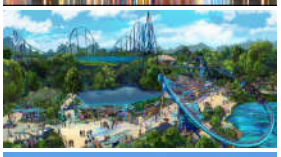
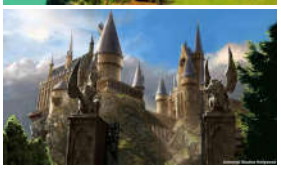



## Welcome Message



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.

IEEE 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). IEEE DASC'17 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.

### Sponsors

IEEE
IEEE COMPUTER SOCIETY
TCSC IEEE

## Scope and Topics

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
- 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
- Evaluation Platforms for Dependable, Autonomic and Secure Computing Systems