Using Semantic Rules to Determine Access Control for Web Services

Brian Shields, Owen Molloy, Gerard Lyons, Jim Duggan
Department of Information Technology
National University of Ireland
Galway, Ireland
brian.shields@geminga.it.nuigalway.ie
{owen.molloy, gerard.lyons, jim.duggan}@nuigalway.ie

ABSTRACT

Semantic Web technologies are bring increasingly employed to solve knowledge management issues in traditional Web technologies. This paper follows that trend and proposes using Semantic rule languages to construct rules for defining access control rules for Web Services. Using these rules, a system will be able to manage access to Web Services and also the information accessed via these services.

Categories and Subject Descriptors: K.6.5 [Management of Computing and Information Systems]: Security and Protection

General Terms: Security

Keywords: Web Service Security, Authorisation, OWL, SWRL

1. INTRODUCTION

Access to information using internet technologies is becoming increasingly popular. Incorporating data security in application design, previously an afterthought, is now a priority. Security in information transport was one of the first resolved, using standards such as SSL. This problem domain is less complex than the one we present a solution to in this paper. Securing information "over the wire" is a blanket solution, what the information is, or what it means is irrelevant. Securing access to this information is more difficult. Access control depends directly on what information is trying to be accessed, and we believe that understanding what this information is or means will aid its protection.

This abstract presents a novel approach to authorisation in a Web Services framework. We embrace existing standards in our solution, using standards from a number of fields such as Web Services, security and Semantic Web.

1.1 Underpinning Technologies

The Semantic Web is a family of specifications and proposed technologies that are maturing in parallel to Web Services. First coined by Tim Berners-Lee at the XML 2000 conference [5], the Semantic Web, as with Web Services, has consistently increased in popularity. Interest and research in the Semantic Web however remains primarily driven by the academic community.

The Web Ontology Language (OWL) [9] is a World Wide Web Consortium (W3C) standard for defining semantically rich languages. OWL Description Logic (OWL-DL) is a subset of OWL which guarantees completeness and decidability. The Semantic Web Rule Language (SWRL) [7] is a combination of the decidable subset of OWL and the Rule Markup Language.

WWW 2006, May 23–26, 2006, Edinburgh, Scotland.
ACM 1-59593-332-9/06/0005.

2. IMPLEMENTATION

It is necessary, for completion and testing of the above mentioned hypothesis, to develop a full security architecture. From research conducted into Web Service security frameworks [10] [6] [8] the principal components of a Web Service security architecture have been identified as encryption and decryption, signing and signature verification, key management and access control.

2.1 Web Service Security

The security framework designed and implemented as part of this research is built in Java using Apache Axis as the SOAP implementation. The core encryption and decryption engine is developed using Apache's Web Service Security for Java (WSS4J) implementation of the WS-Security specification from OASIS. It adheres to the W3C specification for XML-Encryption. The signing and signature verification engine is also developed using WSS4J and adheres to the W3C specification for XML-Signature. The key management is built according to the XML Key Management Specification (XKMS).

2.2 Semantically Defined Knowledge Base

The knowledge base which will be used in the authorisation process will be defined in OWL. This will be a description of the information being protected. The decidable subset of OWL, OWL-DL, will be used to represent the information in the system. All information does not have to be defined. This information base must contain at least a description of Web Service endpoints along with the the description of all the information at the level at which the user wants authorisation decisions to be made. This will be discussed more in Section 2.5.

2.3 Semantically Defined Rules

The rules used to define the access rights of individuals to the information represented in the knowledge base are writ-

ten in a semantically aware language. SWRL was chosen as the rule language in our system. The main advantage of using SWRL is its ability to provide support for complex relationships between properties, therefore extending the expressiveness of what we can define in OWL-DL. The subjects of the rules will be defined in the knowledge base, as described in Section 2.2. Rules may be written to protect access to two specific resources; the web service endpoints and the information they return. Return values from a Web Service call will usually differ, depending on the parameter list of each call.

2.4 Evaluating Rules

Since both the knowledge base and the authorisation rules are essentially written in OWL-DL, we can use an OWL-DL reasoning engine to evaluate the rules. The main advantage of SWRL, which was discussed in Section 2.3, can also present a new problem domain since it extends the expressiveness of OWL-DL beyond the decidable subset of OWL. There are two ways in which this can be overcome. Either restrict the expressiveness of SWRL and use an existing reasoning engine such as Pellet or Racer, or use a reasoner such as Hoolet which has been extended to handle SWRL rules.

