CYBERSEC & AI CONNECTED WORKSHOPS

Call for presentations

Theme: AI for Privacy and Security

Cybersecurity, in accordance with the growing proliferance and complexity of cyberthreats, is among the fastest growing fields of applied computer science. The severity of cyberattacks and cybercrime can only be expected to increase with advances in adversarial AI technology. Industries have no other option than to invest in AI themselves to counter new trends and provide customers with safe cyberenvironments.

But safety is not just about cyberthreats. The exponential spread of computer technology into all areas of human existence has put privacy at the forefront of cybersecurity. The rapid evolution of technology has led to previously unimagined privacy-related consequences. Apart from being an essential ethics problem, privacy is also a notoriously difficult technical challenge which requires original and provably safe solutions across all technological stacks.

ABOUT CYBERSEC & AI CONNECTED

CyberSec & AI Connected is an annual conference where academic and industrial leaders come together to discuss developments at the intersection of AI and cybersecurity. 2019 brought together a stellar group of speakers from industry and academia to discuss and debate these intellectual challenges (see the 2019 conference report and speaker list at **cybersecai.com**).

CYBERSEC & AI CONNECTED WORKSHOPS

A key element of CyberSec & AI Connected will be our technical workshops. Our workshops provide a platform for cybersecurity practitioners and researchers to deep dive into the latest research, case studies, technology, challenges, and opportunities around AI and machine learning in cybersecurity and privacy.

Our Workshop Program Committee is soliciting presentations and tool demonstrations in any aspect of cybersecurity and privacy technology, with particular emphasis on AI-based real-word deployments. In addition, we also seek presentations and tool demonstrations on fundamental and applied research concerning the interplay of AI with cybersecurity and privacy.

avast

CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE

Each author of an accepted workshop submission will be awarded a free registration for the entire CyberSec & AI Connected conference.

TOPICS OF INTEREST

Authors are invited to submit technical presentations covering, but not limited to, the following topics:

Privacy

- *Data anonymity and de-anonymization, censorship-resistant systems*
- *Privacy in AI systems*
- *Theoretical foundations of AI-based privacy preservation*
- *Differential privacy, privacy-preserving AI systems*
- *Security and privacy policies*
- *Privacy-preserving systems*
- *Privacy in social media and online services*
- *Privacy in pervasive sensing*
- *Fairness and privacy of deep learning systems*
- *Location and activity privacy and exposure*
- *Formal verification of privacy properties for AI models*
- *Accountability and anonymity*

Security

- *Malware detection and classification*
- *Spam and phishing detection and filtering*
- *Network security, packet analysis, and intrusion detection*
- *Smart systems, smart cities, and IoT*
- *Computer forensics and embedded system security*
- *Vulnerability detection and exploitation, security modeling*
- *Asset management and infrastructure security*
- *Access control, authentication, and identification*
- *Information integrity*
- *Usability of security in the network*
- *Fair AI technology*
- *Explainability and fairness of AI models*
- *Adversarially robust AI models*
- *Theoretical foundations of AI-based security*
- *Formal verification of security properties for AI models*

HOW TO SUBMIT FOR WORKSHOP PRESENTATIONS

We accept extended abstract submissions of up to two pages, double-column (not including references and appendix), in PDF or Microsoft Word format. Submissions will be reviewed and the best academic and industrial themed submissions will be selected for a 20 minute oral presentation or demonstration, followed by a ten minute Q&A at the respective workshops.

Submissions can be uploaded via our online submission form at **cybersecai.com** or sent via **academia@cybersecai.com** (for academic-themed topics) or **industry@cybersecai.com** (for industry-themed topics).

DEADLINES FOR SUBMISSIONS

The closing date for abstract submissions is 31st May, 2020.
Successful applicants will be notified on or after the 1st July, 2020.
The final agenda for the workshops will be made public on the 15th July, 2020.

avast CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE

FUNDING

Academics and students can apply for funding for their travel and/or accommodation costs by sending a request to **academic@cybersecai.com** (along with their presentation submission). Decisions for funding will be based on individual requests.

DATES & VENUE

CyberSec & AI Connected will take place live online and in four cities across the world: Prague, London, New York, and San Francisco. Full details on how to register, watch or attend can be found on our website **cybersecai.com**.

WORKSHOP PROGRAM COMMITTEE

- *Fabrizio Biondi, Avast, Prague*
- *Lorenzo Cavallaro, King's College London*
- *Sebastián García, Czech Technical University, Prague*
- *Petr Somol, Avast, Prague*
- *Celeste Fralick, McAfee, Lubbock, Texas*
- *Lukas Bajer, Cisco Security, Prague*

WEBSITE

Main conference site: **cybersecai.com**