53 AN APPROACH FOR ESTABLISHING TRUST RELATIONSHIPS IN THE WEB SERVICE TECHNOLOGY

Diego Zuquim Guimarães Garcia, Maria Beatriz Felgar de Toledo
Institute of Computing, University of Campinas, BRAZIL
{diego.garcia,beatriz}@ic.unicamp.br

Some solutions have been proposed to deal with the establishment of Web service relationships. For instance, a consortium has developed the Web Services Trust Language (WS-Trust) that offers a trust model for Web services. However, trust is one aspect in a set of aspects involved in Web service security that includes, for instance, privacy preservation. Based on this fact, the goal of this paper is to propose a trust approach for Web services. The approach integrates WS-Trust with standards for policy and ontology, which are used to preserve privacy.

1. INTRODUCTION

In the current market, organizations depend on getting involved in collaborations with other organizations for responding to some market opportunities. Significant progress has been done towards making the Web service technology a suitable solution for supporting such collaborations. For example, the interoperability among software systems is an important benefit of this technology. However, there are still open issues hindering this, including the lack of suitable mechanisms to support trust management.

A base for collaborations among organizations is the trust among them (Msanjila and Afsrarmanesh, 2007). This paper deals with technical aspects for the establishment of trust relationships. It focuses on trust relationships among entities in the Web service technology. Thus, the proposed approach is suitable for the establishment of trust relationships among software systems representing organizations in the dynamic Web service environment.

Some solutions have been proposed to deal with trust management in Web services. Among them, the Web Services Trust Language (WS-Trust) (Nadalin et al., 2007) deserves special consideration. At present, it is an OASIS (Organization for the Advancement of Structured Information Standards) standard. It defines a Web service trust model. However, trust is just one aspect involved in Web service security and some security aspects have relationships among them (Geuer-Pollmann and Claessens, 2005).

The goal of this paper is to propose an approach for trust relationship establishment that, differently from the current approaches, integrates WS-Trust with the Web Services Policy Framework (WS-Policy) (Bajaj et al., 2006). This

Please use the following format when citing this chapter:

Garcia, D.Z.G. and Felgar de Toledo, M.B., 2008, in IFIP International Federation for Information Processing, Volume 283; *Pervasive Collaborative Networks*; Luis M. Camarinha-Matos, Willy Picard; (Boston: Springer), pp. 509–516.

paper deals specifically with policies for privacy preservation and uses the Platform for Privacy Preferences (P3P) (Cranor et al., 2002).

The use of WS-Policy may restrict relationships among interoperable services. In order to overcome this limitation, a privacy ontology in Web Ontology Language (OWL) (Patel-Schneider et al., 2004) is used for annotating policies. This semantic information is used to verify if providers and consumers have compatible policies.

The rest of the paper is organized as follows. Section 2 presents basic concepts. Section 3 describes the proposed approach for trust establishment. Section 4 discusses related work. Finally, Section 5 closes the paper with conclusions.

2. BASIC CONCEPTS

2.1 Web Services and Policies

In the Web service technology, organizations (providers) provide Web services to other organizations (consumers). An organization can take both roles. A Web service is an electronic service identified by a URI (Uniform Resource Identifier). XML (eXtensible Markup Language) standards are used to specify service interfaces and to invoke services through the Web. The Web service technology comprises three basic standards (Alonso et al., 2004):

- Web Services Description Language (WSDL): a format for describing the functionality of a service;
- Universal Description Discovery & Integration (UDDI): a registry that supports service publication and discovery;
- SOAP (formerly Simple Object Access Protocol): a protocol for message exchange among services.

Additional standards are under development. One example is WS-Policy (Bajaj et al., 2006). It provides a model for expressing service properties as policies. Policies can be associated with XML elements, as defined in the Web Services Policy Attachment (WS-PolicyAttachment) specification. A policy is a collection of alternatives and each policy alternative is a collection of assertions. An assertion is defined as an individual requirement, capability or other property. Assertions specify characteristics that are critical to service selection and use, for instance, Quality of Service (QoS) attributes.

