Lecture Notes in Computer Science

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available.

The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes

- proceedings (published in time for the respective conference)
- post-proceedings (consisting of thoroughly revised final full papers)
- research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.)

More recently, several color-cover sublines have been added featuring, beyond a collection of papers, various added-value components; these sublines include

- tutorials (textbook-like monographs or collections of lectures given at advanced courses)
- state-of-the-art surveys (offering complete and mediated coverage of a topic)
- hot topics (introducing emergent topics to the broader community)

In parallel to the printed book, each new volume is published electronically in LNCS Online.

Detailed information on LNCS can be found at
www.springer.com/lncs

Proposals for publication should be sent to
LNCS Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany
E-mail: lncs@springer.com

ISSN 0302-9743

ISBN 978-3-540-76291-1

Lecture Notes in Computer Science
LNCS LNAI LNBI

springer.com

Hainaut et al. (Eds.)

LNCS 4802

Advances in Conceptual Modeling – Foundations and Applications

ER 2007 Workshops

LNCS 4802

Advances in Conceptual Modeling – Foundations and Applications

**ER 2007 Workshops CMLSA, FP-UML, ONISW, QoIS, RIGiM, SeCoGIS
Auckland, New Zealand, November 2007, Proceedings**

Springer

Lecture Notes in Computer Science 4802

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Jean-Luc Hainaut Elke A. Rundensteiner
Markus Kirchberg Michela Bertolotto
Mathias Brochhausen Yi-Ping Phoebe Chen
Samira Si-Saïd Cherfi Martin Doerr Hyoil Han
Sven Hartmann Jeffrey Parsons Geert Poels
Colette Rolland Juan Trujillo Eric Yu
Esteban Zimányi (Eds.)

Advances in Conceptual Modeling – Foundations and Applications

ER 2007 Workshops CMLSA, FP-UML,
ONISW, QoIS, RIGiM, SeCoGIS
Auckland, New Zealand, November 5-9, 2007
Proceedings

Springer

Volume Editors

Jean-Luc Hainaut E-mail: jean-luc.hainaut@fundp.ac.be
Elke A. Rundensteiner E-mail: rundenst@cs.wpi.edu
Markus Kirchberg E-mail: M.Kirchberg@massey.ac.nz
Michela Bertolotto E-mail: michela.bertolotto@ucd.ie
Mathias Brochhausen E-mail: mathias.brochhausen@ifomis.uni-saarland.de
Yi-Ping Phoebe Chen E-mail: phoebe@deakin.edu.au
Samira Si-Saïd Cerfi E-mail: sisaid@cnam.fr
Martin Doerr E-mail: martin@ics.forth.gr
Hyoil Han E-mail: hhan@ischool.drexel.edu
Sven Hartmann E-mail: s.hartmann@massey.ac.nz
Jeffrey Parsons E-mail: jeffreyp@mun.ca
Geert Poels E-mail: geert.poels@ugent.be
Colette Rolland E-mail: rolland@univ-paris1.fr
Juan Trujillo E-mail: jtrujillo@dlsi.ua.es
Eric Yu E-mail: eric.yu@utoronto.ca
Esteban Zimányi E-mail: ezimanyi@ulb.ac.be

Library of Congress Control Number: 2007938044

CR Subject Classification (1998): H.2, H.4, H.3, F.4.1, D.2, C.2.4, I.2, J.1

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743
ISBN-10 3-540-76291-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76291-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12181322 06/3180 5 4 3 2 1 0

Preface

The 26th International Conference on Conceptual Modeling in Auckland, New Zealand, hosted six workshops which allowed participants to focus their presentations and discussions on advanced topics that cannot easily fit the general conference scope.

Thirteen good quality proposals were received and nine were selected. Due to the similarity of their scope, two pairs were suggested to merge, leading to seven proposals. One workshop attracted fewer submissions than expected, so that its selected papers were integrated into the conference. Finally, six workshops were kept. Interestingly, four of them (FP-UML, ONISW, QoIS, SeCoGIS) were a sequel of workshops that were held in the last few years, while two were new (CMLSA, RIGiM), exhibiting both the maturity and the innovation of the workshops.

Following the call for papers, we received 114 complete submissions, from which 40 quality papers were selected, giving an acceptance rate of 35% (a fairly standard score for workshops).

