Call for Papers

March 4 – 6, 2015, Milan, Italy
In cooperation with: (pending) ACM SIGSAC and SIGSOFT and IEEE CS (TCSP).
http://distrinet.cs.kuleuven.be/events/essos/2015/

International Symposium on Engineering Secure Software and Systems (ESSoS)

CONTEXT AND MOTIVATION

Trustworthy, secure software is a core ingredient of the modern world. So is the Internet. 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 seventh 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. In addition to academic papers, the symposium encourages submission of high-quality, informative industrial 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

Paper submissions are solicited in all areas relating to secure software and secure systems research, including but not limited to:
- Cloud security, virtualization for security
- Mobile devices security
- Automated techniques for vulnerability discovery and analysis
- Model checking for security
- Binary code analysis, reverse-engineering
- Programming paradigms, models, and domain-specific languages for security
- Operating system security
- Verification techniques for security properties
- Malware: detection, analysis, mitigation
- Security in critical infrastructures
- Security economics
- Security by design
- Static and dynamic code analysis for security
- Web applications security
- Program rewriting techniques for security
- Security measurements
- Empirical secure software engineering
- Security-oriented software reconfiguration and evolution
- Computer forensics
- Processes for the development of secure software and systems
- Human-computer interaction for security
- Security testing
- Embedded software security

IMPORTANT DATES

Abstract submission:	September 8, 2014
Paper submission:	September 15, 2014
Demo submission:	October 24, 2014
Author notification:	November 17, 2014
Camera-ready:	December 7, 2014

ESSoS 15

Engineering Secure Software and Systems

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.

Online submission for papers is available through EasyChair, at
https://www.easychair.org/conferences/?conf=essos15

DEMO SESSION SUBMISSION

This year we are planning to include a demonstration session in the symposium. If you are working on practical solutions to industrial-relevant problems in key areas of ESSOS, consider disseminating about your experience at our demonstration session. To be considered for presentation, a proposal describing the demonstration should be e-mailed to the Industry Chair, Luca Compagna (luca.compagna@sap.com). The following type of submission will be accepted:

Demo presentation (short description, max 4 pages, not published in proceedings) - May shortly describe (i) the overall problem, (ii) the architecture underlying the system demonstrated, and (iii) one or more use case scenarios that present how the audience will gain an understanding of the underlying technology.

Submissions will be evaluated based on the motivation of the work behind the use of the system to be demonstrated and its novelty. Demo presentations will not be included in the formal proceeding of ESSOS.

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: Stefano Zanero (Politecnico di Milano, IT)
Program co-chairs: Frank Piessens (Katholieke Universiteit Leuven, BE), Juan Caballero (IMDEA Software Institute, ES)
Doctoral Symposium co-chairs: Haris Mouratidis (University of Brighton , UK); Federico Maggi (Politecnico di Milano, IT); Christos Kalloniatis (University of the Aegean, Greece)
Publication chair: Nataliia Bielova (INRIA Sophia Antipolis-Méditerranée, FR)
Industry chair: Luca Compagna (SAP Product Security Research, FR)
Publicity chair: Raoul Strackx (Katholieke Universiteit Leuven, BE)
Local arrangements chair: TBA
Web chair: Ghita Saevels (Katholieke Universiteit Leuven, BE)



PROGRAM COMMITTEE

Aslan Askarov, Harvard University, US
Leyla Bilge, Symantec Research Labs, FR
Stefano Calzavara, Università Ca' Foscari Venezia, IT
Lorenzo Cavallaro, Royal Holloway, University of London, UK
Bruno Crispo, University of Trento, IT
Werner Dietl, University of Waterloo, CA
Michael Franz, University of California, Irvine, US
Christian Hammer, Saarland University, DE
Marieke Huisman, University of Twente, NL
Somesh Jha, University of Wisconsin, US
Martin Johns, SAP Research, DE
Christian Kreibich, Lastline, US
Wenke Lee, Georgia Institute of Technology, US
Zhenkai Liang, National University of Singapore, SG
Jay Ligatti, University of South Florida, US
Patrick McDaniel, Pennsylvania State University, US
Nick Nikiforakis, Stony Brook University, US
Georgios Portokalidis, Stevens Institute of Technology, US
Joachim Posegga, University of Passau, DE
Alexander Pretschner, Technische Universität München, DE
Tamara Rezk, INRIA, FR
Konrad Rieck, University of Göttingen, DE
Andrei Sabelfeld, Chalmers University of Technology, SE
Ahmad-Reza Sadeghi, TU Darmstadt, DE
Kapil Singh, IBM Research, US
Asia Slowinska, Vrije Universiteit Amsterdam, NL
Pierre-Yves Strub, IMDEA Software Institute, ES
Carmela Troncoso, Gradiant, ES
Xiaofeng Wang, Indiana University, US
Mohammad Zulkernine, Queen's University, CA