A Governance Framework for Mitigating Risks and Uncertainty in Collaborative Business Processes

Ziyi Su[1], FrédériqueBiennier[1], Wendpanga Francis Ouedraogo[1]

[1] LIRIS, CNRS, INSA-Lyon, University of Lyon, 20, Avenue Albert Einstein, 69621 cedex Lyon, France
{ziyi.su,frederique.biennier,wendpanga-francis.ouedraogo}@insa-lyon.fr

Abstract. The development of collaborative business process relies mostly on software services spanning multiple organizations. Therefore, uncertainty related to the shared assets and risks of Intellectual Property infringement form major concerns and hamper the development of inter-enterprise collaboration. This paper proposes a governance framework to enhance trust and assurance in such collaborative context, coping with the impacts of Cloud infrastructure. First, a collaborative security requirements engineering approach analyzes assets sharing relations in business process, to identify risks and uncertainties and, therefore, elicits partners' security requirements and profiles. Then, a 'due usage' aware policy model supports negotiation between asset provider's requirements and consumer's profiles. The enforcement mechanism adapts to dynamic business processes and Cloud infrastructures to provide end-to-end protection on shared assets.

Keywords: End-to-end security, governance, framework, policy, risk and uncertainty, collaborative business process

1 Introduction

With the development of knowledge and service economy, enterprises focus more on their core business while building business federation strategy to provide a better service for their clients. Accordingly, corporate Information Systems are developing toward collaborative paradigm, using different software components. This allows new opportunities for business development, taking advantage of new computing paradigm as Service Oriented Architecture and Cloud Computing. These phenomena suggest a collaborative IT-based service ecosystem trend, where enterprises use the dynamic organization offered by service composition to set flexible business processes and enhance enterprise assets value.

Nevertheless, security risks and uncertainty related to the intellectual property due to shared assets are seen as a major challenge for enterprises to participate in

[1] This work was partially supported by ANR project 'semeuse' and GDCIS project 'process 2.0'.

collaborative business process [1]. Security engineering in such complex and dynamic collaborative contexts should offer end-to-end security governance concerning partners' shared assets value. This involves a multi-layered viewpoint ranging from security requirements engineering phase to security configuration and enforcement phases, paying attention to the challenges of interoperability and virtualization which stem from collaborative IT infrastructure.

After presenting the context and related work in section 2, we present our security governance framework (section 3). Built as a security policy generation and combination, our solution can enhance trust and assurance in the virtual-enterprise level collaboration context as security requirements and usage control can be used to select the convenient partners. Moreover, the 'due usage control' monitoring module [2] continuously regulates consumers operations upon assets so that shared assets (data or services) can get a life-long consistent protection in a dynamic environment.

2 Context and Related Work

Security engineering in a collaborative context is a multi-folded task among business process model and analysis, risks assessment and management, collaborative authorization and virtualization-aware security auditing. After presenting the IS context and risk analysis and management methods, we focus on the implementation level, paying attention to security policy and to cloud security particular models.

2.1 Security Requirements Identification

Recent years have seen the development of many Information System-based business process engineering methods, such as the activity-oriented, product-oriented, decision-oriented, context-oriented and strategy-oriented process meta-models that can be selected and combined [3]. To cope with interoperability constraints involved by collaborative / federated business development, standardized modeling languages can also be used [4]. However, few attentions are paid on the risks related to information assets (i.e. service and information) shared beyond security administrative domains, which are major barriers for the development of collaborative business process [1].

Of course, several methods and standards have been defined since the 1980s to capture security requirements / identify vulnerabilities and risks:

- Evaluation criteria used to certify software / hardware components have been defined as the DoD Rainbow series in the 80s or the EEC ITSEC standard in the 90s, both of them integrated in the international Common Criteria standard.
- Risks analysis can be guided by different methodologies either focusing on "standard criteria" (as the French Information System Security Agency for the EBIOS method), on particular infrastructure vulnerabilities (for example the CERT OCTAVE method focuses on the network elements) or by integrating Business Process and resources organizations (as the CERT SNA or the french CLUSIF (federation of IS managers) MEHARI methods which pay attention

on the BP organization as identified as major risks by the ISO/IEC 17799, ISO/IEC27002.

Table 1 presents a comparison of these methods used to identify risk and countermeasures in a rather "fixed" environment. Nevertheless, the dynamic context of service based collaborative organization involves an end-to-end protection on shared asset value and re-funding this security evaluation according to usage and protection agreement signed between partners. In former work, we have proposed an asset sharing relation analysis method to deal with such security concerns, i.e. extract enterprises' security requirements adapted to business federation strategy [5]. Other researchers focus more on the collaborative security engineering thoughts and explore toward secured business processes [6].

