同行专家业内评价意见书编号：20250854447

附件1

浙江工程师学院（浙江大学工程师学院）
同行专家业内评价意见书

姓名：丁建春

学号：22260266

申报工程师职称专业类别（领域）：电子信息

浙江工程师学院（浙江大学工程师学院）制

2025年05月20日

填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位＋申报工程师职称专业类别(领域)4位+流水号3位，共11位。

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1.对本专业基础理论知识和专业技术知识掌握情况(不少于200字)

一、在基础理论知识方面，本人系统掌握电子信息领域的基础理论知识，包括电路理论、自动控制原理、嵌入式系统设计、通信原理、计算机网络等经典理论知识，以及强化学习、优化算法、大模型微调等现代方法，能够在解决复杂工程问题时灵活应用。熟悉当前电子信息领域的技术前沿，包括人工智能、物联网、形式化验证、自动化测试等领域的最新技术与发展趋势。
二、在专业技术知识方面，能够熟练使用各类专业软件进行程序分析与数据采集，包括利用IDA软件和Ghidra软件进行程序逆向分析与调试，利用Wireshark软件进行数据嗅探。掌握c/c++/python/shell多种编程语言和模糊测试方法原理，能够进行实时操作系统（RTOS）的开发和自动化测试系统的构建。此外，熟悉Pytorch框架和Transformer架构，能够对大模型进行有监督学习和微调。

2.工程实践的经历(不少于200字)

本人在杭州优稳自动化系统有限公司进行网络安全与漏洞挖掘相关工程实践，主要对实时操作系统固件进行自动化测试和漏洞挖掘，针对黑盒场景下实时操作系统固件自动化漏洞挖掘的难题，提出了静态污点分析和动态模糊测试相结合的混合模糊测试方案，开发了一套针对实时操作系统固件的自动化测试原型系统，并在20余个测试对象中发现了大量的程序崩溃。通过对程序崩溃逐一进行根因分析并编写漏洞利用代码，在9款主流的实际设备中成功复现13个CVE漏洞、挖掘到17个零日漏洞。

3.在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字）

在固件漏洞挖掘方面，由于固件通常以黑盒形式呈现，缺乏源代码和调试信息；固件代码结构复杂，不同组件代码混杂；缺乏适用于多种硬件架构的统一分析框架。传统方法通常依赖大量人工分析，效率低下且准确性有限。针对这些问题，本人提出了一种基于静态污点分析与动态模糊测试相结合的混合测试方案，实现了对黑盒固件的高效、准确漏洞挖掘。该方案通过微调CodeT5大模型自动补全固件中的函数名称，采用静态污点分析提取危险数据流，结合跨架构动态模糊测试，能够高效、准确地挖掘固件中的潜在漏洞，实现对黑盒场景下实时操作系统固件的自动化测试和漏洞挖掘。
1、基于CodeT5大模型的函数名称自动补全。针对黑盒固件缺少符号表的问题，本方案通过微调CodeT5大模型实现函数伪代码语义信息自动补全。具体步骤如下：首先，构建一个跨架构、跨优化层级的训练数据集。从真实环境中收集51个相关二进制工程文件，提取伪代码函数及其对应的函数名称，形成高质量数据集。该数据集覆盖了ARM、MIPS、x86等多种计算机架构，以及不同编译优化级别，确保了模型具备广泛适用性。其次，采用有监督学习方式微调CodeT5模型。通过设计特定任务目标和损失函数，使模型能够从伪代码中提取关键语义信息，并生成符合实际功能的函数名称。微调过程中采用了贪心搜索和术搜索等技术，提高了模型的收敛速度。最后，将微调后的模型应用于目标固件，恢复伪代码的函数名称。恢复后的函数名称为后续污点分析提供了关键入口点，使安全研究人员能够快速识别潜在的污点源函数、风险函数和敏感API调用。
2、基于污点分析的危险数据流提取。针对固件单包架构导致的代码混杂问题，采用污点分析方法提取危险数据流片段，具体步骤如下：首先，基于恢复的函数名称，人工识别出污点源函数(如网络数据接收函数)和汇聚函数(如内存操作函数)，并标注与污点数据对应的风险

参数。这一步骤建立了污点分析的基础，明确数据流的起点和终点。然后，应用静态污点分析技术追踪污点数据在固件中的流动路径。分析过程考虑了函数调用、变量赋值、指针操作等多种数据传递方式，确保全面捕获污点数据的传播轨迹，直至污点数据可能到达的敏感操作或API。最后，基于污点分析结果，采用定向切片技术将固件代码进行切片，提取受污点数据影响的代码片段。同时，通过路径修剪算法过滤掉无关代码路径，减少分析范围，更精准地聚焦于潜在漏洞路径，显著提高了后续动态分析的效率。

