Toward Comprehensive Security Policy Governance in Collaborative Enterprise

Ziyi Su, Frédérique Biennier

Toward Comprehensive Security Policy Governance in Collaborative Enterprise

Ziyi SU[1], Frédérique BIENNIER[1]

[1] Université de Lyon. CNRS
INSA-Lyon. LIRIS. UMR5205. F-69621. France
Villeurbanne, FRANCE
{ziyi.su,frederique.biennier}@insa-lyon.fr

Abstract. The lack of trust among software services spanning multiple organisations and the rather poor adaptability level of the current security policies are often seen as braking forces to collaborative-enterprise development. Removing this impediment involves re-thinking the security policy according to "due usage" requirements and setting security enforcement and regulations according to both the due usage and the runtime environment. This paper analyzes the nature of secured assets exchange management in collaborative enterprise, describing the assets sharing patterns and, accordingly, 'sub-context' partition method. Resource protection can be done by applying a 'collaborative usage control policy model' on each 'sub-context' to manage "due usage" control during service/information aggregation. In this way, a compendious but comprehensive security governance for collaborative enterprise is achieved.

Keywords: Security, Policy, Collaborative Enterprise, Negotiation, Aggregation.

1 Introduction

Information sharing is necessary for global optimization in collaborative enterprise. At the same time, new challenges come up for security governance and Information Control Technology. As information is shared beyond ownership boundary, there is always the risk of misuse of sensitive information, e.g. circumventing of trade secret, or even leakage to a competitor through partner. By now the information providers have partial control over sensitive information as it flows beyond organization borders, despite the persistence of protection requirements. Surveys [1, 2] show that risks as 'handling over sensitive data to a third party' are major barriers from moving to collaborative paradigm. Unfortunately, no much attention has been paid on this new requirement in existing security methods, architectures, toolsets or service security architectures: trust assessment [3] methods focus on the 'pre-decision' about selecting partners for business federation, based on historical comportment and the regulation of the partner behavior on the fly in the collaborative business process is traditionally

out of the scope of concern. Security governance in collaborative enterprise needs not only a static trust assessment, but also a policy to express both participants' security requirements and regulations of the partner behavior, detailing "due usage" (namely information consumption actions) control to set a continuous protection of resources even beyond organization boundary and to coordinate requirements to set a consistent protection policy in a (dynamic) business federation.

In former work [4], we brought to light one solution on continuously regulating (define, grant and deny) 'usage' policy upon corporate assets, giving these rights to a partner according to its 'Quality-of-protection'. This involves the expression of security factors ranging from the IT infrastructure to partner behaviour with a Collaboration Security Policy. This paper formalizes the policy model and presents a multidimensional resource protection framework for collaborative enterprise. The process of the collaborative-context security governance with the framework is discussed using a generalized business federation scenario.

2 Context

With the development of collaborative IS, security governance methodologies are developing toward open and collaborative paradigm, leading to the emerging of new security policy models adapting business federation scenarios.

2.1 Security policies for collaborative contexts

Recent security researches are aware of the trends of Internet-based collaborative Network and shifting to such paradigm. At the infrastructure level, the requirement of supporting basic security services as Integrity, Confidentiality and authentication in Internet-based applications with key technologies as encryption, digital signature, etc. is being addressing by recent works [6, 7], aiming at promoting the security level of collaborative software solutions. At the same time, some discussions have emerged to introduce DRM technology to corporate IT management by implementing digital signature and data watermarking to corporate data [8]. These works shed lights on the service/information 'usage control' level governance for collaborative enterprise. However, as traditional risk evaluation methods, security architectures are designed according to a static vision of the information system organisation, they do not fit the dynamicity required by the collaborative and cloud-based XaaS economical model.

On the other hand, security policy models are developing to accommodate Internet-based, multi-services collaborative enterprise. A trend is evidenced as a paradigm changing toward more expressive policy models [9, 10, 11] beyond ACL and RBAC. Even though a comprehensive formal model is still expected, as well as a thorough security-property analysis as that has been done for RBAC, such thought has lead to a enriched policy language as XACML, which grants enriched access right, i.e. the 'usage' (consumption activity) of resource affiliated by obligations [12], that conditioned on multiple-attributes.

