Context-Aware Access Control for Collaborative Working Environments Based on Semantic Social Networks

Peyman Nasirifard

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

Abstract. Most current shared workspaces within Collaborative Working Environments (CWE) provide role-based coarse-grained access control mechanisms for eProfessionals which do not satisfy their requirements in most cases. When e-Professionals collaborate in CWE, they leave some fingerprints, which contain highly valuable information. These fingerprints can be exported and used to extract the hidden social networks based on the objects that eProfessionals collaborate upon. Social networks have great potentials to be used within different domains like designing access control policies. Context information of eProfessionals is also a great source to be used within access control mechanisms. In this paper, I present an approach for access control mechanism within CWE based on context, trust, and social networks. These are key elements for expressing access control policies. I intend to enrich the framework with Semantic Web technologies and ontologies.

Key words: Social Network, Access Control, Collaborative Working Environment, Context-Aware Access Control, Social Network Analysis, Trust in Social Network, Semantic Social Network, Social Network Mining

1 Introduction

E-professional or "eProfessional" is a term used in Europe to describe a professional whose work relies on concepts of Telework or Telecommuting: working at a distance using information and communications technology [59]. Internet has provided an infrastructure for eProfessionals to collaborate and work towards the same goal in a corporate environment which is so-called Collaborative Working Environment (CWE). The CWEs enable eProfessionals to share different resources, e.g. documents or events among other eProfessionals in a platform which is so-called shared workspaces. One of the main disadvantages of current platforms is the lack of a fine-grained access control mechanism. Most current platforms provide role-based coarse-grained access control mechanisms that do not meet the eProfessionals' requirements, e.g. temporal requirements. Social

networks, which can be represented as graphs, have great potentials to be used in different domains like designing access control policies based on relationships among actors. When eProfessionals collaborate in CWE, they leave some fingerprints that are highly valuable and can be used for extracting social networks. Most current environments are able to export the activities (events) that are done as feeds or log files. The social networks among eProfessionals, extracted partially from fingerprints, and enriched with trust and context, are good candidates to be used within access control policies. The whole framework can be enriched with Semantic Web technologies to make it more machine-understandable.

In this paper, which is actually my Ph.D. proposal, first I focus on background information: I present essential definitions and concepts regarding social networks, collaborative working environments, different access control mechanisms, context-aware access controls etc. Then I consider the problem that currently exists in access control mechanism within most shared workspaces for eProfessionals and finally I have a rough overview of my approach towards solving the problem. During this paper, I try to answer following questions regarding my Ph.D. proposal:

- What is the problem that I am going to solve?
- What do I want to do?
- Why my approach is important?
- How does my approach differ from prior works?
- What do I have so far?
- How am I going to do the work?

2 Relevant Background

2.1 Social Networks and Social Acquaintances

Social networks [36], as a sort of Scale-free networks [21], can be represented as graphs using the famous notions of nodes and edges between them. Obviously, the concept of social network is not something new and its origin is not also computer science. Social networks are good means to model the connections between people based on different relationships that the actors may acquire during a period of time. The small world phenomenon [37], based on Milgram's idea of six degrees of separation [22], presents the concept that everyone in the world is connected to all people in the world by a short chain of social relationships. Some practical efforts like *The small world project* [1] at university of Columbia have proved this theoretical phenomenon. It is obviously a good indicator for the hidden power of social networks.

Roughly speaking, social networks fall into two main groups: object-centric social networks and non-object-centric which I call them user-centric social networks. The term object-centric social network has been coined by Jyri Engeström in his blog post [2] and indicates those social networks that are built on top of

[1] `http://smallworld.columbia.edu/`

[2] `http://www.zengestrom.com/blog/2005/04/why_some_social.html`

objects, e.g. the actors make a social network conceptually around a photo or a movie clip. Engeström argues that the main reason that some Web-based social network sites fail after a while is the fact that they are not object-centric and the users lose their motivations to be connected.

A social network can be analyzed based on different metrics, like *Centrality Closeness* and *Betweenness* [40], [41]. These metrics can identify different characteristics and potentials of social networks.

