Machine Learning Security and Privacy Summer School

Join us for the inaugural Machine Learning Security and Privacy Summer School. Machine learning architectures impact everyone's lives, whether they are aware of it or not. This intensive program aims to introduce students to the risks associated with developing novel machine learning architectures focused solely on achieving the best accuracy, regardless of the potential dangers. Participants will enhance their knowledge of machine learning architectures, the threats they face, and the protective measures that can be employed to counteract these attacks.

Course Overview:

The Machine Learning Security and Privacy Summer School will educate students on the vulnerabilities of machine learning architectures, including jailbreaking, data stealth, GenAI worms, and physical attacks. The course will also cover practical defense mechanisms to safeguard the privacy and security of these architectures. Participants will engage in hands-on activities and interactive discussions. No prior knowledge of artificial intelligence is required.

Day 1:

- Python 101
- PyTorch vs TensorFlow
- JAX
- Prompt Engineering

Day 2:

- Introduction to Machine Learning
- Exploratory Data Analysis (EDA)
- Training and Evaluating ML Models
- Neural Networks
- Model Interpretability and Adversarial Attacks

Day 3:

- Data Anonymizations
- Privacy Preserving Architectures
- Attacks on Machine Learning Architectures
- How to jailbreak a LLM?

Other Details:

- This summer school takes place July 28-30.
- Instructors: Răzvan Rughiniș, Andrei Ouatu, Andrei Dugăeșescu, Alex Deonise
- You need to enroll to participate.

Register now for Machine Learning Security and Privacy Summer School: Register for MLSP Summer School Machine Learning Security and Privacy Summer School is organized by the security community at the Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, supported by our industry partners: Keysight Technologies Romania (our main industry partner)