

'ACM SAC 2005 TRECK Track' Selected Papers

Jean-Marc SEIGNEUR

This special issue contains four revised and extended papers presented and discussed at the track on Trust, Recommendations, Evidence and other Collaboration Know-how (TRECK) of the 20th ACM Symposium on Applied Computing (SAC).

Since Stephen Marsh* wrote his PhD thesis on a computational model of the human notion of trust, computational artificial trust has been gaining momentum in both academia and industry.

One of the reasons for this momentum is the failure of traditional security mechanisms in the face of open global computing environments such as the Internet. Generally, traditional security mechanisms assume that trust can be bootstrapped via external means and a priori trust information based on real-world information. For example, the administrators of two computing domains agree that a common third-party will be trusted to certify the link between a virtual digital entity and a real-world identity: a public key is certified to be owned by a specific user. This approach fails when no agreement about a common third-party between two virtual identities from two different domains has been a priori set up in the real-world.

Computational artificial trust does not require a priori information set in the real-world: trust can be built from scratch. Interaction after interaction, evidence about the trustworthiness of the interacting entities is used to compute a level of trust in these entities. Based on a risk analysis including the level of trust, the requested entity decides which level of privileges should be granted to the requesting entity. If the outcome is positive, greater privileges may be granted during the next interaction.

The paper from [Bicakci et al.](#) focuses on this facet of computational trust, namely security. Bicakci *et al.* propose an approach to incorporate revocation status into the trust metric of public key certification. [Kinateder et al.](#)'s paper also tackles further security enhancements: this time from the point of view of privacy in peer-to-peer reputation systems. [Zuo and Panda](#)'s paper moves away from pure security to information quality assurance in virtual organisations. However, that is [Avesani et al.](#)'s paper that clearly shows that another facet of computational trust is about collaboration, beyond security. Avesani *et al.* extend standard recommender systems with computational trust to improve their performance. Thus, this special issue covers where collaboration and computational artificial trust intermingle: security through collaboration and collaboration filtering.

Many persons have to be thanked for their contributions to this special issue: Christian Jensen who co-chairs the ACM SAC TRECK tracks; the external reviewers and the program committee of the TRECK tracks; all the authors who have submitted their papers to the TRECK tracks; the members of the trustcomp.org online community; the organisers of the ACM SAC; the ACM SIGAPP; the EU iTrust Working Group; and the IJI team.

TABLE OF CONTENT

- Bicakci K., Crispo B., Tanenbaum A. S.
'How to incorporate revocation status information into the trust metrics for public-key certification'
- Kinateder M., Terdic R., Rothermel K.
'Trusting pseudonyms – anonymous communication in peer-to-peer reputation systems'
- Zuo Y., Panda B.
'Object trust management for information quality assurance in virtual organisations'
- Avesani P., Massa P., Tiella R.
'Moleskiing.it: a trust-aware recommender system for ski mountaineering'

* Marsh S. (1994), Formalising Trust as a Computational Concept, PhD Thesis, Department of Mathematics and Computer Science, University of Stirling; citeseer.nj.nec.com.