

Call For Papers

International Symposium on Engineering Secure Software and Systems (ESSoS)

February 16 - 17, 2012

Eindhoven, The Netherlands

In cooperation with ACM SIGSAC and SIGSOFT and (pending) IEEE CS (TCSE).

CONTEXT AND MOTIVATION

Trustworthy, secure software is a core ingredient of the modern world. Unfortunately, the Internet is too. Hostile, networked environments, like the Internet, can allow vulnerabilities in software to be exploited from anywhere. To address this, high-quality security building blocks (e.g., cryptographic components) are necessary, but insufficient. Indeed, the construction of secure software is challenging because of the complexity of modern applications, the growing sophistication of security requirements, the multitude of available software technologies and the progress of attack vectors. Clearly, a strong need exists for engineering techniques that scale well and that demonstrably improve the software's security properties.

GOAL AND SETUP

The goal of this symposium, which will be the fourth in the series, is to bring together researchers and practitioners to advance the states of the art and practice in secure software engineering. Being one of the few conference-level events dedicated to this topic, it explicitly aims to bridge the software engineering and security engineering communities, and promote cross-fertilization. The symposium will feature two days of technical program, and is also open to proposals for both tutorials and workshops. In addition to academic papers, the symposium encourages submission of high-quality, informative experience papers about successes and failures in security software engineering and the lessons learned. Furthermore, the symposium also accepts short idea papers that crisply describe a promising direction, approach, or insight.

TOPICS

The Symposium seeks submissions on subjects related to its goals. This includes a diversity of topics including (but not limited to):

- scalable techniques for threat modeling and analysis of vulnerabilities
- specification and management of security requirements and policies
- security architecture and design for software and systems
- model checking for security
- specification formalisms for security artifacts
- verification techniques for security properties
- systematic support for security best practices
- security testing
- security assurance cases
- programming paradigms, models and DLS's for security
- program rewriting techniques
- processes for the development of secure software and systems
- security-oriented software reconfiguration and evolution
- security measurement
- automated development
- trade-off between security and other non-functional requirements
- support for assurance, certification and accreditation

SUBMISSION AND FORMAT

The proceedings of the symposium are published by Springer-Verlag in the Lecture Notes in Computer Science Series (<http://www.springer.com/lncs>). Submissions should follow the formatting instructions of Springer LNCS. Submitted papers must present original, non-published work of high quality.

Two types of papers will be accepted:

Full papers (max 12 pages without bibliography/appendices) - May describe original technical research with a solid foundation, such as formal analysis or experimental results, with acceptance determined mostly based on novelty and validation. Or, may describe case studies applying existing techniques or analysis methods in industrial settings, with acceptance determined mostly by the general applicability of techniques and the completeness of the technical presentation details.

Idea papers (max 8 pages with bibliography) - May crisply describe a novel idea that is both feasible and interesting, where the idea may range from a variant of an existing technique all

the way to a vision for the future of security technology. Idea papers allow authors to introduce ideas to the field and get feedback, while allowing for later publication of complete, fully-developed results. Submissions will be judged primarily on novelty, excitement, and exposition, but feasibility is required, and acceptance will be unlikely without some basic, principled validation (e.g., extrapolation from limited experiments or simple formal analysis).

Online submission for papers is available through EasyChair, at <http://www.easychair.org/conferences/?conf=essos12>

Proposals for both tutorials and workshops are welcome. Further guidelines will appear on the website of the symposium.

IMPORTANT DATES

Abstract submission:	September 18, 2011
Paper submission:	September 25, 2011
Author notification:	November 19, 2011
Camera-ready:	December 11, 2011

PROGRAM COMMITTEE

Program Committee Co-Chairs

Gilles Barthe, IMDEA Software Institute
Ben Livshits, Microsoft Research

Program Committee

Davide Balzarotti, EURECOM
David Basin, ETH Zurich
Hao Chen, UC Davis
Manuel Costa, Microsoft Research
Julian Dolby, IBM Research

Maritta Heisel, U. Duisburg Essen
Thorsten Holz, U. Ruhr Bochum
Collin Jackson, CMU
Martin Johns, SAP Research
Jan Jürjens, TU Dortmund
Engin Kirda, NorthEastern U.
Javier Lopez, U. Malaga
Sergio Maffeis, Imperial College
Heiko Mantel, TU Darmstadt
Fabio Martinelli, CNR
Haris Mouratidis, University of East London
Anders Møller, Aarhus University
Frank Piessens, KU Leuven
Erik Poll, RU Nijmegen
Pierangela Samarati, U. Milano
Ketil Stølen, SINTEF and U. Oslo
Laurie Williams, North Carolina State University
Jianying Zhou, Institute for Infocomm Research Singapore