SemID: Combining Semantics with Identity Management

Mohammad M. R. Chowdhury[1], Juan Miguel Gomez[2], Josef Noll[1] and Angel García Crespo[2]
[1]*UniK-University Graduate Center, Kjeller, Norway.*
[2]*Departamento de Informática, Escuela Politécnica Superior, Universidad Carlos III de Madrid, Madrid, Spain.*
[1]*{mohammad},{ josef}@unik.no;* [2]*{juanmiguel.gomez}@uc3m.es*

Abstract

The need for information security and privacy in today's connected systems is overwhelming. In this paper, we focus on the identity management in corporate environment to access various project resources. Capabilities of semantic web technology are utilized in the proposed SemID ontology for formal representation of identity management domain. Proposed ontology contains roles, policies and rules to control access to resources and to ensure privacy. A use case scenario is modeled using Protègè ontology editor platform.

1. Introduction

To protect sensitive information that is often contained in today's connected systems; there is an increased need for adequate security and privacy support. Identity management in distributed and dynamic systems is crucial for secure service access. We believe that capabilities of semantic technology can contribute to provide solutions to these problems. This paper is expected to handle the identity management and privacy issues in corporate social network. To provide these services, we have formulated policies and rules to control access to resources owned by a group or community. These information need to be encoded in ways to facilitate understanding and manipulation by computer programs. This encoding is achieved through the specification and utilization of ontologies – formal representation of a domain. Using semantic technology, we propose SemID (semantic identity) ontology to handle the growing need of identity management and privacy supports in corporate network.

Semantic Web technology is the next generation of contemporary Web. It is focusing on the meaning of information (the Semantic Web) and on community awareness (Web 2.0). Most agrees that the impact of Semantic Web technology is wide ranging. The Project10X (a consulting firm) study found that more than 190 companies including Adobe, AT&T, Google, HP, Oracle and Sony are involved in developing Semantic Web based tools [1]. But making it easier to comb through online data carries security implications. Therefore, a key need for the vision of semantic web technology to succeed will be the ability for handling security, privacy and trust in the process of information access. This paper presents an approach to combine semantics with identity management to provide access control and privacy services.

2. Identity management and semantics

People currently rely on various forms of identities to deal with numerous services in their personal, professional and social life. Managing these identities is crucial for service access. Chowdhury in his paper [2] proposes a concept of "My digital identity" that comprises 'My personal identities (PID)', 'My corporate identities (CID)' and 'My social identities'. PIDs can be used to identify ourselves in very personal and commercial interactions. Similarly, CIDs and SIDs can be used in our professional and interpersonal interactions respectively. SemID focuses on the identity management in corporate environment. Now-a-days people increasingly work in a project oriented groups. Such a group can be formed by members of different partner organizations. Managing identities of members and thereby ensuring privacy to a corporate social community is a big concern. In this paper, we propose to incorporate the concept of Semantic Web technology to manage identities of people in communities.

Semantic Web is seen as the next generation of information management system in web where information has machine-readable and machine understandable semantics. In this paper, OWL, Web

Ontology Language is used to formalize and define the proposed identity management domain. It is intended to make the information contained in this domain ready to be processed by future applications. OWL is chosen because it facilitates greater machine interpretability of Web content than that supported by XML, RDF, and RDF Schema (RDF-S) by providing additional vocabulary along with a formal semantics. Among the sublanguages of OWL, we use OWL DL because of its computational completeness and decidability.

3. Related work

There is a critical tradeoff associated with the tension between users' privacy requirements and providing persistent and increasingly broad visibility of their activities. Identity tradeoff in community networks are even greater - in exchange for our privacy we expect to gain a sense of security and well-being. Significance of adding privacy-enhancing technologies (PET) in virtual community networks is overwhelming [3], [4]. Not many works have been done in providing identity management and privacy support in community environment involving semantic technology.

