

Leveraging Access Control in CSCW based on User-Defined and Hidden Semantic Social Networks

Position Paper

Peyman Nasirifard, Vassilios Peristeras

Digital Enterprise Research Institute
National University of Ireland, Galway
firstname.lastname@deri.org

1 Motivation

In our offline life, we share the resources that we own based on social acquaintances or credits that we give to people with whom we communicate. These resources may vary from books to the key of our apartment and the people that we communicate vary from our parents to some friends of our friends. Internet provided the required infrastructure and technologies for a better Computer Supported Co-operative Work (CSCW) by means of online shared workspaces, where a group of users are able to share documents, presentations, events, calendars etc. in most cases by using an online user interface. However the nature of online resources is different from offline ones, but obviously there should exist an access rights management to restrict unauthorized accesses to them.

2 Shortcomings of the Current Solutions and Requirements

To address these issues (authorizations) of shared workspaces, different approaches and mechanisms have been introduced so far. Most current shared workspaces provide a role-based coarse-grained access rights management which in most cases does not meet users' requirements. As an example, users are able to share a resource with some colleagues, but the required conditions (like for a specific time, or with a specific context) can not be expressed. In other words most current mechanisms provide a Boolean-based access rights management which is not parametric and does not accept pre-conditions and post-conditions. To overcome these problems *partially*, most users do email the confidential stuff to each other which offers a huge overload and perhaps versioning problems that brings the functionalities of shared workspaces under question.

To explore the requirements, suppose following access control scenarios that make sense within shared workspaces (Bob is the name of main actor):

- Bob wants to give access of a work-in-progress document to all supervisors plus director of an organization and if some of them are not available (e.g. on vacation), to their proxies.
- Bob wants to give access of a confidential contract only *once*
- Bob wants to give access of a particular presentation only during the meeting and only to meeting participants.

- Bob wants to give access of a particular background document only to members of shared workspace that are currently working on a particular document and they have already read a background document.
- Bob wants to share a photo only to his close friends (or his colleagues from his company)
- Bob's friends can access his birthday photos, only for one week after his birth date.
- Bob does not want to give access of a document to friends that were not present in a particular meeting and their trust levels are less than a threshold.

To generalize these requirements, we can say that "user wants to give access the X of Y to Z with condition W". In above formula, the variable X is whatever that has meaning in relation to accessing the Y and the variable Y is the sharable resource, e.g. read access of a document. The variable Z is the user (or group of users, application or whatever) that can get access and the variable W is the conditions (roles, context, time, location, etc). If we replace above variables with suitable instances, we can build a meaningful set of user requirements, for example: "user wants to give *delete access of document1* to *whomever* that is *administrator and only during 10-12am of Mondays*). The above general sentence can be more fine-grained indeed.

3 Access Control based on Social Network Analysis

Taking into the account above simple scenarios, one key candidate towards building a more flexible, parametric, extensible, and fine-grained access rights management is benefiting from social networks, like we do in our offline world for sharing offline resources. This kind of access control based on social networks can be analysed from two complementary approaches:

One part of social network can be defined by users based on a close set of vocabularies that defines relationships, e.g. supervisor, teacher, student, coordinator, co-worker, etc. or an open set of vocabularies that can be utilized for naming relationships. Semantic Web technologies and ontologies are good candidates to store and handle these vocabularies.

The other part of social network is hidden, but can be extracted by mining and analyzing the behaviour of users, when they communicate or collaborate within shared workspaces. In other words, this kind of social network can be extracted and analysed from the fingerprints that the users leave when they collaborate and can be exported as log files from most shared workspaces. Some examples follow:

- If two users are working on the same document, the hidden bi-directional relationship between them is "co-authoring".
- If user A is reading a document that has been written by user B, the hidden relationship is "ReadWrite" from user A to user B and "WriteRead" from user B to A.
- If user A, user B and user C are participating in an event, the hidden relationship between these three persons can be expressed as "Participate" or "EventParticipate".

There is no doubt that social networks should be enriched with context information of users and perhaps the trust level that a user assigns to his contacts. The whole infrastructure can be enriched with Semantic technologies for machine-understandability.

The other moot point is the fact that the analysis of characteristics of social networks based on different criteria brings some interesting results and can be used within access control mechanisms. In other words, one of the main goals of analysis of (hidden) social networks is giving the opportunity to the users to select the appropriate candidates among other users for sharing a resource. In an organization with more than fifty thousands employees, where users are not able to recognize authorized persons for sharing resources, this analysis will come into the account for proposing some appropriate candidates. For example, user A wants to share a resource only to those members in the community that have the most *in-degree* or located in the *center* of some clusters within social network. Note that these concepts, like being in the *center* of a community, should be well-defined. For example, in an organisation, the secretary or director can be the persons with the most in-degree.

4 Conclusion

Social networks are great means to provide the required infrastructure for a more fine-grained access rights managements, as they represent the model that we use in our real life for sharing resources. The other key players are Semantic Web technologies and context providers which feed the infrastructure. Currently, we are working at DERI Galway towards this direction to provide an open infrastructure for access control mechanism for shared workspaces based on semantic social networks and analysis of hidden social networks.