One of the research areas in social networks is addressing the different relationships that the actors may acquire in a period of time. Ontological consideration on human relationships has been considered by some researchers: Matsuo et al. [51] provide some consideration towards this direction and present several distinctions across relationships between humans. Davis et al. [38] introduce RELATIONSHIP which is a set of vocabularies for describing relationships between people. Carminati et al. [39] propose REL-X vocabulary, which is another effort towards this direction. Gan et al. [52] provide several vocabularies as FOAF extensions to cover the often changing variables in FOAF. This work can be considered as providing context information for FOAF profiles.

2.2 Collaborative Working Environment

Collaborative Working Environments (CWE) are platforms and infrastructures that support working between people (eProfessionals) by means of different technologies and tools. The CWE was in existence before the birth of computers and Internet. The concept of e-Collaboration, which first appeared in 1980s, have been studied by many researchers. Kock [42] defines e-Collaboration and has an overview of six key conceptual elements of e-Collaboration.

2.3 Semantic Web and Semantic Social Network

Semantic Web [1], as an extension to current Web, is actually a set of technologies and standards which tries to help machines to understand concepts and extract new information based on existing well-defined information. Using Semantic Web, software engineers are able to build interoperable systems that can benefit from machines to combine data and reason on existing data and infer new information. Ontologies are main building blocks and fundamental elements of Semantic Web and try to define a specific domain in a systematic way. Ontologies can be represented using different standards and languages like RDFS [3] and OWL [2]. Both are based on Resource Description Framework (RDF) [63] which is a language for representing information about resources. OWL comes in three main flavors: OWL Lite, OWL DL and OWL Full which have been sorted according to expressivity and complexity levels.

Combining Semantic Web and social networks is an interesting area for many researchers. One of the main initiatives towards building a semantic social network is FOAF [3] (Friend of a Friend) project [44]. In brief, FOAF provides some

[3] `http://www.foaf-project.org/`

basic vocabularies that are needed to describe people, their interests, their friends etc. Efforts like XFN [4] (XHTML Friends Network) tries to embed social networks and human relationships using hyperlinks like HTML. Neumann et al. [9] compare different online social networks based on different criteria and try to conclude with the importance of combining social networks and Semantic Web portals for a better collaboration in online communities. Downes [10] tries to address the need of social network metadata within semantic metadata. Jung et al. [14] propose a three-layer architecture (social layer, ontology layer, and concept layer) for semantic social networks which all these three layers are connected together and can influence each other. In [62] Mika extends the model of ontologies with social dimension and shows how community-based semantics can appear from this new model through a process of graph transformation.

Most researchers [47], [46], [50] in this area use FOAF as a basis model and extend it partially and gather a benchmarking corpus from extracted information which is available mostly on the Internet. Mika [13], [48] did some work on mining social networks based on a hybrid approach from FOAF profiles and also information extracted from Google and ranked through Google Mindshare [45] for building and analyzing social networks among Semantic Web researchers (Flink [5] project). Due to availability of semantic search engines and open data like [49], this approach sounds to be more interesting among others. Goecks et al. [54] provide an infrastructure that uses social networks for information sharing. They extract social networks from users' email messages. Mori et al. [53] have the similar approach, but they use different sources like Web pages, emails, sensors and enable users to control their resources. This is performed automatically, but end users can also access and obviously change their social networks.

2.4 Trust in Social Networks and Semantic Web

One of the most famous works in defining a computational model of trust is [11]. In this work, Marsh took into the account the concept of trust in different domains and based on this consideration, he developed a trust model for a distributed environment. In [12], Golbeck has studied trust in social networks and proposed several algorithms for computing trust in social networks and evaluated this model using some applications like TrustMail.

Trust and Semantic Web have been studied in different domains, mainly for recommendation systems. In [4], Bedi et al. suggest a semantic recommendation system based on trust and they apply their model to a tourism recommender system which generates recommendations for a selection of destinations.

2.5 Context in Social Networks and CWE

It is difficult to give one valid global definition to context. The main reason is that there is no absolute context and context gets its meaning in relative to

[4] `http://gmpg.org/xfn/`
[5] `http://flink.semanticweb.org/`

something [64]. The lack of sufficient literature on studying the roles of contexts and contextualizations in social networks is apparent. There exist some works like [5], [6], [7] which try to address some aspects of contextualizations in social networks, but they seem to be preliminary works. Using shared context in CWE to improve and support collaborative tasks has been also studied in some works like [8].