In [5], [6] authors provided a solution for community driven identity management with access rights delegation. It also showed the way, how social network information can be protected in a distributed environment. Instead of maintaining centralized access control list, trust based access rights group has been proposed to delegate access rights. Social networks acted as a mean to delegate trust. The system utilized FOAF (friend of a friend) to build social networks [7]. It has considerable computational complexity to derive trust between users. Private key based signature scheme ensured the privacy of social networks and user's profile management systems. Secure distribution and maintenance of private keys may make the situation complicated. The similar concept of trust or reputation also has been used by [8] to model a community aware identity management solution. The authors intended to provide this solution only through trust or reputation management which is not acceptable to apply instead of identity. Distributed trust management approach is also considered as one of the main components to secure the Semantic Web [9]. But it is also evident from all these works that trust is affected by various factors and it is also difficult to quantify.

In this paper, we propose a community or group based identity management solution which can be implemented in corporate environment. Instead of FOAF used in [7], this paper uses OWL which has more facilities for expressing meaning and semantics than FOAF. OWL is more appropriate when machines are expected to perform useful reasoning tasks on data. Using clearly defined ontologies, communities can solve identity management and privacy problems with relatively less complexity. Security and privacy requirements are defined through policies and rules. Finini proposed to describe ontology for policies using semantic language like OWL in paper [9]. In another paper [10], Smith introduced role-based access control (RBAC) policy management concepts. Several efforts are underway across NASA to use semantic technologies like OWL to manage many of such policies and mechanisms. Smith used the algorithms introduced by Kolovski [11]. Few of these concepts are also applied to develop policy and rules in our paper. Besides these efforts, Chou designed role based access control and delegation model for Web-based information systems through authorization and delegation policies [12]. These policies were encoded in XML.

4. Goal and use case

4.1 Goals

In corporate environment a project group composed of several different types of project members. It is categorized based on the roles played by these project members. Each of them has different privileges or rights to access different project resources. Table 1 shows examples of such scenario.

Table 1. Project roles and their privileges to access project resources.

Project roles	Privileges	Project Resources
Project leader	Administrator	Membership management
	Final decision	Deliverables
	Read/Write	Documents
	Visibility	Member details
Project member	Read/Write	Documents
	Visibility	Member details
Visitor	Read only	Documents
	No visibility	Member details

It is evident that a project has roles and individuals play these roles. 'He is leader of Rel9 project' refers to his corporate identity in professional life. Based on roles, he has different privileges. Project leader has administrative privilege which the project members do

not have. Leaders and members of a project hold both read and write rights. One of the crucial requirements of privacy is to ensure that a visitor should not be allowed to see the project member details (for example, contact address, email, phone number etc.). It means that project leader and members have visibility of member details but visitors have no such visibility. These are the goals to ensure the access control to project resources and privacy of project group. Individual's identities and roles in a group protect privacy of the group he/she belongs to.

4.2 Use case: corporate identity management

Figure 1 illustrates the use case scenario. A new project named Rel9 (Release 9) Project has been created in Telenor AS. It consists of Gyorgy Kalman, Josef Noll and Erik Swansson as members. They represent Telenor Hungary, Telenor R&I and Ericsson respectively in Rel9 project. Therefore, they are part of their group/company and the newly created project. The project has some resources like a webpage, member details, budget, various documents and deliverables etc. One of the members will serve as project leader and other members will work as ordinary members. Visitors are any persons from Telenor or Erikson who are not the members of Rel9 project but want to know about the project and its status. Based on the use case descriptions and requirements, SemID ontology and instances will be formulated.

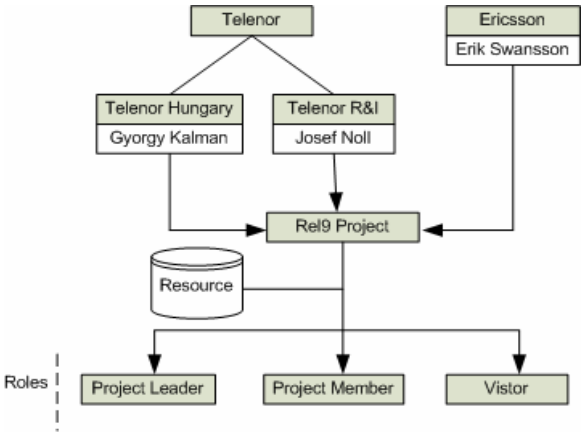

Figure 1. Use case scenario.

