

## 市场监管科研成果奖公示材料

一、基本信息				
奖项名称	中文	IT 产品信息安全检测认证关键技术研究与应用		
	英文	Key technology research and application for information technology products information security detection and certification		
申报等级	<input checked="" type="checkbox"/> 一等奖 <input type="checkbox"/> 二等奖 <input type="checkbox"/> 三等奖		是否同意调级	<input checked="" type="checkbox"/> 是 <input type="checkbox"/> 否
主要完成人	吴迪, 刘玉岭, 甘杰夫, 霍珊珊, 张俊彦, 刘戡, 李冰, 刘海峰, 刘思蓉, 布宁			
主要完成单位	中国网络安全审查技术与认证中心, 中国科学院软件研究所, 中国电子科技集团公司第十五研究所, 上海市信息安全测评认证中心, 北京中电华大电子设计有限责任公司, 国家信息技术安全研究中心, 北京信息安全测评中心			
推荐单位	中国网络安全审查技术与认证中心			
奖项的主要项目来源	<input checked="" type="checkbox"/> 国家级 <input checked="" type="checkbox"/> 省部级 <input type="checkbox"/> 其他			
具体计划、基金的名称和编号: 1. “十二五”国家科技支撑计划课题“IT 产品信息安全认证关键技术研究”(2012BAK26B01); 2. 国家质检总局科技计划“信息安全认证认可标准体系研究”(2009IK303); 3. 质检公益性行业科研专项“边界信息产品安全评价技术标准研究”(200910119)。				
奖项的主要项目起止时间	起始: 2009年1月1日	完成: 2014年12月31日		
组织验收单位	国家质检总局科技司; 国家质检总局科技司; 国家质检总局科技司			
成果登记号	G2015-819; G2015-817; G2015-818	成果登记时间	2015年9月24日; 2015年9月24日; 2015年9月24日	

## 二、奖项简介

习总书记高度重视网络安全问题，在十九大、中央网信领导小组历次会议等重要会议上指出：要加快构建网络安全保障体系。检测认证作为国家网络安全保障体系的基础性技术支撑，对提升信息技术产品（下简称“IT产品”）安全水平、保障国家网络空间安全具有重要作用。自2008年以来，作为国家唯一信息安全检测认证的支撑单位，项目团队针对IT产品安全检测认证关键技术开展研究，解决了国家信息安全认证制度建立过程中面临的标准规范缺失、技术方法落后、工具平台零散等关键技术问题。

**（一）技术成果：**1) 提出了我国自有的IT产品信息安全检测认证技术体系框架，可以覆盖全部IT产品，**填补了国内空白**，形成了适应新技术、新应用发展的IT产品信息安全检测认证能力；**检测认证技术体系被国际FIDO联盟（由谷歌、微软、英特尔、三星等发起）大力推荐，并与国际顶级信息安全检测认证技术体系等效**；2) 突破了芯片后门指令分析、安全漏洞插装测试、抗侧信道攻击等检测技术，实现了国内首个高安全等级操作系统、数据库、智能卡、智能家居产品的安全检测认证，打破了国外高等级IT产品检测认证技术的封锁，**主要技术指标达到国际先进水平**；3) 发明了面向关键攻击路径的渗透性检测方法，首次构建了融合3000余种攻击渗透能力的知识库，突破了传统合规性检测对漏洞发现和验证能力的局限，将关键路径分析效率从多项式时间复杂度提升到线性时间复杂度；4) 提出了覆盖证书全生命周期的IT产品安全认证方法，突破了IT产品技术和形态快速变化引发的认证有效性不足、时效性偏低的技术瓶颈，**解决了IT领域证后持续监督难和认证风险控制差的技术难题**；5) 研制了我国第一个自主可信的IT产品安全检测认证支撑平台，面向操作系统、智能卡等建立了检测工具集，规范了检测认证程序，提高了检测认证准确性和自动化程度，效率提升近5倍。

**（二）知识产权成果：**制定国家标准16项（发布8项）、行业标准15项（发布8项）、检测技术规范139项和认证实施规则38项；发表SCI/EI检索论文23篇，申请国家专利14项（授权7项），登记软件著作权12项。

**（三）技术成果应用：**1) 为国家信息安全产品认证制度的建立和实施，及建立中的国家网络安全法第23条、35条配套的认证审查制度提供不可或缺的关键技术；2) **支撑了2015至2020年的信息安全“国抽”工作**，为加强IT产品质量监管提供了支撑技术；3) 颁发认证证书2183张，助力20余款产品复用国内检测技术结果获得国外证书，包括国内全部通过国际最高安全等级认证的产品；4) 提升了IT产品进入军队、政府、金融、能源等重要行业部门的安全门槛，应用于60余次国家重大活动安保和关键信息基础设施安全检查中，获得国家主管部门表彰；5) 提升了军队、金融、能源等重要行业的IT产品安全检测服务能力，提高了阿里云、联想、奇安信、麒麟软件等企业的研发测试效率。

