国家科技进步奖提名材料公示

一、项目名称

高级持续性威胁(APT)攻击检测关键技术及应用

二、提名者

中国科学院

三、提名意见

有组织的高级持续性威胁(APT)攻击已对国家安全、社会经济稳定造成严重影响，对传统的网络空间安全防御体系形成了严重威胁。先进的 APT 防御技术产品是欧美各国限制出口的重要技术产品，是我国自主发展的重要技术方向。该项目针对 APT 攻击检测的技术对抗难题，经过十余年技术攻关，构建了一套基于硬件模拟的软件深度分析技术和方法，解决了传统系统安全产品面临的同系统平台技术竞争难题；以此为基础，突破了漏洞利用攻击检测、基于数据流的攻击机理分析、网络攻击追踪溯源等核心技术，研制了金刚软件智能分析系统、高级持续性威胁检测系统、天眼新一代威胁感知系统等系列产品，实现了对 APT 攻击检测、机理分析和追踪溯源等业务的支撑，并形成了规模化产业应用，有效提升了 APT 攻击的检测、分析和处置能力。

项目成果广泛应用于通信、能源、交通、金融、公共服务等国家关键信息基础设施，网信办、工信部、公安、军队等党政军重要部门，以及航天、中船等大型集团，近三年新增产值 11.57 亿元。项目成果还在 APEC 会议、抗战胜利 70 周年纪念等重大活动和重要部门保障工作中发挥重要作用，多次获得主管部门和国家领导人的肯定和嘉奖；项目成果在海莲花、蓝宝菇等重大 APT 攻击事件的发现与处置过程中作出突出贡献，取得了显著的经济效益和社会效益。部分成果获得 2018 年中国通信学会科学技术一等奖和 2017 年北京市科学技术二等奖。

提名该项目为国家科学技术进步奖二等奖。

四、项目简介

该项目属于计算机信息技术领域。

网络空间安全是关乎国家安全、社会稳定、百姓利益的重大战略问题。《国家中长期科学和技术发展规划纲要（2006-2020）》将网络空间安全技术列为重点发展的关键技术方向。高级持续性威胁(APT)攻击以强大的、有组织的技术力量作支撑，

以特定的高价值任务为目标，攻击破坏性强，对抗能力高，是当前网络空间安全的重要威胁。该项目在国家 863 计划、国家自然科学基金等项目的支持下，历经十多年的关键技术研发，形成了一套以基于硬件模拟软件深度分析技术为核心的 APT 攻击检测关键技术和产品体系，完成了面向 APT 攻击的漏洞利用攻击检测等系列关键技术突破，研制了金刚软件智能分析系统等多款产品，有效提升了 APT 攻击的检测、分析和处置能力。主要技术创新包括：

1) 基于硬件模拟的软件深度分析技术。提出了基于硬件模拟的软件动态分析方案，解决了进程运行场景恢复等问题，实现了纯硬件层的数据监控分析和指令级/字节级的软件动态分析能力，改变了传统安全产品依赖于操作系统接口的数据获取方式，提高了分析过程的透明性和技术对抗能力，为 APT 攻击检测技术方案构建和产品研制奠定了方法与技术基础；

2) 基于漏洞利用过程异常的网络攻击检测技术。以指令级/字节级的细粒度动态分析技术优势，提出了基于异常控制流转移的漏洞利用攻击检测技术，解决了类攻击代码识别等问题，有效降低了异常控制流转移识别开销，实现了动态检测中样本行为不完全触发条件下的攻击检测，提高了 APT 攻击的检测能力和检测准确性，研制了金刚软件智能分析系统、天眼新一代威胁感知系统等 APT 攻击检测产品，检测效果优于国际同类方案和国内外同类产品。

3) 基于细粒度数据流分析的网络攻击机理分析技术。提出了细粒度的动态数据流分析方案，实现了全系统重放与录制、指令级/字节级的数据流分析能力，有效解决了数据流分析中的随机性干扰的影响、自修改代码分析难等问题，研制了 TCA 软件动态分析系统，提高了网络攻击机理分析能力。

