

中国网络空间安全协会

协函字〔2022〕121号

关于组织开展网络安全学院学生创新资助 计划创新任务申报工作的通知

各一流网络安全学院：

为认真贯彻落实习近平总书记关于坚持网络安全教育技术产业融合发展的重要指示精神，推动形成网络安全人才培养、技术创新、产业发展良性生态，由中央网信办指导，天融信科技集团、奇安信集团、蔚来、蚂蚁集团4家网信企业，10家一流网络安全学院，中国网络空间安全协会、中国互联网发展基金会共同发起的网络安全学院学生创新资助计划已正式启动，现将有关事宜通知如下：

一、申报组织工作

请各院校按照申报流程组织有意愿参与创新资助计划的学生认真填报申请相关材料，并于8月25日前将初审推荐名单和申报资料提交至创新资助计划项目执行办公室（以下简称项目办）。

二、线上宣讲会

为便于学生全面了解创新资助计划，深入理解创新任务选题，有序推进申报工作开展，项目办将于7月统筹协调4家资助企业，以线上会议的形式为10家一流网安院校学生举办多期专场宣讲会，请各院校组织学生有序参与，并于7月11日前报送时间意向。每家院校将组织4场宣讲会，每场

宣讲会预计 2 小时。

三、申报资料提交工作

请各院校提交的申报资料包括：创新任务申请书（推荐院校意见处须由学院院长签字并盖章）、项目申请汇总表。

提交方式：电子版和扫描件发送至项目办邮箱，同时纸质版快递至项目办。

邮件主题和快递请注明“XX 院校资助计划申报资料”

联系人：仇钰娴 18801380104

王 静 13426331591

座机：010-65228906

邮箱：xuanpei@cybersac.cn

地址：北京市西城区车公庄大街 9 号五栋大楼 A2 座 301

附件：

1. 网络安全学院学生创新资助计划申报流程
2. 2022 年度网络安全学院学生创新资助计划创新任务选题清单

电子版压缩文件包：

1. 创新任务书(每项创新任务有一份任务书,共 103 份)
2. 创新任务申请书
3. 项目申请汇总表
4. 资助计划执行流程方案

创新资助计划项目执行办公室
(中国网络空间安全协会秘书处代用章)

2022 年 7 月 5 日

7101010341965

附件 1

网络安全学院学生创新资助计划申报流程

一、报名事项

报名对象：一流网络安全学院建设示范项目高校（不含军队院校）网络安全学院的全日制在读本科生、硕士生、博士生。

报名时间：2022 年 7 月 28 日-8 月 7 日

报名方式：有意申报的学生向项目负责老师领取、填报《任务申请书》并提供相关资料。

相关要求：每位学生每年最多申请一次。项目研究周期为一年，学生毕业前需完成项目。

项目金额：每位学生资助税前 6 万元，学生应在 1 个月内按要求自主完成税款缴纳，即税后 4.8 万，用于创新项目研究。

资助单位：4 家网信企业为出资方，负责提出创新任务，对每位获资助学生资助 5 万元。中国互联网发展基金会对每位获资助学生配套奖励 1 万元。

二、评审阶段和立项结果

1、学院初审和推荐

申报工作结束后，学院组织专家老师进行资料审核和项

目评选，并形成初审推荐名单，和申请资料统一提交至项目办。

2、企业评审和立项结果

资助企业组织立项评审会，项目办协调专家共同参与，每家企业可遴选资助 60 位学生。

立项结果在学院及相关单位内进行公示，由企业评审组负责答疑。

三、项目结题和评优

一流网络安全学院支持并指导学生完成创新项目，创新项目实施半年后，学生可申请结题，由创新资助计划实施工作专班视情集中组织项目结题评审会，并于项目期满前 1 个月完成全部项目结题评审。

项目结题评审后，由项目办确定优秀学生遴选标准和原则，组织专家评审，按照每年资助学生总数的 5% 择优推荐优秀学生。

由中国互联网发展基金会网络安全专项基金向优秀学生拨付 10 万元奖金，项目办向优秀学生及指导教师发放证书。评选结果面向社会公布。

一流网络安全学院对获奖学生在评优、保送研究生等事项上给予重点支持。

附件 2

2022 年度网络安全学院学生创新资助计划 创新任务选题清单

本创新任务选题清单仅限在学院内部向学生公布，请勿社会公开发布。

天融信科技集团、奇安信集团、蔚来、蚂蚁集团 4 家资助企业各自提出创新选题，数量不一，共 103 个选题。每家企业面向 10 家一流网络安全学院共资助 60 位资助对象，4 家企业共计资助 240 位资助对象。

天融信科技集团 20 个创新选题（平均每个题目选择 3 个资助对象）

1. linux 系统异常行为发现与控制方法研究
2. 基于流量特征的网络安全事件检测技术研究与应用
3. 基于正常流量规则的自学习机器学习算法研究
4. 容器环境流量的拓扑展现技术研究
5. 容器的网络流量行为基线研究
6. 基于 eBPF 的容器逃逸验证和检测
7. 针对三层业务架构系统的关联技术研究
8. 创建 android APK 安全加载运行环境研究
9. 基于代码语义的恶意代码同源分析方法研究

