同行专家业内评价意见书编号：20250854355

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：凌茜

学号：22260087

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12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)

我具备扎实的计算机技术基础，系统掌握了系统安全与漏洞挖掘领域的核心理论知识，包括网络安全原理、攻击检测机制、符号执行、程序分析和渗透测试等关键技术。我熟悉计算机科学的基础理论，包括计算机体系结构、操作系统、编译原理和密码学等，并能够将这些知识应用于安全研究。在DDoS攻击分析与检测以及符号执行在安全分析中的应用方面，我进行了深入研究，并在国际会议ACNS 2024上发表了论文《DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining》。此外，我申请了“基于符号执行的DDoS攻击漏洞挖掘方法、系统、设备、介质”专利，进一步推动了研究成果的落地。

在行业知识方面，我对DDoS攻击检测与防御技术、自动化漏洞挖掘方法有深入了解，并熟悉行业相关标准，包括NIST网络安全框架、MITRE ATT&CK、CWE（Common Weakness Enumeration）以及CVSS（Common Vulnerability Scoring System）评分机制。我密切关注AI在网络安全中的应用以及联邦学习在安全检测中的前沿发展，并结合符号执行技术进行自动化安全分析。在研究过程中，我积累了丰富的实践经验，熟练使用符号执行工具（如angr、KLEE）和漏洞挖掘工具（如AFL、QEMU），并能根据实际需求优化和改进这些工具。我还结合真实网络环境，对DDoS攻击检测系统的有效性进行了深入测试，并探索提升安全防御能力的方法。

我的研究涉及人工智能、程序分析和计算机网络等交叉领域，能够结合机器学习技术提升安全检测能力，同时具备软件工程思维，能够利用程序分析和自动化测试技术提升安全工具的可扩展性和适用性。在研究过程中，我全程参与了安全漏洞分析与检测系统的开发和测试，具备独立完成安全研究的能力。我能够从攻击者视角分析系统安全问题，并结合符号执行技术进行漏洞挖掘，并在ACNS 2024国际会议上汇报了研究成果，有较强的国际学术交流能力。

2.工程实践的经历(不少于200字)

在实际工程应用和实践方面，我能够综合运用现代研究工具和方法开展安全工程研究，掌握安全工具开发的核心技能，并能结合企业安全需求进行优化。我提出了DDoSMiner工具，结合符号执行和动态分析技术，实现自动化DDoS攻击行为分析与漏洞挖掘，并具备解决复杂工程问题的能力。我注重技术创新，在研究过程中不断优化DDoS攻击检测和防御机制，推动研究成果在实际系统中的应用。我也具备较强的团队协作能力，在学术研究团队中负责系统安全实验，与团队成员协作优化漏洞挖掘方法，推动安全工具的工程化落地。

我始终保持安全工程创新思维，关注国内外前沿安全研究，并结合自身研究方向探索新的安全检测方法。我通过论文发表、专利申请、会议交流和口头报告等方式推动技术成果转化，并在国际会议中与全球安全研究人员交流最新技术趋势，提升跨文化交流与合作能力。通过参与国际会议和学术交流，我不断扩展自身的技术视野，使研究方向更加贴合全球网络安全的发展趋势。

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）

在实际工程实践中，我积极参与了多个科研项目，并综合运用所学知识解决复杂的工程问题。在校期间，我参与了国家重点研发计划项目：面向终端的高隐蔽公害跨域特征分析与无感

化取证方法研究。在专业实践实习期间，我参与了基于符号执行的DDoS攻击模式识别项目。随着互联网技术的发展，网络安全问题日益严峻，其中分布式拒绝服务（DDoS）攻击已成为当前网络安全领域最严重的威胁之一。近年来，DDoS攻击不断演变，虽然已有多种变种，但仍然有大量攻击依赖于协议漏洞或新漏洞挖掘，因此，对现有协议和系统的攻击模式挖掘和漏洞查找至关重要。

