物联网安全测评技术综述

陈 钊, 曾凡平, 陈国柱, 张燕咏, 李向阳
中国科学技术大学 计算机科学与技术学院 合肥 中国 230027

摘要 近年来, 物联网大规模应用于智能制造、智能家居、智慧医疗等产业, 物联网的安全问题日益突出, 给物联网的发展带来了前所未有的挑战。安全测评技术是保障物联网安全的重要手段, 在物联网应用的整个开发生命周期都需要进行安全测评工作, 以保证物联网服务的安全性和健壮性。物联网节点面临计算能力、体积和功耗受限等挑战, 智慧城市等应用场景提出了大规模泛在异构连接和复杂跨域的需求。本文首先总结了目前物联网中常用的安全测评方法和风险管理技术; 然后从绿色、智能和开放三个方面分析物联网安全技术的发展现状和存在的安全问题, 并总结了物联网安全测评面临的挑战以及未来的研究方向。

关键词 物联网; 安全测评; 绿色; 智能; 开放
中图法分类号 TP309.2 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.05.01

A Survey for IoT Security Assessment Technologies

CHEN Zhao, ZENG Fanping, CHEN Guozhu, ZHANG Yanyong, LI Xiangyang
School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China

Abstract In recent years, the Internet of Things(IoT) has been widely deployed in intelligent manufacturing, smart homes, and smart medical services, etc. The security concerns of the IoT systems are becoming increasingly prominent, posing an unprecedented challenge to the underlying IoT system design. Security assessment, an important means for ensuring IoT security, needs to be performed throughout the development lifecycle of IoT applications. IoT nodes face challenges such as computing power, size and power consumption. The application scenarios such as smart cities propose large-scale ubiquitous heterogeneous connections and complex cross-domain requirements. We first survey the current security assessment methods and threat management technologies that are widely used in IoT. We then analyze the security technologies of IoT from the aspects of green, intelligence and openness, and summarize the development status and existing security problems from these three dimensions. Finally, we summarize the challenges of IoT security assessment and the future research directions are pointed out.

Key words IoT; security assessment; green; intelligence; openness

1 引言

信息产业在经过互联网时代、移动互联网时代的全面发展后, 已经步入大数据时代和物联网时代。物联网经过近几年的快速发展, 迅速在智能制造、智能电网和智慧城市等大型应用场景中发挥了巨大的作用, 为政府机构、企业和个人用户提供着越来越丰富的服务, 正在朝着万物互联互通目标前进。根据国际数据公司 2013 年报告, 预计到 2020 年互联设备数量将快速增长到 410 亿, 市场规模将达到 8.9 万亿美元 [1]。据《2017-2018 年中国物联网年度发展报告》[2], 2017 年以来, 我国物联网市场进入了实质性发展阶段, 全年市场规模突破 1 万亿元, 年复合增长率超过 25%, 其中物联网云平台成为竞争核心领域, 预计 2021 年我国物联网平台支出将位居全球第一。物联网在快速发展的同时, 也面临着来自安全、绿色、智能以及开放服务等方面的巨大挑战。

物联网被攻击造成的安全问题往往涉及面广且造成的经济损失严重。2016 年黑客控制来自全球的天量感染 Mirai 病毒的物联网设备对美国东海岸 DNS 服务商 Dyn 发起了 DDoS 攻击, 该攻击严重影响 DNS 服务的客户业务, 甚至导致客户网站无法访问, 受到影响的著名公司有 Twitter、Github、BBC 等[3]。2018 年 1 月, 有报道显示黑客通过损坏指纹传感器, 使用橘子皮解锁手机并成功转账付款,

通讯作者: 李向阳, 博士, 教授, Email: xiangyangli@ustc.edu.cn。
本课题得到科技部网络空间安全项目 物联网与智慧城市安全保障关键技术研究 No.2018YFB080340 资助。
收稿日期: 2019-01-31; 修改日期: 2019-05-13; 定稿日期: 2019-05-14

造成财产损失和隐私泄露等问题[4]。物联网中的设备、网络以及控制系统需要互相配合才能为用户提供完整的服务, 一旦其中某个环节发生安全问题, 服务都会受到影响。

为了提供一个安全稳定的物联网应用服务, 必须保证物联网的感知层、网络层、数据和服务层都达到必要的安全指标, 为此需要对物联网进行安全测试和评估。目前, 物联网应用规模快速发展, 对物联网安全测评技术提出了新的要求。本文第二章分析了国内外物联网安全测评技术的研究现状, 并提出其中的问题和未来的研究方向。

物联网应用除了面临严峻的安全挑战, 还面临着海量设备和大规模网络而带来的能耗问题和智能网络管理问题。为了实现高效节能的物联网设备管理、数据传输以及安全防护, 许多学者提出了轻量级秘钥分配算法、轻量级密码以及轻量级认证算法等技术。以往的物联网系统往往是独立的系统, 不对外部开放, 带来了信息不能共享等问题。为了提升信息的价值, 物联网的开放共享是技术发展的必然趋势。这些物联网安全保障技术在为物联网系统提供安全服务之前, 我们也需要对其进行深入的安全分析和测评, 只有通过了安全测评, 才能大规模地应用到实际的物联网系统中。

随着越来越多的物联网应用的商业化, 接入网络的设备数量骤增, 物联网能耗问题日益突出, 绿色物联网是物联网应用能够保持活力的强有力支撑。物联网庞大的网络对电能的消耗以及节点自身对能源的依赖都迫切需要高能效、低功耗的绿色技术的应用。为了保障物联网服务的安全性, 许多学者提出了轻量级的加密算法、访问控制技术和轻量级 IDS 等, 但这些技术在实现过程中或多或少存在一定的安全漏洞。本文第三章第一节分析了主流的轻量级密码技术及其安全问题, 指出对保证物联网安全的轻量级技术的测评工作是亟需进行的。

物联网中海量大规模异质设备和异质网络的连接管理是个急需解决的问题。近年来物联网的快速发展促进了智能网关的发展。许多厂商提出了边缘侧计算平台, 将智能云服务无缝扩展至设备, 给物联网设备发现与监控、网络管理以及智能服务的提供带来了极大的便利, 但智能网络的发展也存在一定的安全隐患。本文第三章第二节分析了目前智能网络的发展现状及其在安全防护和隐私保护方面面临的问题。

物联网应用和感知设备往往紧紧耦合在一起, 信息存储格式各异, 无法在应用间共享。物联网需要实现万物互联, 那就意味着开放和共享。目前国内外已经有多家公司推出了物联网开放平台, 提供简单易用的应用开发服务。本文第三章第二节简单介绍了国内外已有开放平台的业务内容以及总结这些开放平台存在的安全问题。

本文主要贡献包括 3 个方面:

1) 分析了现有物联网各层安全测评技术的发展现状, 并总结了物联网环境中复杂的安全威胁管理和风险评估技术。

2) 调研了物联网发展过程中出现的新技术: 绿色节点、智能网络、开放平台, 以及其中存在的安全问题, 并指出对新技术的测评是迫切需要的。

3) 总结了物联网安全测评研究面临的挑战, 并探讨了未来该领域的研究方向。

2 物联网安全测评技术

随着越来越多的物联网设备接入互联网, 物联网在给人类生活带来便利以及经济效益的同时, 也给用户带来了巨大的安全隐患, 物联网相关的安全问题越来越受到安全专家和政府部门的重视, 企业界和国家相关部门都对信息系统及物联网系统提出了必要的安全测评要求。信息系统安全等级测评主要包括单元测评和整体测评两部分, 而物联网安全测评指对物联网信息系统进行测评。测评方法指测评人员在测评实施过程中所使用的方法, 主要包括访谈、检查和测试三种测评方法[5]。与传统互联网安全测评相比, 物联网系统在感知设备、感知网络、数据服务等安全测评方面面临更严峻的挑战,物联网安全测评需要更关注于这些方面的研究。本节主要分析了物联网安全测评相关的自动分析方法。我们根据测评方法的不同侧重点将目前已有的方法分为设备安全测评、网络安全测评、数据和服务安全测评。常见的物联网安全测评方法还包括持续的威胁管理与风险分析技术, 能够帮助网络管理员评估漏洞给系统带来的危害。本章最后还综述了物联网安全测评相关的国内外法规和标准。

2.1 设备安全测评

物联网感知层设备具有多源异构的特点, 而且大部分设备的计算能力、存储能力、通信能力、能量储备都存在一定的限制。感知层的安全测评需要考虑设备的物理安全测评、访问控制测评、操作系统及硬件安全测评等方面。本节主要讨论 RFID (Radio Frequency Identification)设备、非 RFID 设备和嵌入式操作系统安全测评技术。

