Computing (2019) 101:75–76
https://doi.org/10.1007/s00607-018-0671-0

EDITORIAL

Special issue on dependable computing: theory and practice

Rogério de Lemos[1]

Published online: 25 October 2018

This special issue of the Journal Computing offers original contributions in all areas of dependable and secure computing. All the publications included in this issue are extended papers presented in the 13th European Dependable Computing Conference (EDCC 2017), held in Geneva, Switzerland on September 4–8, 2017.

EDCC is an international conference for presenting and discussing the latest research in dependable and secure computing. EDCC provides a European-hosted venue for researchers and practitioners from all over the world to present and discuss their latest research results on dependability, security, fault-tolerance, testing, and other related topics.

EDCC 2017 has offered a very unique event that continued and leveraged the history of past years on dependable and secure computing, mixing academic research and industrial experience and representing a forum to discuss today's challenges. In EDCC 2017, we received 50 submissions with an acceptance rate around 26%. Based on the reviewers' comments from the conference, 12 papers were initially invited to submit to the special issue. Each submission was reviewed by at least three reviewers in order to guarantee a successful peer-review process expecting originality, quality, correctness and relevance. We selected 5 papers that cover different areas of dependability and security.

The first paper, entitled *Simulating the Effects of Logic Faults in Implementation-Level VITAL-Compliant Models*, by Tuzov, de Andrés and Ruiz defines fault injection procedures for models compliant with VHDL Initiative Towards Application Specific Integrated Circuit Libraries (VITAL) to accurately simulate the effects of common logic fault models. This has led to the definition of a unified specification of fault models for macrocells to be supported by different Simulation-based fault injection (SBFI) tools.

The second paper, entitled *Scalable Byzantine Fault-Tolerant State-Machine Replication on Heterogeneous Servers*, by Eischer and Distler present OMADA, a Byzantine

✉ Rogério de Lemos
r.delemos@kent.ac.uk
https://www.cs.kent.ac.uk/people/staff/rdl/

[1] School of Computing, University of Kent, Canterbury, UK

fault-tolerant (BFT) system architecture that is able to use additional servers by partitioning the agreement stage into multiple largely independent groups. This enables OMADA to parallelise agreement into multiple heterogeneous groups and varying the ordering workload between them, and thus allowing OMADA to individually adjust the responsibilities of replicas to the particular performance capabilities of their servers.

The third paper, entitled *Emulating Representative Software Vulnerabilities using Field Data*, by Barbosa, Cerveira, Gonçalo and Madeira presents, first, a field study which characterises the most frequent programming mistakes that cause security vulnerabilities, and second, a practical approach to emulate those vulnerabilities. The expected impact of the study is to allow practical emulation of software vulnerabilities for software quality and security assessment.

The fourth paper, entitled *Cluster-based Vulnerability Assessment Applied to Operating Systems and Web Browsers*, by Movahedi, Cukier, Andongabo and Gashi present an approach that uses existing clustering techniques to group vulnerabilities into distinct clusters. Based on this, the approach uses an existing nonhomogeneous Poisson process (NHPP) Software Reliability Model (SRM) to make predictions on the number of new vulnerabilities. Finally, the approach superimposes the SRMs used for each cluster together into a single model for predicting the number of new vulnerabilities that will be discovered in a given time period for a given operating system/web browser.

The fifth paper, entitled *An Empirical Study of Combining Diverse Static Analysis Tools and Business Scenarios*, by Nunes, Medeiros, Fonseca, Neves, Correira and Vieira address the problem of combining the output of several Static Analysis Tools (SATs) searching for SQL injection (SQLi) and Cross-site scripting (XSS) vulnerabilities. The findings from the study reveal that combining the outputs of several free SATs do not always improve the vulnerability detection performance. Following the procedure proposed in the paper a developer is able to choose with is the best combination of SATs that fits better in the project requirements.

Our thanks to all the authors for their contribution, as well as all the reviewers, whose efforts have allowed the selection of good quality papers. Also, our special thanks the editorial team of the Computing Journal for their support in the publication of this special issue containing a selected sample of the ongoing research efforts on recent advancements in dependability and security.