在基于符号执行的DDoS攻击特征识别和漏洞挖掘研究项目中，我负责DDoS攻击的内核级特征识别以及基于符号执行的DDoS攻击漏洞挖掘。本项目采用符号执行技术对TCP协议栈的潜在漏洞进行深入分析，并提出了一种自动化的DDoS攻击挖掘方法，能够有效识别和分析能够躲避现有IDS检测的新型DDoS攻击。在技术实现方面，我参与并完成了以下工作：（1）开发了一种攻击调用流图（Attack Call Flow Graph,
ACFG）模型，用于在内核层面刻画基于TCP的DDoS攻击特征。该模型能够从调用层次分析攻击路径，使得攻击行为的分析更加系统化和可视化。（2）采用选择性符号执行技术，对Linux内核中的TCP协议栈进行漏洞挖掘，优化了符号执行的路径约束，提高了漏洞发现的效率。（3）引入Drop
Nodes机制，通过对探索路径和终止点进行约束，提升TCP协议栈代码的覆盖率，并有效减少符号执行的状态爆炸问题。（4）构建了一个可拓展的自动化框架，用于在系统级别表征DDoS攻击的控制流，并分析可能绕过现有IDS和规则集的新型DDoS攻击。我们在多个版本的Linux内核上验证了该系统的有效性和通用性，确保了该方法在不同环境下的适用性。

在整个研究过程中，我承担了现有工作的研究、实验分析与对比、以及原型系统的实现。首先，我通过分析真实DDoS攻击数据，结合协议解析与流量建模，建立了一套适用于DDoS检测的攻击特征库。然后，我基于符号执行技术，优化了漏洞挖掘的探索策略，并设计了动态污点分析方法来辅助漏洞检测，从而提高了攻击路径的覆盖率。最后，我参与了整个自动化漏洞挖掘框架的开发，并通过实验分析和对比测试，验证了该框架的检测能力和适用性。

本研究最终取得了显著成果，不仅完成了项目任务，还发表了一篇国际会议论文，并申请了相关专利。该研究成果能够有效识别和挖掘DDoS攻击模式，并为现有网络安全防御体系提供了有力支持。此外，我的研究方法为企业网络安全检测提供了新的思路，可推广应用于安全审计、入侵检测和协议漏洞挖掘等多个场景。

通过该研究，我不仅积累了符号执行在安全领域的实际应用经验，还培养了系统性思维和工程实践能力，能够从研究方法、技术实现到工程落地完整解决安全领域的复杂问题。未来，我希望能继续深化该方向的研究，为网络安全防护体系贡献更多创新性方案。

（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
DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining	会议论文	2024年03月08日	24th International Conference no Applied Cryptograph y and Network Security	1/7	
基于符号执行的 DDoS 攻击漏洞挖掘方法、系统、设备、介质	发明专利申请	2024年01月18日	申请号：202410073294.4	2/7	

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： 85 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： 91 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：凌冉	

2226008

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）：　　年 3 月 12 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：22260087	姓名：凌茜	性别：女	学院：工程师学院	专业：计算机技术	学制：2.5年
毕业时最低应获：26.0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	新时代中国特色社会主义理论与实践		2.0	89	公共学位课	2022-2023学年春季学期	研究生英语基础技能		1.0	70	公共学位课
2022-2023学年秋季学期	工程技术创新前沿		1.5	90	专业学位课	2022-2023学年夏季学期	物联网信息安全技术与应用基础		2.0	88	专业学位课
2022-2023学年秋冬学期	工程伦理		2.0	95	公共学位课	2022-2023学年春夏学期	研究生英语		2.0	83	公共学位课
2022-2023学年秋冬学期	研究生论文写作指导		1.0	73	专业学位课	2022-2023学年春夏学期	高阶工程认知实践		3.0	90	专业学位课
2022-2023学年冬季学期	物联网操作系统与边缘计算		2.0	89	专业选修课	2022-2023学年夏季学期	自然辩证法概论		1.0	80	公共学位课
2022-2023学年秋冬学期	科技创新案例探讨与实战		2.0	88	专业选修课	2022-2023学年春夏学期	移动互联网智能设备应用设计与实践		3.0	96	专业学位课
2022-2023学年冬季学期	产业技术发展前沿		1.5	82	专业学位课		硕士生读书报告		2.0	通过	
2022-2023学年春季学期	数学建模		2.0	71	专业选修课						

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

DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining

Xi Ling[1], Jiongchi Yu[2], Ziming Zhao[1], Zhihao Zhou[1], Haitao Xu[1], Binbin Chen[3], and Fan Zhang[1,4(✉)]