2.6 Access Control

Access control is the ability to permit or deny the use of something by someone [43]. There exist plenty of approaches and mechanisms towards controlling the access: access control lists, role-based access control, attribute-based access control, ontology-based access control etc. There exist a lot of formal languages that aim to express access control policies with different perspectives and granularities, like XACML [56], which is an extensible access control language and is currently used in many frameworks, P3P [57], which is too coarse-grained to be used in different domains, EPAL [55], which is more machine-readable, Rei [58], which is an ontlogy-based policy language, and KAoS [60], which is another ontology-based policy framework which is well-suited for Semantic Web services etc. Many researchers try to combine different access control mechanisms to build a more powerful mechanism and decrease the disadvantages of each mechanism. Kern et al. [23] provide an architecture for role-based access control to use different rules to extract dynamic roles. Alotaiby et al. [29] present a team-based access control which is built upon role-based access control. Periorellis et al. [30] 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. Kim et al. [34] propose a collaborative role-based access control (C-RBAC) model for distributed systems which is fine-grained and try to address the conflicts from cross-domain role-to-role translation. Toninelli et al. [61] present an approach towards combining rule-based and ontology-based policies in pervasive environments.

There exist some efforts towards enriching access control mechanisms by means of Semantic Web technologies. Li et al. [25] propose a rule based access control which is based on OWL and SWRL [26]. They propose an OWL ontology to describe the terms and access policy rules will be expressed in SWRL. Priebe et al. [31] discuss that attribute-based access control (ABAC) is a bit complex and error-prone and they propose a solution by pushing Semantic Web technologies and ontologies into ABAC.

The study of access control mechanisms in CWE is not new and was in existence from the birth of e-Collaboration. Shen et al. [33] studied access control mechanisms in a simple collaborative environment, i.e. a simple collaborative text editing environment. Zhao [20] has an overview on three main access control mechanisms and provides a comparison between these three main mechanisms in collaborative environments. Tolone et al. [19] provide a comprehensive study on access control mechanisms in collaborative systems and they compare different mechanisms based to different criteria, e.g. complexity, understandability, ease

of use, etc. There exist also different studies on access control requirements in collaborative systems. Jaeger et al. [28] present basic requirements for role-based access control within collaborative systems. Gutiérrez Vela et al. [32] try to model an organization in a formal way that considers the necessary elements to represent the authorization and access control policies. Demchenko et al. [35] propose an access control model and mechanism for grid-based collaborative applications.

There exist some studies on access control in social networks. Most of the literature focus on relationships that the people may acquire in a social network. In [18], Kruk et al. suggest a role-based policy-based access control for social networks, where the access rights will be determined based on social links and trust levels between people. In [15], Carminati et al. present the same approach and in [16], they extend their model by adding the concept of private relationships in access control, as they noticed that all relationships within social networks should not be public, due to security and privacy reasons.

Using context information in access control mechanisms has been studied by different researchers. Toninelli et al. [17] suggest a semantic context-aware access control framework for secure collaboration in pervasive computing environments. They propose a simple OWL-based context model and based on this model, they propose a context-aware policy model and they support their model by a meeting scenario case study, where the attending people can access the meeting resources only during the meeting. They express policy statements using description logic. Georgiadis et al. [24] provide a model for combining contextual information with team-based access control and they provide a scenario in health care domain, where the model is used. Zhang et al. [27] propose a model for dynamic context-aware role-based access control for pervasive applications. They extend role-based access control and dynamically align role and permission assignments based on context information.

3 Problem

In a collaborative working environment, where the eProfessionals collaborate, there should exist some kind of access control mechanism, as eProfessionals share different resources (e.g. profiles information, documents, events, etc.) and shared resources should be protected against unauthorized accesses within shared workspaces. Most current shared workspaces provide a coarse-grained role-based access control mechanism which is not flexible and in most cases seems to be effectless, especially when the number of eProfessionals increases.

