Chairs' Introduction and Welcome to AISec 2016

It is our pleasure to welcome you to the 9th ACM Workshop on Artificial Intelligence and Security — AISec 2016. AISec, having been annually co-located with CCS for nine consecutive years, is the premier meeting place for researchers interested in the intersection 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 2016 drew a record 38 submissions, of which 12 (32%) were selected for publication and presentation. Submissions arrived from researchers in 16 countries, from a wide variety of institutions both academic and corporate. The accepted papers were organized into the following thematic groups:

- **Security Data Sets:** Collection and analysis of data that can serve as a baseline for AI/ML research in security.
- **Machine Learning and Security in Practice:** Systems that use machine learning to solve a particular security problem.
- **Foundations:** Theoretical constructs and best practices for applying machine learning to security.
- **Privacy:** Attacks on user privacy or anonymity, and privacy-preserving constructions of machine learning systems.

The keynote address will be given by Elie Bursztein of Google, Inc., whose talk is entitled, "Why is applying machine learning to anti-abuse so hard?" In this talk, Dr. Bursztein will discuss challenges in the reproducibility of scientific results from machine learning algorithms and what we can do about it. Dr. Bursztein's talk will touch on issues arising from proprietary hardware, dataset availability, adversarial machine learning, and the ethics of data. He will also consider several privacy questions related to machine learning models.

We wish to thank all of the people who made AISec '16 possible, including foremost the authors of all submissions for offering their work to this venue. We are grateful to the program committee for volunteering their time to review papers and engaging in a great deal of constructive discussion. Finally, we thank our colleagues at ACM for taking care of all of the logistics of this workshop.

We hope you find the program informative and we look forward to a workshop full of engaging discussion.

David Mandell Freeman
AISec'16 Program Chair
LinkedIn Corporation, USA

Aikaterini Mitrokotsa
AISec'16 Program Chair
Chalmers University of Technology, Sweden

Arunesh Sinha
AISec'16 Program Chair
University of Michigan, USA