Jolita Ralyté · Sergio España
Óscar Pastor (Eds.)

The Practice of Enterprise Modeling

8th IFIP WG 8.1. Working Conference, PoEM 2015
Valencia, Spain, November 10–12, 2015
Proceedings

Springer

Editors
Jolita Ralyté
CUI, Battelle - Batiment A
University of Geneva
Carouge
Switzerland

Sergio España
Utrecht University
Utrecht
The Netherlands

Óscar Pastor
Department of Information Systems
and Computation
Universitat Politècnica de València
Valencia
Spain

ISSN 1865-1348 ISSN 1865-1356 (electronic)
Lecture Notes in Business Information Processing
ISBN 978-3-319-25896-6 ISBN 978-3-319-25897-3 (eBook)
DOI 10.1007/978-3-319-25897-3

Library of Congress Control Number: 2015952066

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

Welcome to the proceedings of the 8th Working Conference on the Practice of Enterprise Modelling (PoEM 2015) that was held during November 10–12 in the beautiful and modern city of Valencia, Spain, and hosted by the Research Center in Software Production Methods (PROS) of the Universidad Politécnica de Valencia.

Enterprise modelling (EM) encloses a set of activities by which several perspectives of an organization are elicited, documented, analyzed, and communicated, typically through a structured, iterative, stakeholder-centric, and model-based approach. This way, the knowledge of the enterprise is made explicit and further actions can be performed, such as making strategic decisions, undertaking organizational reengineering, standardizing ways of working, developing or acquiring information and communication technology, etc. As a consequence, EM has an impact on large economic markets such as consulting and information system development, making it a relevant field of research and industrial practice.

The PoEM series of conferences started in 2008 aiming at providing a forum for sharing experiences and knowledge of EM between the academic community and practitioners from industry and the public sector. PoEM is supported by the IFIP WG8.1 and is a very interesting and dynamic event where new research challenges emerge from EM practices – success and failure stories related by practitioners, and vice versa, practitioners take the opportunity to learn about new EM solutions.

This year, PoEM was very successful by receiving 72 submissions covering a large variety of EM topics. Each paper was evaluated by at least three Program Committee members and got constructive recommendations for further improvement. After examining the reviews, 23 papers were selected for presentation at the conference and are included in these proceedings. They are organized in eight sections corresponding to the conference sessions: Evolving Enterprises, Securing Enterprises, Making Empirical Studies, Investigating Enterprise Methods, Acquiring User Information, Managing Risks and Threats, Engineering Methods, and Making Decisions in Enterprises.

In addition to full research papers, we selected nine short papers presenting research works in progress and case studies. During the conference they were presented in dedicated sessions and are published in the CEUR online proceedings (CEUR-WS.org).

The conference audience also enjoyed three outstanding keynote presentations: two from academia and one from industry. Professor Pericles Loucopoulos from the Manchester Business School of the University of Manchester (UK) gave a talk on “What Could the Role of Enterprise Modelling Be During the 5th Economic Phase?” Professor Larry Constantine, a Fellow of the Association for Computing Machinery and a Life Member of the Industrial Designers Society of America, delivered a lecture on “Missing Models: Understanding Human Activity in the Enterprise.” Finally, a presentation with a practitioner perspective was given by a representative from industry, Rafael Montes,

from TecnoGram Procesos, on “Event Sourcing Implementation of a BPM System: A Practical Experience.”

This year’s PoEM introduced a few novelties – a traditionally two-day conference was extended by one day and complemented with three additional events: a workshop named AMINO (TowArds the Model drIveN Organization), a doctoral consortium, and a Young Entrepreneur Seminar (yes!PoEM 2015). We hope that all participants, both from academia and industry, enjoyed the scientific and social program of the conference and received inspiration for their research and industrial innovations.

To conclude, we would like to express our gratitude to a number of people who spent their time and energy in organizing and successfully running PoEM 2015. First of all we thank the Program Committee members and additional reviewers for their help in selecting the papers for the scientific program of the conference, the authors of the papers for their confidence in PoEM, and the presenters and session chairs for lively presentations and discussions. We are grateful to the PoEM Steering Committee chairs for their continuous assistance, and the chairs of workshops, doctoral consortium, and yes!PoEM for creating an exciting event. Finally, we extend our gratitude to the local organizing team at the Universidad Politécnica de Valencia for their hospitality and the organization of the social events of the conference.

November 2015

Jolita Ralyté
Sergio España
Óscar Pastor

Eliciting Security Requirements for Business Processes of Legacy Systems

Nikolaos Argyropoulos[1(✉)], Luis Márquez Alcañiz[2], Haralambos Mouratidis[1], Andrew Fish[1], David G. Rosado[3], Ignacio García-Rodriguez de Guzmán[3], and Eduardo Fernández-Medina[3]

[1] University of Brighton, Watts Building, Lewes Road, Brighton BN2 4GJ, UK
{n.argyropoulos,h.mouratidis,andrew.fish}@brighton.ac.uk
[2] Spanish National Authority for Markets and Competition (CNMC), Madrid, Spain
luis.marquez@cnmc.es
[3] University of Castilla-La Mancha, Paseo de la Universidad 4,
13071 Ciudad Real, Spain
{david.grosado,ignacio.grodriguez,eduardo.fdezmedina}@uclm.es

Abstract. The modernisation of enterprise legacy systems, without compromises in their functionality, is a demanding and time consuming endeavour. To retain the underlying business behaviour during their modernisation, the MARBLE^{TM} framework has been developed for the extraction of business process models from their source code. Building on top of that work, in this paper we propose an integrated approach for transforming the extracted legacy process models into Secure Tropos goal models. Such models facilitate the elicitation of security requirements in a high level of abstraction, which are then incorporated back into the process models of the modernised systems as security features. Therefore high level models can be derived from legacy source code with minimal manual intervention, where security can be elaborated by non-technical stakeholders in alignment with organisational objectives.