2.2 Web Service Security

In Web services, mechanisms to protect SOAP messages are defined in the Web Services Security (WS-Security) standard (Nadalin et al., 2006). They include digital signature, to protect against inappropriate message alteration, and encryption, to deal with incorrect message disclosure.

Services have to exchange security tokens to secure their communications. A security token is a collection of claims. A claim is a statement made by an entity, for instance an identity or capability statement. However, each service needs to determine if it can trust the other one, that is, to accept as true the claims in the token sent by the other service. This can be accomplished directly or by means of a third

party. WS-Trust (Nadalin et al., 2007) defines extensions that build on WS-Security mechanisms to broker trust relationships.

There are standards for other aspects of Web service security (Zhang, 2005). However, the Web service technology still lacks a standard for privacy preservation. There is a privacy standard for the Web. P3P (Cranor et al., 2002) is a World Wide Web Consortium (W3C) Recommendation for a Web privacy framework. It defines a privacy vocabulary. The developing P3P Version 1.1 includes a mechanism that can be used to employ P3P with other protocols and applications, beyond HyperText Transfer Protocol (HTTP) transactions, including XML applications.

3. WEB SERVICE TRUST ESTABLISHMENT

In the approach, to interact with a service, consumers must send policies that satisfy the service policy. Consumers that try to interact with services, but do not possess the trusted tokens required by the services, are rejected. The approach is illustrated in Figure 1.

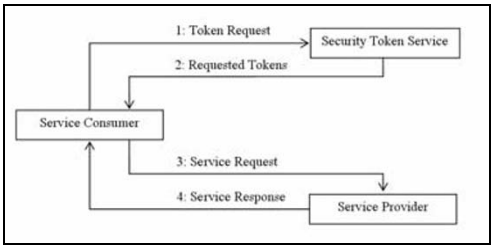

Figure 1 – Approach for Web service trust

Sometimes, consumers do not possess suitable policies to satisfy service policies. In this case, the consumer uses a Security Token Service to obtain the necessary tokens (Step 1 in Figure 1). Security Token Services are trusted third-party authorities defined by WS-Trust that issue tokens. Tokens are included into WS-Policy policies and are signed to guarantee that they have been issued by Security Token Services. After receiving a policy with the necessary tokens from the Security Token Service (Step 2), the consumer uses it to interact with the service to which the policy applies (Step 3). The service verifies the consumer policy in order to confirm that the consumer satisfies its requirements. After the verification, the service responds the consumer request (Step 4).

A proof-of-possession token received by the consumer along with a security token can be used to indicate that it has the right to use the security token.

Security Token Services are Web services and define policies. Thus, consumers must provide suitable tokens to use Security Token Services. After verifying that the tokens received from a consumer have been issued by Security Token Services and that the tokens can be used by the consumer, the Security Token Service issues the requested tokens.

Two messages are used for issuing tokens. The *RequestSecurityToken* message is used for requesting the issuance of tokens. The *RequestSecurityTokenResponse* message is used for returning issued tokens.

The *RequestSecurityToken* message is prepared by the consumer as follows:

1. The message is signed by the consumer with its private key;
2. Then, it is encrypted using the public key of the Security Token Service.

After receiving the *RequestSecurityToken* message, the Security Token Service sends a *RequestSecurityTokenResponse* message. This message includes policies with the requested security tokens and the associated proof-of-possession tokens. The Security Token Service performs the following steps to create a security token:

1. The Security Token Service generates a symmetric key;
2. It encrypts the key using the public key of the service, which the consumer wants to use, and includes the encrypted key into the security token;
3. Then, it includes the requested claims into the token;
4. Finally, it signs the token using its private key.

The Security Token Service creates a proof-of-possession token as follows:

1. It encrypts the symmetric key using the public key of the consumer and includes the encrypted key into the proof-of-possession token;
2. Then, it signs the token using its private key.

