计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180585
55(10):2111-2124,2018

智能家居安全综述

王基策[1] 李意莲[2] 贾 岩[2] 周 威[1] 王宇成[2] 王 鹤[2] 张玉清[1,2]
[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](西安电子科技大学网络与信息安全学院 西安 710071)
(wangjc@nipc.org.cn)

Survey of Smart Home Security

Wang Jice[1], Li Yilian[2], Jia Yan[2], Zhou Wei[1], Wang Yucheng[2], Wang He[2], and Zhang Yuqing[1,2]
[1](*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing* 101408)
[2](*School of Cyber Engineering, Xidian University, Xi'an* 710071)

Abstract With the development of the Internet of things technology, smart home industry has become increasingly prosperous, and its security issues have attracted the attention of more and more researchers. Currently, the related research on smart home security is still in initial stage. This paper first reviews the development history and current status of smart home, and summarizes the architecture of current smart home system. In terms of security, we analyze and summarize the domestic and foreign literatures in recent years, and divide security issues into three aspects: platform security, device security and communication security. Platform security research mainly focuses on designing secure authentication and access control scheme, as well as discovering security issues in new scenarios such as smart home trigger-action and smart speakers; device security research mainly includes device firmware vulnerability discovery and side channel analysis; communication security research mainly includes protocol vulnerability discovery and network traffic analysis. Through in-depth analysis of the shortcomings of existing research work, the challenges and opportunities faced by smart home security are summarized. Finally, based on the current research status of smart home security, we point out four future research directions.

Key words smart home; security; privacy; challenge and opportunity; survey

摘 要 随着物联网技术的发展,智能家居产业日益繁荣,其安全问题受到越来越多研究者的关注,目前相关研究尚在起步阶段.首先回顾了智能家居的发展历程及现状,总结并介绍了当前智能家居系统架构.在安全方面,归纳、分析和总结了近几年的国内外文献,将安全问题划分为3个方面:平台安全、设备安全和通信安全,并分析了这3方面智能家居安全研究现状.目前平台安全研究主要集中于设计安全的认证和访问控制方案,以及发现设备联动和智能音箱等新场景的安全问题;设备安全研究主要包括设备固件漏洞挖掘和设备侧信道分析;通信安全研究主要包括协议漏洞挖掘和网络流量分析.总结了现有

收稿日期:2018-08-28;修回日期:2018-09-11
基金项目:国家重点研发计划项目(2016YFB0800700);国家自然科学基金项目(61572460,61272481);信息安全国家重点实验室的开放课题(2017-ZD-01);国家发改委信息安全专项基金项目((2012)1424);中央高校基本科研业务费专项资金项目(JB182001);西安电子科技大学研究生创新基金项目
This work was supported by the National Key Research and Development Program of China (2016YFB0800700), the National Natural Science Foundation of China (61572460, 61272481), the Open Project Program of the State Key Laboratory of Information Security (2017-ZD-01), the National Information Security Special Projects of National Development and Reform Commission of China ((2012)1424), the Fundamental Research Funds for Central Universities (JB182001), and the Innovation Fund of Xidian University.

研究工作的进展,分析了所存在的不足与问题,并指出了目前智能家居安全研究面临的重要挑战与机遇.最后,结合智能家居安全研究现状,指出了4个未来的研究方向.

关键词 智能家居;安全;隐私;挑战与机遇;综述

中图法分类号 TP393

信息通信产业历经互联网时代、移动互联网时代,正在走向物联网时代,这将带来更多创新应用与发展.其中智能家居是物联网技术运用的典型代表,智能家居以家庭住宅为平台,利用物联网技术将家居生活有关的设施集成,为人们提供舒适、便利、安全和娱乐的居住环境.2012年工业和信息化部就将智能家居列入"物联网十二五发展规划"的九大重点产业[1].目前智能家居产业呈现出快速发展态势,根据Strategy Analytics的统计数据显示,2017年全球智能家居市场规模达到840亿美元,预测2018年将高达960亿美元,并在未来5年内持续增长,2023年将增长至1 550亿美元[2].

智能家居的发展为人们带来了诸多益处,但同时也面临着严重的安全问题.智能家居系统的安全漏洞将不仅给用户带来隐私泄露风险,还可能造成用户财产损失,甚至威胁用户人身安全.例如窃贼可以通过控制智能门锁进行盗窃活动,纵火犯可以通过控制智能烤箱致使受害者遭受火灾威胁,僵尸网络的控制者还可以利用智能摄像头、智能网关、智能家电等设备发动大规模DDOS攻击[3].

通过调研2014—2018年网络与信息安全领域四大顶级会议S&P(IEEE Symposium on Security and Privacy),CCS(ACM Conference on Computer and Communications Security),Security(Usenix Security Symposium),NDSS(ISOC Network and Distributed System Security Symposium)论文,我们发现智能家居安全相关研究成果逐年增多.图1展示了相应变化趋势,并可看出在近2年相关研究呈现爆发趋势.经过分析与总结,现有研究尚存在一些局限性,大多数研究侧重于挖掘智能家居系统安全漏洞,分析安全威胁,但研究仅关注于系统的单一层次或环节.同时智能家居安全防护的研究文献较少,且大多数研究成果适用范围较窄,应用价值不高.此外,目前关注于智能家居安全领域的调研综述或报告极少[4-7],并且存在着调研范围窄、揭示问题不深、跟踪最新成果不及时等问题.为了便于研究者深入了解智能家居安全问题并进一步开展研究工作,本文对智能家居安全研究现状进行了深入分析,指出了智能家居安全面临的挑战和机遇以及未来的研究方向.

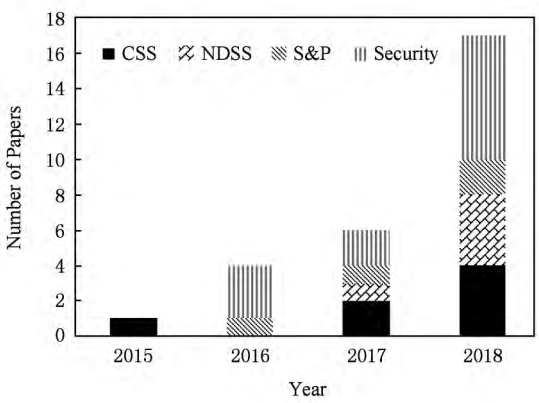

Fig. 1 Number of smart home security papers in the top4 security conferences

图1 四大安全顶会智能家居安全论文统计

本文主要贡献包括3个方面:

1)分析了智能家居的发展历程与现状,总结并介绍了当前智能家居系统架构.

2)深入调研了近几年国内外智能家居安全研究文献,从平台安全、设备安全和通信安全这3个方面介绍并总结了智能家居安全研究现状.

3)通过分析智能家居的安全问题以及现有研究工作的不足,指出了智能家居安全研究中面临的挑战与机遇,并为相关研究者指出了未来的热点研究方向.

1 背景介绍

1.1 智能家居发展历程

智能家居起源很早:20世纪80年代初,随着大量采用电子技术的家用电器面市,住宅电子化开始实现;80年代中期,将家用电器、通信设备与安全防范设备各自独立的功能综合为一体,形成了住宅自动化概念;至80年代末,由于通信与信息技术的发展,出现了通过总线技术对住宅中各种通信、家电、安防设备进行监控与管理的商用系统,这在美国被称为Smart Home,就是现在智能家居的原型.进入21世纪后,智能家居的发展更为多样化,技术实现方式也更加丰富.总体而言,智能家居发展大致经历了4代:第1代主要基于同轴线两芯线进行家庭组网,实现灯光、窗帘控制和少量安防等功能;第2代

主要基于 RS-485 线,部分基于 IP 技术进行组网,实现可视对讲、安防等功能;第 3 代实现了家庭智能控制的集中化,实现安防、控制、计量等业务;第 4 代基于全 IP 技术,终端设备基于 Zigbee、蓝牙等技术,业务提供采用"云"技术,并可根据用户需要实现定制化、个性化[8].

