INTERNATIONAL

INVITED SESSION SUMMARY (KES 2024, Siville, Spain)

Title of Session:

Generative AI and Cybersecurity: Challenges and Perspectives for Strengthening Both Defenses and Threats

Name, Title and Affiliation of Chairs:

- **Fiammetta MARULLI,** Assistant Professor, Università della Campania “Luigi Vanvitelli”, Italy
- **Francesco MERCALDO**, Assistant Professor, Università del Molise, Italy

Details of Session (including aim and scope):

Generative artificial intelligence (AI) holds the potential to enhance cybersecurity by improving threat detection, but complete automation is not expected soon.
Malicious actors are also investigating how generative AI can assist in cyberattacks by developing evolving malware. In today's landscape, both cybersecurity consumers and service providers have opportunities to leverage this new technology while ensuring their protection.

Following the launch of ChatGPT and other products utilizing large language models (LLMs), the cybersecurity sector is strategizing to integrate generative AI as a crucial tool. Despite the initial challenge generative AI faces in cybersecurity due to the sensitive and isolated nature of security data, which hinders the acquisition of high-quality, comprehensive datasets required for training and updating LLM models.

Currently, the primary focus lies in threat identification, where Generative AI is already contributing to the expedited detection of attacks and providing a more comprehensive assessment of their scale and potential impact. For instance, it aids analysts in more efficiently filtering out false positives from incident alerts. The capabilities of generative AI in threat detection and analysis are expected to become increasingly dynamic and automated.

The main goal of this Session is to collect experiences and contributions by the scientific community concerning analysis of novel:

- **Cybersecurity attack and defence Methods;**
- **Attack and Defence Techniques and Scenarios;**
- **Attack and Defence Samples Data Sets and Tools,**
- **Cyber-physical Systems and Applications,**

exploiting generative AI, both as an attack and a defence tool.

By collecting contributions and experiences from different communities, we aim to improve the collective knowledge about the assessment that generative AI holds the most potential in enhancing cybersecurity through improved threat identification.

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

Invited Researchers to contribute to this session:

Dr. Michele Mastroianni, mmastroianni@unisa.it
Dr. Giovanni Paragliola, giovanni.paragliola@icar.cnr.it
Dr. Laura Verde, laura.verde@unicampania.it
Dr. Lelio Campanile, lelio.campanile@unicampania.it
Prof. Stefano Marrone, stefano.marrone@unicampania.it
Dr. Silvio Baccari, silvio.baccari@unicampania.it
Prof. Gianni D'Angelo, giadangelo@unisa.it
Prof. Gennaro Cordasco, gennaro.cordasco@unicampania.it
Prof. Torsten Priebe, torsten.priebe@fhstp.ac.at
Dr. Peter Kieseberg, peter.kieseberg@fhstp.ac.at
Prof. Gladys Diaz, gladys.diaz@univ-paris13.fr
Dr. Carlo Sanghez, csanghez@gameng.it
Dr. Giacomo Iadarola, giacomo.iadarola@iit.cnr.it
Dr. Paolo Valletta, p.valletta@gematica.com

Research Centers Invited to Contribute and currently involved in this research area:

- **CYBHORUS s.r.l., Cybersecurity Research Company, Italy**
- **GAM Engineering s.r.l., IoT and Communication Research and Development Company, Italy**
- **GEMATICA s.r.l., Software and Communication Systems Research and Dev. Company, Italy**
- **RSE s.p.a. (Italian Research Center for Energy Systems), Italy**
- **CNR – ICAR (Italian National Council for Research – High Performance Computing and Networks), Italy**
- **Università della Campania "Luigi Vanvitelli", Dept. of Maths and Physics, Italy**
- **Università del Molise, Dept. of Applied Science and Informatics, Italy**
- **Universitè Sorbonne Paris XIII, Dept. of Informatique, France**
- **St. Pölten University of Applied Sciences, Austria**

Website URL of Call for Papers (if any):

Email & Contact Details:

fiammetta.marulli@unicampania.it
francesco.mercaldo@unimol.it