

附件 4:

北京市重点实验室三年绩效考评报告 (大纲)

实验室名称: 软件安全工程技术北京市重点实验室

依托单位: 北京理工大学

联系人: 危胜军

联系电话: 010-68947950

手机: 18600025801

电子邮箱: shj_w@163.com

依托单位科技主管部门联系人: 刘占东

联系电话: 010-68918668-204

手机: 13910127798

电子邮箱: liuzd@bit.edu.cn

北京市科学技术委员会

二〇一七年制

报告说明

1. 本报告是为北京市重点实验室（以下简称“重点实验室”）绩效考评而设计。各重点实验室确保所写内容真实、客观、准确。
2. 本报告中的相关数据统计时间为自2014年1月1日起至2016年12月31日。各年份相关数据必须和当年提交的年度报告保持一致，与年度报告相关数据不符均视为无效数据。
3. 在确认本报告编写准确无误后，应在依托单位内部进行公示（不少于5个工作日），并出具公示结果。依托单位应在承诺函的相应位置签字盖章，否则本报告无效。
4. 本报告中不得出现《国家科学技术保密规定》中列举的属于国家科学技术涉密范围的内容。

北京市重点实验室绩效考评承诺函

根据北京市重点实验室绩效考评有关文件要求，依托北京理工大学组建的软件安全技术北京市重点实验室参加本次绩效考评。并承诺如下：

- 1、所提供的报表数据、文字资料及有关附件材料真实、准确、完整；
- 2、对所提供的资料真实性负责；
- 3、不干预绩效考评工作。

实验室主任（签字）：

年 月 日

实验室依托单位（盖章）：

年 月 日

一、重点实验室基本情况统计表

基本信息	实验室名称	软件安全工程技术北京市重点实验室		依托单位		北京理工大学		共建单位	中国航天科技集团第七一〇研究所
	目前实验室主任	胡昌振	职称	教授	手机	13911180740	电子邮箱	chzhoo@bit.edu.cn	
	认定时实验室主任			目前学术委员会主任		何积丰		认定时学术委员会主任	
	主要运行地址	北京市海淀区中关村南大街5号							
	认定时研究方向	安全软件工程技术、软件安全认知技术、软件安全测评技术							
目前研究方向	安全软件工程技术、软件安全认知技术、软件安全测评技术								
		承担科技计划项目	年份	国家科技计划项目（科技部项目）、 国家自然科学基金委员会项目		省部级科技计划项目			
	数量			财政经费（万元）	北京市科委科技计划项目		其他省部级科技计划项目		
				数量	财政经费（万元）	数量	财政经费（万元）	数量	财政经费（万元）
	2014		4	482.0000	1	15.0000	12	3424.0000	
	2015		0	0.0000	1	50.0000	3	1593.0000	
	2016		6	2948.0000	0	0.0000	3	380.0000	
	总计		10	3430.0000	2	65.0000	18	5397.0000	

研究水平与贡献	研究成果水平	发明专利申请(项)	国内	PCT申请	发明专利授权(项)	国内	国际		
			31	0		13	0		
	研究论文(篇)	国内(中文核心)		国外(仅限SCI(SSCI)、EI收录)		著作(部)			
		7		45		3			
	制(修)订技术标准(项)	国际标准	国家标准		行业标准		地方标准		
		0	0		4		0		
	其他	(主要填写等同于发明专利的成果数量,如新药证书、动/植物新品种、临床新批件等) 7							
	获奖(项)	国家级奖项			省部级奖项				行业协会等其他奖项
		特等	一等	二等	特等	一等	二等	三等	
		0	0	0	0	0	0	1	4
技术创新的贡献度	技术合同(项)	11	技术性收入(万元)	890.0000	其中委托单位为在京单位(项)	9	技术性收入(万元)	402.0000	

队伍建设与人才培养	队伍结构情况	认定时专职人员数量	49	现有专职人员数量	63	副高级(含)以上职称数量及所占比例	39 61.9048%	副高级(含)以上职称中40岁(含)以下数量及所占比例	10 25.6410%	博士数量及所占比例	28 44.4444%	
	青年骨干人才培养情况	引进数量	0		千人计划	0		海聚工程	0	其他	0	
		培养数量	148		科技北京领军人才	0		科技新星	0	其他	0	
		博士(人)	13			硕士(人)	120			职称晋升(人/次)	15	
开放交流与运行管理	开放交流	开放课题(项)	14	总金额(万元)	91.0000		访问学者(人次)	4				
		学术委员会召开次数(次)	5		主/承办国际会议(次)	0	在国际会议做特邀报告(人/次)	4	主/承办全国性会议(次)	9		
		仪器设备纳入首都科技条件平台数量(台/套)	0	纳入条件平台仪器设备原值总金额(万元)	0.0000	纳入条件平台仪器设备对外提供服务次数	0	纳入条件平台仪器设备对外提供服务总金额(万元)	0.0000			
		国际科技合作基地(国家级/市级/否)	否			科普基地(是/否)	否					
	依托单位支持	实验室现有科研面积(m ²)	考评期内新增科研面积(m ²)	实验室现有仪器设备数量(台/套)	现有仪器设备原值(万元)	考评期内新增仪器设备数量(台/套)	新增仪器设备原值(万元)	经费投入(万元)	2014年	55.0000	年报提交(次)	3
							2015年	49.0000				

		2500	0	467	5894.000 0	38	464.2800		2016年	58.0000		
--	--	------	---	-----	---------------	----	----------	--	-------	---------	--	--

填表说明：

- 1、国家科技计划项目仅指科技部项目，其他部委级项目均在省部级项目中计数。跨年度项目以立项年度为统计依据，财政经费以任务书中约定的经费为统计依据，不能重复计算。例：某项目2013年立项，财政经费300万，但在2014年下拨。该项目统计时纳入2013年，财政经费300万元。
- 2、PCT为Patent Cooperation Treaty（专利合作协定）的简写，是专利领域的一项国际合作条约，即在一个专利局（受理局）提出的一件专利申请（国际申请），申请人在其申请中（指定）的每一个PCT成员国都有效，从而避免了在几个国家申请专利，在每一个国家都要重复申请和审查。
- 3、研究论文无重点实验室署名的不予统计。
- 4、国家级奖项仅指国家最高科学技术奖、国家自然科学奖、国家技术发明奖、国家科学技术进步奖和国际科学技术合作奖5类。
- 5、技术合同是指由重点实验室专职人员为主完成的技术开发、技术转让、技术服务和技术咨询四类活动，技术性收入是指由上述四类活动产生的总金额。
- 6、研究人员培养数量中博士、硕士指研究方向与实验室方向吻合，且在考评期内毕业的学生数量。
- 7、经费投入指依托单位为促进实验室建设的各项投入。

二、重点实验室在考评期内的运行绩效

（一）发展规划与目标完成

1. 2014年-2016年绩效考评期内规划目标完成情况

软件安全工程技术北京市重点实验室，由北京理工大学和中国航天科技集团公司第七一〇研究所共建，2011年5月通过北京市科学技术委员会正式认定。2014年至2016年三年来，实验室结合自身定位，依据学术委员会制定的中长期发展规划，围绕软件安全核心关键技术的突破，在科学研究、平台建设和人才培养、应用推广等多个方面取得了显著的成果，特别是在解决国防建设重大、关键问题上发挥了突出作用，圆满完成了三年期的规划目标。具体情况如下。

1.1 实验室研发投入及科研条件和配套设施改善

1.1.1 平台建设

（1）3年规划目标

- 推动软件生命周期安全性保障与验证环境的应用服务
- 推动软件安全性测试验证平台的应用服务
- 继续推进软件安全认知知识支撑环境与检测平台建设

（2）完成情况

- 已向多家单位提供软件生命周期安全性保障与验证环境的应用服务。完成
- 已向多家单位提供软件安全性测试验证平台的应用服务。完成
- 针对软件安全认知知识支撑环境与检测平台建设，进行了知识库更新、检测方法改进。完成

（3）投入经费

- 投入各类试验设备购置费1375万元。

1.1.2 能力建设

（1）3年规划目标

- 推动软件安全性检测与诊断系统的推广应用
- 推动嵌入式软件系统安全测试平台的推广应用
- 继续推进软件安全认知知识库系统的研制

（2）3年完成情况

- 已推广应用软件安全性检测与诊断系统。完成

- 已推广应用嵌入式软件系统安全测试平台。完成
- 将主动知识库技术应用于软件安全认知知识库系统的研制。完成

(3) 投入经费

- 投入系统研制费用477万元。

1.1.3 科学研究

(1) 3年规划目标

• 深入开展软件安全理论研究，建设2-3个国内领先、具有国际水平的特色技术方向

• 牵头承担至少2-3项软件安全方面的重大基础研究、或国家基础研究、重大关键技术研究项目

- 争取获得2-3项国家级或省部级科技奖励
- 申请国家发明专利35项左右
- 发表高水平的论文60余篇
- 累计科研经费突破8000-9000万元。

(2) 3年完成情况

- 目前已凝练4个特色技术方向。完成

• 牵头1项国家重点研发计划项目（前沿基础）、承担9项国家重点研发计划及国家自然科学基金项目。完成

- 获得省部级科技奖励1项，行业协会奖励4项。完成
- 授权发明专利14项，申请37项。超额完成
- 共发表论文73篇，其中国外SCI/EI收录论文45篇，国内核心期刊论文7篇。完成

