ADAPTIVE SECURITY POLICY MODEL TO DEPLOY BUSINESS PROCESS IN CLOUD INFRASTRUCTURE

Wendpanga Francis Ouedraogo[1], Frédérique Biennier[1] and Parisa Ghodous[2]
[1]*Université de Lyon, CNRS INSA-Lyon, LIRIS UMR 5205, 20 Avenue Albert Einstein 69621, F-69621 Villeurbanne cedex, France*
[2]*Université de Lyon, CNRS Université Claude Bernard Lyon 1, LIRIS UMR5205, 43 Bd du 11 novembre, 69622 Villeurbanne cedex, France*

Keywords: Cloud Computing, Business Process, Risk Analysis Model, Security Model.

Abstract: The development of collaborative service ecosystem relies mostly on software services spanning multiple organisations in order to provide agile support for business applications. By moving part of their information system on Cloud infrastructure, companies take advantage of new Business models and scalable environments, increasing IT productivity while reducing IS management costs. Nevertheless, this underlying outsourcing strategy may be braked by a lack of security and trust on this new infrastructure model as traditional security engineering and deployment methods are not designed for such an agile and opened environment. To overcome this limit, we propose a multi-dimensional model integrating both the cloud level (XaaS) and the cloud characteristics (Private, public, hybrid) to generate convenient security policy in a dynamic way. Based on security patterns, our multi-dimensional solution has been implemented to capture security requirements related to both information system design and runtime environment.

1 INTRODUCTION

To fit the renewed globalised economical environment, enterprises, and mostly SMEs, have to develop new networked and collaborative strategies. This involves increasing the IT support agility and interoperability and allowing end-users to build collaborative Business Process (BP) to "inter-connect" the different partners' information systems. This challenges both BP design and "functional and organisational" security requirements identification before deploying them.

At the same time, cost management strategies, coupled to opportunities provided by the XaaS and cloud economical models, often lead to set IT outsourcing strategies taking advantage of scalable environments. This outsourcing strategy also challenges security policy adaptation according to the "hosting platform" vulnerabilities.

To fit both challenges, the PROCESS 2.0 project (Process 2.0, 2010) aims at building a collaborative platform to allow end-users to model their business processes by composing business services before deploying them on a cloud infrastructure. In this paper, we propose a model-driven approach integrating a "functional and organisational" security requirements and platform related security constraints to set dynamically contextualised security policies.

After introducing the context and state of the art, we present our approach to organise security patterns and build security policies in order to provide an adapted Quality of Protection for distributed Business Processes.

2 RELATED WORK

The openness and flexibility provided by the Web 2.0 involves re-thinking the information system organization. The benefits offered by the web 2.0 allow moving from a global enterprise engineering strategy as proposed in methods such as ARIS (Architecture of integrated Information) (Scheer, A., Nüttgens, M., 2000) to more agile, interoperable and flexible Business Process support, taking advantage of Workflow management frameworks. Such an approach increases end-user involvement and involves improved "connections" to traditional information systems components (ERP, PLM…),

Francis Ouedraogo W., Biennier F. and Ghodous P..
ADAPTIVE SECURITY POLICY MODEL TO DEPLOY BUSINESS PROCESS IN CLOUD INFRASTRUCTURE.
DOI: 10.5220/0003929202870290
In *Proceedings of the 2nd International Conference on Cloud Computing and Services Science* (CLOSER-2012), pages 287-290
ISBN: 978-989-8565-05-1

Table 1: Cloud deployment model and the challenge in each kind of cloud.

	Definition	Challenges for data storage and confidence on the data.
Private Cloud	The cloud belongs to a single company and can be managed by the enterprise itself (internal Private Cloud) or a third party (external private cloud).	Confidentiality and integrity of the data should be guaranteed as for classical IS implementation. The third party is responsible of the consequences of any damages.
Public cloud	The infrastructure is offered to anybody and is owned by an independent organization selling cloud services.	Ensure isolation of data for each customer and ensure that confidentiality and integrity of the data are guaranteed. Ensure also that the application of territorial laws (Sinclair, J., Hudzia, B., Lindner, M., 2011) (e.g.: US Patriot Act), won't compromise data confidentiality.
Community Cloud	The infrastructure is shared by several companies sharing same concerns.	As companies don't have the same security requirements, the challenge here is to enforce the security policies of each company.
Hybrid Cloud	The infrastructure consists in two or more types of Cloud that remain unique entities but are bound together by standardized or proprietary technology.	Combination of the different challenges that can be found in the others clouds.

taking advantage of interoperability and flexibility provided by Service Oriented Architecture (SOA). Within SOA strategy, corporate activities and Business Processes are supported by selecting, composing and orchestrating services depending on the needs. To fit the required openness and interoperability, BPMN (Business Process Modelling Notation) is mostly used to build and integrate executable services. Nevertheless, this standard does not support security aspect. This leads (Rodriguez, A., Fernandez-Medina, E., Piattini, M., 2007) to propose a BPMN extension that allows incorporating security requirements into business process diagram. (Mülle J, von Stackelberg S, Klemen A., 2011) also propose a new security language for BPMN process models. Nevertheless these basic needs must be adjusted to fit the corporate global security policy and pay more attention on vulnerabilities and threats analysis.

