第四研究室

----网电空间安全研究的领先团队

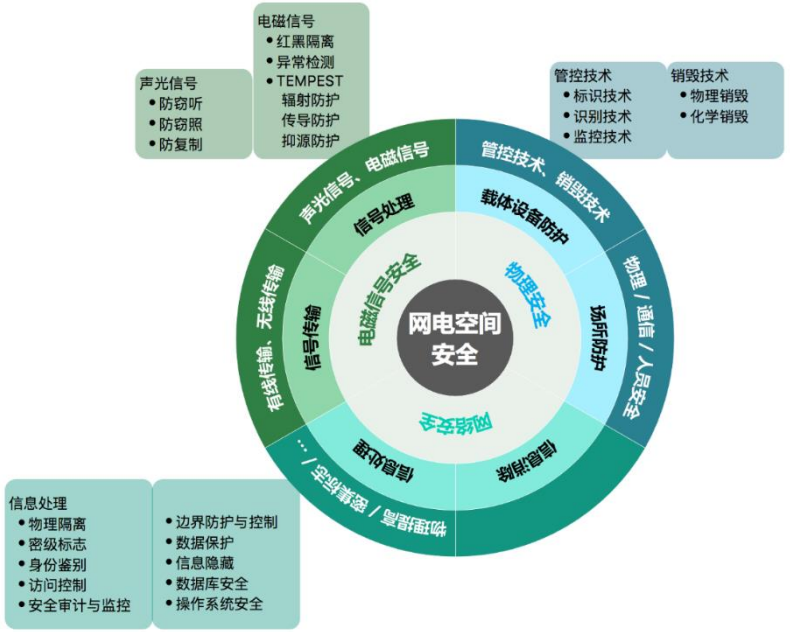
中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

研究室特色

研究室紧紧围绕“网电空间安全”领域展开研究

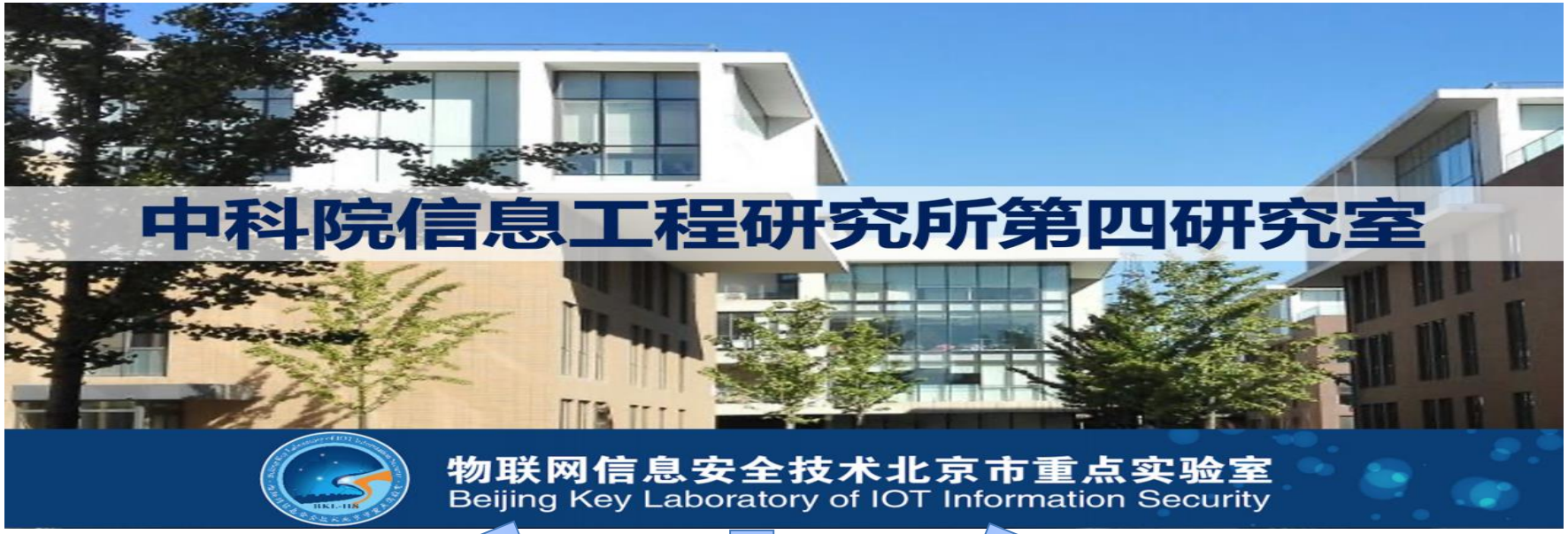
什么是网电空间安全?