成

- 累计科研经费8892万元，技术合同890.0万元，共计9782万元。超额完成

1.2 队伍建设及人才培养

1.2.1 队伍建设

(1) 3年规划目标

• 进一步凝练队伍组成，优化队伍结构，着力现有青年骨干的培养，加大高水平人才引进，形成一个规模为80人左右、拥有20人左右教授的人才队伍，其中培养或引进1-2名长江学者。

(2) 3年完成情况

• 现有固定工作人员64人，其中教授13人。长江学者的引进正在洽谈中，相应培养也在进行中。基本完成

1.2.2 人才培养

(1) 3年规划目标

- 培养博士和硕士毕业生不少于100人。

(2) 3年完成情况

- 培养博士毕业生13人，硕士毕业生120人，职称晋升15人。完成

1.3 技术推广

(1) 3年规划目标

• 面向北京市和国家信息化建设需求，开展所研究技术的成果推广与应用。在现有推广应用的基础上，进一步拓展推广应用领域。

(2) 3年完成情况

- 已完成技术成果推广应用。

2. 未来三年发展规划

2.1 未来三年发展的总体目标

实验室围绕国家创新驱动发展战略、首都经济社会发展需求及国防建设重大问题，以软件安全核心关键技术研究及其推广应用以及网络空间安全人才培养为目标制订了中长期发展规划。依据发展规划，实验室继续在学术队伍建设、科学研究水平、人才培养质量、知识创新意识、科技开发能力、先进条件保障、自主完善机制和综合竞争实力等方面推进实验室建设，使实验室的研究水平和人才培养提升到更高层次，使实验室平台建设迈向更高水平，力争在2020年，实验室整体达到同领域国际先进水平，进一步为国家网络空间安全技术领域的发展奠定坚实的人才基础、技术基础和物质基础，更好地为国家及北京市信息化建设及国民经济建设和社会发展服务。

2.2 主要工作规划、预期目标与水平

未来3年，实验室将瞄准社会重大需求，以软件安全理论创新和关键技术突破为基础，围绕科学研究、平台建设、能力建设、队伍建设、人才培养和技术推广等6方面继续深入开展工作。

2.2.1 研究与推广

- 科学研究

实验室围绕定位与研究方向，具体开展了软件分析与设计理论，软件安全性量

化与评估，软件安全漏洞定量发现、预测与利用，无人机集群信息接管等4个技术方向的科学研究。在目前已取得的研究成果和已形成的研究能力的基础上，实验室将进一步深入开展软件安全理论的研究，以软件安全理论为指导，进一步推进现有技术研究的发展，使研究成果到达国际先进水平。未来三年，牵头承担至少1项重大基础研究、2-3项国家基础研究、重大关键技术研究项目，产生一批原创性的理论与技术研究成果，争取获得1项国家级科技奖励、1-2项省部级科技奖励，申请有影响的发明专利30项左右，发表高水平的论文50余篇，累计科研经费超过亿元。

- 技术推广

面向北京市和国家信息化建设需求，开展所研究技术的成果推广与应用。面向市场需求，将取得的成果产品化，形成市场销售。目前主要对软件安全测评技术、漏洞预测与发现技术进行了技术推广，未来发展规划中，将在现有推广应用的基础上，进一步拓展推广应用领域。

2.2.2 实验室建设

- 平台建设

在平台建设方面，进一步丰富现有平台，推进现有平台的应用服务；结合所承担的科研任务，建设软件安全性评估与验证、无人机信息管控测试与验证、软件安全漏洞自动化发现与领域等平台。

- 能力建设

深入开展软件安全理论研究，揭示软件安全漏洞形成机理，形成软件安全漏洞发现理论方法和机制，以此为指导进一步提高技术研发能力。同时，继续推进软件安全认知知识库系统的建设，加强软件安全性检测与诊断系统、嵌入式软件系统安全测试平台的推广应用，开展软件安全漏洞发现系统及软件安全漏洞利用系统的产品化。

2.2.3 人才队伍建设

- 队伍建设

目前，实验室团队以项目组的形式进行组织管理，根据不同的研究方向设立不同的项目组，采用组长负责制。每个项目组按照年龄和职称比例配备研究人员，形成合理高效的组织结构。未来的工作中，实验室将进一步加大高水平人才的引进，着力现有青年骨干的培养，优化队伍组成，完善队伍结构，维持一个规模在80人左

右、拥有20人左右教授的人才队伍。

- 人才培养

培养博士和硕士毕业生不少于100人，满足北京市、国防、国家信息化建设以及软件安全技术产业发展对人才的需要。

（二）研究水平与贡献

1. 定位与研究方向情况

3年来，实验室定位在：以软件安全核心关键技术突破为核心，系统推进软件安全创新技术工具与手段的研制及技术推广，重点开展了安全软件工程技术、软件安全认知技术和软件安全测评技术等方向研究。

所开展研究方向及定位，与认定时保持了一致。

2. 研究成果水平与技术创新贡献度

2.1 研究成果水平

2.1.1 承担的科技项目

3年来，承担国家级项目（课题）10项、省部级科技计划项目（课题）20项及各类技术合同11项，累计经费9782万元。

（1）国家级项目（课题）（3年累计经费3430.00万元）

- 网络系统安全度量及指标体系，三年累计经费1342万元，国家重点研发计划
- 人类生殖遗传资源管理服务云平台开发及安全标准体系建设，三年累计经费1

160万元，国家重点研发计划

- 网络空间虚拟资源发现与社会画像，三年累计经费94万元，国家重点研发计划

- 网络XXX仿真研究，三年累计经费80万元，863计划

• 航天嵌入式系统设计一致性验证技术及其应用，三年累计经费365万元，国家自然科学基金

- 软件安全漏洞规模化发现技术，三年累计经费266万元，科技部“砺剑”计划

• 基于拓扑不变量的软件漏洞发现方法与技术，三年累计经费66万元，国家自然科学基金

- 基于时间自动机的实时Web 服务组合研究，三年累计经费25万元，国家自然科学基金

- 基于虚拟化技术的内核模块安全加固研究，三年累计经费20万元，国家自然科学基金

- 基于函数调用关系的软件可靠性研究，三年累计经费12万元，国家自然科学基金

(2) 省部级科技计划项目（课题）（3年累计经费5462.00万元）

- 数据跨域单向通信安全研究，三年累计经费1100万元，工信部

- 国防科技XXX保障工程，三年累计经费800万元，国防基础科研

- XXX软件开发支撑平台关键技术，三年累计经费680万元，国防基础科研

- XXX在线发现技术研究，三年累计经费480万元，国防基础科研

- XXX脆弱性分析与发现技术，三年累计经费355万元，国防基础科研

- XXXX软件安全缺陷发现技术，三年累计经费120万元，国防基础科研重点项目

- XXX安全研究，三年累计经费13万元，国防基础科研

- 面向XXX的软件加扰保护技术，三年累计经费610万元，科工局军贸预研项目

- XXX产品软件安全性评价体系及关键技术研究，三年累计经费380万元，科工

局民用航天项目

- XXX及“1+N”软件工程标准体系制定，三年累计经费160万元，科工局民用航天项目

- 面向XXX安全关键软件的安全性保证评估方法研究”，三年累计经费55万元，国防科技技术基础

- 关于国家安全的“低慢小轻目标飞行器”的发展与管理研究，三年累计经费15万元，科工局科技委

- 工业控制入侵检测系统，三年累计经费160万元，财政部信息安全专项

- 嵌入式系统漏洞扫描系统，三年累计经费160万元，财政部信息安全专项

- 工业应用软件恶意行为监测系统，三年累计经费220万元，财政部信息安全专项

- 复杂XXX仿真试验评估与鉴定技术，三年累计经费75万元，总装预研

- XXX关键软件安全性保证评价技术研究，三年累计经费10万元，总装科技委

- 基于有限自动机的软件行为建模及模型评价方法研究，三年累计经费4万元，高等学校博士学科点专项科研基金

- 基于核度理论的软件安全漏洞关联分析技术研究，三年累计经费50万元，科

技创新基地培育与发展工程

- 语义Web实时服务组合研究及预警服务应用，三年累计经费15万元，北京市青年英才项目

(3) 承担各类技术合同11项，累计经费890.00万元。

2.1.2 对外科技服务的数量和水平

(1) 软件安全测评服务

实验室具有国家认证委的软件安全测评服务资质，3年来，实验室继续为航天型号软件和社会机构提供软件安全测评服务，共为157批次的航天型号软件和36种社会机构的软件提供了安全测评服务。

(2) 安全软件工程服务

实验室组建了安全软件工程评估工作组，设计了安全软件开发流程和规范，研制了安全软件自动化评估工具，3年了，实验室继续为大型型号和工程软件的安全性保障提供技术咨询服务，并制定安全保障方案和安全开发计划。这些型号和工程软件包括：

- 新一代长征系列重型运载火箭关键控制软件研发
- 某重大武器型号关键控制软件研发
- “嫦娥”工程二期软件研发
- 星上数管控制系统软件研发
- “921”工程软件研发