4) 基于协议逆向的网络攻击追踪与处置技术。突破了基于指令级数据流分析的网络协议逆向等技术，提出了结构化对等僵尸网络的全球测量方案，并应用到了现实活跃僵尸网络的全球测量中，研制了网络流量异常行为分析与溯源系统产品，提升了网络攻击追踪溯源能力。

项目成功研制了金刚软件智能分析系统、高级持续性威胁防御系统、天眼新一代威胁感知系统等APT攻击检测、分析、处置系列相关产品。项目成果广泛应用于通信、能源、交通等国家关键信息基础设施，工信部等31个国家部委，军队、公安等国家安全职能部门，以及百度、海航集团等知名企业。近三年，新增产值11.57亿元，间接经济效益近60亿元。项目成果还在APEC会议、抗战胜利70周年纪念等

重大活动保障工作中发挥重要作用。项目成果在海莲花、蓝宝菇、毒云藤等重大APT攻击事件的发现与处置过程中作出突出贡献。项目成果在国家重要部门和重大活动的网络安全保障工作中的成绩多次获得主管部门和国家领导人的肯定和嘉奖，取得了显著的经济效益和社会效益。项目部分成果获得2018年中国通信学会科技进步一等奖和2017年北京市科学技术二等奖。

五、客观评价

1）重要科技奖励

该项目成果获得 2018 年中国通信学会科学技术一等奖。

该项目成果获得 2017 年北京市科学技术二等奖。

2）国内外相关技术比较

在攻击检测方面，本项目提出的轻量级漏洞利用攻击检测方案 Xede，相比于国际上 kBouncer 等系统，不仅能检测利用成功的攻击，同时还能检测检测失败的利用攻击。在攻击检测能力横向对比中，Xede 检出的攻击样本中，15%的未知攻击样本无法被同时期最新版本的卡巴斯基、小红伞、诺顿等杀毒软件检出。本项目研制的金刚软件智能分析系统在多次同类产品测评中获得第一的成绩，本项目研制的高级威胁检测防御系统被工信部授予“网络安全试点示范项目”,并获得第十八届中国国际高新技术成果交易会“优秀产品奖”,以及首届江苏省“十佳优秀人工智能产品奖”。在由中国信通院发布的《网络安全产业白皮书（2017）》中评价“中兴通讯……重点围绕 APT 攻击防御领域，构建应对未知、隐蔽、持续威胁的下一代安全防护能力”,“中兴推出的未知威胁检测平台，发现海量数据中的可疑痕迹，并对复杂威胁行为做出自动判定”。

在漏洞模式分析方面，本项目提出的堆溢出漏洞主动挖掘构造方法相比于 DIODE、Dowser 等挖掘方案，构建了更精确的堆溢出模型，能够基于良性输入直接构造漏洞触发样本，同时相比于 AFL、Radamsa 等模糊测试方案，同等条件下针对视频播放软件 PotPlayer 进行挖掘测试，该方案发现 2 倍数量的漏洞。本项目提出的多样利用自动生成方案 PolyAEG ,相比于国际上依赖于固定内存区域实施布局，且只能生成一个利用样本的 AEG、Mayhem 等方案，PolyAEG 利用目标软件内存可控代码动态构造攻击链，在地址随机化条件下的漏洞利用生成成功率更高。本项目首次提出堆溢出漏洞可利用性自动评估方案，相比于国际上卡内基梅隆大学提出的 AEG、Mayhem 和微软的!exploit 等动态分析方案，通过堆溢出区域的数据恢复和继续执行，发现更多的利用点，实现更准确的可利用性评估。以此为基础，项目主要完成人杨轶主导完成的漏洞 AI 攻防机器人方案，在 2018 年 DEFCON China 的漏洞攻防大赛中获得 AI 攻防方案第一名。该项目研发的漏洞自动攻防机器人 99 秒内就完成了第一个漏洞的发掘与利用，而人工完成第一个漏洞用时 17 分；

