Semantic Policy-based Security Framework for Business Processes

Dong Huang[1,2]

[1]Institute for Algorithms and Cognitive Systems (IAKS)
University of Karlsruhe (TH)
D-76131 Karlsruhe, Germany
dong.huang@ira.uka.de
[2]Siemens AG, Corporate Technology
D-81730 Munich, Germany

Abstract. Web service composition and workflow language enable the definition and execution of business process in various application domains. Security is now a major concern for us to implement business process in the context of web service. Meanwhile policy-based approach is becoming popular for the dynamic specification and regulation of web service constraints. We are going to propose a security framework for business process and use policy language enriched with semantics to represent the security concerns and requirements. Furthermore, the challenges will be listed to guide future research.

1 Introduction

Business Processes describe the interaction and collaboration between multiple parties working towards a common objective or a special function. Each party in the Business Process provides its service interface to be accessed and defines by itself how this interface can be invoked. The introduction of Web Services has provided a new way to conduct the business. For example, in the populate travel agent scenario, a travel agency offers its service for booking a travel package by combining several elementary web services such as flight and hotel reservation.

Web Services composition is currently defined by two largely complementary initiatives for developing business processes. The terms *orchestration* and *choreography* have been widely used to describe business interaction protocol. Orchestration describes the business logic and how web service can interact with each other from the perspective of a single endpoint. Business Process Execution Language for Web Service (BPEL or WS-BPEL 2.0)[1] is an orchestration language that is widely used in industry to define the business process and the execution order. Choreography is associated with globally visibly message exchange and is more collaborative in nature than orchestration. Web Service Choreography Description Language (WS-CDL)[10] is a draft document of W3C and introduces a description language which fixes the rule of the interaction between the parts involved in the system. In this paper we focus on the orchestration approach and use BPEL to describe the related business processes.

Security is one of the major concerns when developing business processes. We distinguish two levels of security requirement: *Task Level* and *Process Level*.

- **Task Level Security**. Business Task describes what is to be done in the business model. In the context of web services, a business task is represented by a web service that fulfils the specification of task. Security requirements in this level include basic aspects such as Authentication, Authorization (Access Control), Non-reputation, Data Integrity and Confidentiality. Web service can protect SOAP messages sent over insecure transports by embedding security headers. The WS-Security standard[11] defines how such headers may include signatures, cipher texts and security tokens. There are several emerging specification of web service security such as WS-Policy, WS-Trust, WS-Privacy, and WS-Federation, covering various facets of security in the context of web service. They are built on the top of WS-Security and define enhancements to provide security protection to web service endpoints and the data communication between them.
- **Process Level Security**. Business process defines how business tasks interact and collaborate. Security requirements in this level are normally defined by Business Rules. A business rule is a statement that defines or constrains some aspects of the business. Business rules are usually expressed as *constraints* or in the form **if** *condition* **then** *action*. Business rules provide a means to express and specify high-level security constraints in the form of policy, which are separated logically and physically from the other components through out business processes. Security concerns arisen from business rules concentrate on the critical constraints in the business model and other aspects, such as those for Six Sigma and Sarbanes-Oxley legislation compliance.

WS-Security and other emerging specifications provide the basic security functionalities, but they do not offer enough support for process level security in web service composition. The initial way to solve the process level security is to integrate business rules into BPEL process manually. Business rules are integrated with process by adding activities, which are used to model the consumption and production of messages, tasks, data or goods. But it is not easy for the developer or administrator to handle the complex rules and deal with the impact of dynamically changing of business rules.

In this paper, we propose a semantic policy-based approach to secure the web service composition for business processes. Section 2 includes related approaches and Section 3 gives an overview of our proposed security framework. Section 5 describes the challenges for the work.

2 Related Work

In the project SECTINO[3][1], a system architecture for local and global workflow system is proposed based on the XACML and SAML. Security concerns are

[1] http://qe-informatik.uibk.ac.at

defined in OCL(Object Constraint Language) with model-driven UML tools. SECTINO employs a static specification and enforement of security policies in web services composition. XACML is good for specifying policy in a specified domain. But it is not semantic rich enough for cross-organitaional orchestration and high-level security requirments.

AO4BPEL[4][2] proposes an aspect-oriented extension to BPEL. It uses aspects-oriented concept to modularize cross-cutting concerns like security and performance in business processes. Although the AO4BPEL framework offers the modularity and dynamic adaptability to the web service composition, it lacks semantic description of security aspects, business processes and business rules. This make conflicts detection and policy negotiation infeasible for securing the web service composition. The adoption of a semantic web language can overcome this limitation with the help of a common ontology basis.

