同行专家业内评价意见书编号：20240854234

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： 张子君

学号： 22160008

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

2024年03月30日

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

电子信息计算机技术专业是一个高度综合性的领域，它要求学习者不仅要深入理解数学基础、电路理论、信号与系统等基础理论知识，为后续的专业学习打下坚实的基础，而且需要掌握编程语言与算法、操作系统、数据库系统、计算机网络等专业技术知识，以适应不断变化的技术需求和解决实际问题的能力。此外，随着人工智能和机器学习等领域的快速发展，相关的基础理论和应用技术也成为了该专业学习者必须关注的重要内容。因此，对于电子信息计算机技术专业的学习者而言，不仅要系统地学习和掌握各类基础理论知识，还需要不断地更新自己的技术技能，以保持与时代发展的同步，这样才能在未来的职业生涯中取得成功。

2.工程实践的经历

内核运行时安全是操作系统安全的核心，随着技术的发展，恶意软件也在不断进化，其中Rootkit是一种隐蔽性极高的恶意软件，它能深入操作系统内核，从而控制或者修改操作系统的核心功能。eBPF是一项革命性的技术，它能够在内核中运行自定义的代码，而不需要更改内核源代码或者加载外部模块，因此，eBPF也为内核运行时安全防护提供了新的可能性。在开发eBPF
Rootkit防护技术的过程中，我们面临着多方面的挑战，同时也积累了宝贵的实践经验。以下是我们在这一领域工作时的一些核心经验：
①深入理解eBPF技术：要有效利用eBPF进行安全防护，首先需要对eBPF的工作原理有深刻的理解，包括它的编程模型、核心概念（如BPF Maps、Helper
Functions等）以及如何在内核中安全地执行eBPF程序。
②监控关键内核行为：通过eBPF，我们能够在内核级别监控各种关键行为，比如系统调用、文件系统操作、网络活动等。这使得我们能够及时发现并响应潜在的安全威胁。
③数据收集与分析：eBPF程序能够收集大量的运行时数据，因此开发有效的数据分析策略至关重要。通过分析这些数据，我们能够识别出异常行为模式，从而发现潜在的Rootkit活动。
④性能优化：虽然eBPF程序运行高效，但在内核空间进行大量数据收集和处理仍可能影响系统性能。因此，在开发防护技术时，我们不断地寻找平衡安全与性能的最佳方案，确保安全防护措施不会对系统性能产生负面影响。
总之，开发eBPF
Rootkit防护技术是一项充满挑战的任务，它要求我们不仅要有扎实的技术基础，还需要具备创新思维和持续学习的能力。通过实践，我们不仅提升了自己在内核安全防护方面的技术能力，也为保护操作系统安全作出了贡献。

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）

在当今的网络安全防护领域，操作系统内核级别的安全威胁日益成为关注的焦点。Rootkit作为一种高度隐蔽的恶意软件，能够深入操作系统内核，控制或修改核心功能，给系统安全带来极大挑战。随着eBPF技术的出现和发展，我们有了一种新的防御手段。eBPF可以在内核中运行自定义的代码，而不需要更改内核源代码或加载外部模块，这为内核运行时安全防护提供了新的可能性。以下是我们在开发eBPF

Rootkit防护技术过程中，综合运用所学知识解决复杂工程问题的案例。

（1）问题背景

随着攻击者技术的进步，传统的安全防护手段难以对抗高级的内核级Rootkit攻击。Rootkit能够通过隐藏文件、进程、网络连接等方式，绕过传统的安全检测机制。因此，我们面临的主要挑战是如何在不影响系统性能的前提下，实时监测并防御这些内核级别的威胁。

（2）项目目标

我们的目标是开发一套基于eBPF的Rootkit防护系统，该系统能够：

①实时监控内核级别的关键行为，如系统调用、文件操作和网络活动。

②检测并防止Rootkit的潜在攻击，如未授权的系统调用修改、文件和进程隐藏等。

③确保安全防护措施对系统性能影响最小。

（3）解决方案

我们的解决方案分为三个主要部分：数据收集、数据分析和防御机制。

①数据收集：我们首先利用eBPF技术，通过编写eBPF程序来挂钩（hook）内核中的关键函数，比如sys_enter（系统调用进入点）、文件系统操作接口和网络包处理函数等，实时收集系统运行时的数据。这些数据包括但不限于系统调用的参数、文件操作的细节以及网络数据包的信息。

②数据分析：收集到的数据会被送往用户空间进行进一步的分析。我们开发了一套基于机器学习的分析系统，该系统能够学习正常的系统行为模式，并基于这些学习结果检测异常行为。我们利用已知的Rootkit行为特征训练机器学习模型，以提高检测的准确率和效率。

③防御机制：当检测到潜在的Rootkit活动时，我们的系统会立即采取防御措施。这些措施包括但不限于阻止恶意的系统调用执行、隔离或终止恶意进程、以及实时警告系统管理员等。

（4）技术挑战及解决策略

①性能优化：监控内核行为并实时处理大量数据可能会对系统性能产生影响。为了最小化性能开销，我们对eBPF程序进行了精细的优化，比如减少不必要的数据拷贝、使用高效的数据结构（如BPF
Maps）来存储和访问数据。此外，我们还通过限制监控范围和频率，平衡了监控的深度和性能开销。

