物联网安全研究综述：威胁、检测与防御

杨毅宇[1]，周威[1]，赵尚儒[1]，刘聪[2]，张宇辉[3]，王鹤[3]，王文杰[1]，张玉清[1,2,3,4]

（1. 中国科学院大学国家计算机网络入侵防范中心，北京 101408；2. 西安邮电大学网络空间安全学院，陕西 西安 710121；
3. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；4. 海南大学计算机与网络空间安全学院，海南 海口 570228）

摘 要：基于近 5 年网安国际会议（ACM CCS、USENIX Security、NDSS、IEEE S&P）中发表的物联网安全文献，以及其他部分高水平研究工作，从威胁、检测、防御的视角对物联网安全研究工作进行了系统的整理和分析。首先，介绍了物联网系统的基本架构。然后，将当前研究中提出的主要威胁分为 8 种类型，并分析了威胁的成因和危害。之后，介绍了针对这些威胁所提出的 6 种威胁检测和 5 种防御方案，并对比了它们的技术原理和优缺点。最后，提出了当前研究依然面临的主要挑战，并指出了未来研究发展的方向。

关键词：物联网；安全；威胁；检测；防御

中图分类号：TP391.44

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021124

Survey of IoT security research: threats, detection and defense

YANG Yiyu[1], ZHOU Wei[1], ZHAO Shangru[1], LIU Cong[2], ZHANG Yuhui[3],
WANG He[3], WANG Wenjie[1], ZHANG Yuqing[1,2,3,4]

1. National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China
2. School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China
3. School of Cyber Engineering, Xidian University, Xi'an 710071, China
4. School of Computer Science and Cyberspace Security, Hainan University, Haikou 570228, China

Abstract: Based on the IoT security literatures published in the international conferences on network security (ACM CCS, USENIX Security, NDSS, IEEE S&P) in recent five years, and other prominent researches, the works from the perspective of "threat, detection, defense" were systematically summarized and analyzed. Firstly the basic architecture of the IoT system was introduced. Then the main threats proposed in these works were classified into eight categories, and the causes and hazards of the threats were analyzed. After that, six detection and five defense schemes against these threats were introduced, and their technical principles, advantages and disadvantages were compared. At last, on the basis of the above analysis, the main challenges that the current research still faces were put forward, and the research directions of future works were point out.

Keywords: IoT, security, threat, detection, defense

1 引言

近 5 年来，物联网设备数量呈爆炸性增长，根据权威统计机构发布的数据，全球接入网络的物联网设备数量在 2017 年已达 20.35 亿台，并且到 2025 年将增长到超过 75.44 亿台[1]，物联网将深刻影响人类生产和生活的各个方面。然而，在物联网蓬勃发展的过程中，现有的安全机制难以应对日益增长的安全需求，导致各类应用场景中的安全问题层出不穷[2]，大量设备容易遭受恶意代码威胁或非法控制，

收稿日期：2021−01−03；**修回日期**：2021−04−14

通信作者：张玉清，zhangyq@nipc.org.cn

基金项目：国家重点研发计划基金资助项目（No.2018YFB0804701）；国家自然科学基金资助项目（No.U1836210）

Foundation Items: The National Key Research and Development Program of China (No.2018YFB0804701), The National Natural Science Foundation of China (No.U1836210)

甚至引发大规模安全事故。从 2016 年著名的 Mirai 蠕虫利用物联网设备引发大规模拒绝服务攻击事件[3]，到近期的智能音箱被攻击者利用来窃听用户隐私[4]，物联网安全威胁随着技术发展而不断出现。

及时检测发现安全威胁或提前采取防御是对抗威胁的重要手段，但是物联网系统的特性[1]决定了对其实施完善的安全防护面临诸多挑战。例如，物联网平台在设计开发、通信交互、访问控制等方面缺乏统一的标准，设备的内部和外部运行环境缺乏有效保护，已有的解决方案中存在应用面窄、自动化不足等缺点。因此，面对不断出现的安全威胁，仍需要深入研究更全面可靠的检测和防御方案。

本文基于 2016 年—2020 年网络安全会议（ACM CCS、USENIX Security、NDSS、IEEE S&P）中发表的物联网安全相关文献，以及其他在物联网安全研究方面的高水平工作进行了总结分析。从“威胁、检测、防御”的角度对 104 篇相关文献进行分析与整理，并围绕相应主题进行深入讨论。各类别的文献数量统计结果如图 1 所示，部分文献在发现威胁的同时，建立了有效的检测或防御方案，因此同时计入 2 个类别中。从图 1 可看出，在威胁方面，近 5 年文献数量总体持续增加，说明近有新的威胁被不断发现，本文对这些威胁进行了分类，并分析了它们的成因和危害；在检测和防御方面，后 3 年数量较前两年有显著增加，说明针对已知威胁有更多的对抗方案被提出，本文也对这些检测和防御方案的技术特点进行了分析与总结。

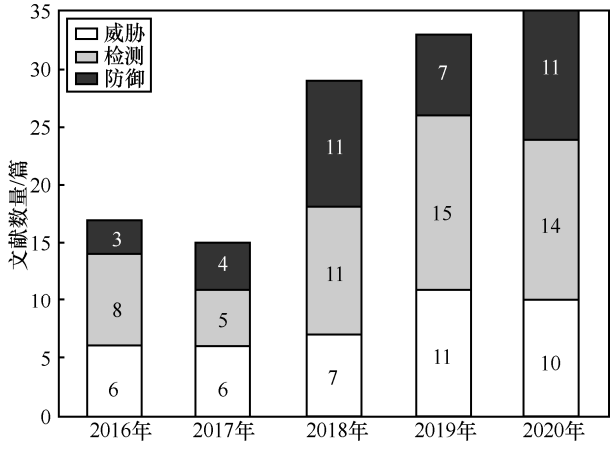


图 1　2016 年—2020 年物联网安全代表性研究统计

虽然当前已有面向物联网安全的综述研究[5-7]，但是专门对现有研究工作提出的攻击和检测防御方案的总结分析较少，本文紧紧围绕“威胁、检测、防御”3 个主题，覆盖近 5 年物联网安全研究工作的主要方向，同时深入分析各类威胁的成因和危害，以及对应的检测和防御机制的技术类型和效果。本文的主要贡献如下：1) 系统总结近 5 年物联网安全研究中发现的主要安全威胁，展示这些威胁产生的成因和危害；2) 深入分析对抗这些安全威胁的主要检测和防御方案，展示这些方案的技术类型和效果；3) 基于威胁、检测和防御 3 个方面的分析来揭示物联网未来发展过程中将面临的主要安全挑战，并指出物联网安全研究下一步的方向。

2　背景介绍

本节对物联网系统的基本架构，以及架构各层对应的主要研究对象进行介绍，如图 2 所示。物联网系统的一般架构主要分为感知层、网络层、应用层 3 个部分。

感知层对应的是各类物联网设备。设备通过传感器实时收集应用场景信息并发送给应用层，或接收应用层指令并执行相应动作。设备的内部架构可以分为硬件层、系统层、用户层。其中，硬件层包括支持设备功能的各种硬件模组（如网络模组、传感器模组等）、处理器、外围电路等；系统层装载了固件程序，其中包括操作系统和应用程序，负责设备功能的实现；用户层主要向用户提供展示数据和接收输入的操作接口。

网络层对应的是设备之间，以及设备、云平台、手机 App 这三类实体之间的通信。设备之间可以通过 ZigBee、Z-Wave 等轻量级协议形成自组网络（如工业设备网络、无人机集群）；设备也可以经路由器连接后形成局域网（如智能家居网络）。设备连接路由器有 2 种形式：一是直接通过 Wi-Fi 连接；二是通过 ZigBee、Z-Wave 等协议与网关设备（如 hub）连接后，再经网关通过 Wi-Fi 与路由器通信。

实体之间通信分为 3 种类型：1) 设备与 App 通信，设备既可以通过蓝牙直接连接手机（如可穿戴设备、车载系统网络），也可以通过局域网 Wi-Fi 与手机通信（如智能家居网络）；2) 设备与云平台通信，设备依靠路由器转发请求和接收响应，而路由器与云平台的通信主要由传统 TCP/IP 网络架构实现；3) 手机与云平台通信：手机 App 可以通过 4G/5G 网络或局域网 Wi-Fi 连接云平台。

应用层对应的主要是云平台和手机 App。云平台主要由厂商在云端部署的各类应用服务组成，负

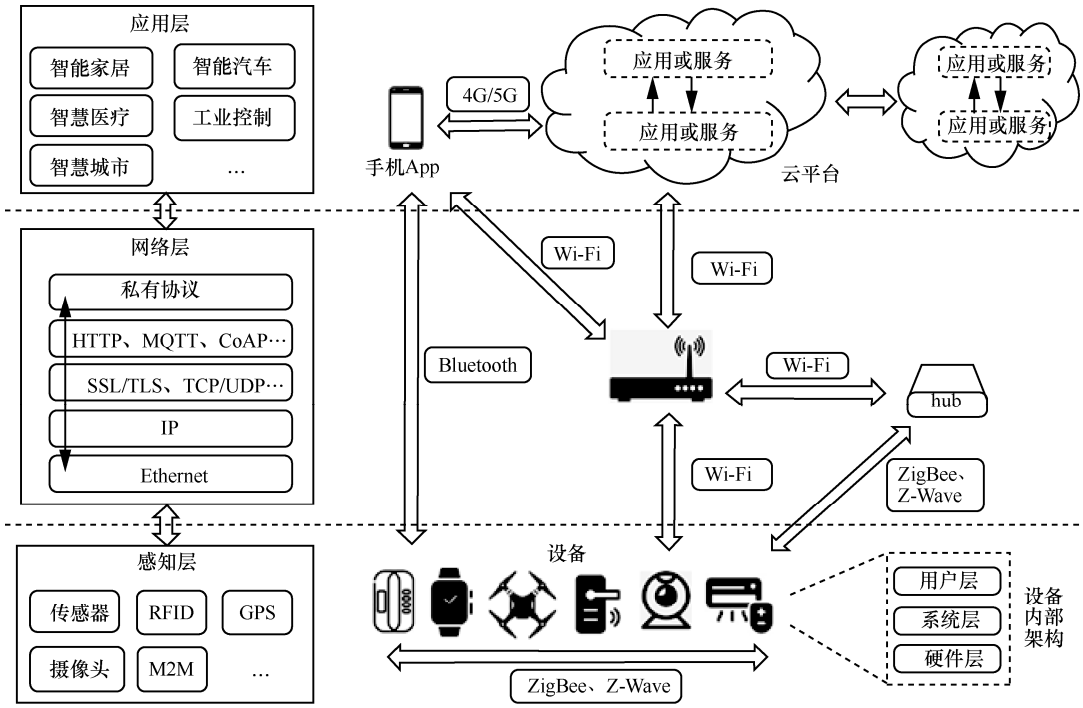


图 2 物联网系统基本架构与研究对象

责管理设备和用户，对设备收集的数据进行处理，或向设备发送远程控制命令。根据云平台提供的功能，可以将其分为设备接入平台、服务联动平台、语音助手平台 3 种。设备接入平台提供了实际的设备接入和管理功能，如 Samsung SmartThings、Google Home、Philips Hue、小米米家等；服务联动平台并没有连接真实的设备，而是将其他平台的功能连接起来，提供“条件−动作”自动执行规则服务，如 IFTTT 平台等；语音助手平台通过智能音箱向用户提供语音控制服务，用户发出的语音命令经语音平台处理后可以与其他控制设备的功能或服务连接到一起，如 Amazon Alexa 等。另外，不同云平台之间也可以在授权后，通过互相调用 API（application programming interface）执行设备控制。手机 App 可看作云平台向用户提供的控制终端，主要用于向用户提供设备相关的功能界面，可以直观展示设备状态，或者执行控制命令。

