OPBUS: RISK-AWARE FRAMEWORK FOR THE CONFORMANCE OF SECURITY-QUALITY REQUIREMENTS IN BUSINESS PROCESSES

A. J. Varela-Vaca, Rafael M. Gasca and Sergio Pozo
Computer Languages and Systems Department (Quivir Research Group), ETS. Ingeniería Informática, University of Seville
Avd. Reina Mercedes S/N, Seville, Spain
{ajvarela,gasca,sergiopozo}@us.es

Keywords: Business process management, Risk assessment, Security.

Abstract: Several reports indicate that one of the most important business priorities is the improvement of business and IT management. Nowadays, business processes and in general service-based ones use other external services which are not under their jurisdiction. Organizations do not usually consider their exposition to security risks when business processes cross organizational boundaries. In this paper, we propose a risk-aware framework for security-quality requirements in business processes management. This framework is focused on the inclusion of security issues from design to execution. The framework provides innovative mechanisms based on model-based diagnosis and constraint programming in order to carry out the risk assessment of business processes and the automatic check of the conformance of security requirements.

1 INTRODUCTION

In the recent years, a new paradigm has receviced considebrable attention in the scope of business IT: Business Process Management (BPM). BPM is defined as a set of concepts, methods and techniques to support the modelling, design, administration, configuration, enactment and analysis of business processes (Weske, 2007).

Gartner's CIO report (Gartner, 2010) indicates that the security is included in the most important business priorities. Security and risk management is gaining importance even in the governmental statements, where there exists some regulations and laws which impose the inclusion of risk and security management inside of business management, like OECD Guidelines (ENISE, 2010).

Companies may deploy Business Process Management Systems (BPMS) to automate their business processes, but they must ensure that those are as dependable as possible. Since the cost and consequences of security failures in these systems range from mildly annoying to catastrophic, dependability is a significant requirement for many kinds of companies: electronic banking and commerce, automated manufacturing, etc.

This paper intends to introduce a proposal risk-aware BPM framework, entitled OPBUS. At modelling level, OPBUS adopts an extension of business process models with security risk assessment capabilities, and also includes mechanisms to check automaticaly the conformance of risks of business processes. Moreover, OPBUS provides mechanisms to transform the business process models to deployable processes considering the security issues identified at design.

This paper is structured as follows: in Section 2, OPBUS architecture is described; in Section 3, the application of model-based diagnosis for risk assessment of business processes is introduced; in Section 4, a review of the most relevant works related with this paper is done; in the last section, conclusions are given.

2 OPBUS: ARCHITECTURE OVERVIEW

Our proposal is structured in various layers:

- *Modelling Layer*, where business processes are designed, validated and transformed.
- *Application Layer*, a set of technologies to support the deployment, diagnosis and deployment of business processes.

- *Fault Tolerance Layer*, different solutions have been adopted for high availability of business process execution (Varela, 2010).
- *Service Layer*, service-based business processes has been selected as implementation thereby service layer represent to the set of services used by business processes.

OPBUS framework has been developed based on the Model-Driven approach proposed by the authors in (Varela, 2011). The approach is structured in at least three stages. In the first stage, Platform Independent Meta-Model (PIM) models are built. Thus, abstract business process models. Then a first transformation between a PIM to Platform Specific Meta-Model (PSM) models is proposed. In this transformation, extra information is introduced in terms of information of a more specific nature information on mechanisms to control or mitigate security problems. For instance, fault tolerance mechanisms to avoid security integrity attacks. Although other intermediate transformations can be introduced between PSM and other PSM models, as a first approach, a transformation from PSM models to final code is proposed. For example, if a countermeasure is specified at PSM level such a particular fault tolerance control. This control can be transformed to a specific configuration of BPEL business processes. A particular diagnosis stage is introduced for the validation of models before each transformation.

Currently, Business Process Management Notation (BPMN) is the most extended modelling method in the BPM market. BPMN provides a meta-model that could be used as a PIM of our framework since makes possible the definition of complex business processes, but without considering specific issues such as execution or security configurations. Furthermore, they lack of mechanisms for the evaluation and validation of their security and risks before to be implemented. In an earlier work (Varela, 2011), an extension of BPMN with risk information has been proposed. The extension permits to assess the risks which the business processes are exposed to due to security threats and vulnerabilities. In general, the risk assessment is a tedious and time-consuming task for several reasons, one of which is due to the manual feature of the process, a subjective valuation of the different elements and the possibility of having to support different kind of valuations such as interval values. The utilization of the diagnosis stage is suggested in order to the automatic risk assessment and check the conformance of these risks. In OPBUS, this diagnosis of conformance stage is solved using constraint programming.

