ACIS2007 SPECIAL COLLECTION

This special collection comprises extended versions of selected papers presented at the Australasian Conference on Information Systems 2007. ACIS2007 was held at the University of Southern Queensland in Toowoomba in December 2007. The theme of the conference was the three Rs: Research, Relevance and Rigour, and in light of the 18th anniversary of the conference, celebrated the ‘coming of age’ of the IS academic discipline in Australia.

We received 176 submissions to our call for papers from authors in over 20 countries. We accepted for publication and presentation 115 papers. All papers were subjected to a double-blind review process with at least two reviewers and a program track chair assessing the quality of the submissions.

We invited authors to extend their papers for consideration in this special collection for JRPIT. Four submissions were received and each revised paper was reviewed by at least two reviewers as well as the special collection editors. As a result of this rigorous process, two papers were selected for publication in this issue.

The first article “A General Framework to Measure Organizational Risk during Information Systems Evolution and its Customization” by Aditya Agrawal, Gavin Finnie and Padmanabhan Krishnan presents the Organization Risk Evaluation (ORE) framework to help decision makers measure risk during organization-wide change initiatives. The ORE framework is customized into the ERP-ORE framework to demonstrate its application in Enterprise Resource Planning applications. The ERP-ORE framework emphasizes the political and process dimensions of systems evolution and uses the Analytic Hierarchy Process to enable management to make disciplined risk mitigation decisions.

In the second article “An Ontology-Driven Approach Applied to Information Security”, Artem Vorobiev and Nargiza Bekmamedova argue that the collaboration of a system’s constituent components is a better way to detect and withstand the new generation of security attacks such as multi-phased distributed attacks and various flooding distributed denial of service attacks. They develop and apply security ontologies that will serve as the common vocabulary understandable for both humans and software agents to share and analyse the received information. They introduce the security attack ontology, the defence ontology, the asset-vulnerability ontology, the algorithm-standard ontology, and the security function ontology, concluding with a demonstration of the applicability of their approach with a case study illustrating the Mitnick attack.

We would like to thank Rosemary Hay for guiding us through the editorial process for JRPIT, and Professor Sidney Morris, the previous Editor-in-Chief of JRPIT for providing the opportunity of this special collection. We are also indebted to the reviewers who provided valuable comments to the authors and helped strengthen the papers.

Professor
Mark Toleman
ACIS2007 Program Chair
School of Information Systems
Faculty of Business
University of
Southern Queensland
Toowoomba

Associate Professor
Aileen Cater-Steel
ACIS2007 Organising Chair