

AOSD Technology for Application-level Security (AOSDSEC) CALL FOR PAPERS

Security is often quoted as an example for Aspect-Oriented Software Development (AOSD) technology. Application-level security is indeed a crosscutting concern: typical security problems such as buffer overflows or access controls have a pervasive nature with regard to the business logic in an application. As long as this is limited to very few problems, this pervasive nature would not be a major issue. However, security becomes more and more a basic requirement of an application due to the increased reliance on IT. Furthermore, recent trends indicate that security is often migrated from the system security perimeter to the internals of the application. As a result, many security requirements are tangled within the business logic of an application. Clearly, typical software engineering techniques such as modularization and encapsulation become crucial. AOSD, being an emerging technology promoting advanced separation of concerns, can offer a solution to this problem.

The modularization of security is not straightforward. The security problem domain is very broad and covers a wide range of security requirements from buffer overflows to complex access-control or non-repudiation models. Interdependencies exist between different security measures. Security measures have considerable requirements regarding the interaction with and the control over the targeted concerns. Some prudent and preliminary success stories of the use of AOSD technology for security are available, but the topic undeniably requires further elaboration.

This workshop aims to provide an interactive forum for researchers and developers in both communities to discuss the use of AOSD technology for security. The goal of the workshop is to explore the opportunities and challenges in the combination of AOSD and security. In particular, the focus of the workshop will be twofold: the extent to which AOSD can be used for the implementation and enforcement of security requirements and the tool support that is necessary to enable a full modularization of these requirements. Suggested topics for position papers include, but are not restricted to:

- Security requirements that can(not) be addressed using AOSD technology
- Experience reports presenting (un)successful security modularization attempts
- Reuse of security aspects: canonical models for specific security requirements and more general frameworks
- Fundamental obstacles of AOSD technology that hinder the development of security aspects
- Application interface: what information related to other concerns is required for security aspects and how should this be provided
- Aspect deployment: what configuration is necessary/desired to deploy security aspects for a specific application

- Discussion of AOSD tools/models and their properties/support that are particularly beneficial for the development of security aspects
- Support for the incorporation of security requirements at the design or at the architectural level
- Organizational impacts, e.g. how AOSD affects the different roles in providing application security (security experts, system administrators, and system developers)
- What kind of AOSD platform support is necessary for effective application security
- How does AOSD support for application security interact with requirements for network security

Workshop Format

The workshop will be structured to encourage fruitful discussions and build connections between workshop participants. To this end, approximately half of the workshop time will be devoted to short presentations of accepted papers, with the remaining half devoted to semi-structured discussion groups. Participants will be expected to have read the accepted papers prior to the workshop, to ensure focused discussions.

Submission Instructions

Prospective participants must submit a 4-6 page position paper in Postscript, PDF or Microsoft Word, by email to aosdsec@cs.kuleuven.ac.be, no later than January 19, 2004. Submissions will be required to be strongly focused on the selected topics/issues. The submissions will be reviewed by the organizers.

All accepted papers will be posted at the workshop web site prior to the workshop date, to give all participants the opportunity to read them before the workshop. Accepted papers will be included in a technical report (from Katholieke Universiteit Leuven).

Important Dates

Submission deadline: January 19, 2004
Notification of acceptance: February 9, 2004
Final paper version: March 1, 2004
Workshop: March 23, 2004

Workshop Organizers

Bart De Win – Katholieke Universiteit Leuven
Viren Shah – Cigital Labs
Wouter Joosen – Katholieke Universiteit Leuven and Ubizen
Ron Bodkin – New Aspects of Security