Table 1. Comparison of some security methods

	Requirements analysis	Design	Implementation
EBIOS	Text risk and objectives Identifications	Protection pattern	
OCTAVE	Structured information access identification	Objectives prioritization Best practices	Audit and implementation project management
SNA	Process and resources workflow identification	"Survival process" design	CERT attacks information and knowledge base
MEHARI	Shortened risk analysis	Best practices	Implementation project management

Based on such thoughts, we propose a structured approach to identify enterprises' security requirements on asset sharing process in business federation. The requirements can then be expressed by a flexible policy model [7] and be used to support security negotiation between enterprises, given that interoperability is achieved using shared domain knowledge reference.

2.2 Implementing a Secured Environment

As far as collaborative organizations are concerned, interoperability constraints often lead to use de-facto IS standards as web services. Many researchers use policy-based models to protect information assets originators' intellectual property in collaborative context [8] [9]. Based on this strategy, we use an expressive policy model that accommodates the factors related to the asset 'usage' operations and security profiles of the consumer, the shared asset, the IT-infrastructure, context and environment [7]. Such model allows a peer-to-peer security configuration of the collaborative context. Furthermore, extensions can still be made to use it to govern the QoS and QoP (quality of protection) of the collaborative context. The enforcement of such policy decisions ensures the end-to-end protection of shared assets. Nevertheless, the monitoring mechanism must cope with the software / hardware infrastructure. software virtualizations in cloud-based collaborative computing systems.

To cope with the scalability, interoperability and agility required in federated collaborative organizations, Cloud computing based solutions are more and more used. Cloud computing relies on software virtualizations to offer flexible service

outsourcing models, i.e. IaaS, PaaS, SaaS, etc. The benefits are mostly related to the reduced costs for IS investment for enterprises and scalable IS upgrading, as well as dynamic choosing of service providers. As to security, the impacts are two-pronged. Positive impacts are mostly due to that the Cloud providers more visible security profiles for customers [10]. Nevertheless, more concerns are related to the negative impacts [11]. Therefore, most recently researchers start to investigate the end-to-end security and have brought forward some solution for trustworthy Cloud virtualizations [12] and auditing [13]. Although very few, these achievements shed light on how transparent security across virtualizations can be achieved. Following this track, we can build a security monitoring and auditing framework adapting to collaborative cloud infrastructure.

3 Security Governance Framework Organisation

The foundation of our framework (see fig. 1) includes a collaboration-oriented security requirements engineering method and a domain knowledge base to define partners' security policies and profiles with. Coupled with a negotiation strategy between the policies and profiles, as well as enforcement of decisions, end-to-end protection for assets can be achieved.

Fig. 1. Framework overview.

Fig. 2 shows detail information of our framework. Collaboration-oriented security requirements engineering includes the security requirement/profile identification and common business goal extraction methods. According to these methods, enterprises' 'RoP' and QoP are extracted. These protection level information (regarding both requirements and protection offer profiles) can be used to define a security-aware business process. Interoperability among enterprises knowledge references is supported thanks to a domain knowledge base. Dedicated information repositories maintain the knowledge base and RoPs/QoPs policies. Negotiation between partners' RoPs and QoPs ensures that providers' requirements must be fulfilled by consumers' security profiles for a collaborative business process to succeed. Enforcement mechanism assures that asset 'due usage control' [2] is achieved, even on a cloud infrastructure.

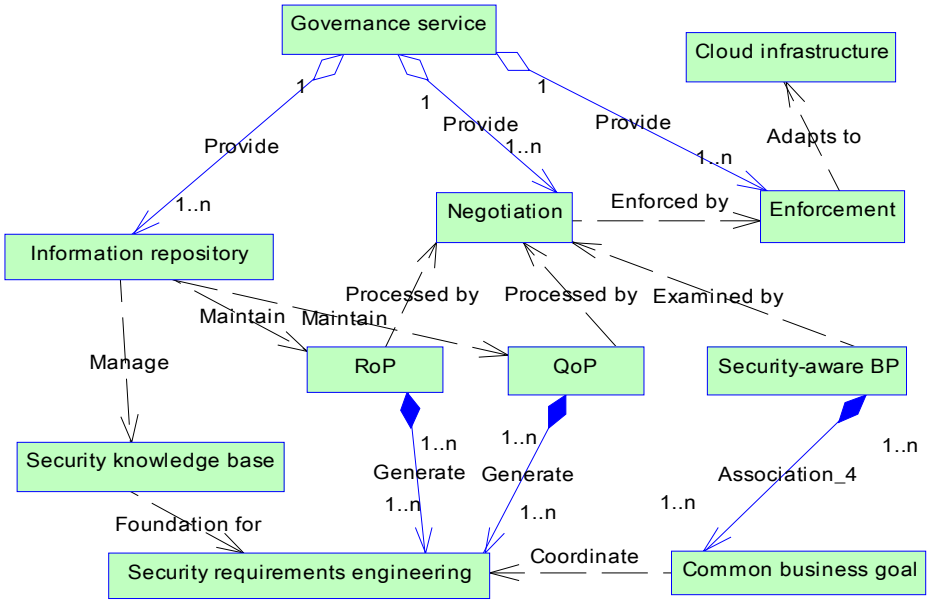

Fig. 2. Framework model.

