Towards SecureBPMN - Aligning BPMN with the Information Assurance & Security Domain

Yulia Cherdantseva[1], Jeremy Hilton[2], Omer Rana[1]

[1] School of Computer Science and Informatics, Cardiff University, UK
y.v.cherdantseva,o.f.rana@cs.cardiff.ac.uk,
[2] Department of Informatics and Systems Engineering, Cranfield University, UK
j.c.hilton@cranfield.ac.uk

Abstract. The participation of business experts in the elicitation and formulation of Information Assurance & Security (IAS) requirements is crucial. Although business experts have security-related knowledge, there is still no formalised business process modelling notation allowing them to express this knowledge in a clear, unambiguous manner. In this paper we outline the foundational basis for SecureBPMN - a graphical security modelling extension for the BPMN 2.0. We also align the BPMN with the IAS domain in order to identify points for the extension. SecureBPMN adopts a holistic approach to IAS and is designed to serve as a "communication bridge" between business and security experts. [1]

Key words: information security & assurance, BPMN, extension

1 Introduction

The importance of Information Security (InfoSec) and Information Assurance (IA) has been escalating over the last several decades as a result of the growing reliance of organisations on Information and Communication Technology (ICT) and the recognition of information as a key business asset. During the last decade, we have observed an increasing tendency to perceive InfoSec as a business enabler and to recognise the importance of IA - a comprehensive and systematic management of InfoSec in a networked world [1]. In this paper we refer to the Information Assurance & Security (IAS) knowledge area, which incorporates the knowledge acquired by both InfoSec and IA [1]. The realm of IAS includes (1) all InfoSec countermeasures; and (2) a systematic and comprehensive management of these countermeasures. IAS is not limited to the technical aspect of information protection, it includes organisational, legal and human-oriented aspects as well.

Until recently, the IAS concerns were not considered at the stage of Business Process Modelling (BPM). Often, it is attributed to the fact that business experts have not enough security-related knowledge or training [2]. Nevertheless,

[1] This is an authors' preprint. The original publication will be available at www.springerlink.com in the Proceedings of the BPMN 2012 Workshop.

the empirical studies show that business experts may express security needs at a high level of abstraction [3]. Business experts have knowledge essential for security design, e.g. knowledge about information levels of sensitivity, internal and external information sharing needs, and about legal and compliance IAS requirements (often sector-specific). Therefore, we see different reasons for the insufficient integration of security modelling into BPM. These are:

- the lack of commonly agreed understanding of the IAS domain;
- the complexity of articulating security requirements together with functional requirements;
- the communication gap between business and security experts (business experts express security needs at the very high level of abstraction, whereas security experts operate at the detailed technical level);
- little software-tool support for incorporating IAS aspects in BPM.

Overall, BPM is deemed to be a suitable foundation in order to fulfil the challenging tasks of security requirements elicitation and high level security design due to the following reasons:

1. the overall purpose of BPM is analysis and improvement of business processes in terms of time-effectiveness and efficiency through allowing easy identification of the problematic areas [6]. Hence, BPM could be used in a similar way to identify security-related problems in business processes.
2. The concept of business process has great importance for business experts [4, 5]. Business experts do not need to familiarise themselves with a new technique to express security concerns.
3. BPM is also used by software developers to capture the initial requirements for the system design [4, 5]. Thus, modelling of InfoSec within business process models allows parallel modelling of functional and non-functional security requirements.

Among a variety of modelling languages the authors have chosen the BPMN [7] as the basis for the extension, guided by the following considerations: (1) it is easily understood by all parties involved in system development - from business analysts to technical personnel [8]; (2) it supports modelling of collaborative business processes; and (3) it allows connection of business process design with implementation in a standardised way [7].

Contribution. In this research we aim to enrich the BPMN with the IAS modelling capabilities by developing SecureBPMN - a graphical security modelling extension for the BPMN 2.0. Here we outline the intermediate results of the SecureBPMN development project. This paper does not go as far as to present the finalised graphical notation, but discusses the need for and outlines the foundational basis of it. In Section 2, we give the overview of the related work. Section 3 outlines the concept behind SecureBPMN and the research method. Section 4 aligns BPMN with the IAS domain to show missing capabilities of the BPMN and points for the future extension. In Section 5, we draw conclusions and sketch a plan of further work.