RFID 系统一般由标签、读写器、应用软件组成, 且存在着较多针对这三个组件的攻击方法。对 RFID 系统的安全测评主要包括两类, 第一类是使用仿真实验模拟应用的运行过程, 并引入错误来评估系统受到的影响。Abdelmalek 等人[6]设计了一个支持错误注入和实时监测的仿真平台。可以通过模拟和观察系统状态来帮助工程师了解芯片错误和协议修改对各部件的影响, 也可以通过分析错误传播过程及行为来评价 RFID 架构的安全性。Mezzah 等人[7]针对文献[6]中没有进行完整错误注入影响分析等问题, 开发了一个基于 FPGA (field-programmable gate array) 的可配置的错误模拟系统, 可以分析单粒子翻转 (Single event upset-SEU) 和单粒子瞬变(single event transient -SET)两种类型的错误。

另外一类方法是对 RFID 系统的安全审计。早在 2009 年, 芬兰的奥卢大学就开源了一款 RFID 安全审计工具 RIDAC[8], 包括对 RFID 标签的外观检查、耦合与频率、能力供应与调制等步骤。Tiago 等人[9]借鉴文献[8]的思想提出了一个类似的更全面的方法, 其步骤包括外观检查、FCC (Federal Communications Commission) ID 检查、频段检测、高低频段标签参数分析、超高频标签参数分析、标准分析等。在企业方面, IBM 公司在美国和欧洲等地方都设置了 RFID 的测试实验室, 可以测试 RFID 芯片、阅读器和应用软件来检测它们之间的通信情况。由中国台湾经济部技术处和商业司建设的“亚太 RFID 应用验测中心”于 2005 年宣布启用, 该中心按照业务流程主要分为: RFID 静态性能测试、RFID 动态性能测试及 RFID 产业应用实验场三大部分。

在设备安全测评方面, 主要的方法包括漏洞扫描、弱密码检测等。Loi 等人[10]设计了一个系统化的方法来识别物联网设备中存在的安全问题。该方法从隐私数据的机密性、传输数据的完整性、设备的访问控制、设备上发起的反射攻击[11]四个维度来评估设备可能受到的威胁。并根据测评结果设计了物联网设备的安全评分机制, 简单易用。Shodan 是全球第一个物联网设备专用的搜索引擎[12], 可以利用 Shodan 检索连接到互联网的所有网络设备。Ali 等人[13]利用 Shodan 扫描了约旦市的物联网设备, 发现很多潜在的漏洞, 目的是警示约旦的物联网设备开发商和开发者应该更多地关注物联网设备的脆弱性。McMahon 等人[14]利用 Shodan 分析了自建的关于医疗器械的测试床, 发现 10%左右的设备都存在漏洞。Anisetti 等人[15]根据 Shodan 的扫描信息构建设备测试知识集, 并检验已知可利用漏洞是否能在被测设备上被利用, 来完成对物联网设备的安全检测。国内的神州绿盟信息安全科技股份有限公司开发的绿盟工控漏洞扫描系统实现了针对 SCADA (Supervisory Control and Data Acquisition)、现场总线、数字化设计制造软件的漏洞扫描, 具备发现漏洞、评估漏洞、展示漏洞、跟踪漏洞等完备的漏洞管理能力[16]。北京匡恩网络科技有限责任公司开发的漏洞挖掘检测平台, 能够检测出工业控制设备、保护设备或工业控制系统中存在的已知漏洞和缺陷, 还能利用优化后的高效模糊测试引擎来挖掘潜在的未知漏洞[17]。

在嵌入式操作系统安全测评方面, 主流工作是基于传统 PC 操作系统的安全测试。对物联网中功能受限的操作系统的测评, 主流工作是建立操作系统的状态机模型, 分析系统的不安全状态形成过程。Ni 等人[18]提出一个嵌入式系统的安全评估模型, 定义了对象模型、消息模型、角色模型及其之间的约束关系, 然后根据对象间交互参数计算出对象的风险级别。Tabrizi 等人[19]通过建立智能电表的抽象模型, 并利用模型检测方法来自动生成让系统进入非安全状态的动作序列, 该动作序列即潜在的恶意序列。该方法能够检测操作系统设计时的安全问题, 能给系统设计提供重要参考。同济大学设计了一个嵌入式系统仿真测试平台[20], 可以将系统代码从目标机器中剥离, 然后在宿主机上进行全数字仿真测试, 能够极大地降低嵌入式系统的安全测试成本。但是该平台只适用于基于 32 位 ARM CPU 内核的嵌入式系统。

在针对物联网设备的嵌入式固件的安全分析方面, 主要有静态分析和动态分析两种方法。法国的通信系统工程师学校(EURECOM)首次提出了大规模嵌入式固件镜像静态分析框架, 包括镜像收集、过滤、解包和分析等步骤。分析了 3.2 万个固件镜像, 发现 38 个未发现的漏洞[21]。Chen 等人[22]通过基于软件的全系统仿真自动化地动态分析固件漏洞, 发现了 14 个未发现的漏洞, 但是该方法基于预编译的插桩的 Linux 系统, 具有一定的局限性, 而且只支持 ARM 和 MIPS 的硬件体系架构。

2.2 网络安全测评

物联网的网络层主要涉及核心网、无线网络以及移动通信网络系统。传统的网络安全测试主要包括功能测试、性能测试、安全性测试以及可用性测试。而物联网网络层测评更多地关注对网络事件以及协议包的仿真测试, 本节主要介绍物联网感知网络仿真工具和测试工具。

物联网系统服务的提供由各层相互协作完成, 交互较多。通过仿真来模拟和建模网络行为是一种常用的测评方法。Liu 等人[23]设计了一个针对电网的集成仿真测试床, 该系统包括电力层、传感器和控制层、通信层和应用层四层。通信层使用了两个常用的工具 ns-2(现在已更新为 Network Simulator-3)[24]和 DeterLab[25]。他们均可以模拟实际网络中的常见的事件, 如网络延迟、分发数据包等, 并且集成了很多网络分析的工具。该测试床还可以用来分析物理攻击、数据攻击、网络通信攻击等。Saxena 等人[26]提出了一个既可以模拟电力系统又可以模拟通信网络的安全评估工具, 其中的通信感知管理模块可以模拟网络组件间的通信并用日志记录, 还可以评估具体网络攻击场景的行为, 安全评估模块通过其他模块的观测数据计算系统的可信矩阵来判断系统模块的健康程度并为管理员提供维护系统安全的策略。其中的通信感知管理模块可以模拟网络组件间的通信并用日志记录, 还可以评估具体网络攻击场景的行为, 安全评估模块通过其他模块的观测数据计算系统的可信矩阵来判断系统模块的健康程度并为管理员提供维护系统安全的策略。

物联网中使用的网络协议种类较多而且安全保护措施各异。对网络协议的测试工作大多需要仿真软件的辅助。Christian 等人[27]开发了 TAP-SNS 系统来进行物联网安全协议的仿真与验证, 可以提供安全测试和仿真服务。TAP-SNS 包含了两个核心组件: encrylib 加密库和 WSN-manager 管理器, 前者提供了 AES 等加密算法的实现, 后者运行于模拟的采集节点和基站之间, 用户可以从 WSN-manager 管理器提供的两个窗口发送消息来验证通信的安全性。丹麦奥尔胡斯大学提出一个医用无线传感网通信协议的安全可用性测试平台, 该平台可以用于验证各类安全协议对网络的影响并评估和比较各类安全协议[28]。该平台还可以模拟内部和外部攻防体系、非授权访问和认证过程, 并根据相关记录信息来验证和评估安全防护措施的可用性。

除了上述使用仿真工具对网络事件、网络协议进行模拟分析外, 许多研究人员利用各种传感器搭建真实的测试平台, 获取真实的测试数据。其面临的关键挑战有三个: 1)支持大规模异构设备; 2)同时支持虚拟节点和真实物理节点; 3)支持异构协议融合。目前针对无线传感网的测试工具或者平台有 LabVIEW[29]、Twist[30]、WISEBED[31]、IoT-LAB[32]等。他们均支持异构设备连接和多种类型的协议测试。Twist 和 WISEBED 还支持混合仿真。

2.3 数据安全测评

物联网中的数据不仅需要保证数据的采集安全, 还需要传输安全、传统的存储和计算安全以及考虑个人隐私保护。用到的方法包括轻量级加密、安全多方计算、数据匿名化、差分隐私以及可加密搜索等。本节主要从恶意数据注入检测方面的工作来描述物联网数据层的安全检测技术。

