Automated Synthesis and Ranking of Secure BPMN Orchestrators

Vincenzo Ciancia, The “Alessandro Faedo” Institute of Information Science and Technology, Pisa, Italy
Jose Martin, The Institute of Informatics and Telematics, Pisa, Italy
Fabio Martinelli, The Institute of Informatics and Telematics, Pisa, Italy
Ilaria Matteucci, The Institute of Informatics and Telematics, Pisa, Italy
Marinella Petrocchi, The Institute of Informatics and Telematics, Pisa, Italy
Ernesto Pimentel, University of Malaga, Malaga, Spain

ABSTRACT

The authors describe a formal methodology for the automatic synthesis of a secure orchestrator for a set of BPMN processes. The synthesized orchestrator is able to guarantee that all the processes that are started reach their end, and the resulting orchestrator process is secure, that is, it does not allow the disclosure of certain secret messages. The authors present an implementation of a forth and back translation from BPMN to Crypto-CCS, that permits them to exploit the previously existing PaMoChSA tool to synthesize BPMN orchestrators. Furthermore, they study the problem of ranking orchestrators based on quantitative valuations of a process, the temporal evolution of such valuations, and their security, as a function of the knowledge of the attacker.

Keywords: BPMN, Partial Model Checking, Quantitative security, Synthesis of Processes, Security, Service Composition

1. INTRODUCTION

Mathematical methods in program semantics and security very often need to be validated through implementation and technology transfer. Traditionally, this task has been hindered by the gap between abstract results and applications. The advent of software engineering brought to light the so-called semi-formal languages and methods, such as Unified Modeling Language (UML) (Object Management Group. (2012)) or Business Process Model and Notation (BPMN) (Object Management Group. (2011)). These formalisms provide clean
syntax to support abstraction in software and system design, and in the development phase. Semi-formal methods are nowadays part of the standard background of software engineers, and may be used to bridge the mentioned gap, providing a clean path from theoretical results to implementation.

In this paper, we consider the research line of verification and synthesis of secure systems using partial model checking (Martinelli, 2003). In particular, we extend the work in Ciancia, Martin, Martinelli, Matteucci, Petrocchi, and Pimentel (2012) by exploiting the PaMoChSA tool for synthesizing secure BPMN orchestrator processes. The workflow we adopt is described in Figure 1. Crypto-CCS is a process calculus that features a tractable form of logical deduction, permitting one to encode various cryptographic primitives. In particular, the calculus faithfully models symmetric and asymmetric cryptography, and hashing.

In the semi-formal approach, various intended semantics can be assigned to a formalism, depending on the application context. Following this tradition, we provide a security-aware execution semantics to BPMN, incorporating secure communication facilities, by means of Crypto-CCS. This is done in Section 3, where we define BPMN processes that exchange cryptographic messages. More precisely, we use existing BPMN facilities to include asymmetric cryptography in the modeling language. In this way, existing tools may be used to design cryptography-aware systems. We provide a proof-of-concept implementation, in the form of two XQuery transformations. The first one translates a BPMN process into Crypto-CCS, whose syntax is represented using a custom XML format. The second transformation turns an XML representation of a sequential Crypto-CCS process back into a BPMN process. The translation is made to interoperate with the previously developed tool PaMoChSA, performing synthesis of (sequential) Crypto-CCS orchestrators (Ciancia, Martin, Martinelli, Matteucci, Petrocchi, & Pimentel, 2012). The result is a tool that accepts a BPMN collaboration diagram, containing a black-box process representing the orchestrator as input. The black-box in the original collaboration diagram is filled with the synthesized process that orchestrates the BPMN processes, driving all components to successful termination. The orchestrator is secure, in the sense that it uses asymmetric cryptography to forbid an attacker to learn a user-specified secret message.

Furthermore, we present a strategy based on semirings (Bistarelli, 2004) to evaluate different synthesized orchestrators so that it provides a ranking that drives the users to select the orchestrator that better fits their requirements. In particular, the ordering relation we propose here depends upon the knowledge of an attacker, so that a system is considered better than another, if it obtains better valuations for all the possible initial knowledge bases of the attacker, i.e., it discloses the least amount of information regardless the knowledge of the attacker.
Web Services for Groupware
[www.igi-global.com/chapter/web-services-groupware/28963?camid=4v1a](www.igi-global.com/chapter/web-services-groupware/28963?camid=4v1a)

Concern Separation for Adaptive QoS Modeling in Distributed Real-Time Embedded Systems
[www.igi-global.com/chapter/concern-separation-adaptive-qos-modeling/36339?camid=4v1a](www.igi-global.com/chapter/concern-separation-adaptive-qos-modeling/36339?camid=4v1a)