(3) 系统安全漏洞挖掘服务

为保障某单位软件系统的安全性，针对该软件系统进行了安全渗透测试，发现高危等级漏洞3个，严重等级漏洞13个，为该软件的安全性升级提供了较好的技术支持。

2.1.3 发明专利、论文、著作和标准

3年来，实验室获得授权14项，申请国家发明专利37项，发表各类论文73篇，被SCI/EI收录论文45篇，申请软件著作权8项，制订行业标准4项。见附件。

2.1.4 科技奖励

3年来，实验室获得部级技术发明三等奖1项，行业协会二等奖4项，具体情况如下。

- 面向重点型号系统安全关键软件的安全性保证评估方法研究，科技进步三等，国防科工局，赵文波、杨海成、庞涪川、张刚、张伟，2014

- 航天器产品软件安全性评价体系及关键技术研究，中国航天系统科学与工程研究院科技进步奖二等，中国航天系统科学与工程研究院，张伟、詹海潭、经小川，2015

- 嵌入式软件运行时错误检查技术研究及工具开发，中国航天系统科学与工程研究院科技进步奖二等，中国航天系统科学与工程研究院，詹海潭、经小川、张伟、李宁，2015

- 航天器产品软件安全性评价体系及关键技术研究，中国航天系统科学与工程研究院科技进步奖二等，中国航天系统科学与工程研究院，张伟、詹海潭、经小川，2015

- 嵌入式软件运行时错误检查技术研究及工具开发，中国航天系统科学与工程研究院科技进步奖二等，中国航天系统科学与工程研究院，詹海潭、经小川、张伟、李宁，2015

2.2 技术创新的贡献度

2.2.1 所开展研究的重大问题及成果

3年来，实验室围绕自身定位，重点针对以下3个关键问题开展研究工作。

- 软件安全漏洞形成机理
- 软件安全漏洞预测与发现
- 软件恶意代码的在线监测
- 安全软件工程控制

2.2.1.1 突破的关键技术

- 软件安全漏洞形成机理

将软件系统视为一个实施逻辑组织控制的代数系统，软件系统的各个组成要素（如模块、组件、子系统等）抽象为代数构件，软件系统是这些代数构件在拓扑空间中的集成，在拓扑空间中满足构件形配特性要求。在软件系统从设计到实现的各个阶段，如果形配条件不满足，则将形成软件安全漏洞。

- 基于拓扑不变量的软件安全漏洞预测

软件代数结构可以采用微分拓扑结构描述，在拓扑结构中，软件的集成具有时空特性，对时空特性采用微分流行建模，可描述软件系统代数构件的形配和传动关系，基于此可实现软件安全漏洞的定量分析和预测。

- 安全软件分析与设计技术

针对软件设计的框架结构、模块结构以及关键信息结构层面，建立相应的连通图、赋权图以及广义映射图模型，利用连通图的核与核度分析软件的框架结构的安全性、利用赋权图的最小路径分析软件模块结构的安全性、利用广义映射图的可达矩阵分析软件关键信息的安全性，共同完成软件设计阶段的安全性建模和分析任务。

- 软件安全性测试用例的动态组合生成

提出了基于编程语言及安全事件的安全漏洞激发特征提取方法，建立了基于激发特征的软件渗透测试用例组合生成技术，同时根据上次测试用例的测试结果，自动分析漏洞之间的关系，挖掘出可能存在的相关联的漏洞，从而有针对性的调整生成新的测试用例。该关键技术的解决，为进一步构建用于武器装备嵌入式软件的高覆盖和高精度渗透测试用例库和工具库提供技术支持。

- 基于软件开发过程的软件安全性度量

建立了覆盖软件生命周期全过程的安全性度量方法，通过四个阶段的量化指标对嵌入式安全关键软件进行度量，同时将各个阶段的度量结果与安全性等级的合理度相结合，对嵌入式安全关键软件的安全性等级进行评价，实际可操作性强，度量结果客观准确。该方法可以为航天型号软件研制的主要开发阶段进行软件安全性评价提供依据和技术指导。

2.2.1.2 研制完成的技术工具与手段

3年来，实验室完成了如下工具和系统的研制。

- 军工嵌入式软件安全性双向分析软件（BDA）
- C语言源代码故障注入软件（CCFIS）
- 基于多阶变异的软件故障注入工具
- 航天C程序源代码安全漏洞检测工具
- 体系仿真数据处理工具

- 仿真试验效能评估与鉴定工具
- 应用软件管控系统
- 航天C程序源代码运行时错误检查软件

2.2.1.3 建设的试验平台

- 软件生命周期安全性保障与验证环境
- 软件安全性测试验证平台
- 嵌入式系统软件开发平台

2.2.2 对首都经济社会发展的支撑与引领作用

- 对首都社会发展的贡献

随着信息化的普及，软件系统已经成为电力系统、金融系统、交通信息系统等国家基础设施和国防武器系统、军事指挥控制系统的核心组成部件，这些软件系统由于各种原因可能存在安全漏洞或者被事先安置安全漏洞，利用这些漏洞实施网络攻击，将威胁到国家安全，因此软件安全对捍卫我国的国家利益和国家安全具有极其重要的意义。

实验室的成果为软件安全性分析提供了理论方法、自主可控的技术手段和工具，对开发高安全性的软件产品提供了可行可靠途径，对北京市的软件产业发展以及信息化建设的安全保障具有支撑作用。

- 对首都经济发展的贡献

在推进信息化和软件技术服务业发展的国家政策导向下，软件安全是支撑培育新的社会经济增长点的重要内容，同时对于节约社会经济成本，提供信息安全的经济增长良好氛围具有重要意义。

实验室开展的软件安全保证技术研究可以为推动促进首都信息消费增长提供技术保障，加扰保护技术研究为国产软件走上国际化舞台、促进软件产业对外交流合作和外贸额增长，同时有效保护我知识产权探索了一种可行途径。在“软件+应用”已成为当前信息消费主要形态的形势下，提供高安全性的软件技术产品和服务支持是增强民众消费信心，推动软件和信息服务业又好又快发展的支撑力量，同时为北京建设全国科技创新中心的新定位贡献力量。

2.2.3 成果转化与产业化

实验室建立了适用我国安全软件工程实施框架，依据软件生命周期中不同阶段的安全需求，研究并研制面向自主知识产权的软件安全性分析工具集。工具集已成功应用在921工程和嫦娥工程中，用于确保工程中自主研发的应用软件在系统运行过程中的安全性，从而确保整个系统的安全性，取得了良好的效果。

实验室利用多年积累的软件安全工程技术，先后研发了工业控制入侵检测系统、嵌入式系统漏洞扫描系统以及工业应用软件恶意行为监测系统。目前已在航天领域超过10家单位，中国工程物理研究院超过4家单位部署使用该产品，销售额超过2000万元。

实验室自主研发的软件运行时错误检查系统，已被多家航天型号软件开发及测试单位使用，取得了500多万元的经济收益。

实验室研制的“低慢小”目标侦测与处置网络安全保障系统已成功装备了3个团级部队，并在反法西斯战争胜利70周年阅兵式、杭州G20峰会、历次博鳌亚洲论坛等活动中成功应用。

（三）队伍建设与人才培养

1. 实验室主任与学术带头人作用

实验室主任：胡昌振教授

学科带头人：胡昌振教授、王崑声研究员

胡昌振，男，1967年9月生，教授、博士生导师，1996年在北京理工大学获博士学位。现任北京理工大学软件学院副院长，近年来，主持了十多项国家级、省部级信息安全重点科研课题，获得省部级科研奖励7项，以第一作者发表学术SCI/EI收录论文80余篇，获得授权国家发明专利70多项，主持自主研发的各类系统，已在国防科技工业、军队、金融等重点行业销售与应用。

目前的社会兼职有：国防科工委信息安全技术专家组组长，国防科工委网络信息安全应急工作小组副组长，国防基础科研信息与控制专家组成员，中国航天信息化专家组成员、公安部“十二五”国家支撑计划专家组成员，中国电子学会信息安全专家组副组长，北京市公安局信息安全专家委员会委员，中国科学院信息工程研究所战略咨询专家组成员，《北京理工大学学报》常务编委，中国科学院客座研究员、兼职博士生导师，南京航空航天大学 and 北京化工大学兼职教授、兼职博士生导师。

王崑声，1960年出生，研究员，国务院特殊津贴专家，中国航天科技710所所长，主要研究方向为信息安全与信息系统工程。近年来，完成多项国防和军工信息安全科研重点课题的研究工作，完成了设计报告、论文、著作达50余篇。近年来，多次参与或负责航天、国防科技工业、总装等信息系统重大科技战略、规划论证和项目评价等工作，负责组织实施多项重大安全课题和系统工程的研究工作，多项工作得到了同行专家和有关部门的肯定，培养和带领出多名信息安全、系统工程和计算机应用的优秀人才。

目前的社会兼职有：国防科工委基础科研计划军民两用技术专家组组长，国防科工委网络信息安全应急工作小组组长，中国电子学会信息安全专家组副组长，中国系统工程学会第六届理事，中国计算机用户协会仿真机分会第六届理事会副理事长，中国宇航学会第四届计算机应用专业委员会主任委员，航天科研管理研究会第四届理事。

实验室主任和学术带头人，分别作为支撑单位的负责人，为实验室的创建和发展创造了良好的环境，并提供了人、财、物的支持。他们为实验室的发展规划了方向，为中青年骨干的成长创造各种机会，激励青年学者接受挑战，鼓励优秀中青年骨干勇挑重担，在国际和国内软件安全领域崭露头角。

