计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170470
54(10):2130-2143,2017

物联网安全综述

张玉清　周　威　彭安妮
(国家计算机网络入侵防范中心(中国科学院大学)　北京　101408)
(zhangyq@nipc.org.cn)

Survey of Internet of Things Security

Zhang Yuqing, Zhou Wei, and Peng Anni
(*National Computer Network Intrusion Protection Center* (*University of Chinese Academy of Sciences*), *Beijing* 101408)

Abstract　With the development of smart home, intelligent care and smart car, the application fields of IoT are becoming more and more widespread, and its security and privacy receive more attention by researchers. Currently, the related research on the security of the IoT is still in its initial stage, and most of the research results cannot solve the major security problem in the development of the IoT well. In this paper, we firstly introduce the three-layer logic architecture of the IoT, and outline the security problems and research priorities of each level. Then we discuss the security issues such as privacy preserving and intrusion detection, which need special attention in the IoT main application scenarios (smart home, intelligent healthcare, car networking, smart grid, and other industrial infrastructure). Though synthesizing and analyzing the deficiency of existing research and the causes of security problem, we point out five major technical challenges in IoT security. They are privacy protection in data sharing, the equipment security protection under limited resources, more effective intrusion detection and defense systems and method, access control of equipment automation operations and cross-domain authentication of motive device. We finally detail every technical challenge and point out the IoT security research hotspots in future.

Key words　Internet of things; security; privacy; intelligent; survey; challenge

摘　要　随着智能家居、数字医疗、车联网等技术的发展,物联网应用越发普及,其安全问题也受到越来越多研究者的关注.目前,物联网安全的相关研究尚在起步阶段,大部分研究成果还不能完善地解决物联网发展中的安全问题.首先对物联网3层逻辑架构进行了介绍,阐述了每个层次的安全问题与研究现状重点;然后分析并讨论了物联网的主要应用场景(智能家居、智能医疗、车联网、智能电网、工业与公共基础设施)中需要特别关注的隐私保护、入侵检测等安全问题;再次,归纳分析了现有研究工作中的不足与安全问题产生的主要原因,指出物联网安全存在的五大技术挑战:数据共享的隐私保护方法、有限资源的设备安全保护方法、更加有效的入侵检测防御系统与设备测试方法、针对自动化操作的访问控制策略、移动设备的跨域认证方法;最后,通过详尽分析这五大技术挑战,指出了物联网安全未来的研究方向.

收稿日期:2017-06-12;**修回日期**:2017-07-26
基金项目:国家自然科学基金项目(61572460,61272481);国家重点研发计划项目(2016YFB0800703);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项目[(2012)1424];国家111项目(B16037)
This work was supported by the National Natural Science Foundation of China (61572460, 61272481), the National Key Research and Development Program of China (2016YFB0800703), 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], and the China 111 Project (B16037).

关键词 物联网;安全;隐私;智能;综述;挑战

中图法分类号 TP393

自 2005 年国际电信联盟正式提出物联网(Internet of things, IoT)概念以来,传感器网络、云计算、微型芯片等技术不断发展成熟,物联网产业也迅速发展扩大.根据 Statista 门户网站最新统计数据[1],2016 年互联设备数量已经达到 176 亿,预计到 2020 年突破 300 亿.国际数据公司预测,到 2020 年物联网市场规模将会突破 7 万亿美元[2].

在物联网飞速发展的同时,其安全面临着严峻挑战.物联网安全问题不仅能给用户带来财产损失,甚至会威胁用户的生命安全.2016 年前 FBI 美国信息安全专家发现,现阶段市场上的心脏起搏器和胰岛素泵等无线嵌入式医疗设备普遍存在可利用的安全漏洞[3].物联网安全也是国家安全和社会稳定的基石.2010 年曝光的震网病毒[4]对多国核电站、水坝、国家电网等工业与公共基础设施造成了大规模的破坏.2016 年 mirar 僵尸网络通过控制大量的物联网设备对美国域名解析服务提供商 Dyn 公司发动 DDOS 攻击,造成美国东部大面积断网,许多热门网站停止服务[5].

目前,国家、企业和个人尚未树立起足够的物联网安全与隐私保护意识.Pew 研究中心 2016 年的统计数据表明[6],52%的用户同意将其个人医疗设备收集的健康数据与医生共享,44%的用户可接受厂商利用恒温器中的传感器收集其家中每个房间的温度.同时,大部分的厂商认为额外的安全措施不会提高设备自身的市场价值只会增加其生产成本[7],因此许多厂商在产品销售后并不为用户提供补丁和更新服务.从而导致现有物联网设备长期存在默认口令、明文传输密钥等[8]大量易利用的高危漏洞.

通过调研近年网络与信息安全领域的论文,我们发现物联网安全相关研究成果逐渐增多,但其中大多数研究成果的适用范围较窄,应用价值不高.目前很少有研究者提出具有前瞻性且广泛适用的物联网安全措施.由于物联网研究范围十分宽泛,其安全问题也繁多杂乱,现有物联网安全调研报告[9-10]主要存在两大问题:

1) 讨论问题不全面

现有物联网安全调研报告大多从应用场景、逻辑层次和安全属性等单一角度来分类讨论物联网安全问题.但是物联网涵盖的内容较为分散,所以仅从某一个角度讨论物联网安全问题,无法全面了解物联网各个方面安全研究现状.

2) 缺乏对物联网安全问题的深入分析

现有的物联网安全调研报告大多仅指出物联网现阶段的安全问题,并没有深入分析产生这些安全问题的根本原因.同时,这些报告也未指出解决这些安全问题所需克服的技术难点,无法为研究者提供具有指导意义的研究方向.

为解决上述两大问题,本文对 2012 年至 2017 年上半年已发表的大量物联网安全相关论文进行了充分调研.

1 物联网架构安全研究现状

本节首先介绍物联网架构层次,然后分层次讨论其安全问题与研究现状.

1.1 物联网逻辑架构简介

无论是最新提出面向服务的物联网架构[11],还是将应用层进一步划分的 4 或 5 层物联网架构[12],其本质均可分为 3 个逻辑层次.其从下至上依次为:感知层(sensing)、传输层(transport)和应用层(application),如图 1 所示.

感知层是所有数据的来源,从智能标签 RFID、GPS、环境传感器、工业传动器、摄像头等各种各样的智能设备中获取原始数据.物联网发展的最终目标是实现万物互联,所以感知层的目标是全面感知和收集所需的外界信息.这里特别注明学术界常把传感器网络归于感知层,但通过调研发现传感器网络的主要安全任务是传感器节点间信息安全传输,其与传输层的安全任务更为一致.所以本文把传感器网络的安全问题划分到传输层去讨论.

传输层通过各种有线和无线的网络通信技术(无线网络、有线宽带、移动网络等)把感知层收集的信息安全可靠地传输到应用层.主要包含两大安全任务:1)单一网络内部的信息安全传递问题;2)不同网络之间的信息安全传递的问题.

