The 14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016)

http://cse.stfx.ca/~dasc2016/

Auckland, New Zealand, 8-12 August 2016

ORGANISING COMMITTEES

General Chairs
Elisa Bertino, Purdue University, USA
Yang Xiang, Deakin University, Australia
Justin Shi, Temple University, USA

Program Chairs
Jiankun Hu, University of New South Wales, Australia
Md Zakirul Alam Bhuiyan, Temple University, USA
Nurul I Sarkar, Auckland Univ. of Technology, New Zealand

Executive Chairs
Kevin Wang, University of Auckland, New Zealand
William Liu, Auckland University of Technology, New Zealand
Dong Seong Kim, University of Canterbury, New Zealand

Steering Committee
Jianhua Ma(Chair), Hosei University, Japan
Laurence T. Yang(Chair), St. Francis Xavier University, Canada
Tadashi Dohi, Hiroshima University, Japan
Yuanshun Dai, Univ. of Electronic Sci. & Tech. of China, China

Workshop Chairs
Ryan Ko, University of Waikato, New Zealand
Yong Yu, University of Electronic Sci. & Tech. of China, China
Yizhi Ren, Hangzhou Dianzi University, China

Demo/Poster Chair
Sheng Wen, Deakin University, Australia
Jianwen Xiang, Wuhan University of Technology, China

Publicity Chairs
Ilsun You, Soonchunhyang University, Korea
Yingjie Xia, Zhejiang University, China
Yu Wang, Deakin University, Australia
Yulei Wu, University of Exeter, UK
Mubashir Husain Rehmani, COMSATS IIT, Pakistan

Program Committee
Please see conference website for complete list

IMPORTANT DATES

Workshop Proposal Due: ~~29 February 2016~~
Submission Due (Research papers): 30 April 2016
Author Notification: 31 May 2016
Submission Due (Demo/Poster papers): 5 May 2016
Author Notification: 31 May 2016
Camera-ready Paper Due: 08 Jun 2016
Registration Due: 08 Jun 2016

SUBMISSION and 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 2016 website:

http://cse.stfx.ca/~dasc2016/sub/.

Research paper (8 pages) should explore a specific technology problem and propose a complete solution to it, with experimental results. Demo/Poster papers (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 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 requested 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, analyse, 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 2016 will be held on 8-12 August 2016 in Auckland, New Zealand, co-located with CyberSciTech 2016, IEEE DataCom 2016 and IEEE PiCom 2016. 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 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
- 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
- Service Oriented Architectures