Guest Editorial: Special Section on the International Symposium on Software Testing and Analysis 2010

Alessandro Orso, Member, IEEE Computer Society, and Paolo Tonella, Member, IEEE

The International Symposium on Software Testing and Analysis (ISSTA) is the premier forum for the presentation of leading edge research results on issues related to software testing and analysis. Every year, ISSTA brings together academics, industrial researchers, and practitioners to exchange new ideas, problems, and experience on how to analyze and test software systems.

ISSTA 2010 was held from 12 to 16 July 2010 at the center for scientific and technologic research of the Fondazione Bruno Kessler (FBK) in Trento, a beautiful historical city in the middle of the Italian Alps. The conference was preceded by four workshops and two tutorials on various themes related to software testing and analysis. ISSTA 2010 attracted more than 100 submissions, each of which was evaluated by at least three members of the ISSTA Program Committee and discussed in the Program Committee meeting. The result was a high-quality technical program with 23 accepted research papers that cover a variety of topics, including formal verification, symbolic execution, test input generation, debugging, and concurrency testing and analysis.

This special section of the IEEE Transactions on Software Engineering contains five papers selected by the ISSTA Program Committee among the best papers presented at the conference. The papers, suitably revised, enhanced, and extended by the authors, went through the standard TSE review process—they were reviewed by three anonymous referees, and the process was overseen by the guest editors. We are delighted to present you the five excellent papers that were the results of this effort.

In the paper “Automatically Generating Test Cases for Specification Mining,” Valentin Dallmeier, Nikolai Knopp, Christoph Mallon, Sebastian Hack, Gordon Fraser, and Andreas Zeller present an improvement of dynamic specification mining, a technique to infer models of the normal program behavior based on observed executions. The improved technique generates test inputs that cover previously unobserved behaviors and systematically extends the execution space, thus enriching the mined specification. The empirical evaluation of the approach shows its effectiveness on a set of real-world Java programs.

The paper “Random Testing: Theoretical Results and Practical Implications,” by Andrea Arcuri, Zohaib Iqbal, and Lionel Briand, provides a rigorous discussion of random testing, its benefits and drawbacks. The authors also address, both theoretically and through simulations, several general questions about the efficiency, effectiveness, scalability, and predictability of random testing techniques. Finally, the authors use their results to assess the validity of empirical analyses reported in the literature and derive guidelines for practitioners and researchers interested in using random testing.

In the paper “Automatic Detection of Unsafe Dynamic Component Loadings,” by Taeho Kwon and Zhendong Su, targets code vulnerabilities that may lead to unintended, or even malicious, components to be loaded at run time. To detect and eliminate such vulnerabilities, the authors perform an analysis based on runtime information collected through binary instrumentation and analyzed to detect and eliminate such vulnerabilities. In their evaluation of the approach, the authors show that it can detect vulnerable and unsafe component loadings in popular software running under both Microsoft Windows and Linux.

In the paper “Fault Localization for Dynamic Web Applications,” Shay Artzi, Julian Dolby, Frank Tip, and Marco Pistoa present a novel approach for locating faults in modern web applications, combining test generation and fault localization. Specifically, the approach extends existing fault-localization algorithms for use on web applications written in PHP and leverages several test-generation strategies with the aim of maximizing their fault-localization effectiveness. The empirical evaluation of the approach, performed on several open-source PHP applications, shows that the test suites generated by the approach exhibit high fault-localization effectiveness.
We wish to thank the authors for providing these contributions, our anonymous reviewers for their detailed and constructive comments, and Bashar Nuseibeh and Debby Mosher for their help throughout the process.

Enjoy these papers!

Alessandro Orso
Paolo Tonella
Guest Editors

Alessandro Orso received the MS degree in electrical engineering (1995) and the PhD degree in computer science (1999) from Politecnico di Milano, Italy. He is currently an associate professor in the College of Computing at the Georgia Institute of Technology, where he has been since March 2000. His area of research is software engineering, with emphasis on software testing and program analysis. His interests include the development of techniques and tools for improving software reliability, security, and trustworthiness, and the validation of such techniques on real-world systems. Dr. Orso has received funding for his research from government agencies, such as the US National Science Foundation and the US Department of Homeland Security, and industries, such as IBM and Microsoft. He serves on the editorial board of the ACM Transactions on Software Engineering Methodology, served as program chair for ISSTA 2010, and will serve as program chair for ICST 2013. He was, among others, on the program committees of ASE, FSE, ICSE, ISSTA, ICST, and OOPSLA, and he is a reviewer for a number of international journals. He has also served as a technical consultant to DARPA. In 2007, Dr. Orso was ranked among the top-50 Software Engineering scholars in an article published by the Communications of the ACM. He regularly reviews papers for journals such as TSE, TOSEM, STVR, EMSE, and JSME. He is on the editorial board of EMSE and JSME. His current research interests include code analysis, web and object oriented testing, and search-based test case generation.

Paolo Tonella received the PhD degree in software engineering from the University of Padova in 1999 with the thesis “Code Analysis in Support to Software Maintenance.” He is the head of the Software Engineering Research Unit at the Fondazione Bruno Kessler (FBK), in Trento, Italy. In 2011 he was awarded the ICSE 2011 MIP (Most Influential Paper) award, for his paper “Analysis and Testing of Web Applications.” He is the author of Reverse Engineering of Object Oriented Code (Springer, 2005). He has participated in several industrial and EU projects on software analysis and testing. He has written more than 100 peer reviewed conference/workshop papers and more than 40 journal papers. He was program chair of ICSM 2011 and ICPC 2007. He was general chair of ISSTA 2010 and will be general chair of ICSM 2012. Among others, he has served on the program committees of ICSE, ICSM, ISSTA, ICST, ICPC, SCAM, CSMR, WCRE. In 2007, he was ranked among the top-50 Software Engineering scholars in an article published by the Communications of the ACM. He regularly reviews papers for journals such as TSE, TOSEM, STVR, EMSE, and JSME. He is on the editorial board of EMSE and JSME. His current research interests include code analysis, web and object oriented testing, and search-based test case generation.