2. 队伍结构与创新团队建设

实验室现有固定工作人员63人，其中科研人员60人，日常管理人员3人。在研究队伍中，教授（研究员）14人，副教授（高工）24人，讲师（工程师）23，助教（助工）2人。50岁以上人员8人，80%以上研究人员具有硕士以上学位，其中具有博士学位的研究人员占40%以上。

从年龄结构看，实验室目前已形成了老中青三代年龄结构合理的研究团队。以老专家为顾问、中青年科学家为学术带头人、青年科学工作者为骨干、研究生为主力军的科研队伍已形成学术气氛浓厚的传统氛围，青年学者老顾问的帮助指导下勇于接受挑战，已开始承担和主持国家重点研发计划专项课题以及国家自然科学基金等项目。

在创新团队的建设过程中，我们着重考虑了以下几个方面。

实验室的研究方向具有世界前沿性，解决问题的方案本身具有极大的创新性。根据研究体系的分解构成以及学科方向的需要，实验室设置了多个不同的项目小组。我们建立了项目小组的共同目标和远景，每个成员制定了三年的工作目标。项目

小组内独立完成该方向的研究任务，小组之间互相协作。首先根据个人自身的特长推荐和任命小组组长，小组组长负责组内研究任务的分解以及一定额度项目经费的支配。项目小组根据学术委员会制定的具体研究目标和任务，制定具体的实施计划。团队的成员之间进行周例会和月度总结交流会议，充分沟通，共同讨论现存的问题以及解决方案。会议能起到三个方面的作用：一是可以沟通存在的问题，制定解决方案；二是可以增强成员之间的互信；三是可以共同学习，相互促进，提高合作意识，强调合作文化。最后实验室根据工作绩效，建立了针对成员的奖励制度。

3. 青年骨干人才培养

(1) 人才引进措施

近5年来，学校层面制定了具体的人员招聘和人才引进计划，实验室结合学校这一人事政策，提供充足的资金和软硬件环境条件，面向海内外招聘和引进人才进入实验室工作。

(2) 人才培养措施

• 启用年轻人担当课题负责人

实验室鼓励年轻人大胆开展工作，启用年轻人担当课题负责人，对他们委以重任，鼓励他们敢于担当，不怕失败，在实际工作中磨练和培养了年轻人。

• 提供资金支持，鼓励年轻人出外访学，进行学术交流

实验室设立了专项资金用于支持年轻老师出国访学，参加国内外高水平交流会议、技术培训课程，为年轻人开阔视野，打开思路创造了有利条件。

3年来，实验室培养了博士生13人，硕士生120人，职称晋升人数到达了15人。

(四) 开放交流与运行管理

1. 学术委员会作用

实验室的学术委员会有成员11人，学术委员会主任由中国科学院院士何积丰教授担任。实验室的学术委员会是实验室的学术咨询、评审机构，对实验室的研究方向、开放基金、重大科研项目、重大设备的引进等实验室建设进行决策，对实验室的学术活动提出建议，推动和促进与国内外的学术交流和科研活动。3年来学术委员会共召开5次会议。

2. 开放交流

实验室的开放交流，主要体现在如下方面。

(1) 建立实验室开放基金

实验室每年设立专项基金对软件安全方向的热点和难点问题立项，面向社会开放，吸引感兴趣研究人员参与研究。3年来已资助项目12项，累计资助经费45万元，参与开放课题两项，经费共计46万。具体课题和资助经费情况见附件。

(2) 建立访问学者制度

实验室建立访问学者制度，提供一定额度的资金定向邀请国内同领域的青年学者到实验室开展研究工作，同时鼓励实验室内部人员出国深造。2014年吸引北京化工大学易军凯教授来实验室访学工作一年，从事软件安全漏洞预测方向的研究；2016年资助实验室危胜军老师在美国天普大学计算机学院访学一年，针对安全软件控制研究内容进行学习交流；2016年资助实验室经小川，李宁两位研究员赴法国国家信息与自动化研究院就嵌入式软件开发过程一致性保证技术的研究重点和难点问题进行交流。

(3) 开展学术交流

3年来，实验室承办国内学术会议9次，实验室人员受邀在国际会议做专题报告4次。详细情况见附件。

(4) 业内技术交流

3年来，实验室定期与业内研究人员开展技术交流和研讨，促进相互了解和学习，具体情况如下。

- 与航天五院502所在北京共同召开技术交流会，重点针对嵌入式软件运行时错误检查技术及工具研制进行讨论，达成主要共识：1) 双方在模型检测和抽象解释两个技术点开展合作与联合开发；2) 双方互相推广对方的技术和软件工具；3) 双方在各层次加强技术合作，双方将合作在航天五院开展该工具的应用示范工作。

- 与航天八院806所一起召开讲座及交流会议，针对“软件安全性分析与验证技术体系”进行研讨，介绍了我国“CE-3”号探测器质量保证的成功经验，显示了软件及软件工程化工作对于航天的重要作用。

- 与中科院软件所开展技术交流与讨论，软件所专家认为软件安全性双向分析系统(BDA)将FMEA和FTA技术有效结合，自上而下和自下而上将软件安全性问题进行综合分析，具有较强的工程实践性。

- 与北京大学信息科学技术学院进行交流，探讨软件安全漏洞产生的深层次原因。
- 与美国Fortify公司技术人员进行交流，探讨软件安全漏洞检测工具的原理、实现以及目前存在的主要问题等。

(5) 仪器设备使用与共享

实验室根据科研需求，不断完善科研环境、丰富科研平台，3年来，实验室继续投入专项经费购置设备和研制试验平台。结合国防科技特色学科“信息安全与保密工程”建设投资（650万元），丰富与完善了实验室环境，在2013年基础上完善和新建设了如下平台：

- 软件安全渗透测试平台（完善）
- 软件安全可靠性评估系统（完善）
- 工业应用软件恶意行为监测系统（新建）
- 嵌入式系统漏洞检测系统（新建）
- 工业控制入侵检测系统（新建）

实验室的研究条件，除了用于科研与对外服务外，重要仪器设备也对外开放与共享。北京理工大学软件学院大学生创新创业基地近年来取得了许多优秀的成绩，在信息安全竞赛中获得多项国内国际奖项，重点实验室为其中的许多项目提供实验环境与学习研究平台，并安排指导教师指导学生。

3. 协同创新

- 与国内相关研究单位紧密合作

目前，已与物联网安全北京市重点实验室建立了广泛的合作关系，两实验室除合作申请课题外，也组织了共性关键技术的共同攻关，胡昌振教授还担任了物联网安全北京市重点实验室的学术委员会委员。同时，与中国电子科学研究院、中国航天科工706所、中国航天科技502所、中国电子信息安全研究院、中科院信工所、北京大学等建立了合作关系。

- 参与产业技术创新联盟

由中国电子信息安全研究院发起，中国电子学会成立了信息安全专家组，专家组实质为信息安全产业创新联盟，实验室是该联盟的主要参与单位，重点实验室学术带头人王崑声研究员和实验室主任胡昌振教授均为中国电子学会信息安全专家组的副组长。

4. 运行管理与机制创新

- 独立运行

实验室作为两家共建单位的一个独立单位，在经费核算、内部管理和仪器设备使用上具有相对独立权。为实验室建设，北京理工大学提供了1000平米、中国航天科技710所提供了1500平米的科研用房，在两家依托单位，这些科研用房相对集中。

- 制度实施

为保障实验室的有序、高效运行，实验室制定专门的激励措施、规章制度和考核评价制度。为保证这些制度的有效实施，配备了3名专门的日常管理人员，负责运行保障、监督管理和评估考核。目前，实验室运行状况良好。

- 激励机制

采用项目负责制，将经费和责任明确到人，项目负责人具有经费使用权限。考核过程中，依据月计划和年度计划实施任务考核，奖功罚过。激励机制使得实验室人员具有高度的工作热情和成就感。

5. 依托单位支持

两家依托单位针对实验室发展，制定了专门的政策措施，对实验室进行了宏观管理。在人才管理、引进及后勤保障上给予了极大的支持。

为支持实验室建设，两家依托单位均制定了专门的反哺政策，即允许按照适当的比例，把技术推广费用于实验室设备购置及实验工具开发。

为实验室的日常运行，3年来，北京理工大学提供了专门经费83万元（其中14年为30万元、15年19万元、16年34万元），中国航天科技710所提供了专门经费79多万元（其中14年为25万元、15年30万元、16年24万元）。这些经费以研究基金的形式下拨到实验室，以支持实验室科学研究和人才培养。

三、重点实验室自评表

评价内容		自评分
发展规划与目标完成 (10分)	2014年-2016年绩效考评期内规划目标完成情况	9
	未来三年发展规划	
研究水平与贡献 (45分)	定位与研究方向情况	45
	研究成果水平	
	技术创新的贡献度	
队伍建设与人才培养 (25分)	实验室主任与学术带头人作用	24
	队伍结构与创新团队建设	
	青年骨干人才培养	
开放交流与运行管理 (20分)	学术委员会作用	20
	开放交流	
	协同创新	
	运行管理与机制创新	
	依托单位支持	
总评		98