Our previous work (see [5] for more detail information) centers on a policy model that defines the access Rights upon the resource thanks to the refined attributes related to requester, resource and infrastructure, as well as obligations fulfilling on the granted rights. Policy is constructed through the logical combination of Assertion, which is a tuple:

$$Assertion = (O, SH, S, CN, R, RN, OB, L, T) \quad (1)$$

where the semantics of the factors are as follows. '**SH**' (Stakeholder) is the owner of the assertion, and is the owner or co-owner of the asset related to the assertion. 'S' (Subject) is the party that can access the Right to the asset. '**O**' (Object) is the asset to be protected by the policy assertions. '**R**' (Right) is the Operation upon the asset defined by 'RH' that the Subject can be allowed to exercise. For example a restriction 'three times' may be used to refine the right 'rendering a piece of multi-media file'. '**CN**' (Condition) is the requirements that must be satisfied for the Subject to access Rights upon the Object. It is related to either *subject attributes (**SAT**), object attributes (**OAT**)* or *context related attributes (**CNAT**)*. '**RN**' (Restriction) is the constraint upon the Right. '**OB**' (Obligation) is the obligation that must be exercised by the Subject when it accesses the Right. '**L**' (Logic Operator) is a set of logic operators as 'imply' ('$\leftarrow$'), 'and' ('$\wedge$') and 'or' ('$\vee$'). '**T**' (Time) is the temporal factor which defines the lifecycle of the rule.

The bidirectional property of trust implicates that a partners is a truster and a trustee at the same time. Thus it uses '*RoP*' assertions to express the 'Requirements of Protection' for its resource and '*QoP*' assertions to declare its security attributes and 'Quality of Protection' for resources it consumes. A temporal factor decorating policy assertions or attribute predicts defines their continuous lifecycles to the scope of beyond direct-requesters.

We can still see a gap between the security requirements of collaborative enterprise and IT management offering. By now, information security grounds mainly on an "instant" protection viewpoint, e.g. the decision to grant resource to customer access and the secured resource delivery channel. Collaborative Security Policy needs to describe not only the security factors from infrastructure level, or access control based on requestor attribute. It should have a "usage control" policy to take care of data even after grant it to partners, so to make continuous cooperating decision that reflecting partners conducts. It should also have a pellucid mechanism supporting coordination of policies from multiple partners, adapting to the complexity and dynamicity of collaborative context security governance.

2.3 Collaborative context management

A collaborative enterprise reveals its global scale 'quality-of-protection' as the aggregation of *QoPs* from the participants. It is also entitled with a consistent, accept-by-all security policy, which roots in the *RoPs* from individual partners, providing global scale protection to their assets. Due to the dynamicity of collaboration strategy, the global scale *QoP* and *RoP* set are updated on-the-fly as new partners join and quit, so to reflect security properties/requirements from current participants as well as global scale protection level and requirements. Collaboration context management involves a

security policy update mechanism, which relies on the analysis of collaboration strategy. For example, the study of security policy interoperability in Virtual Organization [9] enables a subject to access privileges defined in another organization. The Federated Rights Expression Model [8] permits a content provider to trust external render rights. In IT infrastructure level, authors of [13] studied the reliable configuration of security policies from multiple components. A multi-organizational policy modeling mechanism is presented [10] that takes into consideration the business context characteristics, whereas the analysis of business components dependency [14, 15] sheds light on confinement to information access based on service composition, which greatly impacts the protection approach. In spite of such fruitful works, our 'usage control' view upon business federation involves a more in depth analysis of information assets consumption than those presented above.

3 Collaboration context management based on assets-sharing relation

The artifact of collaboration context (called 'C-Asset', i.e. 'C-Asset2' in fig. 1), can comprise information assets from multiple providers (called 'O-Asset', e.g. 'O-Asset1', 'O-Asset2' and 'C-Asset1' in fig. 1).

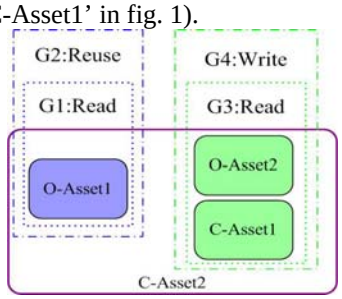

Fig. 1. Information Asset aggregation and Rights aggregation.

