Authorization Control in Business Collaboration

Daisy Daiqin He
Supervised by Jian Yang

Department of Computing, Macquarie University,
North Ryde, NSW 2109 Australia
daiqin,jian@ics.mq.edu.au

Abstract. Authorization control has been well studied for years, and there are quite a few theories and techniques available for handling access control for a single or a centralized system. However unique and challenging security issues concerning business collaboration in the context of service oriented computing (SOC) have arisen due to the dynamic and loosely coupling nature of the environment in which business collaboration is conducted. In this paper, we discuss different authorization control issues in business collaboration and present an overview to our proposed PD-AC framework, which we believe it has laid a good foundation for future work in the area of policy consistency checking, policy negotiation, and security policy enforcement in business collaboration.

Key words: access control, security policy integration, collaboration

1 Introduction

Web services and Service Oriented Computing (SOC) provides infrastructural support for cross-organization collaboration in distributed environments. However security concerns become one of the main barriers that prevent widespread adoption of this new technology. Each organization or business unit has its own interest and security polices for defining who has access right for specific services and how services can be used. In web services environment with complex cross-organization collaborations, Different security challenges will arise with different number of participants involved in collaboration.

Access control is enforced in a single organization by using pre-defined authorization control polices. Common authorization control practices include requester credential verifications, role assignments and access decision makings.

In collaborative business world, a service can be accessed by a party which can pass it to other parties. We shall use some examples in health care to illustrate some issues.

Suppose a patient granted access right to a General Practitioner (GP) in a medical centre on patient's health record. Since the physician is a member of a research institute, he could also let researchers in this institute access to this health record based on the security policy of the medical centre. However the patient may not want the GP give access right to anyone on his health record

unless there is an emergency. How can we use security policies to control the way in which information or service is propagated between organizations?

Problem can also arise from service composition. For example, a medical center allows the patients who hold an OSHC (overseas student health cover) to book appointments on line for general inquiry and ultrasound exam based on its policy. A radiology institute wants to collaborate with the medical center and accepts on line bookings from the medical center. However, OSHC is not accepted by the radiology institute's policy. It is challenge to decide which authorization control policy they should follow if these two organizations collaborated in the presence of this policy conflict.

Moreover, organizations collaborate with each other in various ways. Before organizations engage in collaboration, their authorization policies need to be analyzed to decide the possibility of collaboration under the authorization constraints defined by each individual party. Therefore, we need to evaluate consistencies of access policies of different organizations. Intuitively, the concept of 'access policy consistency' is referred as that the access policies of different organizations are conflict free, for the same service. And organizations are able to collaborate in the intended way securely in terms of access control policies.

To address these complex security policy issues, we need a framework that can analyze, evaluate and integrate security policies if necessary for collaboration purpose, based on which negotiation can be guided and security integrity can be enforced. Security control in business collaboration should take individual organization's access policy into account, as well as the type of the collaboration which is referred as collaboration pattern in the paper.

Access control issues in signle organization or signle domain have been well studied [5, 3, 2]. Access control in collaborative environment has just started to attract the attention of the research community [1], but little attention have been given to consistency study between access control policies of different collaboration participants, particularly in the context of Web Services. Furthermore, these studies only focused on providing solutions to some aspects of security issues in terms of: security policy specification, access control in distributed environment, and access decision making. What is missing is a comprehensive analysis of: (1) what security requirements really are in the context of business collaboration; (2) security policies can be specified; (3) how security policy can be verified, evaluated, and integrated for the purpose of business collaboration. No feasible mechanisms can be developed for policy negotiation and enforcement without this analysis.

The rest of paper is organized as follows. We first explain the basic elements included in the security policy and relationship between these elements in Section 2. In Section 3 we identify and model different types of collaborations. In Section 4 we model and discuss security controls for different types of collaboration in health care environment. We propose our framework in Section 5. Formal definition and of policies and rules are presented in Section 6. Related work is discussed in Section 7. In Section 8, we give some concluding remarks and outline future research directions.

2 Related Work

A number of studies concentrated on authorization architecture [7, 4]. Author in [7] suggested a brokered architecture to build composite Web services according to the specified security constraints. They used security matchmaker to find right collaboration partners who have compatible security policies, which is similar to our research. However, it did not address the issue that inconsistencies and conflicts exist between security policies of prospective partner.

