计算机研究与发展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202330482
60(10): 2271−2290, 2023

物联网设备安全检测综述

张　妍[1,2]　黎家通[1,2]　宋小祎[1,2]　范钰婷[3]　路晔绵[4]　张若定[1,2]　王子馨[1,2]

[1](中国科学院信息工程研究所　北京　100093)

[2](中国科学院大学网络空间安全学院　北京　100049)

[3](成都信息工程大学网络空间安全学院　成都　610000)

[4](中国信息通信研究院　北京　100191)

(zhangyan@iie.ac.cn)

Survey of IoT Device Security Detection

Zhang Yan[1,2], Li Jiatong[1,2], Song Xiaoyi[1,2], Fan Yuting[3], Lu Yemian[4], Zhang Ruoding[1,2], and Wang Zixin[1,2]

[1](*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093)

[2](*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049)

[3](*School of Cyberspace Security*, *Chengdu University of Information Technology*, *Chengdu* 610000)

[4](*China Academy of Information and Communications*, *Beijing* 100191)

Abstract　At present, IoT (Internet of things) devices have been widely used in people's daily life, and their security is closely related to individuals, enterprises and even countries. The increasing importance of IoT devices has also attracted a growing number of attacks. To address the security challenges IoT devices faced, various countries and regions have formulated numerous laws and regulations, security evaluation and certification standards related to IoT device security. We summarize and organize the existing research status in this field. We firse discuss the security threats IoT devices faced and explore the different attack surfaces for IoT devices based on a hierarchical logic division. Furthermore, we analyze and summarize the existing security laws, regulations, security evaluation, and certification status, while focusing on the research on IoT security risk detection cutting-edge technologies from five aspects: chip Trojan horse detection, Interface security risk detection, wireless protocol security, firmware risk detection and application, and service security risk detection. Finally, the possible future development direction of this field is summarized and prospected, in order to provide reference and help for the security development of our country's future IoT device products.

Key words　IoT device security; laws and regulations; security assessment; certification standards; risk detection

摘　要　目前，物联网（Internet of things, IoT）设备已广泛应用于人们的日常生活，其安全性与个人、企业甚至国家密切相关. IoT设备重要性提高的同时也招致越来越多的攻击. 为应对IoT设备所面临的安全挑战，各国各地区已制定众多和IoT设备安全相关的法律法规、安全测评及认证标准. 对该领域现有的研究状况进行了归纳与整理，首先从IoT设备面临的安全威胁出发，按照层次逻辑划分探讨针对IoT设备的不同攻击面，并在此基础上对现有的安全法律法规、安全测评及认证现状进行分析、总结，重点从芯片木马

收稿日期: 2023-06-05; **修回日期**: 2023-08-25

基金项目: 智慧城市核心算法及软件系统研发项目(E2V0211105); 2022年中国信息通信研究院开放课题(E2CK041); 2021年中国移动内容分发网络内容管理平台项目(E1V0731105)

This work was supported by the Project of Smart City Core Algorithm and Software System Research and Development (E2V0211105), the 2022 China Academy of Information and Communications Research Open Project(E2CK041), and the 2021 China Mobile Content Distribution Network Content Management Platform Project (E1V0731105).

通信作者: 张若定(zhangruoding@iie.ac.cn)

检测、接口安全风险检测、无线协议安全风险检测、固件风险检测及应用与服务安全风险检测5个方面对IoT安全风险检测前沿技术进行研究,并在最后对该领域未来可能的发展方向进行了总结和展望,以期为我国未来IoT设备产品的安全发展提供参考和帮助.

关键词 IoT设备安全;法律法规;安全测评;认证标准;风险检测

中图法分类号 TP391

物联网(Internet of things, IoT)设备的数量不断增加,且渗透人们生活的方方面面.据Statista公司估计,至2025年,通过IoT连接的系统和设备的总量将超过210亿台,相当于每人约3.47台IoT设备.作为信息空间与物理空间深度融合的典型范例,IoT设备已向愈来愈智能化的方向发展,并与AI、云计算、计算机视觉等技术全面结合.国内外的IoT设备不断涌现,例如:国外的Verizon、苹果、Samara、Nissho、Bosch、Siemens等品牌的智能家居,以及自动驾驶汽车和智能穿戴设备等,国内的华为、大华、海康威视、海尔、京东、阿里巴巴和小米等品牌的摄像头、路由器、智能家居、体脂秤、运动手环和智能音箱等是最常见的IoT设备.Xenofontos等人[1]将IoT设备按场景分为3类:消费者IoT、商业IoT、工业IoT.3类场景下的IoT设备广泛应用于人们的工作环境与生活环境中,其安全性涉及到财产安全、人身安全、个人隐私、商业机密、国家安全等方方面面,如果被恶意对手成功利用,可能产生不同程度的后果.

近年来,一些典型的IoT设备攻击事件从不同层面给国家、社会、企业和个人带来不同程度的影响.2016年10月美国互联网域名解析服务商DYN遭受攻击,攻击者通过Mirai病毒感染了大批IoT设备,构建僵尸网络对DYN的DNS服务发起分布式拒绝服务攻击(distributed denail of service, DDoS)攻击,造成大面积的网络服务瘫痪[2];2018年APT组织“奇幻熊”(APT28)利用IoT设备漏洞远程获得初始控制权,对乌克兰的氯气蒸馏站发起攻击,此次攻击并未成功,否则工厂将被迫关闭,进而影响乌克兰政府的污水处理工作[3-4];2019年,微软安全响应中心捕获到了APT28入侵IoT设备的攻击活动,利用默认口令和漏洞入侵了视频解码器、VOIP电话设备和打印机,泄露了目标用户的IP地址[5];2020年美国公司iRobot推出的Roomba扫地机器人将使用者的日常照片发布到了网络上,泄露了使用者的隐私[6];2021年6月,美国网络安全和基础设施安全局CISA发布预警,数百万联网安全和家用摄像头中用于传输大型音视频文件的Through-Tek P2P SDK[7]存在一个信息泄露漏洞(CVE-2021-32934),由于本地设备和远程ThroughTek服务器之间明文传输数据,远程攻击者可利用此漏洞窃取个人家庭和社会层面的敏感信息;2月后,同样的厂商再现重磅漏洞[8].2022年12月,哥伦比亚最大的公共能源、水源和天然气供应商之一Empresas Publicas de Medelln(EPM)的IoT系统遭受到了黑猫勒索软件的攻击[9],导致公司IT基础设施瘫痪,在线服务中断,影响了其所服务的大量用户.

只有全面分析并着手解决IoT设备所面临的各种安全问题,才能更好地发展IoT设备.从全球范围来看,已经有越来越多的国家或组织就IoT安全问题提出了相关的法规标准和认证制度,也有越来越多的学者和企业就IoT的安全风险检测技术进行研究.目前国内外已有较多针对IoT安全及防护技术的综述和报告[10-18].文献[10]从IoT环境和IoT架构2个角度分析IoT设备面临的安全问题,在分析IoT架构面临的安全挑战时,将IoT架构分为应用层、网络层和感知层3个层次,依次分析各层次可能存在的威胁,但缺少对物理层安全风险的分析;文献[11]同样从这3个层次来讨论可能的攻击方式,同时也针对各层次提出了相应的解决方案,最后指出没有一个解决方案可以提供完备的安全性,因此需要定期检查和更新IoT设备.文献[12]将IoT整体架构分为物理层、网络层、感知层和应用层4个层次,按层分析可能存在的安全问题并提出相应的解决方案.文献[13]重点从IoT硬件方面对其防护技术进行阐述,并依据防护阶段将攻击层面分为应用层、网络层和感知层.文献[14]调查并分析了针对IoT设备固件更新操作的攻击类型及其可用的安全固件更新方法,并介绍了几种常用的固件分析工具.文献[15]则从软件层面对IoT设备防护策略进行了评估.文献[16]进一步地从通信层面讨论了IoT防护策略的现状并给出了目前IoT设备在通信安全方面的政策建议.文献[17−18]则在软件层和通信层进一步做了深入研究,分别从机器学习与深度学习方面的安全检测技术论述,研究了不同数据集、训练方法和模型对于IoT设备安全防护检测的影响,并给出机器学习在该

领域更为适用的结论. 纵览已有的文献, 聚焦于 IoT 安全架构分层分析的较多, 目前专门针对 IoT 设备本身的安全检测、评估、认证技术和法规标准的工作总结分析尚未有深入的和最新的报道, 且目前的文献在 IoT 设备的分层攻击面划分和检测技术划分不够全面. 本文对各个国家和区域性组织现有的 IoT 设备安全法律法规情况、IoT 设备安全测评及认证现状进行了细致的梳理, 进一步对国内外学术界和业界在 IoT 设备各层面安全风险检测技术进行总结研究, 且做了更细致的层面划分, 以期为建立 IoT 设备安全风险综合评估提供新技术、新模式方法作为参考, 为 IoT 设备安全的科研、产业做出有益的探索.

为达到上述目的, 我们首先确定 IoT security, vulnerability detection, IoT vulnerability, IoT devices vulnerability 等关键词, 随后我们在 ACM Digital Library, IEEE Xplore Digital Library, Wiley Online Library, Springer Link Digital Library, Chinese Science Citation Database, Science Direct Digital 数据库中搜索这些关键词, 在各国政府公开网站搜索相关的 IoT 法律、法规、标准等文件. 对于检索出的文献, 本文作者通过查看其题目、摘要筛选与本综述主题相关的论文, 通过查看简介等筛选与本文相关的法律和标准文件, 共检索到相关论文 130 篇, 相关法律文件 50 份, 随后在知网、谷歌学术等学术论文搜索引擎查找文献被引及作者发表论文情况等, 进一步补充和筛选相关论文及法律文件, 截止到 2023 年 5 月, 最终我们确定最具代表性的高质量论文 116 篇, 法律与标准文件 31 份.

本文的主要工作和贡献为: 1)对不同层次的 IoT 设备的攻击面进行了总结, 并列举了其中经典的攻击风险和实例. 2)对各国家与地区 IoT 设备安全法律法规、安全测评及认证现状进行了梳理, 并对世界各国极具影响力的法律法规进行了系统整理. 3)结合具体实例详细介绍了 IoT 设备安全风险检测的前沿技术, 并从不同维度分析了 IoT 设备安全风险检测的技术方案.

1 IoT 设备安全威胁与攻击面

OWASP 联盟 IoT 攻击面区域项目(IoT attack surface areas project)[19] 基于威胁程度列举出 IoT 的十大安全隐患, 把目光聚焦于不安全的密码、网络服务、生态接口和组件设置、不适当的数据处理方式、设备加固和管理等问题上, 并对其细分领域进行了总结. 然而 OWASP 的攻击面分类以问题为导向, 未将安全风险出现的层次逻辑进行划分.

区分不同安全威胁与漏洞所面向的 IoT 设备层次组件, 辨析安全威胁在不同层次上的作用机理对 IoT 设备的安全研制与加固具有重要意义. 已有一些工作演示了如何利用攻击层[20-21] 构建 IoT 攻击分类. Felt 等人[20] 提供了针对 IoT 设备通信层的漏洞和潜在攻击的划分方法, 将攻击面分为边缘层、访问层和应用程序层. 文献 [21] 将 IoT 系统面临的威胁分类为网络物理攻击、中间件攻击和应用程序攻击; 文献 [22] 根据目标层和执行方式将攻击分为 4 种: cyber-based, network-based, communication-based, physical-based. 参考近年来学者们的攻击分类, 并结合 IoT 设备自身的软硬件架构设计, 如图 1 所示, 我们将对设备各个攻击面自底向上, 按设备物理层攻击面、通信层攻击面、固件层攻击面和应用与服务层攻击面这 4 个层面分层进行总结. 此外我们还将这 4 个层面细分为芯片木马检测分析、接口风险检测、无线协议风险检测、固件风险检测、应用与服务风险检测共 5 个方面, 并在每个方面给出具体技术应用和案例.

1)物理层攻击面. IoT 设备物理层一般由处理器(嵌入式)、内部总线、主板、接口和外部设备等 5 个组件构成. 通过选择适当的组件, IoT 设备物理层可以实现丰富多样的功能, 满足多种需求. 这一层次常见的主要威胁为芯片硬件木马、总线攻击、物理 DoS 攻击和接口攻击等.