I present a scenario to explain this problem in a more detailed manner: Bob is the name of the main actor. He is currently working on an European project in a collaborative distributed infrastructure with other team members from different organizations. Partners are geographically distributed in different countries with different time zones. This project has different Work Packages (WP) and Bob is the leader of WP two. The project has a Web site for public visitors. This Web site includes project news, newsletters, public events, some public deliverables

and information about the scope and the mission of the project. The project has also a private collaborative working environment (shared workspace). The private side includes a wiki, a forum, a calendar to document events, some folders for uploading documents to be accessed by team members, a bunch of documents, presentations, photos from meetings, contracts, time sheets etc. Partners have sometimes conference calls to discuss online or via telephone. They meet regularly each two/three months to setup things and discuss the progress of the project. In this private workspace, Bob has uploaded some documents, photos, and presentations. The issue is that not all project members should access Bob's resources. In our case, Bob wants to set the following access control rules based on the roles defined by the project.

- Bob wants to give access of work-in-progress deliverables to all WP leaders plus the project coordinator 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* and only to a specific person.
- Bob wants to give access of a particular presentation only during the meeting (temporal restrictions) and only to specific meeting participants.
- Bob wants to give access of a particular background document only to members that are currently working on a particular deliverable.
- Bob wants to share a photo only to his close friends (or his colleagues from his company) within this project.
- Bob wants to give access of his presentation, only after finishing it and only to particular members.
- 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.
- Special rule: Bob wants to share a technical report with responsible persons from other projects that are related to his project (same domain)
- and more rules ...

The above items are just some simple requirements for setting access control policies. In general, with current role-based access control mechanisms within most CWEs (shared workspaces), it seems to be very difficult or even impossible to apply above rules. The lack of a fine-grained access control mechanism for shared workspaces within collaborative working environments is the main problem that I want to address in my thesis. The term *fine-grained* refers to a flexible, parametric, context-aware, open and extensible access control mechanism. Towards this direction, in next section, I explain how social networks within most CWEs and context information can help to express and apply more flexible access control rules.

4 Approach

Generally, to realize above scenario, I plan to build a context-aware access control for shared workspaces within collaborative working environments based on social

networks. Social networks are key players, as their model is very similar to what we utilize in our offline lives to give access to the people that we communicate with. To achieve this goal, the first problem that should be addressed is modeling social networks in different layers: based on social acquaintances and also roles within a collaborative working environment and organization. Besides this user-defined (manual) social network, there exist also some (semi-)automated ways to extract the *hidden* social networks in shared workspaces. This hidden social network, which connects people by means of dynamic relationships, is based on the *objects* that connect people (i.e. object-centric social networks), and can be extracted using different mechanisms, like processing the log files and feeds. As an example, if user A reads a document that has been written by user B, the hidden relationship between two users is "ReadWrite" from user A to user B and "WriteRead" from user B to user A. These hidden relationships enable building parametric social networks and help to *recommend* the appropriate candidates for sharing resources.

One key candidate for representing social networks is an extended version of FOAF to meet the new requirements. I believe that this area (mining social network) is a very wide area and different sources can be considered towards this direction, but the main focus of my thesis is not on this section. In this step, I will have an overview of possibilities for defining/mining social networks from shared workspaces and provide a simple proof of concept. This approach should benefit from ontologies for machine-understandability, like an ontology for different sources that help to build social networks, an ontology for properties of a graph, etc.

The next problem is defining a context model that is extensible and suitable enough to model context information of eProfessionals with regards to CWE. This model should contain all required context information that is helpful for expressing access control policies. Obviously, this model and the model of social networks should refer to each other.

The analysis of social networks based on different criteria that make sense for access control and then calculating trust among eProfessionals based on their dynamic relationships are the next sub-problems that should be solved. Different characteristics of social networks should be considered to check whether they make sense to be embedded in access control scenarios or not. These characteristics vary from those related to graph-theory (e.g. in-degree, out-degree) to new defined ones.

One of the main goals is to allow end users to express access control policies based on context information, trust and social network analysis. Probably ontology-based description which is actually a logic-based approach is a key candidate towards this direction.

The final step is related to the construction of the main engine that gets the enriched social networks and access control rules as inputs and decides the accessibility of resources for different users. Figure 1 demonstrates the overall view and the whole process that I plan to work on it.

