Threat Representation Methods for Composite Service Process Models

Per Håkon Meland, Software Engineering, Safety and Security, SINTEF ICT, Trondheim, Norway
Erlend Andreas Gjære, Software Engineering, Safety and Security, SINTEF ICT, Trondheim, Norway

ABSTRACT

The Business Process Modeling Notation (BPMN) has become a popular standard for expressing high level business processes as well as technical specifications for software systems. However, the specification does not contain native support to express security information, which should not be overlooked in today's world where every organization is exposed to threats and has assets to protect. Although a substantial amount of work enhancing BPMN 1.x with security related information already exists, the opportunities provided by version 2.0 have not received much attention in the security community so far. This paper gives an overview of security in BPMN and investigates several possibilities of representing threats in BPMN 2.0, in particular for design-time specification and runtime execution of composite services with dynamic behavior. Enriching BPMN with threat information enables a process-centric threat modeling approach that complements risk assessment and attack scenarios. We have included examples showing the use of error events, escalation events and text annotations for process, collaboration, choreography and conversation diagrams.

Keywords: Business Process Modeling, Business Process Modeling Notation (BPMN), Composite Services, Dynamic Behavior, Service Oriented Architecture, Security, Threat, Trustworthiness

1. INTRODUCTION

A business process is used to define the goals of an organization, and consists of a set of activities that creates something of value – a product or a service – for the customers (Hammer & Champy, 1993). The Business Process Modeling Notation (BPMN) has lately become a de-facto standard language for capturing such business processes, in particular at the level of domain analysis and high-level systems design. While it was originally developed by the Business Process Management Initiative (BPMI), BPMN has since 2005 been standardized and maintained by the Object Management Group (OMG). The BPMN graphical notation was from the start targeted to be readily understood by all business users, from business analysis, to technical developers and those who monitor and manage the business processes (White,
2004). Visually, the notation has a lot in common with the features of flow-charts, and its core concepts should be familiar by people who already know other process languages. BPMN provides a wide range of graphical elements to enable representation of potentially complex process semantics, and now also several different modeling perspectives. It can accordingly be used in many different ways and modeling scenarios, from creating initial drafts of processes to evaluation and management of those same processes. In addition, later development has provided BPMN with well-defined execution semantics that enable the visual representations to be executed in business process engines, no longer dependent on vendor, and facilitate automated code generation. This allows for highly detailed formal process representations that can translate into simulations, or even operative server applications. A survey (Recker, 2008) conducted in 2007 among 590 BPMN modelers showed that already at that time BPMN was quite popular, both used for high level business (51%) and technical (49%) purposes.

As pointed out by Wolter et al. (2009): “it is evident that both security and business domain experts need to be able to define their security goals collaboratively on a common abstraction level, namely the business process model”. We believe that this argument holds for threats as well, which can compromise business goals and damage business critical assets. The term threat, as it underpins our work, has been defined by the US National Institute of Standards and Technology as “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service” (NIST, 2006).

Threats and possible attacks are already being modeled at the business level using various threat modeling dialects, for instance with data flow diagrams (Herman, Lambert, Ostwald, & Shostack, 2006), misuse cases (Sindre & Opdahl, 2005) or Coras (Lund, Solhaug, & Stølen, 2010). According to Shostack (2008), there is no single “best” or “correct” way of performing threat modeling, but rather a question of trade-offs and what we want to achieve by doing it. The purpose can for instance be to assess the risk of critical assets, to describe attacker methods motivation, or you want to analyze a system for exploitable weaknesses. Note that we consider threat modeling to be a sub-task or complementing activity to risk assessment since the focus is on identifying what and how things can go wrong, and not so much on probability and cost/consequence.

In our case we have very specific reasons for representing threats in BPMN. Our work revolves around using BPMN as a service specification language that can be used during service discovery and as a runtime execution language for composite services. We are specifically working with composite services with dynamic behavior (Kim, Kang, Meadows, Ioup, & Sample, 2009; Schaffner & Meyer, 2006; Meland, Guerenabarrena, & Llewellyn-Jones, 2011). These services are for instance able to swap a service component with a similar one, or deploy a completely new service configuration when there are changes to the external threat picture, the services themselves or the environment in which the services and consumers reside in. Our goal is to avoid downtime, and preserve the overall security and trustworthiness of the composite service in an ever-changing Internet of Services. To facilitate this we have seen the need to represent unwanted events, specifically threats, as a part of the process models governing the execution of the composite services. In this way we are able to specify under which circumstances the service execution should defer from its normal behavior and when the service runtime environment needs to react.

Our research method has been to investigate existing literature on BPMN and security, presented in section 2, and analyze the BPMN specifications and meta-model. We have experimented with several options for threat representation using the four diagram types found in BPMN 2.0, namely process, collaboration, choreography and conversation diagrams, and
Service-Composition: Concepts, Techniques, Tools and Trends
www.igi-global.com/chapter/service-composition-concepts-techniques-tools/28949?camid=4v1a

Security Issues of CPS
www.igi-global.com/chapter/security-issues-of-cps/121254?camid=4v1a