Guest Editorial Preface

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

Software Security is about making things that do not break when hammered. Intuitively, most people understand that this is important for security software, but even seasoned developers sometimes forget that the most innocuous software such as PDF readers can be made to do pretty bad things to a user's computer if tricked into doing so by malformed documents.

This Special Issue contains revised and extended versions of the top 3 papers presented at the 6th International Workshop on Secure Software Engineering (SecSE 2012), which was part of the 7th International Conference on Availability, Reliability, and Security (ARES 2012) held 20-24 August 2012 in Prague, Czech Republic. The SecSE workshop series aims to explore all the different ways developers can be helped to make ordinary software more secure.

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 cover many important facets of the software security field, ranging from security modeling to taxonomies.

First, Meland and Gjære investigate several possibilities of representing threats in BPMN 2.0, in particular for design-time specification and runtime execution of composite services with dynamic behavior in the article "Threat Representation Methods for Composite Service Process Models". In their article "Mitigating Type Confusion on Java Card", Dubreuil, Bouffard, Thampi, and Lanet describe a framework based on annotations to switch the Java Card Virtual Machine (JCVM) into a secure mode by activating a set of countermeasures, triggering a transformation of the original program byte codes into a semantically equivalent, but mutant fault proof version. Finally, Corcalciuc ventures to dissect the anatomy of time and state attacks in "A Taxonomy Built on Layers of Abstraction

for Time and State Vulnerabilities", offering a taxonomy based on abstraction layers, thereby classifying attacks according to what they have in common.

I want to thank Editor-in-Chief Khaled M. Khan for his continuous support of the SecSE workshop, and the reviewers for their efforts in improving the quality of this Special Issue. SecSE 2013 will be held in Regensburg, Germany, and we hope to see you there.

Martin Gilje Jaatun
Guest Editor
IJSSE

SPECIAL ISSUE REVIEWERS

Ruben Alonso, Visual Tools
Estibaliz Delgado , Tecnalia
Christophe Feltus, Centre de Recherche Public Henri Tudor
Khaled M. Khan, Qatar University
Chunming Rong, University of Stavanger
Hossain Shahriar, Kennesaw State University
Panagiotis Trimintzios, ENISA
Mohammad Zulkernine, Queen's University

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.