



ARES 2018 - Call for Papers

The 13th International Conference on
Availability, Reliability and Security (ARES 2018)

August 27 – August 30, 2018, Hamburg, Germany



ARES Conference

The 13th International Conference on Availability, Reliability and Security (“ARES – The International Dependability Conference”) will bring together researchers and practitioners in the area of dependability. ARES will highlight the various aspects of dependability – with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of the research issues of dependability as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.





ARES will emphasize the interplay between foundations and practical issues of dependability in emerging areas such as e-government, m-government, location-based applications, ubiquitous computing, autonomous computing, challenges of grid computing etc. ARES is devoted to the critical examination and research challenges of the various aspects of Dependable Computing and the definition of a future road map.

Selected papers that are accepted by and presented at the ARES Conference will be published, after further revision, in special issues of international journals (e.g. Springer EURASIP Journal on Information Security). The acceptance rate of the ARES 2017 conference was 24% (full papers only). ARES 2017 was published by the International Conference Proceedings Series published by ACM (ACM ICPS).

ARES is ranked as B-conference in CORE.

Qualis (backed by Brazilian Ministry) ranked ARES and Esorics as leading security conference in Europe (A2)

ARES Important Dates

Submission Deadline	 March 16, 2018 extended to March 30, 2018 (23:59 UTC-11)
Author Notification	 May 30, 2018
Camera-ready Deadline	 June 29, 2018
Conference	 August 27 – August 30, 2018

Conference Officers

General Chairs 2018

[Mathias Fischer](#), Universität Hamburg, Germany

[Dominik Herrmann](#), Universität Hamburg, Germany

Program Committee Chairs 2018

[Christian Doerr](#), TU Delft, Netherlands

[Sebastian Schrittwieser](#), FH St. Pölten, Austria

Program Committee

The program committee of ARES 2018 can be found here:

<https://www.ares-conference.eu/conference/committee/>

Topics of interest include, but are not limited to:

Authorization, Authentication, and Access Control	Resilience of Computing Systems
Availability, Dependability, and Resilience	Resilience, Security, and Privacy for Smart Grids
Botnets and Botnet Monitoring	Resilience, Security, and Privacy for the Internet of Things
Business Continuity & Resilience	RFID Security and Privacy
Cost/Benefit Analysis	Risk planning, Analysis & Awareness
Cryptography	Safety Critical Systems
Dependability Aspects for Special Applications	Secure Enterprise Architectures
Dependability Aspects of e-Government	Security and Privacy for Ubiquitous Systems
Dependability and Resilience in Open Source Software	Security and Privacy in E-Health
Designing Security Requirements	Security and Trust Management in P2P and Grid applications
Digital Forensics	Security and Privacy for Sensor Networks, Wireless/Mobile Devices and Applications
E-Commerce Dependability	Security and Usability
Identity Management	Security as Quality of Service
IPR of Security Technology	Security in Distributed Systems / Distributed Databases
Incident Response and Prevention	Security in Electronic Payments
Information Flow Control	Security in Electronic Voting
Information Hiding and Steganography	Software Engineering of Dependable Systems
Interoperability Aspects	Software Security
Intrusion Detection and Fraud Detection	Threats and Attack Modelling
Legal Issues related to Security and Privacy	Trusted Computing
Mobile Security	Tools for Dependable System Design and Evaluation
Network and Organizational Vulnerability Analysis	Trust Models and Trust Management
Network Security	Wireless Security
Privacy-Enhancing Technologies	
Process based Security Models and Methods	
Resilience and Security for Critical Infrastructures	