- 随着电磁频谱资源的普遍开发和依赖于电磁波的电子设备的广泛应用，包含物理空间与网络空间在内的网电空间受到了前所未有的关注。国家安全空间已经拓展到包括海洋、太空和网电空间的安全。
- 网电空间安全涉及到万物互连的物理设施及其周围环境所处的物理空间安全、信息网络空间安全、以及携带信息的声光电磁信号空间安全。
- 网电空间安全的研究与实践正是应对这种网络空间的泛化、融合和安全观的变化，着眼长远，注重学科发展、人才培养、成果产出，不断提升网络空间安全的防护能力。



研究室组成

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS



五大研究方向

- 物联网安全
- 物理空间感知与防护
- 无线通信安全
- 工业控制系统安全
- 高安全等级网络与系统防护

四个研究小组

- 物理空间感知与防护组
- 物联网安全组
- 无线安全组
- 高安全等级网络与系统防护组

数百师生队伍

- 185名职工，正高8名，副高26名
- 6名博导，21名硕导
- 10名客座博导
- 研究生 235 名，硕士 113 名，博士122名

研究室成果

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

科研课题

承担数十项863计划、973项目、国家科技支撑计划、国家自然科学基金重点、国家重点研发计划、中科院先导、发改委重要工程、工信部工业互联网创新发展工程等重大项目

保密技术攻防重点实验室

物联网安全重点实验室

科研成果

取得100余项科研成果，包含20多个信息安全技术产品，20余项国家标准，获得国家科技进步二等奖3项，省部级科技进步一等奖4项、二等奖12项和三等奖14项，取得国家重点新产品证书5项；共发表高水平论文400余篇，申请专利100余个。

安城市视频监控仿真实验环境

智能制造仿真实验环境

城市燃气输送管道仿真实验环境

研究室科研团队

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

一、物理空间信息感知与防护

研究方向

- **电磁泄漏发射检测与防护**
- **无线信号及辐射源识别与解析**
- **电磁空间异常监测与管制**
- **卫星频率轨道资源评估与干扰规避**
- **电磁大数据分析与风险挖掘**
- **重要载体与设备管控**

前沿学术成果

- 在IEEE ACCESS 、SENSORS、Computer Networks、 ACM TOSN、WCMC、信息安全学报、软件学报等国内外知名期刊与会议上发表论文30余篇。出版译著1本，编写并出版教材3本。

科研实验平台

- **电磁安全实验研究环境**

面向电磁空间安全监测和防护方向，构建电磁安全研究实验平台，支持全频谱无线信号，广播电视等公众信号，集群、移动通信、WIFI、蓝牙、卫星等通信信号的采集、识别和解析，同时支持构建相关电磁与通信安全对抗仿真环境。目前平台已产出了用于无线电管理等相关业务部门的系统、装备，相关成果获得**省部级科技进步一等奖1项，二等奖3项。**

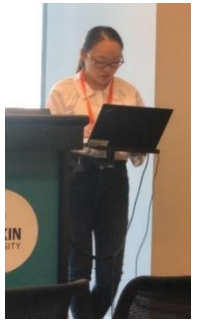
- **人、机、物融合分析及管控实验环境**

针对重要场所安全风险威胁，在物联网安全技术的基础上，结合人工智能、机器学习、无源感知、移动目标跟踪识别等关键技术，设计重要场所多源感知及异常行为分析算法，研制的多维管控系统已应用于国家重要部门的实际系统中，相关关键技术获得**省部级科技奖二等奖3次，三等奖2次。**

