ARTISAN SUMMER SCHOOL 2024

ARTificial Intelligence in Secure ApplicatioNs

ARTISAN

du 15 au 18 Juillet
LCIS 50 Rue Barthélémy de Laffemas 26000 Valence

ABSTRACT

The Summer School ARTISAN (Role and effects of ARTificial Intelligence in Secure ApplicatioNs) tackles the issues related to Artificial Intelligence and Machine Learning with regard to security and safety applications.

The last years have witnessed an increasing adoption of Artificial Intelligence (AI), especially Machine Learning (ML), techniques in many automated systems covering almost all the main domains of our lives. AI-based components have emerged in many industrial domains such as Industry 4.0, aviation and flight control, automotive, medical... They perform complex tasks such as pattern recognition, image recognition, and even control. However, most of the systems and functionalities in domains such as aviation, industrial automation and automotive have security-critical and safety-critical requirements.

The objective of ARTISAN is to illustrate, to security and safety Ph.D. candidates, what the foundations, applications, benefit, misuse and related effects of Artificial Intelligence in critical systems and infrastructures are. ARTISAN's lecturers analyses Artificial Intelligence and Machine Learning to raise awareness on the fact that they are a double-edged sword which can either enhance security and safety of systems or expose them to novel threats.

In ARTISAN, AI/ML is addressed as
* a means to improve security of systems and applications;
* a means to attack applications;
* an enabling technology that is beneficial to build innovative systems and applications, but that can expose itself to novel vulnerabilities.

More precisely, the lecturers will discuss the current and near-term applications of AI/ML technologies as well as the associated security risks, mitigations and existing limitations.

LECTURES

- Introduction to Machine Learning,
  Simon L. Gay, Université Grenoble Alpes, LCIS
- Towards Machine Learning Models that We Can Trust: Hacking and (properly) Testing AI
  Maura Pintor, University of Cagliari, PRALab
- Formal Methods for Machine Learning Pipelines
  Catarina Urban, INRIA, ANTIQUE Team
- Multiagent trust management models
  Laurent Vercouter, INSA Rouen, LITIS
- ML for Cybersecurity in converged energy systems: saviour or a villain?
  Angelos K. Marnerides, University of Cyprus, KIOS Research and Innovation Centre of Excellence
- Decentralized machine learning as an enabler of decentralized online services,
  Sonia Ben Mokhtar, CNRS, LIRIS
- The legal issues of AI
  William Letrone and Ludovica Robustelli, Nantes University, DCS research center