②数据分析准确性：提高Rootkit检测的准确性是另一个挑战。我们采用了多种机器学习算法，并结合专家系统来提高检测率。通过不断地训练和优化模型，我们的系统能够有效地区分正常行为和潜在的Rootkit活动。

③防御策略的制定：在检测到潜在威胁时，如何制定有效的防御措施也是一大挑战。我们采取了灵活的策略，根据威胁的严重程度和类型，动态调整防御措施。同时，我们还提供了一个管理界面，允许系统管理员根据实际情况手动调整防御策略。

通过综合运用eBPF技术、机器学习和系统安全知识，我们成功开发了一套高效、灵活的内核运行时安全防护系统。这套系统不仅能够有效地防御Rootkit等内核级别的安全威胁，而且对系统性能的影响极小。在此过程中，我们深刻理解到，面对复杂的安全挑战，需要不断探索和学习新的技术，并且将不同领域的知识和技术进行综合运用，才能有效地保护系统安全。

（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
一种基于行为特征的eBPF Rootkit攻击形式化建模方法	发明专利申请	2023年10月16日	申请号：202311341779.9	2/4	

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： 83 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： 90 分（要求80分及以上）
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：张子君	

22160008

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 6月 1 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：22160008	姓名：张子君	性别：男	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：24.0学分	已获得：25.0学分			入学年月：2021-09	毕业年月：2024-03
学位证书号：1033532024602123			毕业证书号：103351202402600349		授予学位：电子信息硕士

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学年秋季学期	工业互联网系统安全前沿技术		2.0	90	专业学位课	2021-2022学年春季学期	数学建模		2.0	95	专业选修课
2021-2022学年秋季学期	工业互联网安全系统工程		2.0	94	专业学位课	2021-2022学年春季学期	自然辩证法概论		1.0	67	公共学位课
2021-2022学年冬季学期	研究生英语		2.0	83	公共学位课	2021-2022学年夏季学期	工程伦理		2.0	77	公共学位课
2021-2022学年秋冬季学期	中国特色社会主义理论与实践研究		2.0	89	公共学位课	2021-2022学年夏季学期	工业物联网与大数据实践		2.0	81	专业学位课
2021-2022学年秋冬季学期	研究生论文写作指导		1.0	84	专业学位课	2022-2023学年冬季学期	人工智能安全		2.0	91	专业选修课
2021-2022学年秋冬季学期	工程师实践能力训练		4.0	良	专业选修课	2022-2023学年夏季学期	系统安全与风险管理		2.0	86	专业选修课
2021-2022学年冬季学期	研究生英语基础技能		1.0	80	公共学位课						

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：2024-04-02

国 家 知 识 产 权 局

310012

杭州市西湖区天目山路 46 号宁波大厦 1301 室 杭州中成专利事务所有限公司

李亦慈(13646841609)唐银益(0571-88250015)

发文日：

2023 年 10 月 17 日

申请号：202311341779.9　　**发文序号：**2023101701494690

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：2023113417799

申请日：2023 年 10 月 16 日

申请人：浙江大学

发明人：常瑞,张子君,张卓若,申文博

发明创造名称：一种基于行为特征的 eBPF Rootkit 攻击形式化建模方法

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 2 页,权利要求项数 ： 6 项

说明书 1 份 6 页

说明书附图 1 份 1 页

说明书摘要 1 份 1 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：23-212079-00071544

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：蔡薇薇

联系电话：010-62356655

审查部门：初审及流程管理部

200101 2022.10

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。

国 家 知 识 产 权 局

310012

杭州市西湖区天目山路 46 号宁波大厦 1301 室 杭州中成专利事务所有限公司

李亦慈(13646841609) 唐银益(0571-88250015)

发文日：

2024 年 01 月 09 日

申请号或专利号：202311341779.9 **发文序号：**2024010901594380

申请人或专利权人：浙江大学

发明创造名称：一种基于行为特征的 eBPF Rootkit 攻击形式化建模方法

发 明 专 利 申 请 进 入 实 质 审 查 阶 段 通 知 书

上述专利申请，根据申请人提出的实质审查请求，经审查，符合专利法第 35 条及实施细则第 96 条的规定，该专利申请进入实质审查阶段。

提示：

1.根据专利法实施细则第 51 条第 1 款的规定，发明专利申请人自收到本通知书之日起 3 个月内，可以对发明专利申请主动提出修改。

2.申请文件修改格式要求：

对权利要求修改的应当提交相应的权利要求替换项，涉及权利要求引用关系时，则需要将相应权项一起替换补正。如果申请人需要删除部分权项，申请人应该提交整理后连续编号的部分权利要求书。

对说明书修改的应当提交相应的说明书替换段，不得增加和删除段号，仅只能对有修改部分段进行整段替换。如果要增加内容，则只能增加在某一段中；如果需要删除一个整段内容，应该保留该段号，并在此段号后注明：“此段删除”字样。段号以国家知识产权局回传的或公布/授权公告的说明书段号为准。

对说明书附图修改的应当以图为单位提交相应的替换附图。

对说明书摘要文字部分修改的应当提交相应的替换页。对摘要附图修改的应当重新指定。

同时，申请人应当在补正书或意见陈述书中标明修改涉及的权项、段号、图、页。

国家知识产权局 专利审查业务章 1101081359734

审 查 员：自动审查

联系电话：010-62356655

审查部门：初审及流程管理部

210307
2022.10

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。