应用层的主要工作可以抽象概括为 2 个:

1) 云端数据聚合与智能处理

首先应用层中的云服务平台将从传输层接收到的数据进行智能处理,即对海量分布式信息进行数

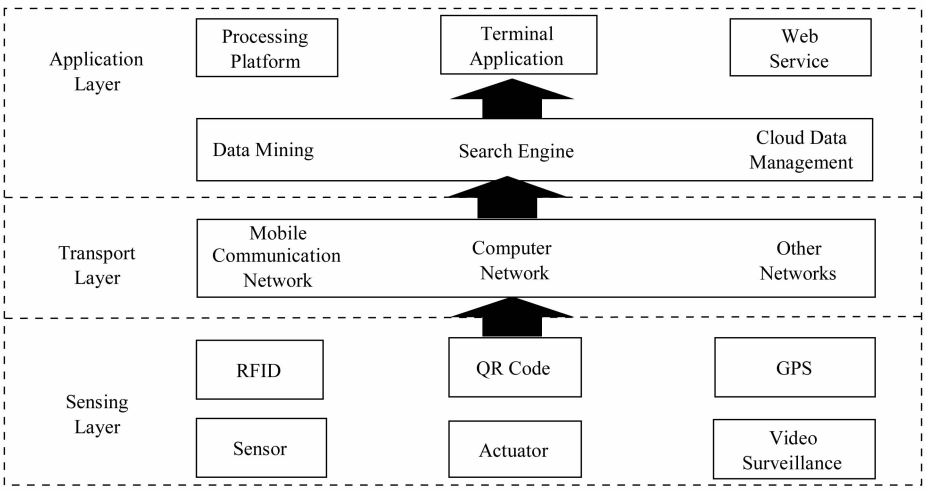

Fig. 1 Logical architecture for IoT

图 1 物联网逻辑架构

据清理并提炼出含有较高信息量的数据. 其主要技术包括搜索引擎、数据挖掘和云数据管理与共享等.

2) 应用平台为用户提供服务

云端将处理后的数据传输给用户、企业和管理部门对应的服务程序(如远程医疗 Web 服务、管理智能家居设备的 APP、智能交通的信息监控与处理平台等),然后由这些应用平台利用这些数据为用户提供所需服务. 需要注意:生活中提及的智能家居、智能交通、智能电网等物联网应用场景,并不直接对应物联网架构中的应用层的应用. 这些应用场景是建立在完整的 3 层物联网架构之上的. 这里应用层对应的只是这些应用场景中经过感知层收集数据和传输层传输数据后展示给用户的服务程序.

1.2 感知层安全问题与研究现状

通过 1.1 节介绍可知,感知层主要负责数据收集,所以其安全措施也是围绕如何保证收集数据的完整性、机密性、可鉴别性来展开. 为了实现这个目标,感知层的主要安全任务除了保障物联网感知层设备的物理安全和系统安全,还需为传输层安全通信提供基础保障. 本节将分别围绕这 3 个主要安全任务进行讨论.

1) 感知层设备的物理安全会比之前的传统计算机受到更为严重的威胁. 因为农业和工业环境中的传感器分布较广,若传感器运转正常可能长时间无人进行检查,很可能被敌手直接捕获[13];对于小型家用和医疗的智能设备,攻击者更加可以容易对其进行侧信道分析[14-17]. 同时,智能医疗设备、穿戴设备和智能家居设备等会比传统的个人计算机收集到更多敏感隐私数据. 香港大学安全研究人员通过侧信道分析智能手表中移动加速度传感器收集的数据,实现对用户击键行为的成功预测[14]. 还有研究人员通过侧信道分析智能插座的用电量来推断与其连接电脑上的运行程序[18].

2) 感知层设备受资源所限,只能执行少量的专用计算任务,没有足够的剩余资源用于实现细粒度的系统安全措施. 此外许多工控专用设备其程序与系统依赖于特定的硬件架构,传统的访问控制、沙箱、病毒查杀等系统防御技术无法在这些特定设备上实现. 这些因素都导致目前感知层设备的系统十分薄弱. Costin 等人[19]通过分析大量的嵌入式设备系统固件,发现了许多可利用的高危系统漏洞. 有研究人员提出在嵌入式系统中建立轻量级可信执行环境来保护其系统安全[20],但该方法计算开销较大,适用范围有限. 还有研究人员设计了针对小型嵌入式设备系统的测试框架[21]. 但静态测试与漏洞检测方法无法实时动态保护嵌入式设备的系统安全.

3) 感知层设备在利用传输层的协议进行通信时,必然需要为传输层安全通信提供基础保障. 主要包括通信密钥生成、设备身份认证以及数据溯源等. 同样由于感知层设备资源有限,经典的加密、认证以及其他密码算法直接部署在传感器等小型嵌入式设备上会严重降低设备处理效率,大幅增加设备功耗. 大部分研究人员通过设计轻量级密码学算法[22-24]或优化经典密码学算法实现方法[25]来解决这一难题. 还有研究人员提出了一些创新性的思路来解决这一难题. Majzoobi 和 Hiller 研究团队分别提出基于设备自身独特的物理特性(physical unclonable functions, PUF)的认证[26]和密钥生成协议[27],该方法不仅节

省了单独存储密钥的设备资源,而且可以有效抵御侧信道分析.也有研究人员利用穿戴设备获取的用户人体生物的特征如步态[28]、滑动屏幕力度[29]等来实现设备认证,该方法在节省资源的同时还可实现了设备和使用者的双重认证.

综上,感知层3个方面的安全要求是相互依赖的,任何一个方面出现漏洞都会引发安全问题.例如有研究人员通过侧信道分析基于心率生成密钥的电信号信息熵[16],从而还原了用户心率信息获取了通信密钥.所以需要全面考虑感知层设备各个方面的安全要求以及相互之间的影响,才能设计出有效的安全防御策略.

1.3 传输层安全问题与研究现状

传输层主要负责安全高效地传递感知层收集到的信息.因此传输层主要是各种网络设施,即包括小型传感器网络也包括因特网、移动通信网络和一些专业网络(如国家电力网、广播网)等.

传感器网络是物联网的基础网络,传感器设备收集的数据首先都要通过传感器网络才能向上传递给其他网络.同时,传感器网络与传统计算机网络有着许多不同,因此传感器网络的安全问题也成为近些年物联网安全研究的热点之一.首先由于传感器网络节点资源有限,特别是电池供电的传感器设备,很容易对其直接进行拒接服务(DoS)攻击,造成节点电量耗尽[30].另外传感器节点分布广泛数目众多,管理人员无法确保每个节点的物理安全.敌手可直接捕获传感器节点进行更加深入的物理分析,从而获取节点通信密钥等.特别一旦传感网关节点被敌手控制,会使整个传感器网络安全性全部丢失.现有许多研究人员通过对密码学算法与协议进行的轻量化[31-33]处理来抵御传感器网络攻击.但这些轻量级算法与协议大多缺乏对设备电量和网络带宽消耗的测试,适用性有待提高.

虽然现阶段对传输层通信网络的攻击仍然以传统网络攻击(如重放、中间人、假冒攻击)等为主.但仅仅抵御这些传统网络攻击[34-35]是不够的,随着物联网的发展,传输层中的网络通信协议会不断增多.当数据从一个网络传递到另外一个网络时会涉及到身份认证、密钥协商、数据机密性与完整性保护等诸多问题.因此面临的安全威胁将更加突出需要研究人员更多地关注[36-37].

1.4 应用层安全问题与研究现状

通过1.1节的介绍可知,应用层需要对收集的数据完成最终的处理和应用.而数据处理与应用的过程都需要对应的安全措施保护.

对于云端数据智能处理平台进行数据统计分析来满足应用程序使用的同时需要防止用户隐私信息泄露.现阶段学术界主要采用同态加密来解决这一矛盾[38-39].同态加密的数据进行处理得到一个输出,将这一输出进行解密,其结果可以保证与用同一方法处理未加密的原始数据得到的输出结果是一样的.但全同态加密算法效率还有待提高,而部分同态加密算法可对加密数据进行的处理十分有限.保护用户隐私的同时,提高了服务器处理效率.有研究人员提出可以根据应用程序对数据的用途不同以及数据的敏感程度不同,对原始数据采用不同的处理方法[40].如为了防止心率等医疗数据被篡改可采用Hash算法;为了统计用户的用电量而不泄露其具体信息可采用同态加密算法;对于无需计算的隐私数据可采用数据混淆的方法[41].同时由于云服务器会保存大量的用户数据,云服务数据的存储[42]、审计[43]与恢复[44]以及共享[45-46]都需要更多的安全措施来保护.Thomas和Ned利用区块链技术在实现物联网设备匿名共享的方法[47]值得学习与借鉴.此外物联网设备数目的增多使得DDOS攻击的规模将会大幅提升,云端服务器还需要提高抵御DDOS攻击[48]的能力.