恶意数据注入是智能电网中最严重的攻击之一。1969 年 Schweppe 等人[33]第一次提出电力系统状态评估方法用于检测和识别系统中的错误。Liu 等人[34]提出存在一种状态评估无法检测到的攻击, 即恶意数据注入攻击。之后, Bobba 等人[35]指出要想检测到恶意数据注入攻击, 至少需要保护一个最小的传感器集合。

卡方检验和正则化残差检验是最常用的恶意数据检测方法。Liu 等人[36]提出一个新的自适应分区状态评估方法, 基本思想是将庞大的系统划分成多个子系统提高检测的敏感度, 用当前检测结果来指导下次的系统分区和更新。在每个子系统内使用卡方检验来检测恶意数据。恶意数据检测和分区会一直重复直到恶意数据被定位到一个非常小的子系统内。

风力发电在电力供应上占据一定的份额, 风力发电系统常因为大量气象传感器暴露在物理环境中, 容易遭到黑客入侵或者物理破坏。Amarjit 等人[37]考虑风电场参数、发电属性和攻击约束, 定义了对风力涡轮机的不可检测数据攻击的通用形式, 将其定义为多目标优化问题, 然后使用约束求解的方法来分析恶意数据注入攻击对整个风力发电系统的影响。

物联网中的数据安全极其重要, 恶意注入数据检测在保护数据的真实性和安全性方面具有重要作用。目前物联网发展急需一种设备安全状态探测与行为智能推断方法, 能够主动探测设备状态, 智能感知设备行为, 保证数据采集的可靠和安全。

2.4 服务安全测评

物联网服务层位于网络层之上, 感知层的数据经过网络传输汇聚到服务层。服务层对数据进行存储和计算并为应用提供智能决策等支持。服务层的安全主要由云平台来提供, 很多服务层的安全测评方法与传统的平台安全测评一致, 包括平台监控、日志审计、渗透测试等手段。本节主要分析文章显示说明是物联网服务相关的安全评估方法, 并不涉及传统互联网服务的安全测评工作。

Keon 等人[38]从物联网体系架构的角度提出了一

个物联网服务的安全评估框架, 他们总结了物联网服务的安全需求并将它们分到 4 个逻辑组: 系统依赖、服务层、网络层、隐私。该框架结合模糊 DEMATEL 方法和模糊 ANP 方法[39]计算得到影响元素的权重和优先级, 能够为系统体系结构的设计和服务的实现提供重要参考。 Huang 等人[40]提出一个层次分析方法来评估物联网云服务的安全。文中提出一个四层安全评估方法, 对于服务层的 RestAPI, 考虑了会话、机器和 bulkiot(机器的传感数据), 并给出一个系统安全性评分的计算公式来评估系统的健康程度。

物联网服务安全主要考虑用户身份认证、设备访问控制、服务接口以及设备间和设备与环境的交互安全等问题研究。当前的研究主要关注在物联网平台的粗粒度授权机制的安全问题和接口访问控制安全研究。相关研究机构和企业还在致力于研究服务的安全提供机制, 暂时缺乏完善的服务安全测评方案。

2.5 漏洞管理和风险评估技术

传统的信息系统安全评估与管理是从风险管理开始进行的, 风险管理能够有效揭示攻击对系统中重要资源的威胁以及相应的损失。风险管理的目的是进行风险评估并给出有效缓解威胁的措施。近年来, 许多基于攻击图[41-44]或者攻击树[45-47]的方法被提出。这些方法的基本思想是将系统中不同节点中存在的不同攻击之间的依赖关系建模为图或者树型结构, 然后研究不同路径的攻击行为, 并针对不同攻击路径提出相应的缓解策略。Poolsappasit 等人[48]于 2012 年提出了基于贝叶斯攻击图的动态安全风险管理方法, 奠定了基于攻击图的安全评估与动态控制分析的研究方向。该方法采用 BAG(贝叶斯攻击图)揭示先验条件、漏洞利用和后验条件之间的因果关系, 帮助系统管理员动态评估目标系统面临的安全风险, 该文献还提出一种遗传算法以便在资源受限的环境中向管理员提供最优的降低风险措施。但文献[48]提出的攻击图构建算法的时间复杂度较高(不小于 O (N^2), N 是节点数量与节点漏洞数量的乘积), 多目标优化遗传算法的时间复杂度也较高。

近几年物联网系统中的安全漏洞和攻击方法不断被暴露出来, 给黑客提供了大量对物联网系统进行攻击的途径。又由于物联网系统更新缓慢, 无法及时打上补丁, 造成物联网系统中长时间存在大量未修复的漏洞。许多研究者将传统的漏洞风险分析方法拓展至物联网系统中, 分析不同漏洞形成的攻击路径带来的风险。Geogre 等人[49]提出根据网络配置和漏洞关联构造漏洞攻击图的方法, 节点间的有向依赖表示通过攻击前一节点后对下一节点完成攻击的可能性, 可能性值是由 CVSS[50]算得出。然后利用图论的方法计算出高风险路径、长度较短的攻击路径以及热点节点, 最后提出缓解被黑客攻击的策略供网络管理员参考。Wang 等人[51]也通过构建漏洞攻击图, 提出最大 flow loss 和 loss 饱和度等度量方式来量化漏洞利用路径的攻击概率。最大 flow loss 和 loss 饱和度是根据 CVSS 的基础评分的相关参数计算得出, 最后根据每次攻击的损失和收益来评估攻击的效果。

Dorsemaine 等人[52]提出一种新的度量方法来评估物联网基础设施对遗留信息系统的影响。他们评估了典型的物联网体系结构: 本地环境层、传输层、数据存储与挖掘层和提供层中不同威胁对信息系统安全要素的影响与可能性, 通过计算每个威胁对信息系统的影响评分来比较威胁的严重程度, 对影响评分超过某一阈值的威胁实施针对性的缓解措施。但是该文章并没有描述威胁发生的可能性和对不同安全要素的影响是如何计算得到的。

赵健等人[53]将物联网系统面临的攻击按照攻击面和攻击点进行分类, 根据每种安全威胁的危害程度、发生概率以及补救措施的复杂程度, 利用模糊综合评价法进行分析, 构建了一个可对物联网系统进行定量安全分析的模型, 实现了物联网系统的安全量化评估。

2.6 安全测评标准

目前, 物联网安全测评和等级保护工作已经受到国家的高度重视, 发布了多项物联网安全相关的条例(意见稿)。例如《网络安全等级保护条例(征求意见稿)》、《信息安全技术 网络安全等级保护基本要求 第 4 部分: 物联网安全扩展要求(征求意见稿)》、《信息安全技术 网络安全等级保护测评要求 第 4 部分: 物联网安全扩展要求》。其中按照等级保护的思想, 对通用物联网架构提出了物联网系统安全等级保护模型, 指出物联网系统从末端节点、传感网、通讯网、物联设备的接入、异构网的融合、应用层、数据安全、控制管理等方面受到安全威胁, 并将物联网系统安全等级分为四级, 给出了各级系统的所有单项测评内容。

美国国家标准技术研究所(NIST)发布了物联网国际网络安全标准化现状报告, 从物联网具体应用的安全风险出发, 提出了密码学、网络事件管理、硬件保证、身份及访问管理、信息安全管理体系、资讯系统安全评估、网络安全、安全自动化和持续监

控、软件保障、供应链风险管理、系统安全工程等11 个方面的安全标准[54]。全球移动通信系统协会(GSMA)发布了 IoT 系统安全检查表, 给物联网设备及服务提供商提供了安全评估自检建议[55]。开放式 Web 应用程序安全项目(OWASP)发布了《物联网安全测试指南》, 也给出了物联网安全测试指标, 旨在帮助测试人员评估物联网空间中的物联网设备和应用程序[56]。

虽然国内外近几年发布了多项关于物联网安全测评的标准和指南, 但是物联网系统中存在的安全问题还是常常发出现, 可见物联网安全测评在实际实施中进行得不够充分, 亟需完善的测评工具对物联网系统进行有效的评估工作, 保证系统的安全可靠。

3 物联网安全保障技术测评需求

物联网节点面临计算能力、体积和功耗受限等挑战, 智慧城市等应用场景提出了大规模泛在异构连接和复杂跨域的需求。为了应对物联网大规模发展带来的挑战, 进几年, 物联网在绿色节点、智能网络管理、开放平台三个方面取得了广泛的研究进展。

为了实现高效节能的物联网设备管理、数据传输以及安全防护, 许多学者提出了轻量级加密算法、轻量级访问控制、轻量级入侵检测系统(IDS)等技术。为了高效管理网络资源, 提供数据传输效率, 智能网关、智能路由和边缘计算平台发展迅速。以往的物联网系统往往是独立的系统, 不对外部开放, 带来了信息不能共享等问题。为了提升信息的价值, 物联网的开放共享是技术发展的必然趋势。