- **物理隔离网络安全实验环境**

在物理隔离网络安全研究领域，开展软硬件植入技术和声光电传输技术多技术融合研究，具有完善的嵌入式、FPGA等硬件开发环境及频谱仪、信号源、逻辑分析仪、网络分析仪等完善的硬件测试环境，平台研制出10余套物理隔离网络安全工具，**科研水平处于国内第一梯队。**




物理空间信息感知与防护研究-导师介绍

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

学科带头人—黄伟庆 正研级高级工程师 博士生导师

第四研究室主任，中国科学院“朱李月华优秀教师”，中国计算机学会信息保密专委会秘书长，国务院政府特殊津贴专家。主要研究方向包括无线通信安全、电磁信号处理与分析、载体管控等。主持重大项目包括863计划、中科院先导专项、发改委信息安全专项、省部级重大专项等，发表论文20余篇、编写并出版教材3本，**获省部级科技进步一等奖1项、二等奖3项。**

学术骨干

张萌 高工 硕导

研究方向：信息处理理论与技术、电磁声光检测与防护
中科院青促会成员
获省部级科技进步一等奖2项
发表论文20余篇、授权专利5项

王思叶 高工 硕导

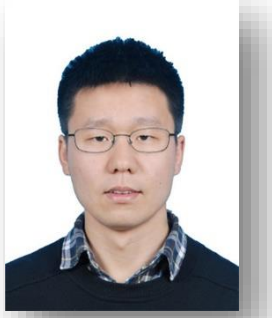
研究方向：载体管控
院青年创新促进会成员
获省部级科技奖二等奖3项，三等奖2项
国科大院级优秀课程获得者
发表论文20余篇

吕志强 副研究员 硕导

研究方向：物理隔离网络安全技术
获省部级科技奖二等奖2项
发表论文20多篇
授权专利20多项

徐艳云 高工 硕导

研究方向：信息处理理论与技术、电磁声光检测与防护
获省部级科技进步二等奖1项
信工所首届“优秀引进青年人才”
中科院院长优秀奖
发表论文20余篇，授权专利4项



魏冬 副研究员 硕导

研究方向：通信物理层安全、电磁信息安全
中科院青促会会员
研究所青年之星
获省部级科技进步一等奖1项

研究室科研团队

二、物联网与工控系统安全

□ 前沿学术成果

在**USENIX Security、S&P、INFOCOM、JASAC等国际顶会和**等发表CCF A类论文20篇，在物联网设备指纹自动化提取、嵌入式设备漏洞挖掘方面取得突破。

□ 全球鹰基础设施安全态势感知系统

全球共探测**7亿**物联网设备，支持近**两千品牌**、**四万型号**硬件属性识别，覆盖主流物联网设备，参加了抗战70周年纪念活动、G20峰会、18届五中全会等国家重要活动的安全保障工作，及时发现并解决了多起安全隐患，收到各级国家部委的认可和奖励。

□ 工控入侵诱捕平台

部署各种蜜罐**123个**，平均每日捕获百兆攻击流量，部署范围**覆盖四大洲**（亚洲、欧洲、北美洲、非洲），遍布全球**20多个国家/地区**有效捕获SYN、FIN、TCP Connect等不少于5类扫描探测行为，工控入侵行为记录、分析、告警。

□ 工控入侵检测系统

目前支持**30种主流工控协议**，包括私有协议逆向协议解析深度：操作指令、指令参数、值域范围。取得软著和销售许可证，在多个大型国企生产加工环境进行试用。

全球鹰网络基础设施安全态势感知系统

视频监控系统深度安全检查工具

工控入侵诱捕平台

石油化工蜜网系统

工控入侵检测系统

管理中心

网络探针

物联网与工控系统安全-导师介绍

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

学科带头人—孙利民 研究员 博士生导师

物联网安全技术北京市重点实验室主任，中科院大学物联网安全首席教授。长期从事物联网安全、工控安全研究工作，牵头承担物联网/工控安全领域的20余国家级项目，针对国家实际需求研究相关的核心技术来解决卡脖子与短板问题，出版学术书籍5部，发表论文200余篇，申请发明专利和软著50余项。