对于应用服务程序,其与用户联系最为紧密,所以其最重要的安全任务是在提供服务的同时保护用户隐私信息[49].Fernandes等人[50]通过分析程序源码发现50%以上的三星智能家居平台上的应用都具有不必要的权能,可导致用户敏感数据泄露或智能家居设备被恶意控制.现有研究人员为保护程序中的敏感操作和隐私数据[51-52]设计了多种访问控制模型,但其适用性和安全性均有待进一步提高.

1.5 小 结

以上虽然是分层次讨论了物联网架构中的安全问题,但各个层次的安全问题并不是相互独立而是相互依赖.最主要体现在数据隐私保护方面,任何一个环节出现问题都会使用户的隐私数据泄露.目前,研究人员提出了许多针对物联网设备的测试框架、安全评估模型以及入侵检测防御系统等.但这些框架与工具可检测出的安全问题并不全面,适用范围有限.

本文统计了2012—2017年上半年中国计算机学会网络安全领域CCF A类和CCF B类会议与期刊164篇论文的讨论主题(剔除了调研类的文章),列出各个层次中讨论次数较多的研究热点,如表1所示.

Table 1 Research Hotspots in Each Level of IoT Layers

表 1 物联网逐层次的研究热点

Layer	Academic Concerns
Sensing (54 papers)	① Lightweight Cryptography Algorithm ② Embedded System Defense Technology ③ Side Channel Attack and Defense ④ Cryptographic Algorithm Based on Biometrics and Device Physical Characteristics
Transport (77 papers)	① Sensor Network ② Privacy Data Protection in Communication Protocols ③ Secure Communication Protocol Against Remote Attacks (Middleman, Replay, DOS, etc.)
Application (50 papers)	① Privacy Data Protection in Application ② Equipment and Application Testing Framework in the Internet of Things ③ Intrusion and Defense Detection System

Note: Some researches involve multiple layers.

2 物联网常见应用场景安全问题与研究现状

现阶段物联网应用场景逐渐增多,不同应用场景需求目标不同,应用技术也不尽相同,故各应用场景对应的安全任务侧重点并不相同. 如果仅按层次整体讨论物联网安全现状[9],则无法全面深入地了解各个物联网应用场景的安全问题. 所以本节将分别从智能家居、智能医疗、智能交通、智能电网以及工业与公共基础设施五大物联网应用场景深入讨论其安全问题与研究重点.

2.1 智能家居

智能家居越发普及的同时,各种智能家居设备保存与传输的用户隐私信息也越来越多. 这些隐私信息不仅包含传统意义上那些银行卡、手机号等身份信息,还包含用户日常生活的行为隐私信息. 如温度传感器记录了家中内各个房间的实时温度信息[53];网络摄像头可以直接远程实时查看家中的状况. 攻击者通过控制这些智能家居设备,从而实现对用户隐私行为的监控. Johannes 和 Martin 就分析市场上主要型号的网络摄像头,发现了大量可轻易利用的安全问题包括弱口令、HTTP 明文传输[54]等. 此外用户隐私保护意识普遍较低,厂商对于设备收集哪些用户隐私数据也无明确声明,加剧了智能家居设备隐私信息泄露的问题[13].

综上所述,智能家居设备首要安全工作是保护用户的隐私数据. 研究人员大多通过监控智能家居终端应用[55]的控制流与数据流来防止隐私数据泄露,但该方法忽视了智能家居设备间的互用问题. 例如市场上有些智能窗户控制器会根据温度传感器收集的室温自动打开或关闭窗户. 在上述情景下敌手仅需控制温度传感器的温度值,从而间接实现对智能窗户的控制[56].

2.2 智能医疗

在智能医疗领域,数据和设备安全显得尤为重要. 因为医疗设备尤其是胰岛素泵[57]、心脏起搏器[4]等人体嵌入式设备[58]一旦被恶意控制会严重威胁用户的生命安全. Martin 调研了大量的智能医疗设备发现其存在弱密钥、过期证书等诸多的安全漏洞[59]. 为了给用户提供更加全面、及时、专业的医疗服务,智能医疗设备的隐私信息会共享给诸多医疗单位,但同时也加剧了用户医疗隐私信息泄露的风险[60]. 此外,针对远程医疗服务平台的网络攻击也逐渐增多,甚至勒索软件也开始将智能医疗设备[61]与医院数据库[62]作为主要攻击目标.

研究人员为提高智能医疗设备的安全性,提出了针对智能医疗设备的专用测试框架[59]以及恶意程序的软[63]、硬[61]件检测方法. 为了防止医疗隐私数据泄露,Duffy 等人提出针对医疗数据使用人员不同,对隐私数据采取不同的保护处理方法. 例如对统计人员提供同态加密的数据,对医生提供只可读不可写的数据等[64]. 董晓蕾设计了动态可撤销权能的多级隐私保护模型[65],可以实施更加灵活的医疗隐私数据保护策略. 同时,对智能医疗设备行为进行可信记录,也有利于及时发现对其的网络攻击行为. Henry 等人通过在胰岛素泵上增加可检测人体进食后肠道生物特征的电路模块,从而判定胰岛素泵的异常行为是否由网络攻击造成[57]. 在未来智能医疗设备生产中可以参考这样的设计方法,增加对设备行为的可信记录模块.

随着人均寿命普遍延长慢性病人数逐渐增多,智能医疗设备会越发普及. 提高智能医疗设备的安

全性显得尤为重要.一旦无法保障医疗设备的安全,医生与病人自然会对智能医疗服务望而却步,严重阻碍智能医疗的推广与发展.

2.3 智能汽车

随着市场上联网的智能汽车逐渐增多,现实中对智能汽车的电子攻击也层出不穷[66].PT&C|LWG 司法咨询服务公司指出 2013 年在伦敦被盗的汽车中 47%的汽车是通过电子攻击来窃取的[67].而受到攻击次数越多的汽车,其联网的部件也越多.文献[68-69]的研究也指出现阶段智能汽车普通存在大量安全漏洞.

目前由于汽车系统固件为厂商所有,一般并不开源.所以学术界重点关注控制器局域网总线技术[70]以及 V2X[71]等智能汽车与其他设备通信技术的安全问题.此外,智能汽车云服务的隐私泄露问题[72]也引起了许多研究人员的关注.

随着车联网技术的发展,预估到 2020 年 60%~75%的汽车都将具有 Web 服务[66],无线联网的汽车数量将达到 1.5 亿.智能汽车的安全将面临更加严峻的挑战.为了全面提高智能汽车的安全性,需要厂商和研究人员更加深入的合作才能设计出更加全面实用的安全防御措施.

2.4 智能电网

智能电网是最早应用于公共基础设施上的物联网技术,其安全研究也开始较早,研究成果较多.故本节先讨论智能电网安全研究现状,在第 2.5 节再讨论其他工业与公共基础设施的安全问题.

早期智能电网的安全研究重点关注智能电网的实时电价调整协议[73]以及其他通信协议的安全问题[74].随着智能电网技术不断发展,更短时间间隔的使用电量信息被统计收集,这些信息与用户用电行为的相关程度逐渐升高.此外,Dimitriou 和 Karame 发现不仅用电信息会泄露用户用电行为,智能电网计划分配给用户的电量信息也会泄露用户的用电习惯[75],故对用户用电信息的隐私保护的研究逐渐增多.研究者大多利用之前提及的同态加密等密码学的算法[76-78]在不影响用电信息统计的前提下,实现用户用电信息的隐私保护.

在未来不只是智能电表、智能水表和智能燃气表等其他智能抄表设备收集的用量信息会泄露更多的用户生活隐私.研究人员需要提前防范智能抄表带来的用户隐私泄露问题.