这些物联网安全保障技术在为物联网系统提供安全服务之前, 我们必然需要对其进行深入的安全分析和测评, 只有通过了安全测评, 才能大规模地应用到实际的物联网系统中。

3.1 绿色节点

对于物联网系统, 传统的密码学方案的部署却遇到了困难, 这主要由几方面的原因造成: 首先, 大多数物联网设备的计算及通信性能较低, 很难满足很多传统密码方案所需的大量计算及通信开销; 同时, 过高的计算及通信开销会使设备能耗增高, 增加系统的维护成本; 其次, 物联网设备的存储模块也是受限的, 很难满足很多传统密码方案的存储需求。很多物联网设备(如 RFID)有着较高的时延要求, 需要密码方案有较好的实时性。近年来, 轻量级密码一直是物联网安全领域以及密码学领域的研究热点, 总结起来, 围绕轻量级密码的研究可以概括为三个方面——轻量级的密钥分发及管理、轻量级的密码算法以及轻量级的认证算法。

3.1.1 轻量级的密钥分发及管理

近年来, 由于轻量级公钥密码的研究(如 ECC)以及对称密码密钥分发的高通信复杂度、中间参数较多、不够灵活等缺点, 有人提出了基于公钥密码的密钥分发方案。 Seo 等人[57]提出一种不需证书的密钥分配方案, 该方案既保留了公钥密码灵活安全的密钥分发特性, 又没有引入高昂的证书管理开销。值得一提的是, 该方案主要针对的是动态网络模型, 该网络模型中, 有三种节点——基站、高性能节点、低性能节点, 三种节点的性能依次降低, 此外, 节点的位置会动态变化, 因此, 对密钥分配方案的灵活性要求较高。

3.1.2 轻量级密码算法

轻量级的密码算法可以分为轻量级的对称、非对称密码算法。与传统的密码算法类似, 密码方案的对称、非对称性是由其密钥是对称或是分为公私钥对的形式来划分的, 但与传统密码方案不同的是, 由于轻量级密码面向的物理设备大都是资源受限的, 轻量级的密码方案不仅需要满足安全性需求, 还需要满足轻量级需求。

Leander 等人[58]基于 DES 提出了 DESL, 其采用串行硬件结构并将 DES 中的 8 个原始 S 盒替换为一个重新设计的单一 S 盒, 降低了门复杂性, 同时采用密钥白化技术提高了加密算法的安全性。该算法能够有效抵抗差分攻击等。eSTREAM 项目[59]包括了 3 个面向轻量级设备的流密码方案: Grain v1、MICKEY 2.0 以及 Trivium。Grain[60] 方案的设计特点是其引入了两个移位寄存器, 一个为线性反馈, 另一个为非线性反馈, 原始 Grain 方案被指出易受相关攻击[61], Grain v1 修复了该问题。MICKEY [62] 的设计亮点是在移位寄存器中引入了不规则的时钟机制以获得更好的周期及更好的伪随机性, 从而提升了其安全性, MICKEY 原方案易受一些侧信道攻击, MICKEY 2.0 修复了这些问题。

与对称密码相比, 非对称密码的轻量化难度更高, 因为传统的公钥密码方案, 包括 RSA、 ECC、El Gamal 等都是基于某种复杂的数学难题, 通常会涉及到模乘、模幂等计算复杂度高的运算。早在 1995 年, Shamir [63]就对 RSA 进行了轻量化设计, 其设计思路是针对较小的明文空间, 选择特定的公钥参数, 这样, 在解密时, 可以减小模幂运算的模数, 进而起到减小解密复杂度的目的, 但是 Gilbert 等人[64]指出 Shamir 的轻量化 RSA 易受选择密文攻击, 之后, Coron[65] 通过对明文填充其自身的哈希值

以抵御上述的选择密文攻击。

3.1.3 轻量级认证算法

物联网中的认证算法不只需要满足轻量级需求, 还需要满足其他一些特殊的安全需求, 同时, 一些认证算法的设计也会利用物联网本身的一些特性进行设计。物联网环境下的认证方案需要应对的一个重要的安全威胁是物理攻击, 即对设备的篡改、复制。为应对该威胁, 需要一个安全机制来唯一标识各个节点, 且保证该标识不可伪造。

一种传统的标识方法为秘密共享, Dimitriou [66] 提出一种利用该思路设计了一种轻量级的面向 RFID 设备的认证方案, 在他们的方案中, 每个 RFID 标签与中心服务器之间共享一秘密的随机 ID 值, 该 ID 值在具体认证中的功能类似于一共享密钥, 且每次认证过后 RFID 标签与中心服务器会使用哈希函数同步更新此 ID 值。Song 等人[67] 的 RFID 认证方案中考虑了对中心服务器的伪装攻击, 作者指出之前的工作中大都未考虑这种攻击模式, 存在被攻击的可能, 他们通过一个中心服务器与 RFID 标签的共享秘密实现了 RFID 标签与中心服务器间的双向认证, 且该方案的计算及存储开销也优于先前的方案。 Cai 等人[68] 指出 Song 的方案对一些主动攻击可能丧失安全性, 并提出了改良方案, 改良方案中会引入一些存储与计算开销, 但修复了原方案的安全漏洞。

另一条重要的思路是在认证中嵌入设备的物理指纹信息。Kulseng [69] 利用 PUF 设计了一个 RFID 的双向认证协议, 该方案中的计算及存储开销都较低, 轻量化程度较高。该设计的主要思想是利用 PUF 生成链式的共享认证秘密, 后一次认证产生的共享秘密必须与前一次共享秘密具有可认证的公共结构, 这样, RFID 读写器通过该共享秘密可验证 RFID 标签的物理特征与前一次认证的标签一致, 而 RFID 标签通过该共享秘密验证 RFID 读写器与前一次认证的读写器一致, 从而完成了双向认证。但是, Gope [70]近期的工作中指出, 现有的工作仍无法满足一些关键的安全性指标, 包括前向安全性、针对 DOS 攻击的安全性及物理攻击。

3.2 智能网络

物联网环境下的海量异构设备、异质网络给设备和网络管理带来前所未有的挑战。目前物联网中使用的设备包括各种感知设备和 RFID 设备, 使用的协议有 RFID、Bluetooth、Zigbee、NB-IoT(Narrowband IoT)、LoRA(Long Range)、WiFi 等, 这使得物联网环境异常复杂, 难以维护和管理。面对这些问题, 需要一种智能化的方法来解决。近年来智能网络管理技术在智能网关、智能路由和边缘计算三个方面发展迅速, 形成了不同的产品和解决方案, 但也面临着数据安全和隐私保护等问题。

3.2.1 智能网关

为了解决不同网络之间的数据传输以及不同协议间的数据转换问题, 达到物联网设备间的全面互联互通和协同感知, 网关的智能化越来越重要。智能网关在协议转换、异构数据理解、设备发现等方面提供了有效保障, 但是也存在着严重的安全问题。

物联网网络层使用的协议众多, 智能网关的基本功能就是需要实现多协议的融合, 支持多协议格式适配。Chang 等人[71]设计了一个支持多接口的智能网关, 每个接口配备一个协议模块且接口间可协同工作。但该网关难以更换端口所支持的协议。为此, Guoqiang 等人[72]设计了一个自适应的智能网关, 该网关内置了六种不同的物联网协议, 当数据传入智能网关时可自动识别协议类型并将数据转化为统一格式, 以实现异质物联网与传统互联网之间的通信。

不同物联网设备会产生不同表示形式的数据, 这种异构数据阻碍了物联网应用程序对数据的解释和有效利用[73-74]。为了解决异构数据传输问题, Mahmud 等人[75]提出了一种基于轻量级语义 Web 的数据注解方法, 该方法利用传感器相关域本体生成数据的语义信息并为与云端数据交互提供服务。Yacchirema 等人[76]提出了一种新型智能网关, 该网关从数据格式转换、协议转换、数据存储和数据处理这四个方面实现了通信协议和数据间的互操作性。该智能网关配有物联网常用协议, 能将来自异构设备的数据转化为标准格式(JSON 格式)。此外该网关还可以存储数据并进行分析, 将满足特定条件的事件发送给用户, 为用户提供个性化服务。

用户购买新的物联网设备时, 需要根据安装手册手动安装设备。针对该问题, Kang 等人[77]提出的网关实现了设备发现和注册的半自动化配置, 利用 CoAP 协议实时监测设备的状态和数据。Iveta 等人[78]设计的智能网关将物理设备抽象表示为虚拟设备, 可以处理设备损坏问题, 并且虚拟设备简化了物理设备和云应用的连接。