2 Related Work

Over the last decade a number of research projects were conducted in an attempt to bridge the gap between the IAS and BPM domains. In 2009, the detailed survey of nine attempts to integrate security and risk aspects into business process management was presented by Jakoubi et al. [9]. Jakoubi et al. identified several gaps in the research. Our research aims to address two of them: (1) Extend a list of security goals and (2) Improve one of the business process modelling notations, namely the BPMN. With regards to the first point, we not only extend a set of security goals, but build a comprehensive model of IAS which, apart from security goals, includes information taxonomy, security mechanisms and stages of the IAS development life-cycle.

In 2007, Rodriguez et al. [2] proposed a BPMN extension that allows incorporation of security into BPM from the business analyst viewpoint. The authors of [2] develop a set of graphical concepts representing security semantics. Rodriguez et al. extend the Business Process Diagram (BPD) metamodel with five security requirements: Non-repudiation, Attack harm detection, Integrity, Privacy and Access control. Each security requirement may be specified only for a certain core element of a BPD and has a graphical representation - a padlock symbol with a corresponding capital letter in the center (Figure 2).

In 2008, Wolter et al. [10] discussed a model-driven transformation from security goals, specified in business process models in a graphical fashion, into concrete security implementations in the process-aware information systems, based on Service-Oriented Architecture (SOA). In this work a security concept is presented, which includes the following entities: object (a basic entity of the concept), security goal, constraint (fulfils a security goal), security mechanism (characterises techniques used to enforce a security constraint) and policy (defines constraints). Wolter et al. [10] use the existing BPMN *Group* element to depict security goals as well as a new element - security annotation - which consists of a graphical symbol and an accompanying text description (Figure 3).

In 2011, Mulle et al. [11] proposed a language for formulation of security constraints embedded in the BPMN. The authors address two gaps in the research: (1) incompleteness of security modelling vocabulary; (2) insufficient user involvement. The proposed language uses a standard BPMN *Artifact* element as a container for constraints. A constraint is presented as a structured text annotation. The main aim of the proposed language is to translate security requirements specified in a BPMN model into the executable specification. Hence, the language is text-based and oriented on technical experts. As a result, business experts find it hard to understand. This complicates the initial security requirements gathering.

In 2012, Saleem et al. [12] developed a Domain Specific Language (DSL), based on the BPMN. The proposed DSL allows modelling security requirements along the business process model in SOA applications. The BPMN metamodel is extended with essential security objectives. In comparison with [2], a limited set of security requirements is considered: Confidentiality, Integrity and Availability

(associated with Non-repudiation). Saleem et al. also developed a set of graphical notations for Confidentiality, Integrity and Availability (Figure 4).

In 2012, Altuhhova et al. [13] conducted an analysis of the BPMN in terms of its suitability for security requirements derivation and expression of security countermeasures. Altuhhova et al. [13] align the BPMN constructs with the domain model of Information Systems Security Risk Management (ISSRM) [14] and conclude that the BPMN requires an extension in order to be fully applicable for security modelling.

Problem statement and solution outline.

The recent research has noticeably extended the existing body of knowledge and advanced the area. Nevertheless, there are still some aspects that are not fully addressed in the works discussed above and which SecureBPMN aims to address.

First, many authors still concentrate purely on the technical aspect of IAS and do not address organisational, human and legal aspects. In order to address this issue SecureBPMN adopts a holistic view on the IAS domain and takes into consideration and allows modelling of security mechanisms of different natures.

Second, the research lacks an agreed, shared understanding of the IAS domain. This leads to the incomprehensiveness of a set of security goals being considered, and to the confusion between security goals and security mechanisms. As a solution to this problem, we develop a solid theoretical IAS foundation for SecureBPMN which is expressed via the ontology of the IAS domain and the Multi-Dimensional Model of IAS (MMIAS) [15].

Third, the existing security extensions suffer from granularity. The research considering the expression of security goals by business experts is isolated from the research considering the selection of security mechanisms which help to achieve those goals. Security modelling does not yet facilitate communication between various experts (e.g. business, domain and security experts) involved in the design of *secure* business processes and does not allow representation of all security-related aspects in a consistent, traceable way. As a response, SecureBPMN aims to provide a notation that, first, allows consistent modelling of all elements of the IAS domain and, second, enables modelling from different viewpoints.

