一、项目名称：数字内容安全评测与综合防护应用研究

二、主要完成人情况：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **排名** | **姓****名** | **职务** | **职称** | **工作单位** | **完成单位** | **对本项目主要学术和技术创造性贡献** |
| **1** | 房鼎益 | 无 | 教授 | 西北大学 | 西北大学 | 提出用petri网的思想来进行逆向攻击建模，并提出用虚拟化的思想从底层保护代码的安全，并发表多篇论文（附件1-1-1，1-1-4，1-1-5，1-1-8，1-1-10，1-1-12），以第一发明人的身份申请多份专利（附件2-1-2，2-1-3）并已授权。 |
| **2** | 汤战勇 | 无 | 副教授 | 西北大学 | 西北大学 | 在数字产权保护及其水印嵌入和提取机制模块，选用PPCT（Planted Plane Cubic Tree）使系统纠错能力和抗攻击性得到了极大提升；在关键内容和核心算法的高强度、多虚拟机防护机制模块，设计出了一种新的反编译工具。以一作身份发表多篇论文（附件1-1-2，1-1-5，1-1-13，1-1-14）。 |
| **3** | 陈晓江 | 副院长 | 教授 | 西北大学 | 西北大学 | 在数字产品版权保护及其水印嵌入和提取机制模块，提出了一种动态图水印保护方法，通过插入与真水印结构相似的伪水印，增加了攻击者分析的难度，实现了水印信息的隐蔽性；针对防动态攻击的软件保护方法，提出了一种基于反调试的JavaScript代码保护方法。作为一作的身份发表了多篇论文（附件1-1-1，1-1-10）。 |
| **4** | 何路 | 无 | 讲师 | 西北大学 | 西北大学 | 在数字版权保护及其水印嵌入和提取机制模块，利用字符间的空间编码技术，以及使用背景纹理引入噪声来抵抗OCR攻击；提出了一种对超短文本版权保护的方法；提出了一种自然语言水印鲁棒性测试的方法；并以一作的身份发表多篇论文（附件1-1-11，），以第一发明人的身份完成多份专利（附件2-1-1，2-1-4，2-1-5）。 |
| **5** | 张洁 | 无 | 未取得 | 西北大学 | 西北大学 | 在关键内容和核心算法的高强度、多虚拟机防护机制模块，提出一种基于双进程的软件保护系统对Windows系统下的PE文件中的关键二进制代码进行保护，并以第一发明人的身份发表软著（附件2-2-1）。 |
| **6** | 叶贵鑫 | 无 | 未取得 | 西北大学 | 西北大学 | 在基于逆向攻击模型驱动的数字内容安全评测分析机制模块，提出用攻击经验组建起来的原子攻击模型为基础，通过一定的攻击规则，将原子模型构建为最终的攻击模型，并以第一发明人的身份发表软著（附件2-2-2）。 |
| **7** | 龚晓庆 | 无 | 副教授 | 西北大学 | 西北大学 | 在基于逆向攻击模型驱动的数字内容安全评测分析机制模块，提出基于petri网的思想并结合六元组表示网中节点的状态，构建一种有效的软件攻击模型，以合作作者的身份发表论文（附件1-1-5）并以负责人身份完成科技创新支撑计划的“网络安全、控制技术研究与应用——软件保护技术研究与综合防护平台”项目 （附件4-1-6）。 |
| **8** | 陈峰 | 无 | 副研究员 | 西北大学 | 西北大学 | 在数字产品版权保护及其水印嵌入和提取识别机制模块，提出了动态图水印保护方法，除此之外，还参与了多个子课题的研究，并以共同作者的身份发表多篇文章（附件1-1-1，1-1-3，1-1-10）。 |
| **9** | 李振 | 无 | 未取得 | 西安腾惟科技有限公司 | 西安腾惟科技有限公司 | 创新和改进了针对不同的实际应用情况的安全防护技术，并参与完成了“软件综合防护平台”（附件4-1-4）、“基于DRM的数字内容安全防护系统”（附件4-1-3）、“数字内容安全防护平台”（附件4-1-5）等多个项目。 |