在 2 分 48 秒内，我们研发的机器人完成了四个漏洞的发掘与利用，绝对领先与人工团队。

在攻击机理分析方面，本项目提出的恶意软件相似性分析方案 DepSim，相比于国际上同时期的 BinHunt 等程序结构比较方法和 MiniMal 等系统调用序列比较方法，通过构建行为依赖关系图，有效提升同族恶意软件相似性分析能力。项目提出的恶意软件二进制文件重构方案，相比于国际上 PolyUnpack 等脱壳重构方法，不再依赖于特定的重构模式，能够面向任何压缩二进制文件实现全内存区域的动态可执行文件重构。本项目提出的攻击特征生成方法，相比于国际上 vigilante 等同类方案，显著降低漏报率，且生成特征简洁准确，特征大小在目标程序的 4%以下。本项目提出的恶意软件网络协议逆向分析方法，相比于国际上 Prospex、Polyglot 等方案，能够还原恶意软件的控制指令与程序代码对应关系，且分析效率提高 20%以上。

在僵尸网络全球测量方面，澳大利亚斯威本科技大学的项阳教授在由国际出版社 Springer 出版的《Briefs on Cyber Security Systems and Networks》(“Advanced Monitoring in P2P Botnets”章节）一书中指出“2014 年 Yan 提出的 SPTracker，相比于传统的测量方式，利用节点注入获得了更好的测量结果。”2016 年德国明斯特大学团队在文章——On the Resilience of P2P-based Botnet Graphs(IEEE CNS ）中指出我们成果是“对 P2P 僵尸网络中的扰动做了测量和刻画”方面的代表性成果，“针对其中的超级节点，分析其覆盖网特征”。本项目提出的结构化对等网测量方案，相比于同期广泛采用的 Blizzard 等穷举测量方案，在基本保持同等测量效果的同时，消耗带宽降低 40%以上。

3）技术验收、技术测评与技术鉴定

国家高技术研究发展计划（863 计划）课题“恶意代码机理分析与特征提取技术研究”（20016AA01Z412）验收结论“课题研制的恶意代码机理分析与检测技术，能够对恶意代码实现机理进行细粒度的动态分析，支持动态污点传播等分析方法，可通过关联分析实现未知恶意代码的辅助检测。该课题成果已获得应用，具有良好的应用前景”。

2017 年 8 月 15 日至 9 月 6 日，中国软件测评中心对该项目研制的成果金刚软件智能分析系统进行了技术鉴定测试，经测试该系统在“样本分析过程中虚拟操作系统不用安装辅助插件，分析过程对样本透明，能够分析具备反虚拟化技术的恶意代码”，“能够对漏洞攻击过程进行指令级分析并发现控制流劫持地址，能够对漏洞攻击行为进行字节级的数据追踪并提取样本执行的异常代码。同时对于漏洞利用失败的样本也能够实现攻击检测”，“能够模拟键盘、鼠标等用户操作进行自动交互”，“断网情况下能够模拟 DNS 解析、网页访问、文件下载等典型网络操作”。

2018 年 9 月 11 日，中国通信学会组织鉴定委员会对该项目成果进行了鉴定，以中国科学院院士陆建华院士为主任委员的专家组鉴定认为：该项目“研究成果整体

达到国内领先，国际先进水平，对类攻击代码的识别等技术达到国际领先水平。成果具有广阔的应用前景”。

六、应用情况

高级持续性威胁（APT）攻击从攻击来源和攻击对象来看，主要可分为两大类：一类是以国家情报为背景，来自境外政府机构组织对我国的政府、军事、科技、金融、军工等重要部门和基础设施的攻击；第二类是以经济利益为目标，来自一系列有组织、成规模的黑客团队，针对大型企业、金融等机构的攻击。针对以上应用单位，本项目成果已部署应用到金融、能源、交通等国家关键信息基础设施，军队、公安、政务等国家重要部门及机构，军工集团、大型互联网公司等大型企业，应用单位共计 2000 余家；在 APEC 会议、“一带一路”国际高峰论坛、十九大、抗战胜利 70 周年纪念等国家重大活动保障工作中发挥重要作用，在海莲花、蓝宝菇等 40 余起重大 APT 攻击事件的发现、分析、处置等工作中作出突出贡献，相关成绩获得主管部门的嘉奖与认可，部分重大事件的处理还得到了国家领导人的批示。下面从以下几个方面详细介绍相关应用情况：

