Klaus-Peter Fischer-Hellmann

Information Flow Based Security Control Beyond RBAC

How to enable fine-grained security policy enforcement in business processes beyond limitations of role-based access control (RBAC)

Springer Vieweg

Corporate IT

Edited by
Prof. Dr. Rainer Bischoff, Hochschule Furtwangen (HFU), Germany

"Corporate IT" is application-oriented and dedicated to practice. The main subjects are represented in a goal-oriented manner and backed by practical business experience. The series is intended for IT professionals and decision makers in enterprises who are responsible for IT-enabled business processes: IT managers, CIOs, executives, project managers in IT and organizational projects. Additionally, the books are suited for practice-oriented studies and advanced vocational training.

www.springer.com

Klaus-Peter Fischer-Hellmann

Information Flow Based Security Control Beyond RBAC

How to enable fine-grained security policy enforcement in business processes beyond limitations of role-based access control (RBAC)

Springer Vieweg

Dr. Klaus-Peter Fischer-Hellmann
Mühltal, Germany

ISBN 978-3-8348-2617-6 ISBN 978-3-8348-2618-3 (eBook)
DOI 10.1007/978-3-8348-2618-3

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Library of Congress Control Number: 2012949281

Springer Vieweg

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE. Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

Foreword

The applicability of RBAC (role-based access control) for information flow control is limited. Business processes are used more and more for applications that imply control and information flows across inter-organisational and intra-organisational security domain boundaries. More fine-grained access control mechanisms than those offered by RBAC are necessary to enforce security policies of different domains involved without overly strict limitations. In this book, methods are introduced based on an analysis of security-relevant semantics of BPEL (Business Process Execution Language) that help to overcome the restrictions mentioned above. Semantic patterns implied by BPEL and Web services invoked are introduced in order to analyse and illustrate their relevance with respect to security policy-implied restrictions.

Procedures to apply the novel methods in practice are defined and a prototypical realisation of a tool for compliance assessment with security policies demonstrates the applicability of the approach.

Prof. Dr. Rainer Bischoff

June 2012

Preface

For a number of years now, Web Services Business Process Execution Language (WS-BPEL or BPEL for short) is broadly used for the definition of executable business processes. By exploiting the fact that BPEL is a platform-independent standard supported by several major vendors of business suites, business processes specified with BPEL may be developed at one site and afterwards be executed at other sites without any further transformation. In this manner, business processes spanning organisational boundaries can be specified or modified at a central site and (re)distributed to the enterprises involved for execution in order to serve a common goal.

Such an approach of centralised definition seems to be particularly useful in scenarios where the need of comparatively small modifications of existing local processes to adapt to changing overall requirements occurs frequently and the requirement changes mainly are caused by one of the partners involved. Supply chain management is an example of such a scenario where typically processes of different suppliers have to be coordinated to serve one manufacturer's needs.

In such scenarios, considerable amount of coordination effort could be avoided by central modification and adaptation of the distributed processes. However, concerns that a remotely defined business process could possibly fail to conform to local security policies or, more generally, local business rules often stand in the way of these potential savings. In particular, worry is dedicated to the risk that a business process defined at a site outside the own enterprise and executed on behalf of this external site would fail to obey the restrictions of information and control flows induced by local security policies, may it occur because of insufficient knowledge or because of intentional disregard of such restrictions.

A local process defined as part of an overall process may need access to protected information or resources that, conforming to local security policies, must not be granted to any site outside the own enterprise. Since such local processes typically communicate with other parts of the overall process, such access will only be granted to the local process if it can be made sure that the protected information will not be disclosed across enterprise boundaries and protected resources will only be used within the limits prescribed by security policies.

Checking a process definition for compliance to constraints of information and control flows, ideally prior to execution of the process, is generally considered a demanding task that may easily require more effort than could have been saved by avoiding coordination overhead. This might be the reason why such exploitation of the capability for platform-independent definition of business processes in order to

reduce adaptation effort with business processes spanning enterprise boundaries often will not even be envisaged.

