Computer Science Department

"Combinatorial Security Testing: Improving Information Security through Combinatorial Testing "

(In Conjunction with the IEEE Reliability Society Fall 2015 Student Outreach)

Dr. Dimitris E. Simos
Researcher with SBA Research, Austria
Adjunct Lecturer with Vienna University of Technology

Abstract

Over the recent years, a number of combinatorial strategies have been devised to help testers choose subsets of input combinations that would maximize the probability of detecting faults, with combinatorial testing being the most prominent one. Combinatorial testing has been successfully applied for testing (critical) software systems in large organizations and is an already proven method for security testing of large-scale software systems.

In this talk, we review recent advances on web application security testing and testing of operating systems and explore the applicability of combinatorial testing to new and promising application domains of information security.

As part of the newly spawned combinatorial security testing project between SBA Research and NIST ACTS project team, we address how combinatorial testing can be applied to (1) ensure proper error-handling of network security protocols and (2) provide the theoretical guarantees for exciting Trojans injected in cryptographic hardware Besides providing the details of the combinatorial models and industry proof-of-concept studies, we also hinder on the technical challenges that need to be solved in the foundations of combinatorial testing. The talk is concluded with some open research problems and directions for future research.

Biography

Dr. Dimitris E. Simos is a Key Researcher with SBA Research, Austria, working on mathematical aspects of information security. He is also an Adjunct Lecturer with Vienna University of Technology. He is leading the Combinatorics, Codes and Information Security (CCIS) research group at SBA Research.

Dimitris has a keen interest on combinatorial designs and error-correcting codes. His research interests extend to the application of combinatorial designs to software testing, combinatorial testing in particular, error-correcting codes and their applications to post-quantum cryptography, optimization algorithms, symbolic computation and in general all mathematical aspects of information security.

He holds a Ph.D. in Discrete Mathematics and Combinatorics (2011) from the National Technical University of Athens. Prior to joining SBA Research, he was within the Project Team SECRET of INRIA Paris-Rocquencourt Research Center working on the design and analysis of cryptographic algorithms. His research was supported by a 3-year Marie Curie Fellow grant (2012-2015) awarded by the ERCIM through the EU-funded "Alain Bensoussan" Fellowship Programme. He is also a Fellow of the Institute of Combinatorics and its Applications (FTICA) since 2012.

Date:	Friday, September 25, 2015
Time:	11:00am to 12:00pm
Location:	ECS South 2.410
Host:	Professor Eric Wong

Refreshments will be served at 10:45am