Dynamic Negotiation Layer for Secure Semantic Service Oriented Architectures

Fabio Sanvido, Daniel Díaz Sánchez, Florina Almenárez Mendoza, Andrés Marín López
Telematic Engineering Department, Carlos III University of Madrid, Spain
Email:{fsanvido, dds, florina, amarin}@it.uc3m.es

***Abstract*—The approach of users connected anytime, anywhere, has led to merging isolated islands of enriched services environments into the WEB, leaving the user free to choose among an huge number of services. In this context the introduction of ontologies and the creation of semantic Web services mainly focus on using reasoners and planning algorithms to achieve automation in basic processes as discovery, composition and invocation. Nevertheless, there is a problem in standardizing one unique ontology that rises in alignment issues between the domain-specific ontologies on which semantic web service description language eventually rely. Moreover, there is no standardized processes that properly face privacy problem when participants require a graduate disclosure of domain sensitive information. We argue in this paper that a negotiation layer that could connect service consumer and service provider is necessary in order to overcome such limitations. The use of SAML as transverse security language is proposed.**

***Index Terms*—Semantic services; SAML; ontology interoperability; semantic policy.**

I. INTRODUCTION

Increasing development and deployment of broadband technologies [1] are bringing modern users more and more pervasive word where they are literally surrounded by services. Moreover, the huge penetration of devices such as smartphones and tablet PCs makes evident this trend will only going to increase. The approach of users connected anytime, anywhere, has led to merging isolated islands of enriched services environments into the WEB, leaving the user free to choose among an huge number of services and so erasing strong barriers between private and public domains. In this context, many users use their private nomadic or mobile devices to access sensible data, both personal such as photo and health data or enterprise data creating very difficult scenarios where different security and privacy needs are blended. Besides, users demands services more and more complex and flexible, so that pervasive systems should be able to dynamically use available services to create mashups that could satisfy users requirements. At the same time, users should be able to actively create personal, high specialized mashups by choosing among available services, or among a narrowed pool of services suggested by the system to fit user's specifications.

Automated service composition had been a hot topic of research during the last years and ontologies have been individuate has a key factor for advanced services features such as composition. The introduction of ontologies and the creation of semantic Web services mainly focus on using reasoners and planning algorithms to achieve automation in basic processes as discovery, composition and invocation. An example of automate composition from service providers perspective is given in [2], where a knowledge-based framework is used to solve the problem of transcoding multimedia contents for adapt distribution to user device capabilities. Here, authors rely on reasoning capabilities in order to compute the most suitable step sequence to obtain seamless transcodification. But, such an ad-hoc approach is not feasible if ported to pervasive scenarios, where users do not know their environment in advance.

In this paper the semantic service scenario is presented in-Section II, where a brief overview of languages and ontologies developed for web services is given. In Section III, the focus is moved over the problem of security for semantic web services, a field where interoperability raise as a fundamental issue. In Section IV, our approach for semantic concept negotiation is depicted.

II. SEMANTICS IN WEB SERVICES

Several efforts have been made in order to provide a semantic frameworks for web services, generally those efforts focus on defining standard ontologies which can be used for describe services and for performing reasoning processes. Between standard service description ontologies, two solutions take particular relevance: the Semantic Web Services ontology (OWL-S) [3] and the Web Service Modeling Ontology (WSMO) [4]. Both initiatives have developed a set of ontologies which aim to provide necessary classes and properties in order to declare and describe services; but, while WSMO attempts to focus on integration, OWL-S keeps more general trying to cover description of services in a wide sense. Deeply comparing advantages and drawbacks of the two approaches keeps out of the scope of this paper, Lara et al. [5] provide good starting point for comparison, being all ontologies and tools available on initiatives web pages. Besides, the Semantic Annotations for WSDL (SAWSDL) was produced by the W3C in order to provide existing web service with semantic annotation. SAWSDL provides sets of XML attributes to establish relations between WSDL tags and the concepts of one or more arbitrary ontology. Flexibility of

This work was partially founded by the Spanish Ministry of Science and Innovation within the framework of the project TEC2010-20572-C02-01 CONSEQUENCE"

 ISBN: 978-1-61208-171-7

SAWSDL allows the use of different ontologies to describe, for instance, technical details of the service and the semantics of the specific business domain. Nevertheless, its limited expressiveness suggests the need for SAWDSL to work in conjunction with richer semantics as OWL-S could be [6].