物联网大量使用无线传输技术, 攻击者可以随意窃取、篡改或删除链路上的数据, 并伪装成网络实体截取业务数据。无线传输中最常见的攻击有窃听攻击、中间人攻击和侧信道攻击等。足以说明目前在对物联网智能网关的安全测评工作不够充分, 需

进一步完善安全测试和评估工作。

3.2.2 智能路由

随着网络规模的扩大, 无线自组织网络在无线通信领域的地位愈发重要, 对路由协议的智能性提出了新的需求。路由协议不仅需要满足大规模网络通信需求, 还应该支持对网络中的恶意节点具有一定的敏感性。Lee 等人[79] 提出了一种自组织的、自适应的智能集群和路由方法。该方案能够自动化识别节点故障并自动调整集群和路由。文献[80]在路由协议中引入信任值概念, 保证只有信任值高的节点才能被选做集群头, 一定程度上保证了网络的安全。

强化学习因其对不同环境的良好学习能力在异质物联网环境中具有广泛的应用。无线传感网中的路由协议设计需要考虑能量消耗、错误容忍、可扩展性和区域覆盖等问题。基于机器学习或者强化学习的路由协议能够提供一个节省能量、延长网络生命周期的最优路径选择策略, 并能通过转化路由问题到子空间中减少路由计算复杂度[81]。Sun 等人[82]在无线自组网中用 Q 学习来增强多播路由算法, 该方法减少了路径搜索开销, 但是能量使用效率是关键需求。Dong 等人[83]借鉴文献[82]的想法, 将强化学习应用于超宽带广播中来增强地理路由, 其奖励计算过程考虑了节点能量消耗和消息延迟。

RPL 是用于低功耗和有损网络的路由协议, 广泛应用于智能家居、智能城市等场景。 RPL 创建网络拓扑的有向非循环图(DAG)。对 RPL 协议的攻击涉及针对网络资源、拓扑结构、网络流量的多种攻击, 其中常见的有 rank 属性攻击、版本号攻击等。Abdul Rehman [84] 等人提出了针对 rank 属性的新型攻击, 通过修改目标函数和 rank 属性, 迫使其相邻节点通过恶意节点路由其数据。

3.2.3 边缘计算

物联网应用场景非常广泛, 包括智能交通、智能家居和智能制造等。这些行业应用业务需求复杂, 除了基本的业务需求外, 还可能包括传输时延、数据分析和智能决策等额外的需求。由于云计算服务延迟较高, 无法满足物联网应用的特定业务需求, 边缘计算除了提供基础的数据存储、按需分配资源等功能外, 还能够保证满足低时延、高算力和隐私保护等特殊需求。

边缘计算相对于云计算而言, 将智能处理能力拓展到感知设备侧, 云计算面临的安全问题在边缘系统中仍然存在。边缘计算除了受到传统的网络安全和物理安全问题影响外, 还受到一些新兴技术带来的安全问题。NFV(Network Function Virtualization) 和 SDN 是边缘平台常用的技术, 面临拒绝服务和恶意注入等攻击。边缘平台和感知节点间任务卸载的分配策略以及任务中用户隐私保护等问题仍有待解决。边缘平台的访问控制和跨域验证等安全机制也会受到伪造攻击等问题。因此边缘计算平台也需要诸如入侵检测、访问控制以及安全防御等安全防护措施的保护, 才能给感知设备提供安全智能的服务。

3.3 开放平台

目前物联网应用和感知设备紧紧耦合在一起, 信息存储格式各异, 无法在应用间共享, 最终会成为信息孤岛。为了促进物联网相关生态系统的发展, Kim 等人[86]指出开放物联网服务需要满足两个重要功能, 一是开放物联网服务框架应该是基于开放软件的架构且面向开发者的架构, 鼓励企业利用开放的物联网平台快速开发和实现创新服务, 促进物联网相关大众市场的快速增长。二是通过为用户提供物联网服务的快速搜索, 大量用户可以在短时间内使用物联网服务, 从而促进与物联网相关的产品、应用程序和服务的快速增长。因此, 物联网开放平台的需求如表 1 所示。本节介绍物联网开放平台的发展现状及存在的安全问题。

表 1 物联网开放平功能需求

Table 1 Requirements of Open Platform for IoT

需求	描述
海量异构受限终端接入	设备功能各异、资源受限且设备数量巨大
资源管理	设备管理、网络管理等
能力开放	允许接入不同应用, 支持开放接口调用
移动性	基本设计标准考虑移动性
语义服务	创建基于语义的智能服务
自组织网络	自组网络、可靠的通信
海量数据存储	设备数量大、数据量大
特殊 QoS 保证	低延迟等特殊 QoS 保证
安全和隐私	保证数据安全和隐私保护

3.3.1 开放平台

近几年物联网开放平台取得了快速的发展, 在学术界及产业界都提出了相关的物联网开放平台, 提供开放的物联网服务, 但是其中也存在一定的安全问题和隐私问题。

许多学者针对上述物联网开放平台需求, 设计了物联网开放平台架构。Park 等人[85]提出了一个包括开放平台和异质网络中间件的功能架构, 如图 1 所示。该开放平台包括 7 个函数实体, 支持即插即用

设备管理和信息查询等功能。Kim 等人[86]从物联网开放平台服务流的角度设计了如图 2 所示的平台架构。该架构包含了 Planet 平台、Mashup 平台、Store 平台和 Device 平台。全部平台都使用开放的 RESTful 接口，各平台各司其职相互协作响应用户请求。上述描述的开放平台只考虑了平台功能的提供，没有考虑底层物联网系统中的安全问题，如接入控制、数据隔离等安全措施。

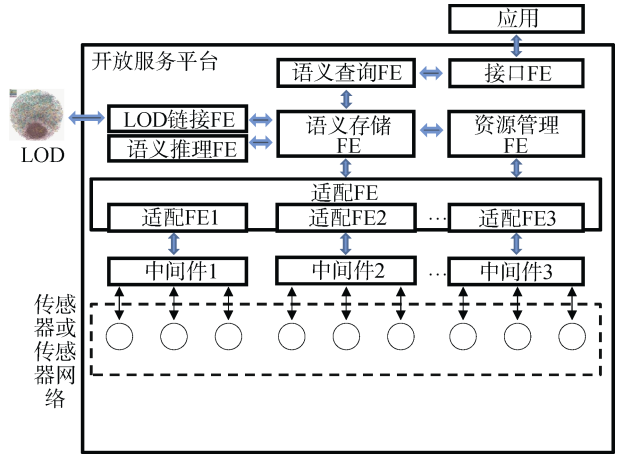

图 1 Park 等人的物联网开放平台[85]

Figure 1 Park et al.'s IoT Open Platform[85]

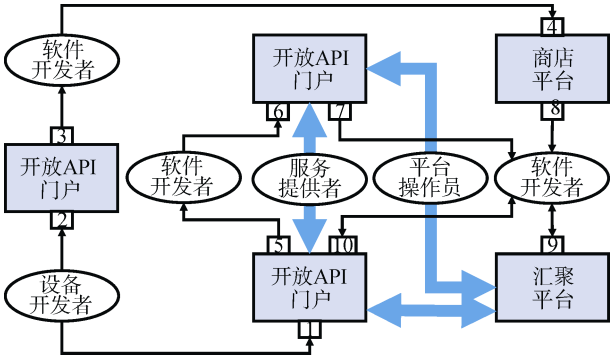

图 2 Kim 等人的物联网开放平台[86]

Figure 2 Park et al.'s IoT Open Platform[86]

国内外互联网企业也纷纷发布了自己的物联网开放平台，为物联网企业和个人开发者提供了丰富简单的开发工具包。亚马逊物联网平台是由云端托管的、支持云应用的开放平台，提供了终端节点和网关等边缘侧设备，提供多种 SDK 集成感知设备，无缝整合了亚马逊云提供的数据库、数据处理、消息队列等云服务。平台还提供设备监控功能和丰富的开发接口说明以及开发者文档[87]。三星的 SmartThings 平台提供各种设备接入、智能应用开发能力，并允许用户使用代码模板创建应用，对开发者十分友好[88]。

阿里云物联网平台致力于实现万物互联的美好世界，提供基于端边云一体化、人工智能、安全的物联网基础平台，可高效连接、管理设备[89]。中国移动的 OneNET 开放平台目前日活跃设备连接量已经达到 4 亿，该平台提供一整套的物联网应用开发服务，可以解决协议适配、海量连接、数据存储设备管理等物联网开发共性问题，能够有效促进物联网快速发展[90]。