芯片硬件木马[22] 指植入芯片电路中的木马, 用于达到攻击、篡改和控制芯片的目的. 芯片木马可以在 IC 设计、制造、运送或是大规模复制期间产生, 具有隐蔽性. 总线攻击是针对 IoT 设备中的内部总线、主板接口等内部通信器件的攻击, 如总线侧信道分析, 通过分析总线上的侧信道信息, 如功耗、电磁辐射等推断出敏感信息或操作模式[23]; 总线外接攻击, 通过在传输线上接入外接线实施监听活动, 或插入干扰信号导致数据错误、系统崩溃或执行恶意操作[24]; 总线间的冲突或竞争机制干扰存储访问, 以达到非法读写数据或访问控制的目的. 物理层的 DoS 攻击主要试图使合法用户无法使用物理资源, 例如, 迫使设备退出低功耗模式, 消耗电池的睡眠剥夺攻击[25]. 此外, 物理层的 DoS 攻击还能够通过使用电磁辐射、射频干扰、电压干扰等手段干扰 IoT 设备中的传感器器件, 使其无法正常工作, 常见如: 光照传感器在高能量激光设备的照射下可能会导致设备短暂地停止工作或永久性损伤[26]; 利用信号干扰器发射信号

Fig. 1 Typical security threats at each layer of IoT devices

图 1 IoT 设备各层次典型安全威胁

使无线通信模块无法正常通信[27].大量 IoT 设备在安装部署后, 装置整体往往处于暴露状态, 物理接口缺乏必要的保护措施, 难以阻止攻击者破坏各种设备的物理完整性. 一种典型的接口攻击方法是针对 USB 接口的攻击, 如 BadUSB[28], 攻击者会提前将恶意代码载入到 USB 设备中, 将 USB设备与目标 IoT 设备连接就可以实施攻击行为.

2)通信层攻击面. IoT 设备的通信层包括有线通信和无线通信. 布局在工业 IoT、智慧楼宇、智慧城市等场景中的 IoT 设备由于具备统一布线的基础条件, 常采用有线通讯方式, 如 IEEE1394, RS-232, RS-485, CAN, Profibus 等; 而在智能家居、无人驾驶、野外传感作业等移动性比较强的场景下, 更多还是会采用无线通信的方式来进行数据传输. 无线通信, 包括短距离通信网络, 以 Wi-Fi, Bluetooth, ZigBee 为代表; 长距离通信网络, 包括 LoRa、基带通信、LTE Cat-M1、NB-IoT 等. 相对而言, 无线通信由于通信信道具有暴露性特征, 通常情况下风险高于有线通信, 下面我们重点探讨无线通信层的攻击面. 不同的无线通信协议面临的安全威胁不同, 针对基带通信, 攻击者可采取空口监听技术破解加密语音与业务数据, 或向目标发送攻击流量实施伪基站攻击获取数据[11-13]; 对于 Wi-Fi 网络协议, WEP 的核心算法 RC4 加密算法易被攻击者破解, 已有成熟的工具[29] 可以对其进行监听, 之后的 WPA2 在 2017 年被 KRACK 攻击攻破[30], WPA3 也被 MathyVanhoef 发现了 FragAttacks 系列漏洞[31].

其他无线通信网络协议, 长期以来也不断曝露各种不同类型的漏洞风险. 如 2022 年 NCC 披露特斯拉 Model 3 和 Model Y 可以被攻击者通过对低功耗蓝牙通讯实施中继攻击解锁[32]. 针对 NFC 协议, 攻击者可以利用 NFC 支付中继攻击实时提取数据[33]. KNX-RF 协议的 PSK 预共享密钥存在泄露风险, KNX 也已被发现大量的攻击载体和安全服务缺陷[34]. Thread 协议[35] 使用网络密钥作为网络级保护, 密钥的分发采用密钥加密钥(keyencryptionkey, KEK)加密传输, 而 KEK 的泄露风险使其陷入安全瓶颈. 对于混合协议方面, 一种 Torii 僵尸网络的典型案例为国外组织“海莲花”利用代理流量的木马对国内外 IoT、OA 服务器进行监听和设备控制, 其利用的协议包括但不限于 Wi-Fi, Li-Fi, 6L0WPAN, NB-IoT 等[36].

3)固件层攻击面. IoT 设备中的固件包括位于应用程序和硬件之间的复杂系统、指令和数据. 由于固件控制硬件与固件相关的攻击一但实施成功可能会造成较大损失. 同时, 随着 IoT 设备智能程度的不断增加, 固件系统的复杂性也在不断增加, 日益复杂的代码引入了更多的攻击面.

固件中较常见的硬编码漏洞会暴露 URL、密码算法、密钥等敏感信息, 固件代码往往也存在大量漏洞. 如 CVE-2021-46008 漏洞将 Totolink a3100r 设备 Telnet 密码直接硬编码在设备的软件代码中, 未进行任何混淆和保护, 在 Verizon 5G Home LVSKIHP InDoor-

Unit(IDU)3.4.66.162和OutDoorUnit(ODU)3.33.101.0设备上，RPC访问使用的静态证书嵌入在固件中，攻击者只需下载固件，提取证书的私有组件即可获得访问权限. 其他常见的漏洞包括固件更新漏洞、命令注入漏洞、信息泄露漏洞、缓冲区溢出漏洞等，表1中列出了2021—2023年不同IoT设备的固件漏洞案例.

Table 1 Examples of Firmware Vulnerabilities for Different IoT Devices in 2021-2023

表1 2021—2023年不同IoT设备的固件漏洞案例

类型	漏洞编号	设备类型	设备型号	固件漏洞描述
硬编码凭据漏洞	CVE-2022-28371	微波通信设备	Verizon 5G Home LVSKIHP	远程RPC访问的静态证书嵌入固件在设备群中共享，攻击者提取证书私有组件能获得访问权限.
	CVE-2021-46008	无线路由器	Totolink a3100r	固件中硬编码Telnet密码.
缓冲区溢出	CVE-2022-22570	门禁读卡器	UniFi	允许已获得网络访问权限的攻击者控制所有连接的UA设备.
	CNVD-2021-18376	Snapdragon产品无线路由器	FiberHome HG6245D devices（China）	在分析GTK帧时，由于整数溢出到缓冲区溢出而导致WLAN内存损坏.
	CNVD-2021-29152	AP管理路由器无线路由器	Tenda100路由器 D-Link DIR-816 A2	存在一个栈溢出漏洞，该漏洞可能允许未经身份验证的远程攻击者在受影响的设备上执行任意代码.
固件更新	CVE-2021-3166	无线路由器	华硕DSL-N14U-81	攻击者可将任意文件内容命名为Settings_DSL-N14U-B1.trx作为固件更新上传.
	CVE-2022-3789	智能相机	摩托罗拉 Binatone Hubble	允许具有物理访问权限的攻击者获取用于解密固件更新包的密钥.
	CNVD-2020-15984	无线路由器	D-Link DSL-2640B	管理界面未对固件更新POST请求执行身份验证检查，攻击者可利用该漏洞安装其选择的固件.
信息泄露	CVE-2022-30563	摄像头	太华IPC-HX2XXX	捕获通过WS-UsernameToken模式进行身份验证的未加密ONVIF请求，诱骗设备创建管理员账户，获得最高权限可实时观看、重放摄像头视频.
	CVE-2022-33175	配电单元设备	Powertek	可通过特定API访问user.token字段，导致泄露当前登录管理员的活动会话ID.
	CVE-2023-23575	CONPROSYS物联网网关产品	M2M网关固件版本3.7.10及更早版本	远程认证攻击者可绕过访问限制，访问网络维护页面，获取该产品网络信息.
命令注入	CVE-2022-30105	无线路由器	贝尔金N300	ASP页面脚本存在远程命令注入漏洞，使用特制参数提交POST请求，可以Root权限执行OS命令.
	CVE-2023-27917	CONPROSYS物联网网关产品	M2M网关固件版本3.7.10及更早版本	产品中的操作系统命令注入漏洞允许经过身份验证的远程攻击者访问网络维护页面，以Root权限执行任意操作系统命令.
	CNVD-2023-43930	无线路由器	锐捷RG-AP850-A	存在命令注入漏洞，具有Web用户权限的攻击者可利用该漏洞以Root权限执行任意命令.

同时在开发固件时，通常会使用嵌入式开发环境和工具链，如Keil, IAR Embedded Workbench, Arduino IDE等. 此外，固件开发还需要熟悉相关的编程语言，如C, C++, Python等，以及硬件驱动程序的开发和调试技巧. 因此，固件层的攻击面往往不仅来自于固件本身，还来自于固件开发时使用的开发工具. 如CVE-2009-4979漏洞，较早的Keil版本允许攻击者执行任意SQL命令，在固件开发阶段远程注入漏洞. CVE-2019-13991漏洞则是Arduino项目的一种嵌入式系统安全漏洞. 该漏洞允许远程攻击者向LEDs发送数据，导致固件开发时被植入恶意数据. 另外，已有的驱动程序也可能会扩大固件自身的攻击面，如CVE-2023-24924漏洞是美国微软(Microsoft)用于PostScript打印机的标准驱动程序的执行漏洞，该漏洞能够利用系统与打印机固件间的通信协议上传代码并远程执行；而CVE-2010-1592漏洞是路由器设备上的驱动程序漏洞，该漏洞可以通过路由器内部固件协议合法地将存储设备中的文件进行替换，并曾被质疑为美国联合特种作战司令部(JSOC)用于攻击非洲和中东各国的路由器设备并收集他国人员信息[37].

4)应用与服务层攻击面. 在IoT时代，IoT设备终端与用户之间、终端与终端之间、终端与后台之间的交互越来越强，终端厂商也正从销售设备转变为提供服务，应用层与服务层是IoT系统中的重要组成部分，包括IoT设备应用、控制端应用以及云端服务. IoT设备应用运行在具体的IoT设备上，用于控制和管理设备的各种功能和操作. 随着IoT设备智能程度的不断提升，APP已成为智能硬件设备的捆绑标配，小程序、快应用等新的应用服务形态也不断出现[38]. IoT设备控制端运行在用户设备(如智能手机、平板电脑、电脑)上，容易被远程控制并接管IoT设备.

云端服务托管在云计算平台上，通过互联网连接IoT设备，控制端应用，提供数据存储和分析服务、设备管理服务、远程监控和控制服务、安全认证服

务等. 它们共同构建了一个完整的 IoT 生态系统, 提供了丰富的功能和服务.但 IoT 设备应用开发门槛低, 且缺乏相应的安全标准, 为了加快产品的开发, 相关应用软件常常直接编译, 使用简单不安全的代码, 这样容易引入未知的漏洞. 以 Android 为固件 OS 平台的设备为例, 应用软件整体质量低, 导致应用本身存在大量安全漏洞[39-40], 开发者可能无意间开发出具有安全隐患的应用, 投入市场后导致大量用户面临安全威胁; 另外手机应用、设备、云的交互是 IoT 的一个重要特征, 复杂的交互关系给 IoT 带来了更多安全挑战, 这 3 者交互过程中需要经历注册、绑定、使用等各个阶段, 每个阶段都需要进行信息交互和状态转换, 转换需要依照特定的模式进行, 然而实际上一些应用并没有按照规定的模式进行[41-42], 这可能导致远程劫持等漏洞的产生. 另外各个应用之间联动时存在的逻辑错误也可能被攻击者利用, 对用户造成威胁.

2 IoT 设备安全法律法规现状

2.1 聚焦数据安全的通用法律法规

全球范围来看, 目前 IoT 设备安全相关的通用法律法规多聚焦于数据安全. 在各类数据法律法规中, 欧盟《一般数据保护条例》[43](general data protection regulation, GDPR)的影响较为深远. GDPR 的前身是 1995 年欧盟为应对数字技术巨变后的新时代安全挑战制定的《计算机数据保护法》(computer data protection act)[44], 2018 年 5 月演变为强制实施的 GDPR, 以及英国的对标法案《UK's data protection act 2018》[45].

GDPR 在第 3 章第 1 部分第 12 条规定, 厂商在收集用户的个人信息之前, 须以“简洁、透明、易懂和容易获取的形式, 以清晰和平白的语言”向用户说明收集信息的行为、范围、存储方式等. IoT 设备的传感器通常会频繁收集与用户有关的信息, 如可穿戴设备所收集并传输的用户坐标位置、智能家居设备所收集并传输的用户家庭能量消耗数据、设备使用频率等. 因此 IoT 设备厂商或集成方案厂商应充分考量 GDPR 的要求, 在网络中获得个人数据之前需要获得用户的同意并说明相关情况. 此外, IoT 设备采集数据的存储与处理常常采用基于云的解决方案, 其存储数据和处理数据的位置也需符合所有 GDPR 要求.

在美国, 自 2020 年 1 月 1 日起, 美国加利福尼亚州开始实施数据保护相关的新法案:《加州消费者隐私法案》(California Consumer Privacy Act, CCPA)[46]. 该法案从隐私保护和数据安全 2 个角度出发保护加州的消费者, 也给在加州生产或者销售智能产品的企业提出了新的要求.

全球各国也先后发布了多部与数据隐私保护相关的法律文件, 如加拿大的《个人信息保护和电子文档法》(personal information protection and electronic documents act, PIPEDA)[47]、南非的《个人信息保护法》(Protection of Personal Information Act, POPI Act)[48] 和日本的《个人信息保护法》(Amended Act on the Protection of Personal Information, APPI)[49] 等. 在我国, 2021 年 9 月《中华人民共和国数据安全法》[50] 开始实施(同年 6 月颁布), 2021 年 11 月《中华人民共和国个人信息保护法》[51] 开始实施(同年 8 月颁布), 标志着在复杂的互联网时代, 我国数据信息安全领域的法律体系得到进一步完善. 以上法案均明确了隐私数据保护的责任、权利与处罚规定, 为各国境内提供数据服务的 IoT 设备厂商提供应遵循的法案.