OASIS has also specified a Reference Ontology for Semantic Service Oriented Architectures (RO-SOA) [7], which aims to describe services without ties with any specific technology. Thus, RO-SOA should provide upper-level semantics with independence from specific implementations.

Coming to more recent initiatives, Minimal Service Model provides a service model first introduced together with hRests [8] and WSMO-Lite [9]. The ontology it provides is intended to be a bridging ontology, which aims at integrating web service and web API semantics as well as provide a bridge between previous works such as OWL-S and WSMO.

The Unified Service Description Language (USDL) [10] enriches the technical description of services with business related information, which is modeled in a pool of non-functional ontology modules. A peculiarity of this framework lies in being able to describe physical services that do not have any implementation. Also, the Reference Service Model (RSM) [11], enhances technical description of services but focusing on the bottom-up social service annotation. One of the scopes of RSM development is to overcome difficulties in aligning concepts from different semantic framework. RSM authors states that the use of a reference model such as RSM as intermediary level of alignment can reduce the scalability problem suffered by systems who try to maps concepts belonging to different service models. While this kind of centralization of the alignment issue could effectively relieve to reduce the number of bilateral mappings among ontology concepts, it in practice shift the issue of choosing a reference ontology onto choosing a reference model.

Moreover, in the last years, industry has begun using ontologies in order to describe internal organization, specific network constructions, roles and hierarchies of employers among others. Different ontologies have been created to represent specific areas of knowledge such as juridical language for archiving purposes or ontologies that collect and represent regulatory remarks whose interaction would be hardly representable in a simplest way. On top of such diverse bases of knowledge run tools for policy definition and validation or software that provide services for control, intrusion detection and data mining for instance. The integration of this kind of information with the description of semantic web service would require more dynamic approaches to concept align that allow participants to negotiate only the information needed to incorporate those concepts really indispensable to the current transaction.

III. Security policies for semantic-WS

Security requirements such as authentication/authorization and cryptographic data protection are extremely stringent in the semantic web scenario. As previously stated, one of the key objective of introduction of semantics in the world of services is automation, which means that systems could autonomously decide what information exchange, when and how do it. If not enough, inferred information should be taken into account. Whether privacy is a primary objective, users and administrators should consider that some information could be derived from other by the reasoning system. Moreover, in automate composition scenarios, not all parties are known in advance so that sensitive information could be collected in very different time or locations without the knowledge of service end user. Thus, it is fundamental need for a semantic web service description language, and its underlay ontology, to be able of represent this kind of interaction and requirements, in particular security parameters have to be considered as much as functional ones by service composition engines. The definition of security policies represents a good way to define this type of constraints and ontologies has already been identifies as helpful tools for define compliant and robust policy environments. There exist several efforts [12] in specifying languages for semantic representation and reasoning over policies for distributed systems but not all previous presented frameworks for semantic web service have a native approach on security parameters management.

WSMO aligns with WS-Policy, which is essentially a mechanism for combining domain-specific policy assertions and attaching them to various policy subjects. Policies are attached to Web service description and treated as non-functional properties of the service. WSMO description elements can thus be views as components for policy assertions, which will be combined as alternative assertions within the same policy.

OWL-S, in turn, has been object of specific enhancement in the security aspect and provides a set of ontologies which describe security mechanisms, credential and privacy elements that allow the definition of security policies elements [13].

USDL service level module tries to abstract technical details of security languages such as XACML or WS-Security providing elements, i.e., *SecurityAttribute* or *SecurityGoal*, which aim to define high level security objectives. However, it eventually relies on WS-SecurityPolicy artifacts for detailed definition of security policies.