5. Managing identity with semantics

5.1 SemID

SemID is proposed to deal with identity management of people in professional life. It is also expected to provide access control and privacy services based on roles they play in project based working environment. The access control and privacy goals are achieved through policies and rules. In this paper, we use OWL DL to formalize the semantics of the proposed identity management.

5.2 Functional architecture

Corporate identity of each member and the project group to which he belongs to are clearly defined in ontology. The members of the project play several explicit roles like project leader, project member and visitor. Each role has certain policy (or policies). A Policy represents the privilege reserved for each role in a community and expressed through a set of Rules. Essentially a Rule is a function that takes an access request as input and results an action (permit, deny or not-application). To determine if a Rule is applicable to an access request, a target is used that consists of several elements. A Target is a set of simplified conditions for the Subject, Resource and Action that must be met for a Rule to apply to a given request [11]. In the proposed SemID ontology, Subjects are the identities (CIDs) that play specific Roles like project leader, project member and visitor. Resource is the project resources. Theoretically, Rules contain triples Target, Action and Policy. However, Targets and roles have not been explicitly defined in the modeled ontology which will be implemented in later works. Therefore, Rule is simplified as triple Subject, Resource and Action. According to the goal of this work, project leader should get the permission to read, write or to take the final decision on any resources of the project. Ordinary member of Rel9 project has only Read and Write permission. A visitor should be denied to write over the project documents. This is how access control issues are handled in SemID.

Privacy requirements are satisfied in SemID ontology using two properties (*hasVisibility* and *hasVisibilityOfGroup*). *hasVisibilityOfGroup* is attached to class: Role and *hasVisibility* is attached to class: Identity (CID). The later is rather a general visibility property which ensures that anyone (having CID) belongs to some groups has visibility of resources of those groups. Whereas Role based visibility represents more specific visibility of resources. Based on Roles; leader, members or visitors of a project have different visibility of member details. Leader and members of Rel9 project has visibility of fellow member's details which visitors cannot see. *hasVisibilityOfGroup* ensures it in SemID.

Therefore, access control to project resources (excluding member details) is maintained through

Policy and Rules. Visibility of member details is provided by *hasVisbilityOfGroup* property.

5.3 Implementations

We model the ontology of the use case scenario with OWL-DL using Protègè ontology editor platform. Left of figure 2 shows the classes and subclasses of SemID ontology to model the proposed use case and to meet the requirements. Figure 2 also illustrates the instances of four different groups described in the use case scenario. *Empty* group has been created to support privacy of a group when visitors try to access resources. Figure 3 illustrates four different policies of roles: Administrator, Final Decision, Read and ReadWrite.

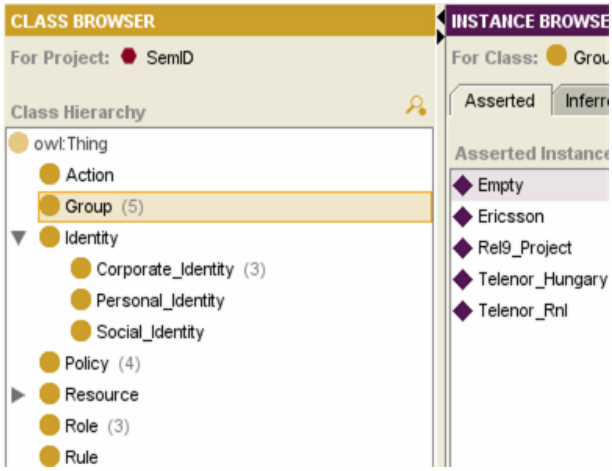

Figure 2. Classes and subclasses of ontology.