After receiving the *RequestSecurityTokenResponse* message, the consumer sends the token together with the service request. This message is prepared as follows:

1. The symmetric key from the proof-of-possession token is decrypted by the consumer;
2. Then, the service request is signed using the symmetric key;
3. The signed service request is encrypted using the public key of the service;
4. Finally, the service request and the security token are included into the request message.

After receiving the request message, in order to execute the requested operation, the service performs the following steps:

1. The service verifies the claims in the token;
2. Then, it decrypts the symmetric key from the security token;
3. Finally, the service decrypts the service request.

3.1 Trust Brokering

In addition to token issuance, that is, the creation of a security token and its proof-of-possession token, Security Token Services are responsible for other actions:

- Validation: the authenticity of an issued token is evaluated;
- Renewal: a new validity period is defined for an issued token whose validity period has expired;
- Cancellation: the use of an issued token is terminated.

These actions are performed using the same messages used for issuing tokens. These messages are specified below.

The *RequestSecurityToken* message includes the following attributes and elements:

- *Context*: a context identifier to enable the correlation of the request and the subsequent related messages;

- *RequestType*: the requested action (token issuance, validation, renewal or cancellation);
- *TokenType*: the type of the requested security tokens;
- *Lifetime*: the desired validity period for the security tokens;
- *AppliesTo*: the service, which the consumer wants to use and to which the security tokens apply;
- *ProviderPolicy*: the policy of the service with the required tokens that the consumer does not possess;
- *ConsumerPolicy*: the policy of the consumer with tokens that are necessary for the execution of the requested action;
- *IssuedTokenPolicy*: a policy with tokens to be validated, renewed or cancelled.

The *RequestSecurityTokenResponse* message includes the following attributes and elements:

- *Context*: the context identifier from the associated *RequestSecurityToken*;
- *Lifetime*: the lifetime of the returned tokens, which can be different from the requested validity period;
- *RequestedSecurityToken*: a policy with the requested security tokens;
- *RequestedProofToken*: a policy with the proof-of-possession tokens associated with the security tokens included in the message;
- *RequestResult*: an indication of the result of the requested action.

3.2 Privacy Policies for Supporting Trust Establishment

In the approach, the establishment of trust relationships is controlled using policies. Policies are used during different phases of the Web service life cycle:

- At design time, service providers define policies describing privacy preservation properties of their Web services and tokens that must be presented and proved by consumers;
- At runtime, service consumers define policies stating their tokens and privacy preservation properties that should be offered by Web services.

The provider and consumer policies are intersected to compute the effective privacy policy. This policy indicates the interoperability between the participants in terms of privacy preservation.

The basic structure of policies is compliant with the WS-Policy normal form, which is shown in Figure 2.

```
01  <p:Policy>
02      <p:ExactlyOne>
03          ( <p:All>
04              ( <Assertion ...> ... </Assertion> )*
05          </p:All> )*
06      </p:ExactlyOne>
07  </p:Policy>
```

Figure 2 – Basic policy structure

In Figure 2, *p* is a prefix for the WS-Policy namespace URI. In addition to the components included into the normal form, other general-purpose components can facilitate policy manipulation. A policy includes the following components:

- *Policy*: the root element that indicates a policy;
- *Name*, *Id*: two kinds of policy identification may be used. Either the policy is associated with an absolute URI, using the *Name* attribute, or it is associated with a reference within the enclosing document, using the *Id* attribute;
- *PolicyReference*: the *PolicyReference* element may be used to include the content of a policy into another policy;
- *Service*: a provider policy includes a *Service* element to describe details of the service implementation for which the policy has been specified. A consumer policy includes this element to specify details of the service type to which the policy applies;
- Operators: in a policy, policy alternatives are grouped into an *ExactlyOne* operator. The *All* operator represents a policy alternative and groups the alternative assertions;
- Assertions: policy assertions are elements that represent consumer privacy requirements and service privacy capabilities. A policy assertion may contain nested assertions and a nested policy.

