Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

MORES 2

Entwicklung sicherer Workflowsysteme

Sicherer Entwurfsweg hin zu einer sicheren Implementierung

Die Entwicklung moderner Softwaresysteme erfolgt in der Regel modular und auf verschiedenen Detaillierungsebenen. Ausgehend von einer abstraken Anforderungsspezifikation werden Anforderungen und getroffene Designentscheidungen schrittweise bis zu einer Implementierung verfeinert.

Das Projekt MORES2 setzt die im Vorgängerprojekt MORES begonnene Entwicklung eines Rahmenwerks zur Entwicklung sicherer Workflow-Systeme fort. Hatte sich MORES hauptsächlich der Sicherheits-modellierung von Workflow-Systemen unter Berück-sichtigung der verschiedenartigen Sicherheitseigen-schaften (Informationsflusskontrolle, Separation-of-Duty, Need-to-know) auf einer Detaillierungsebene gewidmet und entsprechende Dekompositions-techniken entwickelt, so besteht das Ziel von MORES2 in der Entwicklung geeigneter Verfeinerungstechniken für solche Workflowspezifikationen. Dabei müssen zum einen die verschiedenen Aspekte der Workflow-modellierung (z.B. Tasks, Daten, Benutzer) geeignet verfeinerbar sein und zum anderen die in MORES be-trachteten Sicherheitseigenschaften auf entsprechen-de Eigenschaften auf anderen Verfeinerungsebenen übersetzbar sein.

Sicherheitsgarantien auf oberen Ebenen dienen damit als initiale Bausteine für eine Verifikation der Sicherheit auf unterliegenden Ebenen. Es kann dabei nicht erwartet werden, dass der zu entwickelnde Verfeinerungsbegriff die Sicherheitsgarantien invariant lässt, da zum einen dies die möglichen Verfeinerungen derartig reduziert, dass sie in der Praxis kaum noch relevant wären, und zum anderen beim Übergang zwischen den Verfeinerungsebenen es zu einer Modifikation der Beobachtungsmöglichkeiten kommen kann, die zu einem Wechsel der Modellierung der geforderten Sicherheitsgarantien führt. MORES2 wird daher Techniken entwickeln, um die Sicher-heitsgarantien der oberen Ebenen in den Nachweis der entsprechenden Sicherheitseigenschaften auf unteren Ebenen zu integrieren. Eine entsprechende Werk-zeugunterstützung auf Basis existierender interaktiver Theorembeweiser wird hierfür aufgebaut.

In Verbindung mit den in MORES entwickelten Dekompositionstechniken wird mit den Ergebnissen aus MORES2 ein durchgängiges Konzept für Security-in-the-Large für Workflowsysteme zur Verfügung stehen. Dekomposition verringert die Größe der einzelnen zu verifizierenden Komponenten und erhöht dadurch die Skalierbarkeit der Verifikation insgesamt. Die Verfeinerungstechniken erlauben eine weitere Vereinfachung der Verifikation auf der unteren Ebene durch Zuhilfenahme von Sicherheitsgarantien der oberen Ebene.

Dieses Konzept wird in MORES2 unter Verwendung des Schwerpunkt-Referenzszenarios „Security in Web-based Workflow Management Systems“ evaluiert, indem dieses Szenario auf verschiedenen Abstraktionsebenen spezifiziert und die Übertragung der Sicherheitseigenschaften beim Wechsel der Abstraktionsebenen beispielhaft durchgeführt wird.

Projektlaufzeit: 10/2014 – 09/2016

Gefördert durch:

DFG Deutsche Forschungsgemeinschaft

RS³

Die Förderung erfolgt durch die Deutsche Forschungsgemeinschaft (DFG) im Rahmen des Schwerpunktprogramms SPP 1496 „Sicher zuverlässige Softwaresysteme“

Kontakt:
Standort Bremen
Cyber-Physical Systems

Prof. Dr. Dieter Hutter
Telefon: 0421 - 59831
E-Mail: hutter@dfki.de
Internet: www.dfki.de/cps