In the application layer, security policy enforcement at runtime often is performed by exertion of role-based access control (RBAC). Conforming to the underlying principles of RBAC to safeguard confidentiality and integrity, a business process communicating with sites outside the own enterprise, in general, would not be granted access to protected information or resources. Reason for this is that for the decision to grant access RBAC usually does not take into account the disposition of information provided in the further course of action within the process requesting access. Thus, security policy enforcement at runtime using RBAC offers no alternative to complex analysis of business processes with respect to compliance to security policies prior to execution since RBAC would have to prevent courses of action in enterprise-spanning business processes that are reasonable and required in the context of the overall process.

Hence, we are facing the following dilemma: On one hand side, there is the opportunity to save a considerable amount of effort required for development and adaptation of business processes by exploiting the property of BPEL being a platform-independent standard for the definition of executable business processes. On the other hand side, this opportunity either cannot be made use of because of security concerns or the effort possibly saved has to be spent otherwise for checking compliance to security policies in order to dispel such security concerns.

In this book based on the author's research, methods and procedures will be introduced that help to resolve this dilemma. These procedures allow for performing the required check of compliance to security policies prior to execution of a business process in a comparatively easy way. Even more, the procedures to analyse BPEL scripts defining business processes are suited to be performed automatically such that they can be checked quickly and with little effort. This, of course, is of great value in security policy compliance assessment of remotely-defined business processes in enterprise-spanning scenarios. Furthermore, this approach may also be applied beneficially to save effort in quality assurance when assessing compliance to security policies of business processes that have been developed within an organisation for internal use only.

Finally, the procedures developed for the field of organisation-spanning business processes will be generalised in such a way that they also become applicable with Grid and Cloud computing.

Dr. Klaus-Peter Fischer-Hellmann

June 2012

Vorwort | German Preface

Seit einigen Jahren befindet sich Web Services Business Process Execution Language (WS-BPEL oder kurz BPEL) in weitverbreitetem Einsatz bei der Definition von ausführbaren Geschäftsprozessen. Da es sich bei BPEL um einen Plattformunabhängigen Standard handelt, der von einigen wichtigen Herstellern sogenannter Business Suites unterstützt wird, können Geschäftsprozesse, die mittels BPEL spezifiziert werden, an einem Standort entwickelt und anschließend an anderen Standorten ausgeführt werden, ohne dass dazu weitere Transformationen notwendig sind. Auf diese Weise können Geschäftsprozesse, die organisatorische Grenzen überschreiten, an einer zentralen Stelle spezifiziert oder modifiziert werden und an die beteiligten Unternehmen zur Ausführung übergeben werden, um eine gemeinsame Aufgabe zu erfüllen.

Ein solcher Ansatz einer zentralisierten Definition erscheint besonders dann vorteilhaft, wenn es häufig vorkommt, dass vergleichsweise kleine Änderungen an bestehenden lokalen Prozessen zur Anpassung an geänderte Anforderungen notwendig werden und diese Änderungen hauptsächlich von einem der beteiligten Partner veranlasst sind. Supply Chain Management ist ein Beispiel eines solchen Szenarios, bei dem typischerweise Prozesse verschiedener Lieferanten zu koordinieren sind, um den Bedürfnissen eines Herstellers zu genügen.

In solchen Szenarien kann beträchtlicher Koordinationsaufwand eingespart werden, indem die notwendigen Anpassungen zentral erfolgen. Dem allerdings stehen Bedenken entgegen, dass dabei die lokalen Sicherheitsrichtlinien oder Geschäftsregeln nicht eingehalten werden. Insbesondere gilt die Sorge dem Risiko, dass ein Geschäftsprozess, der außerhalb des eigenen Unternehmens definiert wurde und im Auftrag dieser externen Stelle ausgeführt werden soll, die Beschränkungen des Kontroll- und Informationsflusses nicht beachtet, die sich aus den eigenen Sicherheitsrichtlinien ergeben – sei es aus Unkenntnis oder aufgrund absichtlicher Missachtung derselben.

Ein lokaler Prozess, der Teil eines Gesamtprozesses ist, benötigt möglicherweise Zugriff auf geschützte Informationen oder Ressourcen, der normalerweise einer Stelle außerhalb des eigenen Unternehmens nicht gewährt werden darf. Da solch ein lokaler Prozess typischerweise mit anderen Teilen des Gesamtprozesses kommuniziert, kann ein solcher Zugriff nur gewährt werden, wenn sichergestellt werden kann, dass geschützte Information nicht über die Firmengrenze hinweg verbreitet wird und geschützte Ressourcen nur innerhalb der von den Sicherheitsrichtlinien vorgegebenen Grenzen verwendet werden.