3 研究现状

3.1 安全威胁

传统安全问题在物联网系统中具有特殊的表现形式，而物联网系统由于自身特性也引入了新的威胁类型。本节进一步从云平台、通信、设备等角度将研究发现的安全威胁归为 8 类，分别阐述了各类安全威胁的漏洞成因和主要危害，分类结果如表 1 所示。

3.1.1 云平台访问控制缺陷

访问控制是云平台正常运转的重要前提，物联网云平台连接了大量与人类紧密联系的设备，如果身份验证或权限管理出现漏洞，云平台将转变成为攻击者的强大武器。现有研究显示，云平台的访问控制问题突出[8]，本节根据授权类型将权限管理的威胁分为平台内和平台间 2 种。

首先，部分平台对内部应用或服务的权限管理设计存在漏洞。SmartThings 和 IFTTT 是全球范围内广受欢迎的云平台，拥有广大的用户群体，且连接了海量的设备和服务，但是 Fernandes 等[9-10]发现这 2 家平台都对连接设备的应用或服务采取了粗粒度的权限划分方式，应用或服务可以获得其申请范围之外的权限，导致攻击者可以利用这种缺陷对他人的设备轻易发起信息监听或越权控制。

其次，云平台之间进行相互授权的过程中也存在设计漏洞。当前大部分云平台都允许用户将注册在其他厂商平台下的设备，经过“云云授权”后与自家平台联接（例如，可以将小京鱼平台下的设备联接到小米米家平台，通过米家 App 控制小京鱼平台的设备）。然而，在目前缺乏统一的平台间授权标准的情况下，即使厂商在自身范围内做好了安全审核，在权限交接时可能会因为平台之间不对称的

表 1　　各类安全威胁的漏洞成因和主要危害

威胁类型	漏洞成因	主要危害	文献	文献数量/篇
云平台访问控制缺陷	授权粒度过粗，授权标准不对称	越权控制、事件窃听、隐私泄露	文献[8-11]	4
云平台恶意应用	恶意用户上传应用，应用审核机制不完善	隐私泄露、非法控制	文献[4,9,12-17]	8
云平台实体和应用交互漏洞	实体和应用交互复杂，执行冲突难以检测	设备劫持、拒绝服务、隐私泄露	文献[13-14,18-20]	5
通信协议漏洞	协议缺乏内建安全机制，厂商忽略安全因素	拒绝服务、设备劫持、重放攻击、隐私泄露	文献[18-19,21-27]	9
通信流量侧信道信息泄露	物联网通信流量具有突出特征	隐私泄露	文献[28-33]	6
设备固件漏洞	有限的计算和存储资源，缺乏有效检测工具，缺乏内存和权限管理	系统崩溃、保护绕过、恶意命令、隐私泄露	文献[34-41]	8
基于语音信道的攻击	藏匿在语音信道中的命令	越权控制、隐私泄露	文献[42-47]	6
基于物联网设备的僵尸网络	设备规模庞大，设备漏洞广泛存在	大规模拒绝服务、恶意软件分发	文献[48-50]	3

授权要求而暴露新的漏洞。Yuan 等[11]针对这类安全问题进行了系统性研究，在多家全球知名的云平台之间的授权过程中都发现了安全漏洞，这些安全漏洞导致攻击者可以通过代理平台绕过设备自身平台的保护机制，对设备发起非法访问。

3.1.2　云平台恶意应用

云平台提供了面向设备的各类应用，用户通过应用可以实现丰富的控制功能。但是，目前云平台对应用的安全审查不够完善，导致恶意应用混杂其中，本节介绍云平台恶意应用的几种形式。

部分云平台对用户来说是完全封闭的，用户无法获取应用的逻辑或代码，只能安装云平台封装好的应用或自动执行规则。部分平台虽然对用户隐藏底层的运行机制，但会开放一系列基础设计功能（如 API 或编程框架）给用户，用户可以自己编写和发布应用。这类平台包括 SmartThings、IFTTT、Alexa 等，它们虽然提供了更加丰富和灵活的应用生态，但是为攻击者提供了实现恶意应用的机会。

关于 SmartThings 平台的多项研究[9,12-14]都证明该平台的应用开放特性和不完善的审核机制极易引入恶意应用，已公开发布的应用（如 SmartThings 中的 SmartApp）中，近 2/3 都具有泄露设备隐私的风险[12]。在 IFTTT 平台中，Bastys 等[15]发现市场中近 30%的服务（如 IFTTT 中的 Applet）存在安全隐患，攻击者在代码中嵌入的恶意链接会将用户输入的隐私信息发送到攻击者服务器。此外，恶意代码在语音平台中的表现形式是带有恶意意图的 Skill[4]，攻击者可以上传恶意的 Skill[16-17]，在用户不易察觉的情况下暗中劫持正常的语音命令或替换真实 Skill 的功能。

3.1.3　云平台实体和应用交互漏洞

云平台、手机 App、设备三类实体之间的交互是物联网云平台区别于传统云服务的重要特性，然而复杂的交互过程也带来了安全挑战。本节将交互漏洞分为实体间交互和应用间交互 2 种类型。

在用户访问设备的过程中，设备可能经历注册、绑定、使用、解绑、重置等阶段，在各个阶段中，云平台、手机 App、设备这三类实体需要进行信息交互和状态转换，并且各实体的交互和转换次序必须遵照既定模型进行，如图 3 所示，任一实体对交互模型的违背都会破坏模型的完整性。

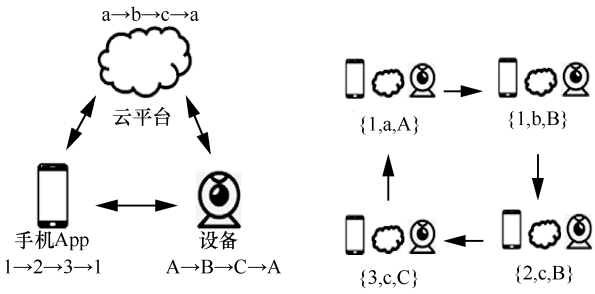


图 3　云平台三类实体交互模型

Zhou 等[18]和 Chen 等[19]分别对多家全球知名厂商平台的实体交互过程进行检测后发现，厂商对功能的实现并未严格遵守通信模型的规定，例如，用户解除云平台中的设备绑定关系后，设备不会回退到初始状态，而是依然与云平台保持连接，所以攻击者可以在此时对该设备发起绑定请求实现远程劫持。

云平台应用或服务的交互情形有 2 种，一是多个应用控制相同的设备，此时设备是应用的“交点”；二是多个应用的触发条件或执行动作重合，此时条件或动作是应用的“交点”。当多个应用在

同一场景下被使用时，它们在“交点”上可能产生不可预期的执行冲突，而这种冲突会改变应用或服务的执行结果[13-14,20]。例如，智能家居场景中部署了 2 条服务，分别为“如果检测到烟雾，则打开水阀”和“如果检测到漏水，则关闭水阀”，当厨房发生火灾时，烟雾传感器命令水阀打开，同时开启屋顶喷水器（第一条服务生效），但是漏水传感器检测到水流后命令水阀关闭（第二条服务生效），最终这种冲突将导致自动灭火的规则失效，引起人身财产损失。值得注意的是，这种威胁不一定来自恶意应用，也可能是由多个良性应用同时执行产生冲突造成的，由于服务规则间交互的复杂性，云平台依靠传统的审核机制难以发现这种问题。

3.1.4 通信协议漏洞

物联网系统通信融合了传统的 TCP/IP 协议，以及在物联网系统中常见的底层协议和私有协议，针对传统协议的威胁会被引入物联网，物联网系统协议在设计和实现过程中的缺陷也会产生新的安全漏洞。本节主要关注与物联网系统密切相关的 2 种协议：物联网常见协议和私有协议。

首先是物联网常用协议，如 MQTT（message queuing telemetry transport）、CoAP、ZigBee、低功耗蓝牙等。这类协议虽然不是专门为物联网系统定制设计的，但是由于其适配于低功耗设备和低带宽需求的特性而受到众多物联网系统的青睐，因此在物联网系统中有较高的使用率，但是其本身并非为存在对抗性的应用场景所设计，因此缺乏内建的安全机制，厂商在应用和实现这些协议时容易忽略对安全属性的考虑。Jia 等[21]在多家全球知名厂商的物联网平台中，都发现其对 MQTT 协议的实现存在缺陷，被攻击者利用后可能引发大规模分布式拒绝服务、远程设备劫持、用户隐私窃取等攻击。Cao 等[22]发现基于 ZigBee 的 ghost 攻击会造成设备能量过度消耗，引发拒绝服务和重放攻击等威胁。低功耗蓝牙是当前可穿戴设备与手机 App 通信的主要渠道，但是该协议在应用过程中被发现隐私泄露[23-24]、设备劫持[25]等威胁。

其次是物联网私有协议。这类协议是指厂商定制设计的协议类型，通常只适用于其平台下设备的通信，且一般不对外开放实现细节。但是，攻击者通过逆向工程仍可以获取通信细节，如果厂商对私有协议的设计存在缺陷，也可能被攻击者利用后发起攻击。当前研究[18-19,26-27]已证明全球多家知名物联网厂商的私有协议在被成功解析后，其关于设备认证与授权检查等方面的漏洞将立即暴露在攻击者眼前。

