing attack on medical infusion pump [C/OL] //Proc of the 10th USENIX Workshop on Offensive Technologies (WOOT). Berkeley, CA: USENIX Association, 2016 [2022-04-22]. https://www.usenix.org/system/files/conference/woot16/woot16-paper-park_0.pdf

[45] Marasco E, Ross A. A survey on antispoofing schemes for fingerprint recognition systems [J]. ACM Computing Surveys, 2014, 47(2): 1-36

[46] Wu Zhizheng, Evans N, Kinnunen T, et al. Spoofing and countermeasures for speaker verification: A survey [J]. Speech Communication, 2015, 66: 130-153

[47] Sahidullah M, Delgado H, Todisco M, et al. Introduction to voice presentation attack detection and recent advances [M] //Handbook of Biometric Anti-spoofing. Switzerland: Springer, Cham, 2015: 321-361

[48] Zhang Guoming, Yan Chen, Ji Xiaoyu, et al. DolphinAttack: Inaudible voice commands [C] //Proc of the 2017 ACM Conf on Computer and Communications Security (SIGSAC). New York: ACM, 2017: 103-117

[49] Son Y, Shin H, Kim D, et al. Rocking drones with intentional sound noise on gyroscopic sensors [C] //Proc of the 24th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2015: 881-896

[50] Kumar D, Shen K, Case B, et al. All things considered: An analysis of IoT devices on home networks [C] //Proc of the 28th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2019: 1169-1185

[51] Stanislav M, Beardsley T. Hacking IoT: A case study on baby monitor exposures and vulnerabilities [EB/OL]. [2022-05-28]. https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

[52] Ronen E, Shamir A, Weingarten A O, et al. IoT goes nuclear: Creating a ZigBee chain reaction [C] //Proc of the 2017 IEEE Symp on Security and Privacy (S&P). Piscataway, NJ: IEEE, 2017: 195-212

[53] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model [C] //Proc of the Int Workshop on Cryptographic Hardware and Embedded Systems (CHES). Berlin: Springer, 2004: 16-29

[54] Kumar S, Sahoo S, Mahapatra A, et al. Security enhancements to system on chip devices for IoT perception layer [C] //Proc of the 2017 IEEE Int Symp on Nanoelectronic and Information Systems (iNIS). Piscataway, NJ: IEEE, 2017: 151-156

[55] Gnad D R E, Krautter J, Tahoori M B. Leaky noise: New side-channel attack vectors in mixed-signal IoT devices [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 2019(3): 305-339

[56] Park K Y, Yoo S G, Kim J H. Debug port protection mechanism for secure embedded devices [J]. Journal of Semiconductor Technology and Science, 2012, 12(2): 240-253

[57] Fawaz K, Kim K H, Shin K G. Protecting privacy of BLE device users [C] //Proc of the 25th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2016: 1205-1221

[58] Celosia G, Cunche M. Fingerprinting bluetooth-low-energy devices based on the generic attribute profile [C] //Proc of the 2nd Int ACM Workshop on Security and Privacy for the Internet-of-Things (IoTSec). New York: ACM, 2019: 24-31

[59] Zuo Chaoshun, Wen Haohuang, Lin Zhiqiang, et al. Automatic fingerprinting of vulnerable ble IoT devices with static uuids from mobile apps [C] //Proc of the 2019 ACM Conf on Computer and Communications Security (SIGSAC). New York: ACM, 2019: 1469-1483

[60] Sivakumaran P, Blasco J. A study of the feasibility of co-located app attacks against BLE and a large-scale analysis of the current application-layer security landscape [C] //Proc of the 28th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2019: 1-18

[61] Wen Haohuang, Lin Zhiqiang, Zhang Yinqian. FirmXRay: Detecting Bluetooth link layer vulnerabilities from bare-metal firmware [C] //Proc of the 2020 ACM Conf on Computer and Communications Security (SIGSAC). Berkeley, CA: USENIX Association, 2020: 167-180

[62] Wu Jianliang, Nan Yuhong, Kumar V, et al. BLESA: Spoofing attacks against reconnections in Bluetooth low energy [C/OL] //Proc of the 14th USENIX Workshop on Offensive Technologies (WOOT). Berkeley, CA: USENIX Association, 2020 [2022-04-19]. https://dl.acm.org/doi/pdf/10.1145/3133956.3134052

[63] Ludant N, Vo-Huu T D, Narain S, et al. Linking Bluetooth le & classic and implications for privacy-preserving Bluetooth-based protocols [C] //Proc of the 2021 IEEE Symp on Security and Privacy (S&P). Piscataway, NJ: IEEE, 2021: 1318-1331

[64] Morgner P, Mattejat S, Benenson Z, et al. Insecure to the touch: Attacking ZigBee 3.0 via touchlink commissioning [C] //Proc of the 10th ACM Conf on Security and Privacy in Wireless and Mobile Networks (WiSec). New York: ACM, 2017: 230-240

