

## The Second ACM Workshop on Scalable Trusted Computing (STC'07)

<http://www.cs.utsa.edu/~shxu/stc07/>

### Call for Papers

In a society increasingly dependent on networked information systems, trusted computing plays a crucial role. Despite significant progress in trusted computing components, the issue of scalability in trusted computing and its impact on security are not well-understood. Consequently, there is a dearth of practical solutions for trusted computing in large-scale systems. Approaches suitable for small- or medium-scale trusted computing systems might not be applicable to larger-scale scenarios.

This workshop, built on the success of its predecessor (STC'06), is focused on trusted computing in large-scale systems -- those involving (at the very least) many millions of users and thousands of third parties with varying degrees of trust. The workshop is intended to serve as a forum for researchers as well as practitioners to disseminate and discuss recent advances and emerging issues.

The workshop solicits two types of original papers that are single-column using at least 11pt fonts. The length of the full-paper submissions is at most 12 pages excluding bibliography, appendix etc. The total number of pages should not be more than 20, whereas the reviewers are not required to read the appendix. The length of short/work-in-progress/position-paper submissions is at most 6 pages excluding bibliography. A paper submitted to this workshop must not be in parallel submission to any other journal, magazine, conference or workshop with proceedings. It is up to the authors to decide whether a submission should be anonymous (i.e., no author names, affiliation information appeared in the submission). It is noted that the proceedings versions of the accepted papers will likely be up to 10 pages for full papers and up to 4 pages for short/work-in-progress/position-paper in ACM format. The workshop proceedings will be published by the ACM Press and appear in ACM Digital Library.

Topics of interest to the workshop include the following:

- models for trusted computing
- principles of trusted computing
- modeling of computing environments, threats, attacks and countermeasures
- limitations, alternatives and tradeoffs regarding trusted computing
- trust in authentications, users and computing services
- hardware based trusted computing
- software based trusted computing
- pros and cons of hardware based approach
- remote attestation of trusted devices
- ensorship-freeness in trusted computing
- cryptographic support in trusted computing
- case study in trusted computing
- applications of trusted computing
- intrusion resilience in trusted computing
- access control for trusted computing
- trust of computing systems
- principles for handling scales
- scalable trust support and service
- trusted embedded computing and systems
- trusted computing in networks and distributed systems
- virtualization and trusted computing

**Important dates:**

Submission due: June 20, 2007  
Notification: Aug. 10, 2007  
Proceedings version due: Aug. 22, 2007  
CCS conference: Oct. 29 - Nov. 2, 2007  
STC workshop: Nov. 2, 2007

**Submission information:**

TBA

**PC co-chairs:**

Shouhuai Xu University of Texas, San Antonio  
Moti Yung RSA and Columbia University

**Program Committee:**

Yongdae Kim	University of Minnesota
Klaus Kursawe	Philips Research
Wenbo Mao	EMC Labs
Cristina Nita-Rotaru	Purdue University
Joon Park	Syracuse University
Luigi Romano	University of Naples
Ahmad-Reza Sadeghi	Ruhr-University Bochum
Jean-Pierre Seifert	University of Haifa
Sean Smith	Dartmouth College
Leendert van Doorn	AMD
Haifeng Yu	National University of Singapore
Xiaolan Zhang	IBM Research
Xinwen Zhang	Samsung Research