Message from the International Workshop on Security and Trust in Decentralized/Distributed Data Structures (STD3S 2006) Organizers

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 depend 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 must 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 were 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 2006 for the possibility to collocate STD3S with ICDE 2006.

Manfred Hauswirth and Andreas Wombacher
Program Co-Chairs