The applications of artificial intelligence, machine learning, and data mining for security and privacy problems continues to grow. One recent trend is the growth of Big Data Analytics and the establishment of Security Information and Event Management systems built to obtain security intelligence and situational awareness. With the advent of cloud-computing, every advantage the cloud offers, such as large-scale machine learning and data-driven abuse detection, is being leveraged to improve security.

We invite original research papers describing the use of AI or machine learning in security and privacy problems. We also invite position and open problem papers discussing the role of AI or machine learning in security and privacy. Submitted papers of these types may not substantially overlap papers that have been published previously or that are simultaneously submitted to a journal or conference/workshop proceedings. Finally we welcome a new systematization of knowledge category of papers this year, which should distill the AI or machine learning contributions of a previously published series of security papers.

Regular research, systematization of knowledge, and open/position paper submissions must be at most 10 pages in double-column ACM format (note: pages must be numbered) excluding the bibliography and well-marked appendices, and at most 12 pages overall. Committee members are not required to read the appendices, so the paper should be intelligible without them. Submissions need not be anonymized. We recommend the use of the ACM SIG Proceedings templates for submissions. The ACM format is the required template for the camera-ready version. Accepted papers will be published by the ACM Digital Library and/or ACM Press.

Submissions can be made through EasyChair using the following link: http://www.easychair.org/conferences/?conf=aisec2012

Topics of interest include, but are not limited to:

- Adversarial Learning
- Robust Statistics
- Online Learning
- Computer Forensics
- Spam detection
- Botnet detection
- Intrusion detection
- Malware identification
- Big data analytics for security
• Adaptive side-channel attacks
• Privacy-preserving data mining
• Design and analysis of CAPTCHAs
• Phishing detection and prevention
• AI approaches to trust and reputation
• Vulnerability testing through intelligent probing (e.g. fuzzing)
• Content-driven security policy management & access control
• Techniques and methods for generating training and test sets
• Anomalous behavior detection (e.g. for the purposes of fraud prevention, authentication)

**Schedule**
Submissions due: July 16, 2012 (23:59 PDT)
Acceptance notification: August 13, 2012
Final manuscript due: August 24, 2012
Workshop date: October 19, 2012

**Organization**

**General Chair**
Ting Yu (North Carolina State University)

**Program Co-Chairs**
Alvaro A. Cárdenas (Fujitsu Laboratories of America)
Blaine Nelson (University of Tübingen)
Benjamin I. P. Rubinstein (Microsoft Research)

**Program Committee**
Christos Dimitrakakis (Frankfurt Institute for Advanced Studies)
Mario Frank (UC Berkeley)
Giorgio Giacinto (University of Cagliari)
Rachel Greenstadt (Drexel University)
Guofei Gu (Texas A&M University)
Ling Huang (Intel Labs)
Anthony D. Joseph (UC Berkeley)
Murat Kantarcioğlu (UT Dallas)
Latifur Khan (UT Dallas)
Pavel Laskov (University of Tübingen)
Justin Ma (UC Berkeley)
Aikaterini Mitrokotsa (EPFL)
Konrad Rieck (University of Göttingen)
Fabio Roli (University of Cagliari)
Elaine Shi (UC Berkeley)
Robin Sommer (ICSI and LBNL)
Natalia Stakhanova (University of South Alabama)
Jessica Staddon (Google)
J. D. Tygar (UC Berkeley)
Sobha Venkataraman (ATT Research)