Service Contracts: Beyond Trust in Service Oriented Architectures

G.E. Jaramillo Rojas, Philippe Aniorte, Manuel Munier

Service Contracts: Beyond Trust in Service Oriented Architectures

Gloria Elena Jaramillo Rojas, Philippe Aniorte, Manuel Munier

Université de Pau et des Pays de l'Adour
371 rue du Ruisseau
40004 Mont de Marsan, France
{gloriaelena.jaramillorojas,philippe.aniorte,manuel.munier}@univ-pau.fr

ABSTRACT. *The Service-Oriented Architecture (SOA) is considered as the most promising paradigm over the last few years for delivering functionalities and allowing business cooperation. In SOA, the traditional vision of security aims to keep properties such as availability, authenticity and confidentiality by protecting the web service itself. However, in such an approach, the particularities of the human interaction in regard to the behaviors of the service stakeholders have been until now based only on trust. In this article, we present an approach based on machine readable contracts and evidences for improving the traditional web service-centered security. Similarly, the usefulness of this approach in context of semi-automatic auditing and risk management is discussed.*

RÉSUMÉ. *L'architecture orientée services (SOA) est considérée comme le paradigme le plus prometteur au cours des dernières années pour fournir des fonctionnalités et faciliter la coopération commerciale.Dans le SOA, la vision traditionnelle de la sécurité vise à garder des propriétés telles que la disponibilité, l'authenticité et la confidentialité, en protégant le service Web lui-même. Cependant, dans une telle approche les particularités de l'interaction humaine en ce qui concerne les comportements des parties prenantes de service ont été jusqu'à présent basée seulement sur la confiance. Dans cet article, nous présentons une approche basée sur des contrats lisibles par la machine et des preuves pour enrichir la vision traditionannelle de la sécurité axée sur les services web. De même, l'utilité de cette approche dans le contexte de la gestion de risques et l'audit semi-automatique est discutée.*

KEYWORDS: *contract, evidences, model, service, SOA, trust.*

MOTS-CLÉS : *contrat, preuves, modèle, service, SOA, confiance.*

DOI:10.3166/ISI.y.y.1-6

1. Introduction

The service-based technologies have revolutionized not only the architecture of the information systems but also the way of doing business. By making use of its proper-

ties of transparency, integration and loose coupling, the Service Oriented Architectures (SOA) fill the gap between the managerial need of adaptation to the rapid changes of markets and the information systems that support the business logic. Therefore, new paradigms of interaction between clients and providers mediated by the services are created based on dynamism and trust.

Just a few decades ago, when someone committed to provide a service, pledging his word was enough to believe that the provider will act in good faith in regarding to the provision of the service according to the client needs and expectations. Nowadays, this practice is reflected in the provision of services via web services and the cloud by creating plain text documents about the way in which the service should be used; that is to say, commitments, obligations and guarantees about the service itself and its provision. In this context, service stakeholders trust that all the parties involved in the service provision will act as stipulated in those governing documents. It has give rose to models of trust-reputation in which the latter is negatively affected if one of the parties loses trust in other party due to breaches in the agreed document. Even if we consider that trust is an important component of both the service provision, and the relation between clients and providers, it is also needed to have more concrete information, which we call *evidences*, to support the compliance with the agreed commitments. Our approach relies therefore in the formalization and modeling of a machine-readable document governing the service provision, which we call *service contract*, and *evidences* which proves compliance with the commitments and guarantees established in the contract. An overview of our approach is presented in Section 2, while its building blocks are further detailed in Sections 3 and 4. An analysis of the usefulness of this approach applied to some aposteriori processes such as auditing and risk management is discussed in Section 5. Finally, the conclusions and future work are presented in Section 6.

2. Approach Overview

Our approach takes as basis security models, of both web services and information systems in general. On the one hand, we address the description, as precisely as possible, of the requirements and wishes on the service stakeholders in order to create policies that regulate the service provision and the stakeholders behavior. On the other hand, we aim to collect evidences and create a log that guarantees the compliance with the defined policy. That collected information is later semi-automatically analyzed in order to draw conclusions useful for the decision-making process, for instance, to identify wronged parties, to find patterns for recurring policy violations, to apply penalties, or to modify the policy.

Traditionally, talking about security in information systems refers to keeping properties such as availability, authenticity and confidentiality, which addresses the security of either the system or the information. Current security models (Layouni, Pollet, 2009) (Mustapha *et al.*, 2012) (Bensaidi *et al.*, 2012) are able to define policies in inter-organizational environments, focusing on trust and penalties. These models, although

based on a first-order logic formalism, focus on the definition of rules considering single observable actions carried out by the stakeholders, such as write and read. Conversely, Service Level Agreements (SLA) are machine-readable documents able to act as a governing document by creating legal obligations and specifying guarantees about the service (Nepal *et al.*, 2008) (Guidara *et al.*, 2012) (Kearney *et al.*, 2010). The main drawback of the most SLAs is its limited expressiveness for representing guarantees which are not associated to the web service performance.

