Guest Editorial Preface

Special Issue from the 5th International Workshop on Secure Software Engineering

Martin Gilje Jaatun, SINTEF, Norway

Per Håkon Meland, SINTEF, Norway

What is software security? It is still considered to be a relatively new field, just a little bit more than a decade old, though of course the wider field of computer security has a much longer history. Judging from the span of submissions that are submitted to our annual workshop on software security, we get the impression that some practitioners tend to put too much into this bag, such as cryptology, firewalls, access control models and trusted computing. So, let us try to narrow it down a bit. We argue that the *art* of software security is about making software systems robust and less exploitable without the need for barriers in the operating system, hardware or surrounding networks. It should address critical software and your ordinary home applications alike; after all, most of the software that surrounds us is found on your everyday device, such as the laptop, TV or mobile phone, and these have not been set up with proper external protection. Our Holy Grail is that software security should be considered a self-evident quality aspect on par with absence of functional bugs. We hope that IJSSE will be of great help to those of us who seek this Grail.

This special issue contains revised and extended versions of the top 4 papers presented at the 5th International Workshop on Secure Software Engineering (SecSE 2011), which was part of the 6th International Conference on Availability, Reliability, and Security (ARES 2011) held 22-26 August 2011 in Vienna, Austria.

The papers in this special issue have all gone through additional review by international experts, and represent a significant extension of the workshop contributions. The papers cover many important facets of the software security field, spanning elicitation of security requirements and security evaluation, via a framework for security protocol implementation, and closing with a survey on security in Model Driven Development.

Faily and Fléchais present how to combine security and usability in "*Eliciting Policy Requirements for Critical National Infrastructure using the IRIS Framework*". Jung, Rudolph, and Schwarz elaborate their architectural-level method for security evaluation of existing SOA configurations in "*Security Evaluation of Service-oriented Systems using the SiSOA Method*". Avalle et al. describe a Model Driven Development framework that allows reliable development of security protocol implementations using Java in "*JavaSPI: A Framework* *for Security Protocol Implementation*", starting from abstract models that can be verified formally. Finally, Jensen and Jaatun dive into the state of the art in security and Model Driven Development in their article "*Not Ready for Prime Time: A Survey on Security in Model Driven Development*", concluding that more empirical evidence is needed before a definite conclusion can be reached on whether MDD/MDA is a good option for developing more secure code.

We thank Editor-in-chief Khaled M. Khan for inviting us as guest editors, and the reviewers for their efforts in improving the quality of this Special Issue. Special thanks to Gary McGraw, CTO of Cigital, for a very inspiring invited talk at this year's workshop. SecSE 2012 will be held in Prague, Czech Republic, and we cordially invite you to submit your contributions. We hope that SecSE will continue to be a vibrant venue for lively discussions in the secure software engineering community!

Martin Gilje Jaatun
Per Håkon Meland
Guest Editors
IJSSE

REVIEWERS FOR THIS SPECIAL ISSUE

Ruben Alonso, Visual Tools
Ana Cavalli, Institut National des Télécommunications
Bart De Win, KU Leuven
Estebaliz Delgado, Tecnalia
Christophe Feltus, Centre de Recherche Public Henri Tudor
Khaled M. Khan, Qatar University
Per Håkon Meland, SINTEF
Khalid Azim Mughal, University of Bergen
Pierre Parrend, Proxiad
Chunming Rong, University of Stavanger
Christoph Schuba, Sun Microsystems, Inc.
Nahid Shahmehri, Linköpings Universitet
Torbjørn Skramstad, NTNU
Emin Tatli, IBM
George Yee, Carleton University
Stephen Wolthusen, Royal Holloway University of London

Martin Gilje Jaatun graduated from the Norwegian Institute of Technology in 1992, and has been employed as a research scientist at SINTEF ICT in Trondheim since 2004. His research interests include software security "for the rest of us", information security in critical infrastructure environments, and security in Cloud Computing.

Per Håkon Meland graduated from NTNU in 2002, and has since been employed as a research scientist at SINTEF ICT in Trondheim. His research interests include software security and service engineering within domains such as healthcare and telecom, and with a special focus on early security awareness and improvements during the software development lifecycle.