Rafael Accorsi and Raimundas Matulevičius

Workshop on Security in Business Processes

A workshop report

The Workshop on Security in Business Processes (SBP'12) was organised in conjunction with the 10th international conference on Business Process Management (BPM 2012). Over 25 attended the workshop to present and discuss 11 papers, the insights they offered and the issues they raised. During one-day workshop, a number of important and emerging issues towards the security in business processes. These were the perspectives of secure business processes, security and compliance, security and Internet services, and engineering secure 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. By combining the successful, past experiences of the First International Workshop on Alignment of the Business Process and Security Modelling (ABPSM'11) and WfSAC - BPM Workshop on Workflow Security Audit and Certification, the Joint Workshop on Security in Business Processes (SBP'12) brought together researchers and practitioners interested in security management of business process models in process-aware information systems.

SBP'12 was co-located with the 10th International Conference on Business Process Management (BPM), which, in 2012, was held in Estonian capital, Tallinn. Over 25 participants attended SBP and enjoyed a day of intensive interaction with other attendees; academics working in the business process and security modelling, practitioners reporting on their experience in using techniques to develop security concerns in business processes.

The SBP'12 workshop received 18 high quality submissions, thereby being one of the most successful, attracting and competitive workshops at the BPM. The programme committee worked very hard to select 5 full papers (acceptance rate 27,78%) and 4 short papers (total acceptance rate 50%) for the presentation at the workshop. Additionally the workshop organizers invited two keynote speakers, representing academia and industry, respectively. This report briefly summarises the papers that were presented. The proceedings containing the papers in full are available from Springer[1].

2 Perspectives of Security Business Processes

The workshop was begun with the keynote speech given by Andreas Opdahl, a professor of Information Systems Development at the University of Bergen, Norway. In his talk *Identifying and Visualising Dependendablity Concerns - Application to Business Process Management,* Andreas reported on the requirements for security project, which had the purpose to evaluate techniques for visualization of security and safety early in the planning of new information systems. Misuse case

[1] La Rosa M., Soffer P. (Eds): Business Process Management Workshops. BPM 2012 International Workshops, Tallinn, Estonia, LNBIP 132, Springer, Heidelberg, 2013.

maps and misuse sequence diagrams were the modelling languages proposed by the project for dealing with security requirements and for depicting attack sequences. Regarding the safety aspect, the project analyzed the failure sequencing diagrams. It was noted that the safety and security techniques are closely related since they both identify what the new system should not do. This resulted in the method for combined harm assessment of safety and security for information systems. The project suggests a number of implications regarding the business process area. For instance, it is important to consider, broader, and handle dependability links, involvement of broad competence, visualisation of key concerns, guidance using the keywords, and investigation of remedies for possible vulnerabilities. This could challenge potentially a broad future research regarding dependability and its various types.

In *A Language for Multi-Perspective Modelling of IT Security: Objectives and Analysis of Requirements* by Anat Goldstein and Ulrich Frank, Anat Goldstein highlighted the importance (i) to assess and reduce risks that originate from within organisation and from its outside, (ii) to overcome and manage the increasing organisational complexity, (iii) to encourage participation of non-technical actors, (iv) to relate security solutions with the cost-benefit analysis, and (v) to design and implement security infrastructure using automated creation of security related policies and coding. To address all these concerns a comprehensive and common conceptual framework to support technical, business and social aspects is needed. The paper suggests a list of general and specific requirements for security risk modelling that potentially could result in a method to support design, realisation and management of system security.

3 Security and Compliance Text Fonts

Towards Compliance of Cross-Organizational Processes and their Changes by David Knuplesch, Manfred Reichert, Jurgen Mangler, Stephanie Rinderle-Ma, and Walid Fdhila give an overview of the requirements and challenges to be addressed in order to ensure compliance with regulations, standards and laws. The David Knuplesch argued that ensuring compliance for cross-organisational processes and their changes it is important to understand what modelling cross-organisational compliance rules are, how changes are propagated and what guidelines should be followed to ensure efficient cross-organisational instance migration. It is also important to ensure compliance regarding the data privacy. Other two challenges also include efficient compliance at change time and the adequate treatment of the user feedback.

Achim D. Brucker presented the paper *Secure and Compliant Implementation of Business Process-driven Systems* authored by Achim D. Brucker and Isabelle Hang. In process-aware information systems (PAIS), manually managing compliance with security and privacy policies generates costs. To address this problem, they present a method for statically checking the security and conformance of the system implementation, e.g., on the source code level, to requirements specified on the business process level. As the compliance is statically guaranteed already at design-time, their method reduces the number of runtime checks for ensuring the security and compliance and, thus, improves the runtime performances. As a result it also reduces the costs of system audits, as there is no need for validating compliance of the generated log files.

A Process Deviation Analysis Framework by Benoit Depaire, Jo Swinnen, Mieke Jans, and Koen Vanhoof address the problem of flexible business process models. Process deviation analysis is becoming increasingly important for companies, as a means to provide agility and to adapt to changes. However, these changes are usually uncontrolled and, in fact, there is not much work dedicated to their understandability. This short paper presents a framework which structures the field of process deviations and identifies new research opportunities. The actual application

of the framework starts from managerial questions which relate to specific deviation categories and methodological steps. The paper sketches a high-level method to detect high-level process deviations, which is being developed in detail as a further work.