2.2 多方利益保护驱动的 IoT 安全法律法规

层出不穷的 IoT 设备攻击事件和漏洞风险给国家和政府机构、制造商、消费者等各方都带来不同程度的损失和影响, 为保护一方或多方利益, 各国和国际组织也在积极推进 IoT 设备安全技术相关的针对性法规的制定.

2016 年 11 月 15 日, 美国国土安全部发布的《保障物联网安全战略原则(V1.0)》[52] 指出, 未在最初设计阶段构建安全并采取基本安全措施“可能会造成制造商的经济成本、声誉成本或产品召回成本损失”. 因此, 该原则为 IoT 利益相关者(联邦机构、制造商、网络连接提供商和其它行业利益相关者)提供了一套非约束性原则和最佳安全实践建议. 英国于 2018 年发布的《消费者物联网安全业务守则》[48] 为消费者物联网制造商提供了 13 条准则, 旨在确保设备的安全性. 该行为准则为 IoT 制造商和其他行业利益相关者制定了实用步骤, 以改进消费类 IoT 产品及其相关服务的安全性. 实施这 13 条准则有助于保护消费者的隐私和安全, 同时使消费者更能安全地使用他们的产品. 2020 年澳大利亚政府发布《实践准则: 为消费者保护物联网》[49], 该准则主要包括: 没有重复的弱口令或默认口令, 实施漏洞披露策略, 软件持续安全更新, 凭证的安全存储等方面要求. 2020 年 11 月 9 日, 欧盟网络安全局发布了《物联网安全准则》[50], 旨在帮助物联网制造商、开发商、集成商及所有物

联网供应链的利益相关者在构建、部署或评估物联网技术时做出最佳决策.

2020 年 12 月 4 日，美国《物联网网络安全改进法案》[53] 签署，首部全美层面的物联网安全法律诞生，该法案的主要目的是考虑联邦政府的安全利益诉求，确保联邦政府设备的安全性，并通过政府采购间接提升消费者设备市场的安全能力. 同年，新加坡网络安全局（Cyber Security Agency of Singapore, CSA）[52] 提出消费类物联网设备网络安全标签计划，根据星号的数量将智能设备分为 4 个等级进行评级，希望该计划能够激励制造商开发更安全的产品，以使其与竞争对手区分开来，提升竞争力. 2022 年，新加坡进一步将该标签计划扩大到对医疗设备进行防护，以防范网络安全风险的增加危及患者的个人信息、临床数据或治疗方案，最终影响患者的人身健康.

3 IoT 设备安全测评及其认证现状

从全球范围来看，各国和国际组织或者通过制定专门针对 IoT 设备的标准，或者沿用通用的安全标准来引导 IoT 设备的安全设计和生产，并将这些作为 IoT 设备安全测试和认证的依据，开展了针对 IoT 产品的上市安全测评与安全认证活动. 图 2 展示了近 20 年各国在 IoT 法规及标准制定实施方面的历程.

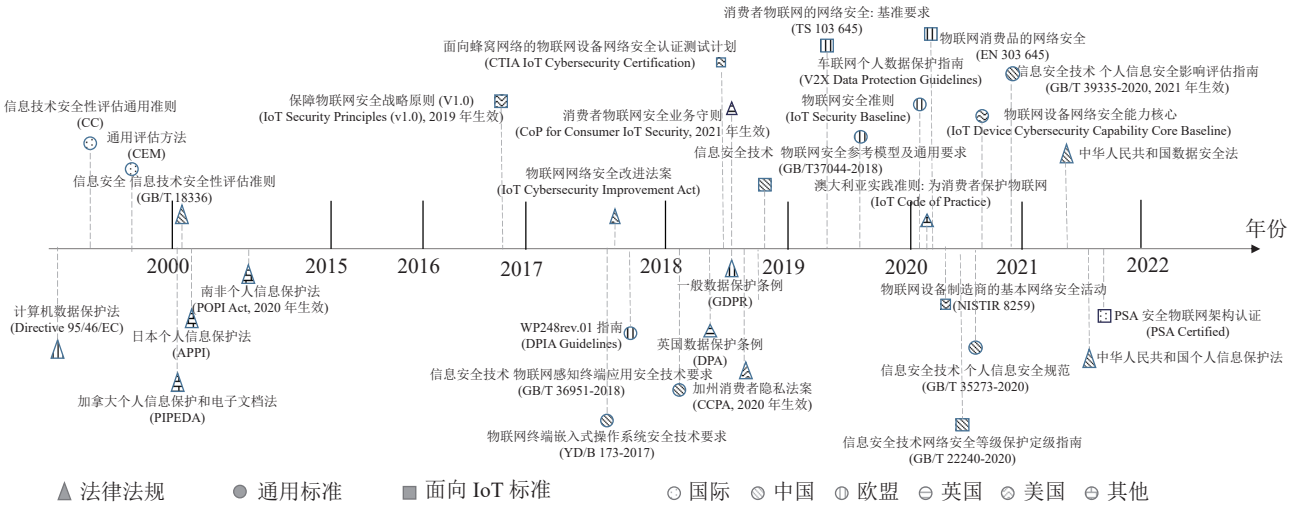


Fig. 2 Progress on the development and implementation of IoT regulations and standards in various countries

图 2 各国 IoT 法规及标准制定实施历程

3.1 通用安全标准、测评与认证

基于通用安全标准的测评与认证方面，国外机构多数遵循基于《信息技术安全性评估通用准则》（The Common Criteria for Information Technology Security Evaluation, CC）[54] 和《通用评估方法》（Common Evaluation Methodology, CEM）[55] 的安全保障等级评估. 我国参考 CC 标准制定了 GB/T 18336《信息安全信息技术安全评估准则》系列国标，以此作为国内的 CC 评估依据，但国内的 CC 评估结果目前尚无法与国际进行互认. 许多 IoT 设备产品陆续通过了基于 CC/CEM/GB18336 标准的安全等级评估认证，如：2016 年，三星为其智能电视实现了 CC EAL 1 级认证；2017 年 4 月，LG 为其智能电视产品实现了 CC EAL 2 级认证；2021 年华为智慧屏通过了中国网络安全审查技术与认证中心[56] 开展的企业智慧屏产品 EAL 2+认证. 同时，在 IoT 设备的数据安全风险评估方面，常采用通用的 DPIA（data protection impact assessment）[57] 作为数据保护影响评估方案. DPIA 是各机构基于 GDPR 原则下的一项风险评估工具，通过对数据处理活动的评估帮助数据控制者提前识别和减轻隐私风险，符合 GDPR 一直倡导的自证合规原则[57]. IoT 设备厂商可借助 DPIA 评估其数据处理全流程的风险性. 很多地区/国家的数据保护监管机构已发布其制作相应的 DPIA 评估标准或指南来帮助厂商完成评估. 2017 年 10 月 4 日，欧盟数据保护委员会（European Data Protection Board, EDPB）[58] 出台的针对 DPIA 的 WP248rev.01[59] 的指南是较早期的指南，2020 年 2 月，EDPB 又发布了《车联网个人数据保护指南（征求意见稿）》[60]，该指南聚焦于车联网和出行相关应用背景下个人数据的保护与处理，揭露风险的同时也为行业从业者提出建议. 我国国家标准 GB/T 39335-2020《信息安全技术个人信息安全影响

评估指南》[61]是根据我国GB/T 35 273-2020《个人信息安全规范》[62]和GDPR要求提出的隐私影响评估和数据保护影响评估方法指南.

3.2 面向IoT设备的安全标准、测评与认证

除国内外通用安全标准的检测评估之外,IoT设备在不同的监管背景、上市需求和应用场景下,可申请不同类别的IoT领域安全标准测评与认证.

欧洲电信标准协会(European Telecommunications Standards Institute, ETSI)[63]于2019年发布了技术规范TS 103 645《消费者物联网的网络安全:基准要求》[64],并于2020年转为标准EN 303645.该标准是专为防止针对智能设备发起的大规模普遍攻击而建立的IoT产品专项安全基准,涉及的产品包括儿童玩具、婴儿监视器、烟雾探测器、智能门锁、智能相机、电视、扬声器和可穿戴式健康追踪器等,该标准从网络安全规定和数据隐私保护条款2方面要求以上产品.产品在满足了EN 303645标准要求的同时也满足了GDPR的相关要求.芬兰网络安全标签计划、新加坡网络安全标签计划,以及英国消费电子IoT产品安全法都采用或参考该标准.美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)[65]针对IoT网络安全制定了一系列的标准、指南和相关文档,其中NISTIR 8 259《物联网设备制造商的基本网络安全活动》标准[66]为物联网设备制造商提供了详细的网络安全路线图.美国无线通信和互联网协会(Cellular Telecommunications and Internet Association, CTIA)[67]于2018年发布了《面向蜂窝网络的物联网设备网络安全认证测试计划》,用于认证在美国使用蜂窝网络或Wi-Fi网络进行数据通信的IoT设备是否具备相应的安全能力.

2021年,Arm与BrightSight、中国信息通信研究院、Risure和UL[68]等独立安全测试实验室,以及咨询机构Prove&Run联合推出的PSA安全物联网认证项目[69](PSA IoT security certification program),旨在支持基于平台安全架构(PSA)框架的安全物联网解决方案的大规模部署.

在我国,全国信息安全标准化技术委员会于2018年发布了国标GB/T 36951-2018《信息安全技术物联网感知终端应用安全技术要求》[70],规定了物联网信息系统中感知终端应用的物理安全、接入安全、通信安全、数据安全等安全技术要求,该标准可作为相应终端网络安全测试依据.随后颁布的GB/T37044-2018《信息安全技术 物联网安全参考模型及通用要求》[71]制定了关于物联网安全参考模型和通用要求的标准,其中描述了安全区的组成和不同功能区的信息安全防护需求.通信标准化协会于2017年发布了行标YD/B 173-2017《物联网终端嵌入式操作系统安全技术要求》[72],对物联网终端操作系统提出了相应的安全要求,包括访问控制、数据安全、通信服务和外设管理、安全审计、入侵检测、防火墙等.GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》[37]中也专门提出了物联网扩展安全要求,其中二级物联网扩展要求提出了安全物理环境、安全区域边界和安全运维管理3个方面的基本要求,三级物联网扩展要求相较二级除了丰富了安全物理环境和安全运维管理2个维度的要求外,还就安全计算环境这一维度新增了数个基本要求.

4 IoT设备安全检测前沿技术研究

基于国内外各类标准的IoT设备安全测试和认证的测评方法常常包括访谈、文档审查、配置检查、工具测试、实地查看等步骤,测评单位在追求测评项覆盖面广的同时,提高其测评技术先进性和测评深度也是需要不断努力的方向.本节我们总结分析当前学术界和业界在IoT设备物理层、通信层、固件层和应用与服务层的典型风险检测目标和检测技术研究现状,为建立IoT设备安全风险综合评估能力提供新技术、新模式方法参考.其中物理层主要聚焦于芯片木马和接口安全风险检测,通信层主要探讨无线通信安全.本文归纳的IoT设备安全检测类别及对应的检测技术研究热点如表2所示.

4.1 物理层芯片木马检测分析技术

IoT设备处理器芯片不同阶段的工艺常常要经过多方制造商来完成,这些制造商的安全性未知,芯片电路在这些环节中存在被植入芯片硬件木马的风险,这给处理器集成电路(IC)芯片的安全性带来挑战.

目前针对芯片硬件木马的风险检测技术可主要分为破坏性和非破坏性.破坏性方法通过芯片剖层(暴露芯片进行芯片逆向)实现,但该方法代价高、耗时久、成功率较低,并对IC造成破坏;非破坏性方法主要分为2个类型:逻辑测试和侧信道分析.逻辑测试是通过功能测试检测木马电路;侧信道分析则通过检查侧信道参数如电源、延时、瞬态/静态电流和最大频率的改变以判定木马的存在.

逻辑测试方法通过给被评估的芯片电路输入不同的刺激,将实际响应与预期响应进行比较,如果电路中的木马在测试时影响到了IC的实际响应就会被

Table 2 Frontier Research Hotspots of IoT Device Security Risk Detection Technology

表 2 IoT 设备安全风险检测技术前沿研究热点

检测类别	涉及文献篇数	检测技术	
芯片木马检测分析技术	11	逻辑测试	
		测信道分析	
接口风险检测	5	放串口检测	
		JTAG 编程接口检测	
		总线/接口交互平台研制	
无线协议风险检测	14	被动检测	信号监听
			信号分析
		主动检测	模糊测试
			中间人攻击
固件风险检测	26	静态分析	逆向分析
			传统程序静态分析
		动态分析	仿真运行
			模糊测试
应用与服务风险检测	30	静态分析	基于规则的分析
			可达路径分析
			静态符号执行
			静态污点分析
		动态分析	模糊测试
			动态符号执行
			动态污点分析
		其他分析	基于 AI 的分析
			信息流分析
			流量分析
			入侵检测

检测出来. 因此, 逻辑测试的首要目标就是在最大化木马激活概率的条件下优化测试向量生成方法.