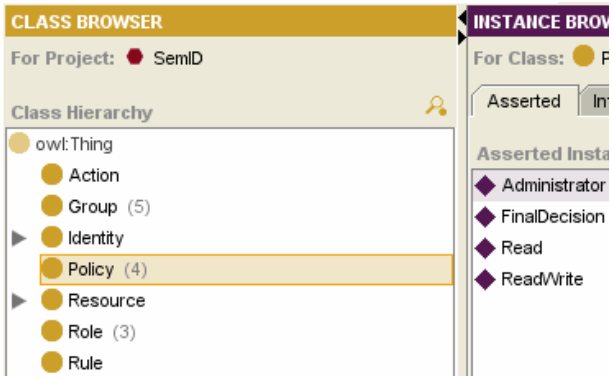

Figure 3. Instances of Policy.

In this ontology, the corporate identity (CID) of each representative from Telenor R&I, Telenor Hungary and Ericsson is defined by his name. These are the instances of CID subclass. Each instance has two properties *hasGroup* and *hasVisibility*. The group to which a member belongs to is explicitly identified using *hasGroup* property. *hasVisibility* points to the groups a member has required visibility. For example, it ensures that 'Erik Swansson has visibility of Ericsson and Rel9 project group as he is member of both of these'. Figure 4 gives an instance of these definitions.

There are three possible roles in Rel9 project. Figure 5 shows the instances of class Role. Each Role has specific policy which is expressed by *hasPolicy* property. Appropriate policies are added to each instance of Role. According to the goal described in previous section, project leader has the policies like Administrator, Final Decision and ReadWrite. In order to deal with the requirements of group privacy, *hasVisibilityOfGroup* property has been created. The Visitor instance has visibility of group *empty* (an instance of Group). It ensures that 'as a visitor I should be allowed to read the documents of project and but I don't have the permission to see the member details of the visited project'. But as a project member I am allowed to see my fellow member details.

Table 2 gives a list of the properties used in this ontology. Each property has its domain and range. The classes to which a property is attached are called domain. Allowed classes for properties are often called a range of a property. These properties linked the classes through the following facts:

- Identity has Group (*hasGroup*).
- Identity has Visibility (*hasVisibility*).
- Group has Role (*hasRole*).
- Role has Policy (*hasPolicy*).
- Role has visibility of Group (*hasVisibilityOfGroup*).
- Policy has Rule (*hasRule*).
- Rule has Subject (*hasSubject*).
- Rule has Resource (*hasResource*).
- Rule has Action (*hasAction*).

hasVisibility and *hasVisibilityOfGroup* ensures the privacy of groups. *hasSubject*, *hasResource* and *has Action* create the simplified Rule.

Table 2. Property list and their domain and range.

Properties	Domain	Range
hasGroup	Identity	Group
HasVisibility	Identity	Group
hasRole	Group	Role
hasPolicy	Role	Policy
hasVisibilityOfGroup	Role	Group
hasRule	Policy	Rule
hasSubject	Rule	Role
hasResource	Rule	Resource
hasAction	Rule	Action

