面向物联网设备的轻量级漏洞挖掘技术原理与实现路径

易　凯
四川警察学院　四川泸州　646000

摘　要：随着物联网技术的广泛应用，物联网设备爆炸式增长。近年来，物联网设备导致的安全事件频发，使得物联网设备安全研究成为热点。物联网设备普遍存在资源有限、硬件异构等问题，传统漏洞挖掘技术难以适配，导致设备安全防护存在短板。为此，本文探讨面向物联网设备的轻量级漏洞挖掘技术原理与实现路径，希望为物联网设备安全防护提供可靠支撑。

关键词：物联网设备；轻量级；漏洞挖掘；技术原理；实现路径

引言

物联网是嵌入式设备与网络技术深度融合发展的产物，因此物联网设备具有典型的嵌入式设备特点，是嵌入式技术的继承与发展。在人们的生活中，到处都有嵌入式设备的身影[1]。在物联网技术的加持下，这些设备具备了网络通信能力，逐渐互联互通，构建起规模巨大的万物互联网。物联网设备的广泛应用以及设备间互联互通的特性，使其成为黑客攻击和数据泄露的高危地带。基于此，从技术原理、实现路径与应用策略三方面展开探讨，能够为物联网设备漏洞挖掘提供可行思路，助力提升设备整体安全防护水平。

一、物联网设备轻量级漏洞挖掘的技术原理

（一）协议交互的模糊测试引导

物联网设备之间传数据，大多靠自定义的通信协议，这些协议又没有统一的标准，很容易出现逻辑漏洞和安全隐患，模糊测试也就成了挖这类漏洞的主要办法。轻量级模糊测试技术跟着协议交互逻辑走，不再像传统方式那样瞎生成测试用例，能够提升挖漏洞的效率和准头。它先抓包解析协议，把设备和终端、云端之间的交互流程理清楚，提取出协议字段格式、校验规则、交互顺序这些关键信息，再搭建起协议交互模型。凭着这个模型生成符合协议规范的测试用例，不会让无效用例浪费设备资源和测试时间，也能减少对设备正常通信的干扰[2]。考虑到物联网协议追求轻便、延迟低，技术又优化了测试用例生成算法，严格控制用例的长度和复杂程度，贴合设备的数据处理能力。

（二）固件混合分析的路径发现

物联网设备固件常带着加密、压缩、指令集不一样这些问题，单靠静态分析或者单靠动态分析，都没法把所有漏洞挖掘场景覆盖到，固件混合分析技术对固件做静态解析，提取出代码结构、函数调用关系、权限控制流程这些基础信息，搭起一个初步的程序执行路径图。遇到加密固件，技术集成轻量级解密算法，通过解析固件头部信息和设备硬件特征，破解加密拿到原始代码，不让静态分析陷入数据盲区。静态分析做完，就挑那些高风险路径做动态验证，通过固件仿真环境加载固件并运行，模拟设备实际工作的情况，盯着路径执行时有没有异常行为。仿真环境采用轻量级架构，去除多余的虚拟硬件组件，只留和固件运行核心相关的模块，降低仿真时的资源消耗[3]，普通测试设备也能跑起来。技术通过静态路径标记和动态执行跟踪的联动方式，修正静态分析里因为代码混淆、间接跳转导致的路径偏差，确保找到的漏洞路径是真实能复现的。

二、轻量级漏洞挖掘的关键技术路径

（一）设备固件自动化提取分析

设备固件是挖漏洞的主要目标，手动提取固件又麻烦又慢，还容易因为操作失误弄坏固件，设备固件自动化提取分析技术就是专门解决这个问题的。它搭建了多接口适配模块，串口、网口、USB这些物联网设备常用的数据接口都能兼容，能自动识别设备有没有连好、固件存在哪里。针对不同厂商的固件传输协议，集成了标准化的通信指令集[4]，发送指令就能触发设备的固件备

基金项目：
1.刑事检验四川省高校重点实验室项目，编号：2024YB04
2.泸州市科技计划项目，编号：2024JYJ027

份功能，实现固件自动读取和存储，全程不用人工插手。固件提取完，自动化分析模块会快速预处理固件，删掉冗余数据、检查固件是否完整，要是遇到压缩格式的固件，会自动调用对应的解压算法，还原固件原本的结构。技术里内置了多指令集解析引擎，ARM、MIPS这些物联网设备主流的指令集都能适配，能把固件的二进制代码转换成可读的汇编代码，提取出函数信息、变量定义、执行流程这些关键内容。同时还加了固件安全性初筛功能，快速检查固件有没有默认密码、硬编码密钥、调试接口没关闭这些基础安全问题，为后续深度挖漏洞打基础。