**三、完成人合作关系说明：**

完成人房鼎益、汤战勇、陈晓江、何路、龚晓庆、陈峰均为西北大学教师，是西北大学网络与信息安全研究团队的核心成员，已进行长期合作。房鼎益为本项目的第一完成人，是论文《A software protection framework based on thin virtual machine using distorted encryption》（附件1-1-3）等主要作者；汤战勇为第二完成人，在整个项目研发期间，参与了若干子课题的研究和理论分析，是论文《Research on java software protection with the obfuscation in identifier renaming》（附件1-1-2）等主要的作者；陈晓江为第三完成人，是论文《A dynamic graph watermark scheme of tamper resistance》（附件1-1-1）等主要作者，在整个项目的研发期间，参与指导了10名博士和硕士研究生；何路是本项目的第四完成人，在软件水印、文档保护子模块，参与指导了5名硕士研究生，是论文《A new chinese text digital watermarking for copyright protecting word document》（附件1-1-11）的主要作者。龚晓庆为本项目的第七完成人，与第一完成人共同承担了项目《网络安全、控制技术研究与应用——软件保护技术研究与综合防护平台》（附件4-1-6），在本项目中主要负责软件保护技术的指导工作；陈峰是本项目的第八完成人，参与了软件水印等若干子课题，是论文《ADynamic Graph Watermark scheme of Tamper Resistance》(附件1-1-1)的主要作者；第五完成人张洁、第六完成人叶贵鑫均为西北大学在读博士，是西北大学网络与信息安全研究实验室的骨干成员，2014年至今，先后参与了软件保护、攻击评测模块的研究及研发工作，分别为软件著作权《基于双进程的软件保护系统V1.0》（附件2-2-1）、《基于Petri网的软件攻击自动化建模系统V1.0》（附件2-2-2）的主要作者，在该项目中主要承担数字内容具体保护技术的研究、项目的开发工作；第九完成人李振是本项目在西安腾惟科技有限公司的技术负责人，为主负责西北大学成果在所在公司的转化应用与后期的软件维护工作和在产业化过程中的创新研究。

**四、主要完成单位排序及贡献：**

|  |  |  |
| --- | --- | --- |
| **排序** | **单位名称** | **主要贡献** |
| 第一完成单位 | 西北大学 | 西北大学负责项目需求管理，主体技术方案选型，进度管理，资金管理，项目风险管理，项目测试；参与逆向攻击模型建立、透明加解密技术、水印技术、混淆技术、虚拟机技术等关键技术的研究；项目的总体设计，详细设计，代码编码以及文档撰写等。 |
| 第二完成单位 | 西安腾惟科技有限公司 | 西安腾惟科技有限公司负责项目实现机理研究，逆向攻击模型建立、透明加解密技术、水印技术、混淆技术、虚拟机技术等关键技术技术点难点攻关，项目总体设计，详细设计，代码编码，文档撰写；参与主体技术方案选型，项目测试等。 |

**五、完成单位合作关系说明：**

西北大学（以下简称甲方）与西安腾惟科技有限公司（以下简称乙方）分别合作完成了“数字内容保护平台”、“基于DRM的数字内容安全防护平台”等项目，详细介绍如下：

2009年1月，与西安腾惟科技有限公司合作申报了“数字内容安全防护平台”，甲方负责课题的总体实施的申报、组织、协调、进度与质量的监督和检查以及向上级汇报等工作，具体负责项目内容中保护理论的研究、关键技术公关和系统研发工作；乙方配合甲方进行课题申报，具体负责组织、协调系统测试与推广应用工作。项目研究所得的知识产权成果（软件著作权、专利、软件产品）甲乙双方共享，其中甲方享有成果75%的权益，乙方享有成果的25%的权益；甲乙双方均需承担保密责任，不得单独转让本课题的研究成果，否则，所获得的权益按甲方75%、乙方25%享有。

2006年3月，与西安腾惟科技有限公司合作开发“基于DRM的数字内容安全防护平台”，该平台分为三个版本：标准版、专业版和企业版，将最终三款产品推向市场。该项目的起止时间为2006年3月至2009年6月，双方约定，项目合作开发期间，甲方派出技术专家，作为项目技术组组长，乙方派出技术负责人，作为项目技术组副组长， 甲方技术人员负责项目实现机理的研究，关键技术难点公关，项目总体设计，详细设计，代码编写，文档撰写；参与主体技术方案选型，项目测试；乙方技术人员负责项目需求管理，主题技术方案选型，进度管理，资金管理，项目风险管理，项目测试，并参与关键技术研究，项目总体设计，详细设计，代码撰写和文档撰写。项目所需的全部开发经费有甲乙双方解决，乙方应就本项目支付甲方开发经费￥100000.00元。项目研发所得成果归属甲乙双方共有，项目销售所得利润按甲乙3:7的比例分配，其由于现有技术水平和条件下难以克服的技术困难，导致已研发的部分或全部失败所造成的损失，风险责任由甲乙双方按3:7的比例共担。

