Electron Commer Res (2010) 10: 235–237
DOI 10.1007/s10660-010-9065-x

Special issue on trust and privacy in electronic commerce

Editors' introduction

Peter Herrmann · Mozhgan Tavakolifard

Published online: 22 October 2010

The most recent developments in computing technology, in particular, the emergence of a new generation of versatile mobile devices will evoke a world in which we nearly always are electronically connected with our environment. In the field of Electronic Commerce, this prospect will offer us undreamed-of business opportunities. It may, however, also cause new security and privacy threats which have to be tackled in order to achieve acceptance for the novel trading possibilities. For instance, we do not want to be bothered by a flood of advertisement messages by companies that are coincidentally in our vicinity but do not have to offer anything, we are currently interested in. To achieve secure and privacy-protecting solutions, we have further to look on trust issues reflecting that the new technologies provide us with the opportunity to cooperate with completely unknown business partners. Yet, to get a realistic and well-funded understanding of an unknown partner, we have to rely on trust management techniques.

This special issue of the Electronic Commerce Research Journal is devoted to present novel research work from leading scientists discussing relevant issues in both trust and privacy of electronic commerce. It contains six contributions which were carefully selected from 13 submissions. Further, we invited the authors of three excellent publications at the Third IFIP WG11.11 International Conference on Trust Management which was held at Purdue University in June 2009 to submit extended versions. The results of the desired amendments are three further outstanding publications completing this special issue.

P. Herrmann (✉) · M. Tavakolifard
Norwegian University of Science and Technology (NTNU), Trondheim, Norway
e-mail: herrmann@item.ntnu.no

M. Tavakolifard
e-mail: mozhgan@q2s.ntnu.no

The most popular method to gain trust in business partners is the use of reputation systems. Here, the experience of several people who already dealt with the intended partner are assembled forming a special kind of reputation. Unfortunately, most practically used systems have major disadvantages, most prominently the collusion of users which makes unjustified good reputations of users possible. Another important drawback is that these systems are vulnerable to confusion by using short-lived online identities. Gayatri Swamynathan, Kevin C. Almeroth and Ben Y. Zhao discuss in their publication a taxonomy on reputation management used to identify adversary threats to reputation systems. Further, they introduce a valuable solution to tackle the two major disadvantages user-collusion and short-lived online identities.

Another relevant topic with respect to reputation systems is how to evaluate their exactitude. Reid Kerr and Robin Cohen present the Trust and Reputation Experimentation and Evaluation Test bed (TREET) that give more accurate results on the strengths of trust and reputation systems than existing evaluation mechanisms.

An important field of application for reputation systems is electronic auction systems. Here, one need mutual trust between the sellers and bidders of a good but also has to assure that the auction server is benevolent and just to all parties. In particular, the correctness of the auctioning process must be verifiable. Giovanni Di Crescenzo, Javier Herranz and Germán Sáez introduce a novel auction scheme guaranteeing minimal interaction among the involved parties and demanding trust in the integrity of only one of the applied auction servers.

Besides more technical issues, an auction system also causes social effects that are often hidden to the ordinary user but should be aware to the system developers in order to adapt the system design in a way making the reputations more trustworthy. Radoslaw Nielek, Aleksander Wawer and Adam Wierzbicki present material collected from Allegro, Poland's largest auction house. In particular, they use special algorithms to extract the sentiment-oriented factors of comments on auction partners. The analysis renders a number of worthwhile results leading to a list of meaningful suggestions to improve the trustworthiness and security of auction platforms.

A new mechanism to handle user feedbacks in peer-to-peer reputation systems is introduced by Thanasis G. Papaioannou and George D. Stamoulis. Here, all peers taking place in a transaction submit a rating on the transaction in general. A divergence of the ratings by the different peers is an unmistakable sign of a liar in the system which leads to punishing the different parties. To get a good guess who is the liar, the authors use a non-credibility metric deciding about the severity of the punishment. The approach is modeled as a Markov chain and experiments prove its high accuracy.

Another trust-related issue in electronic commerce is the handling of electronic bills of lading (e-BOL) which are the enablers for the payment of goods. A zero-knowledge solution to prevent the bills from forgery is presented by Anastasia Pagnoni and Andrea Visconti. In particular, their approach avoids to reveal information about the actually counted quantity of a good using a cryptographic protocol based on digital signatures and blind merchandize counts.

Sunitha Ramanujam, Anubha Gupta, Latifur Khan, Steven Seida and Bhavani Thuraisingham provide an interesting insight in using trust-based methods in Semantic Web technology. In their article, they introduce an algorithm to handle Resource Description Frameworks (RDF) determining the trustworthiness of Internetbased data using provenance information about the data (e.g., how and by whom the data came to be).

The handling of data in electronic commerce-based applications, however, is also a major privacy risk. For this reason, many organizations are reluctant to share their data with business partners. Markus Eurich, Nina Oertel and Roman Boutellier present the results of a study aiming to find out the actual willingness of companies to share data and the privacy risks perceived in this context. From the results, the authors derived a set of requirements to make the sharing of inter-organizational data safe.

The special issue is completed by a paper from Tormod V. Håvaldsrud, Olav S. Ligaarden, Per Myrseth, Atle Refsdal, Ketil Stølen and Jon Ølnes who proved that model-based trust analysis methods are sufficiently mature to render relevant results in an industrial environment. In particular, the authors analyzed an electronic procurement system based on digital certificates in the name of the Norwegian risk management institution Det Norske Veritas (DNV). The results of this analysis enabled a better understanding of the risks of trust-based decisions within procurements.

Acknowledgements

This special issue would not be possible without the help of several people. At most we have to thank the authors of all accepted and rejected papers for presenting a plethora of excellent ideas which were great fun reading. Also most of the rejected papers were of high quality and it was often just a detail which decided about passing the target line. Further, we like to express our deep gratitude to Ebrahim Bagheri, Christian Damsgaard Jensen, Georgous Pitsilis, Stephen Marsh, Yue Xu, Gabriele Lenzini, Jean-Marc Seigneur and Svein Johan Knapskog who took the heavy burden to review the papers. The reviews were not always on time but every single one was carried out highly accurately and helped the authors to improve the publications up to their current standard. Moreover, we are grateful to Bezalel Gavish and Jackie James, the effective engines of the Electronic Commerce Research Journal. Jackie helped the authors to bring the articles into their proper camera-ready state while Bezalel, the editor-in-chief, showed again his trust in our organizational skills. We hope that we fulfilled his expectations.

Trondheim, May 2010 Peter Herrmann and Mozhgan Tavakolifard