同行专家业内评价意见书编号：20250854316

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：刘淳

学号：22260271

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03月04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)

在参与企业的工程实践过程中，我深入学习并系统掌握了工控安全相关的理论知识，包括控制系统架构、网络安全防护、攻击检测与防御技术等。在技术方面，我能够熟练运用先进的分析工具和安全测试工具。比如，在对网络流量分析的过程中掌握了wireshark工具的使用，能在各种网络实验中快速精准定位到对应的数据报文。在研究PLC的过程中，深入了解了西门子、施耐德等系列的多种PLC的组态编程和通信协议结构，掌握了常见的PLC编程方式和工程上的编程习惯，了解到真实工控场景下，不同PLC在编程实现上的差异点，如函数块使用、数据存储方式等。同时接触到linux操作系统，并熟悉了linux环境下的基本命令。在研究通信协议的过程中，深入了解了数据结构和计算机基础知识在实际生产中的应用，学习并掌握了IDA等逆向工具的使用。掌握了常见的静态分析、动态执行等软件逆向方法。

2.工程实践的经历(不少于200字)

我在绿盟科技集团股份有限公司参与工控设备网络安全综合评估与防护项目，负责研究工控设备的通信协议，对设备的脆弱性进行分析。为了更加熟悉工控设备，我参与到工业控制系统设计研发、生产销售、运行管理等全流程实践，在生产车间、在业务一线锤炼自己的实践能力。在项目研发过程中，我利用实验室工作站的靶场模拟真实工业应用场景，分析设备在恶意攻击下的安全性缺陷，并探索有效的防御策略。为提升测试的全面性和自动化水平，我提出采用协议逆向为先导的充分利用反馈信息的高效模糊测试方法，确立易触发漏洞的协议字段。进一步地，我对测试过程进行分析总结，形成完善的PLC安全测试框架。

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）

在工控设备网络安全综合评估与防护项目过程中，由于设备的源码和技术文档一般被严格保密，我们在针对工控设备做协议测试时，需要解决通信协议未知，并且无法有效利用反馈信息来引导测试过程的问题。我们通过结合自身的专业知识积累和国内外相关文献调研，提出一种基于协议逆向和反馈引导的工控协议安全测试方法，从工控私有协议逆向和基于反馈引导的模糊测试方面展开研究，利用协议逆向方法得到协议的报文格式和语义信息，为模糊测试提供必要的先验知识，然后结合模糊测试在自动化程度和普适性上的先天优势，研究反馈引导的模糊测试方法，利用测试目标的反馈信息优化变异策略。

具体而言，在报文格式重构方面，针对现有报文格式重构方法中使用多序列对比技术带来的高计算复杂度问题，提出利用消息自身结构特征规律来实现报文格式重构的方法。首先引入字段模式的概念，将字段内部的字节分布特性和特定数据的编码方式均视为字段的模式，为该方法奠定理论基础。接着从字段内部的字节分布特性入手，通过分析相邻消息字节中位之间的相对变化规律，设计自动化字段边界识别算法，用于初步划分字段。进一步地，针对特定数据类型和常见的序列化模式的编码结构设计专门的检测器，对初步划分的字段边界进行优化。这种方法在确保边界识别精度的同时能有效地减少时间复杂度，可以为后续环节提供可靠的支撑。

在语义解析方面，针对现有语义推断方法局限于分析少数几种字段，对未知协议适应性差的问题，提出基于循环神经网络的语义推断方法。为了从协议流量中尽可能全面地提取字段的特征，充分考虑字段本身、字段时序和字段上下文等多维度特征，利用多个不同的神经网络单元将各种特征分别提取出来之后，再集成为一个大的神经网络模型。为了解决现有方法无法推断超出既有规则覆盖范围之外的语义的问题，构建一种通用性的语义表述方法，将

一些细粒度的语义聚合成粗粒度的语义类别，这样针对私有协议中出现的一些未知或专有的字段，也可以通过计算它们与现有语义类别的距离来推断其归属。这种机制使系统不仅能处理已知语义，还能一定程度上理解和推断未知语义，提高对未知协议的适配能力。

