Access restriction inside ontologies *

– Extended abstract –

Martin Knechtel

SAP AG, SAP Research CEC Dresden
Chemnitzer Str. 48, 01187 Dresden, Germany
martin.knechtel@sap.com

1 Research Problem

This section gives a description of the overall research problem tackled in the context of the Ph.D. thesis and its relevance to the Internet of Services area.

To employ ontologies in commercial applications, there are some requirements to be met. The use case here is semantic management of resources. An ontology can define vocabulary to describe content in resources. Because the ontology alone already allows insights on the content, one important requirement is to allow different access rights inside ontologies to different users.

A resource can be anything identified by a Uniform Resource Identifier, e.g. a file, database table or Web page as well as a Wiki page or Blog entry. In the paper we focus on documents as one type of resource. However the concept is not limited to this type of resource. According to the Semantic Web idea, resources and parts within resources are semantically described with the vocabulary of an ontology. The ontology provides a conceptual structure above the content of resources and enables semantic navigation over resources.

Web services in the Internet of Services are tradable goods which can be described in documents and therefore can be seen as products. Ontologies can be used to provide the definition of common vocabulary to describe products and their properties. The product description is contained in resources. In Fig. 1 only the subset $\{service\ level\ agreement, response\ time, rt\_normal\}$ of the ontology concepts is visible for customers and an even smaller subset $\{rt\_premium\}$ is visible for premium customers. The ontology structure alone already contains valuable information and allows insights which may be not intended for every user.

In this example the question of restriction granularity arises. In the given case it is a difference, if documents containing the concept $rt\_premium$ are hidden or even the concept itself is hidden for customers. In Description Logics [1] the first case means to hide the A-Box individuals and the second means to hide the T-Box concepts.

* The project was funded by means of the German Federal Ministry of Economy and Technology under the promotional reference "01MQ07012". The author takes the responsibility for the contents.

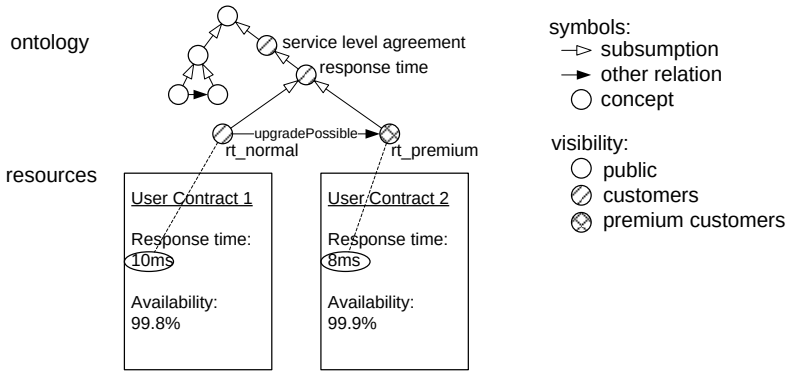

Fig. 1. Parts of the ontology are only visible for customers and for premium customers

2 Related Work

This section discusses the state of the art in the fields affected by access rights inside ontologies.

Semantic content management is studied e.g. for semantic portals [2]. Also wikis can be used for semantic content management [3]. The available works describe the motivation and implementation of content management with ontology support.

Authorization in other fields like file systems, content management systems, database management systems etc. is modeled by access control lists or by capabilities. The approaches often use hierarchies of the objects to inherit access rights. Due to the nature of ontologies, having no tree but a graph structure, access rights inheritance is of limited use. In the subsumption hierarchy a concept can be subconcept of several others, which leads to multiple inheritance. Object relations between concepts may form cycles. And it may be desired that a user can only see the superconcepts but not the subconcepts or the other way round.

Access rights restrict access to a subset of the original ontology. Ontology modularization is involved to decide if a subset in form of a module is complete [4]. In the other direction conservative extensions are extensions of an ontology without changing existing subsumption relations [5]. An interesting question for the thesis is how ontology modularization is influenced by assigned access rights. In the other direction ontology modularization can be a preliminary step to modularize an ontology to assign access rights to these modules.