自动测试向量生成(automatic test pattern generation, ATPG)[73] 技术应运而生, 它通过分析芯片的结构生成测试向量, 输入测试向量, 收集设备的响应结果并与预算的测试向量进行对比[74], 从而筛选出不合格的芯片. 但随着集成电路的规模越来越大, 设计越来越复杂, 硬件木马的体量微小, 可以长期隐藏在大规模复杂电路中且不易被发现, Alkabani[75] 设计了一种对偶电路, 可以辅助发现在常规电路中不易发现的小体积木马. 为了降低开销和提高木马检测概率, Chakraborty 等人[76] 提出基于签名的检测方法, 允许用户输入自定义密钥获取对应签名, 若电路中的模块和节点被芯片硬件木马改变将会导致输出签名与预期签名不符. 芯片硬件木马通常仅在特定情况下被触发, 其余时间处于潜伏状态, 因此提升硬件木马激活率能有效提高逻辑测试能力. 文献 [73−76] 方法都需要在木马处于激活状态下实现, 可是由于攻击者精心设计的触发条件能逃避常规的硬件检测, 所以硬件木马难以被触发, 硬件木马的检测也十分困难, 因此 Sakmani 等人[77]设计了一种可插入的虚拟扫描触发程序, 该程序能够增加木马的活动, 缩短激活时间, 提高检测效率.

侧信道分析主要关注的信号信息如图 3 所示. 在侧信道分析中, 侧信道信号, 如电磁辐射、功耗信息、路径时间延迟等, 会在黄金 IC(golden IC)和木马感染的 IC(infected IC)电路中表现出差异, 这一现象可用于检测 IC 中是否存在木马. Shende[78] 提出基于侧信道的功率分析技术, 比较黄金 IC 模型和木马感染 IC 模型的平均功率从而区分这 2 种模型. Gunti 等人[79] 提出了基于有效静态功率的侧信道分析技术, 利用功率门控将电路划分为多个分区以检测芯片硬件木马. 相比依赖动态功率的检测技术, 基于静态功率的检测技术可以更加灵活地检测潜伏在电路中的木马[51]. Jin 等人[80] 通过 IC 的路径延迟参数(发送方和接收方之间的信号延迟)检测木马. 针对种类繁多的芯片硬件木马, 文献 [81−82] 通过分析功率概况和网络流量数据, 实现对多种类型硬件木马的并行检测防御. 被广泛应用于 IoT 设备的 FPGA 也同样面临着来自硬件木马的威胁. Chen 等人[83] 提出可以通过收集 FPGA 时钟树发出的电磁辐射数据来检测硬件木马. 文献 [84] 提出基于强化学习的芯片硬件木马检测技术.

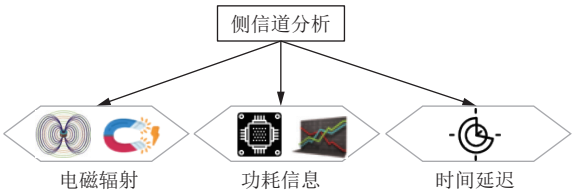


Fig. 3 Side channel analysis method

图 3 侧信道分析方法

综上所述, 逻辑测试方法是通过施加随机测试向量激活木马, 通过比较响应结果和正确结果来判断 IC 中是否含有硬件木马, 因此该方法无法检测不修改原始电路数据和功能的木马. 而侧信道分析方法是当下的研究热门, 其充分利用了硬件木马在非活动状态下也会影响侧信道信号, 即无需激活硬件木马也可以检测到硬件木马, 该方法弥补了逻辑测试方法的不足, 但无法准确判断植入木马的类型[85].

4.2 物理层接口安全风险检测技术

IoT 设备的接口安全风险检测是众多安全测评标准和流程中的重要环节. 常规的检测首先检查是否有开放的串口、JTAG 编程接口、调试接口等, 并评估开放接口风险. 如开放串口是否可以 Telnet 或

者 SSH 到系统中, 然后用 TFTP 将固件导出, 开放的 JTAG 编程接口也可能导致设备破解风险, 如 Xbox360 破解采用 LPC2148 单片机通过 JTAG 接口进行破解, 微软公司在其后的版本已经做了修复[40]. 最终微软公司提出了安全的 JTAG 策略结构, 该结构由多个层级组成, 每个层级都有对应的安全措施和防护措施, 确保 JTAG 接口安全, 在芯片生命周期的不同阶段, 安全 JTAG 策略可达到的安全能力如图 4 所示.

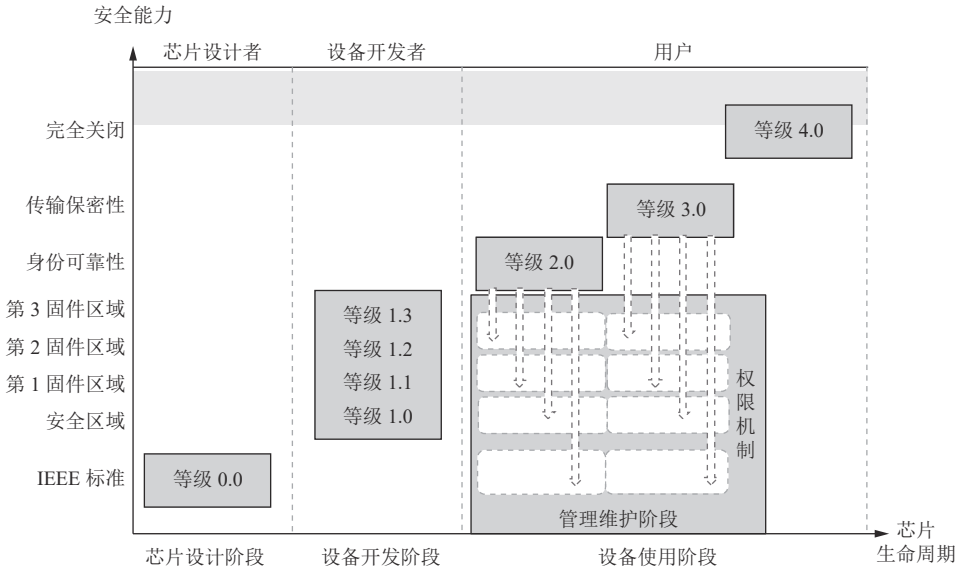


Fig. 4 Security JTAG policy structure

图 4 安全 JTAG 策略结构

IoT 设备调试接口风险的自动化安全检测技术, 通常首先需要对硬件通信接口识别, 其次要连接并驱动这些硬件调试接口, 检查接口数据的交换、传递和控制管理过程, 采用静态分析、动态调试、模糊测试等方法进一步对接口驱动或固件开展漏洞检测; 总线安全检测则尝试采用硬件通信技术嗅探、获取或修改数据, 检测是否存在可利用的漏洞. 因此, IoT 设备在出厂或部署后的接口与总线安全风险检测需要有专业的硬件测试工具平台辅助才能得以开展. 这项工作颇具挑战性, 不过, 当前已经出现了针对硬件安全性评估的测试工具平台. 例如, Hardsploit[86] 就可以被用来开展硬件安全评估工作. Hardsploit 拥有可定制的模块化工具, 能够实现多种数据总线的交互, 数据总线的类型包括 UART, Parallel, SPI, CAN, 以及 Modbus 等. 另外 Xipiter 研发的 Shikra 设备[87], 也可以协助用户连接嵌入式设备, 对设备进行调试、位攻击以及模糊处理等操作. Shikra 采用的 FTDI 的 FT232 芯片支持 Shikra 通过接口(USB)同各种底层数据接口进行交互. 相较于在硬件攻击中使用较为广泛的 Bus Pirate[88], Shikra 可以更快地从设备中提取固件映像, 在使用过程中更加稳定可靠[87].

4.3 通信层无线协议安全风险检测技术

对 IoT 设备无线协议软硬件模块的安全风险检测, 常见的研究方案包括被动检测和主动检测.

被动检测需搭建实际网络环境或仿真实验环境, 随后对真机采集的数据或仿真数据集进行安全风险分析. 被动测试流程如图 5 所示, 该过程通常包括信号监听、信号分析和获得测试结果过程, 其中信号监听过程接收局域网内的信号报文, 随后将接收到的信号传输到信号分析设备实施不同目的的安全分析, 最后根据分析侧重点的不同可获得测试结果. 不同的研究者分析的目标往往各不相同, 常见的安全分析目标包括加密算法密钥信息、用户位置、使用信息、行为习惯等. 如: 对于蓝牙协议方面, 文献 [89] 搭建被动检测平台用于分析蓝牙是否存在, 允许窃听、数据包注入和设备欺骗的弱点, 文献 [90] 分析证明了恶意的同址应用程序可以破坏 BLE 设备的访问控制. 针对 ZigBee 协议, 汤永利在文献 [91] 中搭建了一套信号捕捉仪以捕捉无线信道上的 ZigBee 数据包, 针对 ZigBee Document 053474r17(2008 版本)[46] 采取频数检测算法和块内频数检测算法, 对从 ZigBee 数据包中解析出来的数据进行随机性检测, 分析判断传输的数据和加密算法的可靠性等; 针对 Wi-Fi 协议的风险检测方案中, Liu 等人[29] 搭建了真实的硬件环境, 使用 Airsnort 软件监视无线网络中的传输数据, 利用算法尝试分析计算密钥.

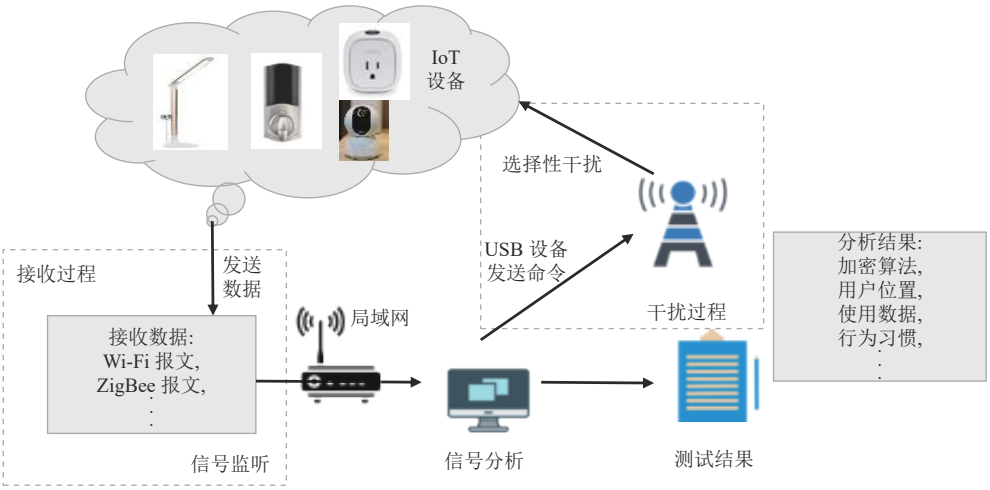


Fig. 5 Passive testing flow

图 5 被动检测流程

然而被动检测只能被动地接收既有信息，并不能检测出潜在或尚未产生的无线协议信息风险，因此 Takanen 等[92]进一步研究了主动检测的方法. 主动检测以测试例为核心，目前比较流行的主动检测方法是模糊测试(Fuzzing)，测试过程如图 6 所示. 模糊测试技术利用计算机生成测试样例，输入目标程序并监视其执行状态，以捕获程序异常行为并发现漏洞. 利用该方法进行测试的研究众多，梁姝瑞[93]研究了被测对象状态转移对模糊测试测试效率的影响，以使用 ZigBee协议的设备为研究对象，提出了基于有限状态机的模糊测试测试序列生成算法，但该生成算法存在部分条件限制，并且未进一步给出规范化的标准流程. Takanen[92]使用基于生成和变异策略结合的模糊测试技术对 NFC 协议层和应用层测试，发现大量 Android NFC堆栈以及 Android 浏览器漏洞等问题，Wiedermann 等人[94]提出基于模糊测试技术的漏洞挖掘架构，并开发测试工具针对 Android NFC API 和 NFC APP 进行测试.

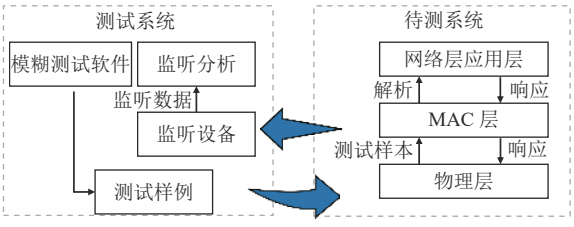


Fig. 6 Active testing flow

图 6 主动检测流程

除模糊测试外，学者们也尝试采用中间人攻击测试方式研究针对无线协议某些特定行为的主动测试方法. Stute[95]发现蓝牙配对过程中无法验证 2 个设备是否执行相同的配对方法，因此，可能会导致中间人(MITM)攻击. 同样是蓝牙协议，Zhang 等人[90]对使用蓝牙低功耗(BLE)4.2 和 5.x 协议的 Android 设备进行了测试，发现如果发起者的 BLE 编程框架没有正确处理启动及管理等步骤，设备的 BLE 配对协议会在用户不知情的情况下运行在一个不安全的模式中，从而导致中间人攻击. 除蓝牙设备外，Akter 等人[96]通过对 NFC 设备进行测试，发现基于 EMV(Europay, MasterCard, and Visa)[97]的非接触式支付协议中卡认证和交易授权阶段分离，攻击者可以利用该漏洞执行恶意的 MITM 攻击来破坏非接触式支付的完整性.