The variety of scenarios depicted raises the need of interoperability solutions able to deal with different policy implementation framework. Service description solutions eventually rely on domain specific ontology description for the representation of atomic services or specific domain environments. For example, during the specification of security or privacy policies will likely be necessary to define the concrete roles organization uses within its domain or, regarding functionality, framework ontologies may be modified in order to add some specific feature they does not capture at first and maybe never does, if there is no extensive use of such a definition. Ontologies cannot be static entities simply because concepts they model are not. As ontology implementations have gained popularity, several private, slightly different representations of the same concepts have been developed. This could not be a real problem in close environments such as specific purpose software, but became essential when more parties interact in the same process. However, construction of a “universal”

 ISBN: 978-1-61208-171-7

ontology that would be used to model all kind of services and concepts are not feasible, unless dynamic evolution is taken into account. Moreover, current system for matching policies works with a centralized paradigm where all information about services is published in one broker or aggregation entity. Exposing complete service description and associated security and privacy policies could reveal a wealth of information about for instance infrastructure management that at first would intended to be maintained hidden.

Besides, entities acting as service brokers, who expose services and match consumer requests in order to find the most suitable service, face a problem that is current unresolved. Those systems, especially if working in a semantic environment, must deal with some degree of uncertainty when they are called to take a decision about how well services match each other. In order to clarify these problems, let us consider the example *a)* where a consumer, either a user or an agent, registry against the service broker asserting it has the capability of authenticate itself. It owns different identities, which use different mechanism for authentication, state username-password pair and X509 certificate, and will use them depending of the trust relationships it has previously established, or will able to establish on the fly, with the available service provider. Furthermore, the user/agent does not want to reveal all its capabilities at the same time for privacy purposes. The service which would match consumer functionality requirements has registered itself with stronger authentication requirements and claims consumer to have an X509 certificate. In this situation, service brokers could fall into a mismatch to preserve the higher degree of security.

Another case of mismatch could derive from participant membership. Consider example *b)*, in which the consumer has registered as member of organization A with access level 1 (A_1) while service provider as member of organization B. Both can prove their membership with credential and service provider will serve only members of its own organization, which access level is α (B_α). Organization B is member of a federation and so it report in registration. Details of federation are not reported to the service broker due to privacy agreements and because organization B dynamically joints and leave several federation environments. When consumer realizes the service request, A and B belong to the same federation but if not all the details of both organizations are clearly specified in both registrations there is no way for the system to correctly match participants. Even if broker would able to identify that A and B belong to the same federation, it will still not be able of matching access levels, which are high specific information. For example, if service provided by B is going to modify one federation's database, only databases admins from participant organizations can access it.

Most of the problems above mentioned could be solved by introducing a negotiation layer, which in case of partial match allows contacting service provider with the consumer and thus allowing them to agree on protocol details, establish or verify a trust level or aligning knowledge bases. More generally, the decision process would be partially moved from one centralized entity, the service broker, to a decentralized schema that could lighten interoperability issues and render more dynamic systems.

IV. NEGOTIATION LAYER

During the last years Security Assertion Markup Language (SAML) [14] has been applied by organizations worldwide in a number of different applications in order to cover their identity management needs, so much so that it could be considered the standard of choice in the global eGovernment and public sectors [15]. SAML assertions can also be used within SOAP messages in order to carry security and identity information between actors in Web service transactions. The SAML SOAP binding specifies how SAML assertions should be used for this purpose [16]. On this premises, we propose to extend SAML in order to support semantic language interactions by providing standard, transverse profiles for interoperability. We are working on the definition of a profile, which could accommodate semantic service description languages and allow the exchange of security assertion in a semi-predefined manner. The aim of such a profile would be to facilitate the request of additional information for align purposes as well as the definition of standard negotiable methods to overcome the privacy limitations depicted in Section III. At the same time proposed SAML profile could fill the bridge between trust and federation frameworks, already deploying SAML based management technologies, and the semantic automation of services.