**六、项目简介：**

互联网时代，电子书、音乐、电影、游戏、软件等数字内容越来越多。随其应用广泛性的增加，软件被恶意逆向、影视产品被盗版、隐私图片和文件被窃取、游戏被破解等安全威胁愈发严重。继“棱镜门”之后，2016年“巴拿马文件泄密事件”引发全球高度关注，再次证明数字内容安全防护水平亟待提升。传统的数字内容安全防护方案侧重于具体防护策略的实现，然而，由于缺少“事前”对数字产品安全性的评测，无法对其脆弱性进行精准定位，导致防护效果应用不佳。针对上述问题，课题组以“精准”防护为目的，利用逆向攻击模型驱动的评测技术，结合透明加解密、信息隐藏，水印嵌入追踪识别、混淆变换等多种防护手段，在保证数字内容防护强度的前提下，引入事前安全性评测手段，进一步提高防护方案的精准性和有效性，降低系统开销并提升防护效果，成果已在国内知名安全公司得到应用，取得良好社会经济效益。

项目《数字内容安全性评测与综合防护技术应用研究》属电子信息类项目，课题组依托于国家科技部中小企业创新基金“基于DRM的数字内容安全防护平台”，国家科技部中小企业创新基金“天威软件服务平台”，陕西省科技厅工业攻关计划项目“数字内容安全防护平台”；陕西省教育厅产业化培育项目“软件综合防护平台”；陕西省教育厅产业化中试项目“基于DRM的数字内容安全防护系统”等项目，取得以下成果：

1. 基于逆向攻击模型驱动的数字内容安全性评测分析方法

为实现“精准”防护，引入基于Petri网的逆向攻击评测手段，通过隐马尔可夫对数字内容的防护强度进行动态预测分析，定位其可能风险点。该项成果已发表论文（附件1-1-5）、并提交软著（附件2-2-2）且已申请专利。最终成果在甘肃海丰、甘肃安信、陕西省信息测评中心应用，主要解决了传统安全评估领域无法解决的软件安全性和可靠性问题，且近三年内取得了2000多万元的经济效益（附件3-2、3-3、3-5）。

1. 基于底层驱动的透明加解密实现多层次、全方位的数字内容完备保护

数字内容的非法复制和传播，会导致重要信息泄露、数字资产被盗窃。课题组利用底层驱动加解密形式，将数据自动加解密过程嵌入操作系统内部，不仅提高数据处理速度，而且加密过程不易被用户进程中止。该项成果已授予专利（附件2-1-2），并实际推广应用。腾惟科技由此开发的“天机”文档保护系统，获得国家保密资质（附件6-1）和公安部销售许可证（附件6-2），部署在涉密院所和政企单位，近三年给腾惟科技带来千万元收入（附件3-8）。

1. 数字产品版权保护及其水印嵌入和提取识别机制

数字内容的非授权篡改会导致最终版权归属的认定存在难度。课题组利用水印技术将水印标识信息隐藏在数字内容中，设计并形成了一套测试方法和系统（附件2-1-1、2-1-4、2-1-5），提高了数字内容版权识别的准确性和识别效率；利用数据流切片的方法，以数据流为特征嵌入软件固有的胎记，对软件进行识别（附件2-1-3）。西安海庄仪器设备以此为基础，在相关的设计图纸、应用方案和机械类SDK开发包中嵌入水印，追回经济损失400多万元（附件3-7）。

1. 关键内容和核心算法的高强度、多虚拟机防护策略

关键数字内容尤其是核心重要软件被恶意逆向攻击，关键代码被获取，使得高知识附加值产品被“山寨”。课题组针对这一问题，利用代码混淆技术和虚拟指令执行技术，重新构造新的运行态系统指令集，且以轻量开销为目标，完美解决上述问题。申请了软件著作权（附件2-2-1，2-2-2），相关技术已申请专利且已授理。

