中国系统工程学会

网络空间安全与社会治理论坛日程

时间：2024 年 1 月 3 日

会议地点：中国科学院数学与系统科学研究院南楼 219 会议室

时间	内容	主持人
09:00-09:10	领导致辞	杨晓光
09:10-09:50	主动网络安全模型构建计算机网络对抗体系 报告人：张小松 电子科技大学	
09:50-10:30	网络空间融合安全 报告人：饶志宏 中国电子科技集团	
10:30-11:00	网络信息内容与认知安全 报告人：王震 西北工业大学	唐锡晋
11:00-11:30	系统工程视角下社会治理系统智能分析方法及其应用 ——数据与知识融合驱动路径 报告人：叶鑫 大连理工大学	
11:30-12:00	基于 PSI 的隐私保护典型应用及新型攻击 报告人：刘哲理 南开大学	
13:30-14:00	工业数据全生命周期保护风险与挑战 报告人：杨震 北京工业大学	孙文
14:00-14:30	四蜜——基于主动式网络欺骗的威胁感知研判系统 报告人：鲁辉 广州大学	
14:30-15:00	集成电路硬件安全威胁与体系化评估技术 报告人：胡伟 西北工业大学	

报告一

报告题目：主动网络安全模型构建计算机网络对抗体系

【报告人简介】 张小松，电子科技大学计算机科学与工程学院（网络空间安全学院）常务副院长兼院长。长江学者特聘教授，CCF 会士，中国通信学会会士。长期致力于计算机系统与网络安全的研究，原创提出以“智感”“透析”“活现”为核心要素的主动网络安全模型，入选十三五国家自然基金项目优秀成果，在威胁感知、检测防御、追踪溯源方面开展系统性、开拓性的创新实践，以第一完成人获 2019 国家科技进步一等奖、2012 国家科技进步二等奖，四次获得省部技术发明/科技进步一等奖；是第二届全国创新争先奖、2017 网络安全优秀人才奖、第三届四川省杰出人才奖获得者，入选天府万人计划杰出科学家，省部共建信息安全协同创新中心、区块链安全与平台技术教育部工程研究中心负责人。截至 2023 年，第一作者出版专著 4 部，发表 SCI/EI 等学术论文 180 余篇，第一发明人授权发明专利 63 项，主持完成国家级、省部级项目 30 多项。

报告二

报告题目：网络空间融合安全

【报告人简介】 饶志宏，中国电子科技集团首席科学家/网安板块总师召集人。国家“万人计划”科技创新领军人才，首届国家网络安全先进个人。担任国家重点研发计划“网络空间安全”重点专项“软件与系统漏洞分析与发现技术”项目负责人，享受国务院政府特殊津贴专家。长期就职于中国电科三十所、中国电子科技网络信息安全有限公司，主要从事网络空间安全总体和关键技术研究工作，在网络空间对抗、认知安全、监测预警和工业控制系统安全等方面取得系列成就，被聘为国家部委、军队和地方等网络安全领域核心专家。获得省部级一等奖三次、二等奖五次，申请专利二十余项，出版《网络空间安全监测预警》《物联网网络安全及应用》等专著，发表各类影响力论文二十余篇。

报告三

报告题目：网络信息内容与认知安全

【报告人简介】 王震，西北工业大学教授，网安学院书记，国家保密学院常务副院长，欧洲科学院院士，IEEE/AAIA/IOP Fellow，全球高被引科学家，国家杰青，国防创新团队负责人。研究方向为博弈智能，智能无人系统，网络空间智能对抗。在 Nature Communications、PNAS、Science Advance、PRL、IEEE 汇刊、 IJCAI、AAAI、NeurIPs、ICML、ICLR、WWW 等发表系列成果，引用 27000 余次，研制的系统应用于数个型号，成果和事迹被人民日报、光明日报、新华社、Nature News、Live Science、Sciencedaily 等知名媒体专题报道，也受到北部战区的点名表扬。在国际会议做大会或特邀报告 80 余次，主持国家自然科学基金重点项目、海外基金、GF 项目等 20 余项，获科学探索奖、全国创新争先奖章、中国青年五四奖章、全国五一劳动奖章，首届 MIT-TR35 China(西部唯一)，教育部、陕西省、中国航空学会、中国电子学会科学技术奖一等奖等。