Context representation in OWL-DL [6] ontologies allows to make the semantics of ontologies dependent on context information [7]. Examples for context of an ontology may be (a) links to other ontologies, (b) confidence and provenance information for elements obtained by automatic ontology learning and (c) collected arguments for and against an axiom. Context can be used for (a) reasoning with distributed ontologies with contradictory information or (b) for

creating a ranking to decide which axioms to drop. Also access rights may be seen as part of context [8].

According to [9] context can be used to separate a general and a public view on an ontology, whereas the latter can be derived from the former by a projection. This projection operation is not further discussed in detail. Surely it has to take several constraints into account, like access rights and completeness. A subset of an original ontology obtained by projection may not be complete enough to have any value. The thesis will investigate this.

Fine grained access control within ontologies is not well investigated in the research community yet. The contribution [8] presents basic access control methods and brings them in relation to ontologies. Although this work does not provide technical details, the recommendation for authority based access control (ABAC) is given and justified. They propose that hierarchies can be used to inherit rights. As stated above we think additional constraints exist for rights inheritance.

There are approaches for access rights inside ontologies. While [10] is based on a three-valued semantics and assumes an RDF tree without cyclic references, we want to use Description Logics and not restrict the ontology structure to a tree. In [11] the focus is to restrict access on syntactically heterogeneous resources with the help of a harmonizing ontology. A security policy is stored separately from the ontology, while we want to integrate it. An own ontology definition is used which is not conform to OWL-DL since e.g. axioms and individuals are missing, while we want to use OWL-DL.

3 Contributions

This section describes how the proposed project will advance the state of the art and summarizes expected contributions.

We conclude regarding the related work section that access rights can be modeled by context within an ontology. Therefore the hypothesis of the Ph.D. thesis which needs to be validated is, that access rights can be modeled sufficiently by context inside OWL-DL ontologies.

But there are no precise concepts available yet in related works and there are open questions. The contribution of the thesis will be a framework, a method and a prototype for access rights restrictions within ontologies. A conception and a syntactical representation of access rights will be developed. In further processing steps the ontology can be stripped down to a version which only contains elements which are accessible with the user's rights like a view in database systems. But this syntactic process will not be enough since the remaining axioms may not make sense alone. This means there is a guiding process needed to assign access rights.

The following research questions are proposed to be subject of the thesis:

1. Is context representation sufficient to model access control inside ontologies?
2. What is the right granularity for access control within an ontology: A-Box element, T-Box element, module, whole ontology, others?

3. What guiding process for rights assignment is appropriate in order to let all restricted views on one ontology remain complete enough?
4. What effect does access control in ontologies have on module extraction and reasoning?

4 Evaluation

This section describes the methodology used to evaluate and validate the results of the thesis project.

In the application scenario PROCESSUS of the research program THESEUS [12], semantic technologies for a Web platform to manage knowledge about solutions and applications are investigated. The application scenario can be used in parts to provide an evaluation scenario for the thesis' results.

The following exemplary test cases are based on the Pilot 2 of the PROCESSUS application scenario. Products and their applications are described in documents. Usage licenses for Web services are understood as products. Vendors are therefore service providers and customers are service consumers. The already introduced Fig. 1 contains concepts accessible for visitors without contract as well as concepts for customers and premium customers with contract. The exemplary test cases introduced here are the following. This is only a selection of the most important ones.

Public access and browsing: A user is interested in products described on the PROCESSUS platform. She browses products by the properties defined in the ontology. Because she has no contract yet, she is restricted to browse only public categories from the ontology. Documents for customers and for premium customers bound to a contract are not accessible, since (a) the user does not have access rights for some resources and (b) the user does not have access rights to browse some ontology concepts which are assigned to the documents' contents.