We have chosen to use the extended reasoner Hoolet. To ensure a decidable result from our authorisation we will restrict how the user may write these rules rather than restricting the language itself.

2.5 Document Filtering

Authorisation decisions will firstly be made with respect to a Web Service endpoint. This can result in one of three results:

- Requester is granted full access
- Requester is refused any access
- Requester is granted limited access

A requester being granted limited access implies that they can access the endpoint but they will potentially be returned sensitive information that they do not have access to. When this happens, the response associated with the initial request is examined and the information being returned must be legally accessible by the requester. Any information which is defined as illegal for the requester will be pruned before the response is sent.

The level of pruning is defined by the user who is responsible for the update of the rules and knowledge stores. Information may only be pruned if it is defined in the knowledge base. For example, assume the information structure in Figure 1 exists in the system. If the user wants to specify that certain clients may not access Test Results then it must be defined in the knowledge base. Anyone with read access to Clinical Information will have read access to all of its undefined children.

3. CONCLUSIONS

There is some similar research being carried out. We have identified four projects that share some similarities to ours.

Rei is a distributed policy language that enables every Web entity to specify policies for its access [1].

Parsia et al, in [4], propose a semantically-aware policy language by translating WS-Policy into OWL-DL.

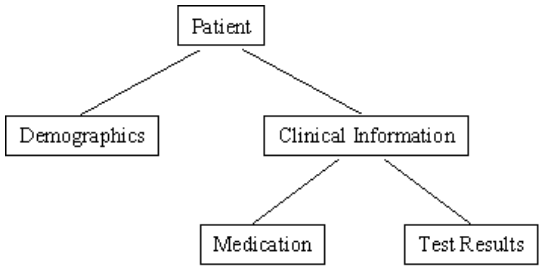

Figure 1: Sample Information Structure

Qin et al propose "an access control model for the Semantic Web that is capable of specifying authorisations over concepts defined in ontologies and enforcing them upon data instances annotated by the concepts" [2].

Damiani et al [3] outline how "current standard policy languages such as XACML can be extended" to be able to semantically define access control policies for the Semantic Web.

The model proposed in this abstract differs from each of these offerings. The first two items deal with policies for Web Services, often confused with authorisation rules. A policy is the information which the owner of the service wishes to share with potential business partners. The final two areas of research are more similar to this paper, although the research by Qin et al does not lend itself specifically to access control for Web Services and the work of Damiani et al enriches XACML with RDF, RDF will not provide the same semantic richness as OWL.

4. ACKNOWLEDGMENTS

This work is funded by Enterprise Ireland as part of the Advanced Technology Research Program.

5. REFERENCES

[1] L. Kagal, T. Finin and A. Joshi. *A Policy Based Approach to Security for the Semantic Web*. 2nd International Semantic Web Conference, Sanibel Islands, Florida, USA, 2003.

[2] L. Qin and V. Atluri. *Concept-Level Access Control for the Semantic Web*. ACM Workshop on XML Security, Fairfax, VA, USA, 2003.

[3] E. Damiani, S. De Capatani di Vimercati, C. Fugazza and P. Samarati. *Extending Policy Languages to the Semantic Web*. 4th International Conference on Web Engineering, Munich, Germany, 2004.

[4] B. Parsia, V. Kolozski and J. Hendler. *Expressing WS Policies in OWL*. 14th International World Wide Web Conference, Chiba, Japan, 2005.

[5] T. Berners-Lee. Keynote address at *XML 2000*. http://www.w3.org/2000/Talks/1206-xml2k-tbl/slide10-0.html, 2000.

[6] B. Hartman, D. J. Flinn, K. Beznosov, and S. Kawamoto. *Mastering Web Service Security*. Wiley, 2003.

[7] I. Horrocks and et al. *SWRL: A Semantic Web Rule Language combining OWL and RuleML*, May 2004. URL: http://www.daml.org/2003/11/swrl/".

[8] P. Kumar. *J2EE Security For Servlets, EJBs and Web Services*. Prentice Hall, 2004.

[9] D. L. McGuinness and F. van Harmelen. *OWL Web Ontology Language*, February 2004. URL: http://www.w3.org/TR/owl-features/.

[10] M. O'Neill. *Web Services Security*. McGraw-Hill/Osborne, 2003.