3 MODEL-BASED DIAGNOSIS OF CONFORMANCE

The risk calculation involves three main parameters: an asset value, a threat frequency and consequence. This risk value permits business security experts the identification of critical tasks based on their values.

$$Risk = AsseValue * Frequency * Consequence$$

A risk can be evaluated with regard to each task, treatment, and threat identified in the business process. Therefore, in our case the risk calculation is, in general, calculated as follows.

$$Risk = \sum_{p \in Threats} \left(AssetValue * \sum_{q \in Treatments} \left(\begin{matrix} (Frequency_p - Frequency_p * RR_q) * \\ (Consequence_p - Consequence_p * RR_q) \end{matrix} \right) \right)$$

This last formula is similar to the one used in ISO/IEC 27004. The formula calculates the risk assessment for an individual task of a business process. However, calculating risk for a business process (BP) is carried out by means of the combination (summation) of the risks calculated for each individual task. In the case business processes contain divisions of the flow path; the previous formula cannot be used since risk assessment is influenced by the structure of the business process. For this reason, risk has to be calculated for each path. This problematic has never been considered in other works. We propose the risk calculation as shown in Figure 1 which shows how to calculate the risk of a business process with regard to the structure of the model. These risk formulas are an adaptation of the time-efficiency calculation proposed by (Huang, 2007). In the case of loops, the risk calculation is not affected since the set of activities execute in the loop is the same for each iteration.

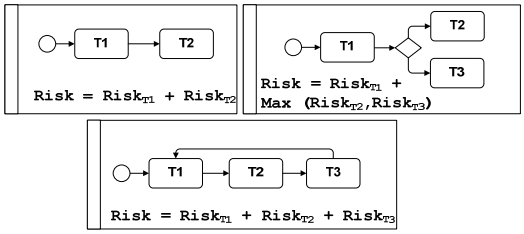

Figure 1: General risk calculation formula.

Once risk values are obtained for each business process, they have to be evaluated in conformance with the specified acceptable risk. If a business process exceeds the specified acceptable risk (*Acceptable Risk*) value implies that there exist risks

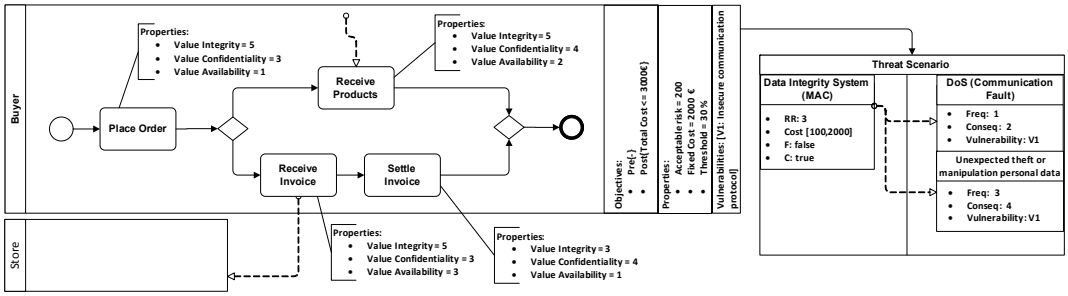

Figure 2: Business process extended with risk information.

that do not comply with the security objectives.

$$\forall\, p \in BP \rightarrow Risk_p \leq AcceptableRisk_p$$

At the same time, a cost assessment is carried out where the cost of a business process is calculated with the sum of the fixed cost and the cost of treatments identified. The main idea is to check the conformance of costs of the business process do not exceed to certain limits. In the formula below there is an initial criterion applied for the cost assessment but other ones can be adapted.

$$\forall\, p \in BP \rightarrow \left(TotalCost_p \geq Cost_p \wedge Cost_p \in \left[FixedCost - \frac{FixedCost * Threshold}{100}, FixedCost + \frac{FixedCost * Threshold}{100} \right] \right)$$

a. Diagnosis Conformance Stage

OPBUS provides a set of transformation rules which permits the mapping of risk information to a constraint model, as shown in Figure 3.

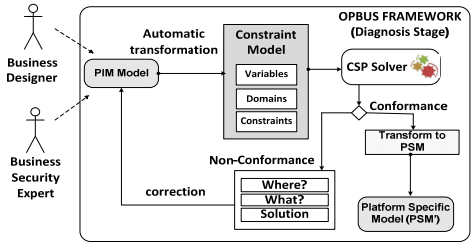

Figure 3: Diagnosis of business processes.