目前,智能家居发展正处于第 4 代,市场上涌现了数量庞大的智能家居平台厂商,据不完全统计已经超过 120 家[9]. 众多国际互联网巨头如苹果、亚马逊、三星等[10-12]均推出了智能家居平台,为传统硬件厂商提供智能化解决方案. 国内企业如小米[13]也在积极推进智慧生活落地,更是联合百度以 AI+IoT 构建生态体系,让人们智慧生活成为可能.

1.2 智能家居系统架构

目前,尽管智能家居平台厂商数量众多,却遵循着相似的系统架构. 如图 2 所示,智能家居系统主要由终端设备、移动 App、物联网云端、通信网络 4 部分组成. 各种各样的终端设备与物联网云端联通,一部分终端设备可直接接入有线或无线网络从而与云端联通,另一部分设备由于缺乏直接接入互联网的通信接口,从而以网关或智能手机为跳板与云端联通. 联通后,设备会将自身感知或收集到的数据发送至云端,云端对数据进行存储、管理与分析处理.

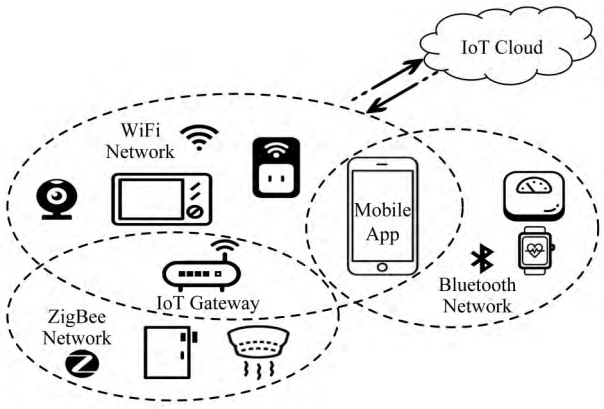

Fig. 2 Smart home system architecture

图 2 智能家居系统架构

1.2.1 智能家居平台

智能家居平台是为方便终端设备接入,加快智能家居应用发展而构建的消费领域平台. 在智能家居系统架构中,移动 App 及物联网云端属于平台的一部分,它们的主要功能包括:

1) 云端数据聚合与分析. 平台将从设备端收集到的数据进行存储及智能分析处理.

2) 管理、控制和协调不同的设备、系统和服务. 平台提供认证管理功能,防止非法设备接入平台;平台提供设备控制功能,用户可通过平台提供的移动 App 控制终端设备;平台协调不同的终端设备,提供了设备联动(trigger-action)功能,设备之间可通过用户预先设置的规则自动化调用.

1.2.2 终端设备

智能家居系统中的终端设备是最终服务于用户并提供家居服务的实体,不同设备为人们生活提供了不同的服务. 在一些研究中,从实施信息安全机制硬件资源多少的角度出发,将终端设备分为受限设备和能力设备 2 类[14-15].

1) 受限设备. 指功率、计算、存储或通信资源有限的设备,例如智能灯泡、智能电表、传感器等,由于设备资源的约束,对安全机制的实施带来了限制.

2) 能力设备. 指由主电源供电、具有足够的计算、存储和通信资源的设备,例如家庭网关、电视等. 由于资源充足,安全机制可以得到较好实施.

1.2.3 通信网络

在智能家居中,设备与云端、设备与设备之间使用了多种协议进行通信,我们按照 TCP/IP 协议分层模型对其进行分层,常用的网络通信协议如图 3 所示.

1) 物理与链路层. 关注网络节点间的数据通信及接口技术,包括以太网、WiFi、IEEE 802.15.4 等协议.

2) 网络层. 确定分组从源端到目的端的路由选择,包括 IP、6LowPan 等协议.

3) 传输层. 负责实现端到端的通信. 最著名的 2 个互联网协议 TCP 和 UDP 就位于这一层.

4) 应用层. 负责定义数据格式并解读数据,实现应用程序到应用程序间的通信. 大部分平台支持 HTTP 协议,但为了更高效快速地交换数据,MQTT[16](Message Queuing Telemetry Transport)、CoAP[17](Constrained Application Protocol)、AMQP(Advanced Message Queuing Protocol)、XMPP[18](Extensible Messaging and Presence Protocol)等协议也被广泛应用. 应用层支持的协议较多,在智能家居系统设计时,需考虑实际场景的通信需求,选择合适的应用协议.

不同层次的协议可以组合起来形成协议栈,目前常用的协议栈包括 Bluetooth、ZigBee 等. 其中,ZigBee 以其低成本、低功耗、自组网、安全性高的特性成为工业控制领域和智能家居领域中最流行的协议之一,例如飞利浦的生态系统已全面支持 ZigBee3.0[19].

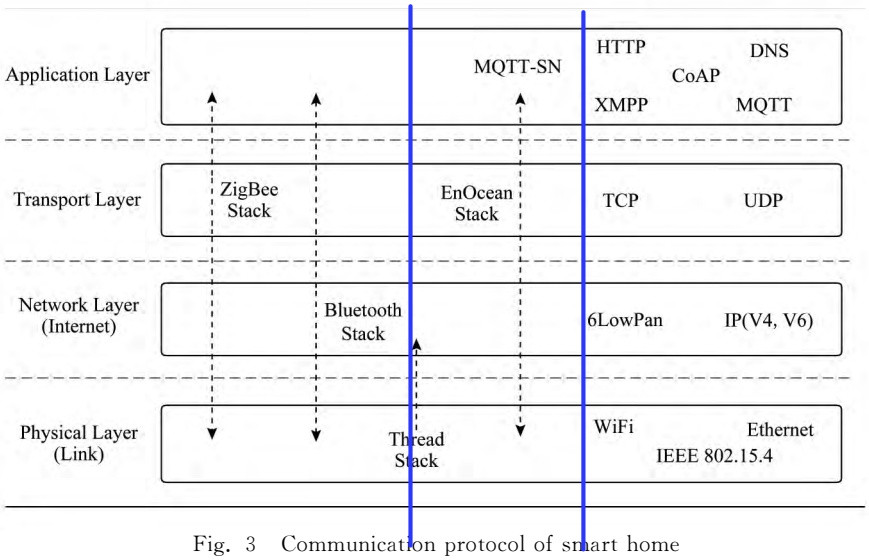

Fig. 3 Communication protocol of smart home

图 3 智能家居中常用通信协议

2 智能家居安全研究现状

除了网络与信息安全领域四大顶级会议外，本文还调研了 2013 年 1 月到 2018 年 6 月智能家居安全领域的高引论文、预印本数据库 arXiv 论文以及中国计算机学会 CCF A 类和 CCF B 类会议与期刊论文，我们将目前智能家居安全研究分为三大方面：平台安全、设备安全和通信安全. 平台安全是指智能家居平台厂商在平台设计与实施中存在的各类安全问题，设备安全是指与智能家居终端设备直接相关的安全问题，通信安全是指与网络通信相关的安全问题. 在表 1 中列出了各方面的研究问题，并以此分类为主题介绍智能家居系统安全问题与研究现状.

Table 1 Smart Home Security Research Issues

表 1 智能家居安全研究问题

Categories	Research Issues
Platform Security	① Authentication for the smart home
	② Access control for the smart home
	③ Trigger-Action security
	④ Security and privacy of the smart speaker
Device Security	① Vulnerability discovery in the smart home device
	② Side channel attack in the smart home device
Communication Security	① Vulnerability discovery in the communication protocol
	② Network traffic analysis for the smart home

2.1 平台安全

通过第 1 节介绍可知，平台联系着各种各样的智能家居设备与服务. 平台的安全问题将会对厂商的智能家居生态带来严重威胁，会影响该平台下所有的设备及终端用户，因此平台是智能家居安全研究的重点. 研究发现：平台的安全问题主要存在于以下方面：智能家居用户身份认证、智能家居设备访问控制、设备联动安全以及智能音箱安全.