**七、主要论文专著目录：**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 论文专著名称 | 刊名 | 作者 | 影响因子 | 年卷页码 | 发表时间 | 通讯作者 | 第一作者 | 国内作者 | SCI他引次数 | 他引总次数 | 知识产权是否归国内所有 | 对应附件编号 |
| 1 | A dynamic graph watermark scheme of tamper resistance | IAS | Xiaojiang Chen, Dingyi Fang, JingBo Shen , Feng Chen |  | 2009,18(20):3-6 | 2009-08-18 | Dingyi Fang | XiaojiangChen | 陈晓江;房鼎益;沈静波;陈峰 | 0 | 5 | 是 | 1-1-1 |
| 2 | A new chinese text digital watermarking for copyright protecting word document | CMC | Lu He,DingYi Fang |  | 2009,v3:435-439 | 2009-01-06 | 何路 | 何路 | 何路;房鼎益 | 2 | 14 | 是 | 1-1-2 |
| 3 | Research on java software protection with the obfuscation in identifier renaming | ICICIC | Tang Zhangyong,Chen Xiaojiang,2Fang Dingyi,Chen Feng |  | 2009,1067-1071 | 2009-12-07 | 汤战勇 | 汤战勇 | 汤战勇;陈晓江;房鼎益;陈峰 | 0 | 3 | 是 | 1-1-3 |
| 4 | 一种基于代码加密 的防篡改软件水印方案 | 中国科学技术大学学报 | 汤战勇;房鼎益;苏琳 |  | 2011,7(41):599-606 | 2011-07-15 | 房鼎益 | 汤战勇 | 汤战勇;房鼎益;苏琳 | 0 | 3 | 是 | 1-1-4 |
| 5 | 基于精简指令集的软件保护虚拟机技术研究与实现 | 微电子学与计算机 | 汤战勇;王怀军;房鼎益;陈晓江 |  | 2011,28(8):1-3 | 2011-08-15 | 汤战勇 | 汤战勇 | 汤战勇;王怀军;房鼎益;陈晓江 | 0 | 5 | 是 | 1-1-5 |
| 6 | A software protection framework based on thin virtual machine using distorted encryption | NCIS | Fang Dingyi, GaoLi, Tang Zhangyong,Chen Xiaojiang |  | 2011,1:266-271 | 2011-05-14 | 房鼎益 | 房鼎益 | 房鼎益;高丽;汤战勇;陈晓江 | 0 | 2 | 是 | 1-1-6 |
| 7 | A tamper-proof software watermark using code | ISI | Tang Zhangyong,Fang Dingyi |  | 2011,156-160 | 2011-07-09 | 汤战勇 | 汤战勇 | 汤战勇;房鼎益 | 0 | 3 | 是 | 1-1-7 |
| 8 | 代码混淆算法有效性评估 | 软件学报 | 赵玉洁,汤战勇,王妮,房鼎益,顾元祥 |  | 2012,23(3):700-711 | 2012-03-15 | 赵玉洁 | 赵玉洁 | 赵玉洁;汤战勇;王妮;房鼎益;顾元祥 | 0 | 11 | 是 | 1-1-8 |
| 9 | 应用变形引擎实现的软件动态保护方法研究 | 小型微型计算机系统 | 王怀军,房鼎益,汤战勇,辛强伟 |  | 2013,(7):1462-1467 | 2013-07-15 | 王怀军 | 王怀军 | 王怀军;房鼎益;汤战勇;辛强伟 | 0 | 0 | 是 | 1-1-9 |
| 10 | Method to evaluate software protection based on attack modeling | HPCC | Fang Dingyi,Wang Ni,Tang Zhanyong,Chen Feng,Gu Yuanxiang |  | 2013,837-844 | 2013-11-13 | 房鼎益 | 房鼎益 | 房鼎益;王妮;汤战勇;陈峰;顾元祥 | 0 | 1 | 是 | 1-1-10 |
| 11 | Software attack modeling and its application | HPCC | Fang Dingyi,Dong Hao,Lei Yuanxiao,Gong Xiaoqing,Gu Yuanxiang |  | 2013,1152-1158 | 2013-11-13 | 房鼎益 | 房鼎益 | 房鼎益;董浩;雷元晓;龚晓庆;顾元祥 | 0 | 0 | 是 | 1-1-11 |
| 12 | NISLVMP: Improved virtual machine-based software protection | CIS | Wang Huaijun,Fang Dingyi, Li Guanghui,Yin Xiaoyan,Zhang Bo,Gu Yuanxiang |  | 2013,479-483 | 2013-12-14 | 王怀军 | 王怀军 | 王怀军;房鼎益;李光辉;尹晓燕;张博;顾元祥 | 0 | 1 | 是 | 1-1-12 |
| 13 | 白盒环境中防动态攻击的软件保护方法研究 | 电子学报 | 王怀军,房鼎益,董浩,陈晓江,汤战勇 |  | 2014,(3):529-537 | 2014-03-15 | 王怀军 | 王怀军 | 王怀军;房鼎益;董浩;陈晓江;汤战勇 | 0 | 0 | 是 | 1-1-13 |
| 14 | 应用改进哨兵的软件攻击威胁自感知方法 | 小型微型计算机系统 | 赵媛,房鼎益,刘强波,王怀军,张聪 |  | 2014,(7):1483-1490 | 2014-07-15 | 赵媛 | 赵媛 | 赵媛;房鼎益;刘强波;王怀军;张聪 | 0 | 0 | 是 | 1-1-14 |
| 15 | 基于反调试的JavaScript代码保护方法研究 | 四川大学学报 | 陈晓江,董浩,房鼎益,王怀军,张凡 |  | 2015,47(1):27-35 | 2014-09-14 | 董浩 | 陈晓江 | 陈晓江,董浩,房鼎益,王怀军,张凡 | 0 | 0 | 是 | 1-1-15 |
| 16 | 一种具有时间多样性的虚拟机软件保护方法 | 软件学报 | 房鼎益,赵媛,王怀军,顾元祥,许广莲 |  | 2015,26(6):1322-1339 | 2015-06-15 | 房鼎益 | 房鼎益 | 房鼎益;赵媛;王怀军;顾元祥;许广莲 | 0 | 0 | 是 | 1-1-16 |
| 17 | 基于攻击威胁监控的软件保护方法 | 计算机应用 | 汤战勇，李振，张聪，龚晓庆，房鼎益 |  | 2017，37( 1) : 120 － 127 | 2017-01-10 | 汤战勇 | 龚晓庆 | 汤战勇，李振，张聪，龚晓庆，房鼎益 | 0 | 0 | 是 | 1-1-17 |
| 18 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 19 |  |  |  |  |   |  |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |  |  |  |  |  |  |  |

