《计算机学报》“人工智能系统安全与攻防技术”征稿

人工智能近年来迅猛发展，核心产业规模日益壮大。以人工智能系统为代表的新技术赋能新业态、新模式，为全球经济复苏注入强劲动力。但是，人工智能系统也面临着严峻的安全与隐私挑战，时刻威胁着人工智能系统的正常发展。同时，这些威胁会随着人工智能技术的普及和发展愈演愈烈，核心攻防技术问题亟待解决。

目前，人工智能系统中存在多种安全与隐私攻击，如数据投毒攻击、后门攻击、成员推理攻击等，这些攻击对人工智能系统的安全与隐私带来严重的冲击。此外，人工智能系统的多样性和对社会伦理方面的影响，都会增加人工智能安全攻防的难度，亟需围绕这些严峻的安全攻防问题开展工作。

因此，为进一步推动我国在人工智能系统安全与攻防领域的研究，《计算机学报》拟征集“人工智能系统安全与攻防技术”方面的研究型论文，并结集出版。征稿内容包括以下但不局限于以下方向：

1.人工智能攻击检测与防御技术
2.人工智能系统安全性分析与验证
3.人工智能系统的漏洞挖掘技术
4.人工智能系统的自动化验证和测试
5.人工智能系统隐私风险评估
6.人工智能系统模糊测试技术
7.模型可解释性理论与方法技术
8.人工智能计算框架安全分析与检测
9.联邦学习和多方安全计算
10.联邦学习模型鲁棒性技术研究

征稿对象为高等院校师生、科研院所及企业科研人员，稿件类型为研究型论文。稿件提交后将经同行评议，择优录用，正刊结集发表（预计会在 2023 年底或次年上半年）。

投稿截止时间为 2023 年 6 月 30 日。

本次活动责任专家为：张玉清、陈恺、付安民、纪守领、刘奇旭

注意事项：

（1）投稿方法：投稿时，投稿领域，请选择“人工智能安全与攻防技术”。

（2）为便于审读，要求稿件符合学报征稿指南要求，可读性强，条理清楚，无中英文语法错误。为了便于快速处理稿件，投稿论文应规范。 稿件彻底准备好后再注册，注册后请马上提交稿件（小于 4M）及投稿声明扫描件（小于 4M），不要先注册后隔段时间再提交。