1）国家关键信息基础设施

2017 年 6 月 1 日实施的《中华人民共和国网络安全法》明确要求：国家对公共通信和信息服务、能源、交通等重要行业和领域，以及遭到攻击可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，实行重点保护。

本项目目前已经在国家关键信息基础设施的安全保障工作中发挥重要作用。其中，在公共通信和信息服务方面，本项目成果在中国移动、中国联通、中国电信等三大运营商部署，在中国移动等基础网络实施的保障工作中发现多起 APT 攻击事件；在金融方面，项目成果已经在中国工商银行、中国建设银行、中国银行、中国农业银行四大行，民生银行、平安银行等商业银行部署应用，为保障金融信息网络安全作出了突出贡献。在能源方面，项目成果已经在中石油、中石化、国家电网等国家大型能源企业部署；在交通方面，项目成果已在中国铁路总公司，海航集团等交通信息基础设施部署，为保障我国交通信息基础设施的安全发挥重要作用。

2）国家政府部门及重要机构

国家计算机网络与信息安全管理中心利用恶意代码分析系统、高级持续性威胁检测系统、网络流量异常行为分析与溯源系统，持续对 31 个部委和全国 5 万多个重要政府信息系统进行安全监测，降低了我国党政机关面临的主机被控、机密文件被盗取的严峻风险，对相关事件的响应和处理多次得到主管部门的嘉奖。

在产品部署方面，金刚软件智能分析系统、天眼新一代威胁检测系统、高级持续性威胁检测系统等产品也已在工信部等国家部委，电子政务信息外网，北京等地

方政务系统，宜昌、无锡等地方智慧城市平台等部署应用，为政务系统、市政设施安全保障提供了有效支撑。

在网络空间安全治理方面，军队、公安等国家安全职能部门既是网络空间安全的重要保卫者，也是境外组织的重点攻击目标。金刚软件智能分析系统、天眼新一代威胁检测系统等产品在部队、各级公安系统均有广泛应用，为打击境外组织入侵，网络黑产等网络犯罪发挥重要作用。

3）大型企业及专业机构

TCA 软件动态分析系统、金刚软件智能分析系统、天眼新一代威胁感知系统等产品在百度、中船、清华大学教育网等大型企业及机构部署应用，为保护企业数据安全发挥重要作用。

金刚软件智能分析系统、TCA 软件动态分析系统、天眼新一代威胁检测系统在中国信息安全测评中心、国家信息技术安全中心、国家计算机网络与信息安全管理中心、国家计算机病毒应急处理中心等国家级的网络空间安全保障技术支撑单位应用，有效支撑了相关单位的日常业务工作，为保障重要部门、重要基础设施的安全作出突出贡献。

七、主要知识产权和标准规范等目录

序号	知识产权（标准）具体名称	国家（地区）	授权号(标准编号)	授权（标准发布）日期	证书编号(标准批准发布部门)	权利人（标准起草单位）	发明人（标准起草人	发明专利（标准）有效状态
1	一种基于虚拟硬件环境的恶意代码自动分析方法及系统	中国	ZL 2008 1 0117899.X	2012年05月23日	9523 67	中国科学院软件研究所	应凌云 苏璞睿，冯登国	有效专利
2	一种恶意代码 捕获方法	中国	ZL 2011 1 0029135.7	2014年09月03日	1473102	中国科学院软件研究所	杨轶，冯登国，苏璞睿，应凌云	有效专利
3	一种自动化的网络攻击	中国	ZL 200910 090178 .9	2012年11月07日	1075570	中国科学院软	刘豫，杨轶，苏璞	有效专利