[65] Akestoridis D G, Harishankar M, Weber M, et al. Zigator: Analyzing the security of ZigBee-enabled smart homes [C] //Proc of the 13th ACM Conf on Security and Privacy in Wireless and Mobile Networks (WiSec). New York: ACM, 2020: 77-88

[66] Al Fardan N J, Paterson K G. Lucky thirteen: Breaking the TLS and DTLS record protocols [C] //Proc of the 2013 IEEE Symp on Security and Privacy (S&P). Piscataway, NJ: IEEE, 2013: 526-540

[67] Wang Qingying, Ji Shouling, Tian Yuan, et al. MPInspector: Asystematic and automatic approach for evaluating the security of IoT messaging protocols [C] //Proc of the 30th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2021: 4205-4222

[68] Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications [C] //Proc of 2016 IEEE Symp on Security and Privacy (S&P). Piscataway, NJ: IEEE, 2016: 636-654

[69] Surbatovich M, Aljuraidan J, Bauer L, et al. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes [C] //Proc of the 26th Int Conf on World Wide Web (WWW). New York: ACM, 2017: 1501-1510

[70] Cobb C, Surbatovich M, Kawakami A, et al. Howrisky are real users' IFTTT applets? [C] //Proc of the 16th Symp on Usable Privacy and Security (SOUPS). New York: ACM, 2020: 505-529

[71] Balliu M, Merro M, Pasqua M. Securing cross-app interactions in IoT platforms [C] //Proc of the 32nd Computer Security Foundations Symp (CSF). Piscataway, NJ: IEEE, 2019: 319-334

[72] Andersen M P, Kumar S, AbdelBaky M, et al. WAVE: A decentralized authorization framework with transitive delegation [C] //Proc of the 28th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2019: 1375-1392

[73] Yuan Bin, Jia Yan, Xing Luyi, et al. Shattered chain of trust: Understanding security risks in cross-cloud IoT access delegation [C] //Proc of the 29th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2020: 1183-1200

[74] Zhou Wei, Jia Yan, Yao Yao, et al. Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms [C] //Proc of the 28th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2019: 1133-1150

[75] Chen Jiongyi, Zuo Chaoshun, Diao Wenrui, et al.Your IoTs are (not) mine: On the remote binding between IoT devices and users [C] //Proc of the 49th Annual IEEE/IFIP Int Conf on Dependable Systems and Networks (DSN). Piscataway, NJ: IEEE, 2019: 222-233

[76] Jia Yan, Yuan Bin, Xing Luyi, et al. Who's in control? On security risks of disjointed IoT device management channels [C] //Proc of the 2021 ACM Conf on Computer and Communications Security (SIGSAC). New York: ACM, 2021: 1289-1305

[77] Ghiani L, Yambay D A, Mura V, et al. Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015 [J]. Image and Vision Computing, 2017, 58: 110-128

[78] Xia Zhihua, Yuan Chengsheng, Lv Rui, et al. A novel Weber local binary descriptor for fingerprint liveness detection [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 50(4): 1526-1536

[79] Yan Chen, Long Yong, Ji Xiaoyu, et al. The catcher in the field: A fieldprint based spoofing detection for text-independent speaker verification [C] //Proc of the 2019 ACM Conf on Computer and Communications Security (SIGSAC). New York: ACM, 2019: 1215-1229

[80] Chen Jiongyi, Diao Wenrui, Zhao Qingchuan, et al. IoTFuzzer: Discovering memory corruptions in IoT through app-based fuzzing [C] //Proc of Network and Distributed System Security Symp (NDSS). Piscataway, NJ: IEEE, 2018: 1-15

[81] Zheng Yaowen, Davanian A, Yin Heng, et al. FIRM-AFL: High-throughput greybox fuzzing of IoT firmware via augmented process emulation [C] //Proc of the 28th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2019: 1099-1114

[82] Lesjak C, Hein D, Winter J. Hardware-security technologies for industrial IoT: TrustZone and security controller [C] //Proc of the 41st Annual Conf of the IEEE Industrial Electronics Society (IECON). Piscataway, NJ: IEEE, 2015: 2589-2595

[83] Zhou Jie, Du Yufei, Shen Zhuojia, et al. Silhouette: Efficient protected shadow stacks for embedded systems [C] //Proc of the 29th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2020: 1219-1236

[84] Luo Xi, Yin Lihua, Li Chao, et al. A lightweight privacy-preserving communication protocol for heterogeneous IoT environment [J]. IEEE Access, 2020, 8: 67192-67204

[85] Alshahrani M, Traore I, Woungang I. Anonymous mutual IoT interdevice authentication and key agreement scheme based on the ZigBee technique [J]. Internet of Things, 2019, 7: 100061

