

28 September 2023

Room 1.6

**08:45 – 09:00 Welcome (Joint CyberISPS, SECPRE, DPM, CBT workshops)**

*Joaquin Garcia – Alfaro, Guillermo Navarro-Arribas, Pantaleone Nespoli, Sokratis Katsikas, Christos Kalloniatis*

**09:00 – 10:00 Keynote talk**

*Speaker: Michal Choras (Bydgoszcz University of Science and Technology, Poland)*

*Topic: Practical applications of trustworthy AI in security: detection of cyberattacks and fake news*

*Abstract: AI solutions are widely used in a plethora of applications, including in the security domain. However, in order to be fully adopted and accepted by societies, those solutions need to fulfill the requirements of trustworthy AI. In this talk, practical examples of trustworthy AI solutions in security will be presented and discussed: cybersecurity and fake news detection. The talk will not only emphasize effective results, security and privacy but also the deployed explainability (xAI) mechanisms and software will be shown. The results of selected EU and national projects will be demonstrated (e.g. AI4Cyber, STARLIGHT, APPRAISE and SWAROG).*

**10:00-10:30 Coffee Break**

**10:30-12:30 Session 1**

*Chair: Sokratis Katsikas*

1. Susanne Barkhald Sandberg, Aida Akbarzadeh and Vasileios Gkioulos, *Effects of Organizational Cyber Security Culture Across the Energy Sector Supply Chain*
2. Stavros Simou, Aikaterini-Georgia Mavroeidi and Christos Kalloniatis, *Review on privacy and trust methodologies in cloud computing*
3. Lennart Bader, Eric Wagner, Martin Henze and Martin Serror, *METRICS: A Methodology for Evaluating and Testing the Resilience of Industrial Control Systems to Cyberattacks*
4. Karl Jonatan Due Vatn, Georgios Kavallieratos and Sokratis Katsikas, *Threat analysis in Dairy Farming 4.0*

**12:30-13:30 Lunch Break**

**13:30-15:00 Session 2**

*Chair: Aida Akbarzadeh*

1. Cihan Eryonucu and Panos Papadimitratos, *Security and Privacy for Mobile Crowdsensing: Improving Modularity and User Relevance*
2. Jens Leicht, Marvin Wagner and Maritta Heisel, *Creating Privacy Policies From Data-Flow Diagrams*
3. Konstantinos Kontogeorgopoulos and Kyriakos Kritikos, *Overview of Social Engineering Protection and Prevention Methods*

**15:00-15:30 Coffee Break**

**15:30-18:00 Session 3**

*Chair: Aida Akbarzadeh*

1. Teodor Sommestad, Henrik Karlzén, Hanna Kvist, and Hanna Gustafsson, Skade – *A Challenge Management System for Cyber Threat Hunting*
2. Thrasyvoulos Giannakopoulos and Konstantinos Maliatsos, *On the Usage of NLP on CVE Descriptions for Calculating Risk*
3. Bjorn Leander, Aida Causevic, Hans Hansson and Tomas Lindstrom, *Evaluation of an OPC UA-based Access Control Enforcement Architecture*
4. Massimiliano Baldo, Tommaso Bianchi, Mauro Conti, Alessio Trevisan, and Federico Turrin, *HoneyEVSE: An Honeypot to emulate Electric Vehicle Supply Equipments*
5. Mario Raciti and Giampaolo Bella, *Up-to-date Threat Modelling for Soft Privacy on Smart Cars*