**八、主要知识产权证明目录：**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 知识产权类别 | 知识产权具体名称 | 国家（地区） | 授权号 | 授权日期 | 证书编号 | 权利人 | 发明人 | 专利有效状态 | 对应附件编号 |
| 1 | 发明专利 | 一种基于中文句式模板变换的文本隐藏方法 | 中国 | ZL200910023743.X | 2012-07-04 | 985361 | 西北大学 | 何路 | 有效 | 2-1-1 |
| 2 | 发明专利 | 基于透明加解密的数字内容安全防护平台及其加密方法 | 中国 | ZL200910218880.9 | 2012-07-25 | 1012653 | 西北大学 | 房鼎益 | 有效 | 2-1-2 |
| 3 | 发明专利 | 一种基于数据流的切片的软件识别方法 | 中国 | ZL201110169906.2 | 2013-07-31 | 1244848 | 西北大学 | 房鼎益 | 有效 | 2-1-3 |
| 4 | 发明专利 | 一种中文超短文本的水印嵌入和提取方法 | 中国 | ZL201210148620.0 | 22015-01-07 | 1563247 | 西北大学 | 何路 | 有效 | 2-1-4 |
| 5 | 发明专利 | 自然语言水印鲁棒性测试方法及其系统 | 中国 | ZL201210284799.2 | 2015-09-09 | 1780352 | 西北大学 | 何路 | 有效 | 2-1-5 |
| 6 | 发明专利 | 一种基于代码变形的二进制代码混淆方法 | 中国 | ZL201410018508.4 | 2017-02-15 | 2378466 | 西北大学 | 王怀军，房鼎益 | 有效 | 2-1-6 |
| 7 | 发明专利 | 一种基于语义的二进制代码反混淆方法 | 中国 | ZL201510158163.7 | 2017-10-31 | 2678472 | 西北大学 | 王蕾，汤战勇 | 有效 | 2-1-7 |
| 8 | 计算机软件著作权 | 基于双进程的软件保护系统V1.0 | 中国 | 2014SR217484 | 2014-12-31 | 0886713 | 西北大学 | 张洁 | 有效 | 2-2-1 |
| 9 | 计算机软件著作权 | 基于Petri网的软件攻击自动化建模系统V1.0 | 中国 | 2014SR217487 | 2014-12-31 | 0886716 | 西北大学 | 叶贵鑫 | 有效 | 2-2-2 |
| 10 | 计算机软件著作权 | 软件攻击与评测系统V1.0 | 中国 | 2014SR212337083 | 2014-12-31 | 0886312 | 西北大学 | 汤战勇 | 有效 | 2-2-3 |