学术骨干

石志强 正研级高级工程师 博导

中国自动化学会工业控制系统信息安全专委会委员，长期从事工控系统安全、软件安全分析理论与技术，主持和参加完成了十多项国家级项目和企业合作课题

朱红松 研究员 博导

物联网安全技术北京市重点实验室副主任，中国计算机学会高级会员、物联网专业委员会委员，长期从事物联网安全、自组织网络安全，安全大数据分析研究，主持20余国家/省部级项目，发表论文60余篇

李　志 高级工程师 硕导

北京市优秀博士毕业生

中科院信工所重大科技进展奖和优秀教材奖

研究方向是物联网设备探测识别、物联网安全大数据分析

李　红 副研究员 硕导

物联网安全技术北京市重点实验室副主任

中科院信工所“优秀青年引进人才”

研究方向包括物联网知识图谱、大数据驱动的物联网安全、隐私保护、区块链

研究室科研团队

三、无线通信安全与检查取证

移动终端安全

- **手机恶意代码检测系统：**多次承担省部级单位公务人员手机检测任务，发现**窃密木马6项**，普通木马若干，获**中办科技进步奖**；
- **手机信息擦除工具：**对安卓、iOS设备进行多任务异步并行擦除，符合擦除标准，有效防止信息泄露，**填补领域空白。**
- **移动终端网络指纹分析系统：**自动抓取终端的网络数据，跟踪网络数据中携带的隐私数据，还原终端**上传或下载的文件**

移动通信安全

- **移动通信管控设备**：多次参与**重大活动保障**工作，屏蔽管控范围内手机通信，发送警示短信，设置的白名单内用户可正常通信；
- **海云安全手机整体办公**： 基于安全沙箱和VMP技术实现应用的安全加固隔离和敏感权限监测 ， 平台侧虚拟化并通过差分视频和本地渲染等技术实现终端核心业务的私有云化；
- **集群通信失泄密分析系统**：解析集群信号，融合多源数据分析**用户的行为轨迹**、通联关系等信息。

异常信号处理

- **通信信号安全保密设备小型化硬件开发**：研制基于超外差、零中频原理的小型化接收机，**用于微弱信号采集、通信信号管控**等；
- **异常信号处理系统分析**：通信与异常信号**盲均衡处理、未知信号调制模式识别与参数估计**；
- **电磁泄漏发射微弱信号检测接收还原分析**：长期承担863、中科院先导、国家部委项目，**创新研制的视频信息接收还原系统。**

声光安全

- **激光语音信息获取**：从其激光特性，传输路径以及设备特征进行研究，形成与之对应检测、定位以及切断传输途径等设备，并已**应用于国家重要部门**的实际应用；
- **光通信信道安全检测**：采用对光信息监测、以及光纤振动、温度信号感知，获取光通信道安全状况，空间白光通信监测系统已在**国家相关部门获得应用；**
- **多媒体设备检测系统**：利用多媒体设备中特有**电磁材料信息**，获取是否有手机等带入敏感场所以及会议室。

研究室科研团队

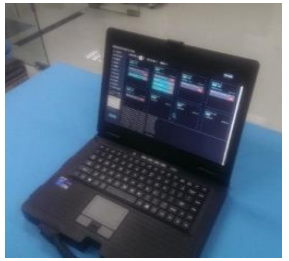
三、无线通信安全与检查取证

□ 前沿学术成果

在**ESORICS、ECAI、FGCS等国际知名期刊**发表论文20余篇，在恶意文档检测、二进制分析、特定文本分析等方面取得突破。

□ 终端检查、取证系统

支持Windows、Linux、麒麟、UOS等操作系统，覆盖主流计算机、服务器等终端，服务全国**1000余**家单位，使用产品**10000余**套，及时发现并解决了多起隐患，受到各单位的认可和感谢。



终端检测系统

□ 邮件检查与溯源取证平台

支持POP/POP3/IMAP等协议，支持Foxmail、Outlook、DreamMail等客户端，在**20多家**单位检查中发现安全事件**10余起**，填补了空白。