四、依托单位内部公示情况

依托单位（盖章）： 年 月 日

五、学术委员会意见

学术委员会主任（签字）（盖章）：

年 月 日

六、依托单位意见

依托单位（盖章）：

年 月 日

七、附件目录

序号	附件名称
1	研究成果情况明细表
2	队伍建设情况明细表
3	学术委员会召开情况表
4	开放交流情况明细表
5	绩效报告公示照片

附件1、研究成果情况明细表

1、科技计划项目

①承担国家科技计划项目（仅限科技部项目）、国家自然科学基金委员会项目（课题）

序号	项目（课题）名称	主持人	年度	财政经费（万元）	项目类型	项目类别
1	网络系统安全度量及指标体系	胡昌振	2016	1342.0	国家重点研发计划	A
2	人类生殖遗传资源管理服务云平台开发及安全标准体系建设	闫怀志	2016	1160.0	国家重点研发计划	A
3	网络空间虚拟资源发现与社会画像	薛静锋	2016	94.0	国家重点研发计划	B
4	网络XXX仿真研究	胡昌振	2014	80.0	863计划	B
5	软件安全漏洞规模化发现技术	胡昌振	2016	266.0	科技部“砺剑”计划	A
6	基于拓扑不变量的软件漏洞发现方法与技术	单纯	2016	66.0	国家自然科学基金	A
7	基于时间自动机的实时Web服务组合研究	胡晶晶	2014	25.0	国家自然科学基金	A
8	基于虚拟化技术的内核模块安全加固研究	田东海	2016	20.0	国家自然科学基金	A
	航天嵌入式系统设					

9	计一致性验证技术及其应用	詹乃军	2014	365.0000	国家自然科学基金	B
10	基于函数调用关系的软件可靠性研究	彭图	2014	12.0	国家自然科学基金	A

备注：

- (1) 项目类型指：863计划、973计划、国家科技重大专项、国家自然科学基金等。
- (2) 项目类别有A、B两类，A是指重点实验室牵头主持的课题，B是指重点实验室参与的课题。
- (3) 如承担国家科技计划项目子课题，可填写子课题名称，任务书约定的财政经费，类别为A。
- (4) 跨年度项目以立项年度为统计依据，财政经费以任务书中约定的经费为统计依据，不包括依托单位配套经费。例：某项目2013年立项，财政经费300万，但在2014年下拨。该项目统计时纳入2013年，财政经费300万元。

②承担省部级科技计划项目（课题）

(1)北京市科委科技计划项目项目

序号	项目（课题）名称	主持人	年度	财政经费（万元）	项目类型	项目类别
1	基于核度理论的软件安全漏洞关联分析技术研究	马锐	2015	50.0	科技创新基地培育与发展工程	A
2	语义Web实时服务组合研究及预警服务应用	胡晶晶	2014	15.0	北京市青年英才项目	A

(2) 其它省部级科技计划项目

序号	项目（课题）名称	主持人	年度	财政经费（万元）	项目类型	项目类别
1	数据跨域单向通信安全研究	胡昌振	2015	1100.0	工信部	A
2	国防科技XXX保障工程	孙建伟	2014	800.0	国防基础科研	B
3	XXX软件开发支撑平台关键技术	张刚	2014	680.0	国防基础科研	A
4	XXX在线发现技术研究	胡昌振	2015	480.0	国防基础科研	A
5	XXX脆弱性分析与发现技术	经小川	2016	355.0	国防基础科研	A
6	XXXX软件安全缺陷发现技术	薛静锋	2014	120.0	国防基础科研计划重点项目	B
7	XXX安全研究	闫怀志	2015	13.0	国防基础科研	B
8	工业应用软件恶意行为监测系统	经小川	2014	220.0	财政部信息安全专项	A
9	工业控制入侵检测系统	经小川	2014	160.0	财政部信息安全专项	A
10	嵌入式系统漏洞扫描系统	经小川	2014	160.0	财政部信息安全专项	A
11	面向XXX的软件加扰保护技术	张刚	2014	610.0	科工局军贸预研项目	A
12	XXX产品软件安全性评价体系及关键技	经小川	2014	380.0000	国防科工局民用航	A

	术研究				天项目	
13	航天“1+N”软件工程标准体系制定	经小川	2014	160.0000	航天标准化	A
14	面向XXX安全关键软件的安全性保证评估方法研究”	经小川	2014	55.0	国防科工局技术基础项目	A
15	关于国家安全的“低慢小轻目标飞行器”的发展与管理研究	经小川	2016	15.0	国防科工局科技委	A
16	复杂XXX仿真试验评估与鉴定技术	张刚	2014	75.0	总装预研	A
17	XXX关键软件安全性保证评价技术研究	经小川	2016	10.0000	总装技术基础	A
18	基于有限自动机的软件行为建模及模型评价方法研究	薛静锋	2014	4.0	高等学校博士学科点专项科研基金	A

备注:

- (1) 项目类型指: 教育部创新团队发展计划、北京市科技计划项目等。
- (2) 项目类别有A、B两类, A是指重点实验室牵头主持的课题, B是指重点实验室参与的课题。
- (3) 如承担省部级项目子课题, 可填写子课题名称, 任务书约定的财政经费, 类别为A。
- (4) 跨年度项目以立项年度为统计依据, 财政经费以任务书中约定的经费为统计依据, 不包括依托单位配套经费。例: 某项目2014年立项, 财政经费300万, 但在2015年下拨。该项目统计时纳入2014年, 财政经费300万元。

2、研究论文（无重点实验室署名的不予填写）、专著

①研究论文（无重点实验室署名的不予填写）

序号	论文题目	作者	发表年度	刊物名称	国内/国际	SCI影响因子
1	An Improved WiFi Indoor Positioning Algorithm by Weighted Fusion	Ma Rui, Guo Qiang, Hu Changzhen, Xue Jingfeng	2015	Sensors	国际	2.7
2	Test Data Generation for Stateful Network Protocol Fuzzing Using a Rule-Based State Machine	Ma Rui, Wang Daguang, Hu Changzhen, Ji Wendong, Xue Jingfeng	2016	Tsinghua Science and Technology	国内	1.3
3	Proactive service selection based on acquaintance model and LS-SVM	Hu Jingjing, Chen Xiaolei, Zhang Changyou	2016	Neurocomputing	国际	3.3
4	A GPU-based multi-resolution approach to iterative reconstruction algorithms in x-ray 3D dual spectral computed tomography	Jingjing Hu, Xing Zhao, Huitao Zhang	2016	Neurocomputing	国际	3.3
5	A Comprehensive Web Service Selection Algorithm on Just-in-Time Scheduling	Jingjing Hu, Xiaolei Chen, Yinyin Cao, Liehuang Zhu	2016	Journal of Internet Technology	国际	1.9

6	Web Service Composition Automation based on Timed Automata	Hu Jingjing, Zhu Wei, Zhao Xing, Zhu Dongfeng	2014	Applied Mathematics & Information Sciences	国际	1.2
7	Real-Time Service Composition Algorithm based on Semantic Web	Hu Jingjing, Ma Siying, Zhao Xing, Cao Yinyin	2014	Applied Mathematics & Information Sciences	国际	1.2
8	An Improved ID-Based Group Key Agreement Protocol	Hu Kangwen, Xue Jingfeng, Hu Changzhen, Ma Rui, Li Zhiqiang	2014	Tsinghua Science and Technology	国内	1.1
9	A Concurrent Security Monitoring Method for Virtualization Environments	Tian Donghai; Jia Xiaoqi*; Chen Junhua; Hu Changzhen	2016	China Communications	国内	0.9
10	A Practical Online Approach to Protecting Kernel Heap Buffers in Kernel Modules	Donghai Tian*; Xiaoqi Jia; Junhua Chen; Changzhen Hu; Jingfeng Xue	2016	China Communications	国内	0.9

备注：只需列举10篇水平高、影响力大的学术论文。

②专著

序号	专著名称	作者	出版年度
1	入侵检测技术	薛静锋, 祝烈煌, 单纯, 徐美芳, 杨顺民	2016
2	嵌入式软件安全保证技术	王崑声、经小川、李宁、张伟、詹海潭、王潇茵	2015
3	计算机网络 系统方法 (原书第5版)	王勇, 张龙飞, 李明, 薛静锋	2015

3、专利、动/植物新品种、新药证书、临床批件、数据库等

序号	名称	编号	申请/授权	获得年度	国内/国际	类型	PCT申请
1	一种基于网络Motif的软件稳定性评估方法	201310750658	授权	2014	国内	专利	否
2	一种基于投影估计的多能谱CT图像重建方法	201310581204	授权	2016	国内	专利	否
3	一种双能谱CT图像迭代重建方法	201310576886	授权	2016	国内	专利	否
4	一种双通道信息融合的情感识别方法	201210225170	授权	2014	国内	专利	否
5	基于增强耦合HMM的语音-视觉融合的情感识别方法	201210435946	授权	2015	国内	专利	否
6	基于多层增强HMM的语音-视觉融合的情感识别方法	201210459173	授权	2015	国内	专利	否
7	基于线索神经网络的语音-视觉融合的情感识别方法	201310304011	授权	2016	国内	专利	否
8	由信誉评估上升到信任管理的跨区域访问控制策略	201110294120	授权	2014	国内	发明	否