**九、客观评价：**

国家科技型中小企业技术创新基金“天威软件保护服务平台”采用控制流平展的源代码混淆技术，增加了攻击者的逆向难度、增强了软件的安全性，目前该项目已验收，且受到验收专家的一致好评（附件4-1-2）；国家科技型中小企业技术创新基金“基于DRM的数字内容安全防护平台”结合内核透明加解密与细粒度插件访问控制满足了企事业单位对电子文档安全保护的需求，在多家企事业单位进行了应用或试用，取得了较好的保护效果，受到了使用单位的好评（附件3-8）；陕西省教育厅产业化中试项目“基于DRM的数字内容安全防护系统” 客服了传统电子文档保护系统扩展性与灵活性差、访问控制粒度粗泛的问题，具有创新性（附件4-1-3）；陕西省教育厅产业化培育项目“软件综合防护平台” 实现了对软件源代码、可执行代码、防核心算法逆向和软件版权等多层次、多方面的保护，设计方案技术先进（附件4-1-4）；陕西省工业攻关项目“数字内容安全防护平台” 采用了构件化软件体系结构、内核透明加解密与细粒度插件访问控制相结合的数字内容安全保护技术、以及在线离线相结合的文档安全控制模型，具有创新性（附件4-1-5）；西安科技创新支撑计划项目“软件保护技术研究与综合防护平台” 可以有效的对抗攻击者的逆向分析，从而确保软件的核心算法等关键信息，保护软件开发者的权益，具有重要的应用价值（附件4-1-6）。

项目开发的数字内容防护SDK在西安中服软件的CServer系列产品中应用，该产品已成功应用到能源、高校、铁路、研究所等行业，已有1000多家企业、50000多个用户在网上使用，访问该网站的用户量达15万次，取得了实际的应用效果（附件3-9）。

项目研发的软件可靠性安全评估工具在甘肃海丰科技应用，对第三方的软件进行安全性和可靠性的评测，同时对评测出的脆弱点进行代码变换和加固服务，除此之外，还为大量的中小企业和公司提供APP的安全可靠性的评测服务，进一步提高了APP的安全性和健壮性，应用效果良好且已成为了该公司近年来安全评测服务的主要来源（附件3-3）。

项目开发的软件攻击评测和二进制代码保护系统在甘肃安信科技应用，通过代码混淆变换，对客户的核心资产进行全方位的保护，利用平台进行专业的可靠性评测，发现问题，并且利用已有的技术解决相关问题，提升服务质量。该服务目前主要应用在政府行业，应用效果良好，且正在配合改造，准备下一步提供基于“云”模式的软件可靠性评测和加固的服务（附件3-2）。

项目研发的软件安全性的评测和防护平台为软件二进制代码的运行安全进行评测，在陕西省网络与信息安全测评中心应用，利用评测的结果针对性的对关键算法和核心代码进行高强度的混淆变换，防止了逆向攻击以及安卓系统中APK的二次打包，系统在长期使用的过程中，稳定性高，获得用户的一致好评（附件3-5）。

项目研发的软件安全检测插件，在北京知道创宇信息技术有限公司应用，快速、高效的实现了软件的漏洞和可靠性的检测，准确定位软件脆弱点，在互联网靶场中应用软件的安全性漏洞检测和可靠性检测，取得了非常好的效果，且该插件在诸多项目中得到了广泛的应用（附件3-1）。

项目开发的文档防护系统，在西安腾惟科技有限公司应用，有效地帮助客户对文档进行权限划分，并对文档以及其他数字内容的流转、二次授权进行了严格的限定，实时记载了用户对文件的使用记录，对于后期的指纹追踪提供了强有力的证据。该系统自身采用代码混淆、虚拟机防护作为软件保护手段，进一步提高了产品的安全性，在军工、教育、科研院所以及制造业等对文档、图纸、软件相对敏感的客户环境中部署使用，应用效果良好（附件3-8）。

项目开发的水印识别、提取和追踪系统，在西安鼎旭电子科技有限公司应用，利用评测的结果，有针对性的嵌入各种文本水印和软件水印，使得视频文件和文案材料能够有效的追踪，且能够在线识别，在线系统整体运行稳定，识别准确度高于同类产品，得到了良好的使用效果（附件3-6）。

项目开发的软件授权管理以高级版本的形式提供，西安海庄机电设备有限公司通过把项目提供的SDK程序包集成到公司的产品中，形成完善的解决方案，应用到客户图纸的权限防护，获得了客户的一致好评（附件3-7）。

