ARTMAN ‘24 Programme

Time	Session
8:30 – 8:45	Opening remarks
8:50 – 9:50	Session 1: ML for Cybersecurity (3 papers x 20 mns) • Benjamin Kolicic, Alberto Caron, Vasilios Mavroudis and Chris Hicks. *Inherently Interpretable and Uncertainty-Aware Models for Online Learning in Cyber-Security Problems* • Shing-Li Hung, Chung-Kuan Chen, Keisuke Furumoto, Takeshi Takahashi and Hung-Min Sun. *Dark Watchdog: A Novel RAG-Driven System for Real-Time Detection and Analysis of Data Leaks on Dark Web Forums* • Kohei Miyamoto, Chansu Han, Tao Ban, Takeshi Takahashi and Jun'Ichi Takeuchi. *Intrusion Detection Simplified: A Feature-free Approach to Traffic Classification Using Transformers*
10:00 – 10:30	Break
10:30 – 11:30	Keynote 1 Melek Önen. *Customized attacks and defense strategies for robust and privacy-preserving federated learning*
11:30 – 12:10	Session 2: Robustness, privacy and safety for ML systems I (2 x 20) • Afshin Hasani, Mehran Alidoost Nia and Reza Ebrahimi Atani. *Balancing Safety and Security in Autonomous Driving Systems: A Machine Learning Approach with Safety-First Prioritization* • Nami Ashizawa, Toshiki Shibahara, Naoto Kiribuchi, Osamu Saisho and Naoto Yanai. *Restoring Unintended Model Learning by Error Correcting Code*
12:10 – 13:30	Lunch
13:30 – 14:30	Keynote 2 Christian Wressnegger. *Prospects and Limits of Explainable AI in Computer Security*
14:30 – 15:10	Session 3: Robustness, privacy and safety for ML systems II (2 x 20) • Muhammad Fakhrur Rozi and Takeshi Takahashi. *Learning to Unfix: Towards ML Robustness in Vulnerability Detection via Structure-Aware Code Generation* • Tsunato Nakai, Kento Oonishi and Takuya Higashi. *Does Prompt-tuning Enhance Privacy in Large Language Models?*
15:10 – 15:40	Break
15:40 – 16:40	Session 4: Attack to ML algorithms • Shae McFadden, Zeliang Kan, Lorenzo Cavallaro and Fabio Pierazzi. *The Impact of Concept Drift Mitigation on Availability Data Poisoning for Android Malware Classifiers* • Avilash Rath, Youpeng Li, Troy Davis, Braden Bronaugh, Darsh Poddar, Sophia Li and Xinda Wang. *When AI Meets Code Analysis: A Study of Adversarial Attacks on Deep Learning-based Code Models via Program Transformation* • Marina Katoh, Weiping Pei and Youye Xie. *AdVul: Adversarial Attack against ML-based Vulnerability Detection*
16:40 – 17:00	Closing remarks