计算机学院科研团队情况介绍表

团队名称	ZJU NESA Lab（https://nesa.zju.edu.cn/）			团队负责人	纪守领
联 系 人	纪守领	Email	sji@zju.edu.cn	电话	0571-87951819

团队致力于人工智能安全、数据驱动安全、软件与系统安全研究。

浙江大学网络系统安全与隐私实验室（Network SystEm Security & PrivAcy Lab，NESA Lab）立足于信息安全、人工智能、数据分析与网络系统的交叉科学领域，致力于研究相关基础理论、关键技术与应用系统。实验室负责人为国家级高层次人才计划入选者纪守领教授，现有教授/研究员 3 人、博士后 3 人、研究助理 1 人，博士生 10 人，硕士生 10 人，本科生 8 人，**当前主要研究方向包括：人工智能安全、数据驱动安全、软件与系统安全，**在 TDSC、TIFS 和 IEEE S&P、ACM CCS、USENIX Security、NDSS 等权威期刊和会议上发表论文 150 余篇，包括 CCF A 类论文 100 余篇，获网络系统安全顶级会议 ACM CCS 2021 最佳论文奖等最佳论文奖 10 项、CCF 科技进步二等奖、华为优秀技术成果奖等。

实验室承担多项国家和省部级科研项目，包括国家重点研发计划项目、国家自然科学基金重点项目和面上项目、国家预研重点/创新特区/基础加强项目、浙江省杰青项目、浙江省重点研发计划项目等,研究经费充足。实验室与多家企业公司具有深入良好合作关系，包括华为、阿里巴巴、蚂蚁金服、腾讯、绿盟、启明星辰，研发的多个系统在大型商业平台上获得应用。

实验室具有优良的国际合作关系，与普林斯顿大学、佐治亚理工学院、UIUC、UCLA、弗吉尼亚大学、宾夕法尼亚州立大学、EPFL、IBM T. J. Watson 研究中心的多位教授/研究员具有长期稳定的合作关系，实验室每年有多位同学被选派至上述学校继续深造、访学研究。

团队主要成员

纪守领，现任浙江大学求是特聘教授/长聘教授、博士生导师，可信人工智能研究中心主任，兼任佐治亚理工学院 Adjunct Research Faculty，获美国佐治亚理工学院电子与计算机工程博士学位、佐治亚州立大学计算机科学博士学位，入选教育部长江学者（2022

年度)、高层次科技创新人才（2022 年度)、国家青年特聘专家（2017 年度)。**主要研究方向为人工智能安全、数据驱动安全、软件与系统安全、大数据分析**，先后主持国家重点研发计划项目、国家自然科学基金重点项目和面上项目、国家预研/创新特区/基础加强项目（课题)、浙江省杰青项目、浙江省重点研发计划项目、阿里巴巴科研基金、蚂蚁金服科研基金、华为科研基金、CCF-腾讯“犀牛鸟”科研基金、CCF-绿盟“鲲鹏”科研基金、CCF-启明星辰“鸿雁”科研基金等多项，作为技术负责人或项目骨干，参加美国 NSF 项目 8 项。**发表 IEEE S&P，ACM CCS，USENIX Security，NDSS 等 CCF A 类论文 100 余篇，**出版英文专编著 6 部。申请专利 30 余项，研制了深度学习模型安全与评估系统 DeepSec、大数据驱动的反欺诈系统 ATF、新型对抗性验证码生成系统 aCAPTCHA (advCAPTCHA)、自适应知识驱动的模糊测试系统 MOPT、模糊测试评估平台 UNIFUZZ、物联网固件漏洞挖掘系统 iFIZZ 等多个系统。其中，多个系统已被部署应用于拥有千万用户级以上的商业大平台，相关成果被央视网、人民网、新华网、凤凰网等二十余家媒体报道，产生了较大经济和社会效益。MOPT 在 Google 模糊测试公开评测平台上位列第一名（截至 2021 年 1 月)；相关漏洞挖掘系统在实际系统和软件中发现漏洞 400 余个，包括工业 PLC 漏洞数十个，IoT 设备固件漏洞 100 余个，IoT 协议漏洞（缺陷）100 余个，已获得 CVE 100 余个，形成了较大影响力。曾获美国著名高校弗吉尼亚理工学院（Virginia Tech)、凯斯西储大学（Case Western Reserve University)、里海大学（Lehigh University)、佐治亚大学（University of Georgia）终身教职系列（Tenure-Track）助理教授职位，获中国国家优秀留学生奖、**网络系统安全领域 CCF A 类顶级会议 ACM CCS 2021 最佳论文奖**等 10 项最佳论文奖、ELSEVIER 高引论文奖、《计算机研究与发展》高引论文奖、华为优秀技术成果奖、浙江大学先进工作者、“个推”青年创新奖等。