A few of studies have touched policy level security issues, which focused on identifying different security requirements and proposed specifications for these requirement. Trust-Serv[11] modeled access control processes in web services using state machine and provides lifecycle management for policies. Ws-AC [6] provides an adaptive system that is capable of asking users to refine their requests to comply with security policies. Again, all of them are concerned security policies in a single organization and none of them addressed policy problems in collaborative environment.

There are few papers on Web service authorization control in the collaborative environment. We are aware of the work presented by [1], which presented a framework for managing authorization policies for Web service compositions. [12] proposed an approach to security policy integration and conflict reconciliation. But they neglected the fact that different types of collaboration affect the way the collaboration policy is developed as well as the requirements on collaborative partner's authorization policy. An evaluation on collaborative partner's access policy has to be carried out before the collaboration be established. Our work is to fill in this gap. We believe this is the first step toward conflicts detection and suitable collaboration partners discovery.

In summary, none of these studies went deep into different types of cross-organization collaboration, which could raise different requirements on access control policy of prospective collaborative partners. Our goal is thus to provide a framework that could identify types of cross-organization collaborations in this context; define collaboration requirements in terms of security policy; generate policy integration rules. Most importantly our work is in the context of business collaboration which involves multiple organizations rather than simple interaction between individual requester and single service provider.

In this paper we present some of our initial results in modeling security requirements and integrating security policies for business collaboration. We believe this study is the first step towards achieving an understanding of a secured of business collaboration in terms of authorization control.

3 The PD-AC Framework

The core function of our PD-AC (Policy Driven Authorization Control) framework is realized by a Policy Evaluation Engine, which is associated with every organization that provides services in business collaboration, see Figure 1. Policy Evaluation Engine is used to analyze the nature of collaboration, make access

decision, and finally generate the collaborative security policies. The proposed framework consists of two components: request mediator and policy evaluation engine. Upon receiving a request for a service, the request mediator firstly identifies the type of requested service, which is a process that identify whether the requested service is a collaborative service. If it is a simple service that does not involve any collaboration, the mediator will perform normal access control functions: looking up database, check which role in the database has the requested privilege; compare requester's credential with security requirement; make access decision.

However, if it is a collaboration request (prospective collaboration partner), the request mediator will pass the request to the Policy Evaluation Engine to perform the following functions:

- Identify requested collaboration type;
- Evaluate requester's authorizaton policy according to policy requirements for requested collaboration type;
- Make collaboration decision;
- Generate collaborative authorization policies for the collaborated service if the requester if acceptable (from previous step);

In the following subsections, we will discuss different types of collaboration and policy evaluation engine in more detail.

3.1 Business Collaboration Patterns

Business collaborations consist of complex relationships and interactions among organizations. Authorization policies of all participate organizations need be carefully considered and evaluated. Our analyze shows that different collaboration types affects the requirements on collaborative partner's authorization policy. We have conclude four different ways of collaboration between organizations and provided simple examples in Health Care domain [8].

- **Simple Access** (**SA**): it depicts the most simplest 'request service - provide service' scenario that involves two organizations.
- **Composite Services**. The Composite Service we discuss here is referring to the service that is based on the integration of multi-service providers. Two different cases are identified in service composition:
  1. **Composite service with agent** (**CSWA**): Multiple numbers of service providers provide their services through an centralized agent, i.e. health insurance company and health service providers.
  2. **Joined service without an agent** (**JSOA**): Two organizations involving in a peer-to-peer collaboration and provide a joined service by integrating their business processes or integrating part of their business processes together to form a new service directly without any agent.
- **Service Outsourcing** (**SO**): As the result of globalization, Outsourcing and offshore Outsourcing has become a popular trend in many industries, SO depicts collaboration relationship between outsourcer and outsourcees.

- **Service Propagation** (**SP**): it depicts collaborations that involving multiple organizations and 'forward' privilege could be passed from one organization to another organization.

3.2 Policy Evluation Engine

Authorization policy of prospective partners are compared and evaluated in Policy Evaluation Engine to determine the suitability for requested collaboration pattern. Before we can compare and evaluate policies from different organizations, we need to understand all the necessary elements and their relationships for a generic authorization policy. Therefore, an authorization policy model is proposed to specify authorization policy in an individual organization. We base our policy model on Role-Based Access Control (RBAC)[9] and encoded the model in Description Logic. The main entities in the model are roles, credentials, privileges, obligations and provisions[8]. Policies from two different organizations can be compared by combining them into a single model.

