© Nottingham University Press
Proceedings of the International Conference on Computing in Civil and Building Engineering
W Tizani (Editor)

Dynamic context-aware information access in virtual organizations

Frank Hilbert, Peter Katranuschkov & Raimar J. Scherer
Institute of Construction Informatics, Dresden University of Technology, Germany

Abstract

Virtual organisations in construction are very dynamic in their composition and operability. In this paper we describe an approach for the realisation of *context-aware access management*, mapping the required dynamic VO behaviour in an ICT environment with the help of a generic platform ontology describing the actors, resources and processes of a VO and enabling personalised context-specific user support complemented with role-based business, access and representation profiles. To demonstrate and verify the benefits of the suggested approach a set of services for *cross-organisational defect management* have been implemented. For this specific sub-area of construction the developed ontology has been extended to store metadata on defect records for tracking and corresponding media data (photos, memos, videos etc.) for the documentation of found defects. By combining the RBAC and ABAC models the developed platform ontology provides for creation of context-aware access permissions to control service access, information access and data representation using flexible access rules. Reported is research undertaken in the frames of the German BauVOGrid project performed by 3 academic and 6 industry partners (2007-2010).

Keywords: role-based information access, RBAC, ABAC, context-awareness, ontology

1 Problem statement

Construction is a project-based industry. Each construction project can be considered unique because the product, the environment, the partners and the techniques used differ heavily from one project to another. Although construction projects are executed with fixed and agreed plans, external conditions cause more dynamic changes than in other industries. In a production period of several months or even years the parties involved or the agreed product may change under various circumstances. This dynamicity necessitates flexible cooperation of the participating organisations, joining their efforts for the duration of a project into a so called virtual organisation (VO), and therefore requires an appropriate cross-company ICT solution.

Typically, information processing in a VO takes place on a virtual platform which organises the access of the VO members (subjects) to the digital information resources (objects). To ensure that the subjects receive the necessary permissions for their work on the objects, the *role-based access control model* (RBAC) has been established in the last years (Hine et al. 2000; Ferraiolo et al., 2007). This standardised access model is based on the concept of *user role* as an intermediary between subjects and permissions. Accordingly, in the initiation of a VO roles are assigned to permissions, and recorded in a VO model. These roles, which correspond to actual positions in a corporate hierarchy, are then assigned to users that later acquire the associated permissions. RBAC is thus more scalable than

identity authorisation, because authorisation information is associated with few roles rather than with many users. However, the RBAC model is purely subject-based and largely unchanging over time. The objects have no effect on the access decision and the VO model does not automatically adjusts to changing situations. Moreover, role assignments and role definitions may no longer be correct after the change of state of the entities (objects or subjects). To overcome these problems, various researchers have extended the RBAC model to *attribute-based access control models* (ABAC) to bring up context-descriptive attributes for the access decision (cf. Yuan & Tong, 2005). The focus of the developed approaches has been on environment attributes (e.g. system status, time, date), subject attributes (e.g. age, location, proofs of identity) or on object attributes, such as size, value, location, state of objects. Common to all these approaches is the idea to control the assignment of subjects to roles based on attributes while the roles-permissions assignment remains unchanged. Several methods have been investigated to determine the needed attribute values. For example, Shen (2009) uses SOAP dialogues, Koufi et al. (2009) use BPEL workflows, and Kulkarni and Tripathi (2008) suggest so-called "Context Agents" to collect context attributes. However, in most known efforts the evaluated attributes are preset and cannot be variably selected. Priebe et al. (2006) describe an attribute-based access control approach with choice of attributes but their solution is not role-based because roles are modelled only as a subject attribute.

In order to make context-sensitive authorisation decisions in dynamic VO environments that have to adapt to rapidly changing conditions, a flexible authorisation and access control system is needed. The analysed approaches do not completely fulfil these requirements. Therefore, we propose a new context-ontology-driven authorisation mechanism as described in the following sections. The presented research was done partially within the German BauVOGrid project (www.bauvogrid.de) performed by 3 academic and 6 industry partners from May, 2007 to May, 2010.

