INTERNATIONAL

INVITED SESSION SUMMARY

Title of Session: Detection of Complex Attacks

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

Bio:
Pierre Parrend is HDR Professor at EPITA and head of Security & Systems team ar LRE - Laboratoire de Recherche de l'EPITA, and member of the ICube laboratory of the University of Strasbourg. His research interests focus on the use of graphs for explainable detection of cyberattacks in critical systems, which he studied in DGA project DAMIAGE, and ANR projects THIA-ArtiC and Correau. Pierre is also deputy director of the LRE. In this context, he coordinates the contribution of EPITA's regional sites in Strasbourg, Rennes, Lyon and Toulouse to the school's partner research laboratories. Pierre was responsible for the BICS (Biostatistics, Informatics, and Complex Systems) research platform at the ICube laboratory, and responsible for the teaching department in computer science and mathematics at ECAM Strasbourg-Europe between 2012 and 2021. He is graduated with a Habilitation to Direct Research from the University of Strasbourg (2017) and a PhD in Computer Science from INSA Lyon (2008).

Details of Session (including aim and scope):

This session intends to address the next challenges in the coupling of cybersecurity and Artificial Intelligence and Knowledge Management techniques by focusing on the detection of complex cybersecurity attacks. Zero-days, Advanced Persistent Threats (APT) or attacks supported by generative technologies require a coordinated and fine-grained effort for modeling and detecting them and reacting to related intrusions.

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. The stack involved goes from data capture to cyber situational awareness and reaction, through automated analysis of attack techniques and malware, characterization of intrusion, detection of known malicious activity as well as abnormal behaviors.

The advent of code and security procedure generation both for defense and pentest increases the threats to yet another level. Being able to hunt these novel threats necessitates supporting 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:

- Novel models and best practices for generative AI in security
- Novel models and best practices for machine learning in security
- Interactions model between users, machines, systems, and services
- 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
- Generative AI for defense
- Generative AI for pentest operations
- Machine learning for security attack and defense

- Graph representation learning for security: knowledge, provenance, connectivity graphs.
- Adversarial machine learning
- Federated learning
- Security of AI pipelines
- Explainable and trustworthy learning models

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.

Submission instructions:

For all updates and comprehensive instructions for autors please refer to:
http://kes2025.kesinternational.org/submission.php

Papers are invited for KES2025 on topics lying within the scope of the session. All contributions must be of high quality, original, and must not have been previously published elsewhere or intended for publication elsewhere.
All papers will be reviewed by members of the International Program Committee and depending on their level and attributes, may be selected for oral or poster presentation, and publication in the conference proceedings.
Full papers will be reviewed by the IPC and if accepted and presented, they will be published in Elsevier's Procedia Computer Science open access journal, available in ScienceDirect and submitted to be indexed/abstracted in CPCI (ISI conferences and part of Web of Science), Engineering Index, and Scopus.
Authors of selected papers may be invited to submit extended versions of their papers for publication as full journal papers, for example in the KES Journal or other journals.

Submitting your work

Submissions for the conference must be made as complete papers (there is no abstract submission stage) submitted as PDF documents through the PROSE online submission and review system.
Full papers should be detailed academic articles in conventional format. The guide length for full papers is 8 to 10 pages (maximum).

More information here: http://kes2025.kesinternational.org/submission.php.
More information here: http://kes2025.kesinternational.org/submission.php.

Guidance notes and templates still to be provided by KES organizing committee: .

Submission site still to be announced by KES organizing committee.

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

- EPITA, Paris, France
- University of Strasbourg, France
- IMT Atlantique, France
- Uni Lyon II, France
- Fraunhofer Institute IOSB, Germany
- Masaryk Uni Brno, Czech Republic
- LIPAH, Tunisia
- Fujitsu, Luxembourg

Program committee (to be completed):

- Juba Agoun, Lyon 2 (France)
- Christophe Biernacki, INRIA Lille (France)

- Tristan Bilot, (France)
- Amel Borgi, LIPAH (Tunisie)
- Nour EL MADHOUN, (France)
- Ghada Gharbi, EPITA (France)
- Martin Husak, Masaryk Uni Brno (Czech Republic)
- Rushed Kanawati, Université Paris 13 (France)
- Sofiane Lagraa, Fujitsu (Luxembourg)
- Valeria Loscri, (France)
- Nidà Meddouri, EPITA (France)
- Ankush Meshram, Fraunhofer Institue IOSB (Germany)
- Mohamed Lamine Messai, University Lyon II (France)
- Julien Michel, EPITA/Unistra (France)
- Marc-Oliver Pahl, IMT Atlantique (France)
- Pierre Parrend, EPITA/Unistra (France)
- Hamida Seba, University Lyon I (France)

Website URL of Call for Papers (if any):
https://kes-dca.lre.epita.fr/
(to be updated from DCA'24)

Email & Contact Details:
- pierre.parrend@epita.fr