Preface

Decentralized/distributed data structures (D3S) have recently received a lot of attention with the successful introduction of peer-to-peer systems, Web services, Grids, and ubiquitous computing systems as specific examples of D3S. The "persuasive" arguments in favor of these systems are that they try to avoid centralization as a performance bottleneck, strive for decreasing infrastructure costs and increasing performance by using available distributed resources, and are relatively easy to deploy and maintain due to inherent self-organization properties. Distribution, decentralization and self-organization are the basic underlying concepts facilitating these advantages. However, they also introduce new security problems and make trust a central issue as the behavior and functioning of the system heavily depends on the cooperation and resource contributions of the participants. In hostile environments and if no trust/reputation management system is in place, systems are doomed to fail. Existing, centralized approaches are not applicable and only limited knowledge of the global situation of the system is available to the participants which requires new approaches to address security and trust.

As security and trust are key issues for making any distributed system applicable in an Internet environment, this workshop puts the focus specifically on these problems. For example, how can attacks be detected and be reacted to; how can confidentiality, access control and authentication be supported; how can the trustworthiness of a party be assessed and what mechanisms need to be in place to manage reputation? These are some of the problems that have to be addressed in the context of D3S. We also see this workshop as a forum for raising awareness and allowing researchers in the area exchange and discuss novel ideas and approaches. We were specifically interested in submissions addressing the following areas:

- new perspectives on security and trust problems specific to D3S
- new problems regarding security and trust that arise from the specific domain of D3S environments and how to address them
- novel approaches to existing problems that promise to influence future research
- describing new problems that requires our attention
- debunking old perspectives about security and trust

The workshop received a total of 13 submissions of which 6 where accepted for presentation at the workshop.

We would like to thank everyone who submitted a paper to the STD3S workshop for their interest, the members of the program committee for their high-quality and on-time reviews, and the organizers of ICDE'06 for the possibility to collocate STD3S with ICDE'06.

Manfred Hauswirth, EPFL, Switzerland (Program co-chair)
Andreas Wombacher, University of Twente, The Netherlands (Program co-chair)

Program Committee

Klemens Böhm, University of Karlsruhe, Germany
Ruth Breu, University of Innsbruck, Austria
Sonja Buchegger, UC Berkeley, USA
Germano Caronni, Sun Microsystems Laboratory, USA
David Chadwick, University of Kent, UK
Anwitaman Datta, EPFL, Switzerland
Sabrina De Capitani di Vimercati, Universita degli Studi di Milano, Italiy
Zoran Despotovic, DoCoMo Euro-Labs, Germany
Schahram Dustdar, Technical University of Vienna, Austria
Patrick C. K. Hung, University of Ontario Institute of Technology (UOIT), Canada
Mark Jelasity, University of Bologna, Italy
Wim Jonker, Philips Research, The Netherlands
Ling Liu, Georgia Tech, USA
Sanjay Kumar Madria, University of Missouri-Rolla, USA
Alberto Montresor, University of Trento, Italy
Evaggelia Pitoura, University of Ioannina, Greece
Thomas Risse, Fraunhofer IPSI, Germany
Pierangela Samarati, Universita degli Studi di Milano, Italy
Kai-Uwe Sattler, TU Ilmenau, Germany
Andreas Schaad, SAP Labs, France
Anna Squicciarini, University of Milan, Italy
Can Türker, ETHZ, Switzerland
Lingyu Wang, George Mason University, USA

Workshop Program

10:00	Opening address by the PC chairs
10:05	Invited talk: *Security and Trust in Peer to Peer Systems: Opportunity and Challenges* Ling Liu, Georgia Institute of Technology Abstract: P2P computing is commonly perceived as an infrastructure offering both opportunities and threats. One way to minimize threats in P2P systems is to understand the potential threats and the level of damages they may cause to a P2P system and to increase the system's ability to defend itself from malicious intents, malicious behaviors, and potential threats incurred by known attacks or unpredicted attacks. Attacks on a general P2P system can be targeted at three layers: the network layer (say, TCP/IP), the overlay network layer (say, lookup protocols) and the application layer. There are marked differences in the security issues concerned at each of these layers. Furthermore, the algorithms used at the higher layers largely depend on the guarantees provided by the lower layers. Breaking any of these guarantees provided by a lower level layer to a higher-level layer can disrupt the entire security infrastructure. This invited presentation will provide an overview of various vulnerabilities and the recent research results on security and trust management in decentralized P2P overlay systems, focusing on challenges and opportunity for developing a secure and trusted infrastructure for massively distributed network computing systems and applications. An open discussion will be provided, surrounding the various p2p security applications.
10:55	Break
11:00	Paper session 1 (25 min + 5 min questions) Thomas Schwarz, Peter Tsui and Witold Litwin *An Encrypted, Searchable Database* Jochen Haller *A Stochastic Approach for Trust Management* Stephan Schosser, Klemens Bhm, Rainer Schmidt and Bodo Vogt *Strategic Properties of Peer-to-Peer Data Structures and Behavior of Human Peers in Economic Experiments*
12:30	Lunch break
14:00	Paper session 2 (25 min + 5 min questions) Lars Olson, Marianne Winslett, Gianluca Tonti, Nathan Seeley, Andrzej Uszok and Jeffrey Bradshaw *TrustBuilder as an Authorization Service for Web Services* Anurag Garg, Alberto Montresor and Roberto Battiti *Reputation Lending for Virtual Communities* Muthuramakrishnan Venkitasubramaniam, Ashwin Machanavajjhala, David Martin and Johannes Gehrke *Trusted CVS*
15:30	Break
15:45	Discussion session
17:00	End of workshop