2.5 工业与公共基础设施

这里讨论的智能工业与公共基础设备主要包括闭路电视、数字视频记录仪等视频监控系统以及监测控制与数据采集[79]等工业控制系统[80].

震网病毒[4]的出现使工业与公共基础设备的信息安全面临更加严峻的挑战.由于工业设备在设计之初没有考虑受到网络攻击的可能,所以当工业设备联网后会受到更加严重的网络攻击威胁[81].Luiijf[82]还指出工业设备的设计与操作人员普遍存在侥幸心理,认为攻击者不具备相关专业知识无法实施网络攻击.此外,这些设备专用于完成特定的工业任务,其软硬件架构与传统计算机均不相同.普通计算机系统防御措施如防火墙、杀毒软件等[83],无法直接应用于上述设备,而单独为每种设备设计相应的系统防御措施开销过高.

现阶段的安全研究人员主要通过设计入侵检测与防御系统来提高工业与公共基础设备的安全性.有研究人员指出[84-85]由于工业设备的异构性,常用的基于通信网络中异常行为进行模式匹配的入侵检测方法,漏报率过高并不适用于工业系统.为了更加有针对性地保护关键工业设备,应该首先统计分析对关键设备的控制命令参数,从而确定其正常的值域范围;然后将其用来与实时通信流量中的控制命令参数进行比较,任何实际观察值在正常值范围之外时,就认为有入侵发生.Colbert 等人[86]进一步指出为了提高入侵检测的准确率,对于关键参数的值域范围还需参考专业的操作人员和设计专家的意见进行人工辅助确定.Henry 研究团队[87]总结了现有的许多工业设备入侵检测模型,对未来设计更加有效的入侵检测模型有很高的参考价值.

随着工业和公共基础设施中联网设备数目的增多,其所受到的网络攻击也将逐渐增多[88].但现阶段的工业与公共基础设备普遍缺乏网络与系统安全保护措施[89-91].如何有效检测与防御对这些专用设施的网络攻击需要更加深入的研究.

2.6 小 结

随着物联网技术的发展,物联网应用范围会愈发广泛.此外,诸如电动车与智能电网交互供电(vehicle-to-grid, V2G)等跨场景物联网应用技术,在节约能源与方便用户生活的同时,也带来了更多的安全与隐私泄露问题[92-93].有效解决物联网应用场景中的安全问题将对未来物联网应用设计与发展起着重要作用.

本文从 1.5 节调研的物联网安全相关论文中选取与特定场景相关的论文,然后统计智能家居(smart home)、智能医疗(digital healthcare)、智能

汽车(intelligent vehicles)、智能电网与其他工业与公共基础设施(smart grid and industrial public infrastructure)各场景中的研究热点,如表 2 所示.

因为智能电网也属于工业与公共基础设施,且单独讨论工业和公共基础设备安全的论文较少,所以表 2 中将这 2 个场景的研究热点划为一类进行统计.

Table 2 Research Hotpots in Each Application Domain of IoT

表 2 每个应用场景下的研究热点

Application Scenarios	Academic Concerns
Smart Home (22 papers)	① Privacy Data Protection and Anonymity ② Authorization Management and Access Control ③ Security Testing Framework ④ Security of Embedded System
Digital Healthcare (17 papers)	① Privacy Data Protection ② Security Application Based on Biometrics ③ Security Communication Protocol
Intelligent Vehicles (8 papers)	① Security Communication Protocol ② Privacy Data Sharing
Smart Grid and Industrial Public Infrastructure (42 papers)	① Intrusion Detection and Defense System ② Sensor Network ③ Security Testing Framework

3 五大物联网安全技术挑战

本节将根据学术界关心的物联网安全问题及现有研究工作的不足,指出未来急需应对的物联网安全挑战. 首先,在之前讨论的物联网安全现状基础上总结出学术界关注的十大物联网安全热点问题,其分布对应的应用场景与逻辑层次如表 3 所示:

Table 3 Security Concerns Correspond to the Hierarchy and the Main Application Domain

表 3 安全问题对应的所属层次与主要应用场景

Security Concerns	Layers	Application Scenarios
① Privacy Concerns	ALL	Smart Home, Digital Healthcare, Intelligent Vehicles, Smart Grid
② Insecure Cryptographic Algorithm/Protocol	Sensing, Network	ALL
③ Insecure Network Communication	Network	ALL
④ Insecure Cloud/Web/Mobile Interface	ALL	Smart Home, Digital Healthcare, Intelligent Vehicles, Smart Grid
⑤ Insecure Software/Firmware	Sensing, Application	ALL
⑥ Insufficient Authentication	ALL	ALL
⑦ Insufficient Access Control/Authorization	ALL	Smart Home, Digital Healthcare
⑧ Poor Physical Security	Sensing	Industrial Public Infrastructure
⑨ Poor Embedded System Security	Sensing	Industrial Public Infrastructure, Digital Healthcare
⑩ Insufficient Security Configurability	Network, Application	ALL

然后,将本文总结的近年学术界关注的安全问题按热度排序后与 2014 年 OWASP 组织总结的物联网十大安全威胁[94]进行对比(如表 4 所示),可发现十大安全问题基本一致但顺序发生了较大变化,其主要原因有 2 点:

1) 近年来随着智能家居、智能医疗设备的增多,导致隐私的问题比 2014 年前更加严重. 同时,随着厂商安全意识提高以及物联网设备安全测试工具[95]增多,不安全的 Web 服务数量有了明显下降.

2) 学术界更加关注可以通过技术手段解决的安全问题,而 OWASP 组织更加关注现实中最容易被攻击者利用的安全问题. 例如学术界研究的侧信道与系统攻击,但实际应用中实现难度较高. 故物理安全问题和系统安全问题在学术界安全问题中的排序比 OWASP 安全问题中的排序位置靠前. 而 Web 服务漏洞以及不安全的网络认证和授权更容易被敌手利用,故这些问题在 OWASP 安全问题中的排序比学术界安全问题中的排序位置靠前.

Table 4 Academic Concerns and OWASP IoT TOP10

表 4 2012—2016 学术界与 2014 OWASP 物联网十大安全问题

2012—2016 Academic Concerns	2014 OWASP IoT TOP10
① Privacy Concerns	① Insecure Web Interface
② Insecure Cryptographic Algorithm/Protocol	② Insufficient Authentication/Authorization
③ Insecure Network Communication	③ Insecure Network Services
④ Insecure Cloud/Web/Mobile Interface	④ Lack of Transport Encryption
⑤ Insecure Software/Firmware	⑤ Privacy Concerns
⑥ Insufficient Authentication	⑥ Insecure Cloud Interface
⑦ Insufficient Access Control/Authorization	⑦ Insecure Mobile Interface
⑧ Poor Physical Security	⑧ Insufficient Security Configurability
⑨ Poor Embedded System Security	⑨ Insecure Software/Firmware
⑩ Insufficient Security Configurability	⑩ Poor Physical Security

进一步分析上述安全问题产生原因,并由此总结出五大急需应对的物联网安全技术挑战分别为:数据共享的隐私保护方法(privacy preserving in data sharing)、有限资源下的设备安全保护方法(the equipment security protection with limited resources)、更加有效的入侵检测防御系统与设备测试方法(more effective intrusion detection and defense systems and test method)、针对自动化操作的访问控制策略(access control of equipment automation operations)、移动设备的跨域认证方法(cross-domain authentication of motive device).上述五大安全技术挑战其分别对应解决哪些学术界关心的安全问题如表 5 所示:

Table 5 The Relationship Between Technology Challenges with Academic Concerns

表 5 安全技术挑战与学术界关注的安全问题对应关系

Academic Concerns	Privacy Preserving in Data Sharing	Equipment Safety Protection Under Limited Resources	More Effective Intrusion Detection Defense Systems & Test Methods	Access Control of Automatic Operation	Cross-domain Authentication of Motive Device
① Privacy Concerns	√	√	√	√	√
② Insecure Cryptographic Algorithm/Protocol		√			
③ Insecure Network Communication	√	√		√	√
④ Insecure Cloud/ Web/Mobile Interface			√	√	√
⑤ Insecure Software/ Firmware		√	√	√	
⑥ Insufficient Authentication		√			√
⑦ Insufficient Access Control/Authorization	√	√	√	√	√
⑧ Poor Physical Security	√	√			
⑨ Poor Embedded System Security	√	√	√		
⑩ Insufficient Security Configurability	√		√		

3.1 数据共享的隐私保护方法

随着物联网应用的普及,更多的用户个人数据会被收集和共享.当地医院通过共享其病人数据与其他地区更加专业的医疗单位来为病人提供更好的医疗服务;智能汽车服务商收集的用户车辆位置信息为用户提供导航服务;智能电网收集的用户的用电信息为其提供更合理的用电规划等.