2.1.1 智能家居用户身份认证

认证技术是信息安全理论与技术的一个重要方面. 在智能家居系统中，用户身份认证的主要目的是验证设备使用者的身份，防范非法用户对智能家居设备进行操控.

智能家居系统中认证机制的缺失会对用户安全与隐私造成极大危害. 例如由于智能音箱缺乏对使用者声音的认证，研究人员发现电视里播放的汉堡王广告可以触发 Google Home 音箱的语音控制指令，使其访问维基百科网页[20]；卡通动画南方公园可以触发 Amazon Echo，使其访问 Amazon 商城并自动填满用户购物车[21]；甚至，攻击者可以通过将恶意语音命令嵌入歌曲中完全控制用户的语音助手或智能音箱[22]. 此外，Zhang 等人[23]研究发现现有平台的认证机制存在安全漏洞，攻击者能够发动设备伪造攻击，导致家庭局域网 WiFi 密码泄露.

研究人员设计了多种多样的身份认证方案. 早期的研究工作关注于设计安全的身份认证协议. Liu 等人[24]设计了一套基于椭圆曲线密码系统(elliptic curve cryptography, ECC)的认证协议，能够有效抵御窃听、重放、中间人等攻击. John 等人[25]提出了一套基于设备自身独特物理特性(physical unclonable functions, PUF)算法的安全协议，用于设备注册、

认证、解密以及数字签名生成,该协议能够安全有效地部署在受限功率和资源的智能家居设备上.另一部分研究工作关注于设计适用于智能家居场景下的认证方式,在表 2 中对这些工作进行了对比分析.Vaidya 等人[26]提出了基于智能卡的密码认证方案,该方案的缺点是需要额外的智能设备且难以抵御智能卡的遗失与窃取.Feng 等人[27]为语音助手设计了一个基于语音的认证方案,该方案需要可穿戴设备支持.Zhang 等人[23]设计了基于近邻的设备认证方案,要求用户手持智能手机在智能家居设备附近完成移动或旋转操作,实现了手机与设备间的相互认证,该方案能够有效抵御攻击者进行侧信道攻击.Han 等人[28]提出了一个基于上下文的设备配对方案,它使用固定时间内传感器测量信息作为密钥协商协议的秘密,实现了智能家居场景下不同设备的自动配对.

Table 2 Comparison and Analysis of Existing Identity Authentication Schemes

表 2 现有身份认证方案对比分析

Reference	Scheme	Technique	Scenario	Threat Model
Ref[26]	One-time password authentication using smart card	HOTP algorithm, hash-chaining technique cryptographic protocol	Remote access and control to home appliances	Stolen smart card attack and forward secrecy with lost smart card
Ref[27]	Voice commands matching	Human speech Model, speech Recognition	Voice assistants for wearables, smart vehicles, and smart home	Mangling voice attacks, replay and impersonate attack
Ref[28]	Proximity based IoT device authentication	Matching between RSS-trace and sensor-trace	Smart home	Powerful active attacker
Ref[29]	Context-based pairing protocol	Abstracting sensor measurements, context fingerprints generation	Smart home	Shamming attack, Man-in-the Middle attack

在智能家居场景下,实施身份认证机制对于保护用户安全与隐私十分必要.由于许多智能家居设备缺乏屏幕、键盘等输入方式,以往基于口令的身份认证机制难以实施,故目前大部分研究工作关注于如何设计有效的设备身份认证方式.第 1 类方法需借助智能卡、可穿戴设备等额外设备支持,实施起来不够便利;第 2 类方法利用智能手机作为设备认证的中介,他们研究智能手机与设备之间的认证方式,而手机与平台间的认证仍使用基于口令的认证方式.然而,目前的研究均未考虑智能家居设备使用场景,智能家居设备通常由多个用户共同使用,如何对不同身份的用户进行认证及身份管理还需深入研究.

2.1.2 智能家居设备访问控制

目前,大部分智能家居平台(例如 Samsung Smartthings,Apple Homekit,Google Weave/Brillo)为第三方开发者提供了编程框架,使得第三方开发者可以开发移动 App 用于控制相应的智能家居设备.在此情景下,访问控制机制扮演了重要角色,它们决定了移动 App 如何访问敏感资源.研究人员对现有平台的访问控制机制进行研究,发现其存在安全缺陷.Fernandes 等人[29]分析了 SmartThings 平台,发现其权限模型粒度过粗,应用能够获得超出用户期望的过度授权,从而有可能对用户生命财产造成威胁.

现阶段,已有一些研究工作关注于如何设计更加安全的访问控制机制.为应对权限粒度过粗问题,Lee 等人[30]设计了一个基于设备功能的访问控制系统,相比基于权限的访问控制系统粒度更细.2017 年 Jia 等人[31]提出了基于上下文的权限控制系统 ContexIoT,提供细粒度的上下文来鉴定敏感动作以及带有上下文信息的运行时提示来帮助用户进行访问控制,但是提示过于专业化,难以被用户理解使用.2018 年 Rahmati 等人[32]设计了一个基于风险的权限访问控制,它将设备操作按其风险相似度分组,并以组为单位授予相应的访问权限.通过实验,证明该方案能够显著降低安全风险.除了直接关注访问控制机制设计,为应对 App 的描述与其实际操作不符的安全隐患,Tian 等人[33]设计了一种以用户为中心、基于语义的智能授权系统 SmartAuth,能自动地从智能家居 App 的自然语言描述、程序、和注释中提取安全相关信息并生成授权用户接口,使得设备访问符合用户期望.为防范恶意应用获得用户授权之后访问并窃取敏感数据,Fernandes 等人[34]设计了一个基于标签的信息流控制系统,使用污点追踪方法限制敏感数据流出,但该方法未考虑侧信道分析问题.

将程序是否存在漏洞问题转化为污点信息是否会被安全敏感操作所使用的问题

智能家居场景下越权访问的危害较智能手机更为严重,对不同智能家居平台的访问控制机制进行深入分析尤为必要,然而目前研究局限于 SmartThings 平台,对其余平台的分析仍非常缺乏. 目前许多研究工作致力于弥补权限访问控制模式下权限粒度过粗的问题,主要思想是将设备按其功能或风险进行分组,并以组为单位授予不同的访问权限. 此外,还有一些工作不再局限于访问控制方案设计,而是关注于如何限制恶意应用对敏感资源的访问,研究包括如何防止恶意应用获得敏感访问权限、如何在恶意应用获得访问权限之后保护敏感资源等问题. 总的来说,研究人员从不同角度对智能家居设备访问控制机制展开了研究,然而智能家居系统应用场景多样复杂,如何设计细粒度的访问控制方案、如何对设备联动(trigger-action)操作、多用户使用设备等场景设计访问控制方案均需要进一步研究.

2.1.3 智能家居设备联动安全

智能家居设备联动是一种自动化的设备使用模式,它使得智能家居设备不仅仅可以通过手机或音箱进行控制,还可以使用用户预先定义的触发规则,使得设备之间进行联动操作. 例如用户可以自定义联动规则,当检测到空气中的一氧化碳超标时,就触发家中所有的灯变为红色,或检测到 PM2.5 时开启空气净化. 许多智能家居平台以及第三方自动化平台(If-This-Then-That(IFTTT)[35], Zapier[36] 和 Microsoft Flow[37])支持设备联动,这些平台也拥有访问用户在线服务和物理设备的特权,一旦被攻陷,攻击者便能任意窃取数据并操作设备.

目前,一些研究者对使用此平台的安全与隐私问题展开了研究. Fernandes 等人[38] 分析了包括 IFTTT 平台在内的 7 个联动平台(trigger-action platform),发现攻击者可能获得过度授权的 OAuth 令牌从而对设备进行提权攻击,为此作者设计了一个去中心化的联动平台,使得攻击者无法使用与用户定义规则不一致的 OAuth 令牌. 不仅联动平台设计存在缺陷,用户自定义的联动规则也潜藏风险,Surbatovich 等人[39] 构建了一个信息流模型用于评估用户自定义联动规则的安全性,发现 50%的规则存在安全风险,其不仅给个人使用带来不便,还能够被攻击者用于分发恶意软件或者发动拒绝服务攻击. 文献[40-41]研究了联动规则错误检测技术,文献[42]发现了一类由于触发条件不足导致的联动规则错误,之后开发了 TrigGen 技术用于自动生成正确的联动规则.