3.3.2 安全问题

目前学术界对物联网开放平台的安全问题研究正在持续进行中，目前主要集中在开放平台粗粒度的权限授予机制和设备交互的安全问题。Fernandes 等人[91]分析了三星 SmartThings 平台开源的 499 个 SmartApp，发现由于该平台粗粒度的能力授予机制，其中 55%的应用存在滥用能力的情况，并且存在许多用户隐私数据盗用和安防问题。该文献还揭露了许多由粗粒度授权管理机制带来的隐私泄露问题。Celik 等人[92]通过将 groovy 代码转换成中间表示，设计了一款智能应用的污点源到 Sink 的数据流分析工具，并提供开放的 Web 接口，只需提供源码即可分析出存在可能的隐私泄露点的数量，但该工具只分析了单应用，无法完成跨应用的污点分析。

Jia 等人[93]考虑到物联网开放平台粗粒度的权限管理机制的缺陷，提出一种基于上下文的权限控制系统 ContextIoT,根据细粒度的上下文信息来描述敏感的数据操作，并使用包含上下文数据信息的运行时提示来帮助用户控制应用的敏感操作，但该工具过于专业化，普通用户难以使用。Ding 等人[94]提取出物联网应用与环境的交互链，并使用聚类算法计算每条交互链的风险值。Fernandes 等人[95]分析了包括 IFTTT[96]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。

3.4 测评需求

轻量级安全保障技术在提出时都会有严格的安全证明，但是在实际的实现过程中往往会存在传统的代码上的漏洞，因此我们需要对秘钥管理协议、密码算法以及认证协议进行完善的安全测评，尤其是密码生成和管理算法。

物联网智能网关面临多种攻击问题，智能路由也存在协议设计上的漏洞，边缘计算平台也遇到拒绝服务和恶意注入攻击。因此，我们需要对物联网网

关进行深入的安全评估, 对协议进行严密的形式化验证和实现上的安全测试, 边缘平台也需要提供充分的安全防御措施。

物联网开放平台的发展可谓百花齐放, 百家争鸣。但是在为用户提供智能服务之前, 缺乏完善地安全防护设计以及安全测评工作, 导致了发生了上述数据盗用、隐私泄露以及安防问题。

目前针对物联网开放平台的研究工作主要关注于平台粗粒度的权限管理机制带来的安全问题及其增强技术实现, 而且目前的方法大多针对三星 SmartThings、IFTTT 平台, 不具备通用性。因此物联网开放平台的安全测评研究需要更加深入, 为开放平台提供通用的测评方案。

4 物联网安全测评面临的挑战和未来研究方向

物联网由于节点种类繁多、功能异构, 泛在异质网络连接等问题使得物联网系统的自动化测试与评估变得异常复杂, 目前的等级保护测评工作大多以手工为主、少量自动化工具为辅的方式进行。而且目前智慧城市等复杂应用场景对物联网系统提出了新的技术要求, 因而在绿色节点、智能网络、开放平台的技术要求下, 实施物联网安全测评也面临更加严峻的挑战。下文将从安全测评、新技术测评需求两个方面分析物联网安全测评研究面临的挑战并探讨未来的研究方向。

4.1 安全测评

目前物联网系统安全测评工作仅存在少量国内外的测评标准, 一方面, 国家有关部门应该实施对物联网相关产品安全测评工作的监督; 另一方面, 安全测评相关的学术研究不够完善, 对产品的测评工作缺乏在大规模场景下的安全检验。

通过前文分析, 我们认为, 可以从以下三个方面, 进一步促进物联网安全测评工作朝着自动化的方向发展。

1) 大规模物联网设备固件分析和漏洞挖掘技术。设计高精度大规模物联网感知设备固件提取及分析方法和硬件安全评估方法。针对设备可能发生的侧信道攻击, 构建攻击和防御模型, 保证设备的安全性。

2) 支持大规模异构真实设备和虚拟设备的混合仿真协议测评技术。针对目前大规模的物联网设备接入现状, 设计大规模并行分布式虚实结合的混合仿真测试平台, 对物联网中不同的感知网络协议进行安全分析和测试。

3) 多端点交互安全分析与评估技术。针对物联网应用参与方较多的特点, 构建物联网应用交互模型, 分析多方交互导致的安全问题, 并揭露安全风险信息。

4.2 绿色、智能、开放技术的安全测评

随着物联网设备的不断增长, 网络环境的愈加复杂, 开放服务的不断丰富, 物联网新技术不断被提出。但是从目前的分析来看, 物联网安全在这几个方面均面临较严重的安全问题。

物联网大规模应用的前提是需要符合绿色发展的理念, 尽可能地降低安全技术的能耗。低功耗的安全技术不仅需要从数学上严格证明算法的安全性, 也需要对实现代码进行深入的安全测试, 从理论上和实现上保证安全算法的安全可靠。

物联网中的异构设备和异质网络资源给安全测评工作带来巨大的挑战。大规模的物联网系统固件提取、分析是个艰巨的任务, 我们还需要深入对系统固件的安全分析工作, 尽可能多地分析系统中可能存在的安全问题, 防止被黑客利用造成不可挽回的经济损失。

智能网关、智能路由以及边缘计算平台的快速发展, 使得物联网更加易于操作, 为用户提供智能便捷的服务。然而智能网关、智能路由都存在各自的安全问题, 我们可以从以下三个方面完善对智能网络的测评工作。

1) 设计物联网安全指纹提取和设备发现的测评方法。构建指纹伪造攻击模型, 分析新兴的指纹提取技术和设备发现和管理技术的安全问题。

2) 针对目前快速发展的边缘计算平台, 设计测评方法对其在访问控制、数据隐私保护以及资源调度等方面的攻击防御能力。

3) 设计常用机器学习及深度学习算法的安全测评方法, 保证智能算法的安全。当然, 目前对 AI 算法的测试分析是个非常火热的方向。

未来几年, 物联网开放平台应该更加关注安全防护手段以及安全开放体系的建设。在安全访问控制方面, 通用的细粒度授权机制、多用户访问机制以及应用与环境交互造成的安全问题的分析将会是物联网开放测评的未来研究重点。

5 总结与展望

在物联网迅速应用于各大产业后, 安全问题层出不穷, 造成的财产损失较大、影响严重。物联网测评技术能够为物联网应用提供安全保障, 本文总结了现有物联网测评技术和风险评估技术, 并指出其

中的不足。调研了绿色节点、智能网络和开放平台的安全现状, 指出这三个方面的安全测评工作亟需进行, 切实保障物联网安全健康地发展。

面对物联网严峻的安全问题和能耗开销、大规模网络管理以及开放服务这三个维度的挑战, 急需设计一个绿色智能开放的安全物联网体系, 并构建一个高效易用的自动化物联网安全测评工具, 能够满足物联网安全测评基本要求, 并提供对物联网新特性新要求的有效评估方法。

致　谢　衷心感谢各位评审专家对本文提出的宝贵意见。本研究得到科技部网络空间安全项目 物联网与智慧城市安全保障关键技术研究 (No.2018YFB08034), 基金委杰出青年项目 (No.6162520), 中国科学院前沿科学重点研究项目(No.QYZDY-SSW-JSC00)资助。

参考文献

[1] IoT analytics, “Iot analytics(2014),” 2014. [Online]. Available: https://iot-analytics.com/Internet-of-things-definition/

[2] 于文平, “《2017-2018 中国物联网发展年度报告》发布,” *物联网技术*, vol. 8, no. 10, pp. 5–6, 10, 2018.

[3] 安天实验室, “Iot 僵尸网络严重威胁网络基础设施安全北美 dns 服务商遭 mirai 木马 ddos 攻击的分析思考,” 2016.

[4] 新浪, “橘子皮解锁手机,” 2018. [Online]. Available: http://news.sina.com.cn/o/2018-01-26/doc-ifyqyqni3427619.shtml

[5] 中国国家标准化管理委员会. GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求[S]. 北京: 中国标准出版社, 2012.

[6] O. Abdelmalek, D. Hely, and V. Beroulle, “Emulation based fault injection on uhf rfid transponder,” in *Design and Diag- nostics of Electronic Circuits & Systems, 17th International Symposium on*. IEEE, 2014, pp. 254–257.

[7] I. Mezzah, H. Chemali, and O. Kermia, “Emulation-based fault analysis on rfid tags for robustness and security eval- uation,” *Microelectronics Reliability*, vol. 69, pp. 115–125, 2017.

[8] O. U. S. P. Group, “Frontier ridac,” https://www.ee.oulu.fi/research/ouspg/RIDAC, accessed Oct 27, 2018.