Keywords: Legacy systems · Business process modelling · Goal-oriented security requirements · Secure Tropos · BPMN · MARBLE

1 Introduction

The essence of legacy system migration is to move an existing, operational system to a new environment, retaining the functionality of the legacy system while causing as little disruption to the existing operational and business environment as possible [1]. Legacy system migration is a very expensive procedure which carries a definite risk of failure. Consequently before any decision to migrate is taken, an intensive study should be undertaken to quantify the risk and benefits and fully justify the redevelopment of the legacy system involved [2,3].

Reverse engineering techniques have become very important within the legacy system migration process, providing several benefits. Firstly, reverse engineering allows the retrieval of abstract representations to facilitate the comprehension

J. Ralyté et al. (Eds.): PoEM 2015, LNBIP 235, pp. 91–107, 2015.
DOI: 10.1007/978-3-319-25897-3_7

of different legacy systems, such as relational databases [4] and aspect oriented systems [5]. Secondly, abstract representations obtained by reverse engineering from legacy systems can be refactored to improve their maintainability or add new functionalities to evolve legacy systems. To meet these demands, business process archaeology has emerged as a set of techniques and tools to recover business processes from source code [6]. One of the main benefits of business process archaeology is that it preserves business behaviour buried in legacy source code and it retrieves business processes, thereby providing more opportunities for refactoring due to the higher abstraction level.

During business process refactoring new security features can also be introduced to evolve the legacy business processes. Since the advantages of the early identification of security requirements are recognised by the consensus of the RE literature [7,8], it is imperative that security concerns are taken into account during the early redesign stages of such systems. An advantage of eliciting security requirements in the early (re-)development stages is the lower possibility of security issues arising when the system is already in use, which would require redesigns and significant downtimes, thus proving costly for enterprises [9].

The security objectives of an enterprise are expressed via security requirements, which are used as input during the redesign of the business processes supported by such legacy systems. The development of *"secure by design"* business processes is considered highly beneficial as information security breaches can impact enterprises both financially and in terms of reputation and trust from the customer's side. It can also be a legal obligation to regulate and ensure the security of sensitive information handled by business processes [10]. However, despite its apparent importance and the potential to greatly benefit modern business processes, security is usually considered as an afterthought during their development in practice [11] and receives little attention from business process management (BPM) approaches developed in research [12,13].

In this work we present a novel approach for the modernisation of legacy systems from an information security point of view. It facilitates the elaboration of security requirements via Secure Tropos goal models, derived from legacy business processes which are automatically extracted from their legacy source code. Therefore, by integrating existing and novel components, the proposed approach facilitates a unique transformation of the lowest abstraction level of legacy systems (i.e., source code) to highly abstract enterprise models in a largely automated manner. As a result it offers to non-technical enterprise stakeholders a platform appropriate for capturing high-level organisational security objectives in the form of security requirements, which can then be integrated back to the business processes as security features.

The rest of the paper is structured as follows; Sect. 2 presents related work in the areas of process archaeology and goal-to-process model transformations. Section 3 introduces our approach and its four building blocks: (i) the MARBLE^{TM} framework for the derivation of a process models from legacy source code, (ii) the IBUPROFEN algorithms for the refactoring of the extracted process model, (iii) the Secure Tropos approach for security-oriented goal modelling and (iv) the

transformation algorithms for the transition from process to goal models and vice versa. In Sect. 4 our approach is applied to a module extracted from a real software application, while final conclusions are provided in Sect. 5.

2 Related Work

2.1 Process Archaeology

Business process archaeology [6] studies the business processes in an organization by analysing the existing software artefacts. The objective is to discover the business forces that motivated the construction of the enterprise information systems. On the one hand, traditional archaeologists investigate several artefacts and situations, trying to understand what they are looking at, i.e., they must understand the cultural and civilizing forces that produced those artefacts. Similarly, a business process archaeologist analyses different legacy artefacts such as source code, databases and user interfaces and then tries to learn what the organization was thinking while also attempting to understand why the organization developed the information system in a particular way. The business process archaeology initiative is being progressively supported by new reverse engineering techniques and tools to retrieve and elicit the embedded business knowledge. One of these tools is MARBLE^{TM} [14,15], a business process archaeology method to rebuild business processes embedded in legacy information systems.

2.2 Aligning Business Processes with Organisational Goals

The organisational context of the enterprise enacting a business process, provides valuable input for its successful (re-)design. Since graphical process modelling standards are not fully equipped to encapsulate such context, goal-oriented modelling languages are better suited for that purpose [16] since they can capture the intentions of stakeholders as system requirements [17]. Nevertheless, while goal models can provide a high-level direction and rationale in the form of goals, they lack the ability to adequately identify the specifics of their implementation at the process level. Thus goal-oriented requirements engineering (GORE) should be used more as a starting point, rather than a complete solution for the further development of process designs [18].

To that end, a number of approaches have been developed starting from goal models and eliciting business process designs. Mappings between organisational goals and process activities are introduced by such approaches in order to facilitate the transition between goal and process models. A variety of GORE frameworks have been utilised, such as KAOS in [19,20], Tropos in [21,22] and i* in [23–25]. Such generic model transformation approaches lack a clear security orientation so they are unable to capture the essence of security requirements, which, as opposed to functional requirements, act as restrictions on the means used for the achievement of goals.

To cover that need, certain security-oriented approaches have been developed. In [26], SecureBPEL is introduced as an extension of the BPEL execution standard enriched with constructs from the Secure Tropos goal-oriented framework, to enforce delegation and trust requirements in web services used to support the designed business process. In [27] the SecCo (Security via Commitments) framework is introduced for the elicitation of security requirements that need to be fulfilled by the organisation's business processes, through the modelling and analysis of objectives, roles and social commitments between actors. Similarly in [28], transformation rules expressed in SecBPMN are used to introduce security requirements, identified using STS-ml, to existing BPMN process models.

