GUEST EDITORIAL PREFACE

Special Issue on Quantitative Aspects in Security Assurance

Alessandro Aldini, University of Urbino, Urbino, Italy

Fabio Martinelli, Pisa Research Area, National Research Council – CNR, Pisa, Italy

Neeraj Suri, Technische Universität Darmstadt, Darmstadt, Germany

As security becomes a key ICT enabler, there has been a corresponding need to provide quantification of security assurance over the multi-level development life-cycle of systems and services. With its specific emphasis on quantification, the International Workshop on Quantitative Aspects in Security Assurance (QASA) has emerged as a forum to bring together researchers and practitioners interested in the quantification research dimensions spanning dependability, security, privacy and risk, and with particular emphasis on techniques for service oriented architectures.

The three past editions of QASA, held alongside the European Symposium on Research in Computer Security (ESORICS), collected contributions on several topics ranging from metrics for trust, security and privacy, to quantitative information flow analysis, and from model-based techniques for assurance to quantitative issues in access and usage control.

This special issue includes five QASA contributions focusing on different quantitative aspects of security assurance. The first paper by Gay, Mantel, and Sudbrock, provides a quantitative evaluation of interrupt-related covert channels, which is based on both empirical experiments and information-theoretic analysis. Chothia, Novakovic, and Singh present an information flow based framework for estimating measures of data integrity for programs written in an imperative language. In this setting, integrity for probabilistic specifications is a notion based on conditional mutual information and entropy. Beckers, Krautsevich, and Yautsiukhin investigate social engineering threats and propose an integrated approach based on attack graphs to detect such vulnerabilities in a context in which also technical threats may be combined by potential attackers. In their work, Armando, Bezzi, Metoui, and Sabetta propose a risk-aware access control framework for information disclosure. Adaptive and on-the-fly anonymization techniques are used to trade risk for privacy. Finally, the purpose of the contribution by Erdogan, Seehusen, Stølen, Hofstad, and Aagedal, is to assess the usefulness of testing security risk models in the practical setting of two industrial case studies.

We are grateful to the security research community for supporting QASA in these years and to IGI Global and the Journal of Secure Software Engineering for the opportunity to host this special issue.

Alessandro Aldini
Fabio Martinelli
Neeraj Suri
Guest Editors
IJSSE

Alessandro Aldini received his PhD at the University of Bologna, Italy, and is currently associate professor at the Department of Base Science and Fundamentals of the University of Urbino "Carlo Bo", Italy. His research interests are focused on the study and application of automated methodologies for the design and verification of computer and network systems, with a particular emphasis on foundations of security, trust, performance, and dependability analysis and design of complex, concurrent, and distributed systems. He has co-authored one book for Springer, about 60 peer-reviewed papers published on international journals and conference proceedings, and guest-edited about a dozen books for international leading publishers.

Fabio Martinelli is a senior researcher of Institute of Informatics and Telematics (IIT) of the Italian National Research Council (CNR) where He leads the cyber security project. His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He founded and chaired the WG on Security and Trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM). He is currently chair of the WG 11.14 in Secure Engineering of the International Federation of Information Processing (IFIP). He is the co-chair of the Italian technological platform in homeland security (SERIT) and He co-chairs the WG3 on Research and Innovation of the Network and Information Security (NIS) Platform promoted by the European Commission.

Neeraj Suri is the TUD Chair Professor of "Dependable Systems and Software" at TU Darmstadt, Germany and also affiliated with the University of Texas at Austin. Following his PhD at the University of Massachusetts at Amherst, he has held both industry and academic positions at Allied-Signal/Honeywell Research, Boston University, Saab Endowed Chair Professor, and also receiving trans-national funding from the EC, German DFG/BMBF/DAAD, SSF/VINNOVA, US-NSF/DARPA/ONR/AFOSR, NASA, Microsoft, IBM, Hitachi, Saab, Volvo, Daimler, GM and others. He is a recipient of the NSF CAREER award, as well as Microsoft and IBM Faculty Awards. Suri's professional services span associate Editor-in-Chief for the IEEE Trans. on Dependable and Secure Computing, editorial boards for IEEE Trans. on SW Eng., IEEE TPDS, ACM Computing Surveys, IEEE Security & Privacy and many others including being PC-chair of the spectrum of dependability/security conferences. He serves on advisory boards for Microsoft (Trustworthy Computing Academic Advisory Board) and multiple other US/EU/Asia industry and university advisory boards. Suri chaired the IEEE Technical Committee on Dependability and Fault Tolerance, and its Steering Committee.