INTERNATIONAL

INVITED SESSION SUMMARY

Title of Session: Detection of Complex Attacks through Advanced Learning Models

Name, Title and Affiliation of Chair: Pierre Parrend, Prof., EPITA/University of Strasbourg

Details of Session (including aim and scope):

This session intends to address the next challenges in the coupling of cybersecurity and AI by focusing on a blind spot of detection of complex cybersecurity attacks: the analysis of weak signals and stealthy interactions inside the systems to be protected.

Attacks and their countermeasures have grown dramatically more complex with the combination of extensive digital transformation in service and industries, the maturation of both defense and attack software, and the growing pressure of increasing cybersecurity threats. In this context, efficient detection requires a radical refinement of these systems which can no longer be considered as monolithic (or monolithic abstractions). The specificities of the user, machine, operating system, and service levels must be considered, while maintaining a technical control, and a cognitive one for the operator in charge, over the ever-growing heterogeneity. In particular: weak signals, traffic betraying an ongoing APT (advanced Persistent Threat), or attacks against the detection systems easily evade state of the art detectors. Being able to hunt these novel threats necessitates to support the identification of emerging behaviors, tracking the evolution of connections as well as connection patterns, or even making correlations through remote systems. And to do so in an antagonist environment where the adversary does not passively wait to be detected but takes actives steps to evade, lure or exploit the detection systems.

The session on "Interactions for security detection" deals with following key challenges:

- How to model interactions between users, machines, systems, and services?
- How to detect low signals and their drift, as well as learn and handle novel threats in antagonist environments?
- How to exploit these low signals to abuse operational and protection systems
- How to design robust systems, detection systems (federated learning), or bricks of detection systems (SOCs at system and user level)

Topics of interest are, but not restricted to:

- Learning emerging behaviors for security detection
- Low signals for detection
- Graph representation learning for security: knowledge, provenance, connectivity graphs.
- Advanced learning paradigms
- Distributed learning and Decentralized learning
- Federated learning
- Stream learning
- User interactions
- Machine learning for security attack and defense
- Detection in heterogeneous environments
- LLM for security, security for LLMs
- Adversarial machine learning
- Trustworthy machine learning

Application domains are, but not restricted to:

- IoT environments
- Critical infrastructures
- Cloud infrastructures
- IT Networks

Fundamental and theoretical as well as applied research work are welcome.

Main Contributing Researchers / Research Centers (tentative, if known at this stage):

Research centers:

- ICube laboratory, University of Strasbourg (France)
- LRE (Laboratoire de Recherche de l'EPITA), Paris (France)
- IMT-Atlantique, Rennes (France)

Contributing researchers :

- Pierre Parrend, LRE/ICube (France)
- Marc-Oliver Pahl, IMT-Atlantique (France)
- Nida Meddouri, Ph.D., LRE (France)

Website URL of Call for Papers (if any):

N/A

Email & Contact Details:

- pierre.parrend@epita.fr
- marc-oliver.pahl@imt-atlantique.fr
- nida.meddouri@epita.fr