Nevertheless, such attempts are unable to incorporate concepts and mechanisms to deal with the whole range of security requirements and also take into account elements of risk analysis (e.g., threats). As a result, in order to cover all aspects of risk and security a number of such approaches have to be used simultaneously, leading to a large overhead in time and specialised personnel and a high level of complexity. In addition, the simple annotation of existing process models with elements of security is not aligned with the notion of *"security by design"*, which requires the derivation of such process designs from high level, security- and risk-aware organisational models. Moreover such attempts cannot adequately capture and reflect the rationale behind security decisions at an appropriate level of abstraction as they usually just impose general restrictions on the interactions between participants of the process (i.e., at conversation diagram level) but not on their specific activities (i.e., workflow level).

3 Proposed Approach

3.1 MARBLE™ Framework

MARBLE™ is a technique and a tool that supports business process archaeology by retrieving business processes from legacy source code [6]. MARBLE™ utilises an extensible, ADM-based framework for recovering business processes. To achieve that: (i) the information is collected into and is used from standard KDM (Knowledge Discovery Metamodel) [29] repositories and (ii) the information of KDM repositories is used to retrieve business process models [30].

MARBLE™ focuses on the reverse engineering stage of the re-engineering process. It proposes four abstraction levels (with four different kinds of models) as well as three model transformations between them, in order to cover the whole path of the business process archaeology method between legacy information systems and business processes (see Fig. 1). The four generic abstraction levels proposed in MARBLE™ are the following:

- Level L0. As the lowest level of abstraction, L0 represents the legacy information system (LIS) in the real world as a collection of different software artefacts (e.g. source code, database, documentation).
- Level L1. This level consists of several specific models, i.e., one model for each different software artefact involved in the archaeology process (e.g., source

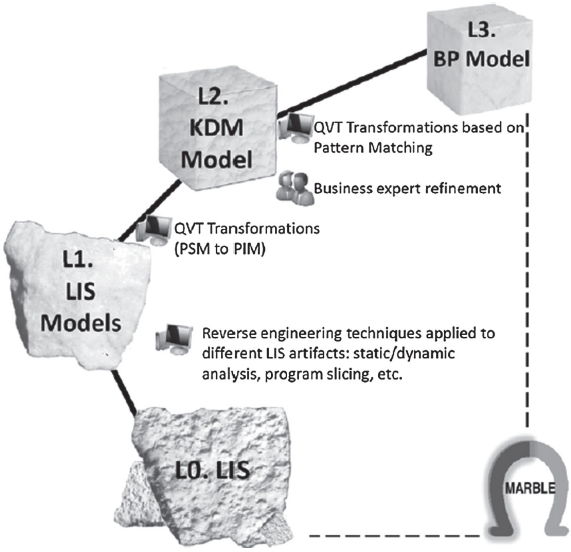

Fig. 1. MARBLE™, a framework to support business process archaeology [6]

code, database, user interfaces). These models are considered to be PSM (Platform-Specific Models) since they depict the software artefacts according to their specific technology or platforms.

- Level L2. It consists of a common PIM (Platform-Independent Model) which represents the integrated view of the set of PSM models at L1. The standard KDM metamodel is used for this purpose, since it makes it possible to model all the artefacts of the legacy system in an integrated and technological independent manner.
- Level L3. As the highest level of abstraction, L3 represents a computational independent model of the system. It depicts the business processes retrieved from the knowledge concerning legacy information systems represented in the KDM repository at L2. Business process models at L3 are represented according to the BPMN (Business Process Model and Notation) metamodel [31].

MARBLE™ provides a Java parser to obtain code models, which are transformed and integrated in a model repository according to the KDM standard. After that, KDMs are transformed to business process models by applying business pattern recognition. Finally, the tool allows the discovery, visualisation and editing of business process models. An in-depth elaboration of the framework's functionality and capabilities is provided at [6,14].

3.2 IBUPROFEN

Business process models derived via the reverse engineering approach followed by MARBLE™ often require some refinement before they can be utilised for

further transformations. For such purposes the IBUPROFEN *(Improvement and BUsiness Processes Refactoring OF Embedded Noise)* approach has been developed, which introduces a set of algorithms for the refactoring of business process models expressed in BPMN [32]. It introduces a set of ten refactoring algorithms which can be applied on business process models represented by graphs, expressed in BPMN. These ten refactoring algorithms are divided into three categories regarding their purpose, namely: maximization of relevant elements, fine-grained granularity reduction and completeness. An overview of the refactoring performed by each of these algorithms is provided in Fig. 2 and in [33].

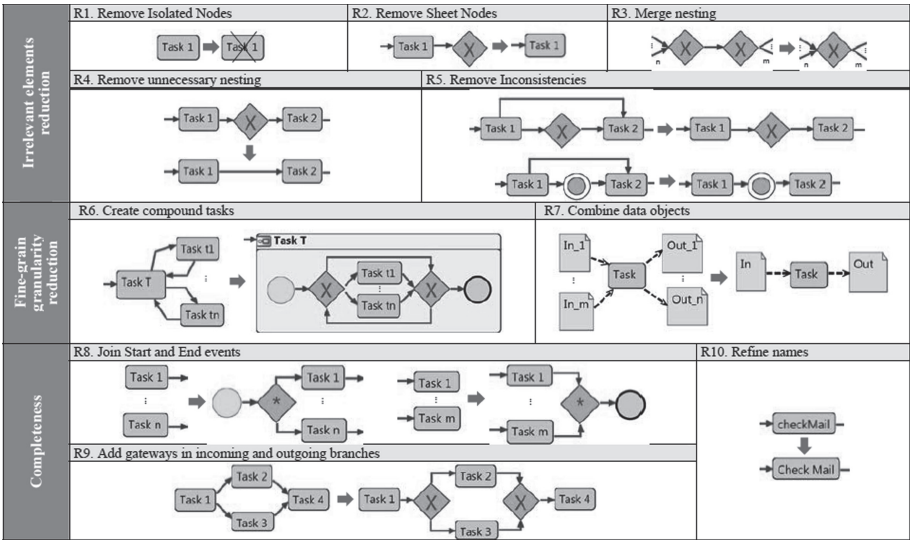

Fig. 2. Process model refactoring algorithms introduced by IBUPROFEN [33]