There are a lot of research works and industry standards on using semantic and non-semantic policy for security. Ponder[5], XACML[15] and WS-Policy[3] are typically non-semantic policy framework. KAoS[2], Rei[9] and SWRL[8] are approaches that enriched with semantics using RDF[13] and OWL[14] as standards for policy specification. A comparative analysis between semantic and non-semantic language is made by [7] to show the advantages of semantic policy approach. After comparing these semantic policy languages [7], Rei and SWRL seems to have sufficient capability to represent the security requirements in the context of business process.

All semantic description should base on the same knowledge base. Security restrictions have to be expressed in underlying knowledge representation formalism for an ontological description of policies. A generic policy description framework based on three ontology layer is defined in [12]. The three ontology layers are: a domain-independent upper-level ontology, a Core Legal Ontology and a Core Policy Ontology. The first two components are off-the-shelf ontologies that are used as modeling basis for the construction of domain specific ontologies. In [6], security ontologies are defined in DAML+OWL[4] that allow the annotation of web service with respect to various security related notions such as access control, data integrity and others.

3 Design of the Framework

A service platform to deploy web service composition whose interaction and security are specified and governed by policy need to address the following challenges:

- Policy languages used in the system should be well-defined, flexible enough to allow new policy information to be expressed and extensible enough to add new policy type. Different policy languages from different domains should also be able to interoperate [7].

[2] http://www.st.informatik.tu-darmstadt.de/static/pages/projects/AO4BPEL
[3] http://www-128.ibm.com/developerworks/library/specification/ws-polfram/
[4] http://www.daml.org

– Effective policy combined and created from policies should be able to negotiate during runtime. Changes in a policy should be reflected in the runtime logic[16] and conflicts arisen should be to be detected and resolved on the fly.

For the task level security we tend to use the WS-Policy framework, because WS-Policy has already been well developed and addressed all the necessary security aspects on the task level. For the process level security Rei and SWRL are suitable, because the business rules usually represented as constraints or *if-then* form can be efficiently expressed by logical functions of these semantic policy languages. Business rules are usually defined by different parties and distributed through out the network, so a policy langugage with rich semantics can also help the interoperation and combination of these business rules. Even though different semantic/non-semantic policies can be used to represent security concerns at both task and process level, policies with semantics built on common security ontology are more general and flexible.

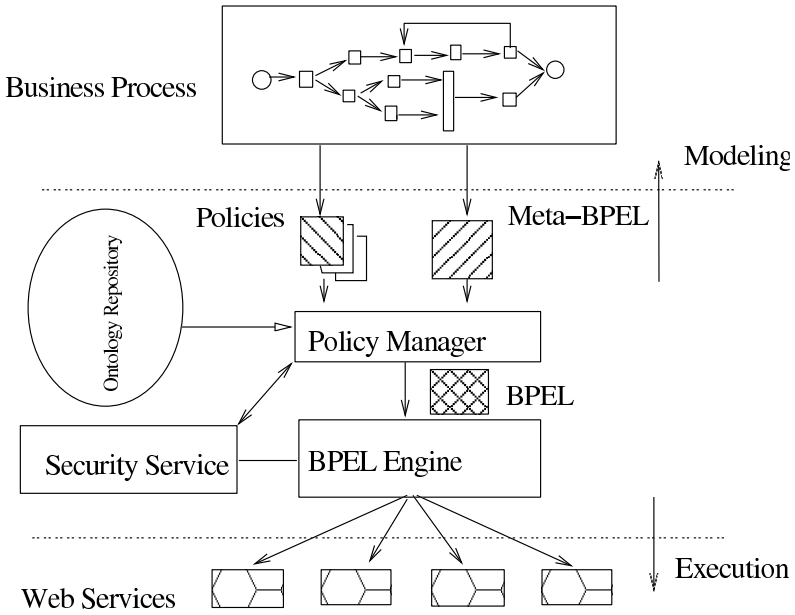

Fig. 1. Architecture of the security framework

Fig. 1 shows the architecture of the semantic policy-based framework for business process. The output of the business process modelling and model-driven security requirements analysis on the top layer are a set of security policies and the meta business process, which describes abstract process with functional tasks. All security concerns arisen from different domains and reasons, such as legal problems, privacy and changes of business rules, will be covered in the

security policies. These policies would be specified and annotated with semantics based on the **Ontology Repository**. Two kinds of ontology in the repository are:

- Business Ontology describes the concepts and relations related to the current business process.
- Security Ontology illustrates the relations among security concepts like authorization and authentication.