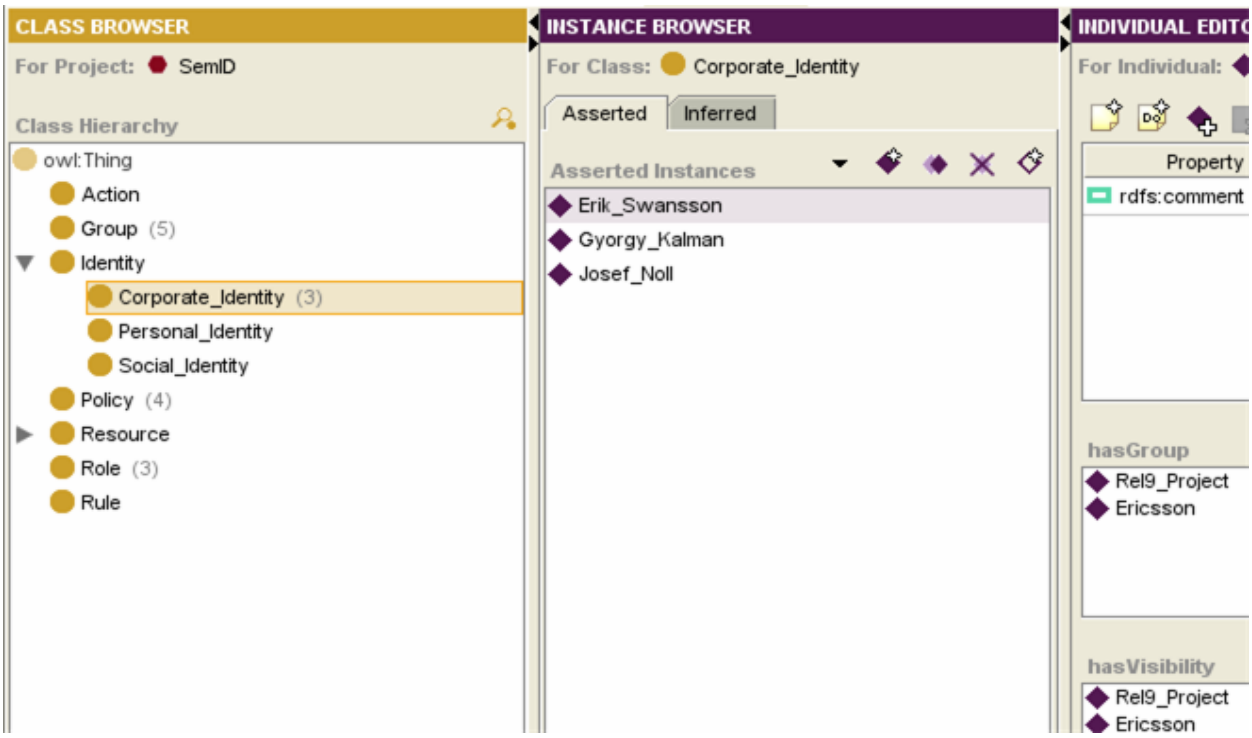

Figure 4. Corporate identity instances and their properties.

