



An Annotation-based Access Control Model and Tools for Collaborative Information Spaces

Title	An Annotation-based Access Control Model and Tools for Collaborative Information Spaces
Author(s)	Nasirifard, Peyman;Peristeras, Vassilios;Decker, Stefan
Publication Date	2008

An Annotation-Based Access Control Model and Tools for Collaborative Information Spaces

Peyman Nasirifard, Vassilios Peristeras and Stefan Decker

Digital Enterprise Research Institute, National University of Ireland, Galway, IDA Business Park, Lower Dangan, Galway, Ireland
firstname.lastname@deri.org

Abstract. We present an Annotation-Based Access Control model supported by a Collaboration Vocabulary (CoVoc) as a more flexible and user-centric access control approach in social platforms and shared workspaces. We present also briefly two SOA-based tools for enabling our approach: Uncle-Share is a gadget that provides annotation-based access control for bookmarks and uses CoVoc for annotating collaborative relationships. Who-With-Whom uses also CoVoc and visualizes extended social networks in order to help users to select the appropriate contacts to grant access to resources.

Keywords: Annotation, Access Control, Social Computing, Collaboration Vocabulary

1 Introduction and Overview

In our real-life, we share the resources we own based on social acquaintances or credits that we give to people, with whom we communicate. As an example, we may share the keys of our apartments with our parents, but not with our friends, as we give more credits to our parents rather than friends. Access Control emerges almost together with the concept of sharing. In brief, Access Control defines Who can access What [1].

“Sharing” is a key concept for collaborative information spaces like Web 2.0 platforms (e.g. Flickr, YouTube, del.icio.us) and/or Collaborative Work Environments (CWE). These platforms and applications provide the infrastructure and services for different types of users to collaborate together and share resources which may vary from songs and photos to documents and calendars. In these Web-based environments of massive-scale sharing, access control takes interesting characteristics as poses additional requirements.

Our analysis and also some other works like [2] show that current access control mechanism within Web 2.0 platforms and shared workspaces suffer from fine-granularity. As an example, users are able to share a resource with some colleagues, but additional restrictions such as temporal, spatial, etc. can not be expressed. This shortcoming undermines the utility of shared workspaces and brings privacy-related issues in Web 2.0 platforms.

In this paper, we propose an annotation-based model to address access control requirements in social and collaborative platforms and implement our approach using Semantic Web [3] technologies (e.g. RDF) and social computing (annotations, social networks analysis, gadgets), two prominent paradigms in Web-based information systems development. More specifically, we present here:

- A model for access control which is applicable both in Web 2.0 platforms and shared workspaces.
- A vocabulary for annotating collaborative relationships amongst people.
- Software tools that implement this approach.

2 Background and Related Work

There are many different approaches and mechanisms for controlling access, e.g. role-based access control (RBAC) [4, 5], attribute-based access control [6], etc. Each approach has its own advantages, disadvantages and feasibility scope. Some researchers have tried to combine different access control mechanisms to build more powerful models.

The study of access control mechanisms in Cooperative Systems is not new and was in existence since the birth of e-Collaboration tools in 1980s. Shen et al. [7] studied access control mechanisms in a simple collaborative environment, i.e. a simple collaborative text editing environment. Zhao [8] provides an overview and comparison of three main access control mechanisms in collaborative environments. Tolone et al. [9] have published a comprehensive study on access control mechanisms in collaborative systems and compare different mechanisms based on multiple criteria, e.g. complexity, understandability, ease of use. Jaeger et al. [10] present basic requirements for role-based access control within collaborative systems. Gutierrez Vela et al. [11] try to model an organization in a formal way that considers the necessary elements to represent the authorization and access control policies. Kern et al. [12] provide an architecture for role-based access control to use different rules to extract dynamic roles. Alotaiby et al. [13] present a team-based access control which is built upon role-based access control. Periorellis et al. [14] introduce another extension to role-based access control which is called task-based access control. They discuss task-based access control as a mechanism for dynamic virtual organisation scenarios. Toninelli et al. [15] present an approach towards combining rule-based and ontology-based policies in pervasive environments. Demchenko et al. [16] propose an access control model and mechanism for grid-based collaborative applications. Massa et al. [17] use the dataset from Epinions.com to do computational experiments on employing global versus local trust metrics. They study the implications of controversial users in product rating community.