It is in the assertion components that a policy is specialized. Policy assertions use concepts from a privacy ontology based on the P3P vocabulary. The ontology supports a high abstraction level for dealing with privacy preservation goals. The elements defined in the privacy ontology are described in Table 1.

Table 1 – Privacy ontology elements

Privacy Element	**Description**
Data items	Data items required to use services
Recipients	Entities that receive data items directly or indirectly
Use purposes	Purposes for which data items are used
Availability duration	Retention time for data items

Policy operations defined by WS-Policy may be used for processing privacy policies. For example, the intersection operation is used to determine providers whose privacy policies are suitable for a given consumer policy.

4. RELATED WORK

Some studies in the area of Web services that use WS-Trust are presented below.

Fang et al (Fang et al., 2004) and Wang (Wang, 2006) describe conversation establishment protocols.

Dini et al (Dini et al., 2005) propose an extension to WS-Trust for supporting self-adaptable trust based on past relationships between services.

Semantics for the main mechanisms of WS-Trust and protocols based on WS-Trust are developed in (Bhargavan et al., 2007).

Most of the work deals with trust in an isolated manner. Relationships among different aspects of security are not considered. Policy management, for instance, may be integrated into the WS-Trust trust model.

Work on Web service policies (Mukhi and Plebani, 2004) offers contributions to trust management. For example, mechanisms such as policy merge and intersection can be applied to manipulate security tokens. The same happens with work on QoS semantics. The approach of using ontologies for specifying QoS is employed in studies on some aspects of security. Kagal et al (Kagal et al., 2004) use the Semantic Web technology to handle authorization for Web services. Shields et al (Shields et al., 2006) propose an approach for the specification of access control policies.

Trust management using policies can employ a similar approach. An ontology may be used to capture semantic information about policy assertions. This information improves policy intersection, since intersection considering only the syntax of policies may not identify all compatible policies. In this case, trust relationships are not restricted by the verifications of characteristics performed during their establishment. In this work, this is accomplished by extending WS-Policy with the use of OWL and integrating it into WS-Trust.

5. CONCLUSIONS

The Web service technology still lacks facilities to deal with security. Particularly, the lack of suitable support for trust management is hindering its wide deployment. In the Web service architecture, the WS-Trust standard offers a framework for trust management. However, the current approach does not offer a mechanism for integrating trust and privacy policy management.

This issue has to be addressed in order to make the Web service technology a suitable solution for supporting collaborations among organizations. Trust is a base for such collaborations (Loss et al., 2007) and privacy is an important concern in this area (Masaud-Wahaishi et al., 2007).

In this paper, an approach that combines WS-Trust, WS-Policy and OWL was introduced to support the establishment of trust relationships with privacy preservation in the Web service technology. Policies are used to control security token exchange and privacy compatibility verification. A P3P-based ontology helps specifying semantics-enriched policies, which describe privacy requirements and capabilities of service consumers and providers.

The main contribution of this paper is extending the trust management approach for Web services with the use of semantic policies to enable service participants to establish trust relationships in conformity with privacy policies.

Future work includes investigating the possibility of extending the proposed approach with the inclusion of components of other privacy approaches, such as the approaches of rights management (Kenny and Korba, 2002) and pseudonym technology (Song et al., 2006). Moreover, the integration of the proposed approach and solutions for other aspects of Web service security may also be considered (Geuer-Pollmann and Claessens, 2005). Finally, a case study may be used to evaluate the benefits of the approach. Future work may be developed on these issues in order to support the applicability of the proposed approach in scenarios with different security constraints.

Acknowledgements

This project is supported by FAPESP.