3.3 Secure Tropos

Secure Tropos [34] is a security-oriented extension of Tropos, a goal-oriented requirements engineering method. This extension includes the concept of security constraint which is defined as a restriction related to security issues, such as privacy, integrity, and availability [35]. Security constraints can influence the analysis and design of the information system under development by restricting some alternative design solutions, by conflicting with some of the requirements of the system, or by refining some of the system's objectives. In addition, Secure Tropos defines secure dependencies which introduces security constraints that must be fulfilled for the dependency to be satisfied. A security mechanism represents potential solutions for the implementation of the security constraints, leading to the fulfilment of security objectives. The advantages of this approach,

compared to other security-oriented software engineering approaches are: (i) its ability to perform social analysis during the early requirements stage, (ii) the simultaneous consideration of security with the other requirements of the system-to-be, (iii) the support for not only requirements stages but also design stages.

3.4 Model Transformations

A series of transformation rules need to be defined in order to facilitate the transition from business process models, expressed in BPMN and derived from legacy source code using the MARBLE^{TM} framework (Fig. 3 *Phase 1*), to Secure Tropos goal models. This process-to-goal transformation will create an additional, higher level of abstraction, represented by a goal model of the legacy system. At this level of abstraction it is easier for non-technical stakeholders to elaborate on the overall system security by defining certain easily comprehensible constraints. Such constraints can be captured by the Secure Tropos goal model and mapped back onto the process model, in order to be implemented during the redesign of the legacy systems.

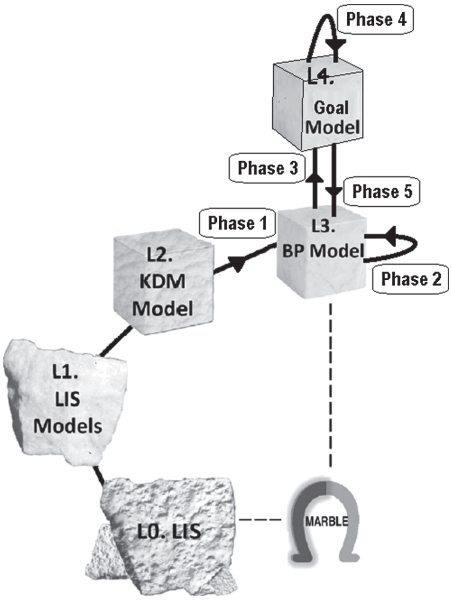

Fig. 3. Extended framework to accommodate goal model reasoning

Essentially, the proposed transformation aims to derive a goal model, on which security will be elaborated and expressed using Secure Tropos. A goal-to-process transformation can then be performed, beginning from the Secure Tropos goal model and deriving a secure business process model, used as input for

the legacy system redevelopment via the MARBLE^{TM} framework. The overall process, containing an extra level of abstraction accommodating the security-oriented, goal model reasoning is illustrated in Fig. 3 and summed-up in Subsect. 3.5.

Transformation rules have been defined which map Secure Tropos and BPMN concepts to each other and provide instructions on how the transformation can take place. Such mappings are based on conceptual similarities between the paired concepts, identified after semantic analysis of the formal documentation and meta-models of the two modelling approaches [31,34]. A process-to-goal transformation algorithm has been defined at Table 1, utilised in order to transform the refactored process model by IBUPROFEN (Fig. 3 *Phase 2*) to a Secure Tropos goal model (Fig. 3 *Phase 3*).

Table 1. Algorithm for Phase 3 of the transformation process

Step 1	*For each* **lane** (l) of the process model:
	Create a corresponding **actor** $a(l)$ in the goal model
Step 2	*For each* **sub-process** (p) of the process model:
	Create a corresponding **goal** $g(p)$ in the goal model
	For each of the **sub-activities** (p') of p:
	Create a corresponding **sub-goal** $g(p')$, within $g(p)$
Step 3	*For each* **data object** (d) of the process model:
	Create a corresponding **resource** $r(d)$ in the goal model
Step 4	*For each* **message exchange** (m) of the process model, between two activities (p_s, p_r) in two different lanes (l_s, l_r):
	Create a **dependency link** $dl(m)$ in the goal model, from the dependent goal ($g(p_s)$) to the dependee actor $a(l_r)$
Step 5	*For each* **exclusive** or **inclusive gateway** (x) between sub-activities $(p_1, ..., p_n)$ of the process model:
	Create an **OR** or **AND decomposition** $or(x)$ of the corresponding goals $(g(p_1), ..., g(p_n))$ in the goal model

By the application of the above transformation rules to a process model derived by the MARBLE^{TM} framework and refactored using the IBUPROFEN algorithms, a basic Secure Tropos goal model can be produced. This basic goal model is the main input upon which the security elaboration of the system will take place by stakeholders of the organisation. As a result of this security elaboration, security constraints, objectives and mechanisms are added to the Secure Tropos goal model to capture the security aspects that will be introduced to the legacy system during its redesign (Fig. 3 *Phase 4*).