Automatically, the constraint model can be evaluated and if it shows unsatisfying results, then this indicates that there exist risks that are not being mitigated or avoided. It can also be useful to identify where and what components are unsatisfying the constraints in order to act providing which business process elements are involved in the not satisfactibility.

b. Example of Mapping to Constraint Model and Diagnosis

An example of mapping to a constraint model and diagnosis of conformance based on the example of the Figure 2 is shown. First of all, a set of variables and domains which compose the constraint model are defined. Most of parameters included in the extension are mapped to variables in the constraint model. Two variables for each task that composes the business process have to be defined. The first one defines its value in relation with security parameters (*Integrity*, *Confidentiality* and *Availability*). The second one defines the risk value that is defined with open domain because its value is unknown when the constraint model is under construction and it will be assigned values in the resolution of the constraint model. In next piece of code, there are statements for the variables of *Place Order* activity is shown.

int PO=ValueIntegrity+ValueConfidentialy+ValueAvailability;
var<CP>{int} RiskPO(manager,1..100000);

Similar variables are defined for treatment and threat parameters.

```
85 //Risk
86 manager.post(Risk_store == (Riskplaceorder +
   max(Riskreceiveinvoice, Riskreceiveproducts + Risksettleinvoice) -
   (Riskplaceorder + max(Riskreceiveinvoice, Riskreceiveproducts +
   Risksettleinvoice))*t1_riskreduction/100), onBounds);
87 manager.post(Riskplaceorder == (Vplaceorder * R1Frequence *
   R1Consequence + Vplaceorder * R2Frequence *
   R2Consequence),onBounds);
88 manager.post(Riskreceiveinvoice == (Vreceiveinvoice * R1Frequence *
   R1Consequence + Vreceiveinvoice * R2Frequence *
   R2Consequence),onBounds);
89 manager.post(Riskreceiveproducts == (Vreceiveproducts * R1Frequence
   * R1Consequence+ Vreceiveproducts * R2Frequence *
   R2Consequence),onBounds);
90 manager.post(Risksettleinvoice == (Vsettleinvoice * R1Frequence *
   R1Consequence + Vsettleinvoice * R2Frequence *
   R2Consequence),onBounds);
91 manager.post(RC2 == (AcceptedRisk >= Risk_store),onBounds);
92 //Cost
93 manager.post(RealCost == (Fixed_cost + t_cost_t1 ), onBounds);
94 manager.post(RC4 == (RealCost >=
   (Fixed_cost-(Threshold_cost*Fixed_cost/100))),onBounds);
95 manager.post(RC5 == (RealCost <=
   (Fixed_cost+(Threshold_cost*Fixed_cost/100))),onBounds);
96 manager.post(RC3 == (RealCost <= Cost), onBounds);
```

Figure 4: Set of constraints.

The constraint model is defined by an objective function. The objective function aims are the evaluation of the risk assessment and check that the risks and cost calculated are in conformance with the objectives of acceptable risk and cost specified. Therefore, the set of constraints that compose the model are two: the first for the risk calculation, and the second for the evaluation of the conformance. Constraint evaluation could retrieve one solution

with the best results or all possible solutions and extra information about value of the parameters. In this case, we have selected a type of search in order to obtain all possible solutions since it is more interesting observe different cases with assignation of variables and values. In the

Table 1, we show two examples of solutions found by the resolution of the constraint model using a constraint solver. One with positive results where all constraints are satisfied and the other with negative results where at least one constraint is not satisfied.

Table 1: Results of the evaluation of constraint model.

CASE 1	CASE 2
Constraints	
RC1 = false; RC2 = true RC3 = true; RC4 = true	RC1 = true; RC2 = true RC3 = true; RC4 = true
Acceptable Risk	
Acceptable Risk = 200	Acceptable Risk = 200
Risk Variables	
Risk_store=903 Riskplaceorder=270 Riskreceiveinvoice=240 Riskreceiveproducts=330 Risksettleinvoice=330	Risk_store = (188)[9..196] Riskplaceorder=270 Riskreceiveinvoice=240 Riskreceiveproducts=330 Risksettleinvoice=330
Treatment Variables	
t1_riskreduction = 3	t1_riskreduction= (21)[79..99]
Cost Variables	
Cost=(101)[2100..2200] Total Cost = 3000 Cost_treatment=(101) [100..200]	Cost=(101)[2100..2200] Total Cost = 3000 Cost_treatment=(101) [100..200]