3.1.5 通信流量侧信道信息泄露

物联网系统中规模庞大和种类丰富的网络流量为侧信道攻击的实施提供了可行性条件，同时物联网系统的通信过程具有区别于其他系统的内在特性，例如，设备只被分配简单的任务和操作，只能发起有限的服务请求，并采用固定的协议和传输模式进行通信，所以物联网的通信流量具有明显的可识别特征。虽然有各类加密机制应用在流量信息保护中，但是仍然不能防止攻击者通过侧信道特征获得设备和用户相关的敏感信息。

表 2 对几种侧信道攻击方法进行了对比。从表 2 可以看出，协议头部特征（如端口号、负载大小、DNS 查询目标等）容易提取，但是能获取的设备知识较少，例如，只能得知目标设备或对象是否存在，或者获知目标设备类型，在简单的交互环境中可以实现信息提取。虽然信号强度、方向、包长、时间等特征提取后需要采用特定的统计学习方法进行分析，但是可以获得较多关于的设备和活动信息。

表 2 侧信道攻击方法对比

文献	采用特征	识别方法	攻击效果
文献[28]	Wi-Fi 信号强度	Wi-Fi 多路信号传播波动模型	①
文献[29]	端口号、负载大小、TCP 窗口值等	CNN（convolutional neural network）+ RNN（recurrent neural network）	①②
文献[30]	DNS 查询目标、NTP 请求数、SSL/TLS 加密套件	朴素贝叶斯多项式分类和随机森林	①②
文献[31]	方向、包长、发包时间间隔平均值和标准差	随机森林、DBSCAN（density-based spatial clustering of applications with noise）	①②③④
文献[32]	包长平均值和方差、时间间隔平均值、tsfresh 和特征工程提取的特征	k 近邻、随机森林、隐式马尔可夫模型	①②③④⑤
文献[33]	方向和包长	DBSCAN	①②③④⑤

注：①判断设备/目标存在，②识别设备类型，③判断设备事件发生，④识别事件，⑤推断用户行为

3.1.6 设备固件漏洞

固件是运行在设备中的二进制程序，负责管理设备中的硬件外设以及实现设备的应用功能。固件不同于传统的个人计算机或手机程序拥有成熟的漏洞检测和系统保护技术，大部分固件所运行的实时操作系统中缺乏基本的安全保护措施，如 DEP（data execution prevention）、ASLR（address space layout randomization）等。同时，当前缺乏对固件程序进行调试和检测的有效工具，导致大量携带漏洞的固件存在于实际产品中，攻击者利用这些漏洞可以对设备进行拒绝服务、非法操作和劫持等攻击。本节根据固件漏洞产生的原因将其分为内存漏洞和逻辑漏洞 2 类。

固件内存漏洞一般由编码或设计错误引起，会导致内存非法访问、控制流劫持等攻击，如堆栈缓冲区溢出。物联网设备固件主要由底层语言（如 C 语言）开发，在开发过程中会不可避免地引入编码缺陷。在硬件层面，设备的 CPU 异构性、外设多样性等特点，使对固件程序开展规模化和自动化的漏洞检测十分困难。在软件层面，设备操作系统呈现碎片化，同时由于有限的硬件资源导致缺乏必要的动态防御措施，如 CFI（control flow integrity）等，导致攻击者更加容易利用内存漏洞。多项研究指出，代码注入[34-36]、控制流劫持[37-38]、跨二进制模块的调用[39]是固件内存漏洞的主要成因。

固件逻辑漏洞指的是固件在认证、授权、应用功能等方面的设计或实现缺陷。与内存漏洞不同，这种漏洞不一定会引发系统崩溃，攻击者利用逻辑设计缺陷，构造特定的输入就可以使程序的正常功能发生偏移。例如，认证绕过漏洞[40]是典型的固件逻辑漏洞类型，攻击者可以通过这种漏洞绕过系统对特权指令的权限检查；在智能网络打印机固件程序中的功能设计缺陷在实际办公场景中会导致任务篡改、机密窃取等后果[41]。

3.1.7 基于语音信道的攻击

语音助手设备（如智能音箱）在物联网系统中处于控制中心的地位，用户可以通过语音助手设备来控制其他设备，所以对语音设备的攻击将会威胁受其控制的所有设备。

首先，部分攻击技术可以在语音信道中藏匿人类无法察觉但设备可以识别的语音信号。Carlini 等[42]首先展示了用于构造可被语音识别系统解释但不被人类发现的语音命令的几种方法，同时证明这些命令会在暗中窥探用户隐私和自行打开钓鱼网站。之后，多项研究发现了传播语音命令的载体，例如，将语音信号调制为人类无法识别的高频超声波信号[43]，或者将语音命令嵌入音乐中[44]；还有研究将承载语音设备的固体作为媒介，通过固体震动频率来传输语音命令[45]，以上攻击的共同特点是语音设备可以正常接收和解释这种信号，但是人类难以察觉交互过程。

另外，隐藏的语音信号在传输过程中面临传播距离和噪声影响的挑战，但这种困难被证明可以克服。例如，Roy 等[46]通过多个扬声器来分离语音信号的频带，显著增加了攻击距离。Chen 等[47]通过提取硬件结构和信道频率造成的信号失真影响因素，以此作为生成语音信号对抗样本的因子之一，可以有效克服传播中的噪声影响，提高语音信号被识别的成功率。

3.1.8 基于物联网设备的僵尸网络

物联网系统中的设备数量众多且规模庞大，其一旦被病毒、木马等恶意软件攻击，就可以组建威力巨大的僵尸网络。被病毒劫持的设备除了无法正常使用之外，组成的僵尸网络还可被攻击者当作其他恶意行为的“跳板”，为后续的大规模分布式拒绝服务攻击、恶意邮件分发等攻击做好准备。

著名的 Mirai 病毒以及由其衍生出的多类变种至今仍然是工控系统设备的主要威胁[48]。例如，MadIoT[49-50]是一种面向电网系统的新型攻击，利用被控制的高功率家庭物联网设备组建僵尸网络，以此操纵电网中的电力需求，进而向电网系统发起攻击，造成局域或大规模停电事故。此外，Ronen 等[51]展示了一种利用 ZigBee 协议漏洞可在物联网设备中进行大规模传播的蠕虫病毒，该病毒可在邻近的智能路灯之间进行快速传播并导致设备接受远程控制，攻击者可接管城市的路灯控制权，从而发起大规模分布式拒绝服务攻击。

3.1.9 安全威胁小结

下面对 3.1 节中关于安全威胁研究的特点和不足进行总结，主要分为以下几个方面。

1) 云平台威胁影响严重，但是当前研究针对的云平台类型有限。物联网云平台在近几年中获得了巨大发展，与之相关的安全研究也不断增多，但是从近 5 年的研究来看，当前研究比较依赖于平台的“开放”特性，大多数研究[9-14]都围绕 SmartThings、IFTTT 等可获取应用内部逻辑的云平台，而当前更

多的云平台并不对外开放内部逻辑。在开放平台中已发现的威胁可能在封闭平台中同样存在，因此对封闭平台的类似威胁研究有待探索。

2) 云平台更注重系统机密性的保护，而轻视了系统的完整性和可用性。当前大多云平台通过加密机制对外隐藏应用和通信协议的实现作为主要的安全机制，而对其他的安全因素疏于维护，如身份和权限检查、交互模型维护等。上述的多项研究[11, 18-19, 26]表明，在物联网系统这种存在对抗性交互的环境中，敌手有能力破解加密保护，因此云平台在授权管理、协议应用、实体交互等过程中如果存在安全漏洞，将会被敌手轻易利用，云平台一旦受到威胁，其连接的各类设备将会被攻击者全部攻破。

3) 交互逻辑漏洞是物联网系统中新出现的威胁类型。物联网系统的一个显著特点是其中功能实现过程涉及用户、云平台、设备三类实体的交互，同时云平台面向用户提供日益丰富的自动控制服务，各类服务在同一个应用场景下也会存在交互。这些交互在实现之初难以准确判定其中是否存在设计缺陷，甚至导致安全隐患[13-14,18-20]。随着物联网系统应用功能不断提升，交互类型不断复杂化，交互过程中的逻辑漏洞是值得深入研究的方向。

4) 设备固件漏洞仍然是设备遭受威胁的主要因素。由于物联网设备的数量庞大，固件漏洞被利用后可以快速传播，造成更大规模的威胁[3, 48]。随着设备硬件性能不断提升，固件包含的功能愈加丰富，内存漏洞的影响仍然是设备面临的主要安全威胁[34-35, 37-39]。但是与内存漏洞相比，逻辑漏洞更难发现，而且攻击者利用逻辑漏洞可以实现更加隐秘却更具危害的威胁[40]，因此如何进一步提升逻辑漏洞检测能力是值得后续研究的方向。

5) 针对语音设备的攻击是物联网系统特有的威胁类型。基于语音信道的控制方式极大地提升了用户访问设备的效率，然而语音信道也引入了新的攻击，一方面是基于语音平台的恶意应用[16-17]，另一方面是利用语音信号的敏感性实施的隐藏语音信号攻击[42-44]，由于语音助手设备在应用场景中的核心地位，基于语音控制的功能越来越丰富，针对这类威胁的研究仍然是研究人员关注的重点。

由此可见，当前物联网系统面临的威胁类型种类繁多，且与物联网特性紧密相关，对这些新型威胁进行检测和防御是未来研究的必然趋势。

3.2 威胁检测

针对物联网应用场景中不同类型的安全威胁，部分研究提出了针对性的检测方案。本文对检测的定义是及时发现物联网系统中潜在或已出现的攻击，在危害产生或扩大之前进行分析或处理。本节根据检测面向的威胁类型和技术原理，将检测方案分为 6 种不同的类型，其对比如表 3 所示。