The security-oriented concepts of Secure Tropos (i.e., security constraints, mechanisms and threats) cannot be directly mapped onto existing BPMN concepts. Therefore, some manual tasks need to be performed in order for the process

Table 2. Algorithm for Phase 5 of the transformation process

Step 1	*For each* **goal** ($g(p)$) or **resource** ($r(d)$) of the goal model, restricted by a *security constraint* (sc):
	Annotate the corresponding **activity** (p) or **data object** (d) of the process model
Step 2	*For each* **security mechanism** (sm) of the goal model:
	Create a **"secure" activity** (sp) in the process model, connected to the annotated activities (p) or data objects (d)
Step 3	*For each* **threat** (t) on a goal ($g(p)$) or resource ($r(d)$) of the goal model:
	Create a corresponding **error event** (e) in the process model, connected to the threatened activities (p) or data objects (d)

model to reflect the security choices captured at the goal model level (Fig. 3 *Phase 5*). Table 2 presents an algorithm providing a precise set of instructions for performing such goal-to-process refinement tasks.

3.5 Overview of Approach

As illustrated in Fig. 3, the proposed approach consists of the following phases:

1. *Extraction* of BPMN process models from the source code of the legacy system using the automated MARBLE^{TM} tool [15].
2. *Refactoring* of the extracted process model using the IBUPROFEN algorithms, automated via an Eclipse plugin [32].
3. *Process-to-goal transformation* using the algorithm of Table 1 to create an initial goal model from the refactored BPMN process model.
4. *Security elaboration* for deriving security requirements, threats and security mechanisms using the Secure Tropos approach via the SecTro tool [36].
5. *Process model refinement* using the algorithm of Table 2 for the addition of the security features elaborated at the Secure Tropos goal model.

The result of the application of above approach is a secure business process model, aligned with the high-level enterprise security objectives. This process model, which operationalises the security requirements captured at the goal model level, can be then used as input for the legacy system redevelopment effort, as proposed by the MARBLE^{TM} framework. Therefore the security features introduced at a high level from the organisation's stakeholders will be included at the legacy system during its modernisation.

4 Illustrative Example

4.1 System Description

JBooks[1] is a Java-based personal finance application utilising a checkbox based interface that allows users to insert and visualize transactions. It is interfaced

[1] Available at: http://freshmeat.net/projects/jbooks/.

with a relational database, and involves a double-entry system for all transactions (i.e., every transaction involves a transfer from one account to another). A module of the JBooks application was selected for the purposes of this example. This module receives a string as input and if it is numeric it converts it to text in order to be further utilised by other modules of the application.

4.2 Method Application

The first phase of the method application is the extraction of a process model from the source code of the JBooks application. By using the MARBLE^{TM} tool we extracted a large amount of process models for the different modules of the JBooks application. For this example we selected a relatively simple process model representing the module that converts numerical strings to text.

After the initial process model is extracted via the MARBLE^{TM} tool it is refactored by applying the algorithms of IBUPROFEN. During refactoring some elements of the process model are replaced by equivalent ones or merged to reduce the complexity of the overall model. Since the refactoring process does not fulfill the commutative property, the order of the application of the algorithms is critical as it can define the quality of the outcome model [33]. The optimal execution order that maximises the understandability and modifiability of the process model has been experimentally identified as: first applying the granularity reduction set of algorithms, then the irrelevant elements reduction set of algorithms and finally the completeness algorithms [33]. The IBUPROFEN algorithms are implemented as a plugin of the Eclipse^{TM} environment on the process model extracted by the MARBLE^{TM} tool. In our example, after applying the refactoring algorithms, the process model illustrated in Fig. 4 is derived.

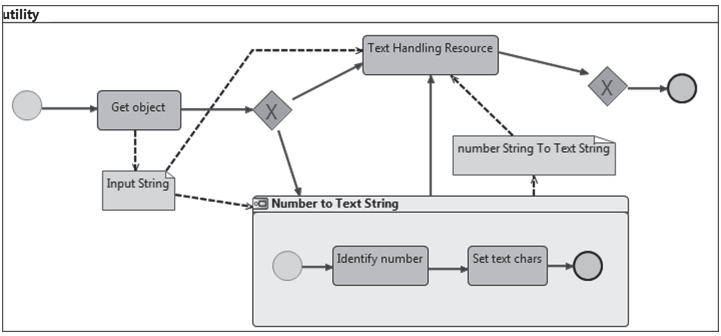

Fig. 4. Process model of JBooks module

Next, the transformation of the derived process model to a Secure Tropos goal model need to be performed. By applying the algorithm in Table 1 to our example one actor is created to correspond to the lane of the process model

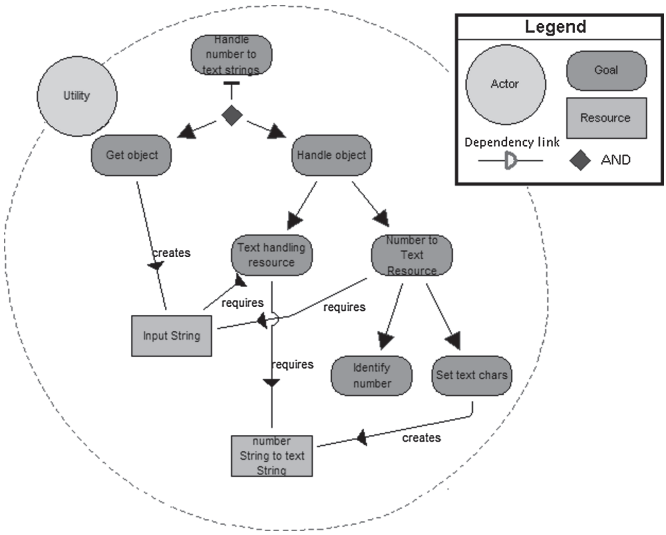

Fig. 5. Derived goal model of selected JBooks module

(Step 1), each sub-process and task is transformed to a (sub-)goal *(Step 2)* and resources are created, corresponding to the data object of the process model *(Step 3)*. In addition to the transformation steps defined by the algorithm, an extra root-level goal has been added to provide context to the derived Secure Tropos goal model, modelled using the SecTro tool [36], as illustrated in Fig. 5.