Two traits can be observed regarding the aggregating process of *RoPs* from these providers. Firstly, if the asset from an individual provider can be separately identified in the collaboration artifact (e.g. inventory information from multiple up-stream providers, stock information from multiple brokers, financial-year report from different subsidiaries, etc.), the due *RoP* don't need to be aggregated. When a use of access a part of the artifact, it needs only to comply to the *RoP* relating to due part.

Secondly, if a provider defined different rights upon its assets, a consumer only needs to follow the part of the policy that concerns its rights upon the asset. An example is when a company defines a piece of data (e.g. price) available for anyone to access but only supply chain partner can modify it. Then a user only need to exhibit appropriate attributes in order to exercise different usages upon the data.

Thanks to this two observations, we can 'split' a collaboration context into several virtual 'sub-contexts' according to different resource aggregation and different consumption rights upon them:

- *Providers for the same C-Asset are deemed as the same 'sub-context'.*

- *All consumers having the same 'rights' upon the C-Asset(s) are deemed as in one 'group'.*
- *A participant can belong to more than one sub-context at the same time. it must follow the RoP of that sub-context.*

Four sub-context patterns can be identified according to these principles. We use a sample supply chain scenario with several information flows to describe each case:

- **EAOG** (Each Asset One Group) mode indicates the situation when each provider can differentiate its resource in the artifact of federated Business Process. In this model each provider attaches its policy to its due part (the O-Asset) in the resulting C-Asset. Future consumers just need to obey the due policy of the part it will request. A sample (see fig. 3) is when a down-stream provider (D) receives information 'Ia…In' (e.g. inventory) from upstream provider (UP) and combines them in one XML file 'I' as separate nodes, Manufactory (M) reads the nodes separately, and follows the due policy of UPs.

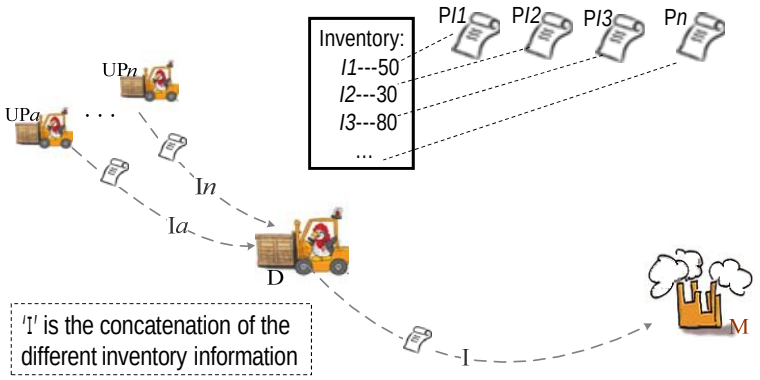

Fig. 3. Sample of **EAOG** mode.

- **SASG** (Single Asset Single Group) mode is that all the consumers are given the same rights upon the artifact and thus is in one single group. The aggregation process should make sure there is no potential contradiction among *RoPs* of all the providers and *QoPs* of all the consumers. A sample of this mode (see fig. 4) occurs when (other information) 'C0a…C0n' (e.g. productivity) are blurred by 'D' to generate 'C4' (e.g. scheduling).

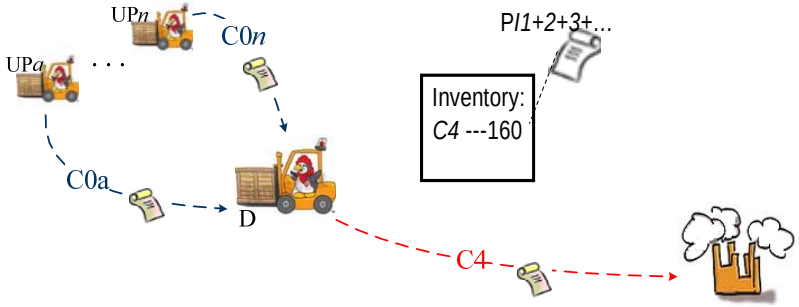

Fig. 4. Sample of **SASG** mode.