Fourth, none of the research discussed above performed an evaluation and validation of the proposed security modelling notation with end-users to ensure its clarity and practical applicability. SecureBPMN has two levels of validation: (1) the IAS ontology and the MMIAS validation by InfoSec and IA experts; (2) SecureBPMN notation validation by business process modelling and security experts.

Fifth, the existing works aim to provide a way for incorporating some security aspects into the BPMN, but omit the fact that the modeller may not have sufficient or complete knowledge about the IAS domain. Foreseeing this issue, we attempt to provide domain- and context-specific security recommendations to a modeller during the process of security annotation.

3 The General Concept behind SecureBPMN and Research Method

SecureBPMN is a firm stepping-stone on the way to solve the problems identified above. The general concept behind SecureBPMN is depicted in Figure 1. A Business Process Model, which is annotated with security elements in line with the SecureBPMN semantic rules is referred to as a Secure Business Process Model (SBPM). Figure 1 shows that a Business Process Model is transformed into a SBPM by undergoing through the Assisted Security Annotation Process (ASAP), when an Expert annotates it with security elements.

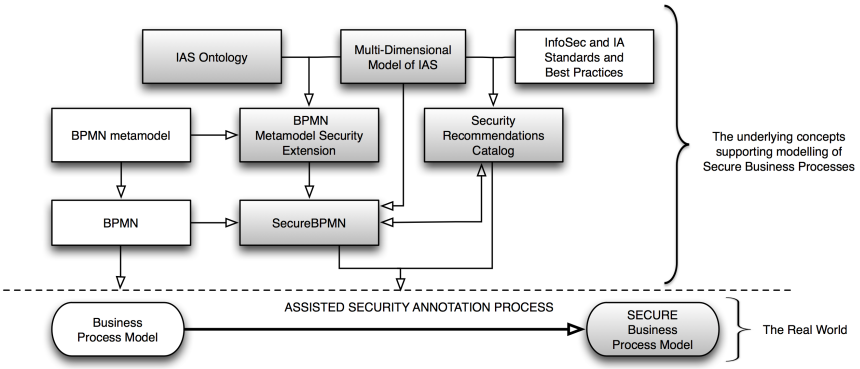

Fig. 1. The General Concept behind SecureBPMN

Above the dotted line, Figure 1 depicts the components required to enable the design of SBPM and the interrelationship between these components. The components shown in Figure 1, which are innovative and developed in this research project, are shaded. The un-shaded components illustrate the existing notations and concepts. Thus, the concept behind SecureBPMN includes the ASAP as well as:

- The IAS Ontology, which clarifies the interdependences between the fundamental elements of IAS, namely asset, security goal, security mechanism, threat, vulnerability and risk.
- The Multi-Dimensional Model of IAS (MMIAS) - a distilled, concise overview of the IAS domain, which has been developed on the basis of the analysis of the existing InfoSec and IA models. It fosters the commonly-shared domain understanding, reuse of the existing knowledge, makes ideas sharing easier, and promotes consistency of security policies and mechanisms across organisations.
- The BPMN metamodel extended with security entities and attributes outlined in the ontology and MMIAS;
- A Security Recommendations Catalog (SRC) - a database of the Security Recommendations, which is formed on the basis of the security-related standards

Table 1. Steps of the research method

Step Title	Input	Output
Mapping of the IAS knowledge area	InfoSec and IA academic and industry publications, standards, existing models of InfoSec and IA	IAS ontology; MMIAS [15]
Metamodelling	IAS ontology; MMIAS	Extended BPMN metamodel
Development of ASAP	IAS ontology; MMIAS; extended BPMN metamodel	ASAP
Development of SecureBPMN Graphical Notation	IAS ontology; MMIAS; extended BPMN metamodel	SecureBPMN
Development of a SRC	IAS ontology; MMIAS; extended BPMN metamodel; SecureBPMN	SRC
Prototype implementation	IAS ontology; MMIAS; extended BPMN metamodel; SecureBPMN; ASAP	Software tool supporting SecureBPMN

and best practices and intended to assist a modeller, who has no in-depth knowledge of the IAS domain;
– SecureBPMN - the syntax, semantics and notation of the security modelling extension.

The research method which is used for the development of SecureBPMN consists of six steps outlined in Table 1 along with the expected output of each step. Although there is a required logical consequence of the steps, in practice the research and development of the extension is conducted in a spiral iterative, rather than a step-by-step manner.