As goal models in general, and Secure Tropos in our case, do not provide the means to capture temporal dimensions (i.e., the sequence of goal achievement), the resulting models cannot always capture all the information contained in process models. In our example, the application of *Step 5* of the transformation algorithm cannot sufficiently capture in the goal model the fact that the activity "Get Object" is followed by either "Text handling resource" or "Number to Text resource". This is due to the fact that Secure Tropos does not offer special notation for illustrating OR decompositions or the specific sequence of execution of goals. In order to resolve this issue a new goal had to be manually added ("Handle object") which includes the two alternatives (i.e., "Text handling resource" or "Number to Text resource") as sub-goals and is connected with an AND relationship with the "Get Object" sub-goal.

During security elaboration process the system stakeholders can express their security requirements and define the basic mechanisms to implement them, using the goal model as a high level representation of the application. For simplicity purposes, our example includes one security constraint, concerning the validity of the input. It is related to the integrity of the input data and can be implemented by a security mechanism validating that it has not been altered before it reached the module. A threat has also been included in the goal model representing the malicious alteration of the module's input by a third party. The complete, security-annotated goal model is presented in Fig. 6.

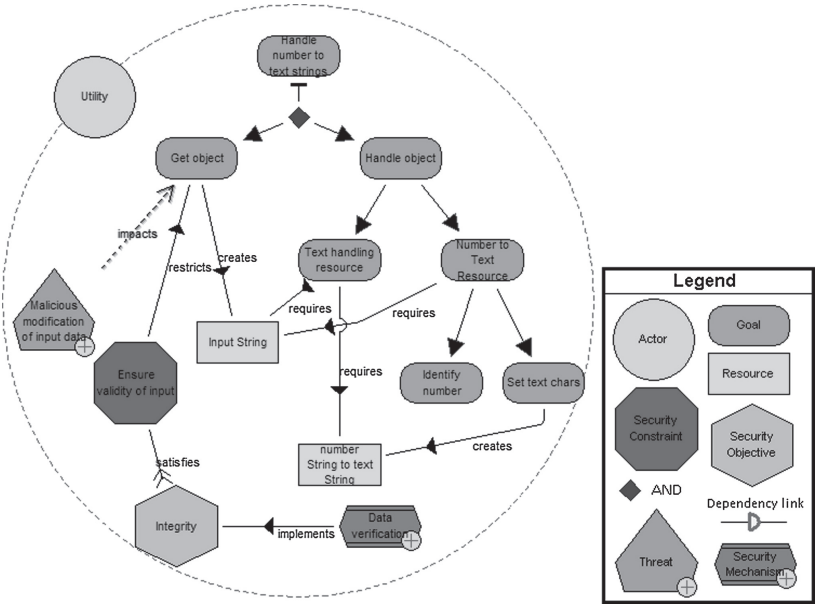

Fig. 6. Security-annotated goal model of JBooks module

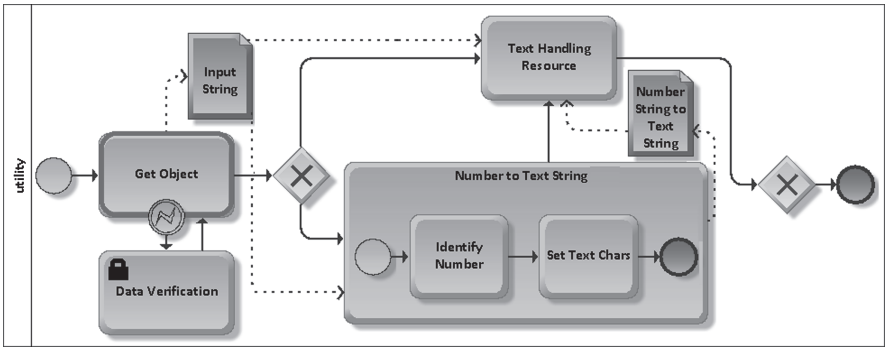

Fig. 7. Secure BPMN process model of JBooks module (Color figure online)

Finally, the security introduced at the goal model level has to be transferred back to the initial process model, by following the steps defined in Table 2. The finalised secure process model, illustrated at Fig. 7, now includes a secure task, denoted by a padlock symbol, representing the data validation security mechanism. The "Get Object" task is annotated with a red border to denote that it is security constraint while it is also an error event, annotated as an orange circle, is attached to represent the malicious data modification threat.

4.3 Lessons Learned

The addition of security in a module of the JBooks legacy system provided insights concerning the completeness and applicability of the proposed approach. Even though the example used was rather limited in size and complexity, we were able to successfully complete each step of our approach without any major complications. Some manual intervention was necessary after the refactoring of the process model in order to make the produced model more readable (e.g., reshaping and spacing elements and association links). Moreover the seamless transition between its different components added to the value of the approach, facilitated by the fact that the output for each phase can be used quite effortlessly as the input of the next. The availability of CASE tools (e.g., MARBLE^{TM} tool, IBUPROFEN plugin, SecTro tool) further contributed in the aspect of automation, as most phases, with the exception of the goal-to-process transformation, required minimal manual efforts. By expanding and interfacing the available support tools, this automation can be further strengthened in the future.

Regarding the transformation process, one addition to the proposed algorithm consisted of creating a root-level goal in the produced goal model, which was decomposed to the rest of the goals and encapsulated the overall purpose of the module. This was performed for reasons of completeness and comprehensibility of the goal model by stakeholders and had no further impact on the rest of the approach. Another point requiring further attention is the inadequacy of goal models to capture the exact sequence by which their (sub-)goals should be accomplished, especially when complex branching (e.g., inclusive, exclusive gateways) is present at the process model. This led to the need for some manual intervention during the fifth step of our transformation algorithm, as explained in the previous section. To address this issue in the future, extensions at the notation of Secure Tropos will be explored, along with the refinement of the transformation rules defined in the algorithm.

