Editorial Preface

Khaled M. Khan, Qatar University, Doha, Qatar

Secure software engineering can address some of the challenging issues posed to contemporary software paradigms such as cloud computing, more specifically software-as-a-service (SaaS) where a single program caters multiple cloud clients using virtualization. Ensuring secure software is a must in such an environment. Vulnerabilities in software offered by SaaS definitely threat hundreds of users of the cloud services. It is interesting to see how secure software engineering could contribute to these security challenges related to cloud computing.

In this issue, we have lined up three papers in three but related research areas. The first paper by Shahriar and Haddad tackles the issue of evaluating vulnerability related risk in web application. It particularly shows how to compute the probability of vulnerabilities and exploitations in web based system. The paper proposes a fuzzy logic based system to compute the risk along with a set of crisp metrics that are used to define fuzzy sets. The second paper by Omoroniya presents an initial process framework for the identification of privacy awareness. The paper argues that a systematic approach for privacy awareness research needs investigation of an appropriate representation language, analysis mechanisms and understanding the socio-technical factors. Nasser Al-Hadhrami and colleagues in the third paper present Role Based Access Control (RBAC) models of software using B specifications and the verification of the consistency of the RBAC specification, using model checking and proof obligations.

We welcome proposals for special issues on any emerging topic related to secure software engineering. We also consider conference or workshop papers for special issues. Our review process usually concludes within ten weeks from the initial submission.

Khaled M. Khan
Editor-in-Chief
IJSSE