DCDS 2022 Call for Papers

4th International Workshop on Data-Centric Dependability and Security

Co-located with the 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks
June 27, 2022, Baltimore, Maryland, USA

http://dcds.lasige.di.fc.ul.pt

Steering Committee

Ibéria Medeiros, University of Lisboa, Portugal
Ilir Gashi, City, University of London, UK
Michael Kamp, University of Monash, Australia
Pedro Ferreira, University of Lisboa, Portugal

Program Committee Members

Alysson Bessani, University of Lisbon, Portugal
Ambra Demontis, University of Bari Aldo Moro, Italy
Antonio Pecchia, University of Sannio, Italy
Cagatay Turkay, City, University of London, UK
Carsten Rudolph, Monash University, Australia
Donato Malerba, University of Bari Aldo Moro, Italy
Gustavo Gonzalez-Granadillo, Atos, Spain
Marco Vieira, University of Coimbra, Portugal
Miguel Correia, Instituto Superior Técnico, Portugal
Rogério de Lemos, University of Kent, UK

Important Dates

Workshop Submission: April 4, 2022
Notification of Acceptance: April 25, 2022
Camera Ready: May 2, 2022
Workshop: June 27, 2022
Conference: June 27-30, 2022

Submission Site

https://easychair.org/conferences/?conf=dcds22

Publication

Authors of accepted regular papers will have 30 minutes for presentation and discussion during the workshop, while authors of position papers will have 15 minutes.

At least one author of an accepted paper must register at the workshop.

Accepted papers (regular and position) will be published in the DSN supplemental volume and made available in IEEE Xplore.

Sponsors

Ciências ULisboa

LASIGE driven by excellence

Workshop Description

Today's computing systems are increasingly networked, complex and diverse, integrating multiple distinct components with different configurations and several software for different purposes. They operate under increasing scales and in dynamic operating environments, generating more and more functional and non-functional data and processing a myriad of data received from other systems. Along with vulnerability assessment information and open-source intelligence (e.g., cyber threat intelligence (CTI)), these data can be fused and exploited to improve the security and dependability of systems, making them more resilient to cyberattacks, like 0-day attacks, accident faults, and unexpected operating conditions. Additionally, as systems grow in complexity and size, they become harder to manage and report on. This calls for solutions combining the latest advances in areas such as large-scale data processing, data science, visualization, and machine and statistical learning.

DCDS'22 aims at providing researchers with a forum to exchange and discuss scientific contributions and open challenges, both theoretical and practical, related to the use of data-centric approaches that promote the dependability and cybersecurity of computing systems. We want to foster joint work and knowledge exchange between the dependability and security communities, and researchers and practitioners from areas such as machine and statistical learning, and data science and visualization. The workshop provides a forum for discussing novel trends in data-centric processing technologies and the role of such technologies in the development of resilient systems. It aims to discuss novel approaches for processing and analysing data generated by the systems as well as information gathered from open sources, leveraging data science, machine and statistical learning techniques, and visualization. The workshop shall contribute to identify new application areas as well as open and future research problems, for data-centric approaches to system dependability and security.

Topics of Interest

The list of DCDS thematic areas includes, but is not limited to, the following areas where authors are invited to submit original papers:

- Data-driven dependability and security
- Machine/statistical learning for dependability and security
- Informed machine learning for security
- Data modelling and Visualization
- Threat detection and prevention
- Faul/Vulnerability detection
- Open source intelligence (OSINT) based threat awareness
- Data-driven improvements for SIEM's
- Risk modeling and assessment
- Fault tolerance

Paper Submission

DCDS welcomes both research papers reporting results from mature work, as well as more speculative papers describing new ideas or preliminary exploratory work. Papers reporting industry experiences and case studies will also be encouraged. Research papers should be work that is not previously published or concurrently submitted elsewhere and will be published in the proceedings. Submissions are accepted in two formats conforming to the IEEE two-column conference style:

- **Regular** research papers of at most **8 pages** including references.
- **Position** research statements of at most **4 pages** including references. Position papers may summarize ongoing research elsewhere or outline new emerging ideas.

All submissions should be made in PDF and must adhere to the IEEE Computer Society 8.5″x11″ two-column camera-ready format (using a 10-point font on 12-point single-spaced leading). Templates are available here:
https://www.ieee.org/conferences_events/conferences/publishing/templates.html
Reviewing is single-blind. The names and affiliations of authors must appear in the submitted papers. Submissions not respecting format requirements may be rejected without review.