3.2.1 云平台恶意应用检测

检测云平台应用的主要思想是提供一种独立于平台审核机制的方法，判断发布在市场中的应用是否

表 3 威胁检测方案对比

检测方案	面向威胁类型	主要技术原理	主要优点	主要缺点	文献	文献数量/篇
云平台恶意应用检测	云平台恶意应用	基于敏感信息的数据流追踪，语音黑盒测试	自动化、大规模检测，有效识别恶意应用	依赖平台特性	文献[4,12, 15-16, 52-54]	7
云平台实体和应用交互漏洞检测	云平台实体和应用交互漏洞	模型检测	识别实体交互复杂过程中的逻辑漏洞	需要人工分析，且对交互解析的方法存在局限性	文献[13-14, 18-20, 55]	6
基于静态分析的固件漏洞检测	设备固件漏洞、基于物联网设备的僵尸网络	符号执行，污点分析，二进制相似性比较	自动化检测固件漏洞	对编译优化和混淆敏感，固件难以获取和自动加载	文献[39-40,42, 56-60]	8
基于动态分析的固件漏洞检测	设备固件漏洞、基于物联网设备的僵尸网络	基于 QEMU（quick Emulator）仿真，推断外设输入	动态调试、准确识别漏洞原因和位置	需要人工分析，面向有限固件类型，仿真效果受限	文献[40, 61-68]	9
基于手机 App 的固件漏洞检测	设备固件漏洞	基于 App 的模糊测试，App 代码相似性分析	不用分析设备和解析固件	需要设备拥有对应 App，App 与设备较强的关联性	文献[69-72]	4
基于侧信道的设备异常检测	设备固件漏洞、基于物联网设备的僵尸网络	基于流量特征，基于物理特征，环境上下文特征	识别设备异常行为、非侵入式方案	容易受到信号强弱、协议类型和通信模式的影响，对设备环境有要求	文献[73-80]	8

会出现有威胁的运行状态，或者出现功能声明之外的运行结果，从而判定该应用是否具有“恶意”性质。

首先，对于 SmartThings 和 IFTTT 平台来说，其中恶意应用或服务引发的典型后果之一是隐私信息泄露，而且这 2 种平台都可以获得应用代码或 API 权限，因此对这 2 种平台可以采用基于数据流分析的检测方案，即追踪敏感数据在应用中的传递过程来识别应用是否将携带敏感信息的数据在未经用户授权的情况下发送给外部不可信的目标[12,15,52-53]。例如，在 SmartThings 平台中，Celik 等[12]在应用中自动定位从产生敏感数据的函数到网络接口函数的数据流，识别应用是否将敏感数据通过网络向外发送。在 IFTTT 平台中，Bastys 等[15]对每个应用的 Trigger 和 Action 打上敏感标签，然后检查每个 Applet 的 Trigger-Action 序列是否违背隐私约束规则。

其次，对于语音平台，由于无法获取 Skill 功能的实现细节，因此当前研究主要采用黑盒测试方案，即通过构造不同形式的 Skill 语音命令输入，来检查执行结果是否产生偏离正常功能的行为。这种方案面临的首要挑战是如何自动构造语音命令输入，Zhang 等[16]通过将 Skill 名称转换为语音表达形式，然后对比不同 Skill 的名称是否具有相似的发音形式来查找可能引起语音劫持攻击的恶意 Skill；Guo 等[4]进一步提出了一种基于语法和语义理解技术，可以自动与平台进行语音交互。此外，对于平台返回的命令执行结果，Guo 等[4]的方案是基于安全策略检测其中是否包含侵犯用户隐私的行为；Zhang 等[54]设计了一种针对语音识别系统中的 NLU（natural language understanding）模块的检测方案，可以发现具有不良意图的 Skill 命令。

3.2.2　云平台实体和应用交互漏洞检测

当前研究中对交互漏洞的检测大多基于模型检测的方法，主要思想是先对实体或应用的交互过程建模，然后将正常模型和实际运行状态进行对比，检测其中出现的异常。

首先是对实体交互漏洞的检测，采用的模型主要是有限状态机，主要通过逆向分析实体的交互过程得到各实体状态的正常转换流程，及其组合而成的三元组状态集合，由此构成了实体的正常交互模型。由于攻击将导致实体出现异常状态转换，或出现异常的三元组集合，因此可根据标准交互模型与实体的实时状态进行对比来检测是否出现异常的交互。Zhou 等[18]和 Chen 等[19]采用了上述的思路，通过对多家全球知名物联网云平台的三方交互过程建立实体交互模型和检测，最终在多家平台中验证了漏洞的存在，该漏洞可影响上亿台设备。

其次是对应用或服务交互漏洞的检测，由于云平台应用具有不同的实现方式，所以建立的模型也有不同的特点，表 4 对部分方案的建模方式和检测效果等进行了对比。

3.2.3　基于静态分析的固件漏洞检测

固件静态分析是指不运行固件程序，通过符号执行、污点分析等技术分析二进制文件的代码结构或逻辑关系，检测其中存在的内存漏洞或逻辑漏洞。

符号执行是固件分析中常用的技术[56-57]，核心思想是将程序输入变成符号，程序执行结束后可以得到与每条执行路径对应的符号表达式和约束条件，对约束条件进行求解即可得到满足路径需求的输入值。例如，Subramanyan 等[56]采用了一种专门的形式来描述固件中关于机密性和完整性的信息流属性，然后通过符号执行检查固件中的执行路径是否违背了属性的安全约定。污点分析的主要思想是在程序中建立数据依赖关系图，通过污点传播算法追踪从敏感数据源到数据聚集点的路径，并检测

表 4　　**应用或服务交互漏洞检测方案对比**

文献	建模方式和检测方法	检测平台	检测效果
文献[13]	通过解析源代码得到多个应用状态转换模型组合，基于安全策略检测动作冲突	SmartThings	在 28 种 SmartApp 组合中识别出 3 种组合违背 11 项安全策略
文献[14]	通过代码插桩在运行过程中动态建立多个应用状态转换模型，基于安全策略检测动作冲突	SmartThings、IFTTT	在 16 个 SmartApp 和 9 个 Applet 的组合中识别出 3 种组合违背 9 项安全策略
文献[20]	基于自然语言处理建立自动执行规则之间的交互模型，基于 SMT 求解技术检测规则间漏洞	IFTTT	在 31.5 万个 Applet 应用中，根据安装数量组成可信的规则集，发现规则集中 66%具有交互漏洞
文献[55]	通过解析应用源代码和文本描述，建立应用之间通过共同物理信道连接的动作模型，基于不同物理信道的风险值计算应用组合风险	SmartThings	在 185 个 SmartApp 中发现 162 种基于共同物理信道的隐式关联，其中 37 种关联可能产生安全隐患

路径中是否存在安全问题[39-40,58]。例如，Karonte[39]基于二进制文件之间交互通常通过一组有限的进程间通信模式集合进行的思想，通过追踪进程间通信的数据传播过程实现了跨文件的污点分析。基于二进制相似性检测的思想是提取已知漏洞在二进制文件中的特征，然后在新的二进制文件中进行匹配查找以定位漏洞[35,59-60]。例如，Feng 等[60]借鉴了计算机视觉技术对图像处理的思路，将提取到的程序控制流图转换为数字特征向量，从而大大降低了特征维度，提高了匹配算法的效率。

3.2.4 基于动态分析的固件漏洞检测

固件动态分析通过获取程序运行的实时状态可以更加准确地发现漏洞，当前研究大多通过将固件程序加载到 QEMU 等仿真软件中，在脱离硬件的情况下模拟固件的功能运行，再结合模糊测试等技术检测漏洞。

这种方法对基于 Linux 内核且具有完整操作系统功能的固件类型进行仿真运行的成功率较高。例如，FIRMADYNE[61]和 FIRM-AFL[62]可以对大部分基于 Linux 内核的固件进行全系统仿真运行。但是对于其他基于实时操作系统的固件，或没有操作系统的“裸机”固件（即应用程序直接与硬件交互而不需要中间的操作系统）来说，这种方案难以应用。主要原因是：这种固件没有统一的文件格式导致难以加载，部分固件被加密导致难以提取核心代码，各种硬件组件和外设的输入输出信息难以获取。

基于以上挑战，部分研究实现了固件部分仿真[40,63-64]，主要思想是从固件中分离出与检测目标相关的代码执行路径，只对这部分路径进行仿真执行。例如，FIoT[63]从容易触发内存越界访问的汇聚点函数出发，采用反向程序切片方法得到从数据输入源到达汇聚点函数的路径，结合符号执行和模糊测试检测该路径执行过程中是否存在内存漏洞。

部分研究克服了设备硬件与固件的耦合性和底层架构的差异性等困难，实现了固件全仿真[65-68]。例如，uEmu[68]通过基于符号执行的路径约束和程序动态运行状态来推断固件运行过程中期望的输入并形成外设反馈知识库，借助此知识库可动态引导程序执行过程，以此实现不需要先验知识和原始硬件环境，即可对固件程序进行全系统仿真。

3.2.5 基于手机 App 的固件漏洞检测

部分物联网厂商向用户提供了手机 App 作为设备控制终端，App 中包含了与设备通信和功能相关的逻辑和数据。利用这种 App 与设备之间的关联性，部分研究人员在不分析设备和固件的前提下，通过手机 App 来检测固件中的漏洞。

由于现阶段实现物联网设备全系统仿真较困难并且难以直接从设备端定位数据输入，IoTFuzzer[69]和 DIANE[70]转换思路，将 App 看作设备的输入接口，将发向设备的请求参数看作可变异的种子数据，首先在 App 中自动定位参数的数据源或处理函数；然后对参数值进行变异，通过 App 的原始业务逻辑将变异数据发向设备；最后动态观察真实设备的崩溃信息，以快速检测固件中的内存漏洞。Zuo 等[71]发现从 App 中可以提取设备 UUID（universally unique identifier）信息，该信息可在蓝牙广播中识别设备，同时从 App 中可以发现当前采用的蓝牙认证模式是否存在缺陷，攻击者结合以上条件可以通过分析 App 对周围的蓝牙设备发起攻击。此外，设备厂商往往会复用相同的开发组件，因此组件中的漏洞将出现在不同的设备中，而这种相似性甚至会通过 App 表现出来，因此通过比较不同设备在 App 上的相似性就可以检测设备是否存在漏洞[72]。

3.2.6 基于侧信道的设备异常检测

受到攻击的设备除了内部功能受到影响之外，其外在的各类侧信道特征也会表现出异常，因此可以利用此特点进行设备的异常检测。

首先，设备与网络交互过程中产生的流量可以反映设备内部的行为，所以可以通过提取流量特征来检测设备的状态。一方面，可以提取流量中未加密的头部信息识别异常设备[73-75]。例如，Yu 等[74]基于设备通信中常见的广播和多播协议，将协议特征看作设备整体特征的一种视图，然后基于多视图学习算法进行设备签名，可以在具有大量设备的复杂环境中准确识别异常或伪造的设备。另一方面，可以提取加密流量的统计特征，如数据包长度、时间戳等。Zhang 等[75]利用 ZigBee 和 Z-Wave 协议的流量特征设计了识别 SmartThings 平台设备行为系统，可以通过流量判断设备是否出现异常行为。

其次，设备工作过程中表现出的外在物理特征，如电量、电压、速度、重力、方向等，也可以反映设备的运行状态，部分研究基于物理特征实现设备异常检测[76-78]。例如，Choi 等[78]对无人机和地面探测器提取控制时的设备参数、物理运动数值、

