

Rafael Accorsi and Raimundas Matulevičius

## Second Workshop on Security in Business Processes

### A workshop report

*The second workshop on Security in Business Processes (SBP'13) was organised in conjunction with the 11th international conference on Business Process Management (BPM 2013). Over 20 participants attended the workshop to present and discuss 6 papers, the insights they offered and the issues they raised. During the half-day workshop, a number of important and emerging issues in this area were discussed from the perspectives of formal methods and security modelling and importance of security properties and requirements in the business processes.*

#### 1 Introduction

Despite the growing demand for compliant business processes, security and privacy incidents caused by erroneous workflow specification, implementation and execution are still omnipresent. In fact, often business process management and security issues stand out as separate silos, and are seldom addressed together towards the development of trustworthy, compliant business processes. The second edition of the Workshop on Security in Business Processes (SBP'13) brought together researchers and practitioners interested in management and modelling of secure business processes in process-aware information systems. In particular, SBP'13 encouraged innovative methods for workflow security modelling, security audit and control along the entire business process lifecycle: from design time verification to online operational support and post-mortem analysis.

SBP'13 was co-located with the 11th International Conference on Business Process Management (BPM), which, in 2013, was held in Chinese capital, Beijing. Over 20 participants attended SBP and enjoyed an intensive interaction with other attendees. The workshop received 9 high quality submissions, thereby being a successful, attracting and competitive workshops at the BPM 2013. The programme committee worked very hard to select 3 full papers (acceptance rate 33,33%) and 2

short papers (total acceptance rate 55,55%) for the presentation at the workshop. Additionally the workshop organizers invited the keynote speaker. This report briefly summarises the papers that were presented. The proceedings containing the papers in full are available from Springer<sup>1</sup>.

#### 2 Workshop Format

All the workshop presentations were carried on in the mutual and interaction between the paper presenters and the audience. Following the previous experience, before the workshop each paper was assigned a discussants. The responsibility of the discussant included reading the paper before the workshop and preparing few questions, which initiate and challenge the discussion after the paper is presented. This worked out at the largest extent and stimulated very interesting discussions involving not only the presenters and discussants, but also the overall audience. This format will remain the base for the future SBP workshop.

#### 3 Scientific Program

The workshop was begun with the keynote speech given by Hejiao Huang, a professor of Harbin Institute of Technology Shenzhen Graduate School,

<sup>1</sup>Lohmann N., Song M., Wohed P. (Eds): Business Process Management Workshops. BPM 2013 International Workshops, Beijing, China, Lecture Notes in Business Information Processing (LNBIP), Springer, Heidelberg, 2014.

China. In her talk *Specification and Conflict Detection for GTRBAC in Multi-domain Environment* (co-authored with Ning Bao and Hongwei Du), Hejiao stressed on the importance of the formal methods to define the security policy for the business processes. The paper, firstly presents the principles of the colour Petri net (CPN). Then it systematically illustrates the application of the CPN models to verify security policies expresses in generalised temporal role-based access control models.

In *Multi-dimensional Secure Service Orchestration* by Gabriele Costa, Fabia Martinelli, and Artsion Yautsiukhin the Web service composition is analysed as the combination of the atomic services to specify the non-functional requirements. The major emphasis of the paper is placed on the verification of the several security metrics at the same time. The authors use the formal methods, such as c-semirings, history expressions and Galois expressions to propose a framework for analysis of security properties and security metrics.

Jens Gulden presented the paper *Explication of Termination Semantics as a Security-relevant Feature in Business Process Modeling Languages*. The author argues that the current business process modelling languages do not have sufficient semantic power to express process termination clear. Thus, in security relevant contexts, it becomes dangerous and imprecise to define exceptional behaviour of individual process steps. To tackle the problem, the paper, firstly, develops a terminological framework for describing multiple facets of process step termination semantics. Secondly, the theoretical concerns are illustrated in two domain-specific languages.

The second session was started by Elham Ramezani, who presented the paper *Supporting Domain Experts to Select and Configure Precise Compliance Rules* authored by Elham Ramezani, Dirk Fahland and Wil M.P. van der Aalst. The paper argues for the importance of bridging the gap between the informal requirements description and a formal requirements specification. The contribution includes the method to ensure process

compliance through the compliance patterns expressed in Petri nets. The method is implemented into the ProM tool and illustrated in the health care domain.