To summarize, below I present a list of items that are related to my research:

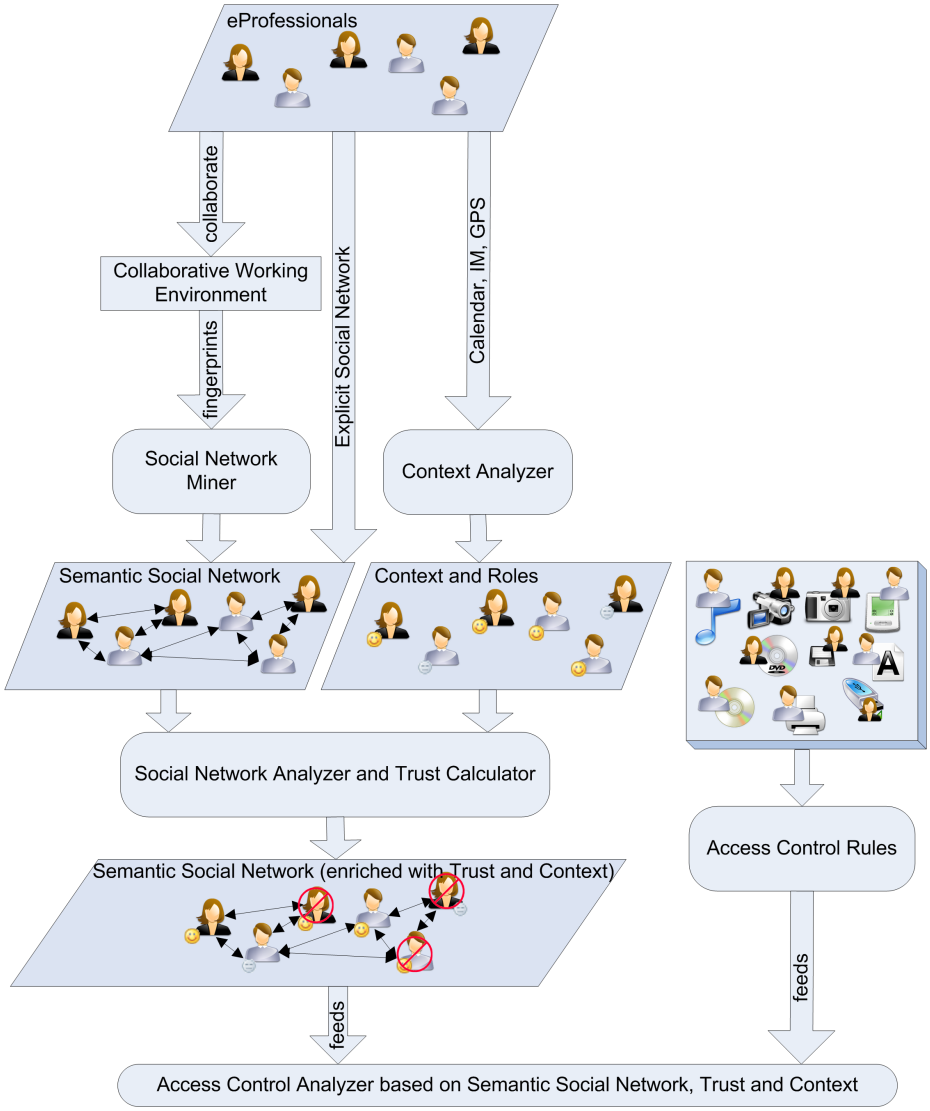

Fig. 1. General Overview of Solution

- Modeling the collaborative working environment as social networks
- Mining social networks from shared workspaces within CWEs based on the objects that eProfessionals collaborate upon and the different roles that they acquire
- Modeling the required CWE context information
- Proposing trust criteria for different characteristics and dynamic relationships in social networks within CWEs

– Expressing access control rules with consideration of the model of social network, trust and context criteria
– Designing an engine that gets access control rules and enriched social networks as inputs and decides the accessibility of resources for different users
– Supporting all layers with semantic technologies to make relevant information more machine-understandable

5 Conclusion

Most current shared workspaces within CWEs provide a role-based access control mechanism which is in most cases inflexible and effectless. Social networks and contexts are two main candidates to enrich the legacy access control mechanism for a more flexible approach. In this paper, I discussed the lack of a fine-grained context-aware access control for CWEs using a scenario and based on requirements, I proposed a context-aware access control mechanism based on social networks within CWEs. In my approach, context information of eProfessionals, trust, and explicit and implicit social networks within CWEs are key concepts. The implicit social network can be extracted by monitoring the behaviors of eProfessionals, when they collaborate in CWEs. I enrich the framework with Semantic Web technologies and ontologies. This approach enables users to express and apply flexible access control rules based on their relationships with other eProfessionals, trust and their context information.