4.4 固件层风险检测分析技术

由于 IoT 设备固件程序往往是商业程序，很少公开源代码或文档，通常只能通过对固件进行逆向，再结合一些传统的程序静态分析技术进行分析，或采用模拟器动态加载固件检测的方式进行检测[98].

早期的固件静态分析常采用从固件二进制文件中手动逆向提取代码进行人工分析的手段，采用的固件二级制分析辅助工具常用的有 Srings[99]，Hexdump[100]，Binwalk[101]等. Costin 等人[102]提出大规模自动化静态分析固件思路，使用模糊哈希的方式匹配固件中存在的弱密钥，通过关联分析从 4 种维度查找不同固件镜像之间的关联性. 自动化固件静态分析过程如图 7 所示，主要包括固件数据库、固件分析和报告数据库收集以及数据包静态分析这 3 个部分. Thomas 等人[103]设计了一种半自动化的静态分析工具 HumIDIFy 来检测 COTS 设备固件的二进制文件内的后门[104]等隐藏功能，该工具使用了一个半监督学习的分类器识别出固件中的二进制文件以及其具有的功能. Shoshitaishvili[105]提出 Firmalice 二进

制分析框架，该框架使用静态程序分析生成固件的程序依赖图，获取一个从入口点到特权程序点的认证切片，再通过符号执行判断路径的约束中是否具有确定性的约束，如果存在，就可以认定为后门.

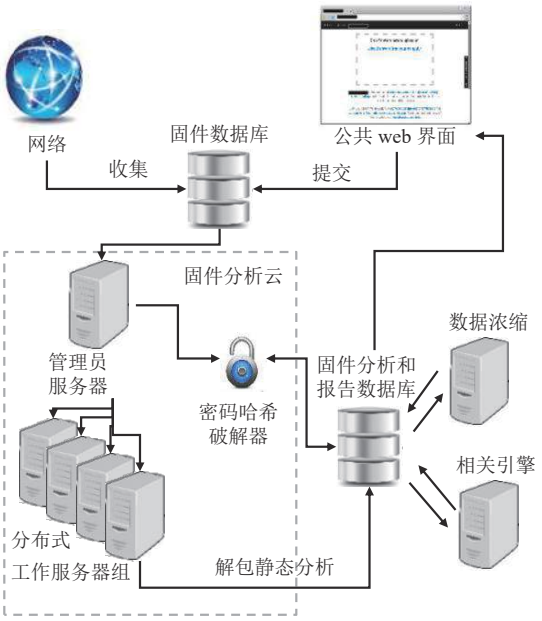


Fig. 7 Firmware static analysis

图 7 固件静态分析

然而静态分析方面同样存在无法真实模拟现实程序随机性和无法获取模拟现实固件的运行状况等缺点. 固件动态分析可部分弥补这些缺陷. 动态分析捕获程序运行时的真实状态来检测可能存在的安全漏洞，且动态分析环境相比静态分析环境更为复杂，目前大多数研究通过将固件整体加载到仿真软件，比如 QEMU 中，并对其进行模糊测试来实现[106-107]，这种实现方法需要消耗大量内存，性能开销大. 文献[106]则基于 QEMU 设计了增强进程仿真的方法，该方法将模糊处理程序设置为在用户模式下而不是系统模式下执行，有效减少了仿真过程的内存开销，如图 8 所示.

固件部分动态仿真技术[108]通过分析固件源代码，抽取出与检测目标有关的部分，只对该部分的代码执行路径进行仿真分析，进一步减少实验仿真的复杂度和开销. 文献[109]针对内存损坏漏洞提出了一些启发式方法比如段跟踪，即通过观察所有内存读写来检测分段错误从而检测非法的内存访问. 为进一步挖掘内存中有关固件的信息，文献[110]提出一种检测内存破坏漏洞的动态固件检测方法，即使用符号执行方法动态运行代码片段，并执行模糊测试，为了提高检测效率，改进了程序控制流图的恢复方

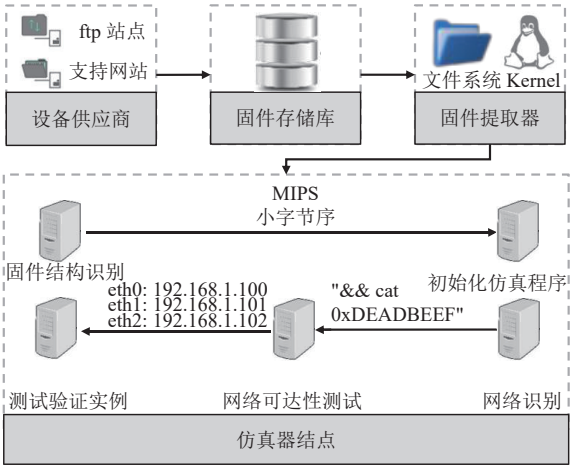


Fig. 8 Firmware dynamic detection process

图 8 固件动态检测流程

法和后向切片方法，在 40 秒内完成模糊测试并且发现了 35 个内存损坏的零日漏洞.

近 2 年，针对硬件与固件之间的耦合性和嵌入式系统的多样性问题，越来越多的学者[111]研究了固件全仿真，即不需要原始硬件环境的固件程序全系统仿真方法. 文献[112]提出硬件抽象层库模拟技术，该技术可以使固件在不需要硬件环境支持的条件下使用 QEMU 模拟器并进行交互式模糊测试. 其他固件相关检测包括基于手机 APP 的固件漏洞检测方法，即利用手机 APP 与设备之间的关联关系检测固件程序漏洞，例如文献[113]，以 APP 为入口向设备发送变异数据，通过观察设备崩溃信息来检测固件漏洞. 另外也可以通过流量分析[114]、物理特征分析[115]等来检测固件安全漏洞.

4.5 应用与服务安全层风险检测技术

4.5.1 传统应用安全漏洞检测

传统的应用安全漏洞检测方法主要包括静态分析技术和动态分析技术.

基于静态分析技术的应用安全漏洞检测方法主要对程序源代码或字节码的语法、语义进行分析，生成调用流、数据流、控制流等抽象语法语义结构，在不运行程序的前提下挖掘目标检测程序中的潜在安全漏洞. 基于静态分析技术的应用安全漏洞检测方法主要包括基于规则的分析技术[116]、可达路径分析技术[117]、静态符号执行技术[118]、静态污点分析技术[119]等.

静态分析技术具备检测速度快的优点，但对于深度安全加固的应用难以逆向获取其代码进行分析. 基于动态分析技术的应用安全漏洞检测方法不同于静态分析技术，其主要对应用程序在运行过程中产生的运行状态、执行路径、寄存器状态进行分析，发现动态调试环境中存在的安全漏洞. 基于动态分析

技术的应用安全漏洞检测方法可以对安全加固型应用进行运行态检测，克服静态检测能力的不足，其主要包括模糊测试技术[108]、动态符号执行技术[120]、动态污点分析技术[23, 121]等. 但动态检测技术也存在检测路径爆炸、检测时长过长、安全风险触发条件覆盖不全面等局限性.

随着人工智能的兴起，应用漏洞分析人员也逐渐结合机器学习和深度学习技术，对应用程序中的漏洞进行挖掘. 这些技术手段使得在应用程序数据集中收集特征的分析更加自动化、智能化. 目前基于人工智能的应用安全漏洞分析方法主要根据对应用代码和行为特征建模的不同，分为基于序列表征的漏洞检测方法[122]、基于抽象语法树的漏洞检测方法[123]、基于图表征的漏洞检测方法[124]和基于文本表征的检测方法[125]等.

4.5.2 云服务应用安全风险检测

现代 IoT 设备制造商正在利用托管的平台即服务（PaaS）和基础设施即服务（IaaS）IoT 云，例如 AWS IoT, Azure IoT 进行安全方便的 IoT 开发和部署. 目前大部分 IoT 应用需要与云平台进行交互，如图 9 所示. 因此，除了应用程序本身可能存在安全漏洞之外，在与云平台进行交互的过程中也存在安全风险.

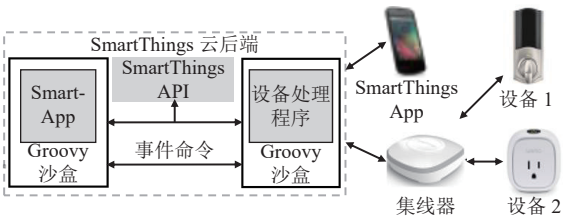


Fig. 9 Intelligent cloud platform workflow

图 9 智能云平台工作流程

根据云平台提供服务类型的不同可以将平台划分为设备接入平台、服务联动平台和语音助手平台 3 类：设备接入平台可提供接入和管理服务如 SmartThing 平台[126]；服务联动平台提供功能的连接功能，根据规则自动执行动作，如 IFTTT 平台[127]；语音助手平台通过智能音箱接受语音命令并通过语音平台控制设备联动等，如 Amazon Alexa[128]. 应用在接入这些平台时，平台会对应用进行安全检查，但是部分平台在权限管理设计方面存在漏洞[129-130]，最终导致大规模用户隐私信息泄露. 针对平台问题，一些学者[131]设计了独立于平台的应用隐私泄露检测方法，比如 Celik 等人[132]设计了一款面向 SmartThings 平台的静态污点分析工具 SainT，该工具会识别敏感数据源和接收器，然后通过静态分析追踪敏感数据流从而判断是否存在敏感信息通过网络转发的情况. 文献 [133] 则从频率的角度考虑，设计了一个信息流模型来分析 IFTTT 方法完整性或机密性违反的频率，通过为应用事件打标签的方式来检测行为是否违反机密性规定和完整性规定. 对于语音平台，由于缺少源代码，所以主要采用黑盒测试方法进行测试[25]，例如文献 [134] 通过测试发现语音助手无法准确识别某些技能的相似调用语音指令，因此攻击者可以发布恶意应用来劫持这些调用指令从而执行恶意技能.

4.5.3 IoT 应用环境入侵检测

面向应用与服务层运行时的 IoT 环境入侵检测也是一个重要的安全研究领域，然而本节探讨的前沿检测技术，主要面向需对 IoT 设备进行安全测试和/或认证的测评单位和研究者，为建立 IoT 设备安全风险综合评估提供新技术、新模式方法参考. 各测评单位往往是在设备入市之前进行认证性检测，因此其检测周期较短. 入侵检测技术常常需要长时间地在线监测或获取大量运行数据进行离线分析，不适于普通测评需求场景，但在一些特殊的测评需求驱动下，如高风险产品的入侵行为验证和高敏感领域的高安全等级测评需求下，也可适时部署实施. 下面我们总结面向 IoT 设备入侵检测前沿技术，以作参考.

1980 年，Andeson[135]率先提出了入侵检测的概念和通过分析计算机审计日志判断主机文件安全程度的方法，奠定了基于主机的入侵检测的基础. 随后，Denning[136]提出了入侵检测专家系统（IDES），通过监控系统审计日志来检测系统是否存在安全违规，给之后的入侵检测提供了通用框架，在通用框架的指导下，入侵检测技术不断发展. 近年来，机器学习和数据挖掘也被广泛地用于 IoT 设备的入侵检测技术中. 例如，文献 [137] 给出了基于机器学习方法检测 IoT 设备和服务行为的异常检测方法从而判断运行时的入侵行为；文献 [138] 中利用 IoT 应用运行中产生的海量流量信息，设计了一种随机森林算法来识别 IoT 入侵检测；文献 [139] 采用了 *K*-means 聚类算法基于规则库特征检测家居设备中应用程序及服务的异常；文献 [38] 给出了大量的基于机器学习、深度学习方面的入侵检测技术，并设计了包括深度残差神经网络、深度卷积网络和深度图神经网络等识别模型，并比较了现阶段 IoT 入侵检测模型的优劣.

5 总结与展望

本文通过对已有研究工作进行梳理，从已有的 IoT

设备安全法律法规、安全测评技术及认证现状、IoT安全风险检测前沿技术等方面详细介绍IoT设备安全检测技术研究成果. 最后本文对该领域的发展趋势做出预测和展望. 在IoT设备安全检测与评估未来的工作方面, 我们提出5点思考:

5.1 加强我国IoT安全专项法律法规建设

世界各国为维护国家安全、保障企业和公民权益, 纷纷为“IoT安全”立法. 然而, 我国IoT安全保护立法仍存在不足, 针对IoT安全的法律法规或政策性文件尚为空白, 关于IoT安全的规定隐含分布在多部法律法规之中, 较为分散, 缺乏体系, 应借鉴国外近年的经验, 加强IoT安全专项法律法规建设, 加大对IoT涉及国家安全、社会安全、用户安全的保护力度, 建立完善的保护机制, 规范IoT市场竞争, 监督多方共同创造一个安全高效的IoT设备发展环境, 推动业界安全水平提升.