随着智能家居设备功能的不断增多,设备联动的使用情景也将愈加丰富,许多研究工作关注于设备联动规则的合理性和安全性,他们分析了联动规则的安全问题,开发出了相应的分析工具,并进一步设计出自动化的联动规则生成工具,对于帮助用户构建安全的设备联动场景具有重要意义. 但另一方面,对于设备联动平台的分析还较为欠缺. 大部分智能家居平台支持设备联动操作,而各自方案实现存在差异,研究人员需更加深入挖掘现有联动平台的安全威胁并设计相应的安全防护方案.

2.1.4 智能音箱安全与隐私

语音识别技术在近几年取得了显著进步,生产厂商通过将语音识别模块与传统音箱结合,创造出智能音箱这一新的产品,其典型代表是 Amazon Echo、Google Home、天猫精灵、小米 AI 音箱等. 在家居生活中,通过语音控制智能家居设备是最自然、高效的一种方式,人们通过与智能音箱进行语音交互,可以点播歌曲、上网购物,还可以对智能家居设备进行控制,比如打开窗帘、打开电灯、设置冰箱温度等,其已经成为与移动 App 并驾齐驱的智能家居控制中心. 一旦攻破智能音箱,攻击者可以完全控制家庭中所有智能家居设备,为智能家居安全带来了极为严重的威胁.

近年来,研究者开始关注于语音识别以及智能音箱的安全与隐私问题. 其研究重点一方面为构造恶意的语音样本攻击语音识别系统,另一方面为研究智能音箱控制系统的漏洞. Zhang 等人[43] 使用人耳无法听到的超声波指令攻击智能音箱的语音识别系统,从而能够使用任意命令完全控制音箱. 其优点是人耳无法听见,缺点是攻击距离较近,仅为 5 英尺(1.524 m). Roy 等人[44] 将攻击距离提高至 25 英尺(7.62 m),使得攻击更易实现,同时还为此类攻击提供了防御方案. 文献[45-46]观察到语音识别系统依靠音频中提取的语音特征识别语音信息,从而首次生成了机器可以识别而人耳无法分辨的恶意语音命令,其缺点是生成的语音对于人类如噪声一般毫无意义. Yuan 等人[22] 对此进行了改进,他们利用语音识别系统中人工智能算法的漏洞,将控制指令嵌入到歌曲中,构造成恶意的对抗样本欺骗语音识别系统,从而控制智能音箱. 该优点是人耳同样无法识别,缺点是攻击条件较为苛刻,必须诱使被攻击者播放恶意样本. Zhang 等人[47] 研究智能音箱语音命令的相似度,发现可以通过构造恶意语音命令以劫持用户发出的正常语音命令,从而窃取用户的谈话数据.

智能音箱将在智能家居系统中扮演越来越重要的角色,也将成为安全研究的热点.目前的研究大部分关注于构造用户无法分辨的恶意语音样本,可将其分为 2 类:1)用户听不见声音,2)用户听不出命令.构造以上 2 类恶意样本利用了智能音箱不同模块软件或硬件的安全漏洞,而智能音箱系统复杂,系统的任一层次与环节都可能潜藏着安全漏洞,如何挖掘音箱的安全漏洞并设计相应的防护方案仍需要深入研究.除此之外,智能音箱还能够听取家居生活的各种对话或声音,如何防范智能音箱窃取用户隐私数据,发现隐私泄露风险点并设计防护方案也亟待研究.

2.2 设备安全

2.2.1 智能家居设备漏洞挖掘

智能家居设备多种多样,智能设备安全漏洞的数目也十分惊人且危害非常严重,其不仅使攻击者能够以本地或远程的方式控制设备,窃取用户隐私数据,甚至还会威胁人身及财产安全.根据国家互联网应急中心(CNCERT)发布的《2017 年我国互联网网络安全态势综述》显示,2017 年国家信息安全漏洞共享平台(CNVD)收录的安全漏洞中关于联网智能设备(此统计中联网智能设备指物联网设备)安全漏洞有 2 440 个,同比增长高达 118.4%[48],漏洞类型分布如图 4 所示:

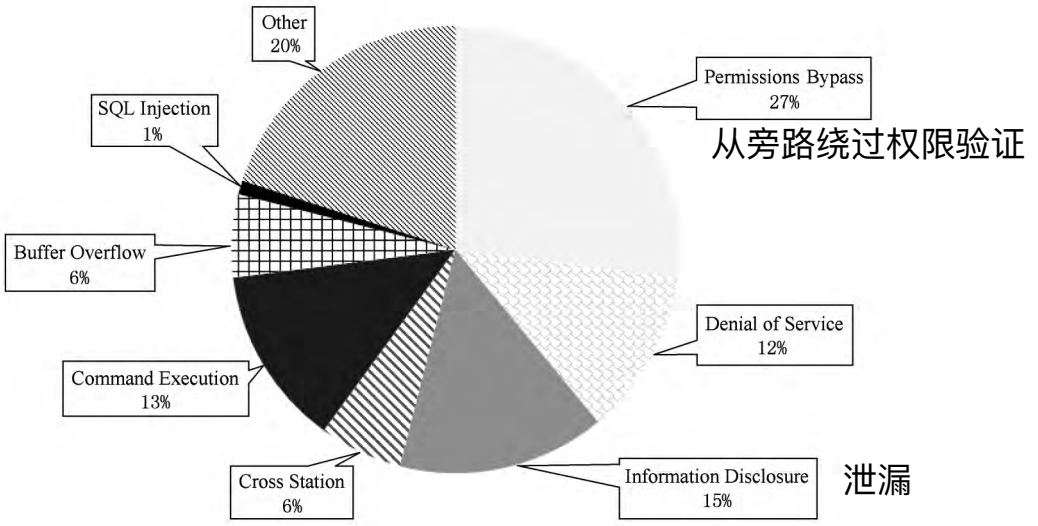

Fig. 4 Type distribution of smart device vulnerabilities

图 4 智能设备漏洞类型分布

目前,在学术界也有许多研究工作关注于智能家居设备安全漏洞挖掘与分析.研究集中于设备固件安全,Ur 等人[49]发现了 Philips Hue 照明系统和 Kwikset 智能门锁存在访问控制问题,影响设备的基本使用.Ronen 等人[50]发现了智能灯泡的安全漏洞并对其实施了扩展功能攻击,它可以窃取用户隐私,此外更严重的是攻击者可以控制智能灯泡发光的颜色、强度和频率,这可能诱发患有光敏性癫痫病的人癫痫发作.

现阶段许多研究工作局限于分析单一设备漏洞,而针对智能设备固件进行系统性安全分析与漏洞挖掘的研究尚处于起步阶段,在表 3 中对现有工作进行了对比分析.2015 年 Shoshitaishvi 等人[51]发表了关于二进制固件中认证绕过漏洞检测的文章,该文提出了一个二进制分析框架 Firmalice,用于检测二进制固件中存在的认证绕过漏洞.然而,该文只对 3 种商用设备的固件进行了分析,数据集不够丰富,同时它在检测每个固件样本时,需要安全分析人员事先对固件进行分析来提取一份安全策略,严重降低了工具的自动化性能.2016 年 Subramanyan 等人[52]对固件中的安全属性进行了研究.他们通过符号执行来检测检测固件信息流的安全性,通过对商业系统芯片设计的评估,发现了仿真测试漏掉的复杂安全漏洞.2017 年 Hernandez 等人[53]开发了一个针对 USB 的特定固件分析框架 FirmUSB,使用 USB 协议的领域知识检查固件文件并分析它们可以产生的活动,基于特定的领域知识他们开发了定位算法,相比于无约束的完全符号执行,其速度增长了 6 倍.2018 年 Muench 等人[54]分析了模糊测试设备固件时面临的主要挑战,随后提出 6 个能够用于挖掘内存破坏漏洞的启发式方法,实验验证了这些方法的有效性.同年,Chen 等人[55]观察到大部分

写入eprom的程序

符号执行,用符号值替代真实值执行,应用于软件测试

模糊测试,提供非预期输入,监视异常结果,发现软件漏洞

智能家居设备由移动 App 控制,从而在 App 端生成畸形数据对设备进行模糊测试,克服了固件获取与分析的难题.