报告四

报告题目：系统工程视角下社会治理系统智能分析方法及其应用——数据与知识融合驱动路径

【报告摘要】社会治理涉及社会治安整体防控、矛盾纠纷调解等诸多方面，是维护国家安全和社会稳定的重要组成部分。我国社会治理系统的多层次、多组分、多主体协同等特征凸显，对提升社会治理体系与治理能力现代化带来诸多挑战。报告从系统工程视角出发，从社会治理系统的复杂性分析入手，设计基于“数据-元数据-知识-实体模型-形式模型-算子”广义知识模式的社会治理综合系统分析体系，提出数据与知识融合驱动的社会治理系统智能分析方法，并介绍相关的应用实践，探索一条系统工程视角下社会治理系统分析的新路径。

【报告人简介】 叶鑫，教授，博士生导师，现任大连理工大学经济管理学院院长，现兼任电子政务模拟仿真国家地方联合工程研究中心主任、辽宁省电子政务工程研究中心主任。主持国家重点研发计划课题、国家自然科学基金项目等科研课题 10 余项，作为主要研究人员参加国家自然科学基金重点项目、国家科技支撑计划等科研课题 10 余项。在领域知名期刊与国际会议上录用、发表学术论文 90 余篇；出版专著 1 部、教材 1 部。主持编制辽宁省“十四五”数字政府发展规划，参与编制了辽宁省地方标准“行政权力运行与监察系统数据采集交换规范”，获软件著作权 9 项。获辽宁省自然科学奖、

山西省科学技术奖（科技进步类）、辽宁省科学技术奖（科技进步类）、辽宁省哲学社会科学成果奖、忻州市科学技术奖（科技进步类）等省、市及行业协会科研奖励近 10 项；获国家教学成果二等奖 1 项，辽宁省教学成果奖 7 项（一等奖 6 项）；获宝钢优秀教师特等奖提名奖、辽宁省教学名师等荣誉称号。

报告五

报告题目：基于 PSI 的隐私保护典型应用及新型攻击

【报告摘要】密文集合交集运算（PSI）在多方数据分析场景中应用越来越广泛。本报告首先介绍典型密文交集运算的方案设计，及其在保护个人隐私的多方精准广告推荐业务中的典型应用方案；进而，介绍以密文集合交集运算为基础协议的安全应用中面临的安全性问题，重点介绍团队在集合成员推理攻击方面的新工作，并针对如何抵御成员推理攻击提供防护建议。

【报告人简介】 刘哲理，南开大学计算机学院副院长、网络空间安全学院副院长，教育部数据与智能系统安全重点实验室主任，中国新一代人工智能发展战略研究院智能网络安全研究中心主任，中国中文信息学会大数据安全与隐私计算专委会秘书长，宝钢优秀教师，天津市中青年科技领军人才，教授，博士生导师。近五年，发表 USENIX Security、Eurocrypt、VLDB、ISSTA、ASE、IEEE TDSC、IEEE TKDE、IEEE TIFS、IEEE TC、IEEE INFOCOM、ACM TOSEM 等顶级期刊论文和会议 40 余篇，有 11 篇 ESI 高被引论文、2 篇热点论文。主要研究方向为密文数据库、密文集合运算、差分隐私、人工智能安全等。目前主持国家自然科学基金重点项目、国家重点研发计划、国防科技创新重点项目、工信部工业互联网创新工程等纵向课题 10 余项，与腾讯、华为等多家知名信息安全企业建立了合作关系，是腾讯广告、华为数据库的紧密合作伙伴，建立了“数据安全联合实验室”，主持密态数据库、密文集合运算、差分隐私相关的横向课题 10 多项。担任多个国际会议的会议主席，包括 ICICS 2023、SOCIALSEC2020、SPNCE 2019、ICA3PP2018、等。《电子与信息学报》编委，《网络与信息安全学报》编委，Springer 期刊《Cybersecurity》编委和 SCI 一区期刊 INS 编委。