Acknowledgments. This work is supported by inContext (Interaction and Context Based Technologies for Collaborative Teams) project: FP6-IST-2006-034718 and Ecospace (Integrated Project on eProfessional Collaboration Space) project: FP6-IST-5-35208

References

1. 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)
2. Bechhofer, S., van Harmelen, F., Hendler, J., Horrocks, I., McGuinness, D.L., Patel-Schneider, P.F., Stein, L.A.: OWL Web Ontology Language Reference. `http://www.w3.org/TR/owl-ref/` (2004) [Online; accessed 2-May-2007]
3. Brickley, D., Guha, R.V.: Resource Description Framework (RDF) Schema Specification. W3C Recommendation. `http://www.w3.org/TR/rdf-schema/` (2004) [Online; accessed 2-May-2007]
4. Bedi, P., Kaur, H., Marwaha, S.: Trust Based Recommender System for Semantic Web. In proceedings of the 2007 International Joint Conferences on Artificial Intelligence (2007) 2677–2682
5. Brézillon, P.: Contextualizations in a social network. Revue d'Intelligence Artificielle, Vol. 19 (2005) 575–594
6. Brézillon, P.: Role of context in social networks. Florida Artificial Intelligence Research Society Conference (2005)

7. Brézillon, P.: A context approach of social networks. In proceedings of the Workshop on Modeling and Retrieval of Context, Ulm, Germany, Vol. 114 (2004)
8. Brézillon, P., Araujo, R.: Reinforcing shared context to improve collaboration. Revue d'Intelligence Artificielle, Vol. 19 (2005)
9. Neumann, M., O'Murchu, I., Breslin, J., Decker, S., Hogan, D., Macdonaill, C.: Semantic social network portal for collaborative online communities. Journal of European Industrial Training, Emerald Group Publishing Limited, Vol. 29 (2005) 472–487
10. Downes, S.: Semantic networks and social networks. The Learning Organization: An International Journal, Emerald Group Publishing Limited, Vol. 12 (2005) 411–417
11. Marsh, S.P.: Formalising Trust as a Computational Concept. (1994)
12. Golbeck, J.A.: Computing and applying trust in web-based social networks. University of Maryland at College Park, College Park, MD, USA (2005)
13. Mika, P., Elfring, T., Groenewegen, P.: Application of semantic technology for social network analysis in the sciences. Scientometrics, Vol. 68 (2006) 3–27
14. Jung, J.J., Euzenat, J.: Towards Semantic Social Networks. In proceedings of the 4th European Semantic Web Conference, Innsbruck, Austria (2007)
15. Carminati, B., Ferrari, E., Perego, A.: Rule-Based Access Control for Social Networks. OTM Workshops (2). Lecture Notes in Computer Science, Vol. 4278. Springer-Verlag, Berlin Heidelberg New York (2006) 1734-1744
16. Carminati, B., Ferrari, E., Perego, A.: Private Relationships in Social Networks. In proceedings of ICDE Workshops (2007) 163–171
17. Toninelli, A., Montanari, R., Kagal, L., Lassila, O.: A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments. In proceedings of the 2006 International Semantic Web Conference (2006) 473–486
18. Kruk, S.R., Grzonkowski, S., Gzella, A., Woroniecki, T., Choi, H.: D-FOAF: Distributed Identity Management with Access Rights Delegation. In proceedings of the 2006 Asian Semantic Web Conference (2006) 140–154
19. Tolone, W., Ahn, G., Pai, T., Hong, S.: Access control in collaborative systems. ACM Comput. Surv. Journal, Vol. 37 (2005) 29–41
20. Zhao, B.: Collaborative Access Control. T-110.501 seminar on Network Security (2001)
21. Wikipedia: Scale-free network — Wikipedia, The Free Encyclopedia. `http://en.wikipedia.org/w/index.php?title=Scale-free_network&oldid=128937758` (2007) [Online; accessed 17-May-2007]
22. Milgram, S.: The Small World Problem. In Journal of Psychology Today, Vol. 1 (1967) 61–67
23. Kern, A., Walhorn, C.: Rule support for role-based access control. In proceedings of the tenth ACM symposium on Access Control Models and Technologies, ACM Press, New York, NY, USA (2005) 130–138
24. Georgiadis, C.K., Mavridis, I., Pangalos, G., Thomas R.K.: Flexible team-based access control using contexts. In proceedings of the sixth ACM symposium on Access control models and technologies, ACM Press, New York, NY, USA (2001) 21–27
25. Li, H., Zhang, X., Wu, H., Qu, Y.: Design and Application of Rule Based Access Control Policies. In proceedings of the Semantic Web and Policy Workshop, held in conjunction with the 4th International Semantic Web Conference , Galway, Ireland (2005)

26. Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B., Dean, M.: SWRL: A semantic web rule language combining OWL and RuleML. http://www.w3.org/Submission/SWRL/ W3C Member submission (2004) [Online; accessed 17-May-2007]
27. Zhang, G., Parashar, M.: Dynamic Context-aware Access Control for Grid Applications. In proceedings of the Fourth International Workshop on Grid Computing, IEEE Computer Society, Washington, DC, USA (2003) 101
28. Jaeger, T., Prakash, A.: Requirements of role-based access control for collaborative systems. In proceedings of the first ACM Workshop on Role-based access control, ACM Press, New York, NY, USA (1996) 16
29. Alotaiby, F.T., Chen, J.X.: A Model for Team-based Access Control (TMAC 2004). In proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), Vol. 2, IEEE Computer Society, Washington, DC, USA (2004) 450
30. Periorellis, P., Parastatidis, S.: Task-Based Access Control for Virtual Organizations. Scientific Engineering of Distributed Java Applications (2005) 38–47
31. Priebe, T., Dobmeier, W., Kamprath, N.: Supporting Attribute-based Access Control with Ontologies. In proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society, Washington, DC, USA (2006) 465–472
32. Gutiérrez Vela, F.L., Isla Montes, J.L., Paderewski, P., Sanchez, M.: Organization Modelling to Support Access Control for Collaborative Systems. Software Engineering Research and Practice (2006) 757-763
33. Shen, H., Dewan, P.: Access Control for Collaborative Environments. In Proceedings of Computer-Supported Cooperative Work Conference (CSCW), ACM Press (1992) 51–58
34. Kim, H., Ramakrishna, R.S., Sakurai, K.: A Collaborative Role-Based Access Control for Trusted Operating Systems in Distributed Environment(Application) (<Special Section>Cryptography and Information Security). IEICE transactions on fundamentals of electronics, communications and computer sciences, The Institute of Electronics, Information and Communication Engineers, Vol. 88 (2005) 270–279
35. Demchenko, Y., Gommans, L., Tokmakoff, A., van Buuren, R.: Policy Based Access Control in Dynamic Grid-based Collaborative Environment. In proceedings of the International Symposium on Collaborative Technologies and Systems, IEEE Computer Society, Washington, DC, USA (2006) 64–73
36. Wikipedia: Social network — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Social_network&oldid=131310005 (2007) [Online; accessed 17-May-2007]
37. Wikipedia: Small world phenomenon — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Small_world_phenomenon&oldid=130656468 (2007) [Online; accessed 18-May-2007]
38. Davis, I., Vitiello Jr, E.: RELATIONSHIP: A vocabulary for describing relationships between people. http://vocab.org/relationship/ (2005) [Online; accessed 18-May-2007]
39. Carminati, B., Ferrari, E., Perego, A.: The REL-X vocabulary. OWL Vocabulary. http://www.dicom.uninsubria.it/~andrea.perego/vocs/relx.owl (2006) [Online; accessed 18-May-2007]
40. Scott, J.P.: Social Network Analysis: A Handbook. SAGE Publications (2000)