这些收集与共享的数据中包含医疗数据、用电

信息、车辆位置等大量用户隐私信息.此外,随着数据挖掘与机器学习技术的不断发展,许多并不直接包含隐私信息的数据也会给用户带来隐私泄露的风险.例如有研究人员分析通过分析大量温度传感器中的温度数据,进而总结出温度变化与用户在家中的作息之间的关联规则[53].数据共享下的隐私保护逐渐成为了物联网安全的一大难点.

现有的隐私数据保护方法大多只考虑到终端设备隐私数据采集[50]、云端隐私数据共享[43]等数据传输中某一环节,缺乏对隐私数据生命周期中所有环节(采集、传输、使用、存储、共享等)的完整保护方案.此外,在对隐私数据进行保护时还需保证隐私数据对提供服务商的可用性.许多研究人员[38-39,96]采用同态加密算法来完成上述需求,但效率均有待提升.

3.2 有限资源下的设备安全保护方法

在未来传感器与小型嵌入式设备会广泛应用于人们的生产生活.对于嵌入式医疗设备、偏远环境监测设备、特殊工业环境中的传感器等需要长时间连续工作,对功耗体积等都有着严格要求.故为了设备微型化、降低功耗和节约成本,厂商为这些设备提供的计算与存储资源更加有限.如何在更低的资源以及更低功耗的要求下保障嵌入式设备系统与通信安全成为现阶段物联网安全的一大挑战.

为了解决这一难题,研究者设计了各种轻量级加密算法、认证算法、通信协议[31,97-98]等.但其大多只注重减少对设备计算与存储资源的使用,缺乏对算法的电量消耗的评估.而过高的电量消耗会大大降低这些算法的使用价值.此外,由于这些传感器设备长期无人看管,其还会面临物理攻击的威胁.敌手可直接物理捕获这些设备,再进行侧信道分析来寻找算法中的漏洞[99-100].所以相关研究人员在设计和实现这些轻量级安全算法时,还需充分考虑设备可能受到的物理攻击.

3.3 更加有效的入侵检测防御系统与设备测试方法

随着物联网设备逐渐增多[1],其产生的数据规模也逐渐增大.而大量的物联网设备和数据也成为攻击者实施大规模拒绝服务攻击与构建 IoT 僵尸网络的[5]有力工具.

目前,研究人员提出对拒绝服务攻击的防御与检测方法局限于某一应用场景[101]或协议[102],适用范围有限.但有许多创新性的研究成果与设计思路值得学习参考.例如 Hoeve 提出检测数据包的异常插入来识别加密数据中的恶意攻击行为[103].该方法很好地解决了加密数据无法检测恶意攻击行为这一难题.还有 Kasinathan 等人设计的拒绝服务攻击检测框架可以在检测网络入侵行为的同时保障网络在大规模拒绝服务攻击下的正常运行[102].

此外,攻击者大多利用默认用户名口令或明文传输密钥等网络与系统基础安全漏洞,对物联网设备实施攻击.故对物联网设备与网络进行有效的安全测试,可提高敌手入侵物联网设备的难度.Sachidananda 等人在 2016 年提出了可动态调节与扩展的物联网设备测试框架,但其缺乏对实际市场中物联网设备的大规模测试[21].

3.4 针对自动化操作的访问控制策略

随着物联网设备的智能化,人对设备的操作会逐渐减少,设备会根据收集到外界的信息自动触发相应的操作.例如智能空调自动根据室内温度变化改变空调的温度;智能浇水器自动根据土壤湿度变化进行浇水等.如何对上述物联网设备的自动化操作进行合适有效的访问控制成为物联网安全研究的一大挑战.

现阶段物联网系统大多沿用基于角色、基于属性等传统计算机系统访问控制方法.但这些访问控制方法过度依赖于用户制定的规则,同时无法对物联网设备的自动化操作进行很好地管控.为了解决上述问题,Mahalle 等人提出物联网设备程序在执行自动化操作时需要将其使用的权能与该程序设计之初所要求的权能[104]进行比较,如果不符合就自动终止该程序的操作.但许多的物联网设备应用程序要求的权能往往会大于其真正实际使用所需要的权能[50].文献[105]提出基于 OAuth 协议的物联网设备授权管理系统.该系统会根据程序自动化执行的敏感操作是否已被用户授权来对其进行合法性判断,从而避免频繁的用户交互.还有研究人员提出基于设备采集信息的自动访问控制策略[106]也具有较高的应用价值.

3.5 移动设备的跨域认证方法

穿戴式设备、智能汽车等移动化物联网设备在未来会逐渐增多.在这些移动设备组成的通信网络中,不再只是人与设备之间的交互,设备与设备之间也存在着自动化交互.同时,移动设备会频繁地从一个网络移动到另一个网络.如何对移动设备跨域时进行有效的安全认证和权限授予是当前物联网安全设计中的一大难点.

有研究人员[107]提出通过评估移动设备所处网络中其他设备的可信度来动态改变该移动设备的安全配置,从而降低其被攻击的风险.还有研究人

员[108]指出对于移动设备可以利用自身位置信息来完成自认证.例如当设备处于某一特定区域才有权执行的操作,程序可根据设备自身的位置信息进行自授权来简化认证过程.

4 未来研究方向

针对第3节介绍的五大物联网安全技术挑战并结合物联网安全现状,总结出未来物联网发展中的五大安全研究热点:

1) 隐私数据保护

随着共享单车、共享汽车等物联网共享服务的增多,如何防止这些共享服务中用户隐私信息的泄露将成为物联网安全研究的一大热点.数据统计与分析技术的发展依赖于大量的用户数据,而这也带来了更大的隐私泄露风险.研究人员需要提出更加实用的基于隐私保护的数据挖掘[109]与机器学习[110]方法.

2) 轻量级安全机制

小型嵌入式系统设备在未来会更加普及,需要研究者提出更加有效的轻量级系统与通信安全机制.研究人员在设计轻量级安全机制时,主要需要满足以下要求:首先对设备的电量和资源消耗要降到更低,其次不能大幅增加原有设备的成本和设计难度.

3) 入侵检测与防御系统

物联网设备和通信协议种类不断增多,需要研究人员提出适用范围更广的入侵检测与防御系统[103]和设备安全测试工具[95].近年来,对工业与公共基础设备的网络APT(高级持续性威胁)攻击逐渐增多,如果这些关键的基础设施长期停止工作或被恶意控制,国家和社会将受到严重危害.研究人员需要对这些工业和公共基础设施设计出更加有效的入侵检测与防御系统.

4) 针对自动化操作的访问控制策略

随着机器学习技术的不断发展以及物联网设备计算能力的不断提升,设备的自动化操作会逐步取代人为操作.研究者需为物联网设备的自动化操作设计出更加有效的访问控制策略来防止攻击者的恶意利用.