3、跨架构动态模糊测试与漏洞验证。对经污点分析得到的危险代码切片进行动态模糊测试，实现固件的跨架构动态分析，并为模糊测试发现的程序崩溃设计自动化PoC生成方法，具体步骤如下：首先，设计了基于Unicorn模拟执行框架的UnicornAFL利用框架。该框架能够加载固件切片的上下文环境，通过hook插桩机制获取模拟执行的状态反馈，实现对不同架构固件的统一分析。框架集成了内存访问监控、异常处理等功能，确保模拟执行的稳定性和准确性。其次，采用8线程并行框架加快模糊测试进程，大幅提高固件切片的测试效率。测试过程中动态调整突变策略和执行路径选择算法，使模糊测试更加智能地探索可能存在漏洞的代码区域。最后，对于模糊测试得到的程序崩溃结果，设计了基于崩溃点导向的PoC(概念验证)生成方法。该方法能够自动分析崩溃现场，提取关键触发条件，并生成可在真实设备上重现漏洞的验证代码，实现从固件切片崩溃到设备漏洞验证的自动转化，显著提高了大规模漏洞批量验证的效率。

本方案通过结合大模型技术、静态污点分析和动态模糊测试，构建了一套完整的固件漏洞挖掘流程。实验结果表明，该方案能够高效、准确地从黑盒固件中挖掘出潜在安全漏洞，为嵌入式设备和物联网安全提供了有力保障。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】

1.
公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
面向物联网设备固件的漏洞挖掘方法及装置、电子设备	发明专利申请	2024年11月26日	申请号：202411702330.5	2/5	导师一作，学生二作
第五届中国研究生人工智能创新大赛	获奖	2023年08月25日	https://mp.weixin.qq.com/s/zJku9xx6gQ2egSaVWvrJ5A	3/3	浙江大学校内选拔赛一等奖
	行业工法				

2.其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

参与浙江大学控制科学与工程学院XYY-111200-E22301科研项目，负责系统设计和算法实现，研究基于智能化定向模糊测试的固件漏洞检测技术，设计并实现了一套面向物联网设备固件的自动化分析与漏洞挖掘的原型系统。

（三）在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 84 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1 年（要求1年及以上） 考核成绩： 84 分
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！ **申报人签名：** 丁建春	

22260266

二、日常表现考核评价及申报材料审核公示结果

日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ☑优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）：2025年 5月 20日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因： ） 工程师学院教学管理办公室审核签字（公章）： 年 月 日

浙 江 大 学 研 究 生 院

攻读硕士学位研究生成绩表

学号：22260266	姓名：丁建春	性别：男	学院：工程师学院	专业：电子信息	学制：2.5年
毕业时最低应获：24.0学分		已获得：28.0学分		入学年月：2022-09	毕业年月：
学位证书号：			毕业证书号：		授予学位：

学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2022-2023学年秋季学期	工业互联网系统安全前沿技术		2.0	94	专业选修课	2022-2023学年冬季学期	产业技术发展前沿		1.5	87	专业学位课
2022-2023学年秋季学期	工程技术创新前沿		1.5	86	专业学位课	2022-2023学年冬季学期	研究生英语		2.0	84	公共学位课
2022-2023学年秋季学期	工业互联网安全系统工程		2.0	84	专业学位课	2022-2023学年春季学期	数学建模		2.0	61	专业选修课
2022-2023学年秋季学期	研究生英语基础技能		1.0	83	公共学位课	2022-2023学年春季学期	自然辩证法概论		1.0	87	公共学位课
2022-2023学年秋冬学期	工程伦理		2.0	94	公共学位课	2022-2023学年春夏学期	优化算法		3.0	76	专业选修课
2022-2023学年秋冬学期	研究生论文写作指导		1.0	89	专业学位课	2022-2023学年春夏学期	高阶工程认知实践		3.0	86	专业学位课
2022-2023学年冬季学期	新时代中国特色社会主义理论与实践		2.0	90	公共学位课		硕士生读书报告		2.0	通过	
2022-2023学年秋冬学期	工业系统动态建模求解及优化		2.0	81	专业学位课						

说明：1.研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2.备注中“*”表示重修课程。

学院成绩校核章：

成绩校核人：张梦依

打印日期：2025-06-03

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119939588 A
(43)申请公布日 2025.05.06