Social networks and their analysis have lots of potential in various domains, from learning [18] to knowledge management [19] and access control [20]. Social computing (the use of wikis, blogs, networking sites, collaborative filtering, and so on) helped to the birth of a new broad phase in knowledge management [21, 22]. In [23] a theoretical notion of virtual community is developed that is based on the idea of dynamic, self-organizing social systems. [24] investigates some studies of the concept

of social networks through several different areas of interests, including the World Wide Web and human and biological sciences in the economic arena. [25] discuss also the economic impact of social networks by studying a test bed from Google Answers, a fee-based knowledge market which was fully closed by late December 2006.

In the area of social acquaintances between people, various vocabularies have been proposed so far, like RELATIONSHIP [26] and REL-X [27]. We have used some concepts from RELATIONSHIP in our work however, these vocabularies have been mainly developed to be of general purpose and do not capture the specific relationships that exist in a collaborative working environment.

3 Annotation-Based Access Control

Annotation is a common mechanism which is used nowadays by social platforms for annotating shared informational resources and is based on mechanisms that allow users to describe resources with “tags”. In this way, users are allowed to attach metadata in commonly shared resources (social tagging). These tags later facilitate browsing and discovery of relevant resources. Annotation and tags are important mechanisms of what has been called Web 2.0 or Social Web.

Our access control model is based on annotations, too. End users are able to annotate their contacts (social network) and define policies for granting access to their resources based on these annotations. In this context, only those contacts that fulfill the required policies get access to specific resources. Annotation-based access control is very close to how we share resources in our real-life. We may share our credit card details with our parents, but not with our friends. Based on this simple scenario, in annotation-based access control, both our parents and friends are parts of our social network, but our parents have been tagged as *parent* and our friends have been tagged as *friend* and our credit card details are resources with a policy to be shared only with *parent*.

Our current access control model composes of three main entities and two main concepts: *Person*, *Resource*, and *Policy* are the three entities; *Annotation* and *Distance* are the two main concepts. A Person is an entity with the RDF type *Person*. A Person is connected to zero or more other Persons. A Person owns zero or more Resources. A Person defines zero or more Policies. An Annotation is a term or a set of terms that are connected together and aims to describe the Person. Each connection between Persons can be annotated with zero or more Annotations. A Resource is an entity with the RDF type *Resource* and is owned by (isOwnedBy) one or more Persons. Resources are in the form of URIs and/or short messages. A Resource can be either private or public. A private Resource has zero or more Policies, whereas a public resource has one or more Policies. A Policy is an entity with the RDF type *Policy*. A Policy is defined by (isDefinedBy) one Person and belongs to (belongsTo) one Resource. A Policy has one Annotation and one Distance. Again an Annotation is a term or a set of terms that are connected together and aims to describe the Person that the Resource should be shared with. A Distance is a numerical value which

determines the *depth* that the Policy is valid. The depth is actually the shortest path among two Persons with consideration of Annotations.

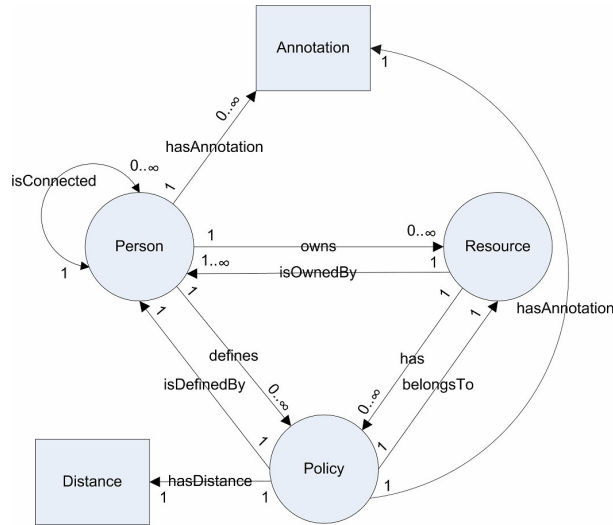


Fig. 1. Main elements in access control mechanism and their relationships

Fig. 1 demonstrates the elements and relationships of our access control model. The model becomes clearer with the use case scenario in the next part.