6. REFERENCES

1. Alonso, G., Casati, F., Kuno, H., Machiraju, V. Web Services: Concepts, Architectures and Applications. Springer. 2004.
2. Bajaj, S., et al. Web Services Policy 1.2 - Framework. W3C, April 2006. http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/, accessed on 02/2008.
3. Bhargavan, K., Corin, R., Fournet, C., Gordon, A. D. Secure Sessions for Web Services. ACM Transactions on Information System Security. Vol. 10, No. 2, pg. 8, 2007.
4. Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C, April 2002. http://www.w3.org/TR/2002/REC-P3P-20020416/, accessed on 02/2008.
5. Dini, O. A., Moh, M., Clemm, A. Web Services: Self-adaptable Trust Mechanisms. In Proceedings of the Advanced industrial Conference on Telecommunications/Service Assurance with Partial and intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT-2005), pg. 83-89, Lisbon. July 2005.
6. Fang, L., Meder, S., Chevassut, O., Siebenlist, F. Secure Password-based Authenticated Key Exchange for Web Services. In Proceedings of the Workshop on Secure Web Services (SWS-2004), pg. 9-15, Fairfax. October 2004.
7. Geuer-Pollmann, C., Claessens, J. Web Services and Web Service Security Standards. Information Security Technical Report. Vol. 10, No. 1, pg. 15-24, 2005.
8. Kagal, L., Paolucci, M., Srinivasan, N., Denker, G., Finin, T., Sycara, K. Authorization and Privacy for Semantic Web Services. IEEE Intelligent Systems. Vol. 19, No. 4, pg. 50-56, 2004.
9. Kenny, S., Korba, L. Adapting Digital Rights Management to Privacy Rights Management. Computers & Security. Vol. 21, No. 7, pg. 648-664, 2002.
10. Loss, L., Schons, C. H., Neves, R. M., Delavy, I. L., Chudzikiewicz, I. S., Vogt, A. M. C., Trust Building in Collaborative Networked Organizations Supported by Communities of Practice, in Establishing the Foundation of Collaborative Networks, Springer, pg. 23-30, 2007.
11. Masaud-Wahaishi, A., Ghenniwa, H., Shen, W., A Privacy-Based Brokering Architecture for Collaboration in Virtual Environments, in Establishing the Foundation of Collaborative Networks, Springer, pg. 283-290, 2007.
12. Msanjila, S. S., Afsrarmanesh, H., Towards Establishing Trust Relationships among Organizations in VBEs, in Establishing the Foundation of Collaborative Networks, Springer, pg. 3-14, 2007.
13. Mukhi, N. K., Plebani, P. Supporting Policy-driven Behaviors in Web Services: Experiences and Issues. In Proceedings of the International Conference on Service Oriented Computing (SOC-2004), pg. 322-328, New York. November 2004.
14. Nadalin, A., Goodner, M., Gudgin, M., Barbir, A., Granqvist, H. WS-Trust Version 1.3. OASIS, March 2007. http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf, accessed on 02/2008.
15. Nadalin, A., Kaler, C., Monzillo, R., Hallam-Baker, P. Web Services Security: SOAP Message Security. OASIS, February 2006. http://oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, accessed on 02/2008.
16. Patel-Schneider, P. F., Hayes, P., Horrocks, I. OWL Web Ontology Language Semantics and Abstract Syntax. W3C, February 2004. http://w3.org/TR/owl-semantics/, accessed on 02/2008.
17. Shields, B., Molloy, O., Lyons, G., Duggan, J. Using Semantic Rules to Determine Access Control for Web Services. In Proceedings of the World Wide Web Conference (WWW-2006), pg. 913-914, Edinburgh. May 2006.
18. Song, R., Korba, L., Yee, G. O., Pseudonym Technology for E-Services, in Privacy Protection for E-Services, IGI, pg. 141-171, 2006.
19. Wang, J. A Web Services Secure Conversation Establishment Protocol Based on Forwarded Trust. In Proceedings of the International Conference on Web Services (ICWS-2006), pg. 569-576, Chicago. September 2006.
20. Zhang, J. Trustworthy Web Services: Actions for Now. IT Professional. Vol. 7, No. 1, pg. 32-36, 2005.