产生直接经济效益3.79亿元，间接经济效益数十亿元。

## 一、已授权专利证明目录

序号	类别（代表作/其他）	专利类别	专利名称	授权号	发明人	授权时间	授权国别或组织
1	代表作	发明专利	识别脆弱性利用安全威胁并确定相关攻击路径的方法	ZL201210080975.0	吴迪, 冯登国, 陈恺等	2015.09.09	中国
2	代表作	发明专利	一种识别业务系统中关键攻击路径的方法	ZL 2011 10359347.1	吴迪, 冯登国, 连一峰等	2011.11.14	中国
3	代表作	发明专利	一种网络安全最佳防护策略的选择方法	ZL 2010 10033849.0	刘玉岭, 冯登国, 连一峰等	2012.8.29	中国
4	其他	发明专利	攻击密钥的方法及装置	ZL201310535334.4	谢蒂、王亚伟、王冠华等	2016.11.23	中国
5	其他	发明专利	一种攻击密钥的方法和装置	ZL201410252680.6	王冠华、王亚伟、谢蒂等	2017.03.29	中国
6	其他	发明专利	一种基于多秘密可视密码的多级访问控制方法及系统	ZL 2018 10161921.4	刘思蓉、胡浩、严妍等	2020.11.03	中国
7	其他	发明专利	基于关联分析的风险评估方法和系统	201910172197X	刘玉岭、李枫、连一峰等	2020.10.29	中国
注：已授权专利包括国际专利、国家发明专利、实用新型专利、外观专利等。“专利类别”应填写已授权专利的具体类别。已授权专利的填写不超过 10 项。							

## 二、标准及其他技术规范证明目录

序号	类别（代表作/其他）	标准及其他技术规范类别	名称	编号	发布日期	前三完成人	前三完成单位
1	代表作	国家标准	信息安全技术 网站数据恢复产品技术要求与测试评价方法	GB/T 29766-2013	2013-09-18	甘杰夫、布宁、赵婷	中国信息安全认证中心、公安部计算机信息系统安全产品质量监督检验中心
2	代表作	国家标准	信息安全技术 反垃圾邮件产品技术要求和测试评价方法	GB/T 30282-2013	2013-12-31	布宁、陈清明、甘杰夫	中国信息安全认证中心、上海市信息安全测评认证中心
3	代表作	国家标准	信息安全技术 智能卡安全技术要求 (EAL4+)	GB/T 36950-2018	2018. 12. 28	霍珊珊、张永刚、刘健	住房和城乡建设部 IC 卡应用服务中心、中外建设信息有限责任公司、深圳航信德诚科技有限公司
4	其他	国家标准	信息安全技术 数据备份与恢复产品技术要求与测试评价方法	GB/T 29765-2013	2013-09-18	刘海峰、布宁、侯海波	中国信息安全认证中心、北京信息安全测评中心、清华威视数据安全研究所
5	其他	国家标准	信息安全技术智能卡通用安全检测指南	GB/T 31507-2015	2015-05-15	方进社、宫亚峰、隋忻	国家信息技术安全研究中心、中国电子技术标准化研究院、国民技术股份有限公司
6	其他	国家标准	信息安全技术 工业控制系统安全控制应用指南	GB/T 32919-2016	2016-08-29	李京春、范科峰、李冰	国家信息技术安全研究中心、中国电子技术标准化研究院、中国电监会信息中心
7	其他	国家标准	信息安全技术 网络安全等级保护安全管理中心技术要求	GB/T 36958-2018	2018. 12. 28	霍珊珊、任卫红、刘健	中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、公安部第三研究所、公安部第一研究所
8	其他	行业标准	上网行为管理系统安全评价规范	RB/T 204-2014	2014-08-20	布宁、刘思蓉、陈世翔	中国信息安全认证中心、上海市信息安全测评认证中心、上海安达通信息安全技术股份有限公司
9	其他	行业标准	抗拒绝服务系统安全评价规范	RB/T 205-2014	2014-08-20	布宁、陈世翔、刘思蓉	中国信息安全认证中心、上海市信息安全测评认证中心、安徽中新软件有限公司
10	其他	行业标准	实时数据库管理系统安全评价要求	RB/T 020-2019	2019. 06. 26	兰丹妮、布宁、霍珊珊	中国网络安全审查技术与认证中心、信息产业信息安全测评中心、北京庚顿数据科技有限公司

