CALL FOR PAPERS

The Fifth International Workshop on Security Testing (SECTEST 2014)

https://sites.google.com/site/sectestworkshop/

ICST 2014, Cleveland, Ohio USA

To improve software security, several techniques, including vulnerability modelling and security testing, have been developed but the problem remains unsolved. SECTEST workshop tries to answer how vulnerability modelling can help users understand the occurrence of vulnerabilities so to avoid them, and what the advantages and drawbacks of the existing models are to represent vulnerabilities. At the same time, the workshop tries to understand how to solve the challenging security testing problem, how security testing is different from and related to classical functional testing, and how to assess the quality of security testing. This is in particular interesting since testing the mere functionality of a system alone is already a fundamentally critical task. The objective of SECTEST workshop is to share ideas, methods, techniques, and tools about vulnerability modelling and security testing to improve the state of the art. In particular, the workshop aims at providing a forum for practitioners and researchers to exchange ideas, perspectives on problems, and solutions. Both papers proposing novel models, methods, and algorithms and reporting experiences applying existing methods on case studies and industrial examples are welcome. The topics of interest include, but are not restricted to:

- network security testing
- application security testing
- security requirements definition and modelling
- security and vulnerability modelling
- secure interoperability
- runtime monitoring of security-relevant applications
- security testing of legacy systems
- cost effectiveness issues
- comparisons between security-by-design and formal analyses
- formal techniques for security testing and validation
- security test generation and oracle derivation
- specifying testable security constraints
- test automation
- penetration testing
- regression testing for security
- robustness and fault tolerance to attacks
- test-driven diagnosis of security weaknesses
- process and models for designing and testing secure system
- when to perform security analysis and testing
- "white box" security testing techniques
- compile time fault detection and program verification
- tools and case studies
- industrial experience reports

Submission

We solicit both full papers (8 pages) and short papers (2 pages) in IEEE two-column format. We also solicit demonstrations of security testing tools (4 pages). All submissions will be peer-reviewed. Authors of accepted papers must guarantee that their paper will be presented at the workshop. Authors are invited to submit their papers electronically, as portable document format (pdf); please, do not send files formatted for work processing packages (e.g., Microsoft Word or Wordperfect files). The only mechanism for paper submissions is via EasyChair.

Publication

The proceedings will be published in the IEEE digital library.

Workshop Chairs

Ana Cavalli (Telecom SudParis, France)
Matthias Büchler (Technische Universität München, Germany)
Yafei Yang (Qualcomm Inc., USA)

Important Dates

Papers due: January 7, 2014
Notification: February 4, 2014
Camera-ready due: February 18, 2014