底层控制算法等数据作为正常运行标准，任何偏离标准的微小偏差都被视为异常，以此检测来自物理或网络的攻击。

此外，有部分研究基于邻近的设备或传感器对于活动发生时的物理环境感知应具有上下文一致性这一特点，将邻近设备的状态和动作数据作为特征进行恶意行为识别[79-80]。例如，Birnbach 等[79]基于智能家居环境中多个传感器对同一事件的感知数据集合作为签名，可以检测出由于传感器故障或攻击者造成的欺骗事件。

3.2.7　威胁检测小结

下面对 3.2 节中关于威胁检测研究的特点和不足进行总结，主要分为以下几个方面。

1) 云平台恶意应用检测方案存在局限性。不难看出，大部分恶意应用检测[12,15,52-53]都面向 SmartThings 和 IFTTT 这 2 个平台。这些方案虽然获得了较好的识别效果，但是实现方案显然都要基于平台应用开发语言的特性，在其他不开放应用逻辑的云平台中难以适用。与之相对的是 FlowFence[81]，该方案与具体平台特性无关，通过在平台中预先建立沙箱隔离所有敏感操作，平台应用必须通过沙箱定义的接口才能访问敏感数据，以此隔离应用中所有可能产生隐私泄露的行为，但是该方案的应用需要高度定制化的系统支持。

2) 交互逻辑漏洞的检测仍然面临挑战。对三类实体交互漏洞检测的研究[18-19]探索了面向“黑盒”平台进行漏洞检测的方案，取得了较好的检测效果，但是不难看出，其中的建模过程需要大量人工分析，而且当前云平台对通信过程的保密机制越来越严格，例如，双向证书验证机制对研究中采用的解密通信方法带来了极大挑战，因此建立有效的交互过程建模方案是值得探索的方向。

3) 固件分析面临的共同问题是如何获取固件和加载固件。现有研究中提出了可以通过网站下载、截获 OTA（over the air）更新、从 App 提取、从设备硬件调试接口提取等方式获取固件，但是目前大多数物联网厂商对固件的保护越来越严格，不提供公开下载链接，或者消除了硬件调试接口，或者对更新的固件进行加密，因此可以获取固件的方式越来越少。对于固件加载，部分研究通过人工分析建立固件格式的数据库，但是此方法难以大规模扩展，而 Wen 等[82]提出了一种通过绝对指针自动定位固件基址的方案，可以有效提高加载效率，但是该方案的加载成功率也会受到绝对指针数量不足的影响。

4) 3 种固件漏洞检测方案（静态、动态、App）在真实设备固件检测中各有不足。首先，静态分析中常用的符号执行和污点分析技术分别面临路径爆炸和过污染的挑战，因此在实际应用中需要在使用这些技术前针对分析目标缩减问题的求解空间[56-58]。对基于二进制相似性比较的漏洞检测方法来说，二进制特征的提取严重依赖于构建代码的编译环境[59-60]，编译器中不同的优化和混淆措施会对生成的二进制代码产生影响，从而降低识别的准确率。其次，在动态分析中，固件的仿真效果受限于如何处理各种不同类型的硬件组件属性，以及如何兼容不同的底层架构[65-68]。再次，基于 App 的固件漏洞检测[69-70]要求设备必须具有对应的 App 控制端，App 与设备的功能实现具有密切关系，而且此种方案对种子数据的生成和变异完全依赖于 App 的内部逻辑，因此只能发现固件是否存在会引发系统崩溃的漏洞，对于漏洞的具体原因和位置还需要人工验证。

5) 基于侧信道特征的检测方案的最大优点是可以通过外部手段发现设备异常，但其检测效果受限于应用场景中的特征选择和采用的学习算法，例如，流量特征容易受到信号强弱[74]、协议类型和通信模式的影响[75]，物理特征严重受限于物理环境因素[76-77]，而上下文特征的提取则要求检测目标周围必须存在能够提供丰富特征的其他设备[79]。

3.3　威胁防御

针对物联网应用场景中不同类型的安全威胁，部分研究提出了针对性的防御方案，本文对防御的定义是在威胁出现前就实施阻止措施，直接避免危害产生。本节根据防御面向的威胁类型和技术原理，将威胁防御方案分为 5 种不同的类型，其对比如表 5 所示。

3.3.1　细粒度的云平台访问控制

物联网云平台访问控制问题产生的原因主要是云平台实现功能时未能遵循最小权限原则，因此当前研究利用云平台的特性设计了细粒度的访问控制机制。

对于 SmartThings 平台，当前研究从 SmartApp 中提取应用运行过程中实时的上下文，为当前操作是否符合访问控制策略提供细粒度的参考信息。例如，ContextIoT[83]通过提取 SmartApp 内部的执行路

表 5 不同威胁防御方案对比

防御方案	面向威胁类型	主要技术原理	主要优点	主要缺点	文献	文献数量/篇
细粒度的云平台访问控制	云平台访问控制缺陷	提升权限管理粒度	有效识别越权操作，弥补平台审核机制不足	依赖平台特性，需要用户参与	文献[10, 83-87]	6
安全的通信协议	通信协议漏洞	增加内在安全机制，设计新型配对协议	增强协议机密性和完整性	安全配对协议需要感知装置支持，邻近设备不完全可信	文献[21, 88-94]	8
流量特征隐藏	通信流量侧信道信息泄露	数据包封装，流量塑形	有效对抗侧信道信息泄露	增加通信时延和负载，增加流量噪声	文献[30, 32-33, 75, 95-96]	6
基于可信计算的固件安全防护机制	设备固件漏洞、基于物联网设备的僵尸网络	程序组件权限和内存地址空间隔离，控制流完整性保护，远程认证	有效防御传统固件漏洞，大规模管理中有效发现异常设备，设备自组网络安全运行	性能和适用面需要进一步提升，细粒度的控制流认证影响系统实时性	文献[34, 37-38, 97-101]	8
语音攻击防御	基于语音信道的攻击	安全提示和语音确认，声纹识别，信号过滤	有效阻止藏匿的恶意语音命令	面临可用性和成本的额外开销	文献[42-45, 102]	5

径、数据依赖关系、实时变量值、环境参数等信息来表示应用执行操作时的上下文信息，然后在操作执行前主动征求用户授权许可，只有获得用户授权的操作才可以继续执行。SmartAuth[84]通过自然语言处理技术提取 SmartApp 对功能的文本说明中关于操作的信息，再通过污点分析技术在应用运行时获取真实操作，对比真实操作与文本说明是否一致，若不一致则主动通知用户以征求授权。这 2 种方案在实际应用中都可以准确防止恶意应用产生的隐私泄露，但是也不可避免地增加了用户操作。

对于 IFTTT 中基于访问令牌联动的服务规则，Fernandes 等[10]针对令牌管理模式中存在的问题提出了一种权限管理的优化方案，该方案引入应用代理方，并使用权限粒度更小的“规则令牌”将集中式的权限管理模式分散为以应用代理为单位的分布式管理，可以有效解决集中式管理和粗粒度令牌的问题。

此外，还有部分研究面向物联网中特殊应用场景，基于其他领域的理论，如 SDN（software defined network）、智能手机访问控制等，提出了新的访问控制模型[85-87]，但其实现需要特殊架构支持。

3.3.2 安全的通信协议

为了保障物联网系统通信安全，在物联网常用协议中需要增加稳健的安全机制，然而协议的制定和改进是多方参与且长期演进的过程，因此更重要的是协议应用方必须在业务逻辑中对通信实体的身份和权限实施严格检查。例如，针对 MQTT 协议模型中缺失的安全属性，应增加通信会话的管理机制、面向消息的访问控制机制，以及限制通配符的功能范围[21]；针对 ZigBee 协议的内在缺陷，应增强设备在加入网络和正常通信这 2 个阶段的加密级别[88]。此外，也有部分研究基于物联网系统特性设计了安全的通信协议[89-90]。例如，Alshahrani 等[89]提出了一种基于 ZigBee 通信的设备间进行互相认证和密钥交换的模型，可以增强 ZigBee 协议在对抗性环境中应用时的稳健性。

还有部分研究面向设备近距离通信设计了新型的安全配对协议[91-94]，可以克服传统配对协议存在密钥信息易被窃取、需要人工参与等问题。例如，Han 等[92]基于邻近的智能设备在相同时间周期内对物理活动的感知具有一致性这一特征，利用相同时间周期内的物理感知参数来生成对称密钥，可有效对抗设备伪装和中间人攻击。Jin 等[93]利用射频信号噪声在不同介质（如人体表面和空气）中传播时产生的信号特征具有高度随机性和不可预测性的特点，设计了针对可穿戴设备的新型配对方案。

3.3.3 流量特征隐藏

为了应对形式多样的通信流量侧信道分析，部分研究关注如何隐藏流量特征。流量特征推理主要是提取流量中的头部特征和统计特征，所以对应的防御方案是消除这 2 种特征与设备和活动的对应关系。

对于头部特征，主要目标是在不影响流量转发和不改变负载数据的基础上进行头部信息的再次封装，令攻击者无法获得有意义的头部信息。例如，通过 DNS 加密技术阻止对网络请求目标的分析[30]；通过隧道转发技术将设备与云服务之间的通信转换为 VPN 节点之间的通信，间接阻止了对设备的识别和行为推理[33,75]。对于统计特征，主要目标是在不破坏正常功能的前提下，改变流量的整体特

表 6　　固件安全防护机制对比

文献	技术原理	主要特点	性能开销
文献[34]	组件权限和内存地址空间隔离	识别与分离特权指令，实现栈保护、代码和数据区域隔离，无法实现进程级别的代码隔离	平均增加 1.8%执行时间和 0.5%能耗
文献[97]	组件权限和内存地址空间隔离	基于 MPU 实现进程内存空间的隔离，但是划分进程内数据与代码区域的方法不灵活	最高可减少 93%进程内存空间
文献[98]	组件权限和内存地址空间隔离	对固件执行单元进行更细粒度的权限划分，基于定制的安全策略对分离的组件灵活实施最小权限模型	最高引入 13%的运行开销，比现有技术减少 59%的 Flash 占用，减少 84%的内存占用
文献[37]	控制流完整性保护	将函数的有效返回地址集合放到不可写的内存区域中，不需要特殊硬件模块支持	平均运行开销只有 0.1%，内存开销可忽略，平均增加 54.1%的 Flash 占用
文献[38]	控制流完整性保护	基于“影子栈”技术，配置内存保护单元来实施内存访问规则，确保程序返回到合法目标地址	平均增加 1.3%和 3.4%的性能开销，以及 8.9%和 2.3%的代码体积