漏洞广泛存在于智能家居设备,尤其是设备固件之中.现阶段一些研究工作结合了固件逆向分析、通信协议分析、模糊测试等方法挖掘设备固件漏洞,但其研究多局限于单一设备分析,系统性的挖掘固件漏洞是研究的努力方向,主要方法是将模糊测试、符号执行、污点分析等常用漏洞挖掘技术应用于设备固件分析,但目前研究尚在起步阶段.对于静态符号执行、静态污点分析等静态分析技术,目前尚缺乏对于 ARM 架构和其他轻量级架构的支持.对于模糊测试技术,现有研究的阻碍在于无法对轻量级固件进行模拟执行,因而难以监控固件运行情况,模糊测试难以实施.以上问题均需要研究人员深入研究并开发出相应工具.

对固件进行分析,包括文件系统和内核
然后进行逻辑测试,查找固件所使用的通用库的漏洞
或者说iot设备功能上的漏洞

Table 3 Comparison and Analysis of Existing Vulnerability Discovery Technology of Firmware

表 3 现有设备固件漏洞挖掘技术对比分析

Reference	Vulnerability Type	Vulnerability Discovery Method	Dynamic/Static	Analyzed Code Type
Ref[52]	Authentication Bypass	Symbolic Execution	Static	Binary
Ref[53]	Information Flow Properties	Symbolic Execution	Static	Binary
Ref[54]	Malicious Activity in USB	Symbolic Execution	Static	Binary
Ref[55]	Memory Corruptions	Fuzzing Test	Dynamic	Source Code or Binary
Ref[56]	Memory Corruptions	App-based Fuzzing	Dynamic	No Access to the Code

2.2.2 智能家居设备侧信道分析

侧信道攻击是针对电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的信息进行攻击的方法.智能家居的设备接收、交换、传输有关用户家庭环境和个人活动的各种数据.然而,智能设备在执行这些特定的数据任务时往往会伴随着一些物理现象,这使得他们很容易受到侧信道攻击.通过调研近几年的智能家居平台下的侧信道攻击文献,本文将智能家居平台下的侧信道攻击划分为设备攻击和网络通信攻击 2 种.

1) 设备攻击.设备攻击是通过破解智能设备在使用过程中产生的如声音、光线、温度等物理现象来获取用户的隐私信息.在文献[56]中,作者成功地在几秒钟时间内利用光线变化识别出 70 m 外的电视播放内容.Barbosa 等人[57]发现可以通过观察智能电表的细粒度的仪表读数来推断出住户的特定的活动或行为模式.

2) 网络通信攻击.当设备与设备或设备与云端进行网络通信时,带宽、流量的消耗可能会发生变化,攻击者通过分析这些信息的变化来获取相关的隐私数据.Fafoutis 等人[58]发现可穿戴设备中传感器收集的身体活动水平信息与无线信道的变化密切相关,而无线信道的变化恰好可以通过测量被窃听帧的信号强度来捕获,因而佩戴者的身体活动信息通过物理层泄露给窃听者.Copos 等人[59]发现可以使用流量分类技术来推断建筑物内发生的事件,通过分析 Nest 恒温器及烟雾二氧化碳检测器的网络流量信息获取家中的敏感信息.目前,视频监控已被广泛采用以确保家庭安全,大多数的视频编码采用差分编码来有效压缩视频流.Li 等人[60]发现即使是加密的视频流,在进行差分编码压缩时也会导致旁道信息泄露.攻击者可以根据加密视频流的流量大小数据来容易地推断用户的日常生活的基本活动,并利用 2 个相机验证了这种攻击的可行性.

智能家居的出现给我们的生活带来了极大的便利.智能设备大多通过摄像头、麦克风、运动探测器等传感器来收集信息以便为人们提供更有用的服务,但是,设备在收集和传输信息的同时也可能增加了隐私安全风险.目前发现的攻击主要是针对设备自身特性和网络通信 2 方面进行分析,从而获得用户的隐私信息.智能家居的隐私泄露已经成为其被广泛应用的重要阻碍之一,用户对分享家庭活动的信息仍存在不同的担忧.因此,如何有效地抵抗侧信道分析攻击并提出切实可行的用户隐私保护方案至关重要.

2.3 通信安全

2.3.1 协议漏洞挖掘

通信协议安全是用户敏感信息传输保护的基础,发现通信协议的安全问题一直是网络安全研究的重点.在智能家居安全研究中,研究者主要关注于流行的 ZigBee, Bluetooth 等协议以及常用的 MQTT, CoAP 等应用层协议在配置和实施中的安全问题.

1) 物理层安全漏洞.物理层的协议主要解决的是物体互联以及接入网络的问题.其常用的协议有

物理层协议?

ZigBee、WiFi、蓝牙等. Cognose 公司[61]在 2015 年的黑客大会中指出由于 ZigBee 的标准协议支持不安全的初始密钥的传输,再加上部分制造商直接使用默认的链路密钥,使得黑客有机会从外部嗅出网络的交换密钥;为了将新设备快速接入到 ZigBee 网络,ZigBee 技术提供了轻触连接调试模式,Armknecht 等人[62]指出这种调试是不安全的,并利用该漏洞实现了对设备接管和数据的获取. Mathy 等人[63]采用“KRACK”密钥重装攻击演示了对 WPA2 的攻击,该攻击可攻陷所有的 WiFi 网络. 通过这种新型攻击,攻击者能够读取安全加密的信息. Qu 等人[64]揭露了部分通信协议在特定场景下使用是存在安全问题,例如在自动打开智能锁这一场景下,使用蓝牙低功耗(BLE)的传输范围作为物理邻近的验证是极为不安全的. Fouladi 等人[65]发现 Z-Wave 在应用于智能门锁时存在漏洞,利用该漏洞可以绕过密码直接打开门锁. Aghili 等人[66]证明了超轻量级 RFID 并不安全,并实现了对该协议的 DOS 和去同步攻击. 通过去同步攻击,攻击者可以得到用户隐私数据.

2) 应用层协议安全漏洞. 应用层的协议主要是用于应用之间的数据交换. MQTT 协议是一个即时通信的协议. Andy 等人[67]演示了多种针对 MQTT 协议的数据完整性、数据隐私和身份认证的攻击方案,如:对连接在 MQTT 公共服务器的客户端进行拒绝服务、嗅探及修改网络数据包等攻击. CoAP 协议是一种专门针对受限设备的传输协议,并很容易被转换成 HTTP 协议来与 Web 应用集成. Rathod 等人[68]发现 CoAP 代理存在安全漏洞,在其中以明文格式转换的数据易受攻击.

目前,智能家居设备通信没有统一的标准,各类协议都有各自的应用场景. 智能家居平台常在配置和实施这些协议时产生不规范行为,从而引发安全漏洞. 随着智能家居的流行,智能家居生产企业应更加重视协议的规范使用,研究者也需深入研究适用于智能家居场景的轻量级通信协议.

2.3.2 智能家居网络流量分析

网络流量分析是计算机信息安全研究的一个重要方法,它将一组设备产生的网络流量作为输入,将与这些设备、用户、应用程序或流量本身有关的信息作为输出. 分析智能家居系统的网络流量,了解网络流量特征与设备行为之间的关系,能够评估智能家居系统的安全状况,管控智能家居设备隐私泄露,缓解智能家居系统安全威胁,在网络层对智能家居系统进行安全管理.

