secUnity
supporting the security community

INVITATION

Workshop: Artificial Intelligence and Cybersecurity

focusing on
Security and Data Protection for Machine Learning
Accountability and Transparency for Information Quality
Artificial Intelligence Use in Business

HESSEN

With the friendly support of the Representation
of the State of Hessen to the European Union

The scientists of the
BMBF sponsored joint project secUnity

are delighted to invite you to a workshop and dialogue dedicated to:

Artificial Intelligence and Cybersecurity

on Tuesday, 05 February 2019, 16h00 – 18h00
at the Representation of the State of Hessen to the EU
Rue Montoyer 21, 1000 Brussels

Welcome
Dr Parinas Parhisi
Representation of the State of Hessen to the EU,
Head of Unit Higher Education, Research and the Arts

Keynote
Mady Delvaux-Stehres
Member of the European Parliament

Session I – Scientific Background
Prof Dr Thorsten Holz
Ruhr University Bochum,
Chair for Systems Security

Session II – Disinformation and Fake News: The Role of AI
Ninja Marnau
Helmholtz Center for Information Security (CISPA),
Senior Researcher

Session III – Artificial Intelligence Use in Business
Prof Dr Peter Buxmann
Technische Universität Darmstadt,
Chair of Software & Digital Business

RSVP via https://eu.hessen.de/Cypersecurity

Artificial Intelligence and Cybersecurity
Artificial intelligence (AI) is well on its way to becoming a basic technology of the 21st century. However, AI harbours new risks for security and privacy. Hence it is important not to simply rely on the approach of the – mostly non-European – market leaders in the AI and IT sector, but to pursue a sovereign strategy for Europe. In this regard, the integration and combination of AI and IT security could become a characteristic feature for "AI made in the EU".

In three sessions we will examine different aspects of AI and IT security: from manipulation detection through private learning and to fair business models. Each session employs the respective speaker's scientific lens and will be followed by rounds of open discussion for questions, comments and remarks.

Session I – Scientific Background
Security and Data Protection for Machine Learning – An Introduction
Machine Learning is the foundation of autonomous and neural systems. Current algorithms are vulnerable, can make mistakes and possibly process personal information. We give an overview of the challenges from an IT security and data protection perspective.

Session II – Disinformation and Fake News: The Role of AI
Facilitating Accountability and Transparency for Information Quality
The exposure of citizens to large scale disinformation is a major risk to the EU's democratic processes and its values. We will present scientific results with regard to analysis, detection and countermeasures as well as discuss the role of AI and IT security within the EU's action plan against disinformation.

Session III – Artificial Intelligence Use in Business
Artificial Intelligence – New Business Models, Cases and Privacy Issues
AI is well on its way to becoming the base technology of the 21st century and AI use can help solve important societal challenges. However, by linking data, AI algorithms can threaten individual privacy and the intransparency of many AI algorithms might lead to economically and socially undesirable application scenarios. Without fear or hype, this section will weigh up potential advantages against disadvantages of AI use and show how fair and AI-based business models could represent a competitive advantage for the European economy.

About secUnity *(it-security-map.eu)*:
The joint interdisciplinary project secUnity, sponsored by BMBF – Federal Ministry of Education and Research, pools the expertise for European IT security research and policy of the three competence centers KASTEL, CRISP, and CISPA, and the Technische Universität Darmstadt, the Ruhr-University Bochum, the Karlsruhe Institute of Technology and the Fraunhofer Institutes SIT and AISEC.

In this secUnity workshop, aspects of the roadmap "Cybersecurity Research: Challenges and Course of Action", which was initiated and coordinated by secUnity, will be presented and discussed with attendees. The roadmap process involved European experts and almost 30 distinguished scientists from academic and industrial research contributed as co-authors. The official release of the final roadmap will take place at the same venue subsequent to the workshop: we would kindly like to draw your attention to this consecutive event at 19h00 "Civil Cybersecurity Research for Digital Sovereignty – Official Release of the secUnity Roadmap".

Registration for the evening event is open: https://eu.hessen.de/secUnity