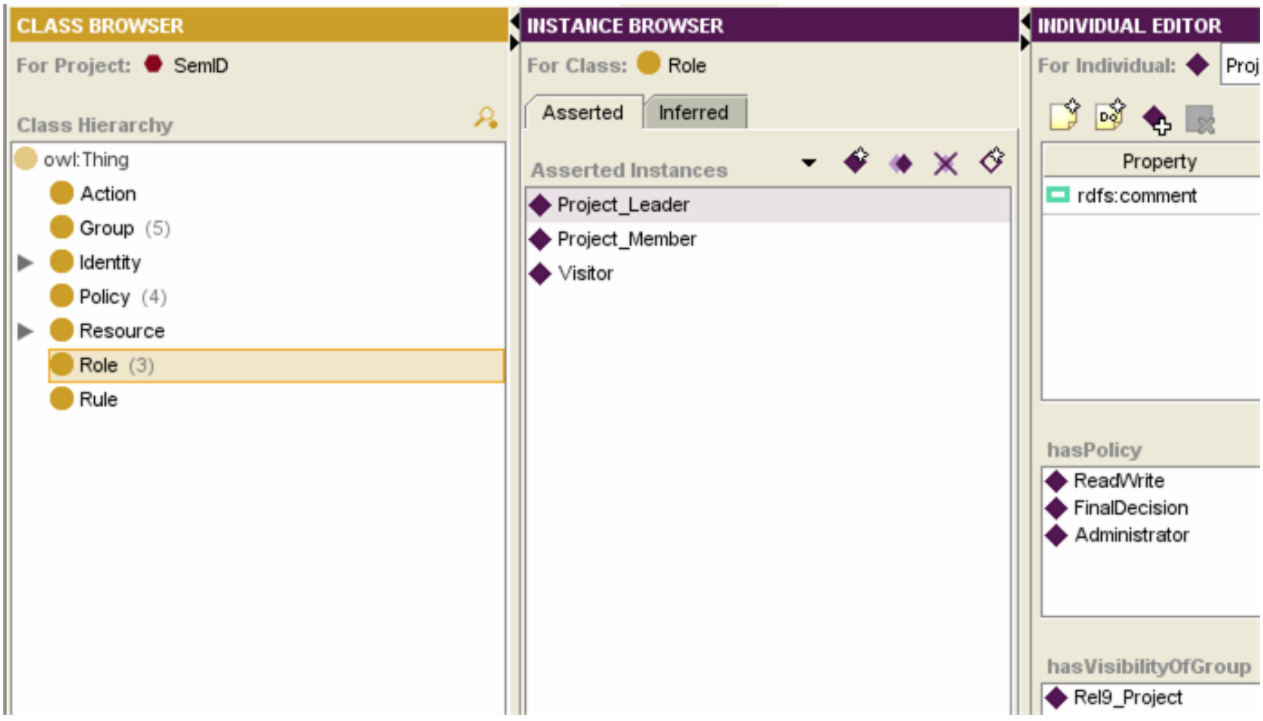

Figure 5. Instances of Role and their properties.

6. Conclusion

Security and privacy is a big concern in today's distributed but connected working environment. This work is an approach to provide identity management services using semantic web technology in current project oriented corporate working culture. A formal representation of a use case scenario is implemented in the proposed SemID ontology which is expected to handle identity management and privacy issues. Similar concepts can be extended to currently open social community domain to add privacy. These extensions and the implementation of applications based on these ontologies will be taken care of in our future works.

7. Reference

[1] The Project10X: http://www.semantic-conference.com/semanticwave.html

[2] Mohammad M R Chowdhury, J.Noll, 2007, "Distributed Identity for Secure Service Interaction", *the Third International Conference on Wireless and Mobile Communications, ICWMC07*, Gaudeloupe, French Caribbean.

[3] C. M. Chewar, D. Scott McCrickard and John M. Carroll, "Persistent virtual identity in community networks: Impact to social capital value chains", *Technical Report TR-03-01*, Computer Science, Virginia Tech, 2003.

[4] G. J. Walters, "Privacy and Security: An Ethical Analysis", *Computers and Society*, 2001, pp. 8-23.

[5] Sebastian Ryszard Kruk, Slawomir Grzonkowski, Adam Gzella, Tomasz Woroniecki, and Hee-Chul Choi, "D-FOAF: Distributed Identity Management with Access Roghts Delegation", *1st Asian Semantic Web Conference*, Beijing, China, 2006.

[6] Sebastian Ryszard Kruk, Adam Gzella and Slawomir Grzonkowski, "D-FOAF Distributed Identity Management based on Social Networks", *In demo session of ESWC 2006*

[7] FOAFRealm project: http://www.foafrealm.org/

[8] Hee-Chul Choi et al., "Trust Models for Community-Aware Identity Management", *Identity, Reference and the Web IRW2006, WWW2006 Workshop*, Scotland, May 23, 2006.

[9] Tim Finin and Anupam Joshi, "Agents, Trust, and Information Access on the Semantic Web", *ACM SIGMOD, vol. 31, issue 4, Special Issue: Special section on semantic web and data management*, December 2002, pp. 30-35.

[10] Michael A. Smith, Andrew J. Schain, Kendall Grant Clark, Arlen Griffey, and Vladimir Kolovski, "Mother, May I? OWL-based Policy Management at NASA", *in press of European Semantic Web Conference 2007, ESWC2007.*

[11] Vladimir Kolovski, James Hendler, and Bijan Parsia, "Analyzing Web Access Control Policies", *16th International World Wide Web Conference, WWW2007*, Alberta, Canada, May 8-12, 2007.

[12] Shihyi Chou, Eric Jui-Lin Lu, amd Yi-Hui Chen, "X-RDR: A Role-based Delegation Processor for Web-based Information Systems", *ACM SIGOPS Operating Systems Review, vol. 39, issue 1*, 2005, pp. 4-21.

.