5.2 推动IoT设备安全国际互认体系构建

当前, 多个国家或组织针对IoT设备的安全标准、测评与认证已陆续建立相应准则和要求, 这些准则和要求之间相似但不同. 目前, 由于各国认证制度差异, 许多国家之间并不认同其他国家的安全准则, 这就导致出口的IoT设备往往需要多次进行安全测评和认证, 耗费巨大的人力、物力成本, 造成了资源的浪费. 为打破技术贸易壁垒, 促进市场国际共治, 在推进各国认证制度规范化基础上应逐步建立起国际互认体系, 推动各国安全测评认证结果互认, 为大量IoT设备出口提供“一次检测, 一次认证, 全球通行”的便利化服务.

5.3 建立体系化IoT设备分层安全检测技术能力

第4节中我们总结分析了当前学术界和业界在IoT设备物理芯片层、接口层、无线通信层、固件层和应用层安全风险检测技术方面的研究技术现状, 目前各层安全检测技术种类繁杂, 各有优劣, 如何结合IoT实际应用场景, 优选最为合适的技术簇, 构建具有先进性的IoT设备分层安全风险深度综合测评技术平台, 实现标准化测量验证方法, 提供体系化分析和安全测试服务, 需要各测评单位进行深度思考和布局, 以最大限度发现IoT终端设备中存在的安全隐患, 指导问题修复.

5.4 探索面向IoT智能环境的安全评估框架

随着智能模型的飞速发展, IoT设备融合了越来越多的本地或远程智能模型, 例如人脸识别、物体识别和智能对话等, 从而形成了IoT智能环境. 对于IoT智能环境, 建立有效的安全标准和评估框架需求成为趋势, 而本文研究中讨论的许多现有安全标准和评估框架尚无法直接解决这一问题. 我们建议开发和测试基于IoT的智能环境安全评估框架, 应用于IoT设备安全测试评估与认证项目.

5.5 融合新兴技术不断提升检测评估技术能力

随着深度学习、联邦学习、大模型等新兴技术的不断涌现, IoT设备各层安全风险的检测评估方法也在不断更新换代. 深度学习由于人工先验知识依赖较少, 具有出色的可移植性等优势已逐渐应用于IoT设备安全风险检测[140-141]. 大模型技术也开始被用于安全领域[142-145], 并呈现出了强大的检测分类、逻辑推理和可解释性效果. 研究人员可针对IoT设备安全检测的深度学习或大模型, 创新设计更实用、更有效, 真正可应用于实际检测现场工作的检测方案.

此外, 基于联邦学习的IoT设备异常检测方法也已成为一大研究趋势[146-147], 通过利用分散设备上的数据, 可以主动识别IoT设备中存在的安全威胁, 仅通过与联邦的中央服务器共享学习到的权重, 以保持本IoT设备上的数据不出本地, 最大限度地保护数据隐私. 效率更高、鲁棒性更强的联邦学习架构和检测方案也有望在未来融入IoT设备安全检测平台.

作者贡献声明: 张妍提出论文整体思路、理论与实践技术方法总结, 以及负责论文撰写; 黎家通、宋小祎、范钰婷负责具体技术调研和论文精修; 路晔绵完成研究现状的撰写及部分论文修订; 张若定负责论文法律法规条文研究和把控论文方向与思路以及审核和修改论文; 王子馨负责部分技术调研、论文精修及润色.

参 考 文 献

[1] Xenofontos C, Zografopoulos I, Konstantinou C, et al. Consumer, commercial, and industrial IoT (in) security: Attack taxonomy and case studies[J]. IEEE Internet of Things Journal, 2021, 9(1): 199−221

[2] Li Bosong, Chang Anqi, Zhang Jiaxing. Internet of things botNet seriously threatens network infrastructure security——Analysis of Dyn company's botNet attack[J]. Information Security Research, 2016, 2(11): 1042−1048 (in Chinese)
(李柏松, 常安琪, 张家兴. 物联网僵尸网络严重威胁网络基础设施安全——对Dyn公司遭僵尸网络攻击的分析[J]. 信息安全研究, 2016, 2(11): 1042−1048)

[3] Catalin Cimpanu. Ukraine says it stopped a VPNFilter attack on a Chlorine distillation station[EB/OL]. (2018-07-12) [2023-08-25]. https://www.bleepingcomputer.com/news/security/ukraine-says-it-

stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/

[4] Alpha_h4ck. Vpnfilter malware attacked critical infrastructure in Ukraine[EB/OL]. (2018-07-16) [2023-08-25]. https://www.freebuf.com/news/177669.html(in Chinese)
(Alpha_h4ck. Vpnfilter恶意软件突袭了乌克兰的关键基础设施[EB/OL]. (2018-07-16) [2023-08-25]. https://www.freebuf.com/news/177669.html)

[5] Tang Zhe's cat. APT28 attack and control methods fot IoT devices (networks)[EB/OL].(2020-10-28)[2023-08-25].https://www.freebuf.com/news/253332.html(in Chinese)
(唐哲的猫. APT28针对IoT设备(网络)的攻击和控制方式[EB/OL]. (2020-10-28) [2023-08-25]. https://www.freebuf.com/news/253332.html)

[6] Evan. Data on Roomba vacuum cleaner leaked[EB/OL]. (2022-12-23) [2023-08-25]. https://technews.tw/2022/12/23/robot-vacuum-took-photo-of-woman-on-toilet-that-was-shared-on-facebook/(in Chinese)
(Evan. Roomba扫地机器人资料泄露[EB/OL]. (2022-12-23) [2023-08-25]. https://technews.tw/2022/12/23/robot-vacuum-took-photo-of-woman-on-toilet-that-was-shared-on-facebook/)

[7] ThroughTek. ThroughTek p2p sdk. [EB/OL]. (2021-06-15) [2023-08-25].https://www.cisa.gov/news-events/ics-advisories/icsa-21-166-01

[8] Labumbard J. Enterprise vulnerability management: US08789192B2 [P]. 2014-07-22

[9] Tanner D A, Hinchliffe A, Santos D. Threat assessment: Blackcat ransomware[EB/OL]. (2022-01-27) [2023-08-25]. https://unit42 Paloaltonetworks com/blackcatransomware/

[10] Abdulsattar K, Al-omary A. A survey: Security issues in IoT environment and IoT architecture[C] //Proc of the 3rd Smart Cities Symp. New York: Curran Associates, Inc, 2020: 298-304

[11] Veluvarthi R, Rameswarapu A, KalyanA K V S, et al. Security and privacy threats of IoT devices: A & short review[C] //Proc of the 2023 4th Int Conf on Signal Processing and Communication (ICSPC). Piscataway, NJ: IEEE, 2023: 32-37

[12] Murzaeva A, Kepceoglu B, Demirc S. Survey of network security Issues and solutions for the IoT[C] //Proc of the 2019 3rd Int Symp on Multidisciplinary Studies and Innovative Technologies (ISMSIT). Piscataway, NJ: IEEE, 2019: 511-516

[13] Zhang Qian, Ni Lin, Wu Bo. Research on security protection technology based on IoT device vulnerability detection[J]. Network Security Technology and Application, 2023(5): 24-26 (in Chinese)
(张骞, 倪林, 吴波. 基于IoT设备漏洞检测的安全防护技术研究[J]. 网络安全技术与应用, 2023(5): 24-26)

[14] Bettayeb M, Nasir Q, Talib M A. Firmware update attacks and security for IoT devices: Survey[C] //Proc of the ArabWIC 6th Annual Int Conf Research Track. New York: ACM, 2019: 1-6

[15] Kawakani, Claudio, Toshio, et al. A survey of intrusion detection in internet of things[J]. Journal of Network & Computer Applications, 2017, 84: 25-37

[16] Noor M B, Hassan W H. Current research on internet of things (IoT) security: A survey[J]. Computer Networks, 2019, 148(15): 283-294

[17] Nugroho E P, Djatna T, Sitanggang I S, et al. A review of intrusion detection system in IoT with machine learning approach: Current and future research[C] //Proc of the 2020 6th Int Conf on Science in Information Technology (ICSITech). Piscataway, NJ: IEEE, 2020: 138-143

[18] Khan A R, Kashif M, Jhaveri R H, et al. Deep learning for intrusion detection and security of Internet of things (IoT): Current analysis, challenges, and possible solutions[J/OL]. Security and Communication Networks. [2023-08-25]. https://doi.org/10.1155/2022/4016073

[19] Miessler D, Guzman A, Rudresh V, et al. Open web application security project[EB/OL]. [2023-08-25]. https://owasp.org/www-project-internet-of-things/#tab=IoT_Attack_Surface_Areas

[20] Felt A P, Wang H J, Moshchuk A, et al. Permission re-delegation: Attacks and defenses[C] //Proc of the 20th USENIX Security Symp. Berkeley, CA: USENIX Association, 2011: 19-34

[21] Meneghello F, Calore M, Zucchetto D, et al. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices[J]. IEEE Internet of Things Journal, 2019, 6(5): 8182-8201

[22] Musleh A S, Chen G, Dong Z Y. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2218-2234

[23] Sun Mingshen, Wei Tao, Lui J C. Taintart: A practical multi-level information-flow tracking system for Android runtime[C] //Proc of the 2016 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2016: 331-342

[24] Liu Ting, Liu Pengfei, Wang Jiazhou, et al. Method for detecting physical intrusion attack in industrial control system based on analysis of signals on serial communication bus: US20200302054A1 [P]. 2020-09-24

[25] IFTTT. Over 800 APPs, services, and devices (and millions of their users) rely on IFTTT for their most important integrations[EB/OL]. [2023-08-25]. https://ifttt.com

[26] Wang Lei, Yang Zhaojin, Li Gaoping, et al. Research on backscattering energy in large aperture high energy laser measurement[J]. Laser Technology, 2006, 30(1): 43-46 (in Chinese)
(王雷, 杨照金, 黎高平, et al. 大口径高能量激光测量中后向散射能量研究[J]. 激光技术, 2006, 30(1): 43-46)

[27] Grover K, Lim A, Yang Q. Jamming and anti–jamming techniques in wireless networks: A survey[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2014, 17(4): 197-215

[28] Wikipedia. BadUSB[EB/OL]. [2023-08-25]. https://en.wikipedia.org/wiki/BadUSB

[29] Liu Y, Li L. Testing and analysis of the security of WLAN based on WEP[J]. Journal of Wuhan University of Technology (Transportation Science & Engineering), 2006, 30(1): 60-62

[30] Vanhoef M. Fragment and forge: Breaking wi-fi through frame aggregation and fragmentation[C] //Proc of the 30th USENIX Security Symp (USENIX Security'21). Berkeley, CA: USENIX Association, 2021: 161-178

[31] KU Leuven. FragAttacks[EB/OL]. [2023-08-25]. https://www.fragattacks.com/

[32] Liu Guangxu, Chen Duyu. Discussion on Tesla auto network security specifications[J]. Chancheng, 2021(4): 56-57 (in Chinese)
(刘桄序, 陈杜宇. 基于特斯拉汽车网络安全的规范探讨[J]. 产城,

2021(4): 56−57)

[33] Wang Ying. Research on NFC-based mobile payment security technology [D]. Guangzhou: Guangdong University of Technology, 2016 (in Chinese)
(王影. 基于NFC的移动支付安全技术研究 [D]. 广州: 广东工业大学, 2016)

[34] Marksteiner S, Jiménez V J E, Vallant H, et al. An overview of wireless IoT protocol security in the smart home domain[C] //Proc of the 2017 Int of Things Business Models, Users, and Networks. Piscataway, NJ: IEEE, 2017: 1−8

[35] Thread group. Thread[EB/OL]. [2023-08-25]. https://www.threadgroup.org/

[36] Microstep online Research Response Center. An IoT botNet operated by the Sea Lotus Organization[EB/OL]. [2023-08-25]. https://mp.weixin.qq.com/s/v2wiJe-YPG0ng87ffBB9FQ(in Chinese)
(微步在线研究响应中心. “海莲花”组织运营的物联网僵尸网络[EB/OL]. [2023-08-25]. https://mp.weixin.qq.com/s/v2wiJe-YPG0-ng87ffBB9FQ)

[37] GA/T 1390.5-2017. Information security technology basic requirements for network security level protection part 5: Industrial control security expansion requirements [S]. Domestic-Industry Standard-Industry Standard-Public Safety Standard CN-GA, 2017 (in Chinese)
(GA/T 1390.5-2017. 信息安全技术网络安全等级保护基本要求第5部分: 工业控制安全扩展要求 [S]. 国内-行业标准-行业标准-公共安全标准 CN-GA, 2017)

[38] Wang Zhendong, Zhang Lin, Li Dahai. A survey of machine learning-based intrusion detection systems for the Internet of things[J]. Computer Engineering and Applications, 2021, 57(4): 18−27 (in Chinese)
(王振东, 张林, 李大海. 基于机器学习的物联网入侵检测系统综述[J]. 计算机工程与应用, 2021, 57(4): 18−27)

[39] Li Rui, Diao Wenrui, Li Zhou, et al. Android custom permissions demystified: From privilege escalation to design shortcomings[C] //Proc of the 2021 IEEE S&P. Piscataway, NJ: IEEE, 2021: 70−86

[40] Yang Zhemin, Yang Min, Zhang Yuan, et al. AppIntent: Analyzing sensitive data transmission in Android for privacy leakage detection[C] //Proc of the 2013 ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 1043−1054

[41] Zhon Wei, Jia Yan, Yao Yao, et al. Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms[C]// Proc of the 28th USENIX conf on Security Symp. Berkeley, CA: USENIX Association, 2019:1133-1150. DOI:10.48550/arXiv.1811.03241.