4 RELATED WORK

There exist different proposals of extensions of business processes with risk information and non-functional requirements (Korherr, 2007) (Lambert, 2006), (Jakoubi, 2009), (Menzel, 2009), (Muhelen, 2005), (Cope, 2010). Most of them only pay attention in the modelling of risk information or requirements but do not include mechanism for the automatic evaluation of the risk assessment and the diagnosis of the conformance of the objectives of the business process. Moreover these proposals do not consider the transformation of the requirements to specific artefacts in the implementation level. Other works (Menzel, 2009), (Wolter, 2009) consider the introduction of new elements in order to annotate BPMN diagrams with parameters which are transformed into a specific security configuration of a server.

5 CONCLUSIONS

In this work, an overview of the OPBUS architecture has been presented. OPBUS has been extended with a MDA approach that provides an extension of BPMN models with risk information. We propose to include constraint programming techniques in order to automate the checking of conformance of the risk assessment of business processes. For this reason we have presented a mapping to constraint models. Once business process are validated the countermeasures identified in design stage of business processes can be aligned with specific control in next layers, for instance with specific fault tolerance mechanism already included in OPBUS framework.

ACKNOWLEDGEMENTS

This work has been partially funded by Consejería de Economía, Innovación y Ciencia of the Regional Government of Andalusia project under grant P08-TIC-04095, and by Spanish Ministerio de Ciencia e Innovación project under grant TIN2009-13714, and by FEDER (under ERDF Program).

REFERENCES

Cope E. W., Kuster J. M., Etzweiler, D., Deleris , L. A., and Ray B., "Incorporating risk into business process models," *IBM Journal of Research and Development*, vol. 54, no. 3, pp. 4:1 –4:13, 2010.

ENISE, *"Integration of Risk Management with Business processes"*. Available at: http://www.enisa.europa.eu/act/rm/cr/business-process-integration. 2010.

Gartner Inc., *"Gartner CIO report,"* Available at: http://www.gartner.com/it/page.jsp?id=1283413, 2010.

Model-Driven Architecture, Available at: http://www.omg.org/mda/

S. Huang, Y. Chu, Shing-Han Li, D. C. Yen, Enhancing conflict detecting mechanism for Web Services composition: A business process flow model transformation approach, *Information and Software Technology*, Vol. 50, pp. 1069-1087, 2008.

Jakoubi, S. and Tjoa, S., "A reference model for risk-aware business process management," *4th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2009, pp. 82 –89, 2009.

Korherr B. and Beate List, "Extending the EPC and the BPMN with Business Process Goals and Performance Measures", *International Conference on Enterprise Information Systems*, 2007.

Lambert, J. H., Jennings, R. K., and Joshi N. N., "Integration of risk identification with business process models*," Syst. Eng*., vol. 9, no. 3, pp. 187–198, 2006.

Menzel, M.; Thomas, I.; Meinel, C., "Security Requirements Specification in Service-Oriented Business Process Management," *ARES '09*, pp.41-48, 16-19 2009.

Muehlen M. and Ho D. T.-Y., “Risk management in the bpm lifecycle,” in *Business Process Management Workshops*, pp. 454–466, 2005.

Van Hentenryck P.,“Constraint programming,” in *Proceedings of the 5th International Conference on Evolutionary Multi-Criterion Optimization*, *ser. EMO ’09*. Berlin, Heidelberg: Springer-Verlag, 2009.

Varela-Vaca A. J., Gasca R.M., Diana Borrego, Pozo S., "Towards Dependable Business Processes with Fault-Tolerance Approach,” *3rd International Conference on Dependability (DEPEND)*. Venecia, Italy. ISBN 978-0-7695-4090-0, 2010.

Varela-Vaca A.J., Gasca R. M., Jiminez-Ramirez A. "A Model-Driven Engineering approach with Diagnosis of Non-Conformance of Security Objectives in Business Process Models*," 5th IEEE International Conference on Research Challenges in Information Science (RCIS 2011)* ISBN 978-1-4244-8671-7 to be published.

Weske, M. “*Business Process Management: Concepts, Languages, Architectures*”, Springer, 2007.

Wolter, C., Menzel, M., Schaad A. , Miseldine P., and Meinel C.,“Model driven business process security requirement specification,” *Journal of Systems Architecture-Embedded Systems Design*, vol.55, no. 4, pp. 211–223, 2009.