Conference in Coperation with

Call for Papers

The Second International Conference on Availability, Reliability and Security (AReS)
ARES 2007 - "The International Security and Dependability Conference"

April 10th – April 13th, 2007
Vienna University of Technology
http://www.ares-conf.org

http://www.ares-conference.eu

Conference

The Second International Conference on Availability, Reliability and Security ("ARES 2007 – The International Security and Dependability Conference") will bring together researchers and practitioners in the area of IT-Security and Dependability.

ARES 2007 will highlight the various aspects of security – with special focus on secure internet solutions, trusted computing, digital forensics, privacy and organizational security issues.

ARES 2007 aims at a full and detailed discussion of the research issues of security as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.

Important Dates

Workshop Proposal: September, 10th 2006
Submission Deadline: November, 19th 2006
Author Notification: January, 7th 2007
Author Registration: January, 21st 2007
Proceedings Version: January, 21st 2007

Workshop Proposal

In conjunction with the AReS2007 conference, a number of workshops will be organised.

Workshop proposals which should include the call for papers, the number of papers to be accepted, the contact person, etc. are to be sent to the Workshop Organizing Committee (**tho@ifs.tuwien.ac.at**), by September 10th 2006. Proceedings of the ARES 2007 workshops will be published by IEEE Computer Society Press.

Topics of interest include, but are not limited to:

- Process based Security Models and Methods
- Autonomous Computing
- Authorization and Authentication
- Availability and Reliability
- Common Criteria Protocol
- Cost/Benefit Analysis
- Cryptographic protocols
- 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 Business Models with security requirements
- Digital Forensics
- E-Commerce Dependability
- Failure Prevention
- IPR of Security Technology
- Incident Response and Prevention
- Information Flow Control
- Internet Dependability
- Interoperability aspects
- Intrusion Detection and Fraud Detection
- Legal issues
- Mobile Security
- Network Security
- Privacy-enhancing technologies
- 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 issues for sensor networks, wireless/mobile devices and applications
- 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
- Trusted Computing
- Tools for Dependable System Design and Evaluation
- Trust Models and Trust Management
- VOIP/Wireless Security

Submission Guidelines

Authors are invited to submit research and application papers following the IEEE Computer Society Proceedings Manuscripts style: two columns, single-spaced, including figures and references, using 10 fonts, and number each page. You can confirm the IEEE Computer Society Proceedings Author Guidelines at the following web page:

URL: **http://computer.org/cspress/instruct.htm**