（二）通信协议逆向建模测试

很多物联网设备用的是自定义私有通信协议，没有公开的技术文档，协议逆向建模测试技术靠还原协议逻辑，才能挖出这类协议里的漏洞。它先靠网络抓包工具捕获设备和交互对象之间的通信数据包，把数据包分类整理好，再提取出包头标识、数据字段、校验码、结束符这些关键信息。借助统计学分析和协议格式推导算法，还原字段含义、取值范围、交互时序规则，搭起初步的协议模型，同时标记出含义不明确的模糊字段[5]。对着模型里的模糊字段，发送变异数据包观察设备反应，一步步验证字段功能和约束条件，完善协议模型细节，确保模型能准确反映协议实际的交互逻辑。模型建好后，基于模型设计针对性的测试用例，对协议字段合法性校验、权限控制、异常处理这些环节做测试，排查有没有字段越界、校验缺失、时序混乱等漏洞。技术优化了协议逆向算法，降低了解析数据包、构建模型的算力消耗，适合轻量级测试场景，还支持增量建模，设备协议版本更新时，只需要对新增的字段和交互流程做逆向分析，不用重新搭建整个模型。

（三）运行时内存轻量级监测

物联网设备运行时的内存管理机制很简单，容易出现内存泄漏、缓冲区溢出这些漏洞，这类漏洞只有在设备运行的时候才能监测到，运行时内存轻量级监测技术也就应运而生了。它使用了轻量化的监测代理模块，通过设备调试接口植入固件，占用的内存和系统资源特别少，不会影响设备正常工作。监测代理实时跟踪内存分配和释放的全过程，记录内存块地址、大小、所属进程、生命周期这些关键信息，同时监测内存访问行为，排查越界访问、空指针引用这些异常操作。技术优化了内存数据采集算法，采用增量记录的方式，只记录变化的内存信息，减少数据传输和存储的开销，还会在本地初步分析筛选异常数据，只把高风险信息传到测试终端，进一步降低资源消耗。考虑到物联网设备对实时性要求高，监测代理采用优先级调度机制，保证监测任务不抢占设备核心业务资源，不会让设备出现卡顿、通信延迟等问题。监测时定了内存异常的判断规则，一旦检测到内存泄漏累积超过阈值、触发缓冲区溢出条件等情况，会立刻报警并记录漏洞上下文信息，包括触发进程、内存地址、操作指令等，给定位和验证漏洞提供准确依据。

（四）漏洞模式知识库构建

物联网设备的漏洞有不少共性特征和重复模式，漏洞模式知识库构建技术把各类漏洞信息整合起来，能给轻量级漏洞挖掘提供精准参考，进而提高挖掘效率和准度。技术广泛收集物联网设备常见的漏洞案例，覆盖固件、协议、内存、权限管理等多个方面，提取每个漏洞的触发条件、代码特征、表现形式、危害等级等关键信息，构建标准化的漏洞描述模型。把收集到的漏洞信息分类整理，按漏洞类型、影响设备类型、触发场景等维度建立索引，方便快速检索和匹配漏洞信息。知识库加了自动更新机制，通过爬虫技术实时抓取物联网安全平台、厂商公告、漏洞库等渠道的新增漏洞信息，经过人工审核和标准化处理后补充到知识库，保证信息及时、准确。同时支持手动录入自定义漏洞模式，测试人员能把挖掘过程中发现的新型漏洞特征添加进去，扩大知识库的覆盖范围。挖漏洞的时候，分析技术会把设备固件代码、协议交互数据、内存监测结果和知识库中的漏洞模式对比，快速识别出匹配的潜在漏洞，同时获取漏洞验证方法和修复建议。

三、轻量级漏洞挖掘的应用策略

（一）设计分层模型，适配异构硬件平台

物联网设备的硬件架构差异很大，有低功耗单片机、嵌入式处理器、边缘网关等多种类型，硬件性能差距明显，设计分层模型才能更好地适配不同设备。这个模型按功能分成感知层、分析层、适配层三个部分，每个部分独立封装又能协同工作，通过灵活配置满足不同硬件平台的运行需求。感知层装在目标设备上，集成了轻量化的数据采集和初步监测模块，只保留核心功能，适配低配置设备的资源约束，专门负责收集固件数据、协议交互信息、内存运行状态等基础数据。分析层部署在边缘节点或本地测试终端，算力比较强，负责对感知层上传的数据做深度分析、漏洞匹配和异常判定，不让大量计算任务占用目标设备资源。适配层作为中间衔接部分，负责协调感知层和分析层的数据传输与功能适配，会根

据目标设备的硬件性能，动态调整数据传输速率、分析深度和功能模块的启用状态。面对高性能边缘网关，适配层可以开启全量分析功能，挖掘深层的复杂漏洞；针对低功耗单片机，就只保留核心数据采集和简单异常监测功能，确保设备稳定运行。