[1] College of Computer Science and Technology, Zhejiang University, Hangzhou, China
[2] School of Computing and Information Systems, Singapore Management University, Singapore, Singapore
[3] Information Systems Technology and Design, Singapore University of Technology and Design, Singapore, Singapore
[4] Zhengzhou Xinda Institute of Advanced Technology, Zhengzhou, China
fanzhang@zju.edu.cn

Abstract. With the proliferation of Internet development, Distributed Denial of Service (DDoS) attacks are on the rise. As rule-based traffic analysis frameworks and Deep Packet Inspection (DPI) defense measures can effectively thwart many DDoS attacks, attackers keep exploring various attack surfaces and traffic amplification strategies to nullify the defense. In this paper, we propose DDoSMiner, an automated framework for DDoS attack characterization and vulnerability mining. DDoSMiner analyzes system call patterns of the TCP-based DDoS attack family, then generates Attack Call Flow Graph (ACFG) by discerning the differences between DDoS attack traffic and benign traffic. Furthermore, DDoSMiner identifies and extracts drop nodes and pivotal TCP states from the distinctive characteristics of attack traffic, then passes to the symbolic execution framework for exploring variants of the DDoS attack. We collectively analyze six types of TCP-based DDoS attacks, construct the corresponding ACFG, and identify a set of attack traffic variants. The attack traffic variants are evaluated on the widely used Network Intrusion Detection System (NIDS) Snort with three popular rule sets. The result shows that DDoSMiner indeed discovers the new DDoS attack trace, and the corresponding attack traffic can bypass all three defense toolkits.

Keywords: TCP-based DDoS attacks · Attack Call Flow Graph · Symbolic execution

1 Introduction

With the evolution of the Internet, the security issues of the Internet have garnered increasing attention. Among the various threats to networks, Distributed

C. Pöpper and L. Batina (Eds.): ACNS 2024, LNCS 14584, pp. 283–309, 2024.
https://doi.org/10.1007/978-3-031-54773-7_12

经检索“Engineering Village”，下述论文被《Ei Compendex》收录。（检索时间：2024 年 5 月 24 日）。

<RECORD 1>
Accession number:20241215763826
Title:DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining
Authors:Ling, Xi (1); Yu, Jiongchi (2); Zhao, Ziming (1); Zhou, Zhihao (1); Xu, Haitao (1); Chen, Binbin (3); Zhang, Fan (1, 4)
Author affiliation:(1) College of Computer Science and Technology, Zhejiang University, Hangzhou, China; (2) School of Computing and Information Systems, Singapore Management University, Singapore, Singapore; (3) Information Systems Technology and Design, Singapore University of Technology and Design, Singapore, Singapore; (4) Zhengzhou Xinda Institute of Advanced Technology, Zhengzhou, China
Corresponding author:Zhang, Fan(fanzhang@zju.edu.cn)
Source title:Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
Abbreviated source title:Lect. Notes Comput. Sci.
Volume:14584 LNCS
Part number:2 of 3
Issue title:Applied Cryptography and Network Security - 22nd International Conference, ACNS 2024, Proceedings
Issue date:2024
Publication year:2024
Pages:283-309
Language:English
ISSN:03029743
E-ISSN:16113349
ISBN-13:9783031547720
Document type:Conference article (CA)
Conference name:22nd International Conference on Applied Cryptography and Network Security, ACNS 2024
Conference date:March 5, 2024 - March 8, 2024
Conference location:Abu Dhabi, United arab emirates
Conference code:308919
Publisher:Springer Science and Business Media Deutschland GmbH
Number of references:63
Main heading:Denial-of-service attack
Controlled terms:Flow graphs - Graphic methods - Intrusion detection - Model checking - Network security - Transmission control protocol
Uncontrolled terms:Attack call flow graph - Attack traffic - Denialof- service attacks - Distributed denial of service - Flow-graphs - Internet development - Rule based - Symbolic execution - TCP-based distributed denial of service attack - Vulnerabilities minings
Classification code:721.1 Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 902.3 Legal Aspects - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory
DOI:10.1007/978-3-031-54773-7_12
Database:Compendex

注：
1. **以上检索结果来自 CALIS 查收查引系统。**
2. **以上检索结果均得到委托人及被检索作者的确认。**

教育部科技查新工作站（Z09）
检索人（签章）：应湘艺
2024 年 5 月 24 日

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118101242 A
(43)申请公布日 2024.05.28