	生成方法						
9	基于语义扩展的海量短文本信息过滤方法	201310376206	授权	2016	国内	专利	否
10	一种基于内存管理的模式化软件关键行为跟踪方法	201310502650	授权	2014	国内	专利	否
11	一种基于抽象解释模型验证的运行时错误分析方法	201310529070	授权	2014	国内	专利	否
12	由信誉评估上升到信任管理的跨域访问控制策略生成方法	201110294120	授权	2014	国内	专利	否
13	一种基于抽象解释和模型验证的运行时错误分析方法	201310529070	授权	2015	国内	专利	否
14	一种基于情感分析和隐马尔科夫模型融合的股市预测方法	201410023154	授权	2016	国内	专利	否
15	一种网络协议模糊测试方法和装置	201410056870	申请	2014	国内	专利	否
16	一种有状态协议的规则化状态机模型设计方法	201410333944	申请	2014	国内	专利	否
	一种分布式无线						

17	传感网络节点复制攻击检测方法	201510107472	申请	2015	国内	专利	否
18	一种基于WIFI信号强度的室内定位方法	201510119340	申请	2015	国内	专利	否
19	一种有状态网络协议的模糊测试系统	201510219969	申请	2015	国内	专利	否
20	基于有限状态机网络协议半合法化模糊测试用例生成方法	201510420048	申请	2015	国内	专利	否
21	一种基于测试工作量的软件安全缺陷发现模型的建模方法	201510711745	申请	2015	国内	专利	否
22	基于粒子群优化算法的Android自动化测试方法	201610069905	申请	2016	国内	专利	否
23	一种软件缺陷预测方法和软件缺陷预测系统	201410056780	申请	2014	国内	专利	否
24	一种基于JCUDAS A_BP算法的软件缺陷预测方法	201510148728	申请	2015	国内	专利	否
25	一种面向安全代码静态分析方法	201510347630	申请	2015	国内	专利	否
26	一种基于Redis的对象智能检索方法	201510362468	申请	2015	国内	专利	否

27	一种基于代码替换和正则表达式的静态分析工具改进方法	201510707442	申请	2015	国内	专利	否
28	一种基于符号执行的数组越界检测方法	201610202058	申请	2016	国内	专利	否
29	基于虚函数表劫持的防御方法	201610202853	申请	2016	国内	专利	否
30	一种用于预测软件缺陷的方法和系统	201410056820	申请	2014	国内	专利	否
31	一种基于调表的跨站脚本攻击防御方法	201510170489	申请	2015	国内	专利	否
32	一种基于函数调用的缓冲区溢出漏洞动态检测方法	201510170818	申请	2015	国内	专利	否
33	一种基于系统调用短序列的软件漏洞检测方法	201510176840	申请	2014	国内	专利	否
34	一种基于网络行为分析的Hadoop恶意节点检测系统	201510292116	申请	2015	国内	专利	否
35	一种基于系统调用的软件行为评估方法	201510629665	申请	2015	国内	专利	否
	基于系统调用分						

36	析的软件行为评估方法和装置	201410240266	申请	2014	国内	专利	否
37	一种基于图的个性化推荐方法	201610202060	申请	2016	国内	专利	否
38	一种基于复杂网络的脏数据传播路径发现方法	CN104731705A	申请	2015	国内	发明	否
39	一种基于复杂网络的软件缺陷度量方法	CN103838671A	申请	2014	国内	发明	否
40	一种发现大型面向对象软件系统关键测试函数的方法	CN105022689A	申请	2015	国内	发明	否
41	基于复杂网络的软件缺陷评估模型的构建方法	CN105808435A	申请	2016	国内	发明	否
42	软件安全缺陷发现系统	CN105068925A	申请	2015	国内	发明	否
43	一种针对虚函数表劫持攻击的防御方法	201510333582	申请	2015	国内	发明	否
44	一种面向航天高可信软件的软件可信性度量方法	201410178238	申请	2014	国内	专利	否
45	一种安全攸关系统的软件安全性保证的实现方法	201410178301	申请	2014	国内	专利	否
46	一种Shellcode的动态检测方法	201510134655	申请	2015	国内	专利	否

47	一种嵌入式安全关键软件的安全性度量方法	201518010618	申请	2015	国内	专利	否
48	一种将x86汇编语言数据寻址方式可视化演示的方法	2016111911572	申请	2016	国内	专利	否
49	一种将事件驱动编程模型机理可视化的方法	2016111836016	申请	2016	国内	专利	否
50	一种将Java语言内部类与外部类交互机制可视化的方法	2016111837926	申请	2016	国内	专利	否
51	一种软件运行时故障定位方法	2016111020154	申请	2016	国内	专利	否

备注:

- (1) 国内外内容相同的不得重复统计。
- (2) 类型: 分为专利(仅包括发明专利)、新药证书、数据库、动/植物新品种、临床批件等。
- (3) PCT为Patent Cooperation Treaty(专利合作协定)的简写, 是专利领域的一项国际合作条约, 即在一个专利局(受理局)提出的一件专利申请(国际申请), 申请人在其申请中(指定)的每一个PCT成员国都有效, 从而避免了在几个国家申请专利, 在每一个国家都要重复申请和审查。
- (4) PCT申请填写是、否即可。

4、制（修）订技术标准

序号	名称	编号	类型	类别
1	航天型号软件验证与确认指南	Q/QJA298-2014	行业标准	A
2	航天型号软件测试规范	Q/QJA300-2014	行业标准	A
3	航天外协外购与出口型号软件管理要求	Q/QJA299-2014	行业标准	A
4	航天型号软件文档管理要求	Q/QJA301-2014	行业标准	A

备注：

(1) 类型分别为国际标准、国家标准、行业标准、地方标准四类。

(2) 类别有A、B两类，A是指重点实验室牵头制（修）订的技术标准，B是指重点实验室参与制（修）订的技术标准。

5、获奖成果

序号	项目名称	奖项名称	奖项等级	奖项类别	评奖单位	主要完成人	主要完成人排名	获奖年度
1	面向重点型号系统安全关键软件的安全性保证评估方法研究	科技进步	三等	省部级	工业和信息化部	张刚、张伟	4, 5	2014
2	航天器产品软件安全性评价体系及关键技术研究	中国航天系统科学与工程研究院科技进步奖	二等	行业协会	中国航天系统科学与工程研究院	张伟、詹海潭、经小川	1, 2, 5	2015
3	嵌入式软件运行时错误检查技术研究及工具开发	中国航天系统科学与工程研究院科技进步奖	二等	行业协会	中国航天系统科学与工程研究院	詹海潭、经小川、张伟、李宁	1, 2, 3, 4	2015
4	航天器产品软件安全性评价体系及关键技术研究	中国航天系统科学与工程研究院科技进步奖	二等	行业协会	中国航天系统科学与工程研究院	张伟、詹海潭、经小川	1, 2, 5	2015
5	嵌入式软件运行时错误检查技术研究及工具开发	中国航天系统科学与工程研究院科技进步奖	二等	行业协会	中国航天系统科学与工程研究院	詹海潭、经小川、张伟、李宁	1, 2, 3, 4	2015

备注：

- (1) 奖项名称指国家自然科学奖、北京市科学技术奖等。
- (2) 奖项等级指特等、一等、二等、三等四类。
- (3) 奖项类别指国家级、省部级、行业协会三类。其中国家级仅限“国家最高科技技术奖、国家自然科学奖、国家技术发明奖、国家科学技术进步奖和国际科学技术合作奖”5类。
- (4) 评奖单位指科技部、教育部、北京市科委等单位。

6、技术合同

序号	技术合同名称	主持人	委托单位	委托省份	年度	技术合同类型	合同额（万元）
1	软件运行时错误检查系统	经小川	航天科技第八研究院第八设计部、航天科技第七研究院第七设计部	上海	2014	技术服务	460.0
2	漏洞分析与风险评估技术研究	单纯	中国信息安全测评中心	北京	2016	技术开发	12.0
3	北方车辆全成本核算系统	薛静锋	北京北方车辆集团有限公司	北京	2014	技术开发	88.0
4	基于POSIX标准的操作系统接口改造	薛静锋	北京控制工程研究所	北京	2015	技术开发	22.0
5	某某试样弹上软件开发方测试	薛静锋	北京航天自动控制研究所	北京	2016	技术服务	58.0
6	信息安全自行评估研究与系统研制	薛静锋	北京信息控制研究所	北京	2016	技术开发	74.0
7	复杂协同办公系统软件开发	闫怀志	61932部队	北京	2016	技术开发	10.0
8	XXX辅助分析工具	王勇	中国信息安全测评中心	北京	2016	技术开发	75.0
9	协同办公系统	闫怀志	61662部队	北京	2015	技术开发	38.0
10	孕优平台安全接口技术	闫怀志	国家卫生计生委科学技术研究所	北京	2015	技术开发	25.0

11	100G光网络损伤建模仿真	闫怀志	中兴通讯股份有限公司	广东	2016	技术开发	28.0
----	---------------	-----	------------	----	------	------	------