4 Aligning the BPMN with the IAS domain

The IAS ontology and the MMIAS, which are elaborated in this research project, form a grounded conceptual foundation of SecureBPMN. The detailed description of the ontology and MMIAS is given in [15]. The ontology and MMIAS define security elements and their attributes that are essential for the IAS domain and, therefore, should find their representation in the business process models. This section analyses how identified essential security elements and their attributes could be illustrated by the existing BPMN elements. Table 2, shows (1) correspondence between the IAS ontology elements and their attributes, and the MMIAS elements; (2) how elements of the IAS ontology and MMIAS may be represented by the BPMN elements; and (3) representation of security elements in the existing security extensions for the BPMN.

Table 2 shows that the majority of security elements could be represented with a *Text Annotation* BPMN element. Unfortunately, the usage of Text Annotation for expression of security elements of different nature is highly likely to lead to multiple misinterpretations of the security annotations in business process models. Although the security extension of the BPMN should fully use

Table 2. Alignment of the BPMN with the IAS ontology and the MMIAS

IAS Ontology Elements and their attributes	**MMIAS elements**	**BPMN elements**	**Representation in other works**
Security Goal	Security Goal	None; Possible: Text Annotation	[2] - padlock symbols (security requirements) (Figure 2); [10] - group element, text annotation with icon (Figure 3); [12] - colour symbols (security stereotypes) (Figure 4)
Criticality of Security Goal	Prioritisation of security goals	None Possible: Text Annotation	[2] - Security requirement has a level of criticality. No visual representation.
Asset	Information Taxonomy characterises the asset	DataObject, Message, DataStore	Present in the BPMN, no need for extension
Asset Sensitivity	Information Level of Sensitivity	None; Possible: Text Annotation	Not found
Asset State	Information State	Defined according to the position within a model	Not found
Asset Position/Location	Information Position/Location	Defined according to the position within a model	Not found
Security Mechanism	Security Mechanism	Activity, Task, Group, Association, Transaction, Compensation	[10] - group element, text annotation with icon (Figure 3); [11] - text annotation; [16] - blue circle with text description
Vulnerability	Not present	None; Possible: Text Annotation, Association, Message Flow, Task, Activity	[13] - Message Flow
Threat	Not present	None; Possible: Pool, Lane, Activity, Task, Message Flow	[13] - Message Flow, Text annotation, Pool, Lane
Risk	Reflected by the criticality of security goals	None; Possible: Text Annotation	[16] - red triangle with exclamation mark accompanied by text description
Access Permissions depend on Asset Sensitivity	Access Permissions depend on Information Level of Sensitivity	None; Possible: Text Annotation	[2] - a padlock symbol accompanied by text annotation (access permissions; security role);

the existing BPMN elements, there is still a need to introduce new graphical elements for the visualisation of the following key security elements: security goal and its level of criticality; security mechanism; asset level of sensitivity; and access permissions for all actors within the model.

Thus, the analysis summarised in Table 2 confirms that (1) the BPMN syntax is insufficient for the representation of all elements outlined in the IAS ontology and the MMIAS, and requires an extension to facilitate effective security modelling, and (2) currently, there is no comprehensive security modelling extension for the BPMN that allows clear, consistent representation of all elements of the IAS domain and their attributes.

Fig. 2. The Representation of Security Requirements by Rodriguez et al. [2]

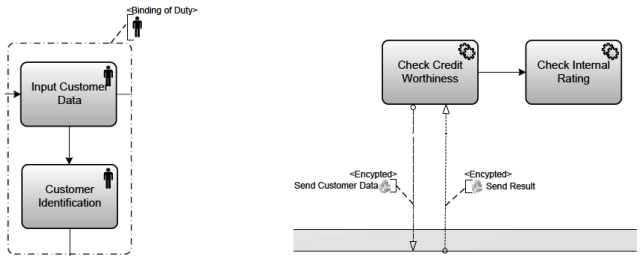

Fig. 3. The Representation of Security Goals by Wolter et al. [10]

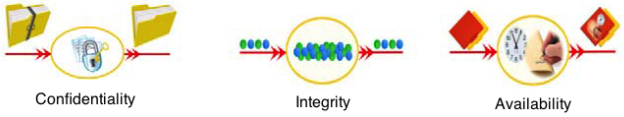

Fig. 4. The Representation of Security Stereotypes by Saleem et al. [12]