核查取证机

□ 重要信息系统文件输入输出检查系统

支持对信息系统之间文件输入输出存在的文件**嵌套、夹带、伪装**等问题进行检测，已在多家单位部署试用。

□ 数据库检查系统

支持对Oracle、SQLServer、MySQL、人大金仓、达梦等**20多种**主流数据库进行快速、准确的分析和检查，及时发现违规行为。

邮件检查与溯源取证平台

溯源服务器

无线通信安全与检查取证-导师介绍

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

学科带头人：朱大立　正高级工程师　博士生导师

中国科学院信息工程研究所第四研究室副主任。

从事网络空间安全、移动互联网安全、信息安全与保密技术、网络系统安全技术等领域的研究和产品开发工作主持或参与各种级别的科研项目、涉密工程、国家保密标准制定、安全保密防护产品开发累计23 项。获得中办科技进步二等奖3 次，三等奖1 次。撰写内部研究报告4 篇，发表学术论文15 篇，制定国家保密标准5 项。获得国家实用新型专利3 项，申请国家发明专利7 项。

成员

冯维淼　高级工程师，硕导

研究所青年之星

从事移动终端安全研究
主持多项省部级课题
省部科技进步奖3项，SCI/EI检索论文6篇，授权发明专利7项

刘银龙　副研究员，硕导

研究所引进优秀青年人才

从事通信系统与安全研究
主持国家和省部级多项科研项目发表SCI/EI论文20篇，申请发明专利20余项

范伟　高级工程师，硕导

研究所青年之星

从事异常信号识别理论研究
主持多项国家和省部级项目
国家保密标准10项，SCI/EI检索论文8篇，发明专利授权8项，软著25项

曾华林　副研究员，硕导

从事声光电保密攻防技术研究
主持国家和省部级多项科研项目
发表论文20余篇
授权发明专利10余项

无线通信安全与检查取证-导师介绍

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

刘超 正高级工程师 硕导

曾获省部级科技进步奖5次，中国科学院信息工程研究所“重大科技进展奖”、“青年之星”等奖励和荣誉称号。主要研究方向为信息保密技术、移动终端安全等。近年来主持和参与了多项国家重点项目、国家部委重大项目、中国科学院先导专项等科研工作。

张顺亮 高级工程师 硕导

从事4G/5G/6G移动通信网络及安全攻防方面的研究工作。主持中国科学院天地一体化重点项目子课题。到目前为止已经提交近50项PCT国际发明专利申请，其中近30项PCT发明专利申请已经获得欧州、美国、中国等主要国家授权。在国内外著名期刊/会议上发表了20多篇网络通信方面的学术文章。

冯志杰 高级工程师 硕导

从事网络空间安全、电磁与移动通信安全、车联网安全评测等领域的研究和应用工作，主持和参与各种级别的科研项目、安全工程、国家标准制定、安全产品开发10余项。研发的多项科研成果如“车辆安全保密检测云平台”等，产生了较好的社会和经济效益。

研究室科研团队

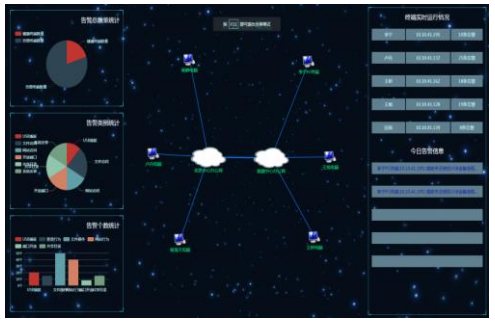
四、高安全等级与系统防护组

研究方向

- **高安全等级网络应用安全防护**
- **系统与产品安全风险评估及测试测评技术**
- **内网用户安全风险持续监测与分析**
- **高速网络数据流分析处理技术**

重大活动保障

围绕网络安全技术，开展一系列理论和技术攻关研究，同时与组内多年的项目实践相结合，将技术成果转化为产品，服务于国内高安全等级网络的安全防护，为保障信息安全做出贡献。



