



Call For Papers

February 27 - March 1, 2013, Paris, France

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

<http://distrinet.cs.kuleuven.be/events/essos/2013/>

International Symposium on Engineering Secure Software and Systems (ESSoS)

CONTEXT AND MOTIVATION

Trustworthy, secure software is a core ingredient of the modern world. 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 fifth 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 (in particular economic considerations)
- support for assurance, certification and accreditation
- empirical secure software engineering

IMPORTANT DATES

Paper submission:	September 30, 2012
Author notification:	November 29, 2012
Camera-ready:	December 13, 2012



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.

For selected papers, there will be an invitation to submit extended versions to a special issue in the International Journal of Information Security.

Two types of papers will be accepted:

Full papers (max 14 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). In the proceedings, idea papers will clearly identified by means of the "Idea" tag in the title.

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

STEERING COMMITTEE

Jorge Cuellar (Siemens AG)

Wouter Joosen (Katholieke Universiteit Leuven) - chair

Fabio Massacci (Università di Trento)

Gary McGraw (Cigital)

Bashar Nuseibeh (The Open University)

Daniel Wallach (Rice University University)

ORGANIZING COMMITTEE

General chair: Valérie Issarny (Inria Paris-Rocquencourt, Fr)

Program co-chairs: Jan Jürjens (TU Dortmund and Fraunhofer ISST, DE), Ben Livshits (Microsoft Research in Redmond, US)

Publication chair: Riccardo Scandariato (Katholieke Universiteit Leuven, BE)

Industry chair: Andreas Schaad (SAP, DE)

Publicity chair: Pieter Philippaerts (Katholieke Universiteit Leuven, BE)

Local arrangements chair: Chantal Girodon, Stéphanie Chaix, Emmanuelle Grousset (Inria Paris-Rocquencourt, Fr)

Web chair: Ghita Saevels (Katholieke Universiteit Leuven, BE)

PROGRAM COMMITTEE

Davide Balzarotti, EURECOM, France

Ruth Breu, University of Innsbruck, Austria

Cristian Cadar, Imperial College, UK

Julian Dolby, IBM Research, US

Matt Fredrikson, University of Wisconsin, US

Dieter Gollmann, TU Hamburg-Harburg, Germany

Maritta Heisel, U. Duisburg Essen, Germany

Peter Herrmann, NTNU, Trondheim, Norway

Thorsten Holz, U. Ruhr Bochum, Germany

Sergio Maffei, Imperial College, UK

Heiko Mantel, TU Darmstadt, Germany

Anders Møller, Aarhus University, Denmark

Haris Mouratidis, University of East London, UK

Zachary Peterson, Naval Postgraduate School, US

Frank Piessens, KU Leuven, Belgium

Erik Poll, RU Nijmegen, NL

Alexander Pretschner, TU Munich, Germany

Wolfgang Reif, University of Augsburg, Germany

Jianying Zhou, Institute for Infocomm Research, Singapore

Mohammad Zulkernine, Queens University, Canada