	特征生成方法					件研究所	睿	
4	一种恶意代码网络协议解析方法	中国	ZL 2011 10427999.4	2011年12月19日	215230	中国科学院软件研究所	王明华聂眉宁杨轶，苏璞睿，应凌云	有效专利
5	一种基于硬件模拟器的自修改代码识别方法	中国	ZL 2008 1 024110 5.0	2011年8月7日	814094	中国科学院软件研究所	王祥根冯登国司端锋苏璞睿	有效专利
6	一种内存分配 方法及装置	中国	ZL 2010 1 011451 2.2	2010年02月12日	1364571	中兴通讯股份有限公司	王继刚李翌	有效专利
7	用于分析在各主机上执行的命令的分析设备、系统和方法	中国	ZL 2013 1 049270 0.2	2018年11月09日	3143636	北京奇安信科技有限公司	张卓，杨卿，刘小雄，李洪亮	有效专利
8	金刚(KingKong)软件智能分析系统	中国	2017SR366739	2017年07月12日	软著登字第1952023号	中国科学院软件研究所	苏璞睿应凌云、杨轶、聂眉宁、闫佳	其他有效的知识产权
9	Xede: Practical Exploit Early Detection	美国	ISBN:978-3-319-26361-8	2015年11月02日	doi:10.1007/978-3-319-26362-5_10	中国科学院软件研究所	聂眉宁苏璞睿李琦，王志，应凌云，胡金龙，冯登国	其他有效的知识产权
10	Towards Efficient	美国	ISBN:978-1-931971-4	2017年08	989-1006	中国科	贾相堃	其他

	Heap Overflow Discovery		0-9	月14日		学院软件研究所	张超，苏璞睿，核轶，黄构烽，冯登国	有效的知识产权

八、主要完成人情况

苏璞睿，排名第 1，研究员，就职于中国科学院软件研究所，成果完成于中国科学院软件研究所，是本项目的主要设计者和组织者，负责软件深度分析、漏洞利用攻击检测、攻击特征提取等核心技术攻关与 TCA 软件动态分析系统、金刚软件智能分析系统等产品的研制工作。是 6 项核心专利的共同发明人，2 篇代表性论文的共同作者。

严寒冰，排名第 2，教授级高工，就职于国家计算机网络与信息安全管理中心，成果完成于国家计算机网络与信息安全管理中心，主要负责网络攻击检测、恶意软件深度分析、网络攻击追踪溯源等研究与开发工作，负责组织研发了恶意软件深度分析与检测系统，并完成了在国家关键信息基础设施的部署和应用。

王继刚，排名第 3，教授级高工，就职于中兴通讯股份有限公司，成果完成于中兴通讯股份有限公司，研发了高级持续性威胁防御系统等产品，负责 APT 攻击检测关键技术的成果转化和应用推广工作，产品在国家政务系统、通信、金融等行业机构，及智慧城市等基础信息平台应用。

张　卓，排名第 4，高级工程师/副总裁，就职于北京奇安信科技有限公司，成果完成于北京奇安信科技有限公司，主持完成了 360 天眼新一代威胁感知系统等产品的研制工作，是 1 项代表性专利的第一完成人，主要负责天眼等技术成果的应用

推广，完成了技术成果在政务、能源等部门和行业单位的部署应用。

应凌云，排名第 5，高级工程师，就职于北京奇安信科技有限公司，成果完成于中国科学院软件研究所和北京奇安信科技有限公司，负责软件动态分析与漏洞利用攻击检测等核心技术攻关与 TCA 软件动态分析系统等产品的研制工作。是 3 项核心专利的共同发明人，1 篇代表性论文的共同作者。

钟　宏，排名第 6，高级工程师/副总裁，就职于中兴通讯股份有限公司，成果完成于中兴通讯股份有限公司 ,完成了高级持续性威胁检测系统等产品的研发工作，作为项目的主要完成人，负责企业级 APT 攻击防御及恶意软件深度分析的技术总体设计，以及相关产品的研发与组织工作。

杨　轶，排名第 7，副研究员，就职于中国科学院软件研究所，成果完成于中国科学院软件研究所，负责软件动态分析与漏洞利用攻击检测、网络攻击特征提取等核心技术攻关与 TCA 软件动态分析系统等产品的研制工作。是 3 项核心专利的共同发明人，1 篇代表性论文的共同作者。

聂眉宁，排名第 8，高级工程师，就职于北京奇安信科技有限公司，成果完成于中国科学院软件研究所和北京奇安信科技有限公司，负责基于硬件模拟的软件动态分析框架、漏洞利用攻击检测等核心技术攻关与金刚软件智能分析系统等产品的研制工作。是 1 项核心专利的共同发明人，1 篇代表性论文的共同作者。