Access rights upgrade: The user just signed a contract, so she now also can see documents containing subscribed service level agreements. If she further upgrades to a premium user account, she will see documents describing product properties available to premium users. In the example in Fig. 1 she now has access to a document describing the higher response time of 8 ms.

Access rights assignment: A provider wants to describe offered Web services in documents. The documents are semantically annotated with elements from the domain ontology. The ontology contains different concepts for service level agreements for different types of customers. The provider assigns rights to ontology concepts and afterwards connects text chunks in documents to the appropriate ontology concepts.

5 Work Plan

This section sketches the different stages of the project and differentiates between the current status, the work in progress and planned future work.

Results achieved. The overall thesis work time is planned to be three years. Six months have passed so far. Currently the idea outline exists as presented in this abstract.

Current work. The current work is to investigate access rights within ontologies on behalf of an example case. The next planned step is a paper in 2008/07 to present a first concept and a deeper related work analysis than given in this extended abstract.

Planned work. Further steps are the following. Until 2008/08 a first draft of the exposé is planned. Until 2008/10 the structure of the manuscript and potential diploma thesis topics are formulated. Until 2009/10 the conceptual part of the thesis shall be ready. In parallel the implementation shall be ready until 2010/05. The thesis manuscript is planned to be ready in 2010/09.

References

1. F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. Patel-Schneider, *The Description Logic Handbook: Theory, Implementation and Applications*. Cambridge University Press, 2nd ed., 2007.
2. J. Hartmann and Y. Sure, "An infrastructure for scalable, reliable semantic portals," *IEEE Intelligent Systems*, vol. 19, pp. 58–65, 5 2004.
3. M. Krötzsch, D. Vrandecic, and M. Völkel, "Semantic MediaWiki," in *ISWC '06: Proceedings of the 5th International Semantic Web Conference*, (Athens, GA, USA), pp. 935–942, Springer, 11 2006.
4. B. C. Grau, I. Horrocks, Y. Kazakov, and U. Sattler, "Just the right amount: extracting modules from ontologies," in *WWW '07: Proceedings of the 16th international conference on World Wide Web*, (New York, NY, USA), pp. 717–726, ACM, 2007.
5. B. C. Grau, C. Lutz, M. Milicic, and U. Sattler, "Techniques for ontology integration and merging," Deliverable TONES-D19, TONES Project, 7 2007.
6. S. Bechhofer, F. van Harmelen, J. Hendler, I. Horrocks, D. L. McGuinness, P. F. Patel-Schneider, and L. A. Stein, *OWL Web Ontology Language Reference*. World Wide Web Consortium (W3C), 2 2004. W3C Recommendation, available at `http://www.w3.org/TR/owl-ref/`, retrieved January 3, 2008.
7. G. Qi, P. Haase, and S. Pinto, "Context representation formalism," Deliverable 3.1.2, NeOn Project, 2007.
8. M. Dzbor, A. Kubias, L. Gridinoc, A. Lopez-Cima, and C. B. Aranda, "The role of access rights in ontology customization," Deliverable 4.4.1, NeOn Project, 2007.
9. P. Haase, P. Hitzler, S. Rudolph, G. Qi, M. Grobelnik, I. Mozetic, D. Bojadziev, J. Euzenat, M. d´Aquin, A. Gangemi, and C. Catenacci, "Context languages - state of the art," Deliverable 3.1.1, NeOn Project, 2006.
10. S. Kaushik, D. Wijesekera, and P. Ammann, "Policy-based dissemination of partial web-ontologies," in *SWS '05: Proceedings of the 2005 workshop on Secure web services*, (New York, NY, USA), pp. 43–52, ACM, 2005.
11. C. Farkas, A. Jain, D. Wijesekera, A. Singhal, and B. Thuraisingham, "Semantic-aware data protection in web services," in *IEEE Web Services Security Symposium (WSSS) 2006*, (Berkeley, California, USA), 5 2006.
12. THESEUS research program, "PROCESSUS - optimisation of business processes." available at `http://theseus-programm.de/scenarios/en/processus`, retrieved March 7, 2008.