Software Quality Journal (2019) 27:921–922
https://doi.org/10.1007/s11219-019-09450-9

Special issue on trustworthy systems and software

Sudipto Ghosh[1] · **Zhenyu Chen**[2]

Published online: 28 June 2019

Today in many fields and tasks, systems and software play a critical role and can sometimes replace humans to improve efficiency and safety. The world has come to depend on local and wide-area software systems to support essential economic, social, and government services. However, severe consequences such as loss of life and property can be caused by compromised systems and defective software. To make systems and software more robust, reliable, and trustable, and to protect them from various threats such as security intrusion, misuse, and unauthorized access, both academia and industry are seeking novel techniques, tools, and applications to produce dependable and trustworthy systems and their applications in a more cost-effective way. However, in spite of decades of research and practical experience in software testing and the evolution of underlying theories, methods, and tools, the development of trustworthy systems in industry is still very challenging.

In this Special Issue on Trustworthy Systems and Software, four papers are presented that investigate issues in diverse areas ranging from defect prediction, API trustworthiness, fault tree analysis, and cross-architecture vulnerability search in firmware.

The first paper, "A New Weighted Naive Bayes Method Based on Information Diffusion for Software Defect Prediction," by Haijin Ji, Song Huang, Yaning Wu, Zhanwei Hui, and Changyou Zheng proposes an approach to identify the most defect-prone modules for allocating limited testing resources.

The second paper, "API Trustworthiness: An Ontological Approach for Software Library Adoption," by Ellis E. Eghan, Sultan S. Alqahtani, Christopher Forbes, and Juergen Rilling proposes an Ontological Trustworthiness Assessment Model to analyze and assess trustworthiness attributes of libraries and APIs in open-source systems, and their impact on the quality and trustworthiness of the project in which they are used.

The third paper, "A Minimization Algorithm for Automata Generated Fault Trees with Priority Gates," by Nidhal Mahmud proposes an approach to reduce the fault tree expressions that are generated from automata representations of failure behaviors. The minimal

✉ Sudipto Ghosh
ghosh@cs.colostate.edu

Zhenyu Chen
zychen@nju.edu.cn

[1] Department of Computer Science, Colorado State University, Fort Collins, CO, USA

[2] State Key Laboratory for Novel Software Technology, Software Institute, Nanjing University, Nanjing, China

failure sequences that can be determined from the reduced models are used to improve the analysis of fault sequencing and propagated errors, resulting in the design of improved failure prevention measures.

The fourth paper, "CVSSA: Cross-architecture Vulnerability Search in Firmware Based on kNN-SVM and Attributed Control Flow Graph," by Dongdong Zhao, Hong Lin, Linjun Ran, Mushuai Han, Jing Tian, Liping Lu, Shengwu Xiong, and Jianwen Xiang seeks to improve the accuracy of searching for known vulnerabilities in binary firmware across different architectures. The approach uses support vector machines and an attributed control flow graph to improve the accuracy using prior knowledge.

We, the guest editors, thank the authors for their hard work in preparing and revising their manuscripts. We thank the reviewers for taking the time to write detailed reviews. Finally, we thank the Editor-In-Chief, Prof. Rachel Harrison, and the editorial staff for their patience and hard work in getting this special issue ready for publication.