征。例如，在正常通信过程中注入欺骗流量妨碍窃听者对真实设备和活动的识别[32]；或采用流量塑形技术，通过增加发送时延或注入无关流量来降低或提高单位时间内的通信速率，改变流量传输曲线的形状，以混淆攻击者对行为的提取[32,95-96]。

3.3.4　基于可信计算的固件安全防护机制

物联网设备内在的软硬件资源受限是导致固件漏洞的主要原因之一，因此部分研究关注如何基于有限条件构建可信的固件运行环境。

首先，考虑将传统安全机制应用于固件程序，增强固件本身的防护性能。一方面，对固件程序组件权限和内存地址空间实行分离机制。针对物联网设备的实时操作系统或“裸机”系统中没有内存或数据隔离的缺点，部分研究将固件划分为不同组件以实施最小权限隔离，如 EPOXY[34]、MINION[97]、ACES（automatic compartments for embedded system）[98]等。另一方面，对固件程序实施控制流完整性保护，确保函数返回地址完整性，以应对控制流劫持攻击，如 μRAI[37]、Silhouette[38]等。表 6 对几种固件安全防护机制的特点和性能进行了对比。

其次，远程证明是对远程设备执行状态的可信性进行认证的关键技术，其主要思想是可信的远程校验方通过获取本地证明方的状态信息，来检查证明方当前是否处于可信状态。在物联网系统中，远程认证的主要目标是设备需要提供高时效且细粒度的可认证信息[99-101]。例如，C-FLAT（control-flow attestation）[99]将证明方的信息细化到程序的控制流层面上，向校验方提供细粒度的程序执行路径信息以判断程序控制流完整性是否被破坏。DIAT（data integrity attestation）[101]设计了面向自动协作网络（如无人机集群）的认证方案，将软件分解为不同模块，证明方发送数据时还需发送数据在模块中的生成和处理过程信息，校验方以此检测数据的正确性。

3.3.5　语音攻击防御

针对隐藏在语音信道的各种媒介中，且用户无法察觉的恶意语音攻击样本，部分研究提出了对应的防御方案，本节分析了这些方案的原理和不足。

1) 在语音设备的交互过程中增加基于安全提示和语音确认的交互模式，用户需要对敏感操作进行主动确认来提高安全性[42]，但是这种方法会带来额外的可用性开销，且确认操作容易被用户忽略。2) 通过添加专用硬件模块对具有特殊信号特征的语音信号（如高频超声波）进行过滤[43]，或者物理隔断语音设备与桌面等硬件媒介的直接接触[45]，但是前者需要特殊硬件支持，后者为语音设备的可用性增加了负担。3) 通过增加噪声干扰或降低输入音频的采样频率，影响语音识别系统对恶意命令的识别率[44]，但是这种方案也会影响正常语音的识别率。4) 通过机器学习算法实现声纹识别区分人类和机器生成的语音[42-43,45]，但是这将使语音识别系统产生额外运行开销。

另外，由于人工生成的语音命令缺少了人类在现场说话引起的无线信号干扰，因此可以利用这个特征来区分隐藏语音命令。例如，Meng 等[102]利用人类发音时引起的 Wi-Fi 信道状态信息变化模式和语音信号的关联，可以准确区分生成的恶意语音信号与真实人声。但是该方案目前依赖 Wi-Fi 信号覆盖度较强的环境，且识别过程对信号波动强度敏感，如果发音者距离信号接收天线过远则会由于捕捉不到信号扰动而无法进行识别。

3.3.6　威胁防御小结

下面对 3.3 节中关于威胁防御研究的特点和不

足进行总结，主要分为以下几个方面。

1) 云平台访问控制的适用面有限。相较于传统的云服务，在物联网云平台中，用户访问设备的过程具有更加复杂的关系，例如，多个用户可以对同一个设备进行共享或交互，因此需要精准且高效的访问控制机制。当前研究提出的新型访问控制方案虽然解决了已知的授权管理问题[10,83-84]，但目前只能面向有限云平台。值得一提的是，Shezan 等[103]基于迁移学习思想提出了一种可在不同平台之间进行权限知识迁移的权限管理模型，在建立新平台的权限模型时，可以直接采用来自其他平台的权限管理规则。

2) 保障通信协议安全仍面临困难。一方面，在物联网系统这种存在对抗性的环境中建立安全且适配的通信协议是一个需要多方参与且长期演进的过程，此过程中更重要的是协议应用方应根据应用场景在业务逻辑中增加协议当前不具备的安全机制，以保障通信安全。另一方面，当前提出的设备安全配对协议均建立在“物理邻近即安全”的假设之上[91-93]，而物联网中复杂的设备应用环境是对这个假设的最大挑战，由于邻近的设备也可能是伪装的恶意设备，因此对设备的认证是配对协议需要重点考虑的问题。

3) 固件的安全防护机制需要进一步提升。设备固件受限于物联网设备有限资源的特性而无法直接应用传统的软件安全保护机制，因此现有研究[37-38,98]通过一些硬件辅助方案（如 MPU 或者最新的 ARMv8 TrustZone）来实现特殊的系统防御，如数据执行保护、控制流完整性保护等措施。但一方面这些硬件组件在现有设备上不一定存在，另一方面在现有的程序中配置和使用这些方案也需要投入过高的人工成本，此外，可能引入过多的功耗和时延，而物联网设备往往对功耗和时延有着更高的要求，因此这些方案的性能和适用面也需要进一步提升。

4) 面向语音攻击的防御措施不够完善。现有的语音攻击防御方案虽然在实际研究中被证明有效[42-45]，但是不难看出各方案在实现时都面临可用性和设备性能的额外开销。综合来看，目前对于藏匿在语音信道中的恶意命令没有完善的防御方法，这也使面向语音攻击的防御成为后续研究的热点。

4 挑战与机遇

本节基于第 3 节中对安全威胁，以及检测和防御方案的分析，提出当前面临的研究挑战和未来研究机遇。图 4 中展示了挑战和机遇的对应关系。

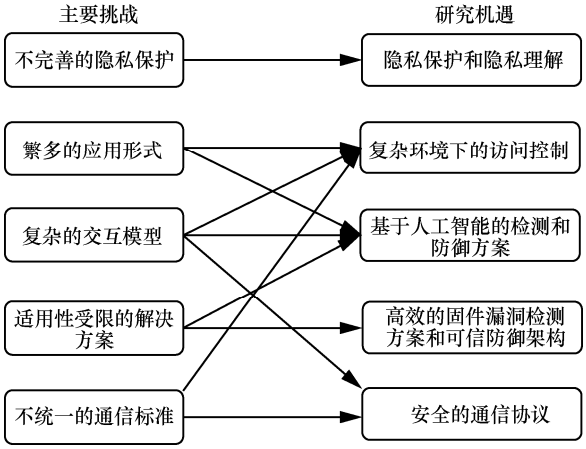


图 4 挑战与机遇的对应关系

4.1 当前面临的主要挑战

4.1.1 不完善的隐私保护

物联网设备与人类生活密切相关，通过设备感知的信息可以推断出人的生活习惯、行为特征等，而当前在物联网系统中存在的各类攻击可能导致设备收集的信息被窃取。从表 1 可以看出，当前物联网系统中的大部分威胁都会导致隐私泄露的危害。此外，导致隐私保护不够完善的另一个重要因素是隐私信息理解问题[104]，即用户使用设备前对设备的隐私收集和使用方式不能充分了解，或者现行的隐私信息保护法案不能完全满足真实的使用需求。

4.1.2 繁多的应用形式

云平台提供的应用或服务不仅数量庞大而且种类繁多，然而当前的云平台安全审核机制难以满足安全需求。现有研究充分证明，厂商在发展新应用和维护其安全性之间存在不平衡，依靠静态分析应用的方式难以发现其中的动态特性导致的问题，而动态分析应用安全的方案匮乏，人工审核方式有一定效果，但是耗时耗力且容易出现疏漏。随着物联网应用层生态的不断发展，在发布大量应用的同时，需要高效、准确、自动化的应用安全审核机制。

4.1.3 复杂的交互模型

物联网系统功能提升的同时，系统内的交互形式也不断增多，交互过程日益复杂，不仅有应用之间的交互、设备之间的交互，更有跨平台的交互，所以对平台或设备安全性的保护不能只限于单个实体，还要考虑交互过程可能引入的风险，典型的问题是即使实体单独运行过程中的安全性得到保

障，然而在与其他实体的交互过程中原有的保护机制很可能被打破。当前检测和防御方案大多通过交互行为建模来检测其中的威胁，但是由于交互模式的差异，各类模型方案只能应用于特定平台或场景，彼此之间难以复用。

4.1.4 适用性受限的解决方案

当前研究提出的威胁检测和防御方案大多针对特定的应用类型和场景，或者特定的设备结构和系统。在云平台中，恶意应用和交互逻辑漏洞检测的大部分方案基于特定平台的开发特性建立分析框架；在设备固件分析中，固件运行依赖的底层架构和底层硬件多种多样，所以只能针对特定类型的固件进行仿真。这些特点使当前研究得到的分析方案只能应用在特定的领域中，组件之间无法移植或组合，在出现新的问题时难以达到预期的效果。

4.1.5 不统一的通信标准

物联网系统的通信具有网络类型多且结构差异大的特点，由于通信过程缺乏统一的协议或授权标准，各类网络的安全约束参差不齐。同时，物联网设备有限的资源和对实时性的要求令其更适配计算量低且逻辑简单的轻量级通信协议，而当前被广泛使用的各种轻量级协议一般缺乏内建的安全机制，设备厂商应用协议时容易忽略对安全机制的实现，导致引入安全威胁。

4.2 未来研究机遇

4.2.1 隐私保护和隐私理解

在物联网发展的过程中，隐私安全问题一直是研究关注的重点。一方面是物联网应用场景中隐私信息泄露的检测和保护措施[105-106]；另一方面是对隐私理解问题的研究，如调研用户对隐私政策的使用和理解现状[107]，或当前物联网生态中的各参与方对隐私保护措施的合理性[108]，以推动物联网系统中隐私保护机制的发展。

4.2.2 复杂环境下的访问控制

物联网系统的应用环境复杂，身份认证和授权管理缺陷导致的安全漏洞体现在多个方面，当前研究提出的访问控制增强方案存在不足。因此，设计既满足物联网系统的安全需求，又能够适应物联网的低能耗和高实时性要求，同时还具有扩展性的访问控制机制是物联网未来进一步发展的实际需要。