闫　佳，排名第 9，高级工程师，就职于中国科学院软件研究所，成果完成于中国科学院软件研究所，负责软件协议逆向、僵尸网络监测等核心技术攻关与恶意软件深度分析与检测系统等产品的研制工作。

韩志辉，排名第 10，工程师，就职于国家计算机网络与信息安全管理中心，成果国家计算机网络与信息安全管理中心，主要负责恶意软件深度分析、网络攻击追踪溯源等研究与开发工作，参与研发了恶意软件深度分析与检测系统，并参与了在国家网关基础设施的建设与应用。

九、主要完成单位情况

中国科学院软件研究所，第 1 完成单位，负责面向 APT 攻击检测的流量深度分析与检测项目总体设计、核心技术攻关和部分系统平台的研制和推广应用工作。完成了基于硬件模拟的软件深度分析技术总体设计、基于漏洞利用过程检测的网络攻击检测技术、网络攻击特征提取技术、网络攻击追踪溯源等技术攻关工作，研制了 TCA 软件动态分析系统、Wookon 恶意代码分析系统、金刚软件智能分析系统、恶意软件深度分析与检测系统等系列产品，完成了成果在政府、企业、国家基础设施等单位的应用推广工作。利用项目成果，完成 APEC 会议、抗战胜利 70 周年等重大活动的安全保障工作，累计形成直接经济效益 1000 余万元。

中兴通讯股份有限公司，第二完成单位，负责面向 APT 攻击防御的流量深度分析检测技术成果转化、产品研制、应用推广等工作。负责研发了中兴深度威胁分析平台、中兴高级持续性威胁分析检测系统、中兴网络流量异常行为分析与溯源系统、面向邮件附件恶意软件检测的企业级电子邮箱安全检测系统等产品，产品在政务系统、通信、金融、互联网等行业机构，及智慧城市等基础信息平台得到广泛应用，产生直接经济效益 7 亿元以上。

国家计算机网络与信息安全管理中心，第三完成单位，参与了恶意软件深度分

析与检测集成平台的研发，负责该平台在国家关键信息基础设施的应用工作，负责网络攻击的溯源、追踪与应急处置等工作，获得软件著作权 1 项，负责完成了成果在 30 余个国家部委网络安全保障工作中的应用，发现重大安全事件 1500 多起，负责项目成果在国家各重大活动保障工作中的应用。

北京奇安信科技有限公司，第四完成单位，完成了 APT 攻击检测、APT 攻击溯源等关键技术攻关工作，完成了天眼新一代威胁感知系统等产品研制工作，完成了成果在国家关键信息基础设施、国家政务系统、重点行业等单位的应用，完成了成果在重大活动和重大安全事件处置工作中的应用。形成直接经济效益 4 亿元以上。

十、完成人合作关系说明

完成人苏璞睿，负责项目的总体设计、规划与组织工作。在项目中，完成人苏璞睿、应凌云、杨轶、聂眉宁、闫佳等共同完成了基于硬件模拟的软件动态分析技术、基于指令级执行异常的漏洞利用过程检测技术、网络攻击机理分析技术、恶意软件同源性判定、僵尸网络测量与攻击溯源等技术研究工作。

完成人苏璞睿、应凌云、杨轶、聂眉宁、闫佳等共同完成了 Wookon 恶意代码分析系统、TCA 软件动态分析系统、金刚软件智能分析系统等产品研发。

完成人严寒冰、韩志辉、杨轶、闫佳等共同完成了恶意软件深度分析与检测系统的研发组织工作和在国家基础设施的应用推广工作。

完成人张卓、应凌云、聂眉宁等共同完成了 360 天眼新一代威胁感知系统的研制工作和在国家关键信息基础设施和政务、金融等行业的应用推广工作。

完成人钟宏、王继刚、杨轶、闫佳等共同完成了中兴深度威胁分析平台、中兴

高级可持续性威胁检测系统、中兴网络流量异常行为分析与溯源系统等产品的研制工作。

完成人王继刚、钟宏、苏璞睿等共同完成了高级持续性威胁检测系统在政务、通信、金融等行业的应用推广工作。