Different methods can be used to set a consistent security policy, based on vulnerability and threat models such as EBIOS (ANSI, 2004), MEHARI (CLUSIF, 2010), and OCTAVE (Alberts, C., Dorofee, A., Stevens J., Woody C., 2003). However, they are quite complex to implement so that expert are required, don't fit the "dynamicity" required by the changing collaborative context nor provide any security patterns adapted to Cloud-based deployment.

Indeed, cloud computing provides new opportunities to support agile and flexible deployment allowing sharing resources and taking advantage to XaaS business models. Depending on who owns the cloud and how the infrastructure information system components are shared ("virtualisation level"), different security challenges can be identified (see Table 1). To fit these security challenges, Jericho Forum (Cloud Cube Model, 2009) has developed a cloud security cube model that allows companies to choose the type of cloud that is adapted to their business needs. Nevertheless this work doesn't integrate the XaaS dimension and is not "end-user" oriented.

This leads to "rethink" both Business Process models in security architecture according to Cloud and XaaS visions.

3 A SECURITY POLICY GENERATION FRAMEWORK

In order to allow end user to build their own processes, deploy them on a cloud infrastructure before running them safely without requiring an IT specialist intervention, the Process 2.0 project proposes a design studio modelling Business Processes as a service chain, selecting and composing services from a shared repository before customizing them with an adapted security policy. To this end, we propose to use a Model-Driven Engineering approach to identify security requirements, define an adapted Quality of Protection and generate adapted security policies, paying attention on the deployment platform. Different meta-models (related to process, security means, platform organisation…) are used so that security patterns are selected and combined with the basic process to generate both the requested security policies and the secured services (Figure 1).

3.1 Model Driven Security Engineering Method

As shown in Figure 1, the Process 2.0 framework includes 3 steps:

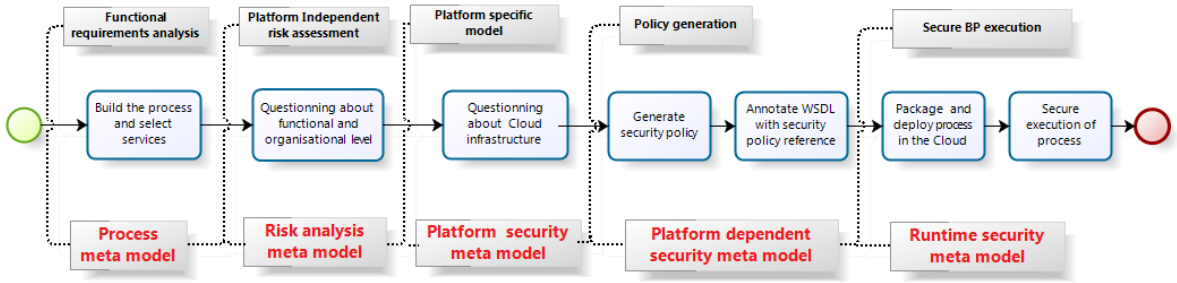

Figure 1: Process 2.0 Design framework and its connection to the runtime environment.

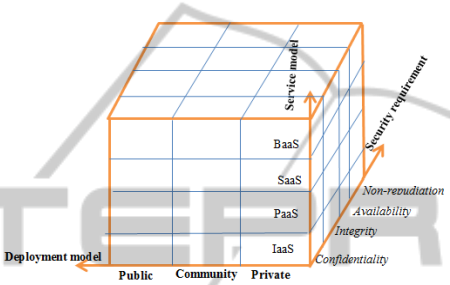

Figure 2: Platform model.

- **Functional requirements analysis**
  allows designing the process workflow as a set of interconnected activities defined by BPMN. These activities are supported by services which are defined by WSDL.
- **Platform Independent risk assessment**
  is performed on the workflow specification. Our risk meta-model consists in a set of questions/answers to analyse the different assets (process, services, attached data) according to the following two steps:
  - *Functional security* deals with "legal constraints" (regarding personal data) and patrimonial value" (and the non-security costs) of the different assets.
  - *Organisational security* refers to the process organisation (namely the actors and their role identification). This allows identifying the impact of access control features and is also used to identify the way users will access to the application (on site / remote / mobile).