2 The concept of context-based access control

The main idea of the suggested context-based access control is to define access rights of subjects to objects not statically, but to use their properties dynamically for authorisation. The properties are modelled as attributes and, as opposed to static roles, can be interpreted at run-time. In general, we use the role-based access concept of the RBAC model and expand it to access functionality by applying ideas from the ABAC model. The overall principle is shown on high level in Figure 1 below.

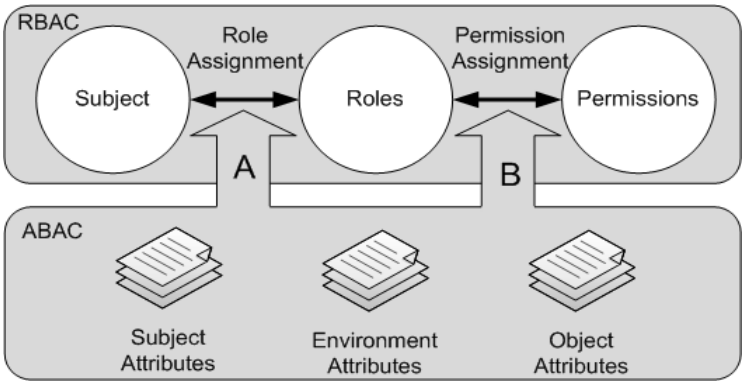

Figure 1, Extending the RBAC model with ABAC functionality

In order to handle the dynamics of virtual organisations, it is important to include the changed subject and object states in authorisation decisions. Therefore, the paramount goal of the suggested new authorisation mechanism is high flexibility. To achieve that, it is necessary to control the role and permission assignments with appropriate context attributes, so that needed variants and changes can be represented by access restrictions.

The subject-object relationship has a decisive influence on the access decision. In the hierarchical RBAC model there are various role holders on the same hierarchy level, which have different relationships with the existing objects. To ensure the "Least Privileges" paradigm, which requires that subjects should have only the permissions needed for their current tasks (cf. Ferraiolo et al., 2007), role holders may not automatically have the same privileges to the objects (see Figure 2). The relations of the subjects of the object are relevant here. Subjects should not have access to objects in which processing they are not involved. Therefore, this relationship is modelled by relational object attributes, which has influence on the role assignment. This role assignment (arrow A in Figure 1) must be attribute-dependent, because a dynamic context requires dynamic role assignments.

Furthermore, throughout its life-cycle each object can have different states with particular permissions depending on its processing states. The transitions of the objects' states can be controlled by the execution of workflows (cf. Katranuschkov et al. 2007), i.e. a role may only change an object if a workflow sets a certain attribute that grants permissions to this role. Consequently, the assignment of permissions to the roles should also not be static and must also be modelled as attribute-dependent (arrow B in Figure 1). All in all, a subject may only access an object if he/she was given a role (temporarily) and the object has a state which grants permissions to that role.