3.1 Collaboration-oriented Security Requirements Engineering

Security engineering in collaborative context can be done in either a top-down or bottom-up way. The former suits the scenarios where one checks whether a business process can be carried out or not, w.r.t. the security aspects of participants and the context. The later is adapted to more dynamic scenarios where enterprises want to firstly define their RoPs and QoPs before leveraging this information to select partners for business federation. The engineering process focuses on the assets value of each enterprise that are going to be shared, with an iterative spiral process, as in SNA and GEM [14], to achieve more precise extraction of security factors. In each iteration, we focus on the enterprise IS infrastructure and internal business process, the assets involved, the exposed functionalities and shared assets as the enterprise opens its IS. This leads to paying attention on the risks and uncertainties brought or made grave by such openness. Table 2 shows examples of some questions that are used for the risk assessment and what security factors the answers should declare.

These questions are generic and used to guide a cycle of the iterative assessment. Some question are decomposed into more detailed question lists or forms for the information officer and personnel to be investigated with (detail discussion will be give in separate paper). In this way, risks of information compromise or misuse associated to each software stack layer of the virtual-enterprise IS infrastructure, as well as lost due to the uncertainty related to dynamic business process are identified.

Table 2. Comparison of some security methods

Security goal	Questions	Answers
	IS & assets questions	
-	Which functionalities & assets?	List of information assets and functionalities
CIAN	Which security goal on these functionalities & assets?	CIAN
CIAN	Which security/assurance mechanisms on these functionalities & assets?	Hardware/OS/platform/network/application/human level mechanisms
	Openness & assets sharing questions	
CIAN	Which functionalities & assets are shared?	List of information assets and functionalities
N	Shared with which partners?	'pre-difined'/ random
	Risks & compensation questions	
CIAN	Which security/assurance mechanisms negatively affected by the openness?	List of mechanisms
CIAN	Which level the negative effects have achieve?	Neutralize/damage/ineffect at times
CIAN	Which level of compensentation you want to have?	Total restore/partial restore
CIAN	Whaich security level should be achieved after the compensentation?	C/I/A/N
CIAN	Should these security level be maintained by partners or collaboration system?	Partner/system
-	Any other requirements on partners?	-
-	Any other requirements for the collaboration system?	-

Legend: C (Confidentiality), I (integrity), A (Availability), N (Non repudiation)

3.2 Policy-based Security Configuration

The RoP and QoP can be expressed by a 'usage control' policy model (see fig. 3), which expresses the 'usage' rights upon the assets, obligations and conditions which includes security factors related to the assets (i.e. OAT), consumers (i.e. SAT) and collaboration context (i.e. CNAT).

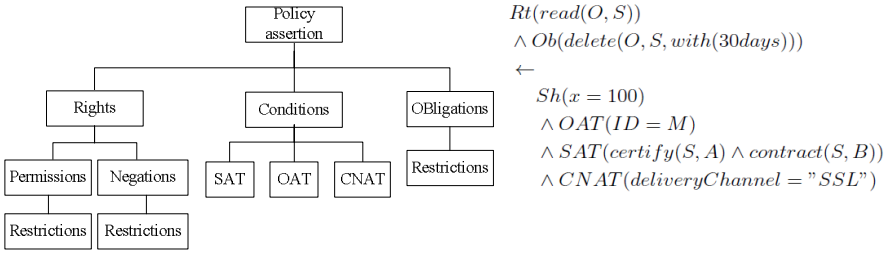

Fig. 3. The context-aware security policy model and a sample policy in concise syntax.

Security configuration of the context is done by assuring that partners related by asset sharing relations have compatible security profiles. Furthermore, a 'standardized' knowledge based can be built to collect the most common security factors, whereas enterprises can develop from it their domain knowledge references. A 'consensus based voting' [15] protocol can be used to ensure that, for the enterprises in a same context, the developed knowledge references are compatible among them.

