SecSoft 2019

The 1st International Workshop on

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

co-located with IEEE NetSoft 2019

June 24th, 2019 – Paris, France

https://www.astrid-project.eu/secsoft/

Call for Papers

The 1st Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft) is a joint initiative from the H2020 EU Projects ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD, and 5GENESIS 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 includes 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 of security functions;
- Novel algorithms for attack detection and threat identification;
- Intelligent attack mitigation and remediation;

- Machine learning, big data, network analytics;
- Secure runtime environments, including trustworthy systems and user devices;
- Formal methods for security and trust;
- Novel threat and attack models;
- Authentication, Authorization and Access control;
- 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 either

- *short papers* (up to 5 pages, including references), presenting industrial innovations, architectural references of research projects, main outcomes from demos and field trials, or
- *regular papers* (up to 9 pages, including references), presenting research results or technical developments.

Accepted and presented workshop papers will be published in the conference proceedings and will be submitted to IEEE Xplore.

For more details about submission forma and procedure, please check the NetSoft conference website at http://netsoft2019.ieee-netsoft.org/authors/call-for-workshop-papers/.

Important: *Please check NetSoft 2019 publication and no-show policy in the conference website at http://netsoft2019.ieee-netsoft.org/authors/publication-and-no-show-policy/.*

Important dates

Workshop paper submission deadline:	**February 15, 2019**
Workshop paper acceptance:	**March 22, 2019**
Camera-ready papers:	**April 5, 2019**
Workshop date:	**June 24, 2019**

Workshop Co-Chairs

Matteo Repetto, *CNIT*, Italy
Nicholas Kolokotronis, *University of Peloponnese*, Greece
Evangelos Markatos, *University of Crete*, Crete

TPC Co-Chairs

Thanassis Giannetsos, *Technical University of Denmark*, Denmark
Stavros Shiaeles, *University of Plymouth*, UK
Georgios Gardikis, *Space Hellas S.A.*, Greece
Panagiotis Sarigiannidis, *University of Western Macedonia*, Greece