In the presentation of the short paper *A Framework for the Privacy Access Control Model* by Sandugash Askarova, Darkhan Mukhatov, Altynbek Sharipbayev, and Dina Satybalдина, the problem of privacy access control is considered. The authors have suggested a framework to link between the organisational context and privacy enforcement in order to capture the privacy requirements. In addition, the framework is supported with the heuristics to guide such a privacy policy definition.

In the final workshop presentation *Role-based Access Control for Securing Dynamically Created Documents*, Kaarel Tark and Raimundas Matulevičius illustrated an example of the model driven security implementation. The dynamic approach was taken into account to define the role-based access control for the content and structure of the XML documents. The proposal shows how to ensure confidentiality and structure integrity of such artefacts.

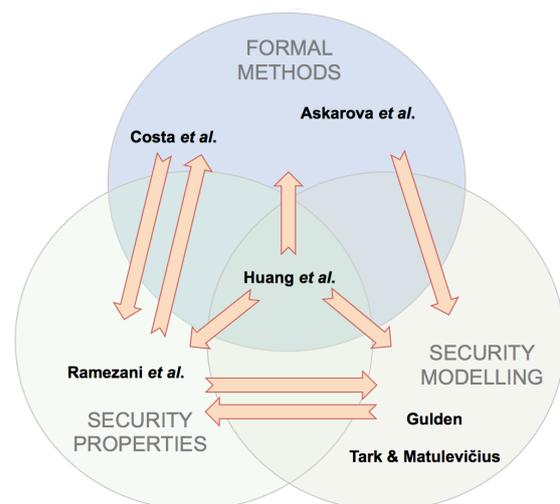


Figure 1: Topic interconnection

#### 4 Observed Trends

This year the workshop's emphasis was placed on the *formal methods*, *modelling* and *security*

*properties and requirements* in business processes as illustrated in Fig. 1. The keynote presentation has highlighted the importance of the formal methods (i.e., the CPN) to verify the security properties within the business process modelling. In all the other presentations it was possible to observe the tendency to relate together at least two of these characteristics. For instance in the study on the process compliance (by Ramezani *et al.*), the emphasis is placed on the necessity to guarantee process requirements, however the compliance method relies both on the modelling and on the formal method application. Formal methods are useful also to ensure the security properties and to provide the security metrics as illustrated by Costa *et al.* or to model the security policies defined by Askarova *et al.* The studies by Gulden, and Tark and Matulevičius uses the security modelling techniques to strengthen the important security concerns. For instance, in the first case the business modelling languages are equipped with the constructs to express the security properties; thus, in the second case the modelling of security policy (in terms of the RBAC model) contributes to the security of the artefacts (i.e., XML document) under analysis.

Many of the issues raised and discussed during the workshop echoed from the Seminar ‘Verifiably Secure Process-Aware Information Systems’ which took place in the week before the workshop in the Castle Dagstuhl, Germany<sup>2</sup>. Besides embracing the topics considered during the SBP’13 workshop, the seminar also considered the runtime analysis of processes, as well as the analysis of log files for a-posteriori analysis. Interestingly enough, the previous editions of SBP (and its predecessors) included contributions on these types of analysis, too. However, we do not believe that this is a trend in research on security in business processes. In fact, recent research has focused on these areas<sup>3</sup>.

<sup>2</sup>Seminar URL: <http://www.dagstuhl.de/mat/index.en.phtml?13341>

<sup>3</sup>G. Müller and R. Accorsi: Why are business processes not secure? In M. Fischlin and S. Katzenbeisser, eds., *Fests-*

### See you next time. . .

The next SBP proposal is about to take place in affiliation with the BPM 2014 in Haifa, Israel (September, 7-11). We would be very happy to see you there!

#### Rafael Accorsi

Albert-Ludwigs-Universität Freiburg,  
Friedrichstr. 50  
Freiburg i.Br.  
Germany  
accorsi@iig.uni-freiburg.de

#### Raimundas Matulevičius

University of Tartu, J. Liivi 2  
Tartu  
Estonia  
rma@ut.ee