The Third IEEE International Workshop on Assured Autonomy, Artificial Intelligence and Machine Learning (WAAM 2024)

October 30, 2024

Part of The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications

http://www.sis.pitt.edu/lersais/conference/tps/2024/

October 28-30, 2024. The Darcy Hotel, Washington D.C., USA

Description

Artificial intelligence (AI) and Machine Learning (ML) systems are increasingly seen in many domains such as self-driving land vehicles, autonomous aircraft, and medical systems. AI systems should equal or surpass human performance, but given the consequences of failure in these systems, how do we determine that the data gathered to train an AI system is suitably representative of the real world? How do we assure the public that these systems work as intended and will not cause harm? This year, the workshop will focus on **security and AI/ML systems**.

The workshop will explore various issues of AI/ML systems and security, including but not limited to: secure design of AI/ML systems, adversarial AI, using AI/ML to secure other systems, and using AI/ML for post incident analysis. Research, experiences and best practices will be discussed to illustrate the challenges and approaches to assured autonomy. Finally, the road ahead will be explored.

This workshop will bring together researchers from government, industry and academia to discuss these challenging issues. **The workshop will be in the form of panel discussions and invited presentations. While the panelist and presenters are invited only, any conference attendee is welcome to attend the workshop.**

A summary of the findings of the Workshop will appear in IEEE *Computer* magazine and IEEE *Reliability* magazine.

Workshop Organizers

Phil Laplante, NIST phillip.laplante@nist.gov
Rick Kuhn, NIST rkuhn@nist.gov

This workshop is sponsored by the IEEE Reliability Society