I am pleased to bring you this special issue on security modeling which is an important area of secure software engineering. The main objective of security modeling is to create abstract representations of security concerns of a software system ranging from threat modeling to security policy manifestation. Various techniques used in security modeling help software engineers to focus on critical security issues, and model them for the understanding of all stakeholders. The model can act as a source for decision making and verification of various security concerns of the system before implementation. It helps software engineers to model potential attack scenarios, malicious behaviors, countermeasures, security policies, risks, vulnerabilities, and so on.

When some members of our editorial board and I decided for a special issue on security modeling, we did not have a clear idea of the quality of the scholarship that we would attract. We also could not anticipate the number of submissions that could be sufficient to publish a special issue. I am delighted to report that many authors did show up for this special issue. Our initial uncertainty was clearly found baseless; many researchers responded to our call for papers with their provocative and interesting research findings and ideas for this special issue. The number of submissions exceeded our expectation. We received so many interesting papers that we have decided to publish the accepted papers in two sequential special issues of IJSSE on the same topic. Having survived a rigorous peer review process, three papers have been published in this issue, and three more will appear in the next issue (Volume 3, Issue 3) of IJSSE. I thank to all reviewers who completed their review within our six-week timeframe despite their busy schedules. I specially thank our Associate Editor Per Håkon Meland for his assistance in the preparation and distribution of call for papers of this special issue.

The line-up of the papers is as follows. Baghato, Kordy, Meland, and Schweitzer lead this special issue with their research paper describing a practical case study with attack–defense trees for a warehouse. The paper explores how to use a rich set of attributes for modeling attack and defense. In the second paper, Pavlidis, Mouratidis, and Islam introduce trust-based concepts to identify trust assumptions, and integrate the trust concepts with security concepts for the development of secure software systems. The paper extends Secure Tropos with trust modeling activities based on trust-based concepts. In the final paper, Karpati, Sindre, and Matulevičius investigate whether mal-activity diagrams are
more efficient than misuse cases for understanding social engineering attacks and finding prevention measures. They present a conceptual comparison of the modeling techniques with a controlled experiment. It compares the efficiency of using the two techniques together with textual descriptions of social engineering attacks.

In sum, this special issue of IJSSE is expected to encourage more research on security modeling tools and techniques, and address the challenges of modeling security concerns of software during the development process.

Khaled M. Khan
Editor-in-Chief
IJSSE