  These steps are used to create a Platform Independent Security Policy: depending on the questions/answers, security patterns are selected and security tags (related to basic security services taken from the OASIS security model (OASIS, 2009) and protection level) are inserted in the WSDL specification.
- **Platform specific model**
  is used to integrate constraints related to the Cloud deployment model. Based on the security challenges we identified in the Related Work Section, we build a Platform Dependent Cloud Security model. This vision incorporates both contextual management of non-functional properties (safety and quality of service) and management interfaces for specific data access. Risks and Security Patterns are identified in a 3 dimension model; paying attention on the basic security service introduced in the OASIS model, the Cloud model and the Virtualisation (XaaS) level (figure 2). A set of questions / answers is used to identify the deployment configuration pattern according to this multi-dimensional model.

3.2 Policy Generation

The Contextual Security Policy is used to describe the risk mitigation measures that must be implemented according to both the protection requirements and the particular vulnerabilities related to the platform model. Consequently, we first parse the security tags added in the service initial WSDL and combine them with the selected platform dependent pattern to identify the security components implementation patterns associated to either data or services regarding, trust management,

operation execution of storage needs (figure 3)...Thanks to these implementation patterns identification, the platform independent tags are turned into real security tags according to the priority level associated to each requirement. Each tag refers to security policy files to apply.

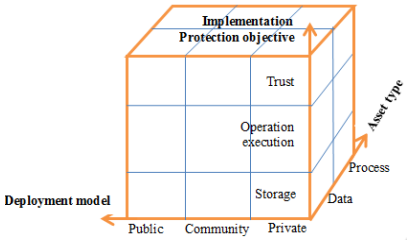

Figure 3: Cloud model security requirement.

3.3 Secure BP Execution

In order to run safely the service workflow, we introduce a security mediator which parses the service WSDL and the associated policy files. The security policy XML file is analyzed and used to invoke security components implemented as web service (security services):

- **Availability manager**: it offers the possibility to access to another clone of the service if the request service is unavailable or does not fit the QoS requirements.
- **The integrity manager**: it allows ensuring the integrity of data during the message exchange.
- **The confidentiality manager**: it includes an authentication service (used to identify the users), an authorization service that control access to data and services, a privacy manager that manages the service/data storage by encrypting them.
- **The non-repudiation manager**: it records the users actions (authentication, access to the service, deleting of data…).

By this way, the security mediator deploys secured services which encapsulate the business services and ensure data security and the security exchange between the service and the client. This mechanism allows providing a secure execution environment for services that are initially devoid of security mechanisms.

4 CONCLUSIONS

To fit the openness, interoperability and agility levels requested for collaborative business, the Process 2.0 project proposes to organize a collaborative process design environment based on service composition. This design studio pays attention to security requirements before deploying the secure BP on the cloud.

In this paper we present our model driven approach to define security requirements and generate contextual security policies depending on the hosting cloud characteristics. Based on security patterns selected thank to questions/answers, ours solution allows a fast security reconfiguration according to the hosting platform. Further works will focus on the propagation of the security policies and detection of conflicts between the policies in order to ease the security specification process.

ACKNOWLEDGEMENTS

This work is partly supported by the Process 2.0 process granted by the French Ministry of Economy and Industry – DGCIS, gathering research work from INSA, INRIA- Merlin, Genigraph and EBM Websourcing.

REFERENCES

PROCESS 2.0 project, 2010. http://research.petalslink.org/display/process20/Process+2.0+Overview.

Scheer, A., Nüttgens, M., 2000. *ARIS Architecture and Reference Models for Business Process Management*, Springer-Verlag London, UK.

Rodriguez, A., Fernandez-Medina, E., Piattini, M., 2007. *A BPMN extension foe the modelling of security requirements in business processes the institute of electronics*, Information and Communication Engineers (IEICE), Vol.E90-D, NO.4.

Mülle J, von Stackelberg S, Klemen A. 2011. *Security Language for BPMN Process Models*, Karlsruhe institute of technology, Germany.

ANSSI, 2004. *Expression des besoins et identification des objectifs de sécurité. la démarche "* France.

Club de la sécurité de l'Information Français (CLUSIF), 2010. MEHARI 2010. *Guide de la démarche d'analyse et de traitement des risques*, France.

Alberts, C., Dorofee, A., Stevens J., Woody C., 2003. *Introduction to the OCTAVE Approach*, Carnegie Mellon University, Pittsburgh.

Cloud Cube Model, April 2009, *Selecting Cloud Formations for Secure Collaboration*, Jericho Forum.

Sinclair, J., Hudzia, B., Lindner, M., 2011. "*Architecture for compliance analysis of distributed service based systems*". The first International Conference on Cloud Computing and Services Science, CLOSER 2011 Belfast, Northern Ireland, U.K.

Organization for the Advancement of Structured Information Standards (OASIS), 2009. OASIS: *Reference Architecture Foundation for Service Oriented Architecture*, Version 1.0, pp. 96-102.