A Person acquires access to a Resource, if and only if (iff) s/he meets *all* policies that have been defined by Resource owner for that Resource. It means that the Person has been already annotated with the Annotations which are already defined in Policies and s/he is also in the scope of the Policies (i.e. Distance criteria).

3.1 Use Case Scenario

In order to clarify the concepts and make our model more understandable, we present a simple scenario. In our scenario, we have four users: Alice, Bob, Mary, and Tom. They perform the following actions:

Alice adds Bob to her contacts and annotates him with *collaborateWith* and *doResearchWith*. Alice adds also Mary to her contacts and annotates her as *director*. Alice owns three resources: *www.resource1.com*, *www.resource2.com* and *I_need_to_talk_to_you_please*. The latter resource is actually a short message but still remains a resource owned by Alice. Alice defines the following three policies:

- *policy1: collaborateWith:1 and doResearchWith:1 for www.resource1.com;*
- *policy2: collaborateWith:2 and doResearchWith:2 for www.resource2.com;*
- *policy3: director:1 for I_need_to_talk_to_you_please resource.*

The numerical value which comes in policies after the annotation is the distance, i.e. the depth that the policy will be valid.

Bob adds Tom to his contacts and annotates him as *collaborateWith* and *doResearchWith*. He also adds Alice and annotates her as *student*. Bob owns also two resources: *www.resource4.com* and *www.resource5.com*. He defines the following policies for his resources:

- *policy4: collaborateWith:1 and doResearchWith:1 for www.resource4.com;*
- *policy5: student:1 for www.resource5.com.*

Tom and Mary do not add any contacts or resources.

In this case, we have granted access to the followings persons/resources.

- Alice has access to her three resources and *www.resource5.com* via Bob, because *www.resource5.com* is accessible to the Bob's contacts that have been annotated as *student* and have maximum distance one to Bob and Alice fulfils this policy (see *policy5*).
- Bob has access to his two resources and also two of Alice's resources: *www.resource1.com* (see *policy1*) and *www.resource2.com* (see *policy2*).
- Tom has access to *www.resource4.com* which was shared via Bob to him (see *policy4*) and also *www.resource2.com* which was shared via Alice to him (see *policy2*).
- Mary will see the short message from Alice: *I_need_to_talk_to_you_please* (see *policy3*).

4 CoVoc: Suggesting Social Annotations

For annotating people and also defining policies, we like to create a tool to recommend/suggest terms to the users. These suggestions should come from a vocabulary. We developed the Collaboration Vocabulary (CoVoc) for this purpose.

In brief, CoVoc is a set of terms that covers various collaborative relationships and social acquaintances that exist between individuals (collaborative users) in a collaborative environment. For developing CoVoc we studied more than forty ontologies from SchemaWeb¹, as they appear relevant to collaboration. We also looked at detailed Curriculum Vitae (CV) of around thirty researchers, Ph.D. and M.Sc. students to determine what they perform together with other people in their professional (research) lives. The researchers came from different computer science areas.

The terms included in the current version of CoVoc follow on two broad categories:

- Terms which are directly related to relationships between persons. These are terms that describe actual relationships between two persons that collaborate (e.g. *writeDocumentWith*).
- Terms which are related to personal characteristics that acquire interest for the users in a collaborative context (e.g. *supervisor*). In other words, these

¹ <http://www.schemaweb.info/>

are attributes of the entities that somehow influence the relationship of the entity with other external entities.

This latter category ideally should not be part of a Collaboration Vocabulary, as it covers personal characteristics that exist at the user profile and not at the relationship layer. These characteristics should have been stored and thus become available through formal user profiles (e.g. FOAF extensions that cover additional collaboration-related personal characteristics). But due to the lack of such profiles, we have included these terms in CoVoc in order to allow users to annotate their relationships using them. We developed a RDF Schema for CoVoc. Due to the space limitation, we do not present the details here. The CoVoc terms and its schema are accessible online².

5 Tools and Implementation Issues

To enable and evaluate the above access control model, we have developed some tools that are presented in this part. Both tools (Uncle-Share and Who-With-Whom) and their documentation are accessible online².

