The AAAI-22 Workshop on

Artificial Intelligence for Cyber Security (AICS)

February 28 or March 1, 2022
Vancouver, BC, Canada

Part of the 36th AAAI Conference on Artificial IntelligenceAssociation
https://aaai.org/Conferences/AAAI-22/

CALL FOR PARTICIPATION

AICS Workshop Description

The workshop will focus on the application of AI to problems in cyber-security. Cyber systems generate large volumes of data, utilizing this effectively is beyond human capabilities. Additionally, adversaries continue to develop new attacks. Hence, AI methods are required to understand and protect the cyber domain. These challenges are widely studied in enterprise networks, but there are many gaps in research and practice as well as novel problems in other domains.

This year the AICS emphasis will be on practical considerations in the real world when deploying AI systems for security with a special focus on convergence of AI and cyber-security in the biomedical field.

In general, AI techniques are still not widely adopted in the real world. Reasons include: (1) a lack of certification of AI for security, (2) a lack of formal study of the implications of practical constraints (e.g., power, memory, storage) for AI systems in the cyber domain, (3) known vulnerabilities such as evasion, poisoning attacks, (4) lack of meaningful explanations for security analysts, and (5) lack of analyst trust in AI solutions. There is a need for the research community to develop novel solutions for these practical issues.

The biomedical space has seen a flurry of activity recently, and cyber criminals have amplified their efforts with health-related phishing attacks, spreading misinformation, and intruding into health infrastructure. These lead to security considerations: (1) securing personal health information, genetic material, intellectual property, and digital health records, (2) balancing privacy rights and data ownership concerns in solutions using network and mobile data, (3) defending AI for biology use cases to deter automated attacks at scale.

Workshop Topics

Topics of interest in the biomedical space include:

- Securing personal information, genomics, and intellectual property
- Adversarial attacks and defenses on biomedical datasets
- Detecting and preventing spread of misinformation
- Usable security and privacy for digital health information
- Phishing and other attacks using health information
- Novel use of biometrics to enhance security
- Threats to biometric security

Topics of general interest to cyber-security include:

- Machine learning (including RL) security and resiliency
  - Natural language processing
  - Anomaly detection
  - Noise reduction
  - Adversarial learning
- Formal reasoning
- Game-theoretic reasoning
- AI assurance and securing AI systems
- Multi-agent interaction modeling
- Modeling and simulation of cyber systems
- Decision-making under uncertainty
- Automation of data labeling and ML techniques
- Quantitative human behavior models
- Operational and commercial applications of AI
- Explanations of security decisions and vulnerability of explanations
- Human-AI teaming for cyber security

Paper Format

Full-length papers (up to overall 9 pages in AAAI format.

Submissions are not anonymized. Please submit PDF via AICS Workshop website by **November 12, 2021.**

Publication

AAAI does not publish workshop proceedings; acceptance to the workshop does not preclude submissions to other conferences. The workshop proceedings will be put on arxiv.

Workshop URL

http://aics.site/AICS2022/index.html

Workshop Organizers

- Tamara Broderick, MIT CSAIL, USA
- James Holt, Laboratory for Physical Sciences, USA
- Edward Raff, Booz Allen Hamilton, USA
- Ahmad Ridley, National Security Agency, USA
- Dennis M. Ross, MIT Lincoln Laboratory, MA, USA
- Arunesh Sinha, Singapore Management University, Singapore
- Diane P. Staheli, MIT Lincoln Laboratory, MA, USA
- William W. Streilen, MIT Lincoln Laboratory, MA, USA
- Milind Tambe, Harvard University, MA, USA
- Yevgeniy Vorobeychik, Washington University in Saint Louis, USA
- Allan Wollaber, MIT Lincoln Laboratory, USA