



Call for Papers

Journal of Systems Architecture

Special Issue on

Security and Dependability Assurance of Software Architectures

General Scope

The ongoing shift from software development from scratch to component and service-based system integration has raised a number of new challenges for software engineering in industrial-strength domains such as embedded systems, telecommunications, and process control. To name but a few, these challenges include the treatment of evolving requirements and assurance of security and dependability properties under unpredictable runtime conditions.

The increasing number of critical processes supported by software systems and the increasing dependence of valuable assets (including human well-being, or even human lives) on the security and dependability of computer support for these processes introduce the need of new mechanisms that can improve the level of trust we have in such systems. One central concept in this direction is certification. Furthermore, the inevitable trend towards distributed systems built by integrating and embedding subsystems, components or services that are frequently under the control of different entities makes the certification of such systems a challenging open issue that current practices for certification fail to address appropriately. In fact, in future scenarios, systems will be dynamically assembled, thus achieving higher levels of flexibility.

In this scenario, traditional techniques for achieving security and dependability assurance seem inadequate, since current S&D assurance and certification are strictly intertwined with the development process, and therefore are only valid for system and environments planned at design time and not changing at runtime.

These two characteristics of new distributed systems and computing environments introduce the need of basing security and dependability (S&D) assurance and certification on rigorous, in-depth system analysis. In this context, methodologies, techniques, and tools for assessing and certifying the security level of software become an important aspect towards the design and development of software components to be integrated in complex system architectures.

Overall Objectives

The aim of this special issue is to select papers that describe comprehensive technological solutions for:

- Developing enhanced Verification and Validation (V&V) mechanisms for software security and dependability assurance and certification;
- Implementing context-aware methodologies, techniques, and tools for assessing and assuring the security level of software as well as certification of S&D properties for complex and embedded systems;
- Ensuring that V&V mechanisms are suitable also for evolving systems (e.g., open source, open services, highly dynamic coalitions, long living systems) where requirements, models, and components can change over time;
- Tool-supported methods and processes for engineering verification, validation, and certification of long-living and evolution-resilient software systems.

Topics

The JSA special issue will focus in particular on context, methodologies, techniques, and tools for V&V of software architectures, with particular focus to supporting assurance and compliance, as well as security and dependability certification, for evolving and long-lived systems. Authors are invited to submit papers on a variety of topics, including but not limited to:

- Foundations and new perspectives of V&V mechanisms and security certifications;
- Solutions, tools, frameworks for S&D assurance and certification;
- New and/or existing certification processes and tools suitable for challenging contexts (e.g., telecommunications, mobile, real time, process control, and embedded systems), and/or experience with them;
- New and/or existing methods and/or tools which are particularly suited to evolving contexts, and/or experience with them;
- Tools and case studies that integrate techniques from different areas, such as V&V mechanisms, Product and process certification; Safety and security, Static verification, dynamic verification, testing; Language design, Empirical software engineering; Evolving systems

Submission Information

All manuscripts and any supplementary material should be submitted via the online submission and peer review systems at <http://ees.elsevier.com/jsa>. Follow the submission instructions given on this site. Please select the article type as "Special Issue: S&D Assurance of SW Arch". All manuscripts should comply with the journal's Guide for Authors. Please refer to the following site:

http://www.elsevier.com/wps/find/journaldescription.cws_home/505616/authorinstructions.

Important Dates

Submission Deadline: September 1st, 2009

Notification of Acceptance: November 15th, 2009

Final Paper: January 10th, 2010

JSA Editor-in-Chief

Iain Bate

Guest Editors

- Ernesto Damiani
Università degli Studi di Milano, DTI, Crema, Italy
ernesto.damiani@unimi.it
- Sigrid Guergens
Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany
sigrid.guergens@sit.fraunhofer.de
- Antonio Maña
GISUM, Universidad de Málaga, Málaga, Spain
amg@lcc.uma.es
- George Spanoudakis
Department of Computing School of Informatics, City University, London
gespan@soi.city.ac.uk
- Claudio A. Ardagna
Università degli Studi di Milano, DTI, Crema, Italy
claudio.ardagna@unimi.it