CALL FOR PARTICIPATION

AICS Workshop Description
The workshop will focus on research and applications of artificial intelligence to cyber security, including machine learning, game theory, natural language processing, knowledge representation, and automated and assistive reasoning. The workshop will emphasize cyber systems and research on techniques to enable resilience in cyber security systems augmented by human-machine interactions.

The human in the loop has been recognized as a common point of weakness in the defense of cyber systems by the cyber security community. One promising approach to mitigate this problem is to build models of human behavior and enable formal reasoning about how human beings interact with cyber systems. Game theory, in particular, has been used to model human behavior and leveraging game-theoretic models of defense for physical security, to suggest incentives and punishments that can be used to induce more secure behavior. Another promising approach is to design automated tools that can perform the task of the human in the loop. This approach mitigates security issues arising from sub-optimal security decision taken by humans. Further, automated tools can be formally specified more precisely, and with stronger guarantees, than human behavior; this enables stating and proving formal guarantees about security of the overall cyber-system.

Both of the above techniques for understanding how humans and systems interact have been extensively studied in AI, but not in the context of cyber security. Addressing these challenges requires collaboration between several different research and development communities including the artificial intelligence, cyber-security, game theory, machine learning and formal reasoning communities.

Workshop Topics
Topics of interest include, but are not limited to:
- Machine learning approaches to make cyber systems secure
  - Natural language processing techniques
  - Anomaly/Threat detection 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 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
- Quantitative human behavior models with application to cyber security

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)
- Challenge or position papers (2 pages in AAAI format)

Submissions are not anonymized. Please submit PDF via AICS Workshop website by October 23, 2015

Workshop URL
http://www-bcf.usc.edu/~aruneshs/AICS2016/index.html

Publication
Accepted papers will be published in the workshop proceedings.

Workshop Co-Chairs
- David R. Martinez, MIT Lincoln Laboratory, MA, USA
- William W. Streilein, MIT Lincoln Laboratory, MA, USA
- Kevin M. Carter, MIT Lincoln Laboratory, MA, USA
- Arunesh Sinha, University of Southern California, CA, USA

Workshop Program Committee
- George Cybenko, Dartmouth College
- Christos Dimitrakakis, Chalmers University of Technology, Sweden
- Christopher Kiekintveld, University of Texas at El Paso
- Robert Laddaga, DARPA/Information Innovation Office
- Richard Lippmann, MIT Lincoln Laboratory
- Mingyan Liu, University of Michigan
- Daniel Lowd, University of Oregon
- Christopher Miller, Smart Information Flow Technologies (SIFT)
- Katerina Mitrokotsa, Chalmers University of Technology, Sweden
- Ranjeev Mittu, Naval Research Laboratory
- Howard Shrobe, MIT/CSAIL

Administrative Contact
Cynthia Devlin-Brooks
MIT Lincoln Laboratory
Voice: 781-981-7501
Email: Cynthia.Devlin-Brooks@ll.mit.edu