5.1 Uncle-Share: Annotation-Based Access Control Tool

To enable annotation-based access control, we have developed Uncle-Share. Uncle-Share has been developed as a gadget. Having this application as a gadget enables end users to use Uncle-Share together with other applications something that increases the tool's usability, as users don't have to launch a new application or browse a new Web page to utilize Uncle-Share. In particular, we decided to use iGoogle for developing our gadget, as Google provides sufficient documentation and support for developing gadgets; however, our gadget can be embedded into any other widget/gadget platform or Web site. The only client-side requirement is that the browser should support JavaScript. The tool fully supports scenarios like the one described in previous sections and successfully executes all the policies defined there. Figure 2 demonstrates the embedded Uncle-Share within iGoogle and BSCW shared workspace.

We have developed Uncle-Share as a Service-Oriented Architecture (SOA) application. All functionalities of Uncle-Share (registration, changing password, adding persons and resources, fetching shared resources, etc.) are wrapped as services. This approach enables developers to utilize all Uncle-Share's functionalities within their own separate applications, ensuring reusability and interoperability with various platforms.

We used Sesame³ 2.0 as RDF repository to store the generated RDF triples. The SOA backbone is based on Apache CXF⁴ which eases the development of Web services. For building the AJAX-based gadget, we used Google Web Toolkit⁵.

² <http://purl.oclc.org/projects/phd>

³ <http://www.openrdf.org/>

⁴ <http://incubator.apache.org/cxf/>

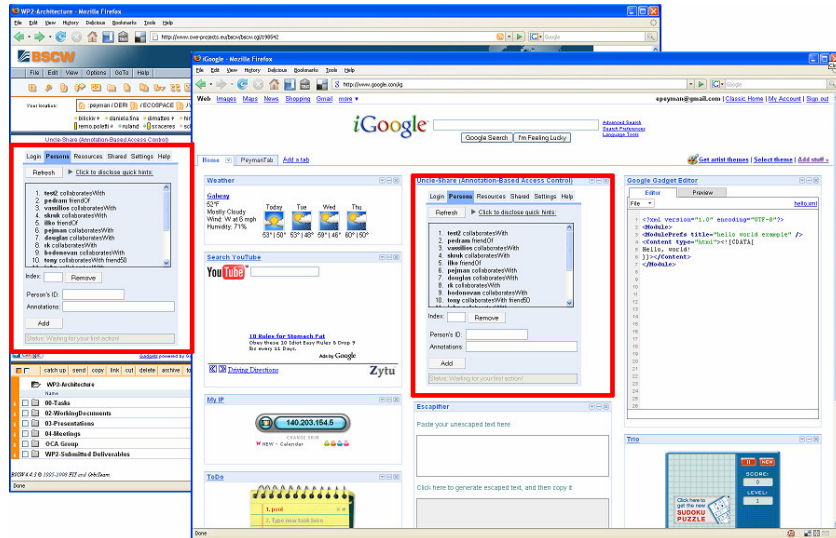


Fig. 2. Embedding Uncle-Share into iGoogle and BSCW shared workspace

5.2 Who-With-Whom: Visualizing Social Networks

Who-With-Whom is a simple prototype that visualizes the annotated social networks based on CoVoc terms. The visualization is a means that helps users to choose/come up with the appropriate persons that should be granted access to resources. We used *Graph Gear*⁶ for visualizing the graphs which is based on Adobe Flash. Who-With-Whom uses Sesame RDF store as input. It fetches the RDF triples that are related to a specific CoVoc term and transforms them into the appropriate input which feeds Graph Gear. If the users' photos were already stored in the repository, it will be shown in the graph as well. Figure 3 demonstrates a snapshot of Who-With-Whom.

6 Discussions and Comparisons

The main difference between RBAC [4, 5] and our approach is that in RBAC, the roles are already defined by a role engineer, but in our approach, we have decentralized concepts (i.e. annotations) which are not necessary roles (from the semantics point of view). It is the user that defines his/her own annotations and assigns them to his/her contacts which is more user-centric. From the RBAC perspective, our model can be seen as an extension to RBAC through assigning user-

⁵ <http://code.google.com/webtoolkit/>

⁶ <http://www.creativesynthesis.net/blog/projects/graph-gear/>

centric roles (i.e. annotations) to a person's contacts. The other main difference is the concept of Distance which increases or decreases the scope of policies in sharing resources, as the people are connected together in a graph-like manner (rather than hierarchy-like manner). Where RBAC can be very useful in large and well-structured organizations, our approach fits well for defining access control policies for personal data.