Consider again example *b)* in Sec. III. The major issue is the different representation of access level rights. As service provider and service consumer belong to different organizations there is no way to establish a relation between level B_α and A_1. We propose to use special SAML assertions to allow entities to request additional information about counterpart organization knowledge until an alignment process can successfully take place. To initiate the profile, the requesting entity sends a <*ManageKnowledgeRequest*> message to the entity from which it wishes additional information, see Fig.1. The <*ManageKnowledgeRequest*> message should be signed or otherwise authenticated and integrity protected by the protocol binding used to deliver the message.

```
<element name="ManageKnowledgeRequest" type="samlp:ManageKnowledgeRequestType"/>
  <complexType name="ManageKnowledgeRequestType">
    <complexContent>
      <extension base="samlp:RequestAbstractType">
            <element ref="samlp:ontelement" maxOccurs="1"/>
      </extension>
    </complexContent>
  </complexType>
<complexType name="TerminateType"/>
```

Fig. 1. Schema fragment defining the <*ManageKnowledgeRequest*> element and its *ManageKnowledgeRequestType* complex type.

This message has the complex type ManageKnowledgeRequestType, which extends RequestAbstractType and adds the element <*ontelement*>, which is intended to be an ontology element belonging to organization A and not present or not knew by organization B. In the context of the

 ISBN: 978-1-61208-171-7

```
<element name="ManageKnowledgeResponse" type="samlp:ManageKnowledgeResponseType"/>
  <complexType name="ManageKnowledgeResponseType">
    <complexContent>
      <extension base="samlp:StatusResponseType">
        <choice minOccurs="0" maxOccurs="1">
          <sequence>
            <element ref="samlp:ontelement"/>
            <attribute name="Relation" type="string" use="required"/>
            <attribute name="URL" type="string" minOccurs="0"/>
          </sequence>
          <element ref="samlp:ontelement" maxOccurs="unbounded"/>
        </choice>
      </extension>
    </complexContent>
  </complexType>
<complexType name="TerminateType"/>
```

Fig. 2. Schema fragment defining the <*ManageKnowledgeResponse*> element and its *ManageKnowledgeResponseType* complex type.

example it represents the access level of service consumer within organization A.

The recipient of a <*ManageKnowledgeRequest*> message must respond with a <*ManageKnowledgeResponse*> message, which is of type ManageKnowledgeResponseType which extends StatusResponseType, see Fig. 2. The element <ontelement> is used to inform the requester of an existent relation between requested ontelement and a third, public ontology element. The responder can opt to send a sequence of ontelement that provide enough information to align B's knowledge with A's one. In the context of the example, service consumer can respond with the A's hierarchy of rights, so that B can understand the role of A in its own organization. In Fig. 3 the sequence of messages during the application of the profile is reported.

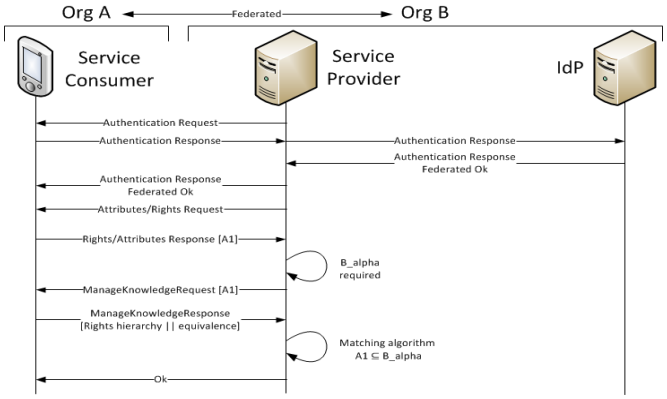

Fig. 3. Message sequence for an application of the profile. The service provider contacts with its Identity Provider in order to authenticate A within the boundaries of the federation.

V. Conclusion and Future Work

In this article a preliminary work for the definition of a SAML profile has been presented. The aim of the proposed profile is to introduce a degree of flexibility in the discovery and selection phase for Semantic Web Services belonging to different domains.

In Section IV, protocol messages for achieving ontology alignment in pervasive scenarios have been presented. The scope of proposed protocol is not to provide a complete matching procedure or a policy resolution protocol, contrariwise the aim of the profile is to use a wide accepted and implemented technology to overcome interoperability issues that appear when clients and providers of different domains interact, a common scenario in ubiquitous environments.

Currently, we are working on enhance the profile specification and evaluate it in real case scenarios. The main steps in this regard are implementation of required SAML assertions and their integration with semantic services frameworks in order to test the usefulness and efficiency of the procedure.

