北京市技术发明奖提名材料公示

一、项目名称

高对抗背景下的复杂软件系统动态分析关键技术及应用

二、提名意见

“高对抗背景下的复杂软件系统动态分析关键技术及应用”项目由中国科学院软件研究所牵头，该项目针对复杂闭源软件系统漏洞挖掘分析，有组织高隐蔽攻击发现等难题，突破了大规模指令数据流高效分析，闭源软件漏洞分析与评估，有组织攻击检测等难题，发明了海量 CPU 指令序列高效高精度分析、数据流驱动的闭源软件漏洞动态分析、有组织高隐蔽攻击行为检测等关键技术，研制了 AOTA 动态污点分析系统、金刚软件智能分析系统等系统平台，有效支撑了我国软件漏洞防治、有组织攻击检测防御等重大需求。项目成果具有完全自主知识产权，申请并获授权发明专利 27 项，发表论著 31 篇，形成国际 ITU-T 技术标准 1 项。

项目成果已形成了规模化应用，广泛应用于国家网络关口等国家关键信息基础设施，党政军重要部门，以及大型企业集团和国家级网络安全专业机构，近三年新增产值 31.72 亿元。项目成果在重大活动安保和国家重要部门的安保工作中发挥重要作用，为避免重大国家安全损失作出突出贡献，取得的成绩多次获得主管部门的肯定，项目成果取得了显著的经济效益和社会效益。

提名该项目为北京市技术发明奖一等奖。

三、候选人

苏璞睿、王继刚、杨轶、闫佳、黄桦烽、和亮、贾相堃、韩志辉、张卓、张晗、贾子骁、魏诚、温森浩、刘娟、马梦娜。

四、候选单位

中国科学院软件研究所，中兴通讯股份有限公司，奇安信网神信息技术（北京）股份有限公司，国家计算机网络与信息安全管理中心。

五、主要支撑材料目录

序号	知识产权（标准规范）类别	名称	国家（地区）	授权号（标准编号）	授权公布日（标准发布）	权利人（标准规范起草单位）	发明人（标准规范起草人）
1	发明专利权	一种多语义动态污点分析方法	中国	ZL201610122106.8	2018年7月3日	中国科学院软件研究所	和亮，苏璞睿，杨轶，闫佳，黄桦烽
2	发明专利权	一种基于动态特征的自定义堆管理函数的自动识别方法	中国	ZL201711248935.1	2021年10月26日	中国科学院软件研究所	贾相堃，张超，苏璞睿，杨轶，和亮，闫佳
3	发明专利权	一种基于隐式污点传播的漏洞分析方法	中国	ZL201710451044.X	2020年8月11日	中国科学院软件研究所	杨轶，苏璞睿，黄桦烽，和亮
4	发明专利权	一种基于动态污点传播的程序异常分析方法	中国	ZL201710894260.1	2021年4月27日	中国科学院软件研究所	黄桦烽，杨轶，聂楚江，苏璞睿，和亮
5	发明专利权	一种基于虚拟化高效HASH的可配置函数API监测方法	中国	ZL201910276437.0	2020年12月4日	中国科学院软件研究所	黄桦烽，闫佳，杨轶，苏璞睿

6	发明专利权	一种Android平台的复合污点传播追踪方法	中国	ZL201610453185.0	2020年3月13日	中国科学院软件研究所	杨轶，黄桦烽，和亮，闫佳，苏璞睿
7	发明专利权	一种APT检测系统及装置	中国	ZL201611091570.1	2021年5月4日	中国科学院软件研究所	吴建华，王继刚，成黎
8	发明专利权	动态行为分析方法、装置、系统及设备	中国	ZL201610596328.3	2021年1月26日	中国科学院软件研究所	王静，马苏安，王继刚
9	计算机软件著作权	AOTA动态污点分析系统[简称：AOTA]V2.0	中国	2020SR1527580	2020年10月28日	中国科学院软件研究所	苏璞睿，杨轶，黄桦烽、和亮
10	标准	Requirements and guidelines for dynamic malware analysis in a sandbox environment	ITU-T	X.1218	2020年10月29日	中国科学院软件研究所	田甜，王继刚，林兆骥，严寒冰，高胜
11	论文	Towards Efficient Heap Overflow Discovery	USENIX Security Symposium		2017年8月16日	中国科学院软件研究所	贾相堃，张超，苏璞睿，杨轶，黄桦烽，冯登国

12	论文	InstruGuard: Find and Fix Instrumentation Errors for Coverage-based Greybox Fuzzing	IEEE/ACM International Conference on Automated Software Engineering		2021年11月15日	中国科学院软件研究所	刘昱玮，王衍豪，苏璞睿，余媛萍，贾相堃
13	论文	COOPER: Testing the Binding Code of Scripting Languages with Cooperative Mutation	Network and Distributed Systems Security (NDSS) Symposium		2022年4月22日	中国科学院软件研究所	徐鹏，王衍豪，Hong Hu，苏璞睿
14	论文	FREEWILL: Automatically Diagnosing Use-after-free Bugs via Reference Miscounting Detection on Binaries	USENIX Security Symposium		2022年8月10日	中国科学院软件研究所	和亮，Hong Hu，苏璞睿，蔡彦，Zhengkai Liang
15	论文	有限资源条件下的软件漏洞自动挖掘与利用	计算机研究与发展		2019年3月1日	中国科学院软件研究所	黄桦烽，王嘉捷，杨轶，苏璞睿，聂楚江，辛伟