The following six workshops were organized:

- Conceptual Modelling for Life Sciences Applications (CMLSA 2007), chaired by Yi-Ping Phoebe Chen and Sven Hartmann. This workshop addressed the specific challenges posed by the large data volumes, the complexity and the data and software heterogeneity involved by life science applications.
- Foundations and Practices of UML (FP-UML 2007), chaired by Juan Trujillo and Jeffrey Parsons. The third edition of this workshop gathered researchers and practitioners on topics related to data warehouses, security, model transformation, state diagrams development and model quality.
- Ontologies and Information Systems for the Semantic Web (ONISW 2007), chaired by Mathias Brochhausen, Martin Doerr and Hyoil Han. The second edition of this workshop focused on the potential and actual roles of ontologies in Web information systems. In particular, the papers addressed ontology extraction from texts, ontology interoperability, automatic semantic annotation and domain modeling.
- Quality of Information Systems (QoIS 2007), chaired by Samira Si-Saïd Cherfi and Geert Poels. The papers of the third edition of this workshop dealt with quality models, model understandability and (at last!) quality assessment of scientific conferences.
- Requirements, Intentions and Goals in Conceptual Modeling (RIGiM 2007), chaired by Colette Rolland and Eric Yu. The workshop goal was to explore the relations between requirements engineering and conceptual modeling. The selected papers particularly addressed such topics as model-driven approaches, the use of i*, refinement of goal-based methodologies, elicitation techniques and visualization.

- Semantic and Conceptual Issues in Geographic Information Systems (SeCoGIS 2007), chaired by Esteban Zimányi and Michela Bertolotto. The fourth edition of this workshop included presentations on data interoperability, spatial data warehouses, spatial data querying, data quality, conceptual modeling, spatio-temporal aspects of moving objects as well as special spatial applications.

We are particularly grateful to all the workshop organizers, the Program Committee members and the authors for the time and effort spent to guarantee the high quality of the programs. Special thanks are due to Markus Kirchberg who took charge of most of the editorial work of these proceedings.

November 2007

Jean-Luc Hainaut
Elke A. Rundensteiner

ER 2007 Conference Organization

General Chair

Bernhard Thalheim (Christian Albrechts University Kiel, Germany)

Program Committee Co-chairs

Christine Parent (University of Lausanne, Switzerland)
Klaus-Dieter Schewe (Massey University, New Zealand)
Veda C. Storey (Georgia State University, USA)

Organization Chair

Gillian Dobbie (University of Auckland, New Zealand)

Steering Committee Liaison

Tok Wang Ling (National University of Singapore, Singapore)

Publicity chair

Markus Kirchberg (Massey University, New Zealand)

Workshop Co-chairs

Jean-Luc Hainaut (University of Namur, Belgium)
Elke A. Rundensteiner (Worcester Polytechnic Institute, USA)

Tutorial Co-chairs

Sven Hartmann (Massey University, New Zealand)
Alberto H.F. Laender (UFMG, Brazil)

Panel Chair

John F. Roddick (Flinders University, Australia)

Industrial Chair

John Grundy (University of Auckland, New Zealand)

Demonstration and Poster Chair

Leszek Maciaszek (Macquarie University, Australia)

Treasurers

Patricia Rood (University of Auckland, New Zealand)
Stephen W. Liddle (Brigham Young University, USA)

Organized By

Massey University, New Zealand
The University of Auckland, New Zealand

Sponsored By

The ER Institute

In Cooperation With

ACM SIGMIS
ACM SIGMOD

ER 2007 Workshop Organization

ER 2007 Workshop Co-chairs

Jean-Luc Hainaut, University of Namur, Belgium
Elke A. Rundensteiner Worcester Polytechnic Institute, USA

CMLSA 2007 – International Workshop on Conceptual Modelling for Life Sciences Applications

Workshop Chairs

Yi-Ping Phoebe Chen, Deakin University, Australia
Sven Hartmann, Massey University, New Zealand