5) 移动设备的跨域认证方法

当前学术界对物联网移动设备安全问题的研究还不够全面,没有意识到移动设备安全问题带来的严重危害.敌手可利用移动设备不安全的跨域认证,进而对其进行控制并传播恶意代码.研究人员需要提出更加有效的方法来解决移动设备跨域认证问题以及移动设备间安全通信问题.

5 总 结

关于物联网安全的研究虽然逐渐增多,但其整体进度还处于起步阶段.物联网的系统、应用、网络各个方面缺少具有代表性的安全研究成果.本文在调研大量物联网安全论文后,首先从物联网架构层次和应用场景2个角度阐述了物联网安全问题和研究现状.物联网架构3个逻辑层次的主要安全工作分别为:感知层需要在有限资源的设备上实现更加有效的安全措施来保证收集数据的完整性、机密性、可鉴别性;传输层需要着重解决数据跨网络传输时产生的安全问题;应用层在为用户提供更多服务的同时需要充分保护用户的隐私信息.不同的物联网应用场景需要侧重解决的安全问题也有所不同:智能家居和智能医疗设备需要更多的隐私保护机制,从而尽可能降低用户隐私泄露的风险;智能电网等工业基础设施需要更加有效的入侵检测和防御系统,从而抵御大规模的拒绝服务攻击和长期潜伏的APT攻击.

然后,通过深入分析物联网安全问题产生的根本原因与现有工作的不足,总结出物联网安全面临的五大技术挑战.最后指出物联网安全未来的研究热点,为相关研究人员提供更有针对性的设计参考.只有尽快发现并解决物联网安全研究中的诸多难点,才能有效地抵御愈发严重的物联网攻击,使人们安全地享受物联网时代带来的便捷.

参 考 文 献

[1] Statista Inc. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [EB/OL]. [2017-05-30]. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Ironpaper Growth Agency. Internet of Things Market Statistics-2016 [EB/OL]. (2016-02-04) [2017-04-08]. http://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/

[3] MARC GOODMAN. Hacking the Human Heart [EB/OL]. [2017-04-24]. http://bigthink.com/future-crimes/hacking-the-human-heart

[4] Langner R. Stuxnet: Dissecting a cyberwarfare weapon [J]. IEEE Security & Privacy, 2011, 9(3): 49-51

[5] Wikipedia. 2016 dyn cyberattack [EB/OL]. [2017-05-09]. https://en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=763071700

[6] Patterson R. How safe is your data with the IoT and smart devices [EB/OL]. [2017-04-29]. https://www.comparitech.com/blog/information-security/iot-data-safety-privacy-hackers/

[7] Wright A. Mapping the Internet of Things [M]. New York: ACM, 2016

[8] GeekPwn. IoT devices have a large number of low-level loopholes [EB/OL]. [2017-04-23]. http://www.sohu.com/a/129188339_198147

[9] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of things [J]. Computer Networks, 2013, 57(10): 2266-2279

[10] Fu K, Kohno T, Lopresti D, et al. security and privacy threats posed by accelerating trends in the Internet of things [EB/OL]. [2017-05-10]. http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-and-Privacy-Threats-in-IoT.pdf

[11] Li Ling, Li Shancang, Zhao Shanshan. QoS-aware scheduling of services-oriented Internet of things [J]. IEEE Trans on Industrial Informatics, 2014, 10(2): 1497-1505

[12] Wu Chuankun. Security Fundamentals for Internet of Things [M]. Beijing: Science Press, 2013 (in Chinese)
(武传坤. 物联网安全基础[M]. 北京: 科学出版社, 2013)

[13] Zhao Kai, Ge Lina. A survey on the Internet of things security [C] //Proc of the 9th Int Conf on Computational Intelligence and Security. Los Alamitos, CA: IEEE Computer Society, 2013: 663-667

[14] Liu Xiangyu, Zhou Zhe, Diao Wenrui. When good becomes evil: Keystroke inference with smartwatch [C] //Proc of the 22nd ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2015: 1273-1285

[15] Das A, Borisov N, Caesar M. Do you hear what I hear?: Fingerprinting smart devices through embedded acoustic components [C] //Proc of the 21st ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2014: 441-452

[16] Vasyltsov I, Lee S. Entropy extraction from bio-signals in healthcare IoT [C] //Proc of the 1st ACM Workshop on IoT Privacy, Trust, and Security. New York: ACM, 2015: 11-17

[17] Mccann D, Eder K, Oswald E. Characterising and comparing the energy consumption of side channel attack countermeasures and lightweight cryptography on embedded devices [C] //Proc of Int Workshop on SIOT2015. Piscataway, NJ: IEEE, 2015: 65-71

[18] Conti M, Nati M, Rotundo E, et al. Mind the Plug! Laptop-user recognition through power consumption [C] //Proc of the 2nd ACM Workshop on Iot Privacy, Trust, and Security. New York: ACM, 2016: 37-44

[19] Costin A, Zaddach J, Francillon A, et al. A large-scale analysis of the security of embedded firmwares [C] //Proc of the 23nd USENIX Security Symposium. Berkeley, CA: USENIX Association, 2014: 95-110

[20] Azab A M, Swidowski K, Bhutkar J M, et al. Skee: A lightweight secure kernel-level execution environment for arm [C] //Proc of the 23th Network and Distributed System Security Symp. Reston, VA: ISOC, 2016

[21] Sachidananda V, Toh J, Siboni S, et al. POSTER: Towards exposing Internet of things: A roadmap [C] //Proc of the 23rd ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2016: 1820-1822

[22] Guo Fuchun, Mu Yi, Susilo W, et al. CP-ABE with constant-size keys for lightweight devices [J]. IEEE Trans on Information Forensics & Security, 2014, 9(5): 763-771

[23] Shi Yang, Wei Wujing, He Zongjian, et al. An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices [C] //Proc of the 32nd Annual Conf on Computer Security Applications. New York: ACM, 2016: 16-29

[24] Buchmann J, Pfert F, Neysu T, et al. High-performance and lightweight lattice-based public-key encryption [C] //Proc of the 2nd ACM Int Workshop on Iot Privacy, Trust, and Security. New York: ACM, 2016: 2-9

[25] Rauter T, Kajtazovic N, Kreiner C. Privilege-based remote attestation: Towards integrity assurance for lightweight clients [C] //Proc of the 1st ACM Workshop on IoT Privacy, Trust, and Security. New York: ACM, 2015: 3-9

[26] Majzoobi M, Rostami M, Koushanfar F, et al. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching [C] //Proc of IEEE Symp on Security and Privacy Workshop on TrustED2012. Los Alamitos, CA: IEEE Computer Society, 2012: 33-44

[27] Hiller M, Önalan A G, Sigl G, et al. Online reliability testing for PUF key derivation [C] //Proc of the 6th Int Workshop on Trustworthy Embedded Devices. New York: ACM, 2016: 15-22

[28] Xu Weitao, Lan Guohao, Lin Qi, et al. KEH-Gait: Towards a mobile healthcare user authentication system by kinetic energy harvesting [C] //Proc of the 24th Network and Distributed System Security Symp. Reston, VA: ISOC, 2017

[29] Scheel R A, Tyagi A. Characterizing composite user-device touchscreen physical unclonable functions (PUFs) for mobile device authentication [C] //Proc of Int Workshop on TrustED2015. New York: ACM, 2015: 3-13

[30] Dudek D. On the Detectability of Weak DoS Attacks in Wireless Sensor Networks [M]. Berlin: Springer, 2013: 243-257

[31] Sultana S, Ghinita G, Bertino E, et al. A lightweight secure provenance scheme for wireless sensor networks [C] //Proc of the 21st Int Conf on Parallel and Distributed Systems. Piscataway, NJ: IEEE, 2013: 101-108