The **Policy Manager** gets the meta process definition and policies as input. Formally described policies can be checked for compatibility via matching. Description Logic will be used to conduct the matching phase and make the policy negotiation and conflicts detection possible. Then the Policy Manager creates as output the BPEL process definition, in which semantic policies that represent the business rules and other security requirements are integrated. New tasks or activities, which access the **Security Service** to get the necessary security token for SOAP message or invoke encryption and signature methods, are inserted into the meta BPEL to create the new BPEL file. Policy changes can be deployed and take effect on the fly without stopping the process by using aspect-oriented extension to BPEL like AO4BPEL.

4 Conclusion and Future Work

In this paper we addressed our ongoing research about a semantic policy-based security framework for business processes. We have distinguished all security concerns and requirements into two levels: Task and Process Level. The architecture of security framework is designed to support runtime policy management and enforcement. Security policies are built on the top of ontology to enrich representation of security concerns and enable reasoning for conflict detection and policy negotiations. The challenges and issues, which deserve future research, will be the following:

- Model-Driven Security Modelling. There are ongoing standardization effort for business process modelling from both OMG[5] and BPMI[6]. Security as an important concern is still not well specified to incorporate with the business process modelling standards from OMG and BPMI.
- How to define and translate security concerns to semantic policies? Ontology and rule language, such as SWRL, should be used to represent declarative policy in the future work.
- How to enforce policies on the business process during the runtime? The aspect-oriented approaches can modularize the crosscutting concerns like security and should be implemented on the process level to enforce the policies dynamically.

[5] http://www.omg.org
[6] http://www.bpmi.org

5 Acknowledgment

The authors would like to thank the team at Siemens CT IC 3 for their guidance and support whilst conducting this research. In particular, we thank Jorge Cuellar for his valuable contributions towards this work.

References

1. Arkin, A., Askary, S., Bloch, B., and Curbera, F. Web services business process execution language version 2.0. Tech. rep., OASIS, December 2004.
2. Bradshaw, J., and Uszok, A. Representation and reasoning for daml-based policy and domain services in kaos and nomads. In *AAMAS '03: Proceedings of the second international joint conference on Autonomous agents and multiagent systems* (New York, NY, USA, 2003), ACM Press, pp. 835–842.
3. Breu, R., and Hafner, M. Sectino:inter-organizational workflow security in e-government, 2004.
4. Charfi, A., and Mezini, M. Aspect-oriented web service composition with ao4bpel. In *ECOWS* (2004), vol. 3250 of *LNCS*, Springer, pp. 168–182.
5. Damianou, N., Dulay, N., Lupu, E., and Sloman, M. Ponder:a language for specifying security and management policies for distributed systems. Tech. rep., Imperial College, October 2000.
6. Denker, G., Kagal, L., Finin, T., Sycara, K., and Paoucci, M. Security for daml web services: Annotation and matchmaking. In *Second International Semantic Web Conference* (September 2003).
7. Felix Clemente, G. P. Representing security policies in web information systems. In *Proceedings of WWW 2005* (May 2005).
8. Horrocks, I., and Patel-Schneider, P. F. Swrl: A semantic web rule language combining owl and ruleml. Tech. rep., The Rule Markup Initiative, May 2004.
9. Kagal, L., Finin, T., and Joshi, A. A policy language for a pervasive computing environment. In *IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (2003).
10. Kavantzas, N., Burdett, D., and Ritzinger, G. Web services choreography description language version 1.0. Tech. rep., December 2004.
11. Kelvin Lawrence, Chris Kaler, S. A. Web services security. Tech. rep., OASIS, 2004.
12. Lamparter, S., Eberhart, A., and Oberle, D. Approximating service utility from policies and value function patterns. In *Proc. of the 6th IEEE Workshop on Policies for Distributed Systems and Networks* (JUN 2005), IEEE Computer Society.
13. Manola, F., and Miller, E. Rdf primer. Tech. rep., W3C Recommendation, February 2004.
14. McGuinness, D. L., and van Harmelen, F. Owl web ontology language overview. Tech. rep., W3C Recommendation, February 2004.
15. Moses, T. extensible access control markup language (xacml) version 2.0 3. OASIS Standard, Feb 2005.
16. Mukhi, N. K., and Plebani, P. Supporting policy-driven behaviors in web services: experiences and issues. In *ICSOC '04: Proceedings of the 2nd international conference on Service oriented computing* (New York, NY, USA, 2004), ACM Press, pp. 322–328.