Publicity Chair

Markus Kirchberg, Massey University, New Zealand

Program Committee

Isabelle Bichindaritz, USA
Leonard N. Bloksberg, New Zealand
Jake Chen, USA
Alexei Drummond, New Zealand
Silke Eckstein, Germany
Amarnath Gupta, USA
David Hansen, Australia
Peter Hunter, New Zealand
Nikola Kasabov, New Zealand
Dirk Labudde, Germany
Sebastian Link, New Zealand
Huiqing Liu, USA
Jingchu Luo, China
Victor Maojo, Spain
Sudha Ram, USA
Keun Ho Ryu, Korea
Amandeep S. Sidhu, Australia
Tanya Soboleva, New Zealand
Thodoros Topaloglou, Canada
Haixun Wang, USA
Jing Wang, New Zealand
Xiaofang Zhou, Australia
Esteban Zimányi, Belgium

External Referees

Claudia Täubner, Germany
Henning Köhler, New Zealand

FP-UML 2007 – International Workshop on Foundations and Practices of UML

FP-UML 2007 was organized within the framework of the following projects: META-SIGN (TIN2004-00779) from the Spanish Ministry of Education and Science and DADS (PBC-05-012-2) from the Castilla-La Mancha Ministry of Science and Technology (Spain).

Workshop Co-chairs

Juan Trujillo, University of Alicante, Spain
Jeffrey Parsons, Memorial University of Newfoundland, Canada

Program Committee

Doo-Hwan Bae, South Korea
Michael Blaha, USA
Cristina Cachero, Spain
Tharam Dillon, Australia
Gillian Dobbie, New Zealand
Brian Dobing, Canada
Dirk Draheim, Germany
Joerg Evermann, New Zealand
Eduardo Fernández, Spain
Jens Lechtenbörger, Germany
Tok Wang Ling, Singapore
Pericles Loucopoulos, UK
Hui Ma, New Zealand
Andreas L. Opdahl, Norway
Oscar Pastor, Spain
Witold Pedrycz, Canada
Mario Piattini, Spain
Ivan Porres, Finland
Colette Rolland, France
Matti Rossi, Finland
Manuel Serrano, Spain
Keng Siau, USA
Il-Yeol Song, USA
Ambrosio Toval, Spain
Antonio Vallecillo, Spain
Panos Vassiliadis, Greece

External Referees

M. Kirchberg
A. Tretiakov
O. Thonggoom
G. Abraham

ONISW 2007 – International Workshop on Ontologies and Information Systems for the Semantic Web

Workshop Co-chairs

Mathias Brochhausen, Saarland University, Germany
Martin Doerr, Foundation for Research and Technology - Hellas, Greece
Hyoil Han, Drexel University, USA

Program Committee

Yuan An, Canada
Sofia J. Athenikos, USA
Boualem Benatallah, Australia
Mathias Brochhausen, Germany
Namyeon Choi, USA
Crisitan Cocos, Germany
Martin Doerr, Greece
Ramez Elmasri, USA
Fabien Gandon, France
Raul Garcia-Castro, Spain
Hyoil Han, USA
Mary Elizabeth Jones, USA
Aneesh Krishna, Australia
Werner Kuhn, Germany
Sang-Koo Lee, Korea
SeungJin Lim, USA
Dimitris Plexousakis, Greece
Barry Smith, USA and Germany
Krishnaprasad Thirunarayan, USA

QoIS 2007 – International Workshop on Quality of Information Systems

Workshop Co-chairs

Samira Si-Saïd Cherfi, CEDRIC-CNAM, France
Geert Poels, Ghent University, Belgium

Steering Committee

Jacky Akoka, CEDRIC-CNAM & INT, France
Mokrane Bouzeghoub, PRISM, University of Versailles, France
Isabelle Comyn-Wattiau, Conservatoire National des Arts et Métiers and ESSEC, France
Marcela Genero, Universidad de Castilla-La Mancha, Spain
Jeffrey Parsons, Memorial University of Newfoundland, Canada
Geert Poels, Ghent University, Belgium
Keng Siau, University of Nebraska, USA
Bernhard Thalheim, University of Kiel, Germany

Program Committee

Jacky Akoka, France
Laure Berti-Equille, France
Andrew Burton-Jones, Canada
Tiziana Catarci, Italy
Corinne Cauvet, France
Isabelle Comyn-Wattiau, France
Marcela Genero, Spain
Paul Johannesson, Sweden
Jacques Le Maître, France
Jim Nelson, USA
Jeffrey Parsons, Canada
Oscar Pastor, Spain
Houari Sahraoui, Canada
Farida Semmak, France
Keng Siau, USA
Guttorm Sindre, Norway
Samira Si-Saïd Cherfi, France
Monique Snoeck, Belgium
Il-Yeol Song, USA
David Tegarden, USA
Bernhard Thalheim, Germany
Dimitri Theodoratos, USA
Juan Trujillo, Spain