[32] Ortiz-Yepes D A. BALSA: Bluetooth low energy application layer security add-on [C] //Proc of Int Workshop on SIOT2015. Piscataway, NJ: IEEE, 2015: 15-24

[33] Szalachowski P, Perrig A. Lightweight protection of group content distribution [C] //Proc of the 1st ACM Workshop on IoT Privacy, Trust, and Security. New York: ACM, 2015: 35-42

[34] Zhu Yihai, Yan Jun, Tang Yufei, et al. Joint substation-transmission line vulnerability assessment against the smart grid [J]. IEEE Trans on Information Forensics & Security, 2015, 10(5): 1010-1024

[35] Niemietz M, Somorovsky J, Mainka C, et al. Not so smart: On smart TV apps [C] //Proc of Int Workshop on SIOT2015. Piscataway, NJ: IEEE, 2015: 72-81

[36] Zhang Yuexin, Xiang Yang, Huang Xinyi, et al. A cross-layer key establishment scheme in wireless mesh networks [C] //Proc of ESORICS 2014. Berlin: Springer, 2014: 526-541

[37] Nguyen K T, Oualha N, Laurent M. Authenticated Key Agreement Mediated by a Proxy Re-encryptor for the Internet of Things [M]. Berlin: Springer, 2016

[38] Chakravorty A, Wlodarczyk T, Rong C. Privacy preserving data analytics for smart homes [J]. IEEE Computer Society Security & Privacy Workshops, 2013, 42(6): 23-27

[39] Lu Zhuo, Wang Wenye, Wang C. Camouflage traffic: Minimizing message delay for smart grid applications under jamming [J]. IEEE Trans on Dependable & Secure Computing, 2015, 12(1): 31-44

[40] Riliskis L, Shafagh H, Levis P. Computations on encrypted data in the Internet of things applications [C] //Proc of the 22nd ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2015: 1668-1670

[41] Ravikumar G K, Manjunath T N, Hegadi R S, et al. A survey on recent trends, process and development in data masking for testing [J]. International Journal of Computer Science Issues, 2011, 8(2): 1709-1720

[42] Xu Jia, Yang Anjia, Zhou Jianying, et al. Lightweight Delegatable Proofs of Storage [M]. Berlin: Springer, 2016

[43] Yang Lei, Humayed A, Li Fengjun. A multi-cloud based privacy-preserving data publishing scheme for the Internet of things [C] //Proc of the 32nd Conf on Computer Security Applications. New York: ACM, 2016: 30-39

[44] Condra G. A plea for incremental work in IoT security [C] //Proc of Int Workshop on TrustED2015. New York: ACM, 2015: 39-39

[45] Tang Yuzhe, Wang Ting, Liu Ling, et al. Lightweight authentication of freshness in outsourced key-value stores [C] //Proc of the 30th Conf on Computer Security Applications. New York: ACM, 2014: 176-185

[46] Pirker M, Slamanig D, Winter J. Practical privacy preserving cloud resource — payment for constrained clients [G] //LNCS 7384: Privacy Enhancing Technologies. Berlin: Springer, 2012: 201-220

[47] Hardjono T, Smith N. Cloud-based commissioning of constrained devices using permissioned blockchains [C] //Proc of the 2nd ACM Int Workshop on Iot Privacy, Trust, and Security. New York: ACM, 2016: 29-36

[48] Altmeier C, Mainka C, Somorovsky J, et al. AdIDoS—Adaptive and intelligent fully-automatic detection of denial-of-service weaknesses in Web services [M]. Data Privacy Management, and Security Assurance. Berlin: Springer, 2015: 65-80

[49] Ali M Q, Al-Shaer E. Configuration-based IDS for advanced metering infrastructure [C] //Proc of the 20th ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 451-462

[50] Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications [C] //Proc of Int Workshop on SIOT2014. Los Alamitos, CA: IEEE Computer Society, 2016: 636-654

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

[52] Mituca A, Moin A H, Prehofer C. Access control for apps running on constrained devices in the Internet of things [C] //Proc of Int Workshop on SIOT2014. Piscataway, NJ: IEEE, 2014: 1-9

[53] Copos B, Levitt K, Bishop M, et al. Is anybody home? Inferring activity from smart home network traffic [C] //Proc of the 2nd Int Workshop on Privacy Engineering. Piscataway, NJ: IEEE, 2016: 245-251

[54] Obermaier J, Hutle M. Analyzing the security and privacy of cloud-based video surveillance systems [C] //Proc of the 2nd ACM Int Workshop on Iot Privacy, Trust, and Security. New York: ACM, 2016: 22-28

[55] Fernandes E, Paupore J, Rahmati A, et al. Flowfence: Practical data protection for emerging IOT application frameworks [C] //Proc of the 25th Usenix Security Symposium. Berkeley, CA: USENIX Association, 2016

[56] Yu T, Sekar V, Seshan S, et al. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-things [C] //Proc of the 14th ACM Workshop on Hot Topics in Networks. New York: ACM, 2015: 5

[57] Henry N L, Paul N R, Mcfarlane N. Using bowel sounds to create a forensically-aware insulin pump system [C] //Proc of USENIX Workshop on HealthTech'13. Berkeley, CA: USENIX Association, 2013

[58] Sicari S, Rizzardi A, Grieco L A, et al. Security, privacy and trust in Internet of things: The road ahead [J].. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2015, 76(C):146-164

[59] Mer M, Aspinall D, Wolters M. Weighing in eHealth Security [C] //Proc of the 23rd ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2016: 1832-1834

[60] Hewlett Packard Enterprise. Healthcare Rx: How technology and IoT can help fix a broken system [EB/OL]. [2017-05-09]. https://insights. hpe. com/reports/healthcare-rx-how-technology-and-iot-can-help-fix-a-broken-system-1701. html

[61] Clark S S, Ransford B, Rahmati A, et al. WattsUpDoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices [C] //Proc of USENIX Workshop on HealthTech'13. Berkeley, CA: USENIX Association, 2013

[62] Krishnan R. Ransomware hijacks hotel smart keys to lock guests out of their rooms [EB/OL]. (2016-04-03) [2017-05-13]. http://thehackernews. com/2016/04/hospital-ransomware. html

[63] Rubin A D. Taking two-factor to the next level: Protecting online poker, banking, healthcare and other applications [C] //Proc of the 30th Annual Computer Security Applications Conf. New York: ACM, 2014: 1-5

[64] Duffy E, Nyemba S, Gunter C A, et al. Requirements and design for an extensible toolkit for analyzing EMR audit logs [C] //Proc of USENIX Workshop on HealthTech'13. Berkeley, CA: USENIX Association, 2013

[65] Dong Xiaolei. Advances of privacy preservation in Internet of things [J]. Journal of Computer Research and Development, 2015, 52(10): 2341-2352 (in Chinese)
(董晓蕾. 物联网隐私保护研究进展[J]. 计算机研究与发展, 2015, 52(10): 2341-2352)

[66] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle[OL]. (2015-08-10) [2017-05-23]. http://illmatics. com/Remote%20Car%20Hacking. pdf

[67] Forensics E. The most hackable cars on the road [EB/OL]. (2015-08-19) [2017-05-29]. http://www. envistaforensics. com/news/the-most-hackable-cars-on-the-road-1

[68] Theguardian. Team of hackers take remote control of tesla models from 12 miles away [EB/OL]. (2016-09-20) [2017-05-06]. https://www: theguardian: com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes

[69] Hartenstein H, Laberteaux K. A tutorial survey on vehicular ad hoc networks [J]. IEEE Communications Magazine, 2008, 46(6): 164-171

[70] Radu A I, Garcia F D. LeiA: A lightweight authentication protocol for CAN [G] //Computer Security-ESORICS 2016. Berlin: Springer, 2016: 283-300

[71] Weimerskirch A. An overview of automotive cybersecurity: Challenges and solution approaches [C] //Proc of Int Workshop on TrustED2015. New York: ACM, 2015: 53