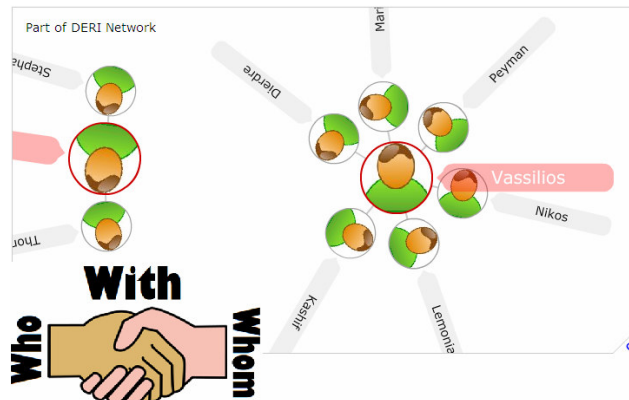


Fig. 3. A snapshot of Who-With-Whom

In our model, all relationships are private, as there is no need to publicly announce the relationships between people. End users can freely publish their own relationships, if this is needed. While fixed vocabulary are used in approaches like [28], in our model and tools, fixed terms are just suggested to end users, as we do not really force users to exclusively use them. They are allowed to use their own terms as well as fixed terms for annotations. This open vocabulary approach enables end users to express the trust level in a more natural way as well. As an example, instead of using percentage for expressing the trust level (e.g. *friend 80%*) like in [20], end users can express degrees of friendship in a more natural way with an annotation like *closeFriendOf*. The model becomes in this way more realistic, as we don't really label our friends in real-life with numerical values. Moreover, we calculate the distance between two persons taking into account the annotation value. For example, if person A is connected to person B and this connection has the annotation *student*, the distance from person A to B (directional) with the consideration of *student* is one. The distance from person A to B (directional) with the consideration of any other annotations (e.g. *friendOf*) is infinity. The distance from person B to A (directional) is also infinity, because person B has no outgoing link to person A.

7 Conclusion and Future Work

In this paper, we presented an annotation-based access control model, a vocabulary for annotating collaborative users and tools to define and visualize access policies for

information resources we own. This approach is applicable in multiple Web-based collaborative information spaces like Web 2.0 social platforms (e.g. Flickr, YouTube, del.icio.us) and/or Collaborative Work Environments (CWE). Our model can be seen as an extension of role-based access control, where people are able to define their own roles and assign them to others in a user-centric model.

We plan to extend our work in several directions: The current access control model that we propose here is not context-aware as it lacks context characteristics. We want to extend the model in order to include context information. For this, we plan to build a simple mashup to fetch context information of users from their Micro-blogs like Twitter . This can be done via defining a fixed set of terms for context or via natural language processing.

Another interesting extension is to use Open Social API to embed the tools into social networking sites like MySpace and Orkut. Open Social follows the idea of *Write once, run anywhere* and enables developers to develop cross-platform applications among social Web sites.

More advanced user models, suggestions/recommendations for access policies, and access policy prioritization are additional possible future improvements.

Acknowledgements

This work is partially supported by the Ecospace project: FP6-IST-5-35208 and the Lion project supported by Science Foundation Ireland under Grant No. SFI/02/CE1/I131.

References

1. Russell, D., Gangemi, Sr.G.T.: Computer Security Basics. 1991: O'Reilly and Associates.
2. Hart, M., Johnson, R. and Stent, A.: More Content - Less Control: Access Control in the Web 2.0. in Web 2.0 security and privacy issues, IEEE Symposium on Security and Privacy. 2007.
3. Berners-Lee, T., Hendler, J., Lassila, O.: The Semantic Web, A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. Scientific American, 2001.
4. Ferraiolo, D.F., Kuhn, D.R.: Role Based Access Control. in 15th National Computer Security Conference. 1992.
5. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer, 1996. 29(2): p. 38-47.
6. Kolter, J., Schillinger, R., Pernul, G.: A Privacy-Enhanced Attribute-Based Access Control System. in DBSec. 2007: Springer.
7. Shen, H., Dewan, P.: Access Control for Collaborative Environments. in Computer-Supported Cooperative Work Conference. 1992: ACM Press.
8. Zhao, B.: Collaborative Access Control, in Seminar on Network Security. 2001.
9. Tolone, W., Ahn, G., Pai, T., Hong, S.: Access control in collaborative systems. ACM Computing Surveys, 2005. 37: p. 29-41.
10. Jaeger, T., Prakash, A.: Requirements of role-based access control for collaborative systems, in 1st ACM Workshop on Role-based access control. 1996: ACM Press.