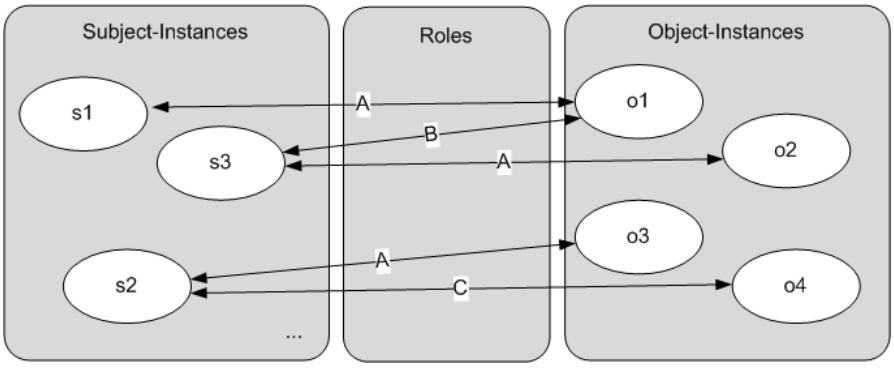

Figure 2, Subject-Object – Relationships

To provide for flexible authorisation conditions, the rules for the specific attributes of the context-based access control must be recorded in easy to change manner and a generally available format. For that purpose, a specification in standardised XML syntax provides the best choice. We opted for the eXtensible Access Control Markup Language XACML (OASIS 2005). This standard defined by the OASIS consortium serves for establishing authorisation rules that can be controlled by their evaluation of the access of subjects to objects. It is particularly suitable for describing access rules for XML objects, web services and files, which is generally suitable for a variety of different scenarios and situations. The result of an authorisation decision based on such rules is simply to accept or reject the request. The authorisation rules define which attributes are influential in assigning roles (i.e. which role is assigned to which subject) and assigning permission (i.e. who gets the right role in this situation).

An issue that requires additional consideration is the run-time performance of the developed approach. In fact, in order to provide for adequate performance, the latency for access checks has to be maximally reduced. In particular, the determination of the context attributes should take considerably less time than collecting of attributes by attribute agents as proposed in (Kulkarni & Tripathi, 2008) or the use of BPEL workflows as proposed in (Koufi et al., 2009). We achieve that with the help of an appropriately configured *platform ontology*. Low latency for the access checks and flexible rule-making are thereby ensured by storing the contextual information of the participating entities in an ontological knowledge base. This information includes the subject, object and environment attributes as well as relational attributes that describe the direct and transitive relations of the entities. Moreover, by using RDF (the Resource Description Framework) and RDF Schema (W3C 2004b, c) wider se-

mantic context can be established which allows definition of all entities (subjects or objects) with their properties and relationships. This, ontology-based approach has several advantages. Firstly, the ontologies know the context attributes directly and do not have to identify them in a time-consuming procedure. Secondly, through an integrated ontology reasoner the required role for a transaction can be determined very quickly. Thirdly, additional transitive rules can be easily defined (e.g. if a subject has write permission, then it automatically also has read permission). Thus, all requests can be evaluated with this authorisation mechanism in real time.

3 Realisation

Realisation and verification of the developed concept of context-based access control is done in the frames of the BauVOGrid project, which aims at developing an extensible and reusable community solution that will improve VO collaboration in construction. To narrow development scope and facilitate achievement of short-term practical results, the focus of the first BauVOGrid pilot application has been put on *defect management*, a significant cost factor in the late construction phases as well as in facilities management.

For the specific goals of BauVOGrid we have created the ontological knowledge base for virtual organisations using two different, yet inter-related ontologies. These are: (1) a *VO Ontology*, describing the structure of the virtual organisation, and specifically which partner takes which potential roles, and (2) a *Defect Ontology*, describing the actual resource objects (defects and related building elements and media data) and the relations of subjects to objects (Gehre et al. 2006). At the time of this writing, a central defect and media management platform has been implemented that combines, in terms of access rights, several object models with one subject model. This platform assists the members of a VO in dealing with various construction and/or operation defects. Actual construction defects at the site are thereby mapped to a digital virtual defect record and forwarded to the local defect management systems of the corresponding VO partner. To provide for the availability of the distributed and heterogeneous defect information both in the office and mobile on site, a uniform defect exchange format based on a harmonised XML schema was developed. Further media information, such as defect photos, videos and voice memos can be additionally attached to the defect information. To warrant the relationship that a subject has an object, in this case a defect record, the subject has also to be linked to the attached media data.

The overall system is implemented as a SOA environment. The users first authenticate themselves via a web portal, before making a SOAP request to the central defect management platform and get permission to perform various actions. We start with a sessionless communication between user and web service, which will recalculate attribute values after each request. When a request is sent, the system evaluates the data using the appropriate access control policy and decides whether the request can be accepted. However, in order to derive properties, relations and conditions between the entities and related information for the access decision, fully structured context information and information, how the entities interact with each other is necessary. The concept of ontologies and reasoning supported by logical inference are particularly well suited for the automatic extraction of such implicitly available data. In the practical implementation we use Jena, an open source Java framework for the development of semantic applications. It provides RDF (W3C 2005) and OWL (W3C 2004a) APIs as well as a SPARQL query engine for requests (OASIS 2005). With Jena, the defect records are XML documents represented ass graph nodes in RDF, the description language implemented for resources and saved as an instance of the Object ontology. The entities, the roles and permissions are also nodes, and their relations are interpreted as the edges of the RDF graph. Using the RDF-based query language SPARQL semantic queries can be made on this graph to evaluate the attributes.

