GUEST EDITORIAL PREFACE

Special Issue on 7th International Workshop on Secure Software Engineering (SecSE 2013)

Martin Gilje Jaatun, Department of Software Engineering, Safety and Security, SINTEF ICT, Trondheim, Norway

Riccardo Scandariato, Department of Computer Science, KU Leuven, Leuven, Belgium

Lillian Røstad, Department of Computer and Information Science, Norwegian University of Science and Technology, Trondheim, Norway

This Special Issue contains revised and extended versions of the top 3 papers presented at the *7th International Workshop on Secure Software Engineering* (SecSE 2013), which was part of the 8th International Conference on Availability, Reliability, and Security (ARES 2013) held in Regensburg, Germany.

The papers in this Special Issue have all gone through additional review by at least 3 international experts, and represent a significant extension of the workshop contributions. The papers are all focused on the theme of security requirements.

Existing approaches to security requirements engineering mostly consider goals and threats separately, and thus neglect the mutual influence between them. In their paper "*Threat Analysis in Goal-Oriented Security Requirements Modelling*", Per Håkon Meland et al. present an approach to security requirements engineering that extends goal modelling with threat modelling and analysis. The purpose is to be able to consider both goals (that express why a system is needed) and threats (that motivate the need for security) at the same time - and not separately.

Isabelle Cote et al. introduce a methodology for security requirements engineering in their paper titled "*A Structured Method for Security Requirements Elicitation concerning the Cloud*

Computing Domain". The methodology is suitable for applications that are to be deployed in the cloud and takes the perspective of a SME that has to select a cloud provider fitting the application's security needs. The methodology is based on analysis patterns and is supported by tools.

Finally, in their paper "*Automated synthesis and ranking of secure BPMN orchestrators*", Vincenzo Ciancia et al. present a methodology for securely creating a composite service through orchestrating a set of Business Process Model and Notation (BPMN) processes. Their method can also rank alternative orchestrators with respect to security based on the knowledge available to the attacker.

We thank Editor-in-chief Khaled M. Khan for his support for the SecSE workshop series throughout the years, and the reviewers for their efforts in improving the quality of this Special Issue.

Martin Gilje Jaatun
Riccardo Scandariato
Lillian Røstad
Guest Editors
IJSSE

Martin Gilje Jaatun graduated from the Norwegian Institute of Technology in 1992, and is now a Senior Scientist at SINTEF ICT in Trondheim, where he has been employed since 2004. His research interests include software security "for the rest of us", information security in critical infrastructure environments, and security in Cloud Computing. He is an Associate Editor of the International Journal of Secure Software Engineering.

Riccardo Scandariato received his PhD in Computer Science in 2004 from Politecnico di Torino, Italy. He leads a team of researcher in secure software at the DistriNet Research Group of KU Leuven, Belgium. His research interests focus on empirical methods for security and security in software architectures. He has published 50 papers in the area of security and software engineering. He is an Associate Editor of the International Journal of Secure Software Engineering.

Lillian Røstad received her PhD in Information security from the Norwegian University of Science and Technology (NTNU) in 2009, and is currently head of the Information Security Section at Difi - the Norwegian Agency for Public Management and eGovernment. She is also adjunct associate professor at NTNU since 2008, where she is teaching courses on Software security and Information security in software systems.