备注：技术合同类型指技术服务、技术咨询、技术开发和技术转让四类。

附件2 队伍建设情况明细表

1、专职人员

序号	姓名	性别	出生日期	职称	实验室职务	所学专业	最后学位	学术兼职	高端人才情况	
									人才类型	获得时间
1	胡昌振	男	1967-06-07	正高	实验室主任	信息安全	博士	国防科工委信息安全技术专家组组长，国防科工委网络信息安全应急工作小组副组长	博士生导师	2004-3
2	李波	男	1955-06-20	正高	其他	计算机应用	博士			
3	闫达远	男	1955-11-16	正高	其他	计算机应用	博士			
4	许承东	男	1965-11-09	正高	其他	计算机应用	博士		博士生导师	2011-8
5	薛静峰	男	1974-02-26	正高	其他	计算机应用	博士		博士生导师	2013-8
			1960-10-2		学科带头	计算机应		国防科工委基础科研计划军民两用技术专家组	享受国务	

6	王崑声	男	5	正高	人	用	博士	组长, 中国电子学会信息安全专家组副组长	院特殊津贴专家	2003-1
7	经小川	男	1973-08-15	正高	实验室副主任	计算机应用	博士			
8	张刚	男	1974-07-15	正高	其他	计算机应用	博士			
9	雷沃宁	男	1957-10-04	正高	其他	计算机应用	学士			
10	李国良	男	1964-06-22	正高	其他	计算机应用	学士			
11	贾德燕	女	1956-12-17	正高	其他	计算机应用	学士			
12	王瑞	男	1975-06-02	正高	其他	计算机应用	博士			
13	杨桂枝	女	1963-07-08	正高	其他	计算机应用	学士			
14	危胜军	男	1975-05-22	副高	其他	信息安全	博士			
15	闫怀志	男	1975-11-19	副高	其他	信息安全	博士			
16	戴银涛	男	1963-10-14	副高	其他	信息安全	博士			
17	马睿	女	1973-07-30	副高	其他	计算机应用	硕士			
18	商建云	女	1965-11-22	副高	其他	计算机应用	硕士			

19	赵小林	男	1972-06-19	副高	其他	计算机应用	硕士			
20	方平	女	1964-02-10	副高	其他	计算机应用	学士			
21	马锐	女	1972-12-21	副高	其他	计算机应用	博士			
22	王勇	女	1975-09-22	副高	其他	计算机应用	博士			
23	孙丹鸣	男	1963-08-12	副高	其他	计算机应用	博士			
24	谢伟华	男	1978-04-17	副高	其他	计算机应用	硕士			
25	姚淑萍	女	1970-10-12	副高	其他	计算机应用	博士			
26	马宽	男	1980-02-18	副高	其他	计算机应用	博士			
27	方华	男	1965-02-16	副高	其他	计算机应用	学士			
28	海卫华	女	1979-09-10	副高	其他	计算机应用	硕士			
29	李雪巍	男	1979-07-16	副高	其他	计算机应用	硕士			
30	张伟	女	1978-06-12	副高	其他	计算机应用	硕士			
31	赵伯毅	女	1955-08-26	副高	其他	计算机应用	学士			
32	戴珊	女	1958-10-13	副高	其他	计算机应用	学士			

33	吴兵	男	1954-06-14	副高	其他	计算机应用	学士			
34	王潇茵	女	1982-09-11	副高	其他	模式识别与人工智能	博士			
35	李宁	男	1981-10-08	副高	其他	计算机应用	博士			
36	胡晶晶	女	1978-08-04	副高	其他	计算机应用	博士			
37	孙建伟	男	1972-04-10	中级	其他	信息安全	博士			
38	张欣	女	1976-02-09	中级	其他	信息安全	博士			
39	田东海	男	1984-07-05	中级	其他	计算机应用	博士			
40	郑平	男	1981-05-27	中级	其他	计算机应用	硕士			
41	陈星	男	1981-09-07	中级	其他	计算机应用	硕士			
42	郑新华	男	1980-07-21	中级	其他	计算机应用	硕士			
43	王婷婷	女	1981-12-08	中级	其他	计算机应用	硕士			
44	郑重	男	1982-05-10	中级	其他	计算机应用	硕士			
45	张晖	女	1983-06-19	正高	其他	计算机应用	硕士			
			1984-06-1			计算机应				

46	陈漠	男	0	中级	其他	用	硕士			
47	巴峰	男	1984-07-08	中级	其他	计算机应用	硕士			
48	佟轶	男	1986-08-11	中级	其他	计算机应用	硕士			
49	高金梁	男	1985-05-19	中级	其他	计算机应用	硕士			
50	詹海潭	男	1989-04-16	中级	其他	计算机应用	硕士			
51	韩博	女	1984-10-14	中级	其他	工业设计	学士			
52	郭栋	男	1984-05-24	中级	其他	计算机应用	硕士			
53	杨昕	女	1981-09-04	中级	其他	计算机应用	硕士			
54	孙凤丽	女	1980-06-08	中级	其他	计算机应用	硕士			
55	吴丹	女	1980-08-13	中级	其他	计算机应用	硕士			
56	杨隽	女	1981-07-12	中级	其他	计算机应用	硕士			
57	费晰	男	1989-02-12	其他	其他	计算机应用	硕士			
58	王昕	男	1985-06-07	其他	其他	软件工程	硕士			
59	单纯	女	1976-08-05	中级	其他	计算机科学与技术	博士			

60	刘振岩	女	1973-05-17	副高	其他	计算机科学与技术	博士			
61	彭图	男	1980-02-19	副高	其他	数学	博士			
62	吕坤	男	1976-10-07	中级	其他	计算机科学与技术	博士			
63	张继	男	1979-09-24	中级	其他	计算机科学与技术	博士			

备注:

- (1) 专职人员: 指经过核定的属于实验室编制的人员。
- (2) 职称只限填写正高、副高、中级、其它四类。
- (3) 实验室职务: 实验室主任、实验室副主任、学术带头人、实验室联系人、其他。
- (4) 学术兼职: 标明兼职机构团体名称、任职情况、任职时间等。
- (5) 高端人才情况: 是否院士、享受国务院特殊津贴专家、博士生导师、万人计划、千人计划、国家杰出青年科学基金获得者、国家优秀青年科学基金获得者、长江学者、百人计划、科技北京领军人才、海聚工程人才、高聚工程人才、市科技新星等。

2、人才引进

序号	类型	2014		2015		2016	
		姓名	数量	姓名	数量	姓名	数量
1	千人计划						
2	海聚工程						

3、人才培养

序号	类型	2014		2015		2016	
		姓名	数量	姓名	数量	姓名	数量
1	科技北京 领军人才						
2	科技新星						
3	职称晋升		4		6		5
4	毕业博士	(填写数量即可)	3	(填写数量即可)	6	(填写数量即可)	4
5	毕业硕士	(填写数量即可)	42	(填写数量即可)	40	(填写数量即可)	38

备注：人才培养中博士、硕士指研究方向与实验室方向吻合，且在考评期内毕业的学生数量。

附件3 学术委员会召开情况表

1、学术委员会名单

序号	姓名	单位	职称	研究方向	学术委员会职务
1	何积丰	华东师范大学	正高	软件技术	主任
2	王崑声	中国航天集团公司第七一〇研究所	正高	系统工程	副主任
3	许进	中国航天科技集团公司第七一〇研究所	正高	信息安全	委员
4	夏春和	北京航空航天大学	正高	信息安全	委员
5	陈建华	武汉大学	正高	密码技术	委员
6	谢小权	中国航天科工706所	正高	信息安全	委员
7	王积鹏	中国电子科学院	正高	信息安全	委员
8	马建峰	西安电子科技大学	正高	信息安全	委员
9	秦志光	电子科技大学	正高	信息安全	委员
10	胡昌振	北京理工大学	正高	信息安全	副主任
11	经小川	中国航天科技710所	正高	信息安全	委员

备注：学术委员会职务指主任、副主任和委员三类。

2、学术委员会召开情况

序号	时间	地点	学术委员会出席名单	学术委员会主要建议
1	2014-12	北京	胡昌振、王崑声、许进、夏春和、谢小权、王积鹏、马建峰、秦志光、经小川	<p>①2014年的开放课题有力支持了重点实验室的主要研究方向，并取得了一定的成果，尤其是在软件安全漏洞关联建模研究方向有了较大进展。②2015年的技术研究应始终围绕安全软件工程、软件安全认知、软件安全测评等方向开展工作，重点针对软件架构的安全性评测技术方向开展研究工作，突破基于风险评估的软件架构安全评估技术。③2015年度实验室应加强开放课题数量和研究范围，进一步在软件漏洞检测方面提高了资助力度，提高实验室成员在软件漏洞检测方面的研究积极性，使得实验室在软件漏洞检测方面取得更大的进步。④2014年发表了多个高质量的论文，申请了国家发明专利。建议2015年取得更好的成果，在SCI刊物上发表一定数量的论文。⑤实验室应该进一步促进成果的产业化过程，开发商用产品，达到一定市场销售规模。⑥实验室在日常管理方面应该加强，应该更加重视每年的成果总结，认真分析</p>