科研小组

□ 基于风险度量的网络安全评估团队

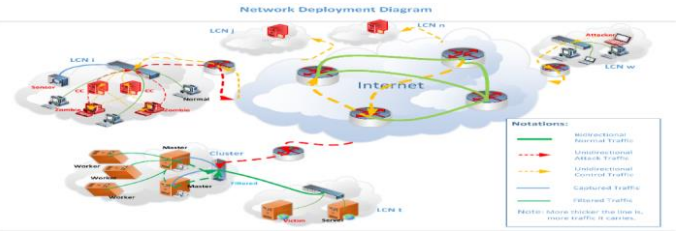
面向高安全等级网络应用实践，研究Web应用异常检测与防护、虚拟化系统安全问题，研发用于风险评估的工具集。支撑项目包括：**国家有关标准制定、重要网络现场风险评估、高安全等级网络防护方案设计、云计算取证与风险评估**

□ 大象行动团队

大数据分析技术与安全相结合，**研究海量异构数据的存储，搜索以及挖掘支撑网络信息安全的业务场景分析。**支撑项目包括：中科院先导专项、加密数据流量分析技术项目、测评机构风评大数据分析、重要场所失泄密监管大数据分析

□ 高安全等级网络威胁检测研究团队

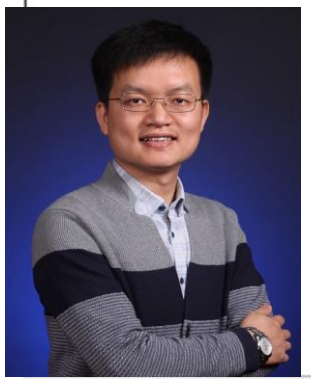
将大数据采集技术、大数据挖掘理论与威胁检测实践相结合，**研究高安全等级网络中的各类威胁检测方法，研发相关产品，提高网络安全防护能力。**支撑项目包括发改委专项项目。



高安全等级与系统防护-导师介绍

学科带头人—姜建国 研究员 博士生导师

中科院大学网络空间安全学院第四教研室主任，北京交通大学兼职教授，计算机学会杰出会员，国家保密专业教育优秀教师。主要研究方向为信息安全和保密技术，主持过多项国家级重大课题如国家自然科学基金课题、国家863课题、国家科技支撑计划课题等。获得过多项奖励，如部级科技进步一等奖、二等奖、三等奖、邓稼先青年科技奖、中国发明协会发明银奖等，在国内外期刊和学术会议发表论文八十余篇。



学科带头人—李敏 正高级工程师 硕士生导师

第四研究室副主任，中国科学院大学网络空间安全学院教授。研究方向：高安全等级网络评估与防护，电子数据检查取证，视频信息智能处理等。先后主持或参与国家科技支撑计划、国家863计划、国家信息安全专项、国家自然基金、中科院先导专项等10余项国家级和部级科研课题，主持或参与多项国家标准制定。在国内外核心刊物和国际学术会议上发表SCI、EI论文20余篇，申请国家专利10余项。获得省部级科技进步奖一二三等奖8次。

高安全等级与系统防护-导师介绍

中国科学院信息工程研究所 INSTITUTE OF INFORMATION ENGINEERING,CAS

学术骨干

王 妍 高级工程师 硕士生导师

长期从事高安全等级网络安全体系结构、风险评估、威胁监测、态势感知等方面的技术研究、产品研制和相关国家标准制修订工作。获得过保密科技进步**二等奖2次**、军队科技进步**三等奖1次**；发表**学术论文10余篇**。

吕 彬 高级工程师 硕士生导师

从事网络与系统安全技术、高安全等级信息系统体系架构及关键安全防护技术、大数据安全分析技术等方面研究工作。获省部级科技进步**二等奖1项**，**三等奖2项**。发表**学术论文10篇。**

胡 波 高级工程师 硕士生导师

主要从事高安全等级网络的安全评测与防护监测、数字检查取证、虚拟化安全等方面的技术研究、工程实践和标准制定工作。**获得省部科技进步奖4项。**

毛 锐 高级工程师 硕士生导师

从事网络安全防护体系及关键技术的研究、业务系统安全防护。获省部级科技奖励**3次**，中国科学院信息工程研究所**优秀员工**、中国科学院信息工程研究所“**重大科技进展奖**”等。