[86] Wang Weicheng, Cicala F, Hussain S R, et al. Analyzing the attack landscape of ZigBee-enabled IoT systems and reinstating users' privacy [C] //Proc of the 13th ACM Conf on Security and Privacy in Wireless and Mobile Networks (WiSec). New York: ACM, 2020: 133-143

[87] Wu Jianliang, Wu Ruoyu, Antonioli D, et al. LIGHTBLUE: Automatic profile-aware debloating of Bluetooth stacks [C] // Proc of the 30th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2021: 339-356

[88] Kumar S, Hu Yuncong, Andersen M P, et al. JEDI: Many-to-many end-to-end encryption and key delegation for IoT [C] //Proc of the 28th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2019: 1519-1536

[89] Lohachab A. ECC based inter-device authentication and authorization scheme using MQTT for IoT networks [J]. Journal of Information Security and Applications, 2019, 46: 1-12

[90] Jia Yunhan, Chen Qi, Wang Shiqi, et al. ContexIoT: Towards providing contextual integrity to appified IoT platforms [C/OL] //Proc of Network and Distributed System Security Symp (NDSS).Piscataway, NJ: IEEE, 2017 [2022-05-28]. https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss2017_08-2_Jia_paper.pdf

[91] Rahmati A, Fernandes E, Eykholt K, et al. Tyche: A risk-based permission model for smart homes [C] //Proc of the 2018 IEEE Cybersecurity Development (SecDev). Piscataway, NJ: IEEE, 2018: 29-36

[92] Celik Z B, McDaniel P, Tan G. SOTERIA: Automated IoT safety and security analysis [C] //Proc of the 2018 USENIX Annual Technical Conf (USENIX ATC 18). Berkeley, CA: USENIX Association, 2018: 147-158

[93] Celik Z B, Babun L, Sikder A K, et al. Sensitive information tracking in commodity IoT [C] //Proc of the 27th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2018: 1687-1704

[94] Fernandes E, Paupore J, Rahmati A, et al. FlowFence: Practical data protection for emerging IoT application frameworks [C] //Proc of the 25th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2016: 531-548

[95] Wang Qi, Hassan W U, Bates A, et al.Fear and logging in the Internet of things [C] //Proc of Network and Distributed System Security Symp (NDSS).Piscataway, NJ: IEEE, 2018 [2022-05-28]. https://www.ndss-symposium.org/wp-content/uploads/2018/03/NDSS2018_01A-2_Wang_Slides.pdf

[96] Celik Z B, Tan Gang, McDaniel P D. IoT Guard: Dynamic enforcement of security and safety policy in commodity IoT [C] //Proc of Network and Distributed System Security Symp (NDSS). Piscataway, NJ: IEEE, 2019 [2022-05-28]. https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_07A-1_Celik_paper.pdf

[97] Tian Yuan, Zhang Nan, Lin Y H, et al. SmartAuth: User-centered authorization for the Internet of things [C] //Proc of the 26th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2017: 361-378

[98] Zhang Wei, Meng Yan, Liu Yugeng, et al. Homonit: Monitoring smart home apps from encrypted traffic [C] //Proc of the 2018 ACM Conf on Computer and Communications Security (SIGSAC). New York: ACM, 2018: 1074-1088

[99] Fernandes E, Rahmati A, Jung J, et al. Decentralized action integrity for trigger-action IoT platforms [C] //Proc of Network and Distributed System Security Symp (NDSS). Piscataway, NJ: IEEE, 2018 [2022-05-28]. https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-3_Fernandes_paper.pdf

Liu Qixu, born in 1984. PhD, professor, PhD supervisor. His main research interests include network attack and defense technology, cyber-attacks discovery, attribution and forensic.

刘奇旭,1984 年生.博士,教授,博士生导师.主要研究方向为网络攻防技术、网络攻击发现和溯源取证.

Jin Ze, born in 1995. PhD candidate. His main research interests include IoT security, network attack and defense technology.

靳　泽,1995 年生.博士研究生.主要研究方向为物联网安全和网络攻防技术.

Chen Canhua, born in 1999. PhD candidate. His main research interests include network attack and defense technology, Web security and program analysis.

陈灿华,1999 年生.博士研究生.主要研究方向为网络攻防技术、Web 安全和程序分析.

Gao Xinbo, born in 1998. Master candidate. His main research interest is cyber security.

高新博,1998 年生.硕士研究生.主要研究方向为网络安全.

Zheng Ningjun, born in 1999. Master candidate. His main research interest is Web security.

郑宁军,1999 年生.硕士研究生.主要研究方向为 Web 安全.

Fang Yiwei, born in 1997. PhD candidate. His main research interests include IoT security, network attack and defense technology.

方仪伟,1997 年生.博士研究生.主要研究方向为物联网安全和网络攻防技术.

Feng Yun, born in 1993. PhD. Her main research interests include cyber security, cyber-attacks discovery, attribution and forensic.

冯　云,1993 年生.博士.主要研究方向为网络安全、网络攻击发现和溯源取证.