External Referees

Ki Jung Lee, USA

RIGiM 2007 – International Workshop on Requirements, Intentions and Goals in Conceptual Modeling

Workshop Co-Chairs

Colette Rolland, Université Paris1 Panthéon Sorbonne, France
Eric Yu, University of Toronto, Canada

Program Committee

Daniel Amyot, Canada
Mikio Aoyoma, Japan
Ian Alexander, UK
Aybuke Arum, Australia
Franck Barbier, France
Daniel Berry, Canada
Sjaak Brinkkemper, The Netherlands
Lawrence Chung, USA
Luiz Cysneiros, Canada
Eric Dubois, Luxembourg
Vincenzo Gervasi, Italy
Aditya K. Ghose, Australia
Peter Haumer, USA
Zhi Jin, China
Aneesh Krishna, Australia
John Krogstie, Norway
Lin Liu, China
Peri Loucopoulos, UK
John Mylopoulos, Canada
Selmin Nurcan, France
Bashar Nuseibeh, UK
Andreas Opdahl, Norway
Barbara Pernici, Italy
Klaus Pohl, Germany
Jolita Ralyte, Switzerland
Bjorn Regnell, Sweden
Camille Salinesi, France
Motoshi Saeki, Japan
Pnina Soffer, Israel
Carine Souveyet, France
Leon Sterling, Australia
Yair Wand, Canada
Roel Wieringa, The Netherlands

External Referees

Arosha Bandara, UK
Chiara Francalanci, Italy
Joy Garfield, UK
Kim Lauenroth, Germany
Thorsten Weyer, Germany

SeCoGIS 2007 – International Workshop on Semantic and Conceptual Issues in Geographic Information Systems

Workshop Co-chairs

Esteban Zimányi, Université Libre de Bruxelles, Belgium
Michela Bertolotto, University College Dublin, Ireland

Program Committee

Gennady Andrienko, Germany
Natalia Andrienko, Germany
Yvan Bédard, Canada
David Bennett, USA
Alex Borgida, USA
Patrice Boursier, France
Bénédicte Bucher, France
James Carswell, Ireland
Christophe Claramunt, France
Eliseo Clementini, Italy
Maria Luisa Damiani, Italy
Clodoveu Davis, Brazil
Max Egenhofer, USA
Fernando Ferri, Italy
Andrew Frank, Austria
Anders Friis-Christensen, Italy
Antony Galton, UK
Bo Huang, Canada
Marinos Kavouras, Greece
Werner Kuhn, Germany
Sergei Levashkin, Mexico
Ki-Joune Li, South Korea
Thérèse Libourel, France
Jose Macedo, Switzerland
Peter van Oosterom, The Netherlands
Dimitris Papadias, China
Fabio Porto, Switzerland
Dieter Pfoser, Greece
Ricardo Rodrigues Ciferri, Brazil
Andrea Rodriguez, Chile
Sylvie Servigne-Martin, France
Stefano Spaccapietra, Switzerland
Emmanuel Stefanakis, Greece
Kerry Taylor, Australia
Christelle Vangenot, Switzerland
Antonio Miguel Vieira Monteiro, Brazil
Agnès Voisard, Germany

Table of Contents

FP-UML 2007 – International Workshop on Foundations and Practices of UML

Improving the Use of UML Diagrams

Model Transformations and Extensions

ONISW 2007 – International Workshop on Ontologies and Information Systems for the Semantic Web

QoIS 2007 – International Workshop on Quality of Information Systems

RIGiM 2007 – International Workshop on Requirements, Intentions and Goals in Conceptual Modelling

Keynote

Requirements and Goals – Methods

Requirements and Goals – Concepts

SeCoGIS 2007 – International Workshop on Semantic and Conceptual Issues in Geographic Information Systems

Moving Objects

Advances in Conceptual Modelling for GIS

Integrity Constraints and Approximate Reasoning

M-BPSec: A Method for Security Requirement Elicitation from a UML 2.0 Business Process Specification

Alfonso Rodríguez[1], Eduardo Fernández-Medina[2], and Mario Piattini[2]