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

[43] Intersoft consulting. General Data Protection Regulation[EB/OL]. (2016-05-04)[2023-08-25]. https://gdpr-info.eu

[44] Bainbiridge D, Pearce G. The UK data protection act 1998 — Data subjects' rights[J]. Computer Law & Security' Review, 1998, 14(6): 401−406

[45] UK Gov. Data Protection Act 2018[EB/OL]. (2018-05-23)[2023-08-25]. https://www.gov.uk/government/collections/data-protection-act-2018

[46] India Internets. California Consumer Privacy Act[EB/OL]. [2023-08-25]. https://www.coralesecure.com/california-consumer-privacy-act.php

[47] GC. Personal Information Protection and Electronic Documents Act (S. C. 2000, c. 5)[EB/OL]. (2000-05-21)[2023-08-25]. https://laws-lois.justice.gc.ca/eng/acts/P-8.6

[48] Entrust. South Africa Protection of Personal Information Act[EB/OL]. (2013-11-03)[2023-08-25]. https://www.entrust.com/digital-security/hsm/solutions/compliance/emea/complying-south-africas-protection-personal-information-act

[49] JPn Gov. Amended Act on the Protection of Personal Information[EB/OL]. (2015-12-09)[2023-08-25]. https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf

[50] Yu Chen. Data Security Law of the People's Repulic of China[EB/OL]. (2021-06-10)[2023-08-25]. http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml(in Chinese)
(余晨. 中华人民共和国数据安全法[EB/OL]. (2021-06-10)[2023-08-25]. http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a-73b56d7938f99a788a.shtml)

[51] Parvin S, Goli M, Torres F S, et al. Trojan-D2: Post-layout design and detection of stealthy hardware trojans-a risc-v case study[C] //Proc of the 28th Asia and South Pacific Design Automation Conf. Piscataway, NJ: IEEE, 2023: 683−689

[52] U. S. Department of Homeland Security. Strategic Principles for Securing the Internet of Things [EB/OL]. (2016-11-15)[2023-08-25]. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016−1115-FINAL_v2-dg11.pdf

[53] Choo K-K R, Gai K, Chiaraviglio L, et al. A multidisciplinary approach to Internet of things (IoT) cybersecurity and risk management [Z]. Amsterdam: Elsevier, 2021: 102136

[54] Tech target. Common Criteria (CC) for Information Technology Security Evaluation[EB/OL]. (2005-05-04)[2023-08-25]. https://www.techtarget.com/whatis/definition/Common-Criteria-CC-for-Information-Technology-Security-Evaluation

[55] Cad. Common evaluation methodology[EB/OL]. (2020-11-23)[2023-08-25]. https://www.connectedautomateddriving.eu/gaps-to-be-addressed-in-the-common-evaluation-methodology/

[56] China Cybersecurity Review Technology and Certification Center[EB/OL]. [2023-06-23]. https://www.isccc.gov.cn/
(中国网络安全审查技术与认证中心[EB/OL]. [2023-06-23]. https: //www.isccc.gov.cn/)

[57] Bieker F, Friedewald M, Hansen M, et al. A process for data protection impact assessment under the European general data protection regulation[C] //Proc of the Privacy Technologies and Policy: 4th Annual Privacy Forum (APF 2016). Berlin: Springer, 2016: 21−37

[58] Edpb. European Data Protection Board[EB/OL]. [2023-08-25]. https://edpb.europa.eu/edpb_en

[59] Commission E. Guidelines on data protection impact assessment

(DPIA)(wp248rev. 01)[Z]. 2017. http://iapp.org/media/pdf/resource_center/wp29-GDPR-DPIA-guidance_final.pdf

[60] Edpb. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications[EB/OL]. (2020-01-26)[2023-08-25]. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en

[61] GB/T 39335-2020. Information Security Technology Personal Information Security Impact assessment Guidelines[S]. Domestic-National Standards-State Administration for Market Regulation CN-GB (in Chinese)
(GB/T 39335-2020. 信息安全技术 个人信息安全影响评估指南[S]. 国内-国家标准-国家市场监督管理总局 CN-GB)

[62] Wu Shenkuo. GB/T 35273-2017 "Information security technology personal information security specifications"[J]. Standard Life, 2018(3): 30−33 (in Chinese)
(吴沈括. GB/T 35273-2017《信息安全技术 个人信息安全规范》[J]. 标准生活, 2018(3): 30−33)

[63] Wikipedia. European telecommunications Standards Institute, ETSI. [EB/OL]. [2023-08-25]. https://en.wikipedia.org/wiki/ETSI

[64] CYBER - Cyber security for consumer Internet of things: Baseline requirements (Endorsement of the English version EN 303 645 V2.1.1 (2020−06) as a German standard)[S]. Berlin: DE-DIN, 2021

[65] USA Gov. National Institute of Standards and Technology, NIST [EB/OL]. [2023-08-25]. https://www.nist.gov/

[66] USA Gov. Foundational cybersecurity activities for IoT device manufacturers, NISTIR 8259[EB/OL]. [2023-08-25]. https://csrc.nist.gov/publications/detail/nistir/8259/final

[67] CTIA. Cellular telecommunications industry association, CTIA[EB/OL]. [2023-08-25]. https://www.ctia.org/

[68] UL. UL solutions[EB/OL]. [2023-04-16].https://www.ul.com

[69] Advanced RISC machines. PSA certified: Building trust in IoT[EB/OL]. (2019-02-25)[2023-08-25]. https://www.arm.com/company/news/2019/02/psa-certified-building-trust-in-iot

[70] Shi mingming, Xie Zongxiao. Analysis of GB/T 37931—2019 "Information security technology web application security detection system security technical requirements and test evaluation methods"[J]. China Quality and Standard Herald, 2020, 270(4): 14−15, 34 (in Chinese)
(施明明, 谢宗晓. GB/T 37931-2019《信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法》浅析[J]. 中国质量与标准导报, 2020, 270(4): 14−15, 34)

[71] National Public Service Platform for Standards Information. Information security technology IoT security reference model and general requirements, Information security technology—Security reference model and generic requirements for internet of things[EB/OL]. (2019-07-01)[2023-08-25]. https://std.samr.gov.cn/gb/search/gbDetailed?id=7E2903B0D5475A63E05397BE0A0AF660 (in Chinese)
(全国标准信息公共服务平台. 信息安全技术物联网安全参考模型及通用要求[EB/OL]. (2019-07-01)[2023-08-25]. https://std.samr.gov.cn/gb/search/gbDetailed?id=7E2903B0D5475A63E05397BE0A0AF660)

[72] YDB 173-2017. Internet of things terminal embedded operating system security technical requirements[S]. Domestic-Industry Standard-Industry Standard-Post and Telecommunications CN-YD (in Chinese)
(YDB 173-2017. 物联网终端嵌入式操作系统安全技术要求[S]. 国内-行业标准-行业标准-邮电通信 CN-YD)

[73] Marinissen E J, Vermeulen H G H, Hollmann H D L. Automatic test pattern generation: W02004104609ALL[P]. 2001-12-02

[74] Mondel A, Karmakar S, Mahalat M H, et al. Hardware Trojan detection using transition probability with minimal test vectors[J]. ACM Transactions on Embedded Computing Systems, 2022, 22(1): 1−21

[75] Alkabani Y. Trojan immune circuits using duality[C] //Proc of the 2012 15th Euromicro Conf on Digital System Design. Piscataway, NJ: IEEE, 2012: 177−184

[76] Chakraborty R S, Paul S, Bhunia S. On-demand transparency for improving hardware Trojan detectability[C] //Proc of the 2008 IEEE Int Workshop on Hardware-Oriented Security and Trust. Piscataway, NJ: IEEE, 2008: 48−50

[77] Sakmani H, Tehranipoor M, Plusquellic J. A novel technique for improving hardware Trojan detection and reducing Trojan activation time[J]. IEEE Transactions on Very Large Scale Integration Systems, 2011, 20(1): 112−125

[78] Shende R , Ambawade D D . A side channel based power analysis technique for hardware Trojan detection using statistical learning approach[C] // Proc of 2016 13th Int Conf on Wireless and Optical Communications Networks. Piscataway, NJ: IEEE, 2016: 1−4

[79] Gunti N B, Lingasubramanian K. Efficient static power based side channel analysis for hardware Trojan detection using controllable sleep transistors[C] //Proc of the IEEE SoutheastCon. Piscataway, NJ: IEEE, 2015: 920−925

[80] Jin Y, Makris Y. Hardware Trojan detection using path delay fingerprint[C] //Proc of the 2008 IEEE Int Workshop on Hardware-oriented Security and Trust. Piscataway, NJ: IEEE, 2008: 51−57

[81] Mohammed H, Odetola T A, Hasan S R, et al. (HIADIoT): Hardware intrinsic attack detection in Internet of things; leveraging power profiling[C] //Proc of the 2019 IEEE 62nd Int Midwest Symp on Circuits and Systems. Piscataway, NJ: IEEE, 2019: 852−855

[82] Mohammed H, Hasan S R, Awwad F. FusIon-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware Trojan attacks[J]. IEEE Access, 2020, 8(99): 36847−36862

[83] Chen Zhe, Guo Shize, Wang Jian, et al. Toward FPGA security in IoT: A new detection technique for hardware Trojans[J]. IEEE Internet of Things Journal, 2019, 6(4): 7061−7068

[84] Gohil V, Guo H, Patnaik S, et al. Attrition: Attacking static hardware Trojan detection techniques using reinforcement learning[C] //Proc of the 2022 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2022: 1275−1289

[85] Hu Tao, Tsukune Songyi, Jiang Ronghua. Hardware Trojan horse detection based on long short-term memory neural network[J]. Computer Engineering, 2020, 46(7): 110−115 (in Chinese)
(胡涛, 佃松宜, 蒋荣华. 基于长短时记忆神经网络的硬件木马检测[J]. 计算机工程, 2020, 46(7): 110−115)

[86] Sermagroup. Hardsploit[EB/OL]. (2017-09-08)[2023-08-25]. https://

hardsploit.io

[87] Xipiter. Using the shikra to attack embedded systems getting started[Z]. 2016

[88] Bus Pirate. The Bus Pirate is an open source hacker multi-tool[EB/OL].(2022-06-03)[2023-08-25].http://dangerousprototypes.com/docs/Bus_Pirate

[89] Antonioli D, Tippenhauer N O, Rasmussen K B. The knob is broken: Exploiting low entropy in the encryption key negotiation of bluetooth bR/edr[C] //Proc of the 28th USENIX Security Symp. Berkeley, CA: USENIX Association, 2019: 1047–1061

[90] Zhang Yue, Weng Jian, Dey R, et al. Breaking secure pairing of bluetooth low energy using downgrade attacks[C] //Proc of the 29th Usenix Security Symp. Berkeley, CA: USENIX Association, 2020: 37−54

[91] Tang Yongli, Zhao Wenjing, Liang Bo, et al. Secure transmission test method of ZigBee protocol based on randomness detection[J]. Journal of Nanjing University of Science and Technology (Natural Science Edition), 2015, 39(1): 78−83 (in Chinese)
(汤永利, 赵文静, 梁博, 等. 基于随机性检测的ZigBee协议安全传输测试方法研究[J]. 南京理工大学学报: 自然科学版, 2015, 39(1): 78−83)

[92] Takanen A, Demott J D, Miller C, et al. Fuzzing for Software Security Testing and Quality Assurance[M]. Canton St. Norwood, MA: Artech House, Inc, 2018

[93] Liang Shurui. Zigbee protocol fuzz testing algorithm based on FSM[D]. Beijing University of Posts and Telecommunications, 2014(in Chinese)
(梁姝瑞. 基于FSM的Zigbee协议模糊测试算法[D]. 北京: 北京邮电大学, 2014)

[94] Wiedemann N, Pfanner N. Mitochondrial machineries for protein import and assembly[J]. Annual Review of Biochemistry, 2017, 86(1): 685−714

[95] Stute M, Heinrich A, Lorenz J, et al. Disrupting continuity of Apple's wireless ecosystem security: New tracking, DOS, and MITM attacks on IOS and MACOS through bluetooth low energy, AWDL, and WI-FI[C] //Proc of the 30th USENIX Security Symp. Berkeley, CA: USENIX Association, 2021: 1−18

[96] Akter S, Chellappan S, Chakraborty T, et al. Man-in-the-middle attack on contactless payment over NFC communications: Design, implementation, experiments and detection[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 18(6): 3012−3023