4.2.3 基于人工智能的检测和防御方案

人工智能技术可以对设备收集的信息进行深度学习和理解，在一定程度上可以弥补现有的检测和防御技术在自动化方面的不足。例如，结合深度学习与模糊测试自动进行恶意应用检测[4]或漏洞挖掘[109]，借鉴迁移学习思想融合不同平台的检测知识[103,110]。随着物联网应用类型不断丰富，以及交互场景越来越复杂，利用人工智能技术提升威胁检测和防御方案的效果是值得继续深入研究的方向。

4.2.4 高效的固件漏洞检测方案和可信防御架构

由于设备固件中普遍存在安全漏洞，需要更加有效的方法进行检测以避免威胁在使用过程中进一步扩大。例如，在固件动态分析方面，如何实现更全面的模拟，以及与其他工具结合检测固件漏洞，仍需要更深入的研究。另外，由于设备自身硬件和软件条件的受限，大多数传统安全机制不能直接应用，如何克服这种限制在固件中实施更可信的防御架构也是需要研究的问题。

4.2.5 安全的通信协议

通信协议是物联网传输层的核心。一方面由于当前厂商在应用缺乏内建安全机制的轻量级协议时容易忽略对安全因素的考虑，因此需要高效自动的协议安全分析方案；另一方面可利用物联网区别于其他系统的特性，如三类实体交互、设备邻近等，结合应用场景设计专属物联网的安全通信协议。

5 结束语

物联网系统由于应用种类多、设备规模大、交互过程复杂等特性在发展过程中不可避免地面临各类安全威胁，对威胁的检测和防御是促进物联网正常发展的关键。本文系统整理了近 5 年物联网安全研究中的代表性工作，从“威胁、检测、防御”的角度分别阐述其中的主要类型，并以此为基础分析了当前面临的挑战，以及提出未来研究机遇。随着物联网技术不断发展，相关的安全研究也必将不断深入，成为物联网发展的重要支柱。

参考文献：

[1] ZHOU W, JIA Y, PENG A N, et al. The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved[J]. IEEE Internet of Things Journal, 2019, 6(2): 1606-1616.

[2] ALRAWI O, LEVER C, ANTONAKAKIS M, et al. SoK: security evaluation of home-based IoT deployments[C]//2019 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 1362-1380.

[3] ANTONAKAKIS M, APRIL T, BAILEY M, et al. Understanding the Mirai botnet[C]//USENIX Security Symposium. Berkeley: USENIX

Association, 2017: 1093-1110.

[4] GUO Z, LIN Z, LI P, et al. SkillExplorer: understanding the behavior of skills in large scale[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 2649-2666.

[5] 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.
ZHANG Y Q, ZHOU W, PENG A N. Survey of Internet of things security[J]. Journal of Computer Research and Development, 2017, 54(10): 2130-2143.

[6] 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.
PENG A N, ZHOU W, JIA Y, et al. Survey of the Internet of things operating system security[J]. Journal on Communications, 2018, 39(3): 22-34.

[7] 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.
WANG J C, LI Y L, JIA Y, et al. Survey of smart home security[J]. Journal of Computer Research and Development, 2018, 55(10): 2111-2124.

[8] HE W, GOLLA M, PADHI R, et al. Rethinking access control and authentication for the home Internet of things (IoT)[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 255-272.

[9] FERNANDES E, JUNG J, PRAKASH A. Security analysis of emerging smart home applications[C]//2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 636-654.

[10] FERNANDES E, RAHMATI A, JUNG J, et al. Decentralized action integrity for trigger-action IoT platforms[C]//Proceedings 2018 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2018: 1-16.

[11] YUAN B, JIA Y, XING L, et al. Shattered chain of trust: understanding security risks in cross-cloud IoT access delegation[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 1183-1200.

[12] CELIK Z B, BABUN L, SIKDER A K, et al. Sensitive information tracking in commodity IoT[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 1687-1704.

[13] CELIK Z B, MCDANIEL P, TAN G. Soteria: automated IoT safety and security analysis[C]//USENIX Annual Technical Conference. Berkeley: USENIX Association, 2018: 147-158.

[14] CELIK Z B, TAN G, MCDANIEL P. IoTGuard: dynamic enforcement of security and safety policy in commodity IoT[C]//Proceedings 2019 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2019: 1-15.

[15] BASTYS I, BALLIU M, SABELFELD A. If this then what?: controlling flows in IoT Apps[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1102-1119.

[16] ZHANG N, MI X H, FENG X, et al. Dangerous skills: understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems[C]//2019 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 1381-1396.

[17] KUMAR D, PACCAGNELLA R, MURLEY P, et al. Skill squatting attacks on Amazon Alexa[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 33-47.

[18] ZHOU W, JIA Y, YAO Y, et al. Discovering and understanding the security hazards in the Interactions between IoT devices, mobile APPs, and clouds on smart home platforms[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2019: 1133-1150.

[19] CHEN J Y, ZUO C S, DIAO W R, et al. Your IoTs are (not) mine: on the remote binding between IoT devices and users[C]//2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE Press, 2019: 222-233.

[20] WANG Q, DATTA P, YANG W, et al. Charting the attack surface of trigger-action IoT platforms[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1439-1453.

[21] JIA Y, XING L Y, MAO Y H, et al. Burglars' IoT paradise: understanding and mitigating security risks of general messaging protocols on IoT clouds[C]//2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 465-481.

[22] CAO X H, SHILA D M, CHENG Y, et al. Ghost-in-ZigBee: energy depletion attack on ZigBee-based wireless networks[J]. IEEE Internet of Things Journal, 2016, 3(5): 816-829.

[23] FAWAZ K, KIM K-H, SHIN K G. Protecting privacy of BLE device users[C]//SENIX Security Symposium. Berkeley: USENIX Association, 2016: 1205-1221.

[24] ANTONIOLI D, TIPPENHAUER N O, RASMUSSEN K. BIAS: bluetooth impersonation attacks[C]//2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 549-562.

[25] SETHI M, PELTONEN A, AURA T. Misbinding attacks on secure device pairing and bootstrapping[C]//Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. New York: ACM Press, 2019: 453-464.

[26] OCONNOR T J, ENCK W, REAVES B. Blinded and confused: uncovering systemic flaws in device telemetry for smart-home Internet of things[C]//Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2019: 140-150.

[27] WEN H, CHEN Q A, LIN Z. Plug-N-Pwned: comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 949-965.

[28] ZHU Y Z, XIAO Z J, CHEN Y X, et al. Et tu alexa? when commodity Wi-Fi devices turn into adversarial motion sensors[C]//Proceedings 2020 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2020: 1-15.

[29] LOPEZ-MARTIN M, CARRO B, SANCHEZ-ESGUEVILLAS A, et al. Network traffic classifier with convolutional and recurrent neural networks for Internet of things[J]. IEEE Access, 2017, 5: 18042-18050.

[30] SIVANATHAN A, GHARAKHEILI H H, LOI F, et al. Classifying IoT devices in smart environments using network traffic characteristics[J]. IEEE Transactions on Mobile Computing, 2019, 18(8): 1745-1759.

[31] WOOD D, APTHORPE N, FEAMSTER N. Cleartext data transmissions in consumer IoT medical devices[C]//Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. New York: ACM Press, 2017: 7-12.

[32] ACAR A, FEREIDOONI H, ABERA T, et al. Peek-a-Boo: I see your smart home activities, even encrypted![C]//Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2020:207-218.

[33] TRIMANANDA R, VARMARKEN J, MARKOPOULOU A, et al. packet-level signatures for smart home devices[C]//Proceedings 2020 Network and Distributed System Security Symposium. Virginia: the

Internet Society, 2020: 1-18.

[34] CLEMENTS A A, ALMAKHDHUB N S, SAAB K S, et al. Protecting bare-metal embedded systems with privilege overlays[C]//2017 IEEE Symposium on Security and Privacy. IEEE Press, 2017:289-303.

[35] PEWNY J, GARMANY B, GAWLIK R, et al. Cross-architecture bug search in binary executables[C]//2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016:709-724.

[36] QUARTA D, POGLIANI M, POLINO M, et al. An experimental security analysis of an industrial robot controller[C]//2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 268-286.

[37] ALMAKHDHUB N S, CLEMENTS A A, BAGCHI S, et al. μRAI: securing embedded systems with return address integrity[C]//Proceedings 2020 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2020: 1-18.

[38] ZHOU J, DU Y, SHEN Z, et al. Silhouette: efficient protected shadow stacks for embedded systems[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 1219-1236.

[39] REDINI N, MACHIRY A, WANG R, et al. Karonte: detecting insecure multi-binary interactions in embedded firmware[C]//2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020:1544-1561.

[40] YAO Y, ZHOU W, JIA Y, et al. Identifying privilege separation vulnerabilities in IoT firmware with symbolic execution[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2019: 638-657.

[41] MÜLLER J, MLADENOV V, SOMOROVSKY J, et al. SoK: exploiting network printers[C]//2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 213-230.

[42] CARLINI N, MISHRA P, VAIDYA T, et al. Hidden voice commands[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2016: 513-530.

[43] ZHANG G M, YAN C, JI X Y, et al. DolphinAttack: inaudible voice commands[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 103-117.

[44] YUAN X, CHEN Y, ZHAO Y, et al. Commandersong: a systematic approach for practical adversarial voice recognition[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 49-64.

[45] YAN Q B, LIU K H, ZHOU Q, et al. SurfingAttack: interactive hidden attack on voice assistants using ultrasonic guided waves[C]//Proceedings 2020 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2020: 1-18.

[46] ROY N, SHEN S, HASSANIEH H, et al. Inaudible voice commands: the long-range attack and defense[C]//USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2018: 547-560.

[47] CHEN T, SHANGGUAN L, LI Z J, et al. Metamorph: injecting inaudible commands into over-the-air voice controlled systems[C]//Proceedings 2020 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2020: 1-17.

[48] GRIFFIOEN H, DOERR C. Examining mirai's battle over the Internet of Things[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020.

[49] SOLTAN S, MITTAL P, POOR H V. BlackIoT: IoT botnet of high wattage devices can disrupt the power grid[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 15-32.

[50] HUANG B, CARDENAS A A, BALDICK R. Not everything is dark and gloomy: power grid protections against IoT demand attacks[C]//Proceedings of the 28th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2019: 1115-1132.

[51] RONEN E, SHAMIR A, WEINGARTEN A O, et al. IoT goes nuclear: creating a ZigBee chain reaction[C]//2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 195-212.

[52] WANG Q, HASSAN W U, BATES A, et al. Fear and logging in the Internet of things[C]//Proceedings 2018 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2018: 1-16.