报告六

报告题目：工业数据全生命周期保护风险与挑战

【报告摘要】工业互联网作为新一代信息技术与制造业深度融合的产物，推动制造业生产方式和企业形态根本性变革，显著提升了制造业数字化、网络化、智能化发展水平。但工业互联网高复杂性、开放性和异构性加剧其面临的安全风险，特别是随之而来的高敏感性工业数

据爆发式增长，使得数据安全共享交换问题已成为制约工业互联网发展的重要瓶颈，也成为长期困扰学术界和产业界的一个基础性、根本性难题。报告面向工业数据全生命周期过程，重点探讨采集、传输、共享三个方面所面临的风险与挑战。

【报告人简介】 杨震，北京工业大学信息学部副主任，计算机科学与技术系主任，智能感知与自主控制教育工程研究中心执行副主任。主持承担了国家自然科学基金重大研究计划（培育）、国家重点研发计划项目课题、ISO/IEC 国际标准研制项目、国家软科学研究计划项目、国家信息安全标准制定项目、国家自然科学基金面上项目、北京市自然科学基金等多项课题。主编了工业互联网平台安全、物联网传输安全领域国际标准、国家标准 2 项。在领域知名期刊和会议上发表论文十余篇，多篇论文入选 ESI 热点论文、ESI 高被引论文和国际会议最佳论文。获中国电子学会、中国人工智能学会科技进步奖一等奖、二等奖和三等奖多项。主讲课程获教育部第二批国家级一流本科课程。获北京市高等教育教学成果奖一等奖，北京工业大学优秀教育教学成果奖特等奖。

报告七

报告题目：四蜜—基于主动式网络欺骗的威胁感知研判系统

【报告摘要】广州大学方滨兴院士团队针对现网主动探查能力不足导致的捕不全，拦不住，看不清，抓不到等问题，自主研发基于逐层诱骗的主动欺骗式防御技术，形成四蜜探查体系，突破蜜点 HoneyPoint、蜜庭 HoneyYard、蜜阵 HoneyFormation、蜜洞 Honeytunnel 等关键技术，实现对网络中攻击企图的全面、快速、准确的逐层威胁探查，提升网络防御水平。

【报告人简介】鲁辉，广州大学网络空间先进技术研究院院长，教授，博士生导师，方滨兴院士班班主任，中国网络空间新兴技术安全创新论坛（新安盟）秘书长，福建省闽江学者讲座教授。长期致力于智能化网络攻防、数据安全防护、人工智能安全等研究工作。主持多项国家重点研发计划课题，国家自然科学基金项目，广东省重点领域研发计划项目等，国家自然基金函评专家。获 2020 年广东省哲学社科成果二等奖，第三届网络空间安全产学协同育人优秀案例一等奖，中国产学研合作成果二等奖以及中央网信办颁发的“冬奥积极参与人”称号等，带领团队保障第 24 届北京冬奥会、杭州亚运会以及多届广交会平台安全，多次获国家重要部门致函感谢。

报告八

报告题目：集成电路硬件安全威胁与体系化评估研究

【报告摘要】集成电路硬件是计算系统的核心，其安全性是网络空间安全的根基。集成电路

硬件安全属于集成电路和网络空间安全两大重点领域的交叉前沿方向。“熔断”和“幽灵”等漏洞爆出以来，硬件安全问题受到了学术界和工业界的广泛关注。报告介绍集成电路硬件安全面临的安全威胁和关键研究挑战，并探讨以人工智能、形式化验证、模糊测试、硬件加速仿真和安全量化分析技术为代表的硬件安全体系化评估方案。

【报告人简介】胡伟，西北工业大学长聘教授，翱翔青年学者，入选国家青年人才计划，研究方向包括集成电路硬件安全、处理器安全、密码学等。在领域知名期刊和会议上发表论文 70 余篇，出版网络空间安全专业“十三五”规划教材 1 部、专著 1 部。主持预研重点项目、国家重点研发课题、国家自然基金重点和面上等科研项目 10 余项。任 IEEE TCAD 客座编辑、硬件安全领域旗舰会议 HOST 和 AsianHOST 组委会委员、AsianHOST 共同大会主席、ATS2023 共同程序主席等职。研究成果获省部级科技奖励 3 项。