5 Conclusion and Further Work

This paper discusses the importance of consideration of IAS issues at the stage of BPM and presents the foundational basis for SecureBPMN - a security modelling extension for the BPMN 2.0. SecureBPMN will operate at the high level of abstraction and serve as a bridge between business and security experts. There are several important features that differentiate SecureBPMN and, as a result, determine its **novelty**: (1) a solid theoretical IAS foundation, (2) a holistic approach to IAS (modelling of technical, organisational, human-oriented and legal security mechanisms); (3) consistent modelling of all key IAS elements (and their attributes), and (4) support of security-decision-making process through the provision of security recommendations.

The research conducted so far allowed us to identify security elements that should be incorporated into the BPMN and to set the basis for the development of a visual notation. Further work involves the elaboration of the SecureBPMN graphical notation and its validation with end-users. The evaluation of the positive effect of the suggested extension will be carried out by applying SecureBPMN on a real-life case study and discussing the results with business and security experts.

References

1. Cherdantseva Y. and Hilton J.: Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. (May, 2012). Available at http://users.cs.cf.ac.uk/Y.V.Cherdantseva/Cherdantseva_Hilton_2012.pdf [accessed on 22.06.2012]
2. Rodriguez A., Fernandez-Medina E. and Piattini M.: A BPMN Extension for the Modeling of Security Requirements in Business Processes. In: IEICE - Trans. Inf. Syst., vol. E90-D, pp. 745-752 (2007)
3. Lopez J., Montenegro J., Vivas J., Okamoto E. and Dawson E.: Specification and Design of Advanced Authentication and Authorization Services. Computer Standards and Interfaces, vol. 27-5, pp. 467-478 (2005)
4. Leymann F.: BPEL vs. BPMN 2.0: Should You Care? In: 2nd International Workshop BPMN, Potsdam, Germany (2010)
5. Volzer H.: An Overview of BPMN 2.0 and its Potential Use. In: 2nd International Workshop BPMN, Potsdam, Germany (2010)
6. Giaglis, G.: A taxonomy of business process modeling and information systems modeling techniques. International Journal of Flexible Manufacturing Systems, vol. 13-2, pp. 209-228 (2001)
7. The OMG, Business Process Model and Notation (BPMN) Version 2.0, 2011-01-03. Available at http://www.omg.org/spec/BPMN/2.0 [accessed on 22.06.2012]
8. Wolter C. and Schaad A.: Modeling of Task-Based Authorization Constraints in BPMN. In: Proceedings of the 5th International Conference on Business Process Management, pp. 64-80 (2007)
9. Jakoubi S., Tjoa S., Goluch G. and Quirchmayr G.: A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management. In: International Workshop on Database and Expert Systems Applications, pp. 127-132 (2009)
10. Wolter C., Menzel M. and Meinel C.: Modelling Security Goals in Business Processes. Proc. GI Modellierung, vol. 127, pp. 197-212 (2008)
11. Mulle J., Stackelberg S. and Bohm K.: A Security Language for BPMN Process Models. Karlsruhe Reports in Informatics (Sept. 2011)
12. Saleem M., Jaafar J. and Hassan M.: A Domain-Specific Language for Modelling Security Objectives in a Business Process Models of SOA Applications. AISS, vol. 4, no. 1, pp. 353- 362 (2012)
13. Altuhhova O., Matulevicius R. and Ahmed N.: Towards Definition of Secure Business Processes. In: WISSE'12, Gdansk, Poland (June, 2012). Available at http://gsya.esi.uclm.es/WISSE2012/papers/paper5.pdf [accessed on 27.06.2012]
14. Mayer N.: Model-based Management of Information System Security Risk. Doctoral Thesis, University of Namur (2009)
15. Cherdantseva Y., Hilton J. and Rana O.: SecureBPMN - a New Approach to Achieving Synergy between Information Security and Business Process Modelling. (Feb. 2012). Available at http://users.cs.cf.ac.uk/Y.V.Cherdantseva/SecureBPMN.pdf [accessed on 22.06.2012]
16. BOC Group. Risk management and compliance with ADONIS:Community Edition. Available at http://www.adonis-community.com/fileadmin/media/documents/RM_with_ADONISCE.pdf [accessed on 21.05.2012]