This inaugural issue marks the publication of the International Journal of Secure Software Engineering (IJSSE) which is considered first in its kind. Prior to this inauguration of the International Journal of Secure Software Engineering (IJSSE), there was no single, dedicated journal to discuss the issue of secure software engineering. I find myself privileged to write this editorial to introduce this new journal. I consider this for any Editor-in-Chief as a once-in-a-lifetime event. This inaugural issue is the culmination of several months' worth of motivation, discussion and planning. My immediate thanks goes out to several of my colleagues for guiding the journal from initial inception to the inaugural issue we see it now. I am immensely grateful to the publisher IGI-Global, well-wishers, fellow professionals, and critics who have been of great help to me bringing out this journal.

The main objective of this journal is that it will be the eminent communication of knowledge for software engineers and security experts. This issue documents contributions from many leading researchers who have been working on secure software systems for a long time. We received many articles—thank you to all the authors for their submission. My deep appreciation and gratitude is due to all reviewers who provided constructive and comprehensive reviews within six weeks time limit. Most of the reviewers set the benchmark for their detailed and thorough reviews. We also thank the external reviewer Achim D. Brucker from SAP Germany for his help in the review process.

This issue presents five articles addressing a broad range of topics in secure software engineering. The first article, by Thuong Doan, Steven Demurjian, Laurent Michel, and Solomon Berhe from the University of Connecticut, presents an interesting approach to integrate role-based and mandatory access control into use-case, class diagrams, and sequence diagrams of the unified modeling language. The article provides a consistent approach to secure software modeling and the development process. San-Tsai Sun and Konstantin Beznosov from the University of British Columbia, in our second article has proposed an approach to runtime SQL injection attack protection, as well as a tool that implements the approach. The tool has an encouraging performance data for the tested applications as reported in the article. Our third article, by Yun Bai from the University of Western Sydney, proposes a protection mechanism and examines a formal approach to secure web-based XML documents. In order to achieve this, the article introduces a high level language to specify an XML document and its protection authorizations.

The fourth article, by Armstrong Nhlabatsi, Bashar Nuseibeh and Yijun Yu from the Open University, provides a review of current approaches to security requirements engineering and their support for managing the effects of software evolution. The article suggests a cross fertilization of the areas of software evolution and security requirements engineering to address the problem of maintaining software systems as they evolve. Our final article comes from the Software Engineering Institute, Carnegie Mellon University. In this article, Nancy Mead reports the results of several pilot case studies in security requirements engineering providing both benefits and challenges to the underlying research, education, and technology transition effort. The article
justifies the benefits and challenges of such case studies, and discusses their practical relevance and application to ensuring adequate information assurance protection.

We look for submissions of interesting research outcome as well as practices in secure software engineering. Whether there are immediate practical implications or not, high quality research outcomes will be nurtured and presented with pride in this journal. Our endeavor is also to cultivate cross disciplinary research between security and software engineering in order to enhance our understanding further of the field.

Our goal is to have a rapid peer review process, and we will make every effort to make an initial decision within six weeks of submission. I believe that an effective peer review process significantly contribute in producing high quality articles with outstanding merits. Our editorial review board includes world-class researchers and a comprehensive international distribution. There are plenty of reasons to expect that this journal will set new standards for the study of secure software engineering.

I look forward to a most interesting and lasting future for the International Journal of Secure Software Engineering.

Khaled M. Khan
Editor-in-Chief

Khaled Khan is serving the Department of Computer Science and Engineering at Qatar University. He also holds an honorary adjunct fellow position in the School of Computing and Mathematics at the University of Western Sydney (Australia). Prior to these positions, Khan served as an academic in computing at the University of Western Sydney for seven years. He was the head of programs for the postgraduate computing courses at the University of Western Sydney for six years. He has taught computing last twenty years at various universities in Asia, Europe, Africa, and Australia. His research interests include software security, software component, software architecture, Web services, and service-oriented software. He received his PhD in computing from Monash University and a BS and MS in computer science and informatics from the Norwegian University of Science and Technology (Norway). He also holds a second bachelor's degree from the University of Dhaka (Bangladesh). Khan has published more than fifty refereed papers and additionally has edited two books. Khan is currently serving several editorial boards of different journals and conference program committees. He contributed to the IEEE-ACM Computing Curricula 2001.