**十、知情同意证明：**









**十一、推广应用情况：**

|  |
| --- |
| 1.应用情况 |
| 本项目的基于逆向攻击模型驱动的数字内容安全评测分析机制利用Petri网对软件的攻击过程进行静态描述，通过对攻击执行条件的判断以及执行后影响的预测，结合马尔可夫链定位脆弱点，做到“事前防护”并为后期全方位的数字内容安全打下坚实的基础。该成果最终以提供API插件的方式在甘肃海丰科技、甘肃安信科技使用；以独立评测平台的形式在陕西省信息安全测评中心单位应用，近三年（2013-2015）以服务提供的新增销售额为2607万元，高附加值利润1441万元在国际知名的互联网安全公司北京知道创宇使用，快速、高效的实现了软件的漏洞和可靠性的检测，准确定位软件的脆弱点。本项目的基于透明加解密的数字内容防护机制利用底层驱动加解密的形式，保证了个人终端电子文档的安全，并实现了用户访问企事业电子文档资源的身份认证和访问控制，进而保证了企事业单位电子文档的机密性和完整性，以及用户相互之间文件交换操作的安全性。该成果最终以和西安腾惟科技有限公司共同开发的“天机”文档保护系统上应用，“天机”系统获得国家保密资质和公安销售许可证，并且部署在大量的涉密院所和政企单位。该系统2013-2015年共计部署终端主机数量5.3万套，销售额1219万元，产生利润360万元。本项目的版权保护及其水印嵌入和提取识别机制利用软件水印技术将程序的版权信息和用户信息嵌入到程序中，通过准确的提取保护后的版权信息和身份认证信息，以证明数字产品的所有权，并结合相应的信息隐藏技术在保证程序正常功能的情况下使攻击者难以去除该版权信息和身份认证信息以鉴别非法复制和盗用的数字产品。该成果在西安海庄仪器设备中应用，西安海庄仪器设备通过在相关的设计图纸、应用方案和机械类SDK开发包中嵌入水印来避免知识版权的丢失。近三年产生经济利润318万元。另外，通过在西安鼎旭科技部署相关在线的水印提取和识别机制，解决了以往知识产权争端无法取证的问题。本项目的基于代码混淆和虚拟机的关键内容和核心算法的防护机制在代码混淆技术理论支持的前提下，将其中两类核心算法思想（即基于控制流的混淆算法和基于目标代码的混淆算法）相结合，并结合虚拟指令执行技术，提高了数字内容的抗攻击能力，该成果在国内知名的安全公司得到了应用推广，取得了良好的效果，有效地抑制了逆向破解和盗版情况的发生。该项技术在甘肃海丰科技、安信科技和陕西省信息测评中心的评估加固服务中广泛应用，通过混淆工具对应用软件进行二次加固操作，增强了软件的安全性，实现利润近1000多万元。 另外，该项技术在国际一流的安全公司得到了应用，其所销售的产品通过加固操作后大大降低了破解率，维护了公司的良好形象，为其赢得了广泛的社会声誉。总之，本项目的推广应用，可以为数字内容提供全面的安全保护，有效防止因信息泄密而造成的商业损失和法律责任，最终达到保护国家和企业机密信息以及核心知识产权的目的。对推动电子商务、电子政务和企业信息化，降低应用IT 技术的风险，提高企业核心竞争力，具有重要的意义。 |

|  |
| --- |
| 2.主要应用单位情况表 |
| 序号 | 应用单位名称 | 应用起始时间 | 应用截止时间 | 应用单位联系人 | 联系电话 |
| 1 | 北京知道创宇信息技术有限公司 | 2013-01-01 | 2015.12 | 秋争超 | 400-060-9587/010-57 |
| 2 | 甘肃安信信息安全技术有限公司 | 2013-01-01 | 2015.12 | 赵晓斌 | 0931-8782081827892 |
| 3 | 甘肃海丰信息科技有限公司 | 2013-01-01 | 2015.12 | 李靖 | 0931-8278968 |
| 4 | 陕西省网络与信息安全测评中心 | 2013-01-01 | 2015.12 | 杨向东 | 029-88319550 |
| 5 | 西安鼎旭科技有限公司 | 2013-01-01 | 2015.12 | 吕 东 | 15902924751 |
| 6 | 西安海庄机电设备有限公司 | 2013-01-01 | 2015.12 | 陈 玲 | 18291450489 |
| 7 | 西安腾惟科技有限公司 | 2013-01-01 | 2015.12 | 张琪 | 029-88496263 |
| 8 | 西安中服软件有限公司 | 2013-01-01 | 2015.12 | 匡 园 | 17756404437 |