3.3 'Usage' Aware Monitoring

The monitoring mechanism inspects consumers 'usage' operations on assets and make sure that providers RoPs are respected. It must be adapted to the Cloud virtualization environments enterprises are moving towards. Positive impact of the Cloud computing paradigm is that enterprises security profiles, to a great extent decided by the security profile of Cloud providers, are more visible to partners. Nevertheless the virtualization segregation between software stack layers makes the task of auditing system events more tricky. To fit with the multi-tenancy scenarios (e.g. a combined Cloud infrastructure with IaaS, PaaS, SaaS from different providers), 'usage' monitors are set at each layer.

The inspection of asset usage operations on consumer system is usually achieved by auditing systems calls or by having a closer look into the system processes, which are conventionally deemed arduous tasks. Nevertheless, very recent research has explored some possible approaches, such as enhanced JAVA runtime platform allowing the auditing of information flows [13], Trust Platform Modula-based attestation [12] for platform integrity. Whereas a great gap still exists between the security concerns for Clouds, we can expect more security-aware Cloud systems, as well as explore toward this goal. Possible approaches will close rely on Trusted Computing technology for trust root of software stack and information flow control technologies for the in-detail auditing. Such auditing, however, might compromise the privacy of Cloud providers. Therefore, trusted third parties, or privacy preserving protocols, should be used, to ensure a security policy compliance examination method without disclosure of partners' inner operations, therefore protecting their trade secrets.

4 Conclusion

This paper proposes a governance framework to enhance trust and assurance in virtual-enterprise, coping with the complex and dynamic collaborative business process. Our security governance framework aims at providing comprehensively management on the business operations of organizations in a collaborative process, helping them to clearly identify the risks of intellectual property infringement when their business value flows through the whole virtual-enterprise architecture. In sum, designed in a layered and modular way, our framework could be used in a wide range of industrial inter-organizational business contexts, giving enterprises more grasp of

the risks related to the assets they provide, promoting the successes of business federation.

References

[1] Linda, B. B., Richard, C., Kristin, L., Ric, T., Mark, E.:The evolving role of IT managers and CIOs–findings from the 2010 IBM global IT risk study. Technical report, IBM (2010)
[2] Su, Z., Biennier, F.: An architecture for implementing 'collaborative usage control' policy - toward end-to-end security management in collaborative computing. In: ICEIS2012, (submitted).
[3] Hug, C., Front, A., Rieu, D., Henderson-Sellers, B.: A method to build information systems engineering process metamodels. J. Syst. Software. 82(10), pp. 1730 – 1742 (2009)
[4] Ducq, Y., Chen, D., Vallespir, B.: Interoperability in enterprise modelling: requirements and roadmap. Adv. Eng. Inf. 18(4), pp. 193 – 203. (2004)
[5] Su, Z., Biennier, F.: Toward comprehensive security policy governance in collaborative enterprise. In: APMS 2011, IFIP WG5.7 (2011)
[6] Maamar, Z., Benslimane, D., Thiran, P., Ghedira, C., Dustdar, S., Sattanathan, S.: Towards a context-based multi-type policy approach for web services composition. Data & Knowledge Engineering. 62(2), pp. 327 – 351. (2007)
[7] Su, Z., Biennier, F.: A collaborative-context oriented policy model for usage-control in business federation. In: 2011 IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering.pp.201 – 204. (2011).
[8] Bussard, L., Neven, G., Preiss, F.-S.: Downstream usage control. In: Proc. 11th IEEE International Symposium on Policies for Distributed Systems and Networks. pp. 22–29, IEEE Computer Society, Washington (2010)
[9] Ma, C., Lu, G., Qiu, J.: An authorization model for collaborative access control. Journal of Zhejiang University - Science C. 11(9), pp. 699–717. (2010)
[10] Wilson, P.: Positive perspectives on cloud security. Information Security Technical Report. 16(3-4), pp. 97 – 101. Elsevier (2011)
[11] Jay, H., Mark, N. Assessing the security risks of Cloud Computing. Technical report, G00157782, Gartner Inc. (2008)
[12] Brown, A. Chase, J. S.: Trusted platform-as-a-service: a foundation for trustworthy cloud-hosted applications. In: Proc. 3rd ACM workshop on Cloud computing security workshop, pp. 15–20. ACM, New York (2011)
[13] Bacon, J., Evans, D., Eyers, D. M., Migliavacca, M., Pietzuch, P., Shand, B.: Enforcing end-to-end application security in the cloud (big ideas paper). In: Proc. 11th International Conference on Middleware, pp. 293–312. Springer-Verlag, Berlin (2010)
[14] Blanc, S., Ducq, Y., Vallespir, B.: Evolution management towards interoperable supply chains using performance measurement. Computers in Industry. 58(7), pp. 720 – 732. (2007)
[15] Rao, P., Lin, D., Bertino, E., Li, N., Lobo, J.: Fine-grained integration of access control policies. Computers & Security. 30(2-3), pp. 91–107, (2011)