最后，针对现有协议测试方法在工业私有协议上效率低下、缺乏反馈信息利用的问题，提出基于反馈引导的协议测试方法，首先建立初始测试用例生成方法，为模糊测试提供高质量的多样性初始测试用例，从一开始增加突变的覆盖范围。其次，收集与交互过程中设备的响应报文，将反馈信息和设备的执行路径对应起来，同时对不同的响应状态赋予不同的重要度，设计变异策略动态调整算法和迭代优化的变异方案，使模糊测试优先关注能触发新执行路径的测试用例和重要响应状态的变异策略，这种基于反馈的迭代过程，使得测试效率和路径覆盖范围不断增强。与此同时，在测试过程中识别易触发更多执行路径的关键语义字段，为私有协议模糊测试提供全面有效的技术支撑。

我们将提出的协议测试方法迁移至真实的工控设备上进行测试实验，发现了四个原创漏洞，其中三个收录进国家信息安全漏洞库，漏洞编号分别为CNVD-2023-27574、CNVD-2023-27576、CNVD-2023-27577，一个获得CVE漏洞认证，编号为CVE-2023-2846。

通过对方法进行总结，我们形成了一套完备的工控设备安全测试框架，这样的方法大大减少了人工分析固件带来的巨额人力成本，并且能锁定一些易触发漏洞的语义字段，对于私有协议的安全测试很有意义。这样的方法也可以为企业带来一定的经济收益和社会效益，例如我们可以基于该安全测试框架对工业场景下的控制器进行安全测试，发现其中存在漏洞，帮助其更好地管理和保护工控网络中的设备，提高其在市场竞争中的优势。在社会效益上，提出的方法通过提升工控网络安全管理水平，减少数据泄露事件的发生，可以推动工控安全行业的发展，针对找到的脆弱性构建相应的修复补丁，构建更安全稳定的工控蓝网。

（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
基于标记流量对比的工控设备信息提取方法及装置	授权发明专利	2023年12月12日	专利号：ZL 2023 1 0174766.0	5/7	
一种基于反馈增强的黑盒模糊测试方法及装置	发明专利申请	2024年10月28日	申请号：CN 202411506771.8	2/5	
一种基于协议逆向的工控设备黑盒模糊测试方法	发明专利申请	2023年09月01日	申请号：CN 202311120692.9	2/6	

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】

（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： 87 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： 87 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： 刘源

22260271

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）：　　2024年3月4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：22260271	姓名：刘淳	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：26.0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
2021-2022学年春季学期	研究生英语基础技能		1.0	免修	公共学位课	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	87	专业学位课
2021-2022学年春季学期	研究生英语		2.0	免修	专业学位课	2022-2023学年秋冬学期	工业系统动态建模求解及优化		2.0	91	专业学位课
2022-2023学年秋季学期	工程技术创新前沿		1.5	91	专业学位课	2022-2023学年春季学期	数学建模		2.0	92	专业选修课
2022-2023学年秋季学期	工业互联网系统安全前沿技术		2.0	94	专业学位课	2022-2023学年春季学期	自然辩证法概论		1.0	68	专业学位课
2022-2023学年秋季学期	工业互联网安全系统工程		2.0	93	专业学位课	2022-2023学年春夏学期	高阶工程认知实践		3.0	88	专业学位课
2022-2023学年秋冬学期	研究生论文写作指导		1.0	91	专业选修课	2022-2023学年夏季学期	“四史”专题		1.0	91	跨专业课
2022-2023学年秋冬学期	工程伦理		2.0	88	专业学位课		硕士生读书报告		2.0	通过	
2022-2023学年冬季学期	产业技术发展前沿		1.5	90	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：2025-03-20