注：根据《中华人民共和国标准化法》有关规定，标准包括国际标准、国家标准、行业标准、地方标准、团体标准、企业标准。其他技术规程和规范等。“标准及其他技术规范类别”应填写标准或其他技术规范的具体类别。标准及其他技术规范的填写不超过 10 项。

### 三、其他知识产权证明目录

序号	类别 (代表作/其他)	知识产权类别	知识产权具体名称	国家 (地区)	授权编号	授权日期	权利人
1	代表作	计算机软件著作权	IT 产品安全评价基准库系统 V1.0	中国	2017SR321361	2017.6.28	中国科学院软件研究所
2	代表作	计算机软件著作权	智能卡 COS 安全性检测平台[简称: COS STP]V3.4	中国	2015SR018562	2015.01.30	中国电子科技集团公司第十五研究所; 中国信息安全认证中心
3	代表作	计算机软件著作权	IT 产品安全风险智能预警系统 V1.0	中国	2018SR213309	2018.1.1	中国信息安全认证中心
4	其他	计算机软件著作权	Java 卡安全性检测平台[简称: Java Card STP]V1.0	中国	2015SR018559	2015.01.30	中国信息安全认证中心; 中国电子科技集团公司第十五研究所
5	其他	计算机软件著作权	USBKEY 安全性检测平台软件[简称: USBKEY STP]V1.0	中国	2015SR017943	2015.01.30	中国电子科技集团公司第十五研究所
6	其他	计算机软件著作权	工控 Linux 安全监测工具系统 V1.0	中国	2019SR0875294	2019.08.22	中国电子科技集团公司第十五研究所
7	其他	计算机软件著作权	工控产品安全审查指标与用例管理系统 V1.0	中国	2019SR0870854	2019.08.21	中国电子科技集团公司第十五研究所
8	代表作	计算机软件著作权	关键 IT 产品安全性测试管理系统[简称: ITPSTMS]V1.0	中国	2011SR075762	2011.10.21	华北计算技术研究所
9	代表作	计算机软件著作权	随机数质量测试工具软件[简称: 随机数质量测试工具]V1.1	中国	2012SR126501	2012.12.17	华北计算技术研究所
10	其他	计算机软件著作权	安全审计产品测试工具[简称: SAPTT]V1.0	中国	2011SR075877	2011.10.21	华北计算计算书研究所

注：“知识产权类别”包括计算机软件著作权、标准物质、标准样品、仪器设备新产品、补充检验方法（国家相关行政主管部门正式发布）等。“授权编号”视“知识产权类别”而定，以“标准物质”为例，“授权编号”处应填写标准物质编号。其他知识产权的填写不超过 10 项。

#### 四、论文论著证明目录

序号	类别（代表作/其他）	作品类别	作品名称	发表刊物/出版社	发表时间	主要作者
1	代表作	论文	Quantitative Method for Network Security Situation Based on Attack Prediction	Security and Communication Networks	2017.7	Hao Hu, Hongqi Zhang, Yuling Liu
2	代表作	论文	一种基于攻击图的安全威胁识别和分析方法	计算机学报	2012.8	吴迪, 冯登国, 连一峰等
3	代表作	论文	基于能量分析技术的芯片后门指令分析方法	电子学报	2019.3	马向亮、王宏、李冰等
4	其他	论文	基于静态贝叶斯博弈的蠕虫攻防策略绩效评估	软件学报	2012.3	刘玉岭, 冯登国, 吴丽辉等
5	其他	论文	面向漏洞生命周期的安全风险度量方法	软件学报	2018.5	胡浩, 叶润国, 张红旗等
6	其他	论文	Optimal Defense Strategies for DDoS Defender using Bayesian Game Model	ISPEC 2013	2013.5	Liu Yuling, FengDengguo, LianYifeng
7	其他	论文	Design and Implementation of Network Attacks Detection Module	CCT 2015	2015.10	GanJifu, Peng Li, Chen Hang
8	其他	论文	基于重采样的差分频域分析方法研究	计算机学报	2015.4	王喆、刘戡、王飞宇等
9	其他	论文	一种基于 UML 的网络安全体系建模分析方法	计算机研究与发展	2014.7	布宁, 刘玉岭, 连一峰等
10	其他	论文	基于攻击树的安全芯片穿透性测试评估	计算机工程	2014.6	张俊彦, 陈清明

注：论文论著的“作品类别”包括论文、专著、编著、译著等。论文论著的填写不超过 10 篇/部。