(21)申请号 202410073294.4

(22)申请日 2024.01.18

(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 郑州信大先进技术研究院

(72)发明人 张帆 凌茜 李振源 许海涛 赵新杰 郭世泽 姚凯强

(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 邱启旺

(51)Int.Cl.
H04L 9/40(2022.01)

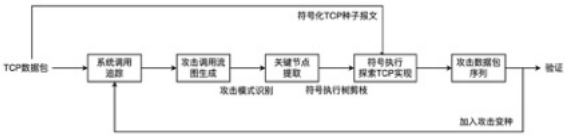
权利要求书2页 说明书7页 附图3页

(54)发明名称

基于符号执行的DDoS攻击漏洞挖掘方法、系统、设备、介质

(57)摘要

本发明公开了一种基于符号执行的DDoS攻击漏洞挖掘方法、系统、设备、介质,所述方法包括:向靶机发送良性数据包和基于TCP的DDoS攻击数据包,从Linux操作系统内核中采集报文运行时TCP协议栈的函数调用链并分析TCP连接状态信息;并据此将函数作为节点,函数间的调用关系作为边,边的权重用于表示在相同流量条件下不同函数之间的依赖程度,生成攻击调用流图,并确定攻击调用流图中的关键节点;配置符号化TCP种子数据包;基于攻击调用流图以构建一个有向生成树;其中,有向生成树的节点对应攻击调用流图中的关键节点;根据符号化TCP种子数据包在有向生成树中所能达到的路径终止点和状态,探索靶机上TCP协议的潜在漏洞,产生候选攻击数据包序列。



CN 118101242 A

国 家 知 识 产 权 局

310013

浙江省杭州市西湖区古墩路 701 号紫金广场 C 座 1506 室 杭州求是专利事务所有限公司

邱启旺(0571-87911726-808)

发文日：

2024 年 01 月 18 日

申请号：202410073294.4　　**发文序号：**2024011801521750

专 利 申 请 受 理 通 知 书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日等信息通知如下：

申请号：2024100732944

申请日：2024 年 01 月 18 日

申请人：浙江大学,郑州信大先进技术研究院

发明人：张帆,凌茜,李振源,许海涛,赵新杰,郭世泽,姚凯强

发明创造名称：基于符号执行的 DDoS 攻击漏洞挖掘方法、系统、设备、介质

经核实，国家知识产权局确认收到文件如下：

权利要求书 1 份 3 页,权利要求项数 ： 10 项

说明书 1 份 8 页

说明书附图 1 份 3 页

说明书摘要 1 份 1 页

专利代理委托书 1 份 3 页

发明专利请求书 1 份 5 页

实质审查请求书 文件份数：1 份

申请方案卷号：邱-241-11-陈

提示：

1.申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。

2.申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。

国家知识产权局 专利申查业务章 1101081359734

审 查 员：自动受理　　审查部门：初审及流程管理部

联系电话：010-62356655

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收

电子申请，应当通过专利业务办理系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

其他佐证材料

- 受邀于 2024 年 3 月 5 - 8 日在阿布扎比纽约大学第 22 届应用密码学和网络安全国际会议(22nd International Conference on Applied Cryptography and Network Security，ACNS 2024）进行口头报告。

جامعة نيويورك ابوظبي
NYU | ABU DHABI

CENTER FOR CYBER SECURITY

January 23, 2024

To Whom It May Concern:

RE: Invitation Letter for Xi Ling Passport Number: EJ2952478 DOB: 08/25/2000

I, the undersigned, Dr. Ozgur Sinanoglu, Director of Center for Cyber Security New York University Abu Dhabi ("NYUAD"), located on Saadiyat Island, Abu Dhabi, United Arab Emirates ("UAE"), hereby certify that **Xi Ling** of Zhejiang University, China is invited to attend the 22nd International Conference on Applied Cryptography and Network Security (ACNS 2024) for presenting a paper on "DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining". The event is scheduled to take place at New York University Abu Dhabi, UAE from March 5-8, 2024.

Sincerely,

Dr. Ozgur Sinanoglu

Ozgur Sinanoglu
Director of Center for Cyber Security
Professor of Electrical and Computer Engineering;
New York University/ Abu Dhabi
Office Tel (UAE): +971 02 628 4388
NYU Abu Dhabi, Saadiyat Campus
P.O. Box 129188
Abu Dhabi, United Arab Emirates