SECURWARE 2025

Forward

The Nineteenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2025), held between October 26th, 2025, and October 30th, 2025, in Barcelona, Spain, continued a series of events covering related topics on theory and practice on security, cryptography, secure protocols, trust, privacy, confidentiality, vulnerability, intrusion detection and other areas related to law enforcement, security data mining, malware models, etc.

Security, defined for ensuring protected communication among terminals and user applications across public and private networks, is the core for guaranteeing confidentiality, privacy, and data protection. Security affects business and individuals, raises the business risk, and requires a corporate and individual culture. In the open business space offered by Internet, it is a need to improve defenses against hackers, disgruntled employees, and commercial rivals. There is a required balance between the effort and resources spent on security versus security achievements. Some vulnerability can be addressed using the rule of 80:20, meaning 80% of the vulnerability can be addressed for 20% of the cost. Other technical aspects are related to the communication speed versus complex and time-consuming cryptography/security mechanisms and protocols.

A Digital Ecosystem is defined as an open decentralized information infrastructure where different networked agents, such as enterprises (especially SMEs), intermediate actors, public bodies and end users, cooperate and compete enabling the creation of new complex structures. In digital ecosystems, the actors, their products and services can be seen as different organisms and species that are able to evolve and adapt dynamically to changing market conditions.

Digital Ecosystems lie at the intersection between different disciplines and fields: industry, business, social sciences, biology, and cutting-edge ICT and its application driven research. They are supported by several underlying technologies such as semantic web and ontology-based knowledge sharing, self-organizing intelligent agents, peer-to-peer overlay networks, web services-based information platforms, and recommender systems.

To enable safe digital ecosystem functioning, security and trust mechanisms become essential components across all the technological layers. The aim is to bring together multidisciplinary research that ranges from technical aspects to socio-economic models.

We take the opportunity to warmly thank all the members of the SECURWARE 2025 technical program committee, as well as all the reviewers. The creation of such a high-quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to SECURWARE 2025. We truly believe that, thanks to all these efforts, the final conference program consisted of top-quality contributions. We also thank the members of the SECURWARE 2025 organizing committee for their help in handling the logistics of this event.

We hope that SECURWARE 2025 was a successful international forum for the exchange of ideas and results between academia and industry for the promotion of progress in the field of security information, systems, and technologies.

SECURWARE 2025 Chairs

SECURWARE 2025 Steering Committee
Steffen Fries, Siemens, Germany
Rainer Falk, Siemens AG, Corporate Technology, Germany
George O. M. Yee, Aptusinnova Inc. / Carleton University, Ottawa, Canada
Hans-Joachim Hof, INSicherheit - Ingolstadt Research Group Applied IT Security, CARISSMA – Center of Automotive Research on Integrated Safety Syst, Germany
Ki-Woong Park, Sejong University, South Korea
Alexander Lawall, IU International University of Applied Science, Germany

SECURWARE 2025 Publicity Chairs
Lorena Parra Boronat, Universidad Politécnica de Madrid, Spain
Laura Garcia, Universidad Politécnica de Cartagena, Spain