智能家居系统网络流量分析的研究尚在起步阶段. Amar 等人[69]分析了智能家居设备的网络轨迹,并构建了一套设备行为指纹识别方法,从而能够评估设备的隐私安全风险. DeMarinis 等人[70]则根据网络流量分析结果构建了一套基于策略的恶意流量限制框架,能够提供智能家居系统网络层的安全性.

目前,智能家居系统网络流量分析相关研究仍不够深入,关键问题在于如何模拟真实的智能家居系统并得到大规模的网络数据,从而提高分析结果的准确性.

radio frequency identification, 射频识别, 非接触通信
dos, 磁盘操作系统
去同步, 指发送对已存在的系统结构进行攻击, 例如不断发送被篡改消息, 使系统放弃原本建立的体系结构

3 挑战与机遇

在深入调研现阶段智能家居安全在平台安全、设备安全、通信安全 3 方面研究现状的基础上,指出智能家居安全面临的六大挑战,并给出可用于应对这些挑战的安全技术机遇,其对应关系如表 4 所示:

Table 4 Security Research Challenges and Opportunities of Smart Home

表 4 智能家居的安全研究的挑战与机遇

Challenges	Opportunities
Lack of user authentication	Multi-user authentication scheme design
Defects of access control mechanism	Fine-grained access control mechanism design
Errors of trigger action rules	Detection of trigger action rules
Numerous vulnerabilities in device firmware	Device firmware vulnerability discover technology
Vulnerabilities in automatic speech recognition of smart speaker	Speech recognition security protection scheme design
Vulnerabilities in communication protocol	Secure communication protocol

细粒度

3.1 用户身份认证缺失

智能手机、平板电脑和智能手表等传统设备通常仅由单一用户使用,因而仅需完成单一用户身份认证. 然而,在智能家居场景下,多个用户会与单个智能家居设备进行交互,例如家庭的共享语音助手和互联网门锁均由多人使用. 因此在多用户场景下,

如何对用户身份进行认证成为了前所未有的研究问题. 同时,智能家居设备多为轻量级设备,它们缺乏屏幕、键盘等人机交互设施,这也为认证方案的设计带来了极大的挑战.

3.2 访问控制机制缺陷

设计良好的访问控制机制能够有效地保护设备敏感资源. 然而目前各智能家居平台的访问控制机制以智能手机的权限模型为基础,存在着权限粒度过粗的问题,威胁设备使用安全. 如何对智能设备敏感资源和操作进行分类分级,从而划分更细粒度的权限组,实施细粒度的访问控制机制成为了亟待解决的一大挑战.

3.3 设备联动规则错误

现有的智能家居平台均提供了设备联动功能,用户可根据自身需要对家中灯光、窗帘、空调等若干设备进行任意组合,形成自定义的设备联动规则,也可使用其他用户共享的联动规则. 然而,大量的设备联动规则存在着安全风险,多个设备同时触发执行多个操作可能存在着冲突及危险. 设备联动规则与用户期望的智能家居使用情景一一对应,挖掘设备联动规则的缺陷就需要充分考虑智能设备的功能特点,考虑设备组合使用的安全风险. 然而智能家居设备数量众多,功能各异,能够组合变化出无数的使用场景,如何对设备功能组合进行抽象,并建立模型对设备联动规则进行系统安全分析成为提高智能家居设备使用安全的一大关键挑战.

3.4 大量存在的设备固件漏洞

智能家居设备中存在着大量的内存漏洞和逻辑漏洞,然而目前的研究工作局限于 2 个方面:1)仅能对某种架构的设备固件进行挖掘,缺乏对多元架构固件的支持[71];2)仅能够挖掘特定类型的内存漏洞或逻辑漏洞,漏洞挖掘的种类少,效率低. 如何系统化的挖掘设备固件漏洞成为一大挑战,主要困难在于目前基于模拟器、基于符号执行等固件分析技术都无法支持多元化的构架. 此外,智能家居设备固件难以获取,通常智能家居供应商不会公开其设备固件. 若从主板中提取固件需要启用调试端口,但是许多设备并不开放这些调试端口.

3.5 智能音箱语音识别漏洞

智能音箱逐渐成为智能家居系统的控制中心,其语音识别系统的安全漏洞成为了攻击者关注的对象. 然而语音识别系统的安全漏洞与传统的软件安全漏洞有所不同,其漏洞源自算法设计时的固有问题. 例如目前的语音识别算法使用基于深度学习的语言模型,而深度学习算法存在误分类问题,攻击者能够利用此特点构造恶意的语音对抗样本,如何增强深度学习的泛化能力也是设计深度学习算法的一大挑战. 对于智能音箱的语音识别系统而言,语音识别系统包括了语音信号处理、特征提取、声学模型处理、语言模型处理等步骤,各层次都可能存在安全漏洞,如何设计一套安全防护方案成为了更重大的挑战.

3.6 通信协议安全漏洞

智能家居系统网络通信协议的漏洞主要来自于应用层,各平台在应用层设计了诸多不同的应用协议. 一旦攻击者发现协议层的安全漏洞,轻则可以进行信道窃听,重则可以远程控制设备. 目前大部分智能家居设备为受限设备,它们的计算、内存、通信资源不足,因而如何设计轻量级的安全通信协议成为了保护智能家居安全的一大挑战.

4 未来研究展望

根据第 3 节介绍的智能家居安全挑战与机遇,结合智能家居安全研究现状,我们指出 4 个未来的研究方向:

1) 多用户场景下认证与访问控制方案设计

随着智能家居产业的快速发展,智能摄像头、智能音箱、智能门锁等设备逐渐走进人们的家庭. 这些智能设备通常由家庭成员共同使用,在使用设备时需考虑对用户身份进行认证,否则会引发潜在的安全风险. 同时,不同身份的用户应该被授予不同的访问权限,例如孩子可以使用智能音箱播放歌曲,而不应使用音箱控制家中微波炉、烤箱等危险的电气设备,成人则应拥有完全的使用权限. 如何对多用户身份进行认证,如何授予不同用户访问权限,如何撤销、管理访问权限,如何设计细粒度的访问控制方案均需深入研究.

2) 设备联动规则错误检测

智能家居设备种类及功能不断增加,设备联动操作将覆盖越来越多的家居生活场景,用户根据生活需要也将自定义数目繁多的设备联动规则. 然而由于用户经验的不足,自定义的联动规则本身即有可能对用户安全与隐私造成威胁. 同时,众多的联动规则之间可能存在冲突操作. 如何检验联动规则的安全性及合理性,如何检测并消除联动规则之间的冲突操作需要得到研究人员的重视.

3) 设备固件漏洞挖掘技术

智能家居产品及其漏洞数量巨大,能够系统性

的挖掘智能家居设备漏洞意义重大.现阶段挖掘智能家居设备固件漏洞多依赖于人工分析设备固件,此种方法效率较低,而以往常用的模糊测试、污点分析、符号执行等漏洞挖掘技术均面临着不同的挑战,目前难以适用于固件漏洞挖掘.因此,如何构建固件模拟执行环境以利于动态漏洞挖掘,如何支持多元化架构的固件静态分析以利于静态漏洞挖掘成为了当前亟待解决的研究问题.

4)智能音箱语音识别漏洞挖掘与防护

智能音箱成为了智能家居设备的控制中心,其存在的安全漏洞对智能家居安全造成了极大的威胁.研究人员已发现了一些智能音箱语音识别系统的安全漏洞,并利用这些漏洞生成了人耳无法辨别的恶意语音命令.然而,智能音箱识别语音命令需经过语音信号处理、特征提取、声学模型处理、语言模型处理等一系列繁杂步骤,任一环节都可能潜藏安全漏洞,目前的研究尚不够充分.另一方面,研究人员需设计出一套易于实施的安全防护方案,能够高效的抵御恶意语音样本攻击.

