10th International Workshop on Artificial Intelligence and Security (AISec 2017)

Battista Biggio
University of Cagliari
battista.biggio@diee.unica.it

David Freeman
Facebook, Inc.
dfreeman@fb.com

Brad Miller
Google Inc.
bradmiller@google.com

Arunesh Sinha
University of Michigan
arunesh@umich.edu

KEYWORDS

Adversarial Learning, Secure Learning, Malware Detection

BACKGROUND

Artificial Intelligence (AI) and Machine Learning (ML) provide a set of useful analytic and decision-making techniques that are being leveraged by an ever-growing community of practitioners, including many whose applications have security-sensitive elements. However, while security researchers often utilize such techniques to address problems and AI/ML researchers develop techniques for Big Data analytics applications, neither community devotes much 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 entailed in the application of their algorithms when they are designing them. While these two communities generally focus on different directions, where these two fields do meet, interesting problems appear. Researchers working in this intersection have raised many novel questions for both communities and created a new branch of research known as secure learning. The AISec workshop has become the primary venue for this unique fusion of research.

In recent years, there has been an increase of activity within the AISec/secure learning community. There are several reasons for this surge. Firstly, machine learning, data mining, and other artificial intelligence technologies play a key role in extracting knowledge, situational awareness, and security intelligence from Big Data. Secondly, industry is increasingly exploring and deploying learning technologies to address Big Data problems for their customers. Finally, these trends are increasingly exposing companies and their customers/users to intelligent technologies. As a result, these learning technologies are being explored by researchers both as potential solutions to security/privacy problems and also as a potential source of new vulnerabilities that need to be addressed. The AISec Workshop meets this need and serves as the sole long-running venue for this topic.

AISec, having been annually co-located with CCS for ten consecutive years, is the premier meeting place for researchers interested in the junction of security, privacy, AI, and machine learning. Its role as a venue has been to merge practical security problems with advances in AI and machine learning. In doing so, researchers also have been developing theory and analytics unique to this domain and have explored diverse topics such as learning in game-theoretic adversarial environments, privacy-preserving learning, and applications to spam and intrusion detection.

AISEC 2017

The tenth annual event in this series, AISec 2017 drew 36 submissions, of which eleven were selected for publication and presentation and approximately four were selected for presentation in a "lightning round." Paper topics included the following:

- **Malware and Intrusion Detection** including approaches to both evasion and improved classification and discovery.
- **Adversarial Learning** spanning evasive and causative attacks from both the attacker and defender perspectives.
- **ML-Powered Attacks** including techniques for defeating security challenges and CAPTCHAs.

The keynote address titled "Beyond Big Data: What Can We Learn from AI Models?" was given by Dr. Aylin Caliskan of Princeton University.

PROGRAM COMMITTEE

- Hyrum Anderson, Endgame, USA
- Sam Bretheim, Craigslist Inc., USA
- Michael Brückner, Amazon.com Inc., Germany
- Alvaro Cárdenas, University of Texas at Dallas, USA
- Nicholas Carlini, University of California, Berkeley, USA
- Clarence Chio, Kaitrust, USA
- Igino Corona, University of Cagliari, Italy
- Anupam Datta, Carnegie Mellon University, USA
- Milenko Drinic, Microsoft Corporation, USA

CCS '17, October 30-November 3, 2017, Dallas, TX, USA
© 2017 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3137048

- Joseph Halpern, Cornell University, USA
- Alex Kantchelian, Google Inc., USA
- Davide Maiorca, University of Cagliari, Italy
- Pratyusa Manadhata, Hewlett Packard Labs, USA
- Patrick McDaniel, Pennsylvania State University, USA
- Katerina Mitrokotsa, Chalmers University, Sweden
- Luis Muñoz González, Imperial College, London, UK
- Michal Nánási, Facebook Inc., UK
- Blaine Nelson, Google, Inc., USA
- Damien Octeau, Google Inc., USA
- Roberto Perdisci, University of Georgia, USA
- Vasyl Pihur, Google Inc., USA
- Konrad Rieck, TU Braunschweig, Germany
- Fabio Roli, University of Cagliari, Italy
- Benjamin Rubinstein, University of Melbourne, Australia
- Tobias Scheffer, Universität Potsdam, Germany
- Michael Tschantz, ICSI, USA
- Doug Tygar, University of California, Berkeley, USA
- Eugene Vorobeychik, Vanderbilt University, USA
- Gang Wang, Virginia Tech, USA

ABOUT THE ORGANIZERS

Battista Biggio received the M.Sc. degree (Hons.) in Electronic Engineering and the Ph.D. degree in Electronic Engineering and Computer Science from the University of Cagliari, Italy, in 2006 and 2010, respectively. Since 2007 he has been with the Department of Electrical and Electronic Engineering, University of Cagliari, where he is currently an Assistant Professor. In 2011, he visited the University of Tübingen, Germany, where he studied the robustness of machine learning to training data poisoning. His research interests include secure machine learning, multiple classifier systems, kernel methods, biometrics, and computer security. Dr. Biggio has served as a reviewer and program committee member for several international conferences and journals, including several AISec editions. He is a senior member of the IEEE and member of the IAPR. He has been recently nominated Associate Editor of Pattern Recognition and chair of the IAPR Technical Committee 1 on Statistical Pattern Recognition Techniques.

David Freeman is a research scientist/engineer at Facebook working on spam and abuse problems. He previously led anti-abuse engineering and data science teams at LinkedIn, where he built statistical models to detect fraud and abuse and worked with the larger machine learning community at LinkedIn to build scalable modeling and scoring infrastructure. He is an author, presenter, and organizer at international conferences on machine learning and security, such as NDSS, WWW and AISec, and is currently writing (with Clarence Chio) a book on Machine Learning and Security to be published by O'Reilly. He holds a Ph.D. in mathematics from UC Berkeley and did postdoctoral research in cryptography and security at CWI and Stanford University.

Brad Miller holds a Ph.D. in Computer Science from the University of California, Berkeley, and has conducted research applying machine learning to problems in security and privacy. In 2015 he joined the SafeBrowsing team at Google, where he works to develop, launch, and land novel machine learning mechanisms to combat phishing and malware on the web. He has received a Best Student Paper award at Privacy Enhancing Technologies Symposium, has served on the program committee for AISec, and has been a reviewer for several journals.

Arunesh Sinha is an Assistant Research Scientist in the Computer Science and Engineering Department at the University of Michigan. He received his Ph.D. from Carnegie Mellon University, where he was advised by Prof. Anupam Datta, and was a postdoctoral scholar with Prof. Milind Tambe at the Computer Science Department of University of Southern California. He was awarded the Bertucci fellowship at CMU in appreciation of his novel research. Dr. Sinha has conducted research at the intersection of security, machine learning and game theory. His interests lie in the theoretical aspects of multi-agent interaction, machine learning, security and privacy, along with an emphasis on the real-world applicability of the theoretical models.