Eine Prozessdefinition auf Einhaltung der Einschränkungen bezüglich Informations- und Kontrollströmen zu überprüfen, idealerweise noch vor deren Ausführung, gilt im Allgemeinen als schwierig und kann sehr schnell einen hohen Aufwand bedeuten. Das könnte der Grund sein, warum an eine solche Ausnutzung der prinzipiell möglichen Plattform-unabhängigen Definition von Geschäftsprozessen zur Reduktion des Anpassungsaufwands bei firmenübergreifenden Geschäftsprozessen häufig nicht einmal gedacht wird.

Auf Anwendungsebene wird die Einhaltung von Sicherheitsrichtlinien zur Laufzeit häufig mit Verfahren gemäß Role-Based Access Control (RBAC) überwacht. Entsprechend den zugrunde liegenden Prinzipien von RBAC zur Sicherstellung von Vertraulichkeit und Integrität dürfte einem Geschäftsprozess, der mit Stellen außerhalb des eigenen Unternehmens kommuniziert, im Allgemeinen kein Zugriff auf geschützte Informationen oder Ressourcen gewährt werden. Dies liegt daran, dass für die Entscheidung, Zugriff zu gewähren, bei RBAC üblicherweise nicht berücksichtigt wird, was im weiteren Verlauf des Prozesses mit der Information geschieht. Daher stellt die Überwachung der Einhaltung von Sicherheitsrichtlinien zur Laufzeit mittels RBAC keine Alternative dar zur komplizierten Analyse eines Geschäftsprozesses vor dessen Ausführung auf Verträglichkeit mit den Sicherheitsrichtlinien, da mit RBAC Abläufe in Firmengrenzen überschreitenden Geschäftsprozessen verboten werden müssten, die jedoch im Sinne des Gesamtprozesses sinnvoll und wünschenswert sind.

Es besteht also folgendes Dilemma: Einerseits besteht die Möglichkeit, beträchtlichen Aufwand bei der Entwicklung und Anpassung von Geschäftsprozessen einzusparen, indem man sich die Eigenschaft von BPEL zunutze macht, ein Plattform-unabhängiger Standard zur Definition ausführbarer Geschäftsprozesse zu sein. Andererseits kann aufgrund von Sicherheitsbedenken von dieser Möglichkeit kein Gebrauch gemacht werden oder der möglicherweise einzusparende Aufwand muss anderweitig wieder investiert werden, um die Vereinbarkeit mit Sicherheitsrichtlinien zu überprüfen, um solche Sicherheitsbedenken zu zerstreuen.

In diesem Buch werden auf den Forschungsarbeiten des Autors basierende Verfahren und Prozeduren vorgestellt, die dazu beitragen, dieses Dilemma zu lösen. Diese Prozeduren ermöglichen es, die notwendige Überprüfung auf Verträglichkeit mit Sicherheitsrichtlinien vor Ausführung eines Geschäftsprozesses auf relativ einfache Weise vorzunehmen. Darüber hinaus eignen sich die Prozeduren zur Analyse von BPEL-Skripten, die Geschäftsprozesse definieren, zur automatischen Durchführung, so dass diese Skripte schnell und mit geringem Aufwand überprüfbar sind. Dies ist natürlich von großem Wert bei der Ermittlung der Verträglichkeit mit Sicherheitsrichtlinien bei an anderer Stelle definierten Geschäftsprozessen in Firmengrenzen überschreitenden Szenarien. Es kann jedoch auch zu verringertem Aufwand bei der Qualitätssicherung beitragen, wenn lokal definierte Geschäfts-

prozesse, die zur rein internen Verwendung gedacht sind, auf Einhaltung der Sicherheitsrichtlinien zu überprüfen sind.

Schließlich werden die Prozeduren und Verfahren, die für Organisationsgrenzen überschreitende Geschäftsprozesse entwickelt wurden, dahingehend verallgemeinert, dass sie auch für Grid und Cloud Computing einsetzbar werden.

Dr. Klaus-Peter Fischer-Hellmann

Juni 2012

Contents