浙江大学研究生院（60）成绩校核章

证书号第6549565号

发明专利证书

发 明 名 称：基于标记流量对比的工控设备信息提取方法及装置

发　明　人：孟捷;邓瑞龙;朱恒晔;车欣;刘淳;程鹏;陈积明

专　利　号：ZL 2023 1 0174766.0

专利申请日：2023年02月28日

专 利 权 人：浙江大学

地　　址：310058 浙江省杭州市西湖区余杭塘路866号

授权公告日：2023年12月12日　　授权公告号：CN 116527303 B

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，颁发发明专利证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。专利权期限为二十年，自申请日起算。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长
申长雨

2023年12月12日

其他事项参见续页

证书号第6549565号

专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年02月28日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

申请日时本专利记载的申请人、发明人信息如下：

申请人：

浙江大学

发明人：

孟捷;邓瑞龙;朱恒晔;车欣;刘淳;程鹏;陈积明

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119475344 A
(43)申请公布日 2025.02.18

(21)申请号 202411506771.8

(22)申请日 2024.10.28

(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 绿盟科技集团股份有限公司

(72)发明人 邓瑞龙 刘淳 车欣 程鹏 王晓鹏

(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 刘静

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 8/41(2018.01)
G06N 5/04(2023.01)
G06F 18/214(2023.01)
G06F 18/23(2023.01)
G06F 18/213(2023.01)
G06N 3/04(2023.01)
G06N 3/08(2023.01)

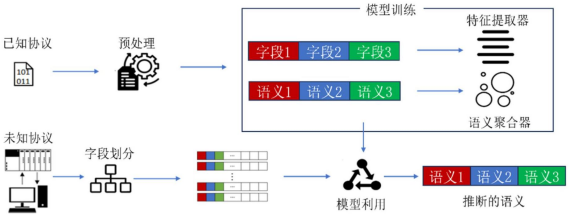
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种基于反馈增强的黑盒模糊测试方法及装置

(57)摘要

本发明公开了一种基于反馈增强的黑盒模糊测试方法及装置。该方法利用消息自身结构特征变化划分出字段边界,在此基础上构建自动化的语义推断方法,从公开协议中学习字段特征与语义类别之间的抽象联系,并将学习到的知识应用于推断私有协议中各个字段的语义;最后在模糊测试过程中收集设备反馈报文以建立新的反馈机制,根据反馈信息调整变异类型和变异策略。本发明能够基于工业现场的网络通信数据自动识别字段边界和语义信息,无需人工参与,并以此作为建立反馈机制的基础,对复杂、私有的工控协议具有较好的测试效果。



CN 119475344 A

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116991743 A
(43)申请公布日 2023.11.03

(21)申请号 202311120692.9

(22)申请日 2023.09.01

(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 绿盟科技集团股份有限公司

(72)发明人 邓瑞龙 刘淳 文宇恒 车欣 程鹏 王晓鹏

(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 刘静

(51)Int.Cl.
G06F 11/36(2006.01)
G06F 21/57(2013.01)

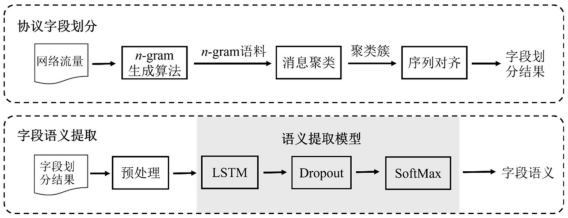
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种基于协议逆向的工控设备黑盒模糊测试方法

(57)摘要

本发明公开一种基于协议逆向的工控设备黑盒模糊测试方法。该方法通过采集工业控制系统现场的网络通信数据,经字段划分和预编码等处理过程后,输入到基于深度学习的语义提取模型,利用该模型实现对未知工控协议的语义提取,最终基于字段划分和语义提取的结果,指导模糊测试中测试用例的生成;并充分结合目标设备的反馈报文信息,选取与上次反馈报文差距最大的测试用例作为新一轮的输入。相比于传统的黑盒模糊测试方法Peach,本发明中的方法提高了黑盒模糊测试中有效测试用例的占比和漏洞触发效率。



CN 116991743 A