5 总 结

关于智能家居系统安全的研究在逐渐增多,但其整体还处于起步阶段.本文在调研大量智能家居安全论文后,首先介绍了智能家居的发展历程及当前的系统架构.然后,我们以平台安全、设备安全、通信安全为主题阐述了智能家居安全研究现状.通过深入分析智能家居的安全问题以及现有研究工作的不足,指出了智能家居安全面临的挑战与机遇.最后对智能家居安全研究方向进行了展望,指出了多用户场景下认证与访问控制方案设计、设备联动规则错误检测、设备固件漏洞挖掘技术、智能音箱语音识别漏洞挖掘与防护等未来热点研究方向.

参 考 文 献

[1] Ministry of Industry and Information Technology. Internet of things "Twelfth Five-Year" development plan [EB/OL]. [2018-08-21]. http://www.gov.cn/zwgk/2012-02/14/content_2065999.htm(in Chinese)
(工业和信息化部.物联网"十二五"发展规划[EB/OL].[2018-08-21].http://www.gov.cn/zwgk/2012-02/14/content_2065999.htm)

[2] Ablondi W. 2018 global smart home forecast [EB/OL]. [2018-08-21]. https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/market-data/report-detail/2018-global-smart-home-forecast

[3] Cox E. Mirai IoT botnet: 5 fast facts you need to know [EB/OL]. [2018-08-21]. https://heavy.com/tech/2016/10/mirai-iot-botnet-internet-of-things-ddos-attacks-internet-outage-blackout-why-is-internet-down/

[4] Batalla J M, Vasilakos A, Gajewski M. Secure smart homes: Opportunities and challenges [J]. ACM Computing Surveys, 2017, 50(5): 75:1-75:32

[5] Yoon S, Park H, Yoo H S. Security issues on smarthome in IoT environment [M]. Berlin: Springer, 2015

[6] Robles R J, Kim T, Cook D, et al. A review on security in smart home development [J]. International Journal of Advanced Science and Technology, 2010, 15(2): 13-22

[7] 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)

[8] Tong Xiaoyu, Fang Bingyi, Zhang Yunyong. Internet of things smart home development analysis [J]. Mobile Communication, 2010, 34(9): 16-20 (in Chinese)
(童晓渝,房秉毅,张云勇.物联网智能家居发展分析[J].移动通信,2010,34(9):16-20)

[9] Postscapes. IoT cloud platform landscape [EB/OL]. [2018-08-21]. https://www.postscapes.com/internet-of-things-platforms

[10] iOS-Home-Apple. Siri makes your voice the on/off switch [EB/OL]. [2018-08-21]. https://www.apple.com/ios/home/

[11] Amazon. Amazon alexa [EB/OL]. [2018-08-21]. https://developer.amazon.com/zh/alexa

[12] Samsung. Smart home [EB/OL]. [2018-08-21]. https://www.samsung.com/us/smart-home/

[13] Xiaomi. Xiaomi IoT developer platform [EB/OL]. [2018-08-21]. http://home.mi.com/index.html (in Chinese)
(小米.小米IoT开发者平台[EB/OL].[2018-08-21].http://home.mi.com/index.html)

[14] Lévy-Bencheton C, Darra E, Tétu G, et al. Security and resilience of smart home environments [EB/OL]. [2018-08-21]. https://www.enisa.europa.eu/publications/security-resilience-good-practices

[15] Keranen A, Ersue M. Terminology for constrained-node networks [EB/OL]. [2018-08-21]. https://tools.ietf.org/html/rfc7228

[16] Kim S M, Choi H S, Rhee W S. IoT home gateway for auto-configuration and management of MQTT devices [C] //Proc of the 3rd IEEE Conf on Wireless Sensors. Piscataway, NJ: IEEE, 2015: 12-17

[17] Son S C, Kim N W, Lee B T, et al. A time synchronization technique for coap-based home automation systems [J]. IEEE Trans on Consumer Electronics, 2016, 62(1): 10-16

[18] Khan A A, Mouftah H T. Secured Web services for home automation in smart grid environment [C/OL] //Proc of the 25th IEEE Canadian Conf on Electrical & Computer Engineering. Piscataway, NJ: IEEE, 2012 [2018-08-21]. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6335018&isnumber=6334811

[19] Philips Home. Zigbee 3.0 support in Hue ecosystem [EB/OL]. [2018-08-21]. https://developers.meethue.com/zigbee3

[20] Wong V. Burger King's new ad will hijack your Google home [EB/OL]. [2018-08-21]. https://www.cnbc.com/2017/04/12/burger-kings-new-ad-will-hijack-your-google-home.html

[21] Pullen J P. Amazon echo owners were pranked by south park and their alexas will make them laugh for weeks [EB/OL]. [2018-08-21]. http://fortune.com/2017/09/14/watch-south-park-alexa-echo

[22] Yuan Xuejing, Chen Yuxuan, Zhao Yue, et al. CommanderSong: A systematic approach for practical adversarial voice recognition [OL]. [2018-08-21]. https://arxiv.org/pdf/1801.08535.pdf

[23] Zhang Jiansong, Wang Zeyu, Yang Zice. Proximity based IoT device authentication [C/OL] //Proc of the 36th IEEE Conf on Computer Communications. Piscataway, NJ: IEEE, 2017 [2018-08-21]. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8057145

[24] Liu Jing, Xiao Yang, Chen C L P. Authentication and access control in the internet of things [C] //Proc of the 32nd Int Conf on Distributed Computing Systems Workshops. Piscataway, NJ: IEEE, 2012: 588-592

[25] Wallrabenstein J R. Practical and secure iot device authentication using physical unclonable functions [C] //Proc of the 4th Int Conf on Future Internet of Things and Cloud. Piscataway, NJ: IEEE, 2016: 99-106

[26] Vaidya B, Park J H, Yeo S S, et al. Robust one-time password authentication scheme using smart card for home network environment [J]. Computer Communications, 2011, 34(3): 326-336

[27] Feng H, Fawaz K, Shin K G. Continuous authentication for voice assistants [C] //Proc of the 23rd Annual Int Conf on Mobile Computing and Networking. New York: ACM, 2017: 343-355

[28] 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] //Proc of the 39th IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2018: 836-852

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

[30] Lee S, Choi J, Kim J, et al. FACT: Functionality-centric access control system for IoT programming frameworks [C] //Proc of the 22nd ACM on Symp on Access Control Models and Technologies. New York, NY: ACM, 2017: 43-54

[31] Jia Yunhang, Chen Qi, Wang Shiqi. ContexIoT: Towards providing contextual integrity to appified IoT platforms [C/OL] //Proc of Network and Distributed System Security Symp. Reston: Internet Society, 2017 [2018-08-21]. http://web.eecs.umich.edu/~jackjia/material/contexiot_ndss17.pdf

[32] Rahmati A, Fernandes E, Eykholt K, et al. Tyche: Risk-based permissions for smart home platforms [OL]. [2018-08-21]. https://arxiv.org/pdf/1801.04609.pdf

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

[34] Fernandes E, Paupore J, Rahmati A, et al. FlowFence: Practical Data Protection for Emerging IoT Application Frameworks [C] / /Proc of the 25th USENIX Security Symp. Berkeley, CA: USENIX Association, 2016: 531-548

[35] IFTTT Platform. One connection, countless possibilities [EB/OL]. [2018-08-21]. https://platform.ifttt.com/

[36] Zapier. Zaps connect the apps you use every day [EB/OL]. [2018-08-21]. https://zapier.com/

[37] Microsoft. Automate processes + tasks—Microsoft flow [EB/OL]. [2018-08-21]. https://flow.microsoft.com/en-us/

[38] Fernandes E, Rahmati A, Jung J, et al. Decentralized action integrity for trigger-action IoT platforms [C/OL] //Proc of the 25th Network and Distributed Systems Symp (NDSS). Reston: Internet Society, 2018 [2018-08-21]. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_01A-3_Fernandes_paper.pdf

[39] 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. Geneva: International World Wide Web Conferences Steering Committee, 2017: 1501-1510