5 Conclusion

The modernisation of enterprise legacy systems can be a demanding and time consuming endeavour. In order to facilitate that process, the MARBLE^{TM} framework has been developed for the extraction of process models from legacy source code. Such process models offer a more comprehensible and flexible platform for the elaboration of potential redesigns of the legacy system in question. The IBUPROFEN framework was also developed since the extracted process models often required some refinement (e.g., removal of excess notation, completeness).

In this work we extend these frameworks by introducing an algorithmic approach for the transformation of the derived business process models to goal models. Goal models provide the means necessary for the elaboration of security for the redesigned legacy system, at a high abstraction level, comprehensible by non-technical stakeholders and aligned with organisational objectives. Using a set of transformation rules, goal models can be created based on such business process models. Secure Tropos offers the means for capturing the security

related aspects of the redesigned system (e.g., security constraints, mechanisms, threats), which can then be incorporated back into the process model via a set of goal-to-process transformation rules. As a result, security choices of the system's stakeholders can be operationalised by the redesigned business processes.

An illustrative example of a legacy system module was utilised as a proof of concept for the proposed transformation approach and led us to useful conclusions about its completeness and effectiveness. Its application resulted in an accurate goal model representation of the selected legacy system's module, upon which security was successfully elaborated and then introduced back into the process model. Some complications sourced from certain elements of process models (i.e., sequence of execution, branching) which cannot always be translated to goal modelling concepts without losing certain information. Nevertheless, this example provided valuable insight on the applicability of the proposed approach while it also brought into consideration aspects which require further attention.

Overall, this novel approach could be a valuable tool for both practitioners and researchers, attempting to introduce security to existing business processes, starting from a high level of abstraction, which allows the alignment of security choices with the overall organisational strategy. Despite the emphasis in business processes extracted from legacy source code, the transformation algorithms introduced by this approach can be utilised for the introduction of security to any available process model, newly designed or already existing. This approach will also be integrated in the extraction activity of a migration process of legacy systems to the cloud (SMILE2Cloud) in which we are currently working [37,38].

Future work will look into the formalisation of the existing transformation algorithms using QVT and the potential addition of further steps or activities in order to eliminate any flaws during the transition between goal and process models and vice versa. As soon as a set of concrete transformation rules has been explicitly defined via an appropriate formal language, already existing support tools (e.g. SecTro tool, Eclipse plugins) can be further extended to automate the majority of this transformation, thus limiting the need for manual intervention. Finally, the validation of this approach via a case study would add great value, especially if it involves a large and more complex enterprise legacy system along with the participation of its stakeholders and analysts.

Acknowledgments. This research is part of the following projects: SERENIDAD (PEII11-037-7035) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain) and FEDER, and SIGMA-CC (TIN2012-36904) financed by the "Ministerio de Economía y Competitividad" (Spain).

References

1. Wu, B., Lawless, D., Bisbal, J., Grimson, J., Wade, V., O'Sullivan, D., Richardson, R.: Legacy system migration: a legacy data migration engine. In: 17th International Database Conference, pp. 129–138 (1997)
2. Bisbal, J., Lawless, D., Wu, B., Grimson, J.: Legacy information systems: issues and directions. IEEE Softw. **16**(5), 103–111 (1999)

3. Bisbal, J., Lawless, D., Wu, B., Grimson, J., Wade, V., Richardson, R., Sullivan, D.O.: A Survey of Research into Legacy System Migration. Technical report (1997)
4. Cleve, A., Hainaut, J.L.: Dynamic analysis of SQL statements for data-intensive applications reverse engineering. In: 15th IEEE Working Conference on Reverse Engineering, pp. 192–196. IEEE Computer Society (2008)
5. Bernardi, M.: Reverse engineering of aspect oriented systems to support their comprehension, evolution, testing and assessment. In: 12th IEEE European Conference on Software Maintenance and Reengineering, pp. 290–293. IEEE Computer Society (2008)
6. Pérez-Castillo, R., De Guzmán, I.G.R., Piattini, M.: Business process archeology using MARBLE. Inf. Softw. Technol. **53**(10), 1023–1044 (2011)
7. Liu, L., Yu, E., Mylopoulos, J.: Security and privacy requirements analysis within a social setting. In: 11th IEEE International Requirements Engineering Conference, pp. 151–161. IEEE Computer Society (2003)
8. Mellado, D., Fernández-Medina, E., Piattini, M.: A common criteria based security requirements engineering process for the development of secure information systems. Comput. Stan. Interfaces **29**(2), 244–253 (2007)
9. Whitman, M.E.: Enemy at the gate: threats to information security. Commun. ACM **46**(8), 91–95 (2003)
10. Leitner, M., Rinderle-Ma, S.: A systematic review on security in process-aware information systems - constitution, challenges, and future directions. Inf. Softw. Technol. **56**(3), 273–293 (2014)
11. Neubauer, T., Klemen, M., Biffl, S.: Secure business process management: a roadmap. In: 1st IEEE International Conference on Availability, Reliability and Security, Vienna, Austria, pp. 457–464. IEEE Computer Society (2006)
12. Pavlovski, C.J., Zou, J.: Non-functional requirements in business process modeling. In: 5th Asia-Pacific Conference on Conceptual Modelling, pp. 103–112 (2008)
13. Rodríguez, A., Fernández-Medina, E., Trujillo, J., Piattini, M.: Secure business process model specification through a UML 2.0 activity diagram profile. Decis. Support Syst. **51**(3), 446–465 (2011)
14. Pérez-Castillo, R., De Guzmán, I.G.R., vila Garca, O., Piattini, M.: MARBLE: modernization approach for recovering business processes from legacy information systems. In: International Workshop on Reverse Engineering Models from Software Artifacts, pp. 17–20 (2009)
15. Pérez-Castillo, R., Fernández-Ropero, M., De Guzmán, I.G.R., Piattini, M.: MARBLE. A business process archeology tool. In: 27th IEEE International Conference on Software Maintenance, pp. 578–581. IEEE Computer Society (2011)
16. Ko, R.K., Lee, S.S., Lee, E.W.: Business process management (BPM) standards: a survey. Bus. Process Manage. **15**(5), 744–791 (2009)
17. Lapouchnian, A., Yu, Y., Mylopoulos, J.: Requirements-driven design and configuration management of business processes. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 246–261. Springer, Heidelberg (2007)
18. Horkoff, J., Li, T., Li, F.L., Salnitri, M., Cardoso, E., Giorgini, P., Mylopoulos, J., Pimentel, J.A.: Taking goal models downstream: a systematic roadmap. In: 8th IEEE International Conference on Research Challenges in Information Science, pp. 1–12. IEEE Computer Society (2014)
19. Koliadis, G., Ghose, A.: Relating business process models to goal-oriented requirements models in KAOS. In: Hoffmann, A., Kang, B.-H., Richards, D., Tsumoto, S. (eds.) PKAW 2006. LNCS (LNAI), vol. 4303, pp. 25–39. Springer, Heidelberg (2006)