References

[1] R. Young Kyun, Kim; Prasad, *4G Roadmap and Emerging Communication Technologies*. Artech House, 2006, pp 12-13. ISBN 1-58053-931-9.

[2] D. Jannach and K. Leopold, "Knowledge-based multimedia adaptation for ubiquitous multimedia consumption," *J. Netw. Comput. Appl.*, vol. 30, pp. 958–982, August 2007.

[3] D. Martin, M. Burstein, H. Jerry, O. Lassila, D. McDermott, S. McIlraith, S. Narayanan, M. Paolucci, B. Parsia, T. Payne, E. Sirin, N. Srinivasan, and K. Sycara, "Owl-s: Semantic markup for web services." [Online]. Available: http://www.w3.org/Submission/OWL-S, Retrieved: September 2011

[4] J. Bruijn, C. Bussler, J. Domingue, D. Fensel, M. Hepp, U. Keller, M. Kifer, B. Konig-Ries, J. Kopecky, R. Lara, E. Lausen, Holger Oren, A. Polleres, D. Roman, J. Scicluna, and M. Stollberg, "Web service modeling ontology (wsmo)." [Online]. Available: http://www.w3.org/Submission/WSMO/, Retrieved: September 2011

[5] R. Lara, D. Roman, A. Polleres, and D. Fensel, "A conceptual comparison of wsmo and owl-s," in *Web Services*, ser. Lecture Notes in Computer Science, L.-J. Zhang and M. Jeckle, Eds. Springer Berlin/Heidelberg, 2004, vol. 3250, pp. 254–269.

[6] D. Martin, M. Paolucci, and M. Wagner, "Bringing semantic annotation to web services: Owl-s from the sawsdl perspective." in *ISWC/ASWC'07*, 2007, pp. 340–352.

[7] OASIS, "Reference model for service oriented architecture 1.0, public review draft 02," 2011. [Online]. Available: http://docs.oasis-open.org/semantic-ex/ro-soa/v1.0/pr02/see-rosoa-v1.0-pr02.pdf, Retrieved September 2011

[8] J. Kopecky, K. Gomadam, and T. Vitvar, "hrests: An html microformat for describing restful web services," in *Web Intelligence and Intelligent Agent Technology, 2008. WI-IAT*, vol. 1, dec. 2008, pp. 619 –625.

[9] T. Vitvar, J. Kopecky, M. Zaremba, and D. Fensel, "Wsmo-lite: lightweight semantic descriptions for services on the web," in *Web Services, 2007. ECOWS '07.*, nov. 2007, pp. 77 –86.

[10] A. Charfi, B. Schmeling, F. Novelli, H. Witteborg, and U. Kylau, "An overview of the unified service description language," in *Web Services (ECOWS), IEEE 8th European Conference on*, 2010, pp. 173 –180.

[11] N. Loutas, V. Peristeras, and K. Tarabanis, "Towards a reference service model for the web of services," *Data & Knowledge Engineering*, vol. 70, no. 9, pp. 753 – 774, 2011.

[12] T. Phan, J. Han, J.-G. Schneider, T. Ebringer, and T. Rogers, "A survey of policy-based management approaches for service oriented systems," in *Software Engineering, 2008. ASWEC 2008*, March 2008, pp. 392 – 401.

[13] L. Kagal, T. Finin, M. Paolucci, N. Srinivasan, K. Sycara, and G. Denker, "Authorization and privacy for semantic web services," *Intelligent Systems, IEEE*, vol. 19, no. 4, pp. 50 – 56, Jul-Aug 2004.

[14] OASIS Technical Overview Committee, "Security assertion markup language (saml) v2.0," March 2008. [Online]. Available: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf, Retrieved: September 2011

[15] Liberty Alliance, "Organizations worldwide leverage saml 2.0 liberty federation to enable new business services, help meet regulatory requirements and provide users with better protection against online fraud and identity theft," January 2008. [Online]. Available: http://www.projectliberty.org/, Press Release. Retrieved September 2011

[16] OASIS Standard, "Bindings for the oasis security assertion markup language (saml)," March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os, Retrieved: September 2011

 ISBN: 978-1-61208-171-7