[72] Wang L, Nojima R, Moriai S. A secure automobile information sharing system [C] //Proc of the 1st ACM Workshop on Iot Privacy, Trust, and Security. New York: ACM, 2015: 19-26

[73] Tan R, Krishna V B, Yau D K Y, et al. Impact of integrity attacks on real-time pricing in smart grids [C] //Proc of the 20th ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 439-450

[74] Vieira B, Poll E. A security protocol for information-centric networking in smart grids [C] //Proc of ACM Workshop on SEGS'13. New York: ACM, 2013: 1-10

[75] Dimitriou T, Karame G. Privacy-friendly planning of energy distribution in smart grids [C] //Proc of ACM Workshop on SEGS'14. New York: ACM, 2014: 1-6

[76] Erkin Z, Veugen T. Privacy enhanced personal services for smart grids [C] //Proc of ACM Workshop on SEGS'14. New York: ACM, 2014: 7-12

[77] Danezis G, Kohlweiss M. Smart meter aggregation via secret-sharing [C] //Proc of ACM Workshop on SEGS'13. New York: ACM, 2013: 75-80

[78] Biselli A, Franz E. Protection of consumer data in the smart grid compliant with the German smart metering guideline [C] //Proc of ACM Workshop on SEGS'13. New York: ACM, 2013: 41-52

[79] Wikipedia. SCADA [EB/OL]. [2017-05-11]. https://en. wikipedia. org/wiki/SCADA

[80] Wikipedia. Industrial control system [EB/OL]. [2017-05-11]. https://en. wikipedia. org/wiki/Industrial_control_system

[81] Cardenas A A, Amin S, Sastry S. Secure control: Towards survivable cyber-physical systems [C] //Proc of the 28th Int Conf on Distributed Computing Systems Workshops. Los Alamitos, CA: IEEE Computer Society, 2008: 495-500

[82] Luiijf E. Threats in Industrial Control Systems [M]. Berlin: Springer, 2016

[83] Edward J M C. Security of cyber-physical systems [J]. Journal of Cyber Security and Information Systems, 2017, 5(1): 41-47

[84] Hadžiosmanović D, Sommer R, Zambon E, et al. Through the eye of the PLC [C] //Proc of the 30th Annual Computer Security Applications Conf. New York: ACM, 2014: 126-135

[85] Lin Hui, Slagell A, Kalbarczyk Z, et al. Semantic security analysis of SCADA networks to detect malicious control commands in power grids [C] //Proc of ACM Workshop on SEGS'13. New York: ACM, 2013: 29-34

[86] Sullivan D T, Colbert E J. Network analysis of reconnaissance and intrusion of an industrial control system, AD1016413 [R]. New York: Defense Technical Information Center, 2016

[87] Henry M H, Zaret D R, Carr J R, et al. Cyber Risk in Industrial Control Systems [M]. Berlin: Springer, 2016

[88] Costin A. Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations [C] //Proc of the 6th Int Workshop on Trustworthy Embedded Devices. New York: ACM, 2016: 45-54

[89] Line M B, Zand A, Stringhini G, et al. Targeted attacks against industrial control systems: Is the power industry prepared? [C] //Proc of ACM Workshop on SEGS'14. New York: ACM, 2014: 13-22

[90] Colbert E J M, Kott A. Cyber-security of SCADA and Other Industrial Control Systems [M]. Berlin: Springer, 2016

[91] Formby D, Sang S J, Copeland J, et al. An empirical study of TCP vulnerabilities in critical power system devices [C] // Proc of ACM Workshop on SEGS'14. New York: ACM, 2014: 39-44

[92] Wang Huaqun, Qin Bo, Wu Qianhong, et al. TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids [J]. IEEE Trans on Information Forensics & Security, 2015, 10 (11): 2340-2351

[93] Rahman M A, Mohsen F, Al-Shaer E. A formal model for sustainable vehicle-to-grid management [C] //Proc of ACM Workshop on SEGS'13. New York: ACM, 2013: 81-92

[94] OWASP. OWASP Internet of Things Top Ten [EB/OL]. [2017-05-20]. https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

[95] Dantas H, Erkin Z, Doerr C, et al. eFuzz: A fuzzer for DLMS/COSEM electricity meters [C] //Proc of ACM Workshop on SEGS'14. New York: ACM, 2014: 31-38

[96] Ayday E, Raisaro J L, Mclaren P J, et al. Privacy-preserving computation of disease risk by using genomic, clinical, and environmental data [C] //Proc of USENIX Conf on Safety, Security, Privacy and Interoperability of Health Information Technologies. Berkeley, CA: USENIX Association, 2013: 1-10

[97] Saarinen M O. The BlueJay Ultra-Lightweight hybrid cryptosystem [C] //Proc of IEEE Symp on Security and Privacy Workshop on TrustED2012. Los Alamitos, CA: IEEE Computer Society, 2012: 27-32

[98] Zenger C T, Chur M J, Posielek J F, et al. A novel key generating architecture for wireless low-resource devices [C] //Proc of Int Workshop on SIOT2014. Piscataway, NJ: IEEE, 2014: 26-34

[99] Ding Lin, Jin Chenhui, Guan Jie, et al. Cryptanalysis of lightweight WG-8 stream cipher [J]. IEEE Trans on Information Forensics & Security, 2014, 9(4): 645-652

[100] Dougherty D J, Guttman J D. Decidability for lightweight Diffie-Hellman protocols [C] //Proc of the 27th Computer Security Foundations Symp. Piscataway, NJ: IEEE, 2014: 217-231

[101] Yan Jun, He Haibo, Zhong Xiangnan, et al. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks [J]. IEEE Trans on Information Forensics & Security, 2016, 12(1): 200-210

[102] Kasinathan P, Costamagna G, Khaleel H, et al. DEMO: An IDS framework for Internet of things empowered by 6LoWPAN [C] //Proc of the 20th ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 1337-1340

[103] Hoeve M. Detecting intrusions in encrypted control traffic [C] //Proc of ACM Workshop on SEGS'13. New York: ACM, 2013: 23-28

[104] Mahalle P N, Anggorojati B, Prasad N R, et al. Identity establishment and capability based access control (IECAC) scheme for Internet of Things [C]//Proc of Int Symp on IEEE WPMC'12. Piscataway, NJ: IEEE, 2012: 187-191

[105] Windley P J. API access control with OAuth: Coordinating interactions with the Internet of things [J]. IEEE Consumer Electronics Magazine, 2015, 4(3): 52-58

[106] Jia Y J, Chen Q A, Wang Shiqi, et al. ContexIoT: Towards providing contextual integrity to appified IoT platforms [C] //Proc of the 24th Network and Distributed System Security Symp. Reston, VA: ISOC, 2017

[107] Chen I R, Bao F, Guo Jia. Trust-based service management for social Internet of things systems [J]. IEEE Trans on Dependable & Secure Computing, 2016, 13(6): 684-696

[108] Ilie-Zudor E, Kemeny Z, van Blommestein F, et al. A survey of applications and requirements of unique identification systems and RFID techniques [J]. Computers in Industry, 2011, 62(3): 227-252

[109] Wang Jian. The study of key technologies of privacy-preserving data mining [D]. Shanghai: Donghua University, 2011 (in Chinese)
(王健. 基于隐私保护的数据挖掘若干关键技术研究[D]. 上海: 东华大学, 2011)

[110] Shokri R, Shmatikov V. Privacy-preserving deep learning [C] //Proc of the 53rd Annual Allerton Conf on Communication, Control, and Computing. Piscataway, NJ: IEEE, 2015: 909-910

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.

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).

Peng Anni, born in 1995. PhD candidate in the University of Chinese Academy of Sciences. Her main research interests include network and system security (pengan@nipc.org.cn).