（二）优化算法开销，实现低资源消耗运行

轻量级漏洞挖掘技术必须控制好资源消耗，只有优化算法开销，才能保证技术在物联网设备上稳定运行。研究人员从算法设计、数据处理、任务调度三个方面做优化，尽可能降低算力、内存和功耗消耗。算法设计上，采用精简的逻辑架构，删掉传统算法里多余的计算步骤和非核心功能，围绕挖漏洞的核心目标设计轻量化算法，比如符号执行时只跟踪关键变量，模糊测试时优先生成关联性强的用例。数据处理上，引入数据压缩、增量传输和本地预处理技术，减少数据存储和传输的开销，同时用低精度计算替代部分高精度计算，在不影响漏洞识别准度的前提下降低算力消耗。任务调度上，建立动态优先级机制，把漏洞挖掘任务分成高、中、低三个优先级，确保设备核心业务优先运行，漏洞挖掘任务只在设备资源空闲时占用资源。同时采用分时复用的办法，合理分配漏洞挖掘和设备业务的运行时间，避免两者争抢资源导致设备故障。针对电池供电的物联网设备，额外优化了功耗控制算法，设备休眠时就暂停漏洞挖掘任务，唤醒后快速恢复分析进度，延长设备续航时间。

（三）集成多源信息，提升漏洞验证效率

只靠单一来源的信息，没法全面支撑漏洞验证工作，很容易出现误判、漏判的情况，集成多源信息就能有效提高漏洞验证的效率和准度。这个策略整合了固件分析数据、协议交互日志、内存监测记录、设备运行状态等多方面信息，构建起全方位的漏洞验证数据体系，给判定漏洞提供充足依据。技术通过数据融合算法对多源信息做关联分析，去掉不同来源数据的冗余内容、化解数据冲突，提取核心关联特征，比如把固件代码里的缓冲区定义信息和内存监测中的越界访问记录对应起来，精准找到缓冲区溢出漏洞的具体位置和触发逻辑。集成过程中采用标准化数据接口，确保不同类型的信息能高效融合、顺畅交互，同时建立数据可信度评估机制，优先用可信度高的信息做漏洞验证，提高验证结果的可靠性。遇到疑似漏洞时，系统会自动调用多源信息交叉验证，通过比对不同维度的数据确认漏洞是否真实存在，避免因为单一信息片面导致误判，同时排除测试环境干扰、设备偶发故障等因素引发的虚假告警。多源信息集成还能给漏洞溯源提供完整的数据链条，帮助测试人员快速理清漏洞产生的根源、传播路径和潜在危害，给修复漏洞提供精准指导。

（四）构建闭环流程，支持持续安全监测

物联网设备的整个使用周期里，固件升级、功能迭代、运行环境变化都可能引入新漏洞，只做一轮漏洞挖掘没法保障设备长期安全，构建闭环流程才能实现持续安全监测。这个流程包含漏洞挖掘、验证、修复、复测四个核心环节，形成完整的安全防护循环，实现对设备全生命周期的安全监测。漏洞挖掘环节靠轻量级技术全面排查设备潜在漏洞，生成漏洞清单和详细报告；验证环节结合多源信息交叉确认漏洞的真实性和危害等级，划分漏洞修复的优先级；修复环节给设备厂商和用户提供针对性修复建议，包括代码修改方案、配置调整方法、固件更新补丁等；复测环节在漏洞修复后再次开展漏洞挖掘，验证修复效果，确保漏洞彻底消除，排查修复过程中可能引入的新漏洞。

结束语

轻量级漏洞挖掘技术恰好填补了传统方案在物联网设备场景的适配缺口，依托原理优化与路径创新，达成低资源消耗和高效挖掘的平衡。后续可细化技术细节，提升复杂场景下漏洞识别精准度，进一步完善对多类型设备的适配效果，让技术更好契合物联网行业发展需求，为各类智能设备安全运行筑牢基础。

参考文献

[1] 刘航天，甘水滔，张超，张红旗，孙文厚，高子聪，赵敏，白雪.物联网设备固件自动化漏洞挖掘技术研究综述[J].网络与信息安全学报，2025，11（02）：26-49.

[2] 刘治军.物联网感知数据分析与网络安全威胁评估[J].网络安全和信息化，2024，（06）：37-39.

[3] 王永刚.基于云计算平台的物联网数据挖掘研究[J].普洱学院学报，2023，39（06）：36-38.

[4] 陈世红，黄小琴.物联网设备漏洞检测技术研究[J].信息与电脑（理论版），2022，34（21）：219-221.

[5] 解超.物联网设备漏洞挖掘技术探究[J].数字通信世界，2022，（07）：30-32.