Access control is realised via a dedicated *access web service.* Its principal functionality is shown on the below Figure 3. It uses SPARQL to collect subject and object context attributes that have influence on the access decision, which is also guided by the defined access policies. For that purpose, at

first the role with the respective privileges is selected. If this role is found in the subject's attributes (as initialised in the VO model), evaluation of the object attributes is done. After that, the relationship between the subject and the object and the state of the object are determined. Only if these attributes fit the respective access policy, the requested access is granted.

Permissions are categorised as "*create*", "*read_parts*", "*read_all*", "*write_all*", "*write_parts*", "*append*" and "*search*". Each permission is understood as authorisation to execute a specific method of the addressed web service. However, it is important to mention that the subjects are not allowed to have rights with which they can change access right assertions in the ontology.

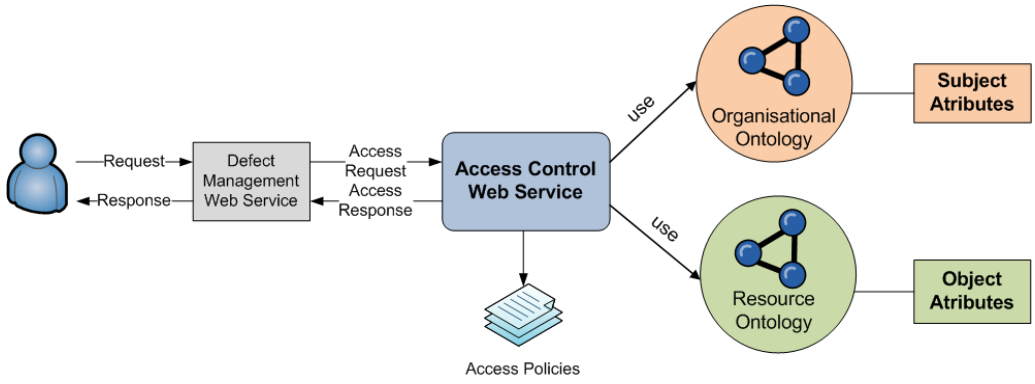

Figure 3, Access Control Web Service

At this stage of work, the SPARQL query interface to the VO ontology is already implemented. Permission assignment to roles is done by hand using a static Java GUI client. For the implementation, we use an Apache 2.2 Web server, a Tomcat server 6.0 with Axis 1.1 and the Jena Framework 1.3 which saves the instances of ontology models in a MySQL 5.0 database for persistence. Development of XACML policies in SPARQL queries and the automated evaluation of requests are in progress.

The prototype of the VO defect management platform was tested with fully satisfying results in the hand-over phase of the new football stadium "Rudolf Harbig" in Dresden. In the applied scenario, defects are collected by means of a mobile client with RFID support and then transferred to the central defect management platform for further processing.

4 Conclusions

In this paper, the objective of context-sensitive access control systems for virtual organisations in construction was defined and the associated problems that had to be solved were presented. The main challenge was that current access control models are primarily static whereas VOs in construction are inherently dynamic. Therefore adapting the access control model to the specific VO requirements in a novel approach was seen necessary. Central issues of our developed approach are (1) the definition of context-sensitive access management using the subject and object attributes for dynamic role and role-permission assignments, and (2) the use and extension of the ontology of the application domain in the context of role-permission assignment, as a vehicle to exchange contextual attributes precisely between the VO parties and between humans and computers. Real-practice tests in the frames of the BauVOGrid project verified applicability. Further work will concern the automatic generation of XSLT patterns for fine-grained access control and the definition of pre-defined rules and profiles.

Acknowledgements

The presented research is partially funded by the German Ministry of Education and Research (BMBF). This support is gratefully acknowledged.

