Summary/Overview for Artificial Intelligence and Security (AISec'13)

Blaine Nelson
University of Potsdam
Building 4, Office 0.20
August-Bebel-Str. 89
14482 Potsdam, Germany
bnelson@cs.uni-potsdam.de

Christos Dimitrakakis
Computer Science and Engineering
Chalmers University
SE-4172
chrdimi@chalmers.se

Elaine Shi
Department of Computer Science
University of Maryland
A.V. Williams Building
College Park, MD 20742
runting@cs.cmu.edu

ABSTRACT

The Workshop on Artificial Intelligence and Security (AISec) focuses on the theory and application of Artificial Intelligence (AI) and machine learning in adversarial settings such as security and privacy applications and conversely, the security and privacy implications arising through the use of large-scale AI methods. The workshop serves as the premier venue for this particular fusion of application, algorithms, and theory and continues to attract submissions from a diverse set of researchers, who address newly arising problems within this ever growing field. AISec provides a forum for researchers within the security, privacy, AI, and learning communities to discuss the role that intelligent technologies play in security and privacy applications and to present the unique needs of these problems to the AI and learning communities.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security and protection (e.g., firewalls)*; D.4.6 [**Operating Systems**]: Security and Protection; I.2.6 [**Artificial Intelligence**]: Learning; I.2.7 [**Artificial Intelligence**]: Natural Language Processing; I.2.8 [**Artificial Intelligence**]: Problem Solving, Control Methods, and Search; K.4.1 [**Computers and Society**]: Public Policy Issues—*privacy*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Algorithms,Security,Theory

Keywords

Artificial Intelligence, Computer Security, Machine Learning, Computer Privacy, Secure Learning

AISec'13, November 4, 2013, Berlin, Germany.
ACM 978-1-4503-2488-5/13/11 ...$15.00.
http://dx.doi.org/10.1145/2508859.2509031

1. BACKGROUND AND MOTIVATION

The potential application of artificial intelligence (AI), machine learning (ML), and data mining to security and privacy problems is ever-expanding. The analytic tools and intelligent behavior provided by these techniques makes AI and learning increasingly important for autonoumous real-time decision-making in domains with a wealth of data or that require quick reactions to ever-changing situations. Particularly, these intelligent technologies offer new solutions to security problems involving *big-data* analysis scaled through cloud-computing. The use of learning methods in security-sensitive domains creates new frontiers for security research, in which adversaries may attempt to mislead or evade intelligent machines. The AISec workshop provides a venue for presenting and discussing new developments in this fusion of security/privacy with AI and machine learning.

AISec, in its sixth consecutive year with CCS, is the premier meeting place for researchers interested in the junction of security, privacy, AI and ML. The past year witnessed intense activity within the AISec community – first with a Dagstuhl workshop followed by the fifth AISec workshop. There are several reasons for this surge. Firstly, machine learning, data mining, and other AI technologies play a key role in extracting knowledge, situational awareness, and security intelligence from *big-data*. Secondly, data-centric companies like Google and Amazon are increasingly exploring and deploying learning technologies to address *big-data* problems for their customers. Finally, these trends are increasingly exposing companies and their customers to intelligent technologies. As a result, these learning technologies are being explored by researchers as potential solutions to security/privacy problems, but also as new potential privacy/security vulnerabilities that need to be secured.

2. WORKSHOP OBJECTIVE

The AISec Workshop serves as a venue where practical security problems merge with advances in AI and ML. In doing so, researchers also are developing theory and analytics unique to this domain and are exploring diverse topics including learning in game-theoretic adversarial environments, privacy-preserving learning, and applications to spam and intrusion detection. AI and ML provide a set of useful analytic and decision-making techniques that are being leveraged by an ever-growing community of practitioners, including in applications with security-sensitive elements. However, while security researchers often utilize such techniques to address problems and AI/ML researchers develop techniques for *big-data* analytics, those communities can only devote limited attention to the other: Within security research, AI/ML components are usually regarded as black-box solvers. Conversely, the learning community seldom considers the security/privacy implications that application of their algorithms entails. While these two communities generally focus on different directions, where these two fields do meet, interesting new problems appear. These have already raised many novel questions for both communities and created a new branch of research known as secure learning. Within this intersection, the AISec Workshop has become the primary venue for this unique fusion of research.