Three categorizes of inconsistencies have been discussed in our work: role, credential and privilege inconsistencies[10]. Each category consists of several inconsistency types. We use a Description Logic reasoner (an automated proof engine) to analyse the inconsistencies in policies. We encode the inconsistency tests as concepts and relations in our model. Individual policies expressed using the model can then be combined and tested. Given a combined policy, with the roles and privileges of the two organisations suitably related, a reasoner will prove that the tests are either satisfiable or unsatisfiable and these results can be analysed to check if they satisfy the requirements for the particular collaboration. Since the tests are part of the general model, so they can be expressed once, proven to encode the required meaning and used to testing any two policies.

We have identified several cross-organization collaboration patterns, different collaboration pattern can result in different requirements for authorization policies of prospect collaborative partners. The requirements we discussed in our work are basic requirements that must be satisfied by the prospect partner to be considered for requested collaboration. Policy requirements for different collaboration patterns are analyzed. Inconsistencies are discussed for each collaboration pattern[10]. Depends on the collaboration pattern, some of the inconsistencies are acceptable, some of them needs further negotiation and some of inconsistencies lead to reject.

4 Conclusion

In this paper, we proposed an authorization conrol framework for business collaboration. Our analyze shows that different ways of collaboration could affects the requirements on authorization policy of collaborative partner. The proposed framework use a policy evaluation engine to analyze collaboration suitability of prospective partners for requested collaboration pattern from authorization policy perspective. In our previous work, we have concluded different business

collaboration patterns and discussed different requirements for the prospective partner's authorization policies in the collaboration. An description logic based authorization policy model has been proposed to specify the authorization policy of an individual organization. Inconsistencies between authorization policies from different collaboration participants are identified and classified based on the model, based on which the collaboration possibility are analyzed. In the future we intend to extend this work to incorporate the following:

- Context constraints that affect access control.
- Inconsistencies that caused by role hierarchies and separation of duty.
- Collaboration access control policy requriements from business transaction and process perspective.

References

1. Rouached, M., Godart, C.: Reasoning about Events to Specify Authorization Policies for Web Services Composition. In: 2007 International Conference on Web Services, IEEE Press, Salt Lake City (2007)
2. Srivatsa, M., Iyengar, A., Mikalsen, T., Rouvellou, I., Yin, J.: An access control system for web service compositions. In: 2007 International Conference on Web Services, IEEE Press, Salt Lake City (2007)
3. Kagal, L., Paolucci, M., Srinivasan, N., Sycara, K., Denker, G.: Authorization and Privacy for Semantic Web Services. IEEE Intelligent Systems. 19, 50-56 (2004)
4. Ziebermayr, T., Probst, S.: Web Service Authorization Framework. In: 2007 IEEE International Conference on Web Services, pp. 614-621. IEEE press, San Diego (2004)
5. Sirer, E. G., Wang, K.: An access control language for web services. In: 2002 SACMAT, pp.23-30. (2002)
6. Bertino, E., Squicciarini, A. C., Mevi, D.: A Fine-Grained Access Control Model for Web Services. In: IEEE International Conference on Services Computing, pp. 33-40. IEEE press, Shanghai (2004)
7. Carminati, B., Ferrari, E., Hung, P. C. K.: Security Conscious Web Service Composition. In: IEEE International Conference on Web Services, pp. 489-496. IEEE press, Chicago (2006)
8. He, D. D., Yang, J.: Security Policy Specification and Integration in Business Collaboration. In: 2007 IEEE International Conference on Services Computing (SCC 2007), pp. 20-27. IEEE press, Salt Lake City (2007)
9. Sandhu R. S., et al.: Role-Based Access Control Models. IEEE Computer. 29, 38-47 (1996)
10. He, D. D., Yang, J.: Identify Authorization Control Requirement in Business Collaboration. In: IEEE Service Oriented COmputing (2) 2008 (SCC 2008). IEEE, 2008
11. Skogsrud, H., Benatallah, B., Casati, F.: Trust-Serv: Model-Driven Lifecycle Management of Trust Negotiation Policies for Web Services. In: 13th World Wide Web Conf (WWW 2004). ACM Press, New York (2004)
12. Yau, S. S., Chen, Z: Security Policy Integration and Conflict Reconciliation for Collaborations among Organizations in Ubiquitous Computing Environments. In: UIC'08, pp. 3-19. (2008)