20. Ghose, A.K., Narendra, N.C., Ponnalagu, K., Panda, A., Gohad, A.: Goal-driven business process derivation. In: Kappel, G., Maamar, Z., Motahari-Nezhad, H.R. (eds.) ICSOC 2011. LNCS, vol. 7084, pp. 467–476. Springer, Heidelberg (2011)
21. Pistore, M., Roveri, M., Busetta, P.: Requirements-driven verification of web services. Electron. Notes Theor. Comput. Sci. **105**, 95–108 (2004)
22. Guizzardi, R.S.S., Guizzardi, G., Almeida, J.P.A., Cardoso, E.: Bridging the gap between goals, agents and business processes. In: 4th International i* Workshop, pp. 46–51. CEUR (2010)
23. Lo, A., Yu, E.: From business models to service-oriented design: a reference catalog approach. In: Parent, C., Schewe, K.-D., Storey, V.C., Thalheim, B. (eds.) ER 2007. LNCS, vol. 4801, pp. 87–101. Springer, Heidelberg (2007)
24. Decreus, K., Poels, G.: A goal-oriented requirements engineering method for business processes. In: Soffer, P., Proper, E. (eds.) CAiSE Forum 2010. LNBIP, vol. 72, pp. 29–43. Springer, Heidelberg (2011)
25. Ruiz, M., Costal, D., España, S., Franch, X., Pastor, O.: GoBIS: an integrated framework to analyse the goal and business process perspectives in information systems. Inf. Syst. **53**, 330–345 (2015)
26. Séguran, M., Hébert, C., Frankova, G.: Secure workflow development from early requirements analysis. In: 6th IEEE European Conference on Web Services, pp. 125–134. IEEE Computer Society (2008)
27. Paja, E., Giorgini, P., Paul, S., Meland, P.H.: Security requirements engineering for secure business processes. In: Niedrite, L., Strazdina, R., Wangler, B. (eds.) BIR Workshops 2011. LNBIP, vol. 106, pp. 77–89. Springer, Heidelberg (2012)
28. Salnitri, M., Giorgini, P.: Transforming socio-technical security requirements in SecBPMN security policies. In: 7th International i* Workshop. CEUR (2014)
29. ISO/IEC 19506: Information technology - Object Management Group Architecture-Driven Modernization (ADM) - Knowledge Discovery Meta-Model (KDM). Technical report (2012)
30. Pérez-Castillo, R., Cruz-Lemus, J.A., De Guzmán, I.G.R., Piattini, M.: A family of case studies on business process mining using MARBLE. J. Syst. Softw. **85**(6), 1370–1385 (2012)
31. Object Management Group: Business Process Model and Notation (BPMN) Version 2.0. Technical report (2011)
32. Fernández-Ropero, M., Pérez-Castillo, R., Piattini, M.: Graph-based business process model refactoring. In: 3rd International Symposium on Data-driven Process Discovery and Analysis, pp. 16–30. CEUR (2013)
33. Fernández-Ropero, M., Pérez-Castillo, R., Cruz-Lemus, J.A., Piattini, M.: Assessing the best-order for business process model refactoring. In: 28th Annual ACM Symposium on Applied Computing, pp. 1397–1402. ACM (2013)
34. Mouratidis, H., Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. Int. J. Softw. Eng. Knowl. Eng. **17**(02), 285–309 (2007)
35. Mouratidis, H., Jurjens, J.: From goal-driven security requirements engineering to secure design. Int. J. Intell. Syst. **25**, 813–840 (2010)
36. Pavlidis, M., Islam, S., Mouratidis, H.: A CASE tool to support automated modelling and analysis of security requirements, based on secure tropos. In: Nurcan, S. (ed.) CAiSE Forum 2011. LNBIP, vol. 107, pp. 95–109. Springer, Heidelberg (2012)
37. Márquez, L., Rosado, D.G., Mouratidis, H., Mellado, D., Fernández-Medina, E.: A framework for secure migration processes of legacy systems to the cloud. In: Persson, A., Stirna, J. (eds.) CAiSE 2015 Workshops. LNBIP, vol. 215, pp. 507–517. Springer, Heidelberg (2015)

38. Shei, S., Márquez Alcañiz, L., Mouratidis, H., Delaney, A., Rosado, D.G., Fernández-Medina, E.: Modelling secure cloud systems based on system requirements. In: 2nd Evolving Security & Privacy Requirements Engineering Workshop: Co-located with the 23rd IEEE International Requirements Engineering Conference, pp. 19–24 (2015)