References

FERRAIOLO, D., KUHN, D. R., CHANDRAMOULI, R., 2007. *Role-based access control* (2nd ed.), Artech House Information Security and Privacy Series, Boston, 381 p.

GEHRE, A., KATRANUSCHKOV, P., SCHERER, R. J., 2006. Management and integration of virtual enterprise information on grid spaces through semantic web ontologies, in: MARTINEZ, M., SCHERER, R. J. (eds.): *eWork and eBusiness in Architecture, Engineering and Construction*, Proc. of the 6th ECPPM, Taylor & Francis Group, London, UK, pp. 255-266.

HINE, J. H., YAO, W., BACON, J., MOODY, K., 2000. An architecture for distributed OASIS services, *Proc. Middleware 2000*, LNCS 1795, Springer-Verlag, Heidelberg - New York, pp. 107-123.

KATRANUSCHKOV, P., SCHERER, R. J., 2009. BauVOGrid: a grid-based platform for the virtual organisation in construction, in: ZARLI A., SCHERER R. J. (eds.): *Proc. ECPPM 2008 – the 7th **E**uropean Conference on Product and Process Modelling*, 10-12 Sept. 2008, Sophia Antipolis, France, CRC Press/Balkema, pp. 339-347.

KATRANUSCHKOV, P., GEHRE, A., SCHERER, R. J., 2007. Reusable Process Patterns for Collaborative Work Environments, in: PAWAR K. W., THOBEN K.-D. & PALLOT M. (eds.): *ICE 2007 - Proceedings of the 13th International Conference on Concurrent Enterprising*, Centre of Concurrent Enterprising, Nottingham, UK, pp. 87-96.

KOUFI, V., MALAMATENIOU, F., VASSILACOPOULOS, G., 2009. A mediation framework for the implementation of context-aware access control in pervasive grid-based healthcare systems, in: *Proc. 4th Int. Conf. on Advances in Grid and Pervasive Computing,* Springer-Verlag, Berlin - Heidelberg, pp. 281-292.

KULKARNI, D., TRIPATHI, A., 2008. Context-aware role-based access control in pervasive computing systems, in: *Proc. 13th ACM symposium on access control models and technologies*, ACM: Estes Park, CO, USA. pp. 113-122.

OASIS 2005. *eXtensible Access Control Markup Language (XACML)*,
Available online at: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

PRIEBE, T., DOBMEIER, W., KAMPRATH, N., 2006. Supporting attribute-based access control with ontologies, in: *Proc. 1st Int. Conf. on Availability, Reliability and Security* (ARES 2006), IEEE Computer Society Press, Los Alamitos, pp. 465–472.

SHEN, H. B., 2009. A semantic-aware attribute-based access control model for web services, in: HUA, A., CHANG, S.-L. (eds.): *Algorithms and Architectures for Parallel Processing* (Proc. 9th Int. Conf. ICA3PP 2009. Taipei, Taiwan, Proceedings: 5574 (Lecture Notes in Computer Science), Springer-Verlag, Berlin, pp. 693-703.

W3C 2004. *OWL Web Ontology Language Reference*. W3C Recommendation, 10.02.2004,
Available online at: http://www.w3.org/2004/OWL/

W3C 2004b. *Resource Description Framework (RDF). Concepts and Abstract Syntax.* (c) World Wide Web Consortium, February 2004. Available online at: http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/

W3C 2004c. *RDF Vocabulary Description Language 1.0: RDF Schema*. (c) World Wide Web Consortium, February 2004,
Available online at: http://www.w3.org/TR/2004/REC-rdf-schema-20040210/

W3C 2005 *SPARQL Query Language for RDF*. World Wide Web Consortium, February 2005,
Available online at: http://www.w3.org/TR/2005/WD-rdf-sparql-query-20050217/

YUAN, E., TONG, J, 2005. Attribute Based Access Control (ABAC) for Web Services. In: *Proc. of the IEEE Int. Conf. on Web Services* (ICWS 2005), July 11-15, 2005, Orlando, Fl., IEEE Computer Society Press, Los Alamitos, pp. 561–569.