				统计各项指标的具体数量并与往年对比，发现问题，肯定成绩，提出解决方案。
2	2015-08	北京	胡昌振、王崑声、许进、夏春和、谢小权、王积鹏、马建峰、秦志光、经小川	<p>(1) 为进一步提高软件安全性，需要按照严格的软件工程规范来开发软件，预防缺陷的引入，通过大量的软件测试和维护工作来移除缺陷。(2) 需要对系统中的软件开展安全性评估工作，以判定软件是否符合系统对安全性的要求，是否存在可能导致重大安全性问题的风险，软件的安全性等级是否具备交付使用的条件等。</p> <p>(3) 国外相关规范的内容较为庞大，实施成本较高，并不适用于我国现阶段军用软件的安全保证要求。因此，在装备型号软件的规模、数量以及关键程度快速增长的背景下，需要结合工程实际，以航天或军工领域的相关软件标准和规范为基础，参照国外成熟的软件安全性开发规范，如NASA-GB-8719.13《软件安全指南》，开展适合我国军用型号软件的安全性保证技术研究，提出一套可行、完整、具体、可剪裁的软件安全性保证规范，既能规范安全软件的设计分析过程，又能从质量管理角度辅助支撑软件安全性的监督评审。(4) 结合装备领域安全关键软件的特点，以软件工程化和软件可靠性检查单、软件安全性保证技术检查单、软件安全性</p>

				设计准则为基础，从软件开发生命周期的四个阶段提出可剪裁的软件安全性的评估准则，以该准则来指导软件安全性评价人员对软件的评估工作。
3	2015-12	北京	胡昌振、王崑声、许进、夏春和、谢小权、王积鹏、马建峰、秦志光、经小川	<p>(1) 2015年通过提出了一种基于软件开发过程的软件安全性度量方法，突破了软件安全性度量关键技术研究，首次建立了覆盖软件生命周期全过程的安全性度量方法。2016年需通过具体的量化指标对这种嵌入式安全关键软件度量方法进行验证，同时将各个阶段的度量结果与安全性等级的合理度进行对比，通过验证和改进得到技术成熟度高、可操作性强、度量结果全面的嵌入式安全关键软件度量方法。(2) 在2015年研制完成的多个技术工具基础上，将基于多阶变异的软件故障注入工具、航天C程序源代码安全漏洞检测工具等进行整合，建设成一个嵌入式系统软件开发平台，进一步支撑软件安全分析工作。(3) 2016年的技术研究还要继续围绕安全软件工程、软件安全认知、软件安全测评等方向开展工作，进一步促进成果的产品化，推进产品在商业市场上的应用，形成一定的市场规模和经济效益。2015年实验室已经发表了多个高质量的论文，申请了国家发明专利。建议2016年取得更好的成果，在SCI等</p>

				高等级刊物上发表一定数量的论文。(4) 实验室应该进一步加强日常管理, 提高学术交流质量, 扩大影响范围, 重视每年的成果总结和转化。
4	2016-07	北京	胡昌振、谢小权、王崑声、马建峰、许进、夏春和、王积鹏	(1) 在信息空间中, 行为是核心, 信息应用的实质是一个行为过程 (2) 拓扑本质是一种几何, 与欧氏几何对应 (3) 欧氏几何采用距离的概念描述了空间的构造关系, 刻画的是空间结构的匹配关系, 满足距离不变性。(4) 拓扑几何中没有距离概念, 具有变形连续性。变形来源于作用, 作用产生于行为。拓扑学是对行为变化描述的几何, 刻画了行为过程的匹配关系。(5) 基于拓扑不变量可对软件安全漏洞进行发现。
5	2016-12	北京	胡昌振、夏春和、王崑声、秦志光、许进、王积鹏、谢小权	(1) 2016年建立了覆盖软件生命周期全过程的安全性度量方法, 分析了安全性技术指标体系。(2) 在2016年研制完成的多个技术工具基础上, 进一步将基于多阶变异的软件故障注入工具、航天C程序源代码安全漏洞检测工具等进行整合, 建设成一个嵌入式系统软件开发平台, 进一步支撑软件安全分析工作。(3) 2017年的技术研究还要继续围绕安全软件工程、软件安全认知、软件安全测评等方向开展工作, 进一步促进成果的产品化, 推

				进产品在商业市场上的应用，形成一定的市场规模和经济效益。（4）实验室应该进一步加强日常管理，提高学术交流质量，扩大影响范围，重视每年的成果总结和转化。
--	--	--	--	---

附件4 开放交流情况明细表

1、开放课题

序号	开放课题名称	负责人	职称	工作单位	起止时间	总经费（万元）
1	基于抽象解释的软件运行时错误检测技术研究	詹海潭	中级	航天科技710所	2014	2.0
2	软件安全特性形式化建模与验证技术研究	高金梁	中级	航天科技710所	2014	2.0
3	软件行为捕获与分析技术研究	李宁	正高	航天科技710所	2014	2.0
4	软件安全漏洞的关联性建模方法	易军凯	正高	北京理工大学	2014	10.0
5	基于风险分析软件架构安全性评估	张红	其他	北京理工大学	2014	3.0
6	航天软件设计一致性验证技术	高金梁	中级	中国航天系统科学与工程研究院	2015	3.0
7	面向软件开发过程的软件安全性度量技术	詹海潭	中级	中国航天系统科学与工程研究院	2015	2.0
8	高安全测控系统软件安全性评估方法	佟轶	中级	中国航天系统科学与工程研究院	2015	2.0
9	航天软件设计一致性验证技术	王潇茵	副高	航天系统科学与工程研究院	2016	6.0
10	面向软件安全漏洞预测技术	陈宗权	其他	北京理工大学软件学院	2016	5.0

11	高安全测控系统软件安全性评估方法	佟轶	其他	航天系统科学与工程研究院	2016	4.0
12	基于拓扑不变量的软件安全漏洞发现技术	张红	其他	北京理工大学软件学院	2015	4.0
13	基于硬件特性的ROP攻击检测与防御研究	田东海	中级	北京理工大学软件学院	2016	1.0
14	嵌入式Linux下的Shellcode检测与分析技术研究	经小川	正高	中国航天系统科学与工程研究院	2014	45.0

2、访问学者

序号	姓名	国别	单位	访问时间与成效
1	易军凯	中国	北京化工大学	2014年易军凯教授来实验室进行学术访问，参与研究课题“软件安全漏洞的关联性建模方法”，对软件安全漏洞的分类方法以及软件安全漏洞的关联性进行研究，进一步完善软件安全漏洞的关联性建模方法，取得一定的成果。
2	危胜军	美国	天普大学	2015.12-2016.12，学习安全软件设计与开发技术，学习软件安全漏洞分析与发现技术
3	经小川	法国	法国国家信息与自动化研究院	2016.10.26-2016.10.30，主要针对2015年国家自然科学基金重点课题《嵌入式系统一致性保证技术研究》中嵌入式软件开发过程一致性保证技术的研究重点和难点问题，到法国国家信息与自动化研究院进行技术交流。
4	李宁	法国	法国国家信息与自动化研究院	2016.10.26-2016.10.30，主要针对2015年国家自然科学基金重点课题《嵌入式系统一致性保证技术研究》中嵌入式软件开发过程一致性保证技术的研究重点和难点问题，到法国国家信息与自动化研究院进行技术交流。

3、向社会开放

序号	开放时间	开放方式与成效
1	2014-2016	实验室的网络攻防对抗平台与试验环境对北京理工大学软件学院大学生创新创业基地的学生开放，学生利用平台从事信息安全竞赛项目的相关研究工作。创新基地取得的名次和奖项离不开实验室平台及环境的有力支持。

4、学术会议交流：（仅限主/承办会议，参与性会议不予填写）

序号	学术会议名称	会议类别	时间	地点	主要议题/内容
1	第九届信息安全漏洞分析与风险评估大会	国内会议	2016.10	无锡	软件安全漏洞的定量分析、安全风险的系统评估与控制
2	软件开发支撑平台关键技术研讨会	国内会议	2015.05	北京	软件开发支撑平台关键技术方案汇报与研讨
3	软件加扰保护技术研讨会	国内会议	2015.06	北京	软件加扰保护技术阶段评审
4	仿真试验效能评估与鉴定技术研讨会	国内会议	2015.06	北京	仿真试验效能评估与鉴定技术阶段评审
5	软件加扰保护技术评审会	国内会议	2015.10	北京	软件加扰保护技术年度结题评审
6	仿真试验效能评估与鉴定技术评审会	国内会议	2015.11	北京	仿真试验效能评估与鉴定技术年度结题评审
7	航天信息化和软件技术交流会	国内会议	2015.12	北京	智能制造、软件安全和软件产品保证技术
8	软件测试技术及体系提升高级研讨	国内会议	2014.12	北京	软件故障定位、嵌入式软件可信技术、安全关键软件测试技术
9	2016年航天信息化和软件技术交流会	国内会议	2016.10	北京	软件安全性保障及软件系统风险评估、软件产品化及软件验证与确认技术

备注：会议类别指国际会议和国内会议。

5、在国际会议做特邀报告

序号	学术会议名称	时间	地点	特邀报告主讲人	报告主题
1	the 11th ACM Asia Conference on Computer and Communication Security	2016.06	西安	马锐, 田东海	内核安全, 网络协议安全性分析
2	CCNIS' 2015	2015.11	杭州	陈漠	Shellix: An Efficient Approach for Shellcode Detection
3	CISP-BMEI2015 Proceedings	2015.10	北京	张伟	Process Models in the Development of Aerospace embedded Software
4	Proceedings of the 17th Asia Pacific Web Conference	2015	广州	刘振岩	A Supervised Parameter Estimation Method of LDA

附件5、绩效报告公示照片