[97] WimsettI B T. Europay/MasterCard/Visa Migration Status [J/OL]. [2023-04-15].http://insidepatientcare.com/issues/2014/october-2014-vol-2-no-5/81-europay-mastercard-visa-migration-status

[98] Mera A, Feng Bo, Lu Long, et al. Dice: Automatic emulation of DMA input channels for dynamic firmware analysis[C] //Proc of the 2021 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2021: 1938−1954

[99] Wang H E, Tsai T L, Lin C H, et al. String analysis via automata manipulation with logic circuit representation[C] //Proc of the Computer Aided Verification: 28th Int Conf. Berlin: Springer, 2016, 241−260

[100] Palavicini JR G, Bryan J, Sheets E, et al. Towards firmware analysis of industrial Internet of things (IIoT) - Applying Symbolic Analysis to IIoT Firmware Vetting[C] //Proc of the 2nd Int Conf on Internet of Things, Big Data and Security: IoTBDS, 2017. S. L. : SciTePress, 2017: 470−477

[101] Nadir I, Mahmood H, Asadullah G. A taxonomy of IoT firmware security and principal firmware analysis techniques[J]. International Journal of Critical Infrastructure Protection, 2022, 38: 100552

[102] Costin A, Zaddach J, Francillon A, et al. A large-scale analysis of the security of embedded firmwares[C] //Proc of the 23rd USENIX Security Symp (USENIX Security 14). Berkeley, CA: USENIX Association, 2014: 95−110

[103] Thomas S L, Garcia F D, Chothia T. Humidify: A tool for hidden functionality detection in firmware[C] //Proc of the Detection of Intrusions and Malware, and Vulnerability Assessment: 14th Int Conf. Berlin: Springer, 2017: 279−300

[104] Schuster F, Holz T. Towards reducing the attack surface of software backdoors[C] //Proc of the 2013 ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 851−862

[105] Shoshitaishvili Y, Wang R, Hauser C, et al. Firmalice-automatic detection of authentication bypass vulnerabilities in binary firmware[C/OL] //Proc of the 22nd Annual Network and Distributed System Security Symp. [2015-02-11]. https://www.ndss-symposium.org/wp-content/uploads/2017/09/11_1_2.pdf.

[106] Chen D D, Woo M, Brumley D, et al. Towards automated dynamic analysis for Linux-based embedded firmware[C/OL] //Proc of the 23rd Annual Network and Distributed System Security Symp. 2016. https://www.ndss-symposium.org/wp-content/uploads/2017/09/towards-automated-dynamic-analysis-linux-based-embedded-firmware.pdf

[107] Zheng Y, Davanian A, Yin H, et al. Firm-AFL: High-throughput greybox fuzzing of IoT firmware via augmented process emulation[C] //Proc of the 28th USENIX Security Symp. Berkeley, CA: USENIX Association, 2019: 1099−1114

[108] Chen Jiongyi, Diao Wenrui, Zhao Qingchuan, et al. IoTfuzzer: Discovering memory corruptions in IoT through app-based fuzzing[C/OL] //Proc of the 25th Annual Network and Distributed System Security Symp. 2018. https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-1_Chen_paper.pdf

[109] 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 Annual Network and Distributed System Security Symp. 2018 [2023-08-25]. https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-4_Muench_paper.pdf

[110] Zhu Lipeng, Fu Xiaotong, Yao Yao, et al. FIot: Detecting the memory corruption in lightweight IoT device firmware[C] //Proc of the 2019 18th IEEE Int Conf On Trust, Security And Privacy In Computing and Communications/13th IEEE Int Conf on Big Data Science and Engineering (TrustCom/BigDataSE). Piscataway, NJ: IEEE, 2019: 248−255

[111] Kim M, Kim D, Kim E, et al. Firmae: Towards large-scale emulation of IoT firmware for dynamic analysis[C] //Proc of the Annual Computer Security Applications Conf. New York: ACM, 2020: 733−745

[112] Clements A, Gustafson E, Scharnowski T, et al. Halucinator: Firmware re-hosting through abstraction layer emulation[C] //Proc

of the 29th USENIX Security Symp. Berkeley, CA: USENIX Association, 2020: 1201−1218

[113] Redini N, Continella A, Das D, et al. Diane: Identifying fuzzing triggers in apps to generate under-constrained inputs for IoT devices[C] //Proc of the 2021 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2021: 484−500

[114] Costion A, Zarras A, Francillon A. Automated dynamic firmware analysis at scale: A case study on embedded web interfaces[C] //Proc of the 11th ACM on Asia Conf on Computer and Communications Security. New York: ACM, 2016: 437−448

[115] Falas S, Konstantionou C, Michael M K. A hardware-based framework for secure firmware updates on embedded systems[C] //Proc of the 2019 IFIP/IEEE 27th Int Conf on Very Large Scale Integration (VLSI-SoC). Piscataway, NJ: IEEE, 2019: 198−203

[116] Schmeidl F, Nazzal B, Alafi M H. Security analysis for smartthings IoT applications[C] //Proc of the 2019 IEEE/ACM 6th Int Conf on Mobile Software Engineering and Systems (MOBILESoft). Piscataway, NJ: IEEE, 2019: 25−29

[117] Wang Huan, Chen Jianping, Zhao Jianping, et al. A vulnerability assessment method in Industrial Internet of things based on attack graph and maximum flow[J]. IEEE Access, 2018, 6: 8599−8609

[118] He Daojing, Gu Hongjie, Li Tinghui, et al. Toward hybrid static-dynamic detection of vulnerabilities in IoT firmware[J]. IEEE Network, 2020, 35(2): 202−207

[119] Yavuz T, Brant C. Security analysis of IoT frameworks using static taint analysis[C] //Proc of the 12th ACM Conf on Data and Application Security and Privacy. New York: ACM, 2022: 203−213

[120] Luo Lannan, Zeng Qiang, Yang Bokai, et al. Westworld: Fuzzing-assisted remote dynamic symbolic execution of smart apps on IoT cloud platforms[C] //Proc of the Annual Computer Security Applications Conf. New York: ACM, 2021: 982−995

[121] Chen Lu, Liu Xing, Ma Yuanyuan, et al. Research on static analysis technology of Android application security defects[C] //Proc of the Int Conf on Electrical Engineering and Automation. Lancaster, PA: Destech Publications, 2016: 525−532

[122] Wu Bolun, Zou Futai. Code vulnerability detection based on deep sequence and graph models: A survey[J/OL]. Security and Communication Networks, 2022 [2023-08-25]. https://doi.org/10.1155/2022/1176898

[123] Feng Hantao, Fu Xiaotong, Sun Hongyu, et al. Efficient vulnerability detection based on abstract syntax tree and deep learning[C] //Proc of the IEEE Infocom 2020-IEEE Conf on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway, NJ: IEEE, 2020: 722−727

[124] Song Zihua, Wang Junfeng, Liu Shengli, et al. Hgvul: A code vulnerability detection method based on heterogeneous source-level intermediate representation[J/OL]. Security and Communication Networks, 2022 [2023-08-25]. https://doi.org/10.1155/2022/1919907

[125] Napier K, Bhowmik T, Wang S. An empirical study of text-based machine learning models for vulnerability detection[J]. Empirical Software Engineering, 2023, 28(2): Article No.38

[126] Smartthing. SmartTHING[EB/OL]. [2023-08-25]. https://www.smartthing.org

[127] IFTTT. IFTTT[EB/OL]. [2023-08-25]. https://ifttt.com

[128] Amazon. Get started with the free Alexa App[EB/OL]. [2023-08-25]. https://www.amazon.com/b?ie=UTF8&node=18354642011

[129] Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications[C] //Proc of the 2016 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2016: 636−654

[130] Fernandes E, Rahmati A, Jung J, et al. Decentralized action integrity for trigger-action IoT platforms[C/OL] //Proc of the 25th Annual Network and Distributed System Security Symp.2018 [2023-08-25]. https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-3_Fernandes_paper.pdf

[131] Wang Xinyu, Sun Jun, Chen Zhenbang, et al. Towards optimal concolic testing[C]//Proc of the 40th Int Conf on Software Engineering. New York: ACM, 2018: 291−302

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

[133] Surbatovich M, Aliuraidan 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. New York: ACM, 2017: 1501−1510

[134] Zhang Nan, Mi Xianghang, Fengxuan, et al. Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems[C] //Proc of the 2019 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2019: 1381−1396

[135] Andeson J P. Computer security threat monitoring and surveillance[R]. Washington, Pa: James P Anderson Company, 1980

[136] Denning D E. An intrusion-detection model[J]. IEEE Transactions on Software Engineering, 1987(2): 222−232

[137] Wang Zhanpeng, Wu Hongguang, Ma Beijiao, et al. Research on intrusion detection technology of industrial Internet of things based on machine learning[J]. Intelligent IoT Technology, 2018, 1(2): 13−17 (in Chinese)
(王展鹏, 吴红光, 马蓓娇, 等. 基于机器学习的工业物联网入侵检测技术研究[J]. 智能物联技术, 2018, 1(2): 13−17)

[138] Pan Tong, Chen Wei, Wu Lifa. IoT intrusion detection method for unbalanced samples[J]. Journal of Network and Information Security, 2023, 9(1): 130−139 (in Chinese)
(潘桐, 陈伟, 吴礼发. 面向不平衡样本的物联网入侵检测方法[J]. 网络与信息安全学报, 2023, 9(1): 130−139)

[139] Hu Xiangdong, Xiong Wentao. Research on intrusion detection method for smart home[J]. Guangdong Communication Technology, 2016, 36(5): 10−16 (in Chinese)
(胡向东, 熊文韬. 面向智能家居的入侵检测方法研究[J]. 广东通信技术, 2016, 36(5): 10−16)

[140] Dong Feng, Wang Junfeng, Li Qi, et al. Defect prediction in Android binary executables using deep neural network[J]. Wireless Personal Communications, 2018, 102: 2261−2285

[141] Cui Jianfeng, Wang Lixin, Zhao Xin, et al. Towards predictive analysis of Android vulnerability using statistical codes and machine learning for IoT applications[J]. Computer Communications, 2020, 155: 125−131

[142] Aghaei E , Niu Xi, Shadid W , et al. SecureBERT: A domain-specific language model for cybersecurity[J]. ArXiv preprint, arXiv.

2204.02685, 2022

[143] Kereopa-yopke B. Building resilient SMEs: Harnessing large language models for cyber security in Australia[J]. ArXiv preprint, arXiv: 2306.02612, 2023

[144] Cintas-canto A, Kaur J, Mozaffari-kermani M, et al. ChatGPT vs lightweight security: First work implementing the nist cryptographic standard ascon[J]. ArXiv preprint, arXiv: 2306.08178, 2023

[145] Zhang Yangyong, Xu Lei, Menaoza A, et al. Life after speech recognition: Fuzzing semantic misinterpretation for voice assistant applications[C/OL]// Proc of the Network and Distributed System Security Symp (NDSS'19). 2019 [2023-08-25]. https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_08-4_Zhang_paper.pdf

[146] Cui Lei, Qu Youyang, Xie Gang, et al. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures[J]. IEEE Transactions on Industrial Informatics, 2022, 5(18): 3492−3500

[147] Mothukuri V, Khare P, Parizi R M, et al. Federated-learning-based anomaly detection for IoT Security attacks[J]. IEEE Internet of Things Journal, 2021, 9(4): 2545−2554

Zhang Yan, born in 1983. PhD, associate researcher. Member of CCF. Her main research interests include software security, Internet of things system security, and artificial intelligence system security.

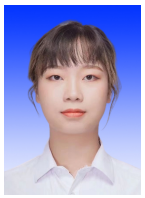
张 妍, 1983 年生. 博士, 副研究员. CCF 会员. 主要研究方向为软件安全、IoT 系统安全、人工智能系统安全.

Li Jiatong, born in 1998. Master. His main research interests include IoT security, graph neural network, deep learning, and natural language processing.

黎家通, 1998 年生. 硕士. 主要研究方向为 IoT 安全、图神经网络、深度学习、自然语言处理.

Song Xiaoyi, born in 1997. Master. Her main research interests include deep learning, natural language processing, and IoT security.

宋小祎, 1997 年生. 硕士. 主要研究方向为深度学习、自然语言处理、IoT 安全.



Fan Yuting, born in 2001. Bachelor. Her main research interest includes IoT security .

范钰婷, 2001 年生. 学士. 主要研究方向为 IoT 安全.

Lu Yemian, born in 1989. PhD, Senior engineer. Her main research interests include mobile terminal security, Internet of things terminal security, and trusted execution environment security.

路晔绵, 1989 年生. 博士, 高级工程师. 主要研究方向为移动终端安全、物联网终端安全、可信执行环境安全.

Zhang Ruoding, born in 1982. PhD, research associate. His main research interests include data security, artificial intelligence, software engineering, and IoT security.

张若定, 1982 年生. 博士, 助理研究员. 主要研究方向为数据安全、人工智能、软件工程、IoT 安全.

Wang Zixin, born in 2000. Master. Her main research interest includes IoT security.

王子馨, 2000 年生. 硕士. 主要研究方向为 IoT 安全.