Consequently, our approach is based on two main components, namely: a machine readable document able to represent policies governing the interaction between service stakeholders, which a richer expressiveness than SLAs, and a log containing evidences about the compliance with the service policy.

3. Service Contract

Service contracts are defined in our approach as machine readable documents reflecting the commitments and obligations of the stakeholders, with a higher expressiveness than SLAs. In this regard, our contribution relies on a formal representation of high-level non-functional service guarantees. Thus, we narrowed down the scope of our approach to only two contractual parties: a service provider and a service client in a Business-to-Business scenario.

For the modeling of our service contract, the following issues showed up due to the fact we move to a high-level definition of policies:

– The commitments and obligations should be clear for both the client and provider in order to avoid misunderstandings which might lead to violations.

– The policy contained in the contract should be based on a representation able to map the knowledge of each organization (regarding mainly the wishes and expected behavior of the external stakeholders) into a representation understandable for the machine.

The aforementioned requirements motivated us to using semantics and its underlying DL formalism for the representation of our contract. The methodology followed for the construction of our machine-readable contract model is presented in detail in (Jaramillo *et al.*, 2015). Basically, we created a collection of contracts and we manually identified the terms belonging to our specific domain as well as the relations among those terms in order to mapped them into the classes and properties of our ontology-based model. For the sake of simplicity, some relations were omitted in Figure 1.

The contract model is composed of two main components. A first component which uses the OWL language for describing the semantic of the concepts described in the contract. Particularly, we associate attributes in the form of triples $<$*element, attribute, value*$>$ to the definition of the contractual concepts. The second component is the contractual policy, which uses the SWRL language for describing the rules

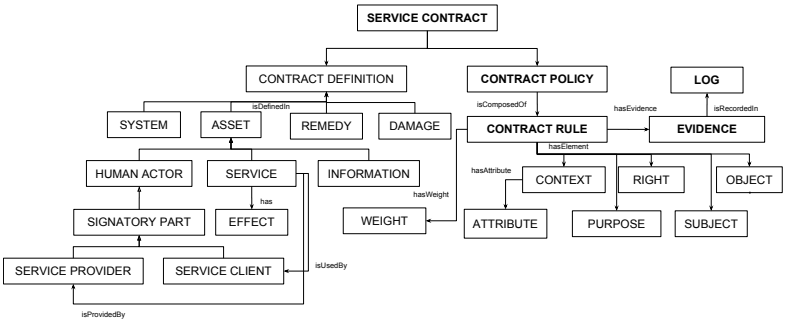

Figure 1. Ontology-based Contract Model

governing the service provision. Note that such a rules could be set either by the provider or the client. As depicted in Figure 1, the policy is a set of rules composed of a subject, an object, a right, a purpose and an attribute-based context. Rules represent therefore the recommendation, obligation, prohibition or permission to execute a right on a object if a certain conditions are fulfilled. In our model, objects are not limited to file or data categories but to the elements defined in the ontology. Similarly, a right is not limited to single actions but they are more coarse-grain and complex activities indicating the external partner "behavior" that need to be controlled during the service provision. Some examples of rules are *(i)* The provider must follow the standard X when process the client's personal information, *(ii)* The provider may delegate the activity W only if the activity is late and the delegate commits to carry out the activity on time.

4. Contract Evidences

As it was previously mentioned, in our policy we do not focus on single observable actions but in more complex behaviors that an external partner may perform during (or after) the service provision, and which may put a contractual party in a disadvantaged situation. Since it is not possible to monitor all the possible behaviors of the contractual parties, firstly by legal reasons and secondly because a behavior is by definition abstract in nature, we propose to attach some evidences to rules described in the policy.

Unlike current SLAs monitoring techniques, in our approach we do not verify the compliance of the policy in real-time or to check the truthfulness of the provided evidence. By contrast, we use evidences as a kind of guarantee. In this way, the mere existence of the evidence could be used to assign responsibilities in case of faults. That is to say, if, for instance, an information leakage is suspected, the sent evidences are used to prove the behavior of the external partner.

A log, recorded during the service provision, collects the evidences and metainformation proving compliance with the service contract. Listing 1 shows an excerpt of

the log describing the evidence *myFirstEvidence* which represents the digital signature of a contractual party named *John Smith*. As shown in the tag *<isEvidenceOf>* that evidence is created for proving compliance with Rule15.