- **SAMG** (Single Asset Multiple Group) mode means that there is only one single C-Asset, with different rights defined on it. Then consumers of different rights are deemed as in different groups. In other words, consumers accessing different rights need only to fulfill the due condition of that right. Fig. 5 shows such a sample case where D blurs information (C5), and aggregates UPs' policies to different CSPs, which are accessed by different down-stream partners 'Da…Dn'. By managing each 'right' and due 'condition' separately, the opportunity for finding adequate consumer increase, less privileged rights usually require less rigorous conditions.

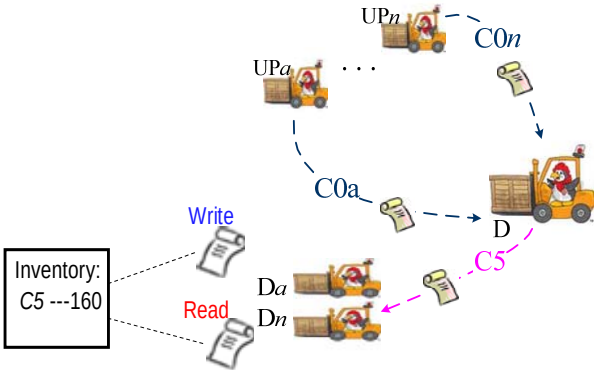

Fig. 5. Sample of **SAMG** mode.

- **MAMG** (Multiple Asset Multiple Group) mode denotes when the artifact can be differentiated as sub-parts, e.g. when there are parallel branches in the business process and some branches will not merge with others till the end of process. A sample of this mode (see fig. 6) denotes if D splits a piece of information (e.g. to C1, C2 and C3) and some pieces (e.g. C3) do not merge with others in future steps.

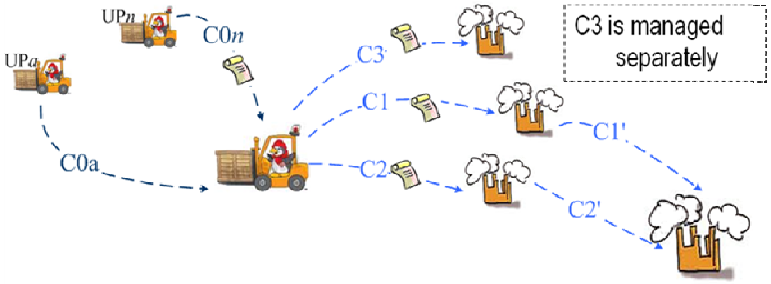

Fig. 6. Sample of **MAMG** mode.

These 4 patterns generally exist in many collaborative contexts, as long as the issue of information asset protection and consumption exists. Imagining changing the sample case by switching the materials providers as Cloud providers or Service providers, the security management approaches still generally fall in our framework, with technical solution possibly variable.

4. Sub-context participation

We can see now that the key issue is to identify the asset exchanging relations between partners. Analysis of the 'Initial example' in 'WS-BPEL 2.0 specification' sheds lights on how this is done.

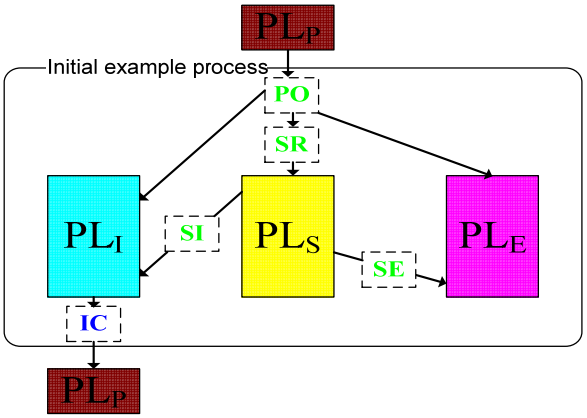

Fig. 7. Information exchanges in the 'Initial example'.

This process receives an asset 'purchase order' (PO) from 'PartnerLink purchasing' (PL_P), then initiate three parallel processes (with temporal dependency defined by 'links'):

- Shipping: Assigning value from variable 'PO' to 'ShippingRequest' (SR), then calling 'PartnerLink shipping' (PL_S) with 'SR' and getting two feedbacks 'ShippingInfo' (SI) and 'ShippingSchedule' (SE).
- Calculating price: Calling 'PartnerLink invoicing' (PL_I) with 'PO' and 'SI', getting a feedback 'Invoice' (IC).
- Scheduling: Calling 'PartnerLink scheduling' (PL_E) with 'PO' and 'SE'.