[40] Luo Hong, Wang Ruosi, Li Ximing. A rule verification and resolution framework in smart building system [C] //Proc of the 19th Int Conf on Parallel and Distributed Systems. Piscataway, NJ: IEEE, 2013: 438-439

[41] Maternaghan C, Turner K J. Policy conflicts in home automation [J]. Computer Networks, 2013, 57(12): 2429-2441

[42] Nandi C. Automatic trigger generation for end user written rules for home automation [C] //Proc of the 24th ACM SIGSOFT Int Symp on Foundations of Software Engineering. New York: ACM, 2016: 1109-1111

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

[44] Roy N, Shen Sheng, Hassanieh H, et al. Inaudible voice commands: The long-range attack and defense [C] //Proc of the 15th USENIX Symp on Networked Systems Design and Implementation Association. Berkeley, CA: USENIX Association, 2018: 547-560

[45] Carlini N, Mishra P, Vaidya T, et al. Hidden voice commands [C] //Proc of the 25th USENIX Security Symp. Berkeley, CA: USENIX Association, 2016: 513-530

[46] Vaidya T, Zhang Yuankai, Sherr M, et al. Cocaine noodles: Exploiting the gap between human and machine speech recognition [C/OL] //Proc of the 9th Workshop on Offensive Technologies. Berkeley, CA: USENIX Association, 2015 [2018-08-21]. https://www.usenix.org/system/files/conference/woot15/woot15-paper-vaidya.pdf

[47] Zhang Nan, Mi Xianghang, Feng Xuan, et al. Understanding and mitigating the security risks of voice-controlled third-party skills on Amazon alexa and Google home [OL]. [2018-08-21]. https://arxiv.org/pdf/1805.01525.pdf

[48] National Internet Emergency Center. Summary of China's Internet network security situation in 2017 [EB/OL]. [2018-08-21]. http://www.cac.gov.cn/2018-05/30/c_1122910613.htm (in Chinese)
(国家互联网应急中心. 2017年我国互联网网络安全态势综述[EB/OL]. [2018-08-21]. http://www.cac.gov.cn/2018-05/30/c_1122910613.htm)

[49] Ur B, Jung J, Schechter S. The current state of access control for smart devices in homes [C/OL] //Proc of Workshop on Home Usable Privacy and Security. New York: ACM, 2013 [2018-08-21]. http://cups.cs.cmu.edu/soups/2013/HUPS/HUPS13-BlaseUR.pdf

[50] Ronen E, Shamir A. Extended functionality attacks on IoT devices: The case of smart lights [C] //Proc of the 1st IEEE European Symp on Security and Privacy. Piscataway, NJ: IEEE, 2016: 3-12

[51] Shoshitaishvili Y, Wang Ruoyu, Hauser C, et al. Firmalice-automatic detection of authentication bypass vulnerabilities in binary firmware [C/OL] //Proc of the 22nd Network and Distributed System Security Symposium. Reston: Internet Society, 2015 [2018-08-21]. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/11_1_2.pdf

[52] Subramanyan P, Malik S, Khattri H, et al. Verifying information flow properties of firmware using symbolic execution [C] //Proc of Design, Automation and Test in Europe Conf and Exhibition. Piscataway, NJ: IEEE, 2016: 337-342

[53] Hernandez G, Fowze F, Tian D J, et al. Firmusb: Vetting USB device firmware using domain informed symbolic execution [C] //Proc of the 2017 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2017: 2245-2262

[54] Muench M, Stijohann J, Kargl F, et al. What you corrupt is not what you crash: Challenges in fuzzing embedded devices [C/OL] //Proc of the 25th Network and Distributed System Security Symp. Reston: Internet Society, 2018 [2018-08-21]. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_01A-4_Muench_paper.pdf

[55] Chen Jiongyi, Diao Wenrui, Zhao Qingchuan, et al. IoTFuzzer: Discovering memory corruptions in IoT through app-based fuzzing [C/OL] //Proc of the 25th Network and Distributed System Security Symp. Reston: Internet Society, 2018 [2018-08-21]. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_01A-1_Chen_paper.pdf

[56] Xu Yi, Frahm J M, Monrose F. Watching the watchers: Automatically inferring TV content from outdoor light effusions [C] //Proc of 2014 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2014: 418-428

[57] Barbosa P, Brito A, Almeida H. Defending against load monitoring in smart metering data through noise addition [C] //Proc of 2015 ACM Symp on Applied Computing. New York: ACM, 2015: 2218-2224

[58] Fafoutis X, Marchegiani L, Papadopoulos G Z, et al. Privacy leakage of physical activity levels in wireless embedded wearable systems [J]. IEEE Signal Processing Letters, 2017, 24(2): 136-140

[59] Copos B, Levitt K, Bishop M, et al. Is anybody home? Inferring activity from smart home network traffic [C] //Proc of Security and Privacy Workshops. Piscataway, NJ: IEEE, 2016: 245-251

[60] Li Hong, He Yunhua, Sun Limin, et al. Side-channel information leakage of encrypted video stream in video surveillance systems [C/OL] //Proc of the 35th IEEE Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2016 [2018-08-21]. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7524621

[61] Zillner T, Strobl S. Zigbee exploited, the good, the bad and the ugly [EB/OL]. [2018-08-21]. https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf

[62] 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. New York: ACM, 2017: 230-240

[63] Vanhoef M, Piessens F. Key reinstallation attacks breaking WPA2 by forcing nonce reuse [EB/OL]. [2018-08-21]. https://www.krackattacks.com/

[64] Qu Yanzhen, Chan P. Assessing vulnerabilities in bluetooth low energy (BLE) wireless network based IoT systems [C] //Proc of IEEE Int Conf on Big Data Security on Cloud. Piscataway, NJ: IEEE, 2016: 42-48

[65] Fouladi B, Ghanoun S. Security evaluation of the Z-Wave wireless protocol [EB/OL]. [2018-08-21]. https://sensepost.com/cms/resources/conferences/2013/bh_zwave/Security%20Evaluation%20of%20Z-Wave_WP.pdf

[66] Aghili S F, Ashouri-Talouki M, Mala H. DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT [J]. Journal of Supercomputing, 2018, 74(1): 509-525

[67] Andy S, Rahardjo B, Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system [C/OL] //Proc of Int Conf on Electrical Engineering, Computer Science and Informatics. Piscataway, NJ: IEEE, 2017 [2018-08-21]. http://journal.portalgaruda.org/index.php/EECSI/article/view/1064/627

[68] Rathod D, Patil S. Security analysis of constrained application protocol (coap): IoT protocol [J]. International Journal of Advanced Studies in Computers, Science and Engineering, 2017, 6(8): 37

[69] Amar Y, Haddadi H, Mortier R, et al. An analysis of home IoT network traffic and behaviour [OL]. [2018-08-21]. https://arxiv.org/pdf/1803.05368.pdf

[70] DeMarinis N, Fonseca R. Toward usable network traffic policies for IoT devices in consumer networks [C] //Proc of the 2017 Workshop on Internet of Things Security and Privacy. New York: ACM, 2017: 43-48

[71] 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)

Wang Jice, born in 1992. PhD candidate in the University of Chinese Academy of Sciences. His main research interests include network and system security.

Li Yilian, born in 1996. Master candidate in Xidian University. Her main research interests include network and information security(liyl@nipc.org.cn).

Jia Yan, born in 1992. PhD candidate in Xidian University. His main research interests include network and information security(jiay@nipc.org.cn).

Zhou Wei, born in 1993. PhD candidate in the University of Chinese Academy of Sciences. His main research interests include network and system security (zhouw@nipc.org.cn).

Wang Yucheng, born in 1995. Master candidate in Xidian University. His main research interests include network and information security (wangyc@nipc.org.cn).

Wang He, born in 1987. PhD, lecturer in Xidian University. Her main research interests include network and information security (wangh@nipc.org.cn).

Zhang Yuqing, born in 1966. PhD. Professor in the University of Chinese Academy of Sciences. His main research interests include network and information system security(zhangyq@nipc.org.cn).