10. 基于图像分类技术的恶意代码同源分析方法研究
11. 基于特征工程的恶意代码同源分析方法研究
12. 基于多分类的恶意 Office 文档检测方法研究
13. 基于分类算法的恶意 PDF 检测研究
14. 基于机器学习的流量分类方法研究
15. 基于 NLP 的网络安全信息抽取技术研究
16. 基于图关联的安全实体关系推理研究
17. 数据驱动的安全本体自动化构建方法研究
18. 基于统一网络安全本体 UCO 安全本体的通用安全本体构建技术研究
19. TLS 加密通信流量整形技术研究
20. 面向大规模网络的安全态势评估

奇安信集团 60 个创新选题（平均每个题目选择 1 个资助对象）

21. 协议深度采集与信息泄露研究
22. DNS 扫描流量和扫描 IP 识别
23. 暗网代理识别及通信测量
24. Excel 4.0 宏代码反混淆技术研究
25. 具有参数或数据特征的子域名识别
26. 蜜罐攻击流量分类研究
27. 互联网蜜罐识别与对抗研究
28. SIP 协议模糊测试技术研究

- 29.使用加密通信的恶意代码活动检测模型及平台研究
- 30.Android App 脱壳技术研究
- 31.Android APP SDK 版本识别
- 32.二进制程序（PE/ELF）的高效开源组件识别
- 33.文本文件的类型精确识别方法研究
- 34.基于二进制模糊测试的流程优化算法
- 35.僵尸网络样本养殖与 C2 监控研究
- 36.基于行为基线分析的特权账号失陷检测模型研究
- 37.白盒密码模块
- 38.关系型大数据抽样技术
- 39.基于 AI 技术的数据内容血缘关系分析技术
- 40.基于开源组件已知漏洞，高效精准修复方法的探索
- 41.大数据组件漏洞的热修复方案
- 42.OPENJDK 漏洞挖掘方案
- 43.主流浏览器的隐私模式安全性分析
- 44.网络黑产移动 APP 分析研究
- 45.数据库 SQL 语句数据安全审核引擎
- 46.基于 AI 算法的个人隐私数据关联性分析技术
- 47.开源 Fuzz 工具改进应用与实验
- 48.微信小程序安全检测方法研究
- 49.基于扫描器插件的漏洞扫描干扰
- 50.心跳域名检测

51. 高质量深度伪造内容鉴别算法的设计与研究
52. 安全知识图谱：基于主机日志和溯源图的攻击事件检测研究
53. Android App 漏洞静态检测方法研究
54. EBPf 在云环境下的应用研究
55. 恶意邮件异常检测模型
56. 安全告警误报减低模型
57. 密码安全测评工具的设计与实现
58. 新增域名恶意网站分析研究
59. 高性能结构化数据库表列识别技术
60. 基于流量还原的指纹模拟
61. Elasticsearch DSL 转 SQL 模块
62. 实时更新的安全资产关系图谱
63. Botnet 恶意活动指令实时持续监测技术
64. 安全知识图谱：大规模图数据威胁分析检测溯源方法及可视化图谱呈现研究
65. 容器的防护方案
66. 相似仿冒域名识别
67. 轻量级虚拟化研究
68. 容器云及 DevOps 场景的特权账号管理引擎
69. 基于 AI 技术对传统静态分析工具的检测结果进行二次自动化审计以提升检测精度、降低误报研究

- 70.推荐算法在 SOAR 系统中应用
 - 71.基于云原生架构的应用拓扑发现技术研究
 - 72.虚拟化设备指纹唯一性检测
 - 73.基于流量重放的高级仿真
 - 74.工控协议模拟器
 - 75.FIDO UAF 协议形式化分析研究
 - 76.AI 日志解析器
 - 77.C&C 攻击识别模型
 - 78.web 类资产数据分级自动化标注组件
 - 79.基于网络内生数据发现未知攻击的本地化情报生产与威胁发现研究
 - 80.基于 Sysmon 主机行为日志的无文件攻击检测模型
- 蔚来 25 个创新选题（平均每个题目选择 2-3 个资助对象）**
- 81.软件供应链中的投毒攻击检测方法研究
 - 82.针对新公开漏洞及受影响软件范围的自动化监控方案研究
 - 83.针对蓝牙协议的模糊测试方法研究
 - 84.网络协议模糊测试测试套自动生成方法研究
 - 85.针对 RTOS 的漏洞检测方法研究
 - 86.针对嵌入式系统的漏洞检测方法研究
 - 87.针对系统驱动的自动化测试方法研究

88. 导向性模糊测试优化方案研究
89. 基于固件模拟技术的模糊测试方法研究
90. 针对安卓/iOS 应用权限滥用问题的检测方法研究
91. 程序静态分析中减少漏报/降低误报率技术研究
92. 程序的运行时形式化验证技术研究
93. 白盒加密方案研究
94. 基于网络流量的轻量级 IDS/IPS 方案研究
95. 针对系统动态行为的 IDS/IPS 方案研究

蚂蚁集团 8 个创新选题（平均每个题目选择 7-8 个资助对象）

96. Oceanbase 及开源数据库安全漏洞分析
97. 安全平行切面开源项目研究 - JAVA 高危漏洞感知防御关键切点研究
98. 可信密态计算技术研究
99. 拆分学习攻防
100. 联邦学习 Secure Aggregation 问题
101. 隐私保护算法实现 KMEANS, SVM
102. SGX 环境下的 Rust 语言 sanitizer 工具研发
103. UAST 统一程序安全分析平台研究