[9] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, and L. Castedo, “Reverse engineering and security evaluation of commercial tags for RFID-based IoT applications,” *Sensors*, vol. 17, no. 1, p. 28, 2016.

[10] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, “Systematically evaluating security and privacy for consumer IoT devices,” in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, 2017, pp. 1–6.

[11] Wikipedia contributors, “Reflection attack, ”2017, [Online;accessed 9-November-2018]. Available: https://en.wikipedia.org/w/index.php?title=reflection_attack&oldid=787717850.

[12] Shodan, “Shodan,” https://www.shodan.io/, accessed Oct 27, 2018.

[13] H. Al-Alami, A. Hadi, and H. Al-Bahadili, “Vulnerability scanning of IoT devices in jordan using shodan,” in Appli cations of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS), 2017 2nd Inter national Conference on the. IEEE, 2017, pp. 1–6.

[14] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, “Assessing medical device vulnerabilities on the internet of things,” in Intelligence and Security Informat- ics (ISI), 2017 IEEE International Conference on. IEEE, 2017, pp. 176–178.

[15] M. Anisetti, R. Asal, C. A. Ardagna, L. Comi, E. Damiani, and F. Gaudenzi, “A knowledge-based IoT security checker,” in *European Conference on Parallel Processing*. Springer, 2018, pp. 299–311.

[16] 神州绿盟信息安全科技股份有限公司, “绿盟工控漏洞扫描系统,” http://www.nsfocus.com.cn/products/details_36_ 1851.html, accessed Oct 19, 2018.

[17] 北京匡恩网络科技有限责任公司, “匡恩工业控制网络安全漏洞挖掘检测平台,” http://www.cechina.cn/company/168104_68597/productdetail.aspx, accessed Oct 19, 2018.

[18] S. Ni, Y. Zhuang, J. Gu, and Y. Huo, “A formal model and risk assessment method for security-critical real-time embedded systems,” *Computers & Security*, vol. 58, pp. 199– 215, 2016.

[19] F. M. Tabrizi and K. Pattabiraman, “Formal security anal- ysis of smart embedded systems,” in *Proceedings of the 32nd Annual Conference on Computer Security Applica tions*. ACM, 2016, pp. 1–15.

[20] Y.Q. Shen and Z.W. Xu, “Design of Universal Embedded System Software Test Platform,” *Computer Engineering and Applications,* 2007, 43(15) : pp. 83-85.
(沈永清, 徐中伟, “通用嵌入式系统软件测试平台的设计,” *计算机工程与应用,* 2007, 43(15): pp. 83-85).

[21] Costin, A., Zaddach, J., Francillon, A., & Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. *In 23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp: 95-110).

[22] Chen, D. D., Woo, M., Brumley, D., & Egele, M. (2016, February). Towards Automated Dynamic Analysis for Linux-based Embedded Firmware. In NDSS (pp. 1-16).

[23] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and K. Srivastava, “Analyzing the cyber-physical impact of cyber events on the power grid,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[24] nsnam, “ns-3 network simulator,” https://www.nsnam.org/, [Online; accessed 8-November-2018].

[25] U.of Utah and the Flux Research Group, “Deterlab: Cyber-defense

technology experimental research labora- tory," https://www.isi.deterlab.net/index.php3, [Online; accessed 8-November-2018].

[26] N. Saxena, V. Chukwuka, L. Xiong, and S. Grijalva, "Cpsa: A cyber-physical security assessment tool for situational awareness in smart grid," in *Proceedings of the 2017 Work shop on Cyber-Physical Systems Security and PrivaCy*. ACM, 2017, pp. 69–79.

[27] Gorecki, C. Behrens, C. Zheng, C. Westphal, D. Jedermann, R. Lang, and W. und Laur, "Tap-sns –a test platform for secure communication in wireless sensor networks for logistic applications," 2007.

[28] J. Andersen and J. E. Bardram, "Blig: A new approach for sensor identification, grouping, and authorisation in body sensor networks," in *4th International Workshop on Wear able and Implantable Body Sensor Networks (BSN 2007)*. Springer, 2007, pp. 223–229.

[29] P. Ballal, V. Giordano, P. Dang, S. Gorthi, J. Mireles, and F. Lewis, "A labview based test-bed with off-the-shelf components for research in mobile sensor networks," in *Computer Aided Control System Design, 2006 IEEE Inter- national Conference on Control Applications, 2006 IEEE International Symposium on Intelligent Control, 2006 IEEE*. IEEE, 2006, pp. 112–118.

[30] V. Handziski, A. Köpke, A. Willig, and A. Wolisz, "Twist: a scalable and reconfigurable testbed for wireless indoor experiments with sensor networks," *in Proceedings of the 2nd international workshop on Multi-hop ad hoc networks*: from theory to reality. ACM, 2006, pp. 63–70.

[31] I. Chatzigiannakis, S. Fischer, C. Koninis, G. Mylonas, and D. Pfisterer, "Wisebed: an open large-scale wireless sensor network testbed," *in International Conference on Sensor Applications, Experimentation and Logistics*. Springer, 2009, pp. 68–87.

[32] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, Vandaele et al., "Fit iot-lab: A large scale open experimental IoT testbed," in Internet of Things (WF-IoT), *2015 IEEE 2nd World Forum on*. IEEE, 2015, pp. 459–464.

[33] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part i: Exact model," *IEEE Transactions on Power Apparatus and systems*, no. 1, pp. 120–125, 1970.

[34] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[35] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in Preprints of the First Workshop on Secure Control Systems, CPSWEEK, vol. 2010, 2010.

[36] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to detect bad data injection attack in smart grid," *in Computer Communications Workshops (INFOCOM WK SHPS)*, 2013 IEEE Conference on. IEEE, 2013, pp. 49–54.

[37] A. Datta and M. A. Rahman, "Cyber threat analysis frame- work for the wind energy based power system," *in Pro ceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. ACM, 2017, pp. 81–92.

[38] K. C. Park and D.-H. Shin, "Security assessment framework for IoT service," *Telecommunication Systems*, vol. 64, no. 1, pp. 193–209, 2017.

[39] Ö. Uygun, H. Kaçamak, and Ü. A. Kahraman, "An inte- grated dematel and fuzzy anp techniques for evaluation and selection of outsourcing provider for a telecommunication company," *Computers & Industrial Engineering*, vol. 86, pp. 137–146, 2015.

[40] Y.-L. Huang and W.-L. Sun, "An ahp-based risk assessment for an industrial IoT cloud," in 2018 *IEEE International Conference on Software Quality, Reliability and Security Companion* (QRS-C). IEEE, 2018, pp. 637–638.

[41] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," *in Proceedings of the 9th ACM Conference on Computer and Communica- tions Security*. ACM, 2002, pp. 217–224.

[42] Y. Liu and H. Man, "Network vulnerability assessment using bayesian networks," in Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005, vol. 5812. International Society for Optics and Photonics, 2005, pp. 61–72.

[43] R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley, "Optimal security hardening using multi-objective optimization on attack tree models of networks," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 204–213.

[44] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow," *IEEE ACCESS*, vol. 6, pp. 8599–8609, 2018.

[45] J. Dawkins, C. Campbell, and J. Hale, "Modeling network attacks: Extending the attack tree paradigm," in *Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection*, 2002, pp. 75–86.

[46] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, "A safety/security risk analysis approach of industrial control systems: A cyber bowtie–combining new version of attack tree with bowtie analysis," *Computers & Security*, vol. 72, pp. 175–195, 2018.

[47] W. Asif, I. G. Ray, and M. Rajarajan, "An attack tree based risk evaluation approach for the internet of things," in *Proceedings of*

the 8th International Conference on the Internet of Things. ACM, 2018, p. 6.

[48] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012.

[49] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnera- bility exploitations," *IEEE Access*, vol. 6, pp. 43 586–43 601, 2018.

[50] M. Schiffman, "Common vulnerability scoring syste (cvss)," http://www.first.org/cvss/cvss-guide.html, accessed Oct 19, 2018.

[51] Wang, H., Chen, Z., Zhao, J., Di, X., & Liu, D. (2018). A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow. IEEE Access, 6, 8599-8609.

[52] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "A new threat assessment method for integrating an IoT infrastructure in an information system," in *Dis- tributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 105–112.

[53] J. Zhao, R. Wang, Z.M. Li, M. Lei, and M.Y. Ma, "Security Threats and Risk Assessment for IoT System," *Journal of Beijing University of Posts and Telecommunications*, vol. 40, pp. 135–139, 2017.
(赵健, 王瑞, 李正民, 雷敏, 马敏耀, "物联网系统安全威胁和风险评估," *北京邮电大学学报*, vol. 40, pp. 135–139, 2017.)

