SPECIAL COLLECTION: Workshop on Security in Information Systems (WOSIS) 2008

Information Systems Security is one of the most pressing challenges currently facing all kinds of organizations. However, ensuring security and quality in information and the systems which manage information is a complex goal which necessitates the combination of two wide research disciplines which are usually separate: security engineering and security software engineering. The first discipline has a long history, and has usually focused on providing advances in security models, protocols, and techniques. Security software engineering, however, is relatively recent but is swiftly maturing and is focused on the integration of security in software engineering techniques, models and processes, in order to develop more secure information systems.

This Special Collection of the International Journal of Research and Practice in Information Technology therefore includes the extended and improved versions of those papers that were selected from the best of the International Workshop on Security in Information Systems, and aims to serve as a forum in which to unite academics, researchers, practitioners and students in the field of security engineering and security software engineering, by presenting new developments and lessons learned from real world cases, and to promote the exchange of ideas and the discussion and development in these areas. This edition is the sixth in a series, which began in Ciudad Real (Spain) in 2002, and has continued in Porto (Portugal), Paphos (Cyprus), Miami (USA), Funchal, Madeira (Portugal), and Barcelona (Spain), respectively. This relatively long history (WOSIS is now in its ninth edition) has given the workshop a considerable reputation, and it receives an average number of submissions of almost fifty, with an acceptance rate of approximately thirty five percent.

Our workshop has matured year by year, and is now established as a forum for high quality research papers in the area of security in information systems. The most valuable assets of this workshop, which make it attractive to authors, are the highly exclusive set of program committee members (comprising 25 members of 11 nationalities), along with the invitation of exceptional speakers who are highly relevant in this scientific area. Among these, we can mention, for example, Yvo Desmedt, Sushil Jajodia, Ernesto Damiani, Leonardo Chiariglione, Ruth Breu, Eduardo B. Fernández, and Sabrina De Capitani. Additionally, selections of the best papers of past editions of the workshop have been published in international journals such as Information Systems Security, Journal of Research and Practice in Information Technology, Internet Research, and Computer Standards and Interfaces.

A brief introduction to each selected paper is presented in the following paragraphs.

In the first paper, entitled "A Multi-Dimensional Classification for Users of Security Patterns", by VanHilst *et al*, the authors offer contributions in the area of security patterns, presenting a method through which to organize patterns to address pattern coverage, and facilitate pattern discovery, exploration, and navigation by the application developer.

The second contribution, entitled "Network Access Control Configuration Management using Semantic Web Techniques", by Fitzgerald *et al*, presents an approach towards using a Description Logic constrained ontology to construct, reason about and manage Network Access Control policies in the context of risk-driven service policy requirements.

The third paper, "Modelling Reusable Security Requirements based on an Ontology Framework", by Lasheras *et al*, also deals with the area of security ontologies, and in this case, proposes a security requirements ontology which represents reusable security requirements, and which is used to produce a method with which to elicit and specify security requirements.

The fourth contribution, "Applying QVT in order to implement Secure Data Warehouses in SQL Server Analysis Services", by Blanco *et al*, introduces an application of the Model Driven

Architecture for the automatic code generation of secure data warehouses to be implemented in SQL Server Analysis Services.

The fifth contribution, entitled "Integrating Privacy Policies into Business Processes", by Chinosi and Trombetta presents new advances in the area of secure business processes, proposing a data model for BPMN and a corresponding XML representation which can be used to check the privacy policy compliance of business processes.

The sixth contribution, "Lightweight Anonymous Routing for Reliability in Mobile Ad-Hoc Networks", by Shao and Huang proposes a trust-aware and lightweight anonymous routing protocol for Mobile ad-hoc Networks to ensure security and privacy in which only trustworthy intermediate nodes can participate in data forwarding activities.

Finally, the seventh contribution, entitled "New Attack Strategy for the Shrinking Generator", by Caballero-Gil *et al*, proposes a new deterministic cryptanalytic attack against the class of shrinking generators, which consists of defining the shrunken sequence as an interleaved sequence, and then using the weaknesses inherent in its interleaved configuration to launch a practical attack.

We would like to thank Professor Sidney Morris, the Editor-in-Chief of The Journal of Research and Practice in Information Technology and Ms Rosemary Hay for their valuable help and support. We are also extremely grateful for the hard work and kindness of all the members of our international program committee when performing their timely, complete and professional reviews. Last, but not least, we would like to thank the authors for their contributions.

Eduardo Fernández-Medina, PhD
Guest Editor
Associate Professor
University of Castilla-La Mancha
Ciudad Real, Spain

Eduardo
Fernández-Medina

Alfonso Rodríguez, PhD
Guest Editor
Associate Professor
University of Bio-Bio
Chillán, Chile
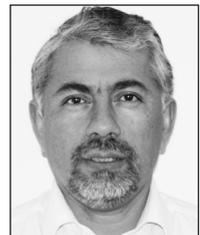
Alfonso Rodríguez

Mariemma Yague, PhD
Guest Editor
Associate Professor
University of Málaga
Málaga, Spain

Mariemma Yague