SecSoft 2022

The 4th International Workshop on

Cyber-Security Threats, Trust and Privacy management
in Software-defined and Virtualized Infrastructures

co-located with IEEE NetSoft 2022

1 July 2022, Milan, Italy

http://www.secsoft-workshop.org

Call for Papers

The 4th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) is a joint initiative from the H2020 EU Projects GUARD, RAINBOW, SIMARGL, PALANTIR, INSPIRE-5GPlus, SIFIS-HOME, ELECTRON and SDN-microSENSE to create a dialogue about emerging cyber-security paradigms for virtualized environments and critical infrastructures.

Scope

Evolving business models are progressively reshaping ICT services and infrastructures, with a growing “softwarization” trend, the massive introduction of virtualization paradigms, and the tight integration with the physical environment. Unfortunately, the evolution of cyber-security paradigms has not followed with the same pace, leading to a substantial gap in solutions capable of protecting the new forms of distributed and heterogeneous systems against an evolving landscape of cyber-threats.

Traditional security tools that organizations have long relied on to protect their networks (i.e., antivirus, intrusion prevention systems, firewalls) are no longer capable of providing sufficient security guarantees against the rapid escalation of advanced persistent threats and multi-vector attacks. The growing complexity of cyber-attacks are urgently demanding more correlation in space and time of (apparently) independent events and logs, and a higher degree of coordination among different security mechanisms.

Topics of interest

This Workshop aims to gather together novel approaches for providing organizations the appropriate situational awareness in relation to cyber security threats allowing them to quickly detect and effectively respond to sophisticated cyber-attacks.

Topics of interest include but are not limited to:

- Cyber-security platforms and architectures for digital services;
- Security, trust and privacy for industrial systems and the IoT (including smart grids);
- Monitoring and advanced data collection and analytics;
- Virtual and software-based cyber-security functions;
- Orchestration and Automatic Configuration of security functions;
- Novel algorithms and models for attack detection and threat identification;
- Authentication, Authorization and Access control;
- Intelligent attack mitigation and remediation;

- Machine learning, big data, network analytics;
- Secure runtime environments, including trustworthy systems and user devices;
- Formal methods and policies for security and trust;
- Trusted computing;
- Information flow control;
- Risk analysis and management, Audit and Accountability;
- Honeypots, forensics and legal investigation tools;
- Threat intelligence and information sharing.

Multi-disciplinary and collaborative research projects are encouraged to submit joint papers describing their integrated architectures and cyber-security platforms, with special emphasis on how they address the challenging cyber-security requirements of softwarized environments and critical infrastructures.

Paper submissions

Interested authors are invited to submit papers according to the following guidelines:

- papers must be up to 6 pages long, including tables, figures and references;
- the style to be used is IEEE 2-column US-letter style using IEEE Conference template, and papers must be submitted in pdf format.

Accepted and presented workshop papers will be published in the conference proceedings and will be submitted to IEEE Xplore.
For more details about submission form and procedure, please check the NetSoft conference website at https://netsoft2022.ieee-netsoft.org/authors/
Only PDF files will be accepted for the review process and all manuscripts must be electronically submitted through EDAS: https://edas.info/newPaper.php?c=29270&track=109968

Important: *Please check NetSoft 2022 publication and no-show policy in the conference website at* https://netsoft2022.ieee-netsoft.org/authors/publication-and-no-show-policy/.

Important dates

Workshop paper submission deadline:	**March 21, 2022 (Extended, Firm)**
Workshop paper acceptance:	**April 21, 2022**
Camera-ready papers:	**May 5, 2022**
Workshop date:	**July 1, 2022**

Workshop Co-Chairs

Fulvio Valenza, Politecnico di Torino, Italy
Antonio Skarmeta, University of Murcia, Spain
Matteo Repetto, IMATI-CNR, Italy

TPC Co-Chairs

Michal Choras, FernUniversitat in Hagen, Germany
Antonio Lioy, Politecnico di Torino, Italy
Andrea Saracino, IIT-CNR, Italy