张旭鸿，获美国中佛罗里达大学计算机工程博士学位，现任浙江大学百人计划研究员，兼任浙江大学滨江研究院百人计划研究员、服务安全与可靠性研究中心主任。先后作为项目负责人在研青年科学基金项目 1 项，中科院软件所横向项目 1 项；骨干参与亿级项目 1 项，国家重点研发项目 1 项，华为科研基金 2 项，美国 NSF 项目 2 项。致力于数据驱动的系统安全、人工智能与安全、大数据系统与分析的研究。目前已发表国际高水平论文 30 余篇(如 ACM CCS、USENIX Security、NDSS、ASE、VLDB、ICDE、TDSC、TPDS 等)，其成果获得国际同行认可。研制了对抗文本检测系统 TextShield、互联网平台智能风控与安全治理技术、海量异构物联网系统的智能化漏洞检测与安全分析系统、工业互联网安全风险感

知与智能化检测技术等，并在大型平台实际部署应用，取得了较好的社会和经济效益，被主流媒体多次报道。在 LinkedIn 任职期间，作为团队核心成员，领导研发了新一代端到端大规模自动化分布式机器学习平台，应用于多项产品（包括工作推荐，人才搜索等），覆盖 6 亿用户，3 千万个公司，2 千万个职位，提升机器学习生产效率近一倍；同时负责公司深度学习平台的设计与研发，促使公司多项产品由深度学习模型驱动，取得了较好的社会和经济效益；提出的亿级 ID 表征学习算法，应用于 LinkedIn 工作推荐服务，在不损失精度的情况下，比上一代模型体积减少近 100 倍，消耗的训练资源减少近 100 倍；相关成果获 3 项美国专利，并开源一套人工智能数据处理系统。

Raheem Beyah 教授（合作研究）. Dr. Raheem Beyah serves as Georgia Tech's Vice President for Interdisciplinary Research, Executive Director of the Online Masters of Cybersecurity program (OMS Cybersecurity), and is the Motorola Foundation Professor in School of Electrical and Computer Engineering. He has held several other leadership roles including chairing ECE's Computer Systems and Software Technical Interest Group (2015-2017), serving as ECE's Associate Chair for Strategic Initiatives and Innovation (2016-2018), and serving as the Interim Steve W. Chaddick ECE School Chair during the 2018-2019 academic year. He leads the Communications Assurance and Performance Group (CAP) and is affiliated with the Institute for Information Security & Privacy (IISP). He is also the Co-Founder of Fortiphyd Logic, Inc. His research interests include Network security and monitoring, Cyber-physical Systems Security, Network traffic characterization and performance, and Critical infrastructure security. He received the National Science Foundation CAREER award in 2009 and was selected for DARPA's Computer Science Study Panel in 2010. He is a member of AAAS, ASEE, and a lifetime member of NSBE, a senior member of IEEE, and an ACM Distinguished Scientist.

承担的主要项目

项目名称	项目性质及来源
分布式学习中的数据安全基础理论	国家重点研发计划项目
面向攻击链的 APT 智能检测与溯源方法及关键技术	国家自然科学基金重点项目

研究	
***技术	重点项目
***研究	重点项目
人工智能安全与鲁棒性	国家重点项目
物联网固件漏洞挖掘与隐私防护技术研究	中央高校基础研究基金
可信人工智能模型与关键技术	华为科研项目
人工智能驱动的模糊测试技术研究	中央高校基础研究基金
海量多源异构数据的使用授权与鉴权体系研究	国家自然科学基金重点项目
机器学习安全与隐私保护研究	浙江省杰青项目
人工智能安全研究	国家重点研发计划项目-课题
基于电商大数据的反作弊对抗学习理论与关键技术	国家自然科学基金面上项目
区块链关键技术研究与技术交易应用	浙江省科技计划项目
工控拟态安全网关研发与应用-工控网关拟态防御技术研究	浙江省科技计划项目
深度神经网络的模型可解释性研究项目	华为科研项目
高维稀疏数据对抗学习	蚂蚁金服科研项目
终端系统安全证明验证测试服务	中科院软件所
基于模糊测试的智能化漏洞挖掘技术研究	CCF-绿盟“鲲鹏”科研基金项目
基于增量学习的异常行为检测理论与关键技术研究	CCF-启明星辰“鸿雁”科研基金
基于大规模图挖掘的对抗学习理论与关键技术研究	阿里巴巴集团研究项目
社交反欺诈模型研究	拍拍贷
社交大数据隐私保护理论与技术	CCF-腾讯“犀牛鸟”科研基金

主要研究成果：

请见： https://nesa.zju.edu.cn/