11. Gutierrez Vela, F.L., Isla Montes, J.L., Paderewski, P., Sanchez, M.: Organization Modelling to Support Access Control for Collaborative Systems, in *Software Engineering Research and Practice*. 2006.
12. Kern, A., Walhorn, C.: Rule support for role-based access control, in *10th ACM symposium on Access Control Models and Technologies*. 2005: ACM Press.
13. Alotaiby, F.T., Chen, J.X.: A Model for Team-based Access Control, in *International Conference on Information Technology: Coding and Computing*. 2004: IEEE Computer Society.
14. Periorellis, P., Parastatidis, S.: Task-Based Access Control for Virtual Organizations, in *Scientific Engineering of Distributed Java Applications*. 2005.
15. Toninelli, A., Bradshaw, J., Kagal, L., Montanari, R.: Rule-based and Ontology-based Policies: Toward a Hybrid Approach to Control Agents in Pervasive Environments, in *Semantic Web and Policy Workshop*. 2005.
16. Demchenko, Y., Gommans, L., Tokmakoff, A., van Buuren, R.: Policy Based Access Control in Dynamic Grid-based Collaborative Environment, in *International Symposium on Collaborative Technologies and Systems*. 2006: IEEE Computer Society.
17. Massa, P., Avesani, P.: Trust Metrics on Controversial Users: Balancing Between Tyranny of the Majority and Echo Chambers. *International Journal on Semantic Web & Information Systems*, 2007. 3(1): p. 39-64.
18. Hoogenboom, T., Kloos, M., Bouman, W., Jansen, R.: Sociality and learning in social software. *International Journal of Knowledge and Learning*, 2007. 3(4/5): p. 501-514.
19. Chatti, M.A., Jarke, M., Frosch-Wilke, D.: The future of e-learning: a shift to knowledge networking and social software. *International Journal of Knowledge and Learning*, 2007. 3(4/5): p. 404-420.
20. Kruk, S.R., Grzonkowski, S., Gzella, A., Woroniecki, T. and Choi, H.C.: D-FOAF: Distributed Identity Management with Access Rights Delegation, in *Asian Semantic Web Conference*. 2006.
21. Liu, H., Maes, P.: Introduction to the Semantics of People & Culture. *International Journal on Semantic Web and Information Systems*, Special Issue on Semantics of People and Culture, 2007. 3(1): p. i-ix.
22. Davies, J., Lytras, M., Sheth, A.P.: Guest Editors' Introduction: Semantic-Web-Based Knowledge Management. *IEEE Internet Computing*, 2007. 11(5): p. 14-16.
23. Fuchs, C.: Towards a dynamic theory of virtual communities. *International Journal of Knowledge and Learning*, 2007. 3(4/5): p. 372-403.
24. Ehrlich, D.M.: Social network survey paper. *International Journal of Learning and Intellectual Capital*, 2006. 3(2): p. 167-177.
25. Rafaeli, S., Raban, D.R., Ravid, G.: How social motivation enhances economic activity and incentives in the Google Answers knowledge sharing market. *International Journal of Knowledge and Learning*, 2007. 3(1): p. 1-11.
26. Davis, I., Vitiello Jr, E.: RELATIONSHIP: A vocabulary for describing relationships between people. 2005. [Available from: <http://vocab.org/relationship/>]
27. Carminati, B., Ferrari, E., Perego, A.: The REL-X vocabulary. *OWL Vocabulary*. 2006. [Available from: <http://www.dicom.uninsubria.it/~andrea.perego/vocs/relx.owl>]
28. Carminati, B., Ferrari, E., Perego, A.: Private Relationships in Social Networks, in *ICDE Workshops*. 2007.