|  |
| --- |
| 3.近三年经济效益 单位：万元（人民币） |
| 自然年 | 完成单位 | 其他应用单位 |
| 新增销售额 | 新增利润 | 新增销售额 | 新增利润 |
| 2015年 | 256.00 | 74.00 | 1412.00 | 605.00 |
| 2016年 | 439.00 | 132.00 | 1805.00 | 761.00 |
| 2017年 | 524.00 | 154.00 | 2318.00 | 968.00 |
| 累计 | 1219.00 | 360.00 | 5535.00 | 2334.00 |
|  主要经济效益指标的有关说明 |
| 本产品主要有三种盈利方式：软件安全评测和软件加固技术服务、软件销售（成套软件销售和SDK包销售）、相关的技术合作和转让。项目投资总额200多万元，经过三年多的应用，产生经济效益6754万元。产品目前和国内一流的安全公司（Known Sec）进行合作，广泛用于其产品和安全评测的服务，为政府、企事业单位、中小的创业型公司提供了良好的事前评测和加固的解决方案，达到了良好的效果，获得了用户方的肯定。另外，通过与省内最大的安全评测机构—陕西省信息安全测评中心合作，利用软件安全性评测特有的基于攻击模型的先进技术进行安全性评测服务，取得了良好的收益，整体带来300多万元的经济收益。同时，该项技术通过封装SDK的方式与甘肃海丰、安信科技进行合作，三年来，共取得了1800多万元的销售额收入。利用底层透明加解密的技术，西北大学和西安腾惟科技联合，面向军工、科研院所推出“天机”文档保护系统（获公安部销售许可和国家保密资质），在军工行业得到了广泛的使用，重点对军工行业的涉密图纸和文档进行了防护，保护了知识产权。西安海庄科技通过在其客户部署使用数字内容防护的系统，为其装备单位客户的主要设计图纸提供权限管理、内容分发的安全防护方案，累积获利300多万元，为客户关键数字内容产品的知识产权的防护起到了重要作用。通过SDK包嵌入OA系统的方式，西北大学和西安中服软件进行合作，在其产品CServer中嵌入相关的保护套件，利用云服务租用的方式进行销售，三年来，应用广泛，累积销售额上千万，获得了较好的经济效益。 |

|  |
| --- |
| 4.社会效益 |
| 数字内容通常指的是综合了数字化的文本、资料、视听内容等多媒体服务，通过数字化终端或互联网传送、销售或发行，如电子书籍、以MP3文件存在的音乐、新闻、游戏、软件或者在线销售的研究报告等。数字内容产品的生成需要智力劳动，生产成本极高，然而，其复制成本极低，趋于零成本且网络传播高速度的特点导致数字内容产品极易被盗版使用。因此，数字内容的安全防护研究是当前国际上的研究热点，荷兰爱迪德公司是该领域解决方案的领导者，可以让媒体内容安全传输到设备以确保盗版者无法获得，其系列产品条件接收、数字版权管理、运营支撑系统、机顶盒软件解决方案以及软件和数据中心安全产品在国际市场具有广泛占有率。六年来，西北大学网络与信息安全实验室（NISL）通过与其合作，取得了重要成果。本团队所设计的水印跟踪取证、文档加密、软件虚拟执行保护技术得到了该公司的高度评价，NISL作为爱迪德公司全球三个重要的合作实验室，爱迪德给予持续的经费支持，共同促进部分成果在多媒体防护方面进一步转化，申请国际专利，并应用于全球市场。所培养的人才，正在申请在该公司工作。近年来，该团队利用SDK工具包与西安中服OA软件CServe高度集成，提供基于云的解决方案，产品已经有1000多家企业、50000多个用户在网上使用，并在第十六届软博会上获得专家认可，荣获软博会创新奖，为陕西地方经济发展作出了巨大贡献。NISL实验室还积极与本地企业西安腾惟科技进行合作，通过共同申报国家科技部中小企业创新基金，在源头进行创新，通过加入事前预测进一步定位数字内容脆弱点的机制，提供了一个Total Solution的行业领先的技术解决方案，形成有效的数字安全防护产品。其成果已在西安、兰州和北京等多家公司得到合作和转化，并在国内知名安全公司得到广泛推广和使用，对于促进陕西企业信息化、推动企业IT技术应用、保证陕西经济和社会健康发展起到了重要作用。基于先进事前防护的逆向攻击的安全性评测技术、防篡改技术、代码混淆技术、水印技术、虚拟机技术等思想的数字产品的保护系统，能够为企业建立起一个安全、放心的信息共享的平台，提高企业的管理水平，促进企业资源和社会资源合理、科学、高效的利用。这对创建效益型企业、促进地区经济发展具有积极的社会意义。软件产业是无污染的绿色环保产业，不会对自然环境及生态平衡造成影响，同时也直接或间接的促进了社会就业。 |