[54] NISTIR Information Technology Laboratory, "Interagency report on status of international cybersecurity standardization for the internet of things (IoT)," 2018.

[55] https://www.gsma.com/iot/iot-security-assessment/

[56] OWASP Internet of Things Project, "Tester IoT security guidance," 2018, [Online; accessed 24-November-2018]. [Online]. Available: https://www.owasp.org/index.php/IoT_Testing_Guides

[57] S.-H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371–383, 2015.

[58] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "Newlightweight des variants," *in International Workshop on Fast Software Encryption*. Springer, 2007, pp. 196–210.

[59] C. Cid and M. Robshaw, "The estream portfolio in 2012," 2012.

[60] M. Hell, T. Johansson, and W. Meier, "Grain: a stream cipher for constrained environments," *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 86–93, 2007.

[61] C. Berbain, H. Gilbert, and A. Maximov, "Cryptanalysis of grain," in *International Workshop on Fast Software Encryption*. Springer, 2006, pp. 15–29.

[62] S. Babbage and M. Dodd, "The stream cipher mickey 2.0," ECRYPT Stream Cipher, 2006.

[63] A. Shamir, "Rsa for paranoids," *CryptoBytes*, vol. 1, pp. 1–4, 1995.

[64] H. Gilbert, D. Gupta, A. Odlyzko, and J.-J. Quisquater, "Attacks on shamir's ' rsa for paranoids' ," *Information Processing Letters*, vol. 68, no. 4, pp. 197–199, 1998.

[65] J.-S. Coron, A. Gouget, P. Paillier, and K. Villegas, "Spake: A single-party public-key authenticated key exchange protocol for contact-less applications," *in International Conference on Financial Cryptography and Data Security*. Springer, 2010, pp. 107–122.

[66] T. Dimitriou, "A lightweight rfid protocol to protect against traceability and cloning attacks," in Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on. IEEE, 2005, pp. 59–66.

[67] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in Proceedings of the *first ACM conference on Wireless network security*. ACM, 2008, pp. 140–147.

[68] S. Cai, Y. Li, T. Li, and R. H. Deng, "Attacks and improvements to anrifd mutual authentication protocol and its extensions," in Proceedings of the *second ACM conference on Wireless network security*. ACM, 2009, pp. 51–58.

[69] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for rfid systems,"*in INFOCOM*, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–5.

[70] P. Gope, J. Lee, and T. Q. Quek, "Lightweight and practical anonymous authentication protocol for rfid systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[71] C.-T. Chang, C.-Y. Chang, K.-P. Shih, R. D. B. Martinez, P.-T. Chen, and Y.-D. Chen, "An IoT multi-interface gateway for building a smart space," *Open Journal of Social Sciences*, vol. 3, no. 07, p. 56, 2015.

[72] S. Guoqiang, C. Yanming, Z. Chao, and Z. Yanxu, "Design and implementation of a smart iot gateway," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, *Physical and Social Computing*. IEEE, 2013, pp. 720–723.

[73] Z. Ding, Q. Yang, and H. Wu, "Massive heterogeneous sensor data management in the internet of things," in Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, *Physical and Social Computing*. IEEE, 2011, pp. 100–108.

[74] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[75] M. Al-Osta, B. Ahmed, and G. Abdelouahed, "A lightweightsemantic web-based approach for data annotation on iot gateways," *Procedia computer science*, vol. 113, pp. 186–193, 2017.

[76] D. C. Yacchirema-Vargas and C. E. Palau Salvador, "Smart iot gateway for heterogeneous devices interoperability," in IEEE Latin

America Transactions, vol. 14, no. 8. *Institute of Electrical and Electronics Engineers (IEEE)*, 2016, pp. 3900–3906.

[77] B. Kang, D. Kim, and H. Choo, "Internet of everything: A large-scale autonomic iot gateway," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 3, no. 3, pp. 206–214, 2017.

[78] I. Zolotová, M. Bundzel, and T. Lojka, "Industry iot gateway for cloud connectivity," in IFIP International Conference on *Advances in Production Management Systems*. Springer, 2015, pp. 59–66.

[79] K. Lee and H. Lee, "A self-organized and smart-adaptive clustering and routing approach for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 8, no. 1, p. 156268, 2012.

[80] M. Conti, P. Kaliyar, and C. Lal, "Remi: A reliable and secure multicast routing protocol for IoT networks," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM, 2017, p. 84.

[81] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014.

[82] R. Sun, S. Tatsumi, and G. Zhao, "Q-map: A novel multicast routing method in wireless ad hoc networks with multiagent reinforcement learning," in TENCON'02. Proceedings. 2002 IEEE Region 10 Conference on Computers, Communications, *Control and Power Engineering*, vol. 1. IEEE, 2002, pp. 667–670.

[83] S. Dong, P. Agrawal, and K. Sivalingam, "Reinforcement learning based geographic routing protocol for uwb wireless sensor network," *in Global Telecommunications Conference*, 2007. GLOBECOM'07. IEEE. IEEE, 2007, pp. 652–656.

[84] A. Rehman, M. M. Khan, M. A. Lodhi, and F. B. Hussain, "Rank attack using objective function in rpl for low power and lossy networks," *in Industrial Informatics and Computer Systems* (CIICS), 2016 International Conference on. IEEE, 2016, pp. 1–5.

[85] Park D H, Bang H C, Pyo C S, et al. Semantic open IoT service platform technology[C]//2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE, 2014: 85-88.

[86] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, 2013.

[87] Amazon, "Amazon IoT," 2018, [Online; accessed 17-November-2018].[Online].Available:https://aws.amazon.com/cn/iot/

[88] Smartthings, "Smartthings IoT," 2018,[Online; accessed 17-November-2018].[Online].Available: https://www.smartthings.com/

[89] 阿里云, "阿里云 IoT," 2018, [Online; accessed 17-November-2018]. [Online]. Available: https://iot.aliyun.com/

[90] 中国移动, "中移物联网," 2018,[Online; accessed 17-November-2018].[Online].Available:https://open.iot.10086.

[91] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *2016 IEEE Symposium on Security and Privacy (SP). IEEE*, 2016, pp. 636–654.

[92] Z. B. Celik, L. Babun, A. K. Sikder, H. Aksu, G. Tan, P. Mc Daniel, and A. S. Uluagac, "Sensitive information tracking in commodity IoT," *arXiv preprint arXiv:1802.08307,* 2018.

[93] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, A. Prakash, and S. J. Unviersity, "Contexlot: Towards providing contextual integrity to appified IoT platforms." in *NDSS*, 2017.

[94] W. Ding and H. Hu, "On the safety of IoT device physical interaction control," in Proceedings of the *2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 832–846.

[95] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Decentralized action integrity for trigger-action IoT platforms," *in Proc. Network and Distributed Systems Symposium* (NDSS), 2018, pp. 18–21.

[96] I. Platform, "IFTTT," https://ifttt.com/discover, accessed Oct 19, 2018.

陈钊 2017 年在四川大学软件工程专业获得学士学位。现在中国科学技术大学计算机软件与理论专业攻读硕士学位。研究领域为物联网安全、安全分析。研究兴趣包括: 物联网安全、安全测评。Email:chen95@mail.ustc.edu.cn

曾凡平 2009 年在中国科学技术大学信息安全专业获得博士学位。现任中国科学技术大学副教授。研究领域为网络信息安全、软件分析与测试。研究兴趣包括: 网络(物联网)与系统安全、软件分析与测试。Email:billzeng@ustc.edu.cn

陈国柱 2018 年在安徽大学软件工程专业获得学士学位。现在中国科学技术大学计算机软件与理论专业攻读硕士学位。研究领域为物联网安全测评、物联网绿色测评。研究兴趣包括: 物联网应用安全分析。Email: chengz18@mail.ustc.edu.cn

张燕咏 2002 年获得美国宾夕法尼亚州立大学计算机科学与工程专业博士。IEEE Fellow, 现任中国科学技术大学教授, 博导。研究领域为无线传感网系统、物联网、普适计算。研究兴趣包括: 物联网、普适计算、未来互联网等。Email: yanyongz@ustc.edu.cn

李向阳 2001 年获得美国伊利诺伊大学厄巴纳-香槟分校(UIUC)计算机科学专业博 士。IEEE Fellow, ACM 杰出科学家, 现任 ACM 中国联合主席, 中国科学技术大学教授、博导。 研究兴趣主要为物联网、物联网安全、大数据共享与交易、机制设计和算法分析等。 六次获国际会议最佳论文奖。Email: xiangyangli@ ustc.edu.cn