Deutsches
Forschungszentrum
für Künstliche
Intelligenz GmbH

MORES 2

Developing Secure Workflow Systems

Security by design to obtain reliablely secure workflow systems

The development of modern software systems is carried out in successive design phases corresponding to different levels of abstraction. Starting with an abstract requirement analysis, these requirements and design decisions made in previous phases are step by step refined to an executable implementation.

The project MORES2 continues the evolution of a framework for developing secure workflow systems started in the predecessor project MORES. MORES was engaged in the modeling and verification of security properties for workflow systems considering the different types of requested security properties (e.g. information-flow control, separation of duty) at a particular level of abstraction, providing various decomposition techniques. Now, MORES2 aims at the development of appropriate refinement techniques for these workflow specifications. In particular, the notion of refinement to be developed has to support the refinement of the various aspects (e.g. activities, data, users) of workflows and also has to be able to translate the security properties considered in MORES to corresponding properties in other refinement levels.

Translated security guarantees of higher abstraction levels will serve as initial building blocks for the verification of security properties on lower levels. However, we cannot expect that the notion of refinement will preserve the security guarantees in general because otherwise the arising restrictions would render such a refinement impracticable. Additionally, changing the abstraction level may also result in a refinement of the abilities of an attacker observing the workflow, which causes a change of how the required security guarantees are formulated. In MORES2 we will develop techniques to make use of security guarantees of higher abstraction levels in verifying the corresponding security properties on lower abstraction levels. We will provide a corresponding verification tool support based on existing interactive proof systems.

Combining the upcoming results of MORES2 with the decomposition techniques developed in MORES, we will provide an integrated approach supporting security-in-the-large for workflow systems. Applying the decomposition techniques reduces the size of the components to be verified and improves the scalability of the verification tasks in general. The refinement techniques allow one to reuse the security guarantees of higher abstraction levels to verify the security of lower levels resulting in simpler proof tasks.

This approach will be evaluated using the reference scenario Security in Web-based Workflow Management Systems of the priority programme by specifying it on various abstraction levels and using it to exemplify the translation of the arising security properties along the refinement hierarchy.

Duration: 10/2014 – 09/2016

Funded by:

DFG Deutsche Forschungsgemeinschaft

RS³

This project is funded by the Deutsche Forschungsgemeinschaft (DFG) within the special priority programme SPP 1496 „Reliablely Secure Software Systems (RS^3)“

Contact:
DFKI Bremen
Cyber-Physical Systems

Prof. Dr. Dieter Hutter
Telephone: +49 421 – 218 59831
E-Mail: hutter@dfki.de
Internet: www..dfki.de/cps