[53] 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]//Proceedings of the 26th International Conference on World Wide Web. New York: ACM Press, 2017: 1501-1510.

[54] ZHANG Y Y, XU L, MENDOZA A, et al. Life after speech recognition: fuzzing semantic misinterpretation for voice assistant applications[C]//Proceedings 2019 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2019: 1-15.

[55] DING W B, HU H X. On the safety of IoT device physical interaction control[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 832-846.

[56] SUBRAMANYAN P, MALIK S, KHATTRI H, et al. Verifying information flow properties of firmware using symbolic execution[C]//Proceedings of the 2016 Design, Automation & Test in Europe Conference & Exhibition. Piscataway: IEEE Press, 2016: 337-342.

[57] HERNANDEZ G, FOWZE F, TIAN D, et al. Firmusb: vetting USB device firmware using domain informed symbolic execution[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 2245-2262.

[58] CHENG K, LI Q, WANG L, et al. DTaint: detecting the taint-style vulnerability in embedded device firmware[C]//2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE Press, 2018: 430-441.

[59] ESCHWEILER S, YAKDAN K, GERHARDS-PADILLA E. discovRE: efficient cross-architecture identification of bugs in binary code[C]//Proceedings 2016 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2016: 1-15.

[60] FENG Q, ZHOU R D, XU C C, et al. Scalable graph-based bug search for firmware images[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 480-491.

[61] CHEN D D, EGELE M, WOO M, et al. Towards automated dynamic analysis for linux-based embedded firmware[C]//Proceedings 2016 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2016: 1-16.

[62] ZHENG Y, DAVANIAN A, YIN H, et al. FIRM-AFL: high-throughput greybox fuzzing of IoT firmware via augmented process emulation[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2019: 1099-1114.

[63] ZHU L P, FU X T, YAO Y, et al. FIoT: detecting the memory corruption in lightweight IoT device firmware[C]//2019 18th IEEE International Conference On Trust, Security and Privacy in Computing and

Communications/13th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE Press, 2019: 248-255.

[64] MUENCH M, STIJOHANN J, KARGL F, et al. What you corrupt is not what you crash: challenges in fuzzing embedded devices[C]//Proceedings 2018 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2018: 1-15.

[65] CLEMENTS A A, GUSTAFSON E, SCHARNOWSKI T, et al. HALucinator: firmware re-hosting through abstraction layer emulation[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 1-18.

[66] FENG B, MERA A, LU L. P2IM: scalable and hardware-independent firmware testing via automatic peripheral interface modeling[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 1237-1254.

[67] CAO C, GUAN L, MING J, et al. Device-agnostic firmware execution is possible: a concolic execution approach for peripheral emulation[C]//Annual Computer Security Applications Conference. New York: ACM Press, 2020: 746-759.

[68] ZHOU W, GUAN L, LIU P, et al. Automatic firmware emulation through invalidity-guided knowledge inference[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2021: 1-19.

[69] CHEN J Y, DIAO W R, ZHAO Q C, et al. IoTFuzzer: discovering memory corruptions in IoT through app-based fuzzing[C]//Proceedings 2018 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2018: 1-15.

[70] NILO R, ANDREA C, DIPANJAN D, et al. DIANE: identifying fuzzing triggers in Apps to generate under-constrained inputs for IoT devices[C]//2021 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2021: 484-500.

[71] ZUO C S, WEN H H, LIN Z Q, et al. Automatic fingerprinting of vulnerable BLE IoT devices with static UUIDs from mobile Apps[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1469-1483.

[72] WANG X, SUN Y, NANDA S, et al. Looking from the mirror: evaluating IoT device security through mobile companion apps[C]// USENIX Security Symposium. Berkeley: USENIX Association, 2019: 1151-1167.

[73] FENG X, LI Q, WANG H, et al. Acquisitional rule-based engine for discovering internet-of-things devices[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 327-341.

[74] YU L, LUO B, MA J, et al. You are what you broadcast: identification of mobile and IoT devices from (Public) Wi-Fi[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 55-72.

[75] ZHANG W, MENG Y, LIU Y G, et al. HoMonit: monitoring smart home Apps from encrypted traffic[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1074-1088.

[76] CHO K-T, SHIN K G. Fingerprinting electronic control units for vehicle intrusion detection[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2016: 911-927.

[77] CHO K T, SHIN K G. Viden: attacker identification on in-vehicle networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1109-1123.

[78] CHOI H, LEE W C, AAFER Y, et al. Detecting attacks against robotic vehicles: a control invariant approach[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 801-816.

[79] BIRNBACH S, EBERZ S, MARTINOVIC I. Peeves: physical event verification in smart homes[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1455-1467.

[80] FENG C, PALLETI V R, MATHUR A, et al. A systematic framework to generate invariants for anomaly detection in industrial control systems[C]//Proceedings 2019 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2019: 1-15.

[81] FERNANDES E, PAUPORE J, RAHMATI A, et al. FlowFence: practical data protection for emerging IoT application frameworks[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2016: 531-548.

[82] WEN H H, LIN Z Q, ZHANG Y Q. FirmXRay: detecting bluetooth link layer vulnerabilities from bare-metal firmware[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 167-180.

[83] JIA Y J, CHEN Q A, WANG S Q, et al. ContexIoT: towards providing contextual integrity to appified IoT platforms[C]//Proceedings 2017 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2017: 1-15.

[84] TIAN Y, ZHANG N, LIN Y-H, et al. SmartAuth: user-centered authorization for the internet of things[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2017: 361-378.

[85] DEMETRIOU S, ZHANG N, LEE Y, et al. HanGuard: SDN-driven protection of smart home Wi-Fi devices from malicious mobile apps[C]//Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2017: 122-133.

[86] SCHUSTER R, SHMATIKOV V, TROMER E. Situational access control in the Internet of things[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1056-1073.

[87] ZENG E, ROESNER F. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2019: 159-176.

[88] WANG W C, CICALA F, HUSSAIN S R, et al. Analyzing the attack landscape of Zigbee-enabled IoT systems and reinstating users' privacy[C]//Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2020: 133-143.

[89] 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.

[90] KUMAR S, HU Y, ANDERSEN M P, et al. JEDI: many-to-many end-to-end encryption and key delegation for IoT[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2019: 1519-1536.

[91] XI W, QIAN C, HAN J S, et al. Instant and robust authentication and key agreement among mobile devices[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 616-627.

[92] HAN J, CHUNG A J, SINHA M K, et al. Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types[C]//2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2018: 836-852.

[93] JIN W Q, LI M, MURALI S, et al. Harnessing the ambient radio frequency noise for wearable device pairing[C]//Proceedings of the

2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 1135-1148.

[94] LI X P, ZENG Q, LUO L N, et al. T2Pair: secure and usable pairing for heterogeneous IoT devices[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 309-323.

[95] APTHORPE N, HUANG D Y, REISMAN D, et al. Keeping the smart home private with smart(er) IoT traffic shaping[J]. Proceedings on Privacy Enhancing Technologies, 2019, 2019(3): 128-148.

[96] OCONNOR T J, MOHAMED R, MIETTINEN M, et al. HomeSnitch: behavior transparency and control for smart home IoT devices[C]//Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2019: 128-138.

[97] KIM C H, KIM T, CHOI H, et al. Securing real-time microcontroller systems through customized memory view switching[C]//Proceedings 2018 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2018: 1-15.

[98] CLEMENTS A A, ALMAKHDHUB N S, BAGCHI S, et al. ACES: automatic compartments for embedded systems[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2018: 65-82.

[99] ABERA T, ASOKAN N, DAVI L, et al. C-FLAT: control-flow attestation for embedded systems software[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 743-754.

[100] SUN Z C, FENG B, LU L, et al. OAT: attesting operation integrity of embedded devices[C]//2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 1433-1449.

[101] ABERA T, BAHMANI R, BRASSER F, et al. DIAT: data integrity attestation for resilient collaboration of autonomous systems[C]//Proceedings 2019 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2019: 1-15.

[102] MENG Y, WANG Z C, ZHANG W, et al. WiVo: enhancing the security of voice control system via wireless signal in IoT environment[C]//Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2018: 81-90.

[103] SHEZAN F H, CHENG K M, ZHANG Z, et al. TKPERM: cross-platform permission knowledge transfer to detect overprivileged third-party applications[C]//Proceedings 2020 Network and Distributed System Security Symposium. Virginia: the Internet Society, 2020: 1-15.

[104] EMAMI-NAEINI P, AGARWAL Y, FAITH CRANOR L, et al. Ask the experts: what should be on an IoT privacy and security label?[C]//2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 447-464.

[105] YU H, LIM J, KIM K, et al. Pinto: enabling video privacy for commodity IoT cameras[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1089-1101.

[106] NASSI B, BEN-NETANEL R, SHAMIR A, et al. Drones' cryptanalysis - smashing cryptography with a flicker[C]//2019 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 1397-1414.

[107] APTHORPE N J, VARGHESE S, FEAMSTER N. Evaluating the contextual integrity of privacy regulation: parents' IoT toy privacy norms versus COPPA[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2019: 123-140.

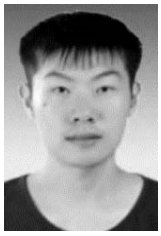
[108] JULIE H, YASEMIN A, SUSANNE F. "It's the company, the government, you and I": user perceptions of responsibility for smart home privacy and security[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2021: 1-18.

[109] ZONG P, LV T, WANG D, et al. FuzzGuard: filtering out unreachable inputs in directed grey-box fuzzing through deep learning[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2020: 2255-2269.

[110] MANANDHAR S, MORAN K, KAFLE K, et al. Towards a natural perspective of smart homes for practical security and safety analyses[C]//2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 482-499.

[作者简介]

杨毅宇（1987− ），男，云南大理人，中国科学院大学博士生，主要研究方向为网络与系统安全。



周威（1993− ），男，河北保定人，中国科学院大学博士生，主要研究方向为网络与系统安全。

赵尚儒（1995− ），男，广东广州人，中国科学院大学博士生，主要研究方向为网络与系统安全。

刘聪（1997− ），男，陕西宝鸡人，西安邮电大学硕士生，主要研究方向为网络与系统安全。

张宇辉（1997− ），男，山西临汾人，西安电子科技大学硕士生，主要研究方向为网络与系统安全。

王鹤（1987− ），女，河南滑县人，博士，西安电子科技大学讲师，主要研究方向为网络与系统安全、密码学。

王文杰（1964− ），男，陕西西安人，博士，中国科学院大学副教授，主要研究方向为信息安全与智能信息处理。

张玉清（1966− ），男，陕西西安人，博士，中国科学院大学教授，主要研究方向为网络与系统安全。