(21)申请号 202411702330.5

(22)申请日 2024.11.26

(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号
申请人 杭州优稳自动化系统有限公司

(72)发明人 王文海 丁建春 徐斌 王秋婷 李昕怡

(74)专利代理机构 杭州君锐达知识产权代理有限公司 33544
专利代理师 应孔月

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 11/3668(2025.01)
G06F 21/56(2013.01)

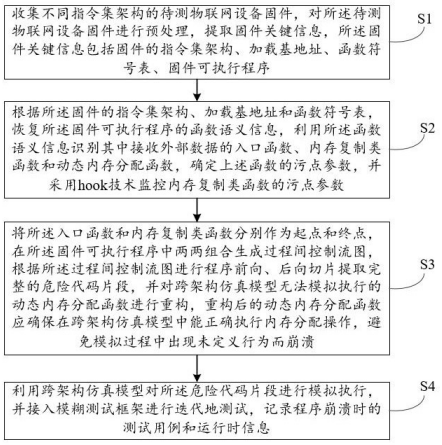
权利要求书2页 说明书8页 附图1页

(54)发明名称

面向物联网设备固件的漏洞挖掘方法及装置、电子设备

(57)摘要

本发明公开了一种面向物联网设备固件的漏洞挖掘方法及系统,其中系统包括:固件预处理模块,提取待测固件的加载基地址、函数符号表、可执行程序等;风险函数识别模块,根据先验知识设计启发式规则识别风险函数,并根据污点参数定义函数规格;程序静态切片模块,采用前向切片与后向切片结合的方法,从程序过程间控制流图中提取出完整的危险代码片段,并对动态内存分配函数进行重构;动态模糊测试模块,利用基于模拟执行的模糊测试框架实现对固件危险代码片段的仿真及模糊测试,同时动态监测漏洞表征。本发明的系统能够对物联网设备二进制固件进行高效地模糊测试和漏洞挖掘。



CN 119939588 A

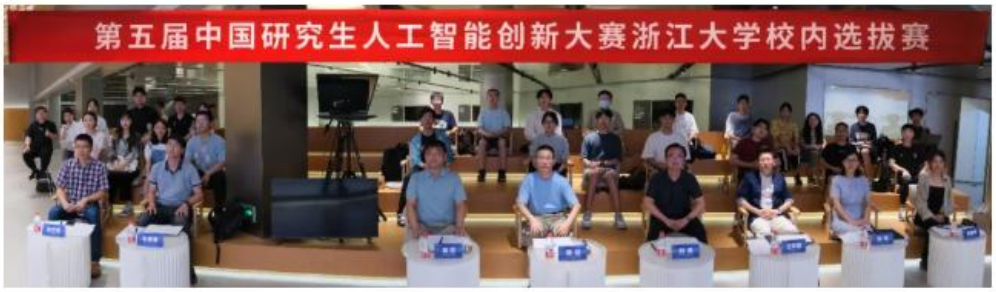
网站链接：第五届中国研究生人工智能创新大赛浙江大学校内选拔赛顺利举行

网站截图：

第五届中国研究生人工智能创新大赛浙江大学校内选拔赛顺利举行

浙江大学计算机学院研究生 2023年08月25日 15:33 浙江

8月21日下午，第五届中国研究生人工智能创新大赛浙江大学校内选拔赛于浙江大学紫金港校区举行。浙江大学党委研究生工作部副部长、研究生管理处副处长刘波老师，浙江大学计算机科学与技术学院和软件学院党委副书记陈璞老师，大赛评委蔡铭老师、张寅老师、朱霖潮老师、王冠云老师、章方铭老师，大赛秘书处滕如萍老师和参赛学生等出席本次活动。



刘波部长为本次大赛致辞。刘部长着重介绍了中国研究生人工智能创新大赛的发展历程，同时强调了其作为"中国研究生创新实践系列大赛"主题赛事之一的重要性和创新性。刘部长也代表学校向承办本次比赛的计算机学院和在场的各位评委老师表示感谢，表达了对各参赛团队以赛促学、赛出成绩的美好祝愿，勉励各位同学不断追求卓越，将个人发展融入党和国家的伟大事业中去。

本届中国研究生人工智能创新大赛浙江大学校内选拔赛共有29支队伍报名，21支队伍完成作品的提交，最终19支队伍进入校赛的答辩。每个参赛团队围绕项目背景，技术框架，以及应用目标等内容，对项目进行了全面展示。

