EDITORIAL PREFACE

Khaled M. Khan, Qatar University, Qatar

As a medium for reporting scholarly work in secure software engineering, IJSSE owes its second year existence to those authors who have been brave enough to share their research findings through this new journal last one year or so. It is also equally encouraging to see that researchers are willing to share their findings and experiences using IJSSE. Like other new scholarly journals, IJSSE is also no exception-struggling to build up its backlogs of quality manuscripts since its inception. In order to keep going at its aim, this issue catalogs four papers from various subfields of security and secure software engineering.

The first paper by Kim Wuyts et al. explores the consequences of integrating patient consent in e-health access control policies. The proposed architecture incorporates patient consent in the access control service of an e-health system, and shows some interesting results. The second paper written by Wesam Darwish and Konstantin Beznosov analyzes access control mechanisms of the Enterprise Java Beans (EJB) architecture and proposes a configuration of the EJB protection system. It also proposes an algorithm that formally specifies the semantics of authorization decisions in EJB.

The third paper by Jan Durand et al. reports a research effort on executable slicing technique as a pre-processing aid to improve the prediction performance of rogue software detection. It shows some interesting findings on the application of randomized projections in detecting rogue software. The fourth paper by Yun Bai and myself proposes a formal technique with modal logic to specify system security policies. The paper demonstrates how this approach handles the situation where the security agent’s knowledge on access decision is incomplete. It is expected that the proposed mechanism would effectively prevent unauthorized access and malicious attempt to the information systems.

Khaled M. Khan
Editor-in-Chief
IJSSE