41. Wasserman, S., Faust, K., Iacobucci, D.: Social Network Analysis: Methods and Applications (Structural Analysis in the Social Sciences). Cambridge University Press (1994)
42. Kock, N.: What is E-Collaboration?. International Journal of e-Collaboration, Vol. 1 (2005) i-vii
43. Wikipedia: Access control — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Access_control&oldid=130640680 (2007) [Online; accessed 22-May-2007]
44. Miller, L., Brickley, D.: FOAF Vocabulary Specification. Technical report, RDFWeb FOAF Project (2003)
45. Calishain, T., Dornfest, R.: Google Hacks: 100 Industrial-Strength Tips and Tools. O'Reilly & Associates, Inc. Sebastopol, CA, USA (2003)
46. Ding, L., Finin, T., Joshi, A.: Analyzing Social Networks on the Semantic Web. IEEE Intelligent Systems, IEEE Computer Society, Vol. 9 (2005)
47. Finin, T., Ding, L., Zhou, L., Joshi, A.: Social Networking on the Semantic Web. The Learning Organization, emerald, Vol. 12 (2005) 418–435
48. Mika, P.: Bootstrapping the FOAF-Web: An Experiment in Social Network Mining. First Workshop on Friend of a Friend, Social Networking and the Semantic Web, Galway, Ireland (2004)
49. Hogan, A., Harth, A.: The ExpertFinder Corpus 2007 for the Benchmarking and Development of ExpertFinding Systems. First International ExpertFinder Workshop, Berlin, Germany (2007)
50. Mika, P.: Social Networks and the Semantic Web. In proceedings of the 2004 IEEE/WIC/ACM International Conference on Web Intelligence (WI'04), IEEE Computer Society, Washington, DC, USA (2004) 285–291
51. Matsuo, Y., Hamasaki, M., Mori, J., Takeda, H., Hasida, K.: Ontological Consideration on Human Relationship Vocabulary for FOAF. First Workshop on Friend of a Friend, Social Networking and the Semantic Web, Galway, Ireland (2004)
52. De Gan, J., DeLong, B.K., Schmidt, C.: MeNowDocument: A FOAF extension for defining often changing variables in FOAF. http://schema.peoplesdns.com/menow/ (2004) [Online; accessed 22-May-2007]
53. Mori, J., Sugiyama, T., Matsuo, Y.: Real-world oriented information sharing using social networks. In proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work, ACM Press, New York, NY, USA (2005) 81–84
54. Goecks, J., Mynatt, E.D.: Leveraging social networks for information sharing. In proceedings of the 2004 ACM conference on Computer supported cooperative work, ACM Press, New York, NY, USA (2004) 328–331
55. Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunter, M.: Enterprise Privacy Authorization Language (EPAL 1.2). http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html (2003) [Online; accessed 22-May-2007]
56. OASIS Standard: eXtensible Access Control Markup Language (XACML) Version 2.0. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf (2005) [Online; accessed 22-May-2007]
57. Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J.: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. http://www.w3.org/TR/P3P/ (2002) [Online; accessed 23-May-2007]
58. Kagal, L.: Rei: A Policy Language for the Me-Centric Project. HP Labs, accessible online http://www.hpl.hp.com/techreports/2002/HPL-2002-270.html (2002) [accessed 27-May-2007]

59. Wikipedia: E-professional — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=E-professional&oldid=123657930 (2007) [Online; accessed 27-May-2007]
60. Uszok, A., Bradshaw, J.M., Johnson, M., Jeffers, R., Tate, A., Dalton, J., Aitken, S.: KAoS Policy Management for Semantic Web Services. IEEE Educational Activities Department, Piscataway, NJ, USA, Vol. 19 (2004) 32–41
61. 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 proceedings of the Semantic Web and Policy Workshop (2005)
62. Mika, P.: Ontologies are us: A unified model of social networks and semantics. Web Semantics, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, Vol. 5 (2007) 5–15
63. Manola, F., Miller, E.: RDF Primer. W3C Recommendation, World Wide Web Consortium (2004) [Online; accessed 27-May-2007]
64. Bazire, M., Brézillon, P.: Understanding Context Before Using It. In proceedings of 5th International and Interdisciplinary Conference on Modeling and Using Context, Paris, France (2005) 29–40