Listing 1: Concrete Representation of Evidences

```
<rdf:Description rdf:ID="#myFirstEvidence">
        <rdf:type rdf:resource="http://ontology/ContractPolicy#Evidence">
        <Description> Description of the evidence linked to the rule 15 </Description>
        <isEvidenceOf rdf:resource="http://ontology/ContractPolicy#myRule15"/>
        <AbstractVerificationElement rdf:resource="http://ontology/ContractPolicy#SubjectElement"/>
</rdf:Description>
<rdf:Description rdf:about="SubjectElement">
        <ConcreteVerificationElement rdf:resource="JohnSmith"/>
        <AbstractEvidence rdf:resource="http://ontology/ContractPolicy#IdentityEvidence"/>
</rdf:Description>
<rdf:Description rdf:about="IdentityEvidence">
        <ConcreteEvidence rdf:resource="http://ontology/ContractPolicy#Signature"/>
</rdf:Description>
<rdf:Description rdf:about="Signature">
        <EvidenceLocation>http://localhost:8080/evidences/mySignature.ks </EvidenceLocation>
</rdf:Description>
```

5. Discussion

As part of the risk management process, organizations implement internal policies that allow to protect and guarantee some security criteria to their assets. Indeed, assets such as business data, processes, customer data, systems or equipment represent competitive advantages and could make the difference in front of their competitors. However, in collaborative environments, some assets are shared and this inherent loss of control makes that asset vulnerabilities may be exploited. Thus, a shortcoming regarding security is associated to the lack of information and strategies that may be used to guarantee that external partners comply with such established policies. Moreover, these vulnerabilities introduce risks that are reflected in organizational consequences such as legal sanctions, economic penalties, loss of clients, reduction of client satisfaction or decreasing of the reputation. Our approach could be used to reduce those risks by defining high-level business rules aiming the control on shared/delegated assets.

Similarly, another important perspective resulted of this work is associated to the accountability process. Accountability plays an important role in collaborative risk management. According to the Directive 95/46/EC "if the controller fails to respect the rights of data subjects, national legislation must provide for a juridical remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for the controller, who *may be exempted from liability if he proves that he is not responsible for the damage* [...]". Clearly, the use of logs and evidences are conceived as a tool for proving compliance with policies and regulations, which could avoid or reduce negative organizational impacts due to undesirable behaviors by external stakeholders.

Finally, a last perspective is associated to the selection of a particular partner for the service provision. Indeed, evidences established in the contract as part of the policy could be used for choosing partners that guarantee their behavior. For example, a particular service provider could be selected if he guarantees that he attaches his digital signature each time he modifies a shared asset.

6. Conclusion and Future Work

In this article, we presented an approach based on service contracts and evidences for improving the traditional web service-centered security. Our approach relies on the DL formalism for representing on the form of policies, the expected behavior of partners. This work leaves however some open issues, notably the creation of negotiation strategies that tackles the modification of the service policies.

References

Bensaidi M., Aboulkalam A., Marzouk A. (2012, April). Politique de contrôle d'accès au cloud computing: Recommandation à base de confiance. In *Network security and systems (jns2), 2012 national days of*, p. 90-96.

Guidara I., Chaari T., Fakhfakh K., Jmaiel M. (2012). A comprehensive survey on intra and inter organizational agreements. In *Proceedings of the 2012 ieee 21st international workshop on enabling technologies: Infrastructure for collaborative enterprises*, pp. 411–416. Washington, DC, USA, IEEE Computer Society.

Jaramillo G. E., Anisetti M., Ardagna C. A. (2015, May). A hybrid representation model for service contracts. In *2015 international conference on information and communication technology research (ictrc2015).* Abu Dhabi, UAE.

Kearney K. T., Torelli F., Kotsokalis C. (2010). Sla*: An abstract syntax for service level agreements. *11th IEEE/ACM International Conference on Grid Computing (GRID)*, Vol. 11, pp. 217 - 224.

Layouni F., Pollet Y. (2009, February). Fi-orbac : A model of access control for federated identity platform. In *Iadis 2009, the international conference on information system.* Barcelona, SPAIN. (ISBN: 978-972-8924-79-9)

Mustapha B. S., Elkalam A. A., Marzouk A. (2012). Torbac: A trust organization based access control model for cloud computing systems. *International Journal of Soft Computing and Engineering (IJSCE)*, Vol. 2, No. 4, pp. 122-130.

Nepal S., Zic J., Chen S. (2008). Wsla+: Web service level agreement language for collaborations. In *Proceedings of the 2008 ieee international conference on services computing - volume 2*, pp. 485–488. Washington, DC, USA, IEEE Computer Society.