



Explore the Walt Disney World

ORGANIZING COMMITTEES

General Chairs

Nobuyasu Kanekawa, Hitachi, Ltd., Japan.
 Mohammad Zulkernine, Queen's University, Canada

General Executive Chair

Jun Wang, University of Central Florida, USA

Program Chair

Md Zakirul Alam Bhuiyan, Fordham University, USA

Program Vice Chairs

Naohiro Hayashibara, Kyoto Sangyo University, Japan
 (Dependable Computing Track)
 Paulo Pires, Federal University of Rio de Janeiro, Brazil
 (Autonomic Computing Track)
 Yier Jin, University of Central Florida, USA
 (Secure Computing Track)

Steering Committee

Jianhua Ma (Chair), Hosei University, Japan
 Laurence T. Yang (Chair), St. Francis Xavier Univ., Canada
 Tadashi Dohi, Hiroshima University, Japan
 Yuanshun Dai, University of Electronic Sci. & Tech. of China
 Stephen S. Yau, Arizona State University, USA

Workshop Chairs

Peter J. Clarke, Florida International University, USA
 Kommy Weldemariam, IBM Research - Africa
 Thaier Hayajneh, Fordham University, USA

Demo/Poster Chair

Zhihan Lv, University College London, UK
 Farzana Rahman, James Madison University, USA

Publicity Chairs

Christian Esposito, University of Napoli "Federico II", Italy
 Wenjia Li, New York Institute of Technology, USA
 Jianwen Xiang, Wuhan University of Technology, China
 Jongmoon Baik, KAIST, Korea
 Koji Iwata, Railway Technical Research Institute, Japan

IMPORTANT DATES

Paper Submission Due (Research Track): July 27, 2017
WiP/Poster Paper Submission Due: Aug. 17, 2017
Special Session Paper Submission Due: Aug. 17, 2017
Author Notification Due: Aug. 27, 2017
Paper Registration Due: Sept. 17, 2017
Camera-ready Manuscript Due: Sept. 21, 2017

SUBMISSION & PUBLICATION

Authors are invited to submit their original research work that has not previously been published or under review in any other venue. Papers should be prepared in IEEE CS Proceedings format and submitted via DASC 2017 website: <http://cse.stfx.ca/~dasc2017/sub/>.

Research paper (6~8 pages) should explore a specific technology problem and propose a complete solution to it. Work-in-Progress (WiP) or special session paper (4~6 pages) is to report on early or ongoing research activities. Demo/Poster papers (2~4 pages) must describe working systems and be within the scope of DASC. These systems may be innovative prototype implementations or mature systems that use related technology. Poster/demo papers need to be submitted to the Poster/Demo Chair. Workshop and Special Session papers (6 pages) need to be submitted to the corresponding workshops and special sessions.

- Once accepted, the paper will be included into the IEEE conference proceedings published by IEEE Computer Society Press (EI indexed).
- At least one of the authors of any accepted paper is required to register and present the paper at the conference.
- Extended versions of selected excellent papers will be considered for fast-track publication in special issues of prestige journals (SCI/EI indexed).

As computer systems become increasingly large and complex, their Dependability, Security and Autonomy play critical role at supporting next-generation science, engineering, and commercial applications. These systems consist of heterogeneous software/hardware/ network components of changing capacities, availability, and in varied contexts. They provide computing services to large pools of users and applications, and thus are exposed to a number of dangers such as accidental/deliberate faults, virus infections, malicious attacks, illegal intrusions, natural disasters, etc. As a result, too often computer systems fail, become compromised, or perform poorly and therefore untrustworthy. Thus, it remains a challenge to design, analyze, evaluate, and improve the dependability and security for a trusted computing environment. Trusted computing targets computing and communication systems as well as services that are autonomous, dependable, secure, privacy protectable, predictable, traceable, controllable, assessable and sustainable.

The scale and complexity of information systems evolve towards overwhelming the capability of system administrators, programmers, and designers. This calls for the autonomic computing paradigm, which meets the requirements of self-management by providing self-optimization, self-healing, self-configuration, and self-protection. As a promising means to implement dependable and secure systems in a self-managing manner, autonomic computing technology needs to be further explored. On the other hand, any autonomic system must be trustworthy to avoid the risk of losing control and retain confidence that the system will not fail. Trusted and autonomic computing and communications need synergistic research efforts covering many disciplines, ranging from computer science and engineering, to the natural sciences and the social sciences. It requires scientific and technological advances in a wide variety of fields, as well as new software, system architectures, and communication systems that support the effective and coherent integration of the constituent technologies.

DASC 2017 will be held in November 6-10, 2017 in Orlando, Florida, USA, co-located with CyberSciTech 2017, IEEE DataCom 2017 and IEEE PiCom 2017 (*the event location is very close to the Walt Disney World, which is in walking distance*). It aims to bring together computer scientists, industrial engineers, and researchers to discuss and exchange experimental and theoretical results, novel designs, work-in-progress, experience, case studies, and trend-setting ideas in the areas of dependability, security, trust and/or autonomic computing systems. Topics of particular interests include the following tracks, but are not limited to:

- Autonomic Computing Theory, Models, Architectures and Communications
- Cloud Computing and Fog/edge Computing with Autonomic and Trusted Environment
- Dependable Automatic Control Techniques and Systems
- Dependability Models and Evaluation Algorithms
- Dependable Sensors, Devices, Embedded Systems
- Dependable Electronic-Mechanical Systems, Optic-Electronic Systems
- Self-improvement in Dependable Systems
- Self-healing, Self-protection and Fault-tolerant Systems
- Hardware and Software Reliability, Verification and Testing
- Software Engineering for Dependable Systems
- Safety-critical Systems in Transportation and Power System
- Security Models and Quantifications
- Trusted P2P, Web Service, SoA, SaaS, EaaS, and PaaS
- Self-protection and Intrusion-detection in Security
- DRM, Watermarking Technology, IP Protection
- Context-aware Access Control
- Virus Detections and Anti-Virus Techniques/Software
- Cyber Attack, Crime and Cyber War
- Human Interaction with Trusted and Autonomic Computing Systems
- Security, Dependability and Autonomic Issues in Ubiquitous Computing
- Security, Dependability and Autonomic Issues in Cyber-Physical System
- Security, Dependability and Autonomic Issues in Big Data, SDN, and IoT Systems
- QoS in Communications and Services
- Information and System Security
- Reliable Computing and Trusted Computing
- Wireless Emergency and Security Systems
- Information Technology in Biomedicine
- Multimedia Security Issues over Mobile and Wireless Networks
- Multimedia in Mobile Computing: Issues, System Design and Performance Evaluation
- Software Architectures and Design for Emerging Systems
- Software Engineering for Emerging Networks, Systems, and Mobile Systems