When these parallel processes terminate, the 'IC' is sent to 'PL_P' as response.

In these processes, security policy/profile negotiations take places between partners having asset exchange relation. Besides, when assets merge (e.g. in 'Calculating price' process, see fig. 8), security policies of providers should aggregation. The resulting policy reflects the security goals of both providers. In other words, if the resulting policy is fulfilled by a consumer, the original policies are also fulfilled.

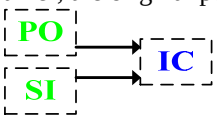

Fig. 8. Information aggregation in the 'Initial example'.

5. Conclusion and Future Work

This paper describes a comprehensive security policy governance method in collaborative enterprise, based on asset sharing relations between partners. Therefore, only

partners who are exchanging assets should have their security policies and profiles compatible, namely, the consumer's security profile fulfilling the provider's policy.

Deciding asset merging requires a more information about the business logic of partners ('PL_I' in above example). A natural thought would be adding annotations to partners descriptions, e.g. WSDL scripts.

Acknowledgements: This work is partly supported by the Process 2.0 process granted by the French Ministry of Economy and Industry – DGCIS.

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] Jay H., Mark N.: Assessing the security risks of Cloud Computing. Technical report, Gartner (2008).

[3] Biennier F., Aubry R., Maranzana M.: Integration of Business and Industrial Knowledge on Services to Set Trusted Business Communities of Organisations. IFIP Advances in Information and Communication Technology, vol. 336/2010, pp. 420-426, Springer (2010).

[4] Su Z., Biennier F. , 2010. End-to-end Security Policy Description and Management for Collaborative System. In: Proc. IAS 2010, pp. 68-73 (2010).

[5] Ziyi Su and Frédérique Biennier. End-to-end security policy description and management for collaborative system. In: Proc. IAS 2010, pages 137 – 142. MIR lab, 8 2010.

[6] Paci F., Bertino E., Crampton J.: An Access-Control Framework for WS-BPEL. Int. J. Web Service Res. Vol 5, pp. 20-43. IGI global (2008).

[7] Martino L., BertinoE.: Security for Web Services: Standards and Resarch Issues. Int. J. Web Service Res. 6, 48-74 (2009).

[8] Sans T., Cuppens F., Cuppens-Boulahia N.: FORM: A Federated Rights Expression Model for Open DRM Frameworks. In: Proc. ASIAN 2006. LNCS, vol 4435, pp. 45-59. Springer (2007).

[9] Cuppens F., Cuppens-Boulahis N., Coma C. 2008. O2O: Virtual Private Organizations to Manage Security Policy Interoperability. In: Proc. ICISS 2006. LNCS, vol 4332, pp. 101-115. Springer (2006).

[10] Cuppens F., Cuppens-Boulahis N., 2008. Modeling Contextual Security Policies. Int. J.Inf. Secur. 7, 285-305(2008).

[11] Wang L., Wijesekera D., Jajodia S.: A logic-based Framework for Attribute Based Access Control. In: Proc. FMSE 2004, pp.45-55. ACM, New York (2004).

[12] Organization for the Advancement of Structured Information Standards (OASIS): eXtensible Access Control Markup Language (XACML) version 2.0. OASIS (2005).

[13] Alfaro J.G., Cuppens-Boulahia N., Cuppens F.: Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies. Int. J.Inf. Secur. 7, 103-122 (2008).

[14] Kheir N., Debar H., Cuppens F., Cuppens-Boulahia N., Viinikka J.: A Service Dependency Modeling Framework for Policy-Based Response Enforcement. In: Proc. DIMVA 2009. LNCS, vol. 5587, pp. 176-195. Springer (2009).

[15] Debar H., Kheir N., Cuppens-Boulahia N, Cuppens F.: Service Dependencies in Information System Security. In: Proc. MMM-ACNS 2010. LNCS, vol. 6258, pp. 1-20. Springer (2010).