The AAAI-17 Workshop on Artificial Intelligence for Cyber Security (AICS)

February 4, 2017
San Francisco, California, USA

Part of the Association for the Advancement of Artificial Intelligence 2017 Conference
http://www.aaai.org/Conferences/AAAI/aaai17.php

CALL FOR PARTICIPATION

AICS Workshop Description
The workshop will focus on research into the use of Artificial Intelligence (AI) for cyber security, including machine learning, game theory, natural language processing, knowledge representation, and automated and assistive reasoning. The workshop will emphasize the application of AI techniques that enable resilience in cyber security systems in operational or mission settings.

Recent improvements in AI have resulted in advances in many technological and scientific fields including medicine, transportation, communication and data analysis. In these cases, AI techniques have assisted humans in several ways, including, dealing with large amounts of information (i.e., Big Data), recognizing abnormal behavior or trends and making complex decisions. Despite its success in these other areas, AI has yet to have a similar level of impact on cyber security. Cyber security faces many of the same challenges as these other areas, and thus, AI has the potential to have similar impact if applied in appropriate ways.

One key way in which AI can benefit cyber security is by enabling security analysts to focus on relevant signals in large amounts of situational awareness data. AI techniques that can be trained to remove unwanted data or ‘noise’ and improve the analysts’ ability to understand their cyber environment and detect anomalous activity. Another way AI can benefit cyber security is through the use of automated techniques to generate cyber courses of action (COAs) in response to cyber threats. Game theoretic reasoning and agent-based modeling techniques can be used to explore potential attacker-defender interactions and their associated outcomes in order to evaluate candidate solutions and to inform decision makers.

The above applications of AI have the potential to impact cyber security in a positive way, bringing automated learning and game theory into the service of improved system resilience. Developing and applying these and other AI capabilities to cyber security problems requires collaboration amongst several different communities including the artificial intelligence, game theory, machine learning and cyber-security communities, as well as the operational and commercial applications communities. This workshop is structured to encourage a lively exchange of ideas between researchers and practitioners in these communities from the academic, public and commercial sectors.

Workshop Topics
Topics of interest include, but are not limited to:

- Machine learning approaches to make cyber systems secure and resilient
  - Natural language processing techniques
  - Anomaly/Threat detection techniques
  - Big Data noise reduction techniques
  - Human behavioral modeling
- Formal reasoning, with focus on human element, in cyber systems
- Game Theoretic reasoning in cyber security
- Economics of cyber security
- Multi-agent interaction/agent-based modeling in cyber systems
- Modeling and simulation of cyber systems and system components
- Decision making under uncertainty in cyber systems
- Automated security aids for system administrators
- Operational and commercial applications of AI for cyber security

Mini-Challenge
For information on this year’s mini-challenge:
http://www-personal.umich.edu/~arunesh/AICS2017/

Workshop Format
Invited speakers, presentations, panel and group discussions

Submission Requirements
Two formats are solicited:
- Full-length papers (up to 8 pages in AAAI format), or
- Challenge or position papers (2 pages in AAAI format)

Submissions are not anonymized. Please submit PDF via AICS Workshop website. The deadline to submit papers has been extended to November 14, 2016.

Workshop URL
http://www-personal.umich.edu/~arunesh/AICS2017/

Publication
Accepted papers will be published in the workshop proceedings.

Workshop Co-Chairs
- William W. Streilein, MIT Lincoln Laboratory, MA, USA
- Robert Laddaga, Institute for Software Integrated Systems, Vanderbilt University, TN, USA
- David R. Martinez, MIT Lincoln Laboratory, MA, USA
- Arunesh Sinha, University of Michigan, MI, USA
- Neal Wagner, MIT Lincoln Laboratory, MA, USA

Workshop Program Committee
- George Cybenko, Dartmouth College
- Christos Dimitrakakis, Chalmers University of Technology, Sweden
- Robert Goldman, Smart Information Flow Technologies (SIFT)
- Christopher Kiekintveld, University of Texas at El Paso
- Brian Lindauer, Software Engineering Institute/Carnegie Mellon University
- Richard Lippmann, MIT Lincoln Laboratory
- Mingyan Liu, University of Michigan
- Daniel Lowd, University of Oregon
- Ranjeev Mittu, Naval Research Laboratory
- Diane Oyen, Los Alamos National Laboratory
- Benjamin Rubinstein, University of Melbourne, Australia
- Howard Shrobe, MIT/CSAIL
- Milind Tambe, University of Southern California
- Robert Templeman, Navy Surface Warfare Center, Crane Division

Administrative Contact
Jennifer Robinson, MIT Lincoln Laboratory
Voice: 781-981-7500, Email: Jennifer.Robinson@ll.mit.edu

http://www.aaai.org/Conferences/AAAI/aaai17.php