附：

第五届中国研究生人工智能创新大赛浙江大学校内选拔赛获奖名单

类别	团队名	队长	队员	指导老师	推荐学院	奖项
技术创新类	Xxu4dv	徐 晟	林浩通 彭思达	周晓巍	计算机科学与技术学院	一等奖
应用创意类	CodeCrafters	叶 童	刘若茗 丁建睿	刘伟宁	控制科学与工程学院	一等奖
华为赛题一	Four2Nine	张知宇	刘晨光 张哲诚		控制科学与工程学院	一等奖
技术创新类	嗅探未来	石颖倩	胡家豪 尚书诺		生物医学工程与仪器科学学院	一等奖
应用创意类	Hypomimia Coach	徐宸瑞	徐瑞特 蔡晋岩 李正可	林 博 姚 玲	软件学院	二等奖
应用创意类	XDC-HUSEE	杨浩浩	汤程杰 潘正华 郑幸迪	厉向东 汤永川	软件学院、计算机科学与技术学院	二等奖
技术创新类	暴食疗愈者	谢晓倩	丁诗雯 张礼义 董赏雯	姚 玲 柴晋晋	工程师学院	二等奖
应用创意类	智能制造AI缺陷预测团队	王才城	张泽民 徐 凡 田佳淳	张树有 王自立	工程师学院	二等奖
应用创意类	我替你写	李元号	张庭榕 凡正波		工程师学院	二等奖
应用创意类	喵喵汪汪	张洪申			控制科学与工程学院	二等奖
技术创新类	星星之火2	杨一帆	吴宇辰 李廷龙 龚小天		工程师学院	三等奖
华为赛题二	文艺复兴	周欣涛	徐伟伟 吴美玲		工程师学院	三等奖
应用创意类	老年人守护者队	汪昊天	陈子龙 骆宇柯		生物医学工程与仪器科学学院	三等奖
应用创意类	老年人的守望者	林 泉	朱镇清	应仰威	生物医学工程与仪器科学学院	三等奖

应用创意类	老年人的守望者	林 泉	朱镇清	应仰威	科学学院	奖
应用创意类	Lit	何 平	戴怀轩 史新民		工程师学院	三等奖
华为赛题三	DreamAI	张佳文	陈 乾 孙吉贡	黄晓艳 张 健	电气工程学院	三等奖
技术创新类	洁霸	曹 靖	范 唯 杨哲斌 徐千一	杨豪强 张晓军	电气工程学院	三等奖
应用创意类	道路千万条	张曼琳	詹水根 杜秉哲 俞丹晋	朱 辰 黄崇文	工程师学院	三等奖
应用创意类	雏鹰翱翔	陈逸源	徐 朗 谢嘉威 储方炜	奚贝特	管理学院	三等奖

排版：石熠韩
今日编辑：石熠韩 | 研究生新媒体中心
责任编辑：章懿颖

征稿启事

投稿邮箱： xmt_zjucs@163.com

学生参与科研项目的情况说明

项目名称：XYY-111200-E22301（ZB-ZF-YY-课题-32057）

合同金额：70 万元

学生姓名：丁建春

学生排名：4

项目主要研究内容：研究基于智能化定向模糊测试的固件漏洞检测技术，设计并实现面向物联网设备固件的自动化分析与漏洞挖掘平台，提升针对物联网设备固件的漏洞挖掘能力。

取得的经济社会效益：1.安全防护价值：成功检测并修复了多款主流物联网设备中的安全漏洞，为防范数据泄露、设备控制权丧失等潜在的安全风险提供基础支撑。2.经济效益：帮助厂商识别并修复潜在安全问题，为降低产品的漏洞修复成本和品牌声誉损失提供技术支撑。3.技术创新价值：开发的自动化分析与漏洞挖掘平台提高了测试效率约 65%，缩短了漏洞发现周期，相比传统方法节省了大量人力和时间成本。

学生承担的主要工作：丁建春同学主要负责系统设计和算法实现，针对固件模糊测试的低成功率和人工构造漏洞 PoC 的复杂性，设计基于前向污点分析的 N 阶传播路径生成、基于后向污点分析的隐式依赖变量追踪、程序崩溃点导向的漏洞 PoC 自动生成等方法，以支持高效、快速、准确的固件模糊测试和漏洞验证脚本生成，复现了 10 余个已知漏洞并发现 3 个零日漏洞。

学生签名：丁建春

2025 年 5 月 19 日

项目负责人签名：

2025 年 5 月 19 日