3. TOPICS OF INTEREST

In terms of author audience, we solicited paper submissions with the following (but not limited to) research topics:

Learning Theory Topics related to Security

- Adversarial learning
- Robust statistics
- Online learning
- Learning in stochastic games

Security Applications

- Computer forensics
- Spam detection
- Phishing detection and prevention
- Botnet detection
- Intrusion detection and response
- Malware identification
- Authorship identification
- Big-data analytics for security

Security-related AI problems

- Distributed inference and decision-making for security
- Secure multiparty computation and cryptographic approaches
- Privacy-preserving data mining
- Adaptive side-channel attacks
- Design and analysis of CAPTCHAs
- AI approaches to trust and reputation
- Vulnerability testing through intelligent probing (*e.g.*, fuzzing)
- Content-driven security policy management and access control
- Techniques and methods for generating training and test sets
- Anomalous behavior detection (*e.g.*, for the purposes of fraud prevention, authentication)

4. PROGRAM COMMITTEE

We are thankful to the members of our program committee:

- Battista Biggio, University of Cagliari, Italy
- Ulf Brefeld, Technische Universitüt Darmstadt, Germay
- Michael Brückner, Amazon.com Inc, Germany
- Mike Burmester, Florida State University, USA
- Alvaro A. Cárdenas, University of Texas at Dallas, USA
- Mario Frank, University of California, Berkeley, USA
- Rachel Greenstadt, Drexel University, USA
- Guofei Gu, Texas A&M University, USA
- Ling Huang, Intel Labs, USA
- Anthony Joseph, University of California, Berkeley, USA
- Ari Juels, RSA Labs, USA
- Pavel Laskov, University of Tübingen, Germany
- Daniel Lowd, University of Oregon, USA
- Pratyusa Manadhata, HP Labs, USA
- Aikaterini Mitrokotsa, Chalmers University of Technology, Sweden
- Roberto Perdisci, University of Georgia, USA
- Vasyl Pihur, Google Inc., USA
- Konrad Rieck, University of Göttingen, Germany
- Fabio Roli, University of Cagliari, Italy
- Benjamin I. P. Rubinstein, IBM Research, Australia
- Robin Sommer, ICSI and LBNL, USA
- Nina Taft, Technicolor, USA
- J. D. Tygar, University of California, Berkeley, USA
- Shobha Venkataraman, AT&T Research, USA
- Ting-Fang Yen, RSA Labs

5. WORKSHOP ORGANIZERS

Blaine Nelson is a postdoctoral researcher at the University of Potsdam. He previously was a postdoctoral research fellow at the University of Tübingen and he obtained his Ph.D. from the University of California, Berkeley. He was a co-chair of the AISec 2012 and was a co-organizer of the Dagstuhl Workshop entitled "Machine Learning Methods for Computer Security" in 2012. His research focuses on learning algorithms particularly in the context of security-sensitive application domains. He investigates the vulnerability of learning to security threats and how resilient learning techniques can be used to mitigate such security threats.

Christos Dimitrakakis is a researcher at Chalmers University of Technology. His main research interest is decision theory, including reinforcement learning and problems in security applications. He obtained his Ph.D. in 2006 from EPFL, and was a researcher at the universities of Leoben, Amsterdam and Frankfurt. Most recently he was a Marie Curie Fellow at EPFL. He has co-organised a workshop on Privacy, Security, Data Mining and Machine Learning (PSDML) in conjunction with ECML 2010.

Elaine Shi is an Assistant Professor in the Computer Science Department at University of Maryland, College Park. Her research combines systems security, cryptography, and data mining to design new computing systems that are secure and privacy-preserving. Dr. Shi obtained her Ph.D. from the Computer Science Department at Carnegie Mellon University in 2008. Prior to joining UMD, she was a Member of Research Staff at Xerox PARC, and a research scientist at UC Berkeley. Elaine Shi has served on the program committees of more than 25 conferences and workshops, and is also currently co-chairing a cloud security workshop under AsiaCCS. She has helped organize an NSF/Intel sponsored security curriculum workshop, and the Cross-Disciplinary Conversations session for the SaTC PI meeting in 2012.