李梅梅 高级工程师 硕士生导师

主要研究领域包括高安全等级系统的信息管控、风险评估与测评、面向失泄密的多源数据融合与分析、工控安全防护及相关标准制定。获得中办科技进步**三等奖**、**中国产学研创新成果奖，**发表**SCI/EI收录论文近10篇**。

石志鑫 高级工程师 硕士生导师

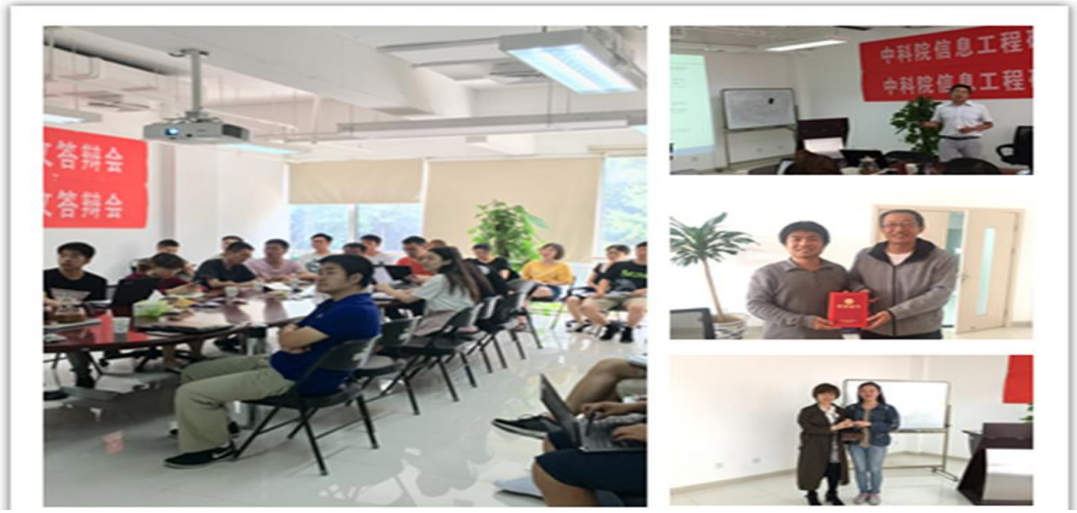
从事特定应用场景大数据挖掘分析、智能信息处理、威胁检测行为分析等相关研究。获**部级科学技术一等奖和二等奖各1项**、研究所“**重大科技进展奖**”及“**青年之星**”人才培养计划，发表**论文20余篇**。

研究室文化

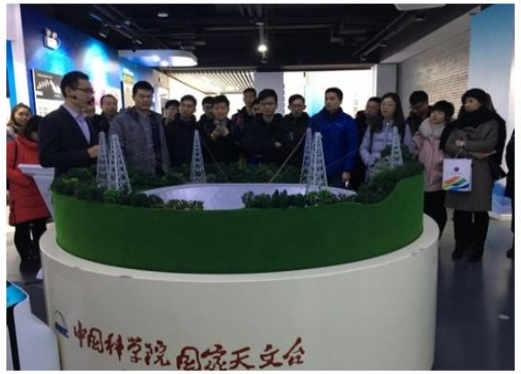
中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

国际学术交流

室内学术交流



党支部活动



体育活动


毕业去向


TSINGHUA UNIVERSITY 1911
PEKING UNIVERSITY 1898
NYU
北京交通大学
电子科技大学
北京邮电大学
Microsoft Research
微软亚洲研究院
CNCERT/CC
国家互联网应急中心
中华人民共和国工业和信息化部
中国农业银行
ICBC
中国工商银行
中国银行
BANK OF CHINA
中国建设银行
China Construction Bank
Baidu 百度
Alibaba 阿里巴巴
Tencent 腾讯
HUAWEI
ByteDance
字节跳动
360
网易游戏
美团
滴滴
快手

第四研究室

----网电空间安全研究的领先团队

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

欢迎报考第四研究室
让我们共同努力见证
中国网络空间安全
事业的发展和腾飞！