ACM Journals

CALL FOR PAPERS

ACM Transactions on Autonomous and Adaptive Systems

Special Issue on Trustworthy Security and Privacy-AI Powered Autonomous Driving

Guest Editors:

- **Dr. Guowen Xu**, City University of Hong Kong, Hong Kong. guowenxu@cityu.edu.hk
- **Prof. Hongwei Li,** University of Electronic Science and Technology of China, China. hongweili@uestc.edu.cn
- **Prof. Rongxing Lu,** University of New Brunswick, Canada. RLU1@unb.ca

As artificial intelligence (AI) technology relentlessly innovates and integrates even more deeply with autonomous driving technology, AI-powered autonomous driving is rapidly finding extensive applications across a wide range of domains. These applications encompass driverless transportation and automated logistics, all of which leverage its increasing intelligence, efficiency, and automation capabilities. Nevertheless, owing to the inherent inexplicability and immaturity of AI technology, AI-powered autonomous driving inevitably faces potential security and privacy concerns throughout its training and decision-making phases. Simultaneously, the distinct attributes of AI-powered autonomous driving, such as its intricate system complexity, limited interpretability in AI decision-making, and the diverse array of perception data from various sources, pose formidable challenges to existing security and privacy protection technologies. These challenges manifest in issues such as concealed attacks, the need for universally applicable defense mechanisms, and the efficacy of privacy safeguards. In simpler terms, the current attack methods targeting AI-powered autonomous driving systems are simplistic and lack adequate concealment, while the corresponding defense measures exhibit limited effectiveness and scalability. Moreover, in the realm of privacy protection, existing technology falls short of meeting the real-time decision making demands which is crucial for AI-powered autonomous driving systems.

The special issue calls for high-quality research contributions addressing foundational, engineering, and technological aspects supporting the development, management, control, and evolution of long-lived trustworthy security and privacy AI-powered of autonomous driving systems. We cordially invite the submission of high-quality original papers, covering fundamental research, experience reports, case studies from leading researchers actively contributing to the emerging field of trustworthy security and privacy of AI-powered autonomous and/or self-adaptive driving with human-AI teaming.

Topics

Topics of interests include, but are not limited to

- Innovative models, design, architectures, and development methods for secure and privacy-aware AI-powered autonomous driving systems, including novel self-adaptive computing and control modalities with human-AI teaming
- Rigorous testing, verification and model checking methods for secure and privacy-aware AI-powered autonomous driving systems, including self-adaptive control modalities with human-AI teaming
- Privacy-preserving training for AI-powered autonomous driving
- Privacy-preserving AI-powered autonomous driving fine-tuning
- Adversary example attacks and defenses on AI-powered autonomous driving
- Backdoor attacks and defenses on AI-powered autonomous driving systems
- Data poisoning attacks and its mitigation on the training data of AI-powered autonomous driving systems
- Certified robustness and explainable theory and practice for AI-powered autonomous driving systems
- Ownership and intelligence property protection for AI-powered autonomous driving systems
- Trusted hardware execution environment for AI-powered autonomous driving systems
- Practical and privacy-preserving inference on AI-powered autonomous driving systems
- Fine-grained access control for AI-powered autonomous driving systems
- Attacks in Human-in-the-loop/Human-AI teaming for AI-powered autonomous driving systems
- Security bugs identification and testing on AI-powered autonomous driving systems
- Self-adaptive security and privacy of AI-powered autonomous driving systems
- Attacks and defenses for LLM-inspired autonomous driving systems
- Ethics and responsibility in the design, control, testing, and verification of autonomous driving systems
- Futuristic and hypothetical studies supported by rigorous theoretical formulation, experimentation, and proof-of-concept

Important Dates

- Submissions deadline: August 20, 2024
- First-round review decisions: October 20, 2024
- Deadline for revision submissions: November 20, 2024
- Notification of final decisions: December 20, 2024
- Tentative publication: February 20, 2025

Submission Information

Authors are invited to submit high quality manuscripts and rigorous contributions reporting important developments in the topics related to the special issue. Papers should describe original and well-evaluated research that is not published nor currently under review by other journals or conferences. Parallel submissions will not be accepted.

Guest editors will prescreen submitted manuscripts for their suitability in the issue and TAAS. Submissions passing the prescreen process will go through a rigorous peer-review process according to the standards of ACM TAAS. Submitting a paper implies the willingness of reviewing one paper submitted to the special issue.

The manuscripts should be formatted according to the ACM TAAS guidelines available from the journal homepage (https://dl.acm.org/journal/taas/author-guidelines), including templates, CCS, author rights, language services, and others. All papers should be submitted online: https://mc.manuscriptcentral.com/taas, where the Special Issue: “Trustworthy Security and Privacy-AI Powered Autonomous Driving” should be selected.

For questions and further information, please contact **Guowen Xu/guowenxu@cityu.edu.hk.**