Call for Papers

The 2014 Asian Conference on Availability, Reliability and Security (AsiaARES 2014)
In conjunction with ICT-EurAsia 2014

AsiaARES Conference

AsiaARES is a new conference that builds on the success of eight subsequent annual ARES conferences and specifically aims at a better access of most current IT-security research results to and from the Asian region. The ultimate goal is to establish a community and a meeting point for security researchers and to make travel shorter and the venues easily accessible for researchers from Asia. To allow a large number of researchers to participate we will also provide interactive sessions for research in progress papers and poster sessions. Moreover, we will offer virtual presentations for which you submit a video presentation in addition to your paper and the paper will be discussed using online collaboration tools.

AsiaARES emphasizes the interplay between foundations and practical issues of security in emerging areas such as e-government, m-government, location-based applications, ubiquitous computing, autonomous computing, chances of grid computing etc. The conference is devoted to the critical examination and research challenges of the various aspects of Secure and Dependable Computing and the definition of a future road map.

The proceedings of the conference will be published in the Lecture Notes in Computer Science of Springer. Selected papers that are accepted by and presented at AsiaARES will be published, after further revision, in special issues of international journals.

Venue

AsiaARES 2014 will be held as a Special Track Conference within ICT-EURASIA (http://www.ifs.tuwien.ac.at/ict-eurasia/).

ICT-Eurasia 2014 will be held in Bali, Indonesia. Bali is frequently referred to as "The Paradise Island" because of its reputation in the world as a tropical paradise of untold beautiful nature, idyllic mood and never ending fascination. It is the perfect place to enjoy high-qualified presentations.
Topics and areas of interest include, but are not limited to:

- Authorization and Authentication
- Availability and Reliability
- Business Continuity & Resilience
- Cost/Benefit Analysis
- Cryptography
- Dependability Aspects for Special Applications (e.g. ERP-Systems, Logistics)
- Dependability Aspects of Electronic Government (e-Government)
- Dependability Administration
- Dependability in Open Source Software
- Designing Security Requirements
- Digital Forensics
- E-Commerce Dependability
- Failure Prevention
- Identity Management
- IPR of Security Technology
- Incident Response and Prevention
- Information Flow Control
- Information Hiding
- Internet Dependability
- Interoperability Aspects
- Intrusion Detection and Fraud Detection
- Legal Issues
- Mobile Security
- Network and Organizational Vulnerability Analysis
- Network Security
- Privacy-Enhancing Technologies
- Process-based Security Models and Methods
- RFID Security and Privacy
- Risk planning, Analysis & Awareness
- Safety Critical Systems
- Secure Enterprise Architectures
- Security Issues for Ubiquitous Systems
- Security and Privacy in E-Health
- Security and Trust Management in P2P and Grid applications
- Security and Privacy for Sensor Networks, Wireless/Mobile Devices and Applications
- Security and Usability
- Security as Quality of Service
- Security in Distributed Systems / Distributed Databases
- Security in Electronic Payments
- Security in Electronic Voting
- Software Engineering of Dependable Systems
- Software Security
- Standards, Guidelines and Certification
- Survivability of Computing Systems
- Temporal Aspects of Dependability
- Threats and Attack Modeling
- Trusted Computing
- Tools for Dependable System Design and Evaluation
- Trust Models and Trust Management
- VOIP, Wireless Security