Towards a BPMN Security Extension for the Visualization of Cyber Security Requirements

Mohamed El Amine Chergui, EEDIS Laboratory, University Djilali Liabes, Algeria
Sidi Mohamed Benslimane, LabRI-SBA Laboratory, Ecole Superieure en Informatique, Sidi Bel Abbes, Algeria
https://orcid.org/0000-0002-7008-7434

ABSTRACT

Business process modeling notation (BPMN) is a widely used business model process. The importance of security is apparent, but traditionally, it is considered after the business processes definition. There is a need for integrated tools and a methodology that allows for specifying and enforcing compliance and security requirements for business process-driven enterprise systems. Therefore, it is very important to capture the security requirements at conceptual stage in order to identify the security needs. BPMN is lacking the ability to model and present security concepts. This will increase the vulnerability of the system and make the future development of security for the system more difficult. This article proposes a novel extension to BPMN notation based on cyber security ontologies. The authors incorporate visual constructs for modeling security requirements. In order to provide a commonly usable extension, these enhancements were implemented as BPMN metamodel extension. The authors illustrate capabilities and benefits of extension with a real-life example.

KEYWORDS

BPMN Extension, Business Process, Modeling, Security Requirements

INTRODUCTION

Users are widely adopting business process modeling standards to express and design the functional requirements of their businesses. Business process modelling is normally performed in a modelling language such as Unified Modeling Language (UML) or Business Process Model and Notation (BPMN). These modelling languages do not support natively annotation security, which may result in significant problems regarding the comprehensibility and maintainability of these ad hoc models. BPMN was originally developed to provide a notation that was easily understandable by all business users, from technical analysts implementing an information system to business analysts to business users who manage the processes (Pullonen et al., 2019). BPMN is used as a modelling language for our work; which is an industry standard for business modelling and fulfils the requirement of visually representation (Rodriguez et al., 2007) and (Salniti et al., 2014). Moreover, BPMN provides an extension mechanism and it is supported by a wide range of modelling tools (Zarour et al., 2019).

DOI: 10.4018/IJTD.2020040101
In addition to the functional characteristics of a business process, there also exist a number of non-functional aspects that need to be taken into consideration. Security is one of the most important of such non-functional aspects (Argyropoulos et al., 2019). Security requirements and compliance regulations are a major concern for designing and running business process driven systems due to the potential impact of its defect for organizations in terms of reputation, finances and legal compliance (Argyropoulos et al., 2019).

Security requirements have been recognized as an important concern among system developers and users. Based on these facts, the association between business process and security is inevitable. Empirical studies show that those who model the business process i.e. business domain expert is able to specify security requirements at high level of abstraction i.e. while designing the system (Rodriguez et al., 2007).

Since the consideration of security during the early design stages of systems is considered highly beneficial (Leitner et al., 2013). Business process modelling is the most appropriate layer to describe security requirements (Menzel et al., 2009). However, in practice, business domain expert mainly focuses on the functionality because business domain expert is not a security expert (Rodriguez et al., 2007) and in many software development methods often treat security, separately at later stage. Further, the main concern of developers is functionality, security is underprioritized and implemented in an ad hoc manner.

Several BPMN security extensions have been proposed to model the security requirements along the business process model. However, those approaches remain theoretical and miss many important security concepts (Maines et al., 2016). They are being constructed unsystematically, without any empirical evidence to support their choice of concepts (Leitner et al., 2013). Most security extensions are not compliant with the BPMN 2.0 standard (Braun et al., 2014).

We propose a new BPMN extension to annotate business security with security concepts. Unlike current approaches, our extension is built upon existing literature and empirical evidence. From our evaluation of existing approaches, we are able to identify the gaps and propose a new set of requirements for avoiding them. An ontology-based BPMN extension approach is proposed with a complete set of security concepts derived from cyber security ontology (Maines et al., 2015) with their graphical presentation. The security concepts are integrated into business process models to operationalize different types of security requirements (e.g. availability, confidentiality, integrity) and are expressed at an abstraction level which is generic enough to be able to be instantiated by different types of security implementing technologies.

We applied Stroppi Method (Stroppi et al., 2011), for the development of extensions to have a valid BPMN 2.0 extension. We implemented our approach as web application to facilitate collaboration between actors (business domain expert, security expert and developer). Furthermore, we defined the extension as XML Schema to be able to integrate it to existing BPMN tools.

The extension is applied to a real-life use case (typical process of admitting a patient) as a proof of concept. We chose this use case because the healthcare industry increasingly relies on technology. Therefore, the security issue can have a profound impact on patient care and privacy (Sang et al., 2015). Moreover, an online questionnaire is used to evaluate the perceived usability of the introduced security concepts and compare them to ad hoc approach.

In addition, we assess the design and modeling of existing security extensions found in the literature review regarding to the standard conformity criterion (syntactical and semantic correctness) (Braun et al., 2014) of the extension in the light of the BPMN standard.

The remaining part of the paper is organized as follows: In section 2, the most related work is briefly reviewed. Section 3 introduces fundamentals in terms of general extensibility of BPMN. In section 4 we present the proposed extension that support security annotation. Section 5 provide an illustration with use case to demonstrate integration of security concepts and an experimentation of comprehension task. Finally, section 6 concludes the paper and outlines directions for future work.
Next Generation Networks: A New Digital Divide?
[www.igi-global.com/article/next-generation-networks/45748?camid=4v1a](www.igi-global.com/article/next-generation-networks/45748?camid=4v1a)

Culture and Consumer Trust in Online Businesses
Robert Greenberg, Bernard Wong-On-Wing and Gladie Lui (2010). *Technological Advancement in Developed and Developing Countries: Discoveries in Global Information Management* (pp. 154-173).
[www.igi-global.com/chapter/culture-consumer-trust-online-businesses/39436?camid=4v1a](www.igi-global.com/chapter/culture-consumer-trust-online-businesses/39436?camid=4v1a)