4 Security and Internet Services

The session opened with the second keynote speech. Sven Heiberg's presentation of *New Technologies for Democratic Elections* overviewed the technological advances and hurdles towards the provision of e-voting facilities in Estonia. The keynote described the challenges, both technical and ethical, involved in the implementation process of the Internet voting (i-voting). The presenter reported on the recent "i-voting" experience at the Estonian Parliamentary elections in 2011. The paper shows and classifies the security attacks (i.e., manipulation, revocation, and reputation attacks) and argues for the individual verifiability as the control to voters and election officials to countermeasure the determined attacks.

In the presentation of the short paper *Securely Storing and Executing Business Processes in the Cloud* by David Martinho and Diogo R. Ferreira, David Martinho addresses the problem of employing cloud computing to store classified data. Since the service provider can access all data, he, accidentally or deliberately, could leak it or use it for unauthorized purposes. As a countermeasure, the authors propose an architectural solution to securely operate their business processes relying on cloud-based services. This solution is built upon a thick client and thin server architectural pattern, where security constructs such as public-key and symmetric cryptographic systems are used to maintain confidentiality between the participants while keeping the server unaware of their participations and business process instances.

Focusing on the secure enactment of business processes, the short paper *Advanced Protection of Workflow Sessions with SEWebSessions* by Maxime Fonda, Stephane Moinard, and Christian Toinard reported on an approach based upon mandatory access control to authorize various confidentiality and integrity properties for the session state. The suggested SEWebSessions approach prevents the security violations associated with malicious accesses. Besides the technical means, the paper also describes experiments with SEWebsessions illustrates its portability to various platforms.

5 Engineering Secure Business Processes

In presenting the first paper in this session, *Modeling Wizard for Confidential Business Processes* by Andreas Lehmann and Niels Lohmann, Andreas Lehmann looked into the problem of avoiding information leaks within and across business process models. He presents a modelling prototype that integrates the non-interference check into the early design phase of an inter-organizational business processes. It not only helps receive the instant feedback on confidentiality assignments, but also automates completion of partial assignments toward guaranteed non-interference. This is an important tool for constructing secure business processes "by design".

Naved Ahmed in this presentation of *Towards Security Risk-oriented Misuse Cases* by Inam Soomro and Naved Ahmed argued for the necessity to understand business security through the security risk management. The presenter illustrated how misuse case diagrams could be extended to support security risk management by introducing construct for security criterion, vulnerability, risk impact, and security requirements. The approach could be generalised to other modelling languages, too. Potentially such language extensions could lead to the alignment of the business and functional perspectives. It could, potentially, result in a comprehensive and systematic development approach of the secure systems.

A Case Study on the Suitability of Process Mining to Produce Current-State RBAC Models by Maria Leitner, Anne Baumgrass, Sigrid Schefer-Wenzl,

Stefanie Rinderle-Ma, and Mark Strembeck was the last but certainly not the least, paper of the workshop. In her short paper presentation Maria Leitner overviewed techniques to derive role-based access control models (RBAC) from the execution logs of business process models. This paper closes an existing gap between the organizational control mining (a segment of process mining, in particular process discovery) and the security reasoning. This contribution is particularly interesting for industry, where the definition of role structures evolve over time and inconsistencies between these roles definitions could appear.

6 Workshop Design

All the workshop presentations were carried on in the mutual and interaction between the paper presenters and the audience. Before the workshop each long paper was assigned two discussants and short paper - one discussant. 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. The organizers were explicitly requested to follow such a workshop format in the future editions.

7 Observed Trends

The provision of security and privacy guarantees is a rapidly growing research area in business process management. One indicator for this is the growing number of submissions (compared to the previous ABPSM'11 and WfSAC'11 workshops) we experienced. Another indicator is the elevated quality of submissions we received for SBP and the topics they approach. Below we report on some trends we observed in SBP considering the overall set of submissions (not only those accepted).

Among the submissions, eight papers address the problem of providing security "by design" - i.e. preventively ensuring that process models and execution environments comply with the requirements - and four papers focusing on the detection of security relevant incidents "after the fact". Less attention has been given to runtime approaches (two papers). This is insofar interesting, as there are powerful mechanisms to enforce processes and even correct them during the execution, thereby guaranteeing compliance. However, these approaches come at the cost of runtime overhead and we speculate this overhead may be prohibitive for practical approaches. Equally interesting is the fact that approaches focussing on the formalisation of requirements are underrepresented. We did not expect that; in fact, the call for papers explicitly mentions this as a desired contribution area, for a non-negligible "expressivity gap" between users and verification tools exist in this point. However, on the one hand there is a plethora of languages to express requirements, on the other hand each analysis mechanism encompasses its own language for the specification of requirements. Hence, works focussing solely on the expression and formalisation of requirements might have become uninteresting. Still, we believe that the whole area of requirements engineering should play a bigger role in the area of business modelling.

Another interesting trend we observed is the use of process mining techniques to address the verification of security properties. This is, in our view, a natural development in the area. Process mining focusses on process analysis in general and provides powerful analysis tool. The security community recognises this potential and shifts the application to security properties. We expect this trend to remain for the next years. However, advances in the area of data-aware process mining will be necessary, otherwise one is only able to reason about the structure of the process. Admittedly, this is not enough for security. Here this is a point where we see the security community advancing process mining.

As for the topics, the workshop sets out to address "security" aspects of business processes. However, one trend we observed regards the fact that the provision regulatory compliance is usually seen in this context. From the viewpoint of analysis, this is not surprising as one is merely changing the flavour of the requirements. Still, we would rather expect papers on privacy (no submissions on this topic) than on compliance. Hence, one interpretation of this trend is that the SBP workshop is understood as a venue to discuss reliability issues of business processes.

See you next time...

The next SBP proposal is planned for the BPM 2013 in Beijing, China (August, 26-30). 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