[1] Departamento de Auditoría e Informática, Universidad del Bio Bio, Chillán, Chile
alfonso@ubiobio.cl
[2] ALARCOS Research Group, Information Systems and Technologies Department UCLM-Indra Research and Development Institute University of Castilla-La Mancha Ciudad Real, Spain
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es

Abstract. The early attainment of requirements in a software development process allows us to improve the quality of the product. Although many methods through which to elicit requirements exist, few of them are specifically designed for security requirements. This paper describes a method - M-BPSec - which permits the elicitation of security requirements which form part of a business process description carried out with a UML 2.0 Activity Diagram. M-BPSec is made up of stages, actors, tools and artifacts which, when applied in a coordinated manner, allow us to specify security requirements in business processes and to obtain class and use cases from this specification.

1 Introduction

The elicitation of requirements is perhaps the activity which is most often regarded as the first step in the requirement engineering process [8]. Since many elicitation techniques are available to the requirements engineer, some guidance on their use is needed. *Methods* provide one way of delivering such guidance. Each method itself has its strengths and weaknesses, and is normally best suited for use in particular application domains [8]. Elicitation methods related to security requirement are scarce. One reason for this is that few elicitation methods are specifically directed towards security requirements. Another reason is that organizations seldom specifically address the elicitation of security requirements and instead lump them in with other traditional requirement elicitation methods [6].

Furthermore, business processes (BP), which are defined as a set of procedures or activities which collectively pursue a business objective or policy goal [15], are not only an important resource in enterprise performance and in maintaining competitiveness, but are also an important requirement source.

Moreover, the business scene, in which there are many participants and an intensive use of communications and information technologies, implies that

J.-L. Hainaut et al. (Eds.): ER Workshops 2007, LNCS 4802, pp. 106–115, 2007.

enterprises not only expand their businesses but also increase their vulnerability. Despite the fact that the importance of business processes security is widely accepted, the business analyst perspective in relation to security has hardly been dealt with until now. At the present it is possible to capture high level security requirements which are easily identifiable by those who model business processes, because: (i) the business process representation has improved in the UML 2.0 version, (ii) the security requirement will tend to have the same basic kinds of valuable and potentially vulnerable assets [3], and (iii) empirical studies show that customers and end users are able to express their security needs [5]. Consequently, in [12], we have extended the UML 2.0 Activity Diagram (UML 2.0-AD) [10] by creating the BPSec-Profile. This profile allows us to capture security requirements and create a Secure Business Process (SBP) specification.

In this paper, we demonstrate a method of security requirement elicitation which uses SBP specification as a starting point. Our method considers stages, workers, tools, models and artifacts which, if grouped together, permit (i) the design of an SBP (ii) the attainment of analysis-level classes and use cases which include security aspects and (iii) the storage of information related to the specification of the business process.

The structure of the remainder of the paper is as follows: in Section 2, we will present our proposal in brief and related works, in Section 3 we will present M-BPSec. Finally, in Section 4 our conclusions will be drawn.

2 Our Proposal and Related Work

Our proposal is a method by which to elicit security requirements which are captured through the application of an extension of a UML 2.0-AD. By using BPSec-Profile, it is possible to represent the business analyst's perspective with regard to security. In this way, a new point of view with a high level of abstraction is obtained, and this complements existing perspectives concerning security.

Given that M-BPSec includes models (at different levels of abstraction) and artifacts (pieces of information that are produced, modified, or used in a method [11]), the Model-Driven Architecture (MDA) [9] approach for the models and the Unified Process (UP) [4] for the use of the artifacts have been used as a reference framework. MDA is composed of the following perspectives: (i) the computation independent viewpoint which focuses on the environment of the system, (ii) the platform independent viewpoint which focuses on the operation of a system whilst concealing the details necessary for a particular platform, and (iii) the platform specific viewpoint which combines the platform independent viewpoint with an additional focus on the details of the use of a specific platform by a system. We have also used the UP, which is composed of a set of activities which are necessary for the transformation of user requirements into a software system.

The basic aspects of our proposal are shown in Figure 1. The first column (on the left) shows three types of models which conform to the MDA. The last column shows the UP disciplines. The central part shows our proposal and the artifacts which are derived from the M-BPSec application. The SBP specification is created by using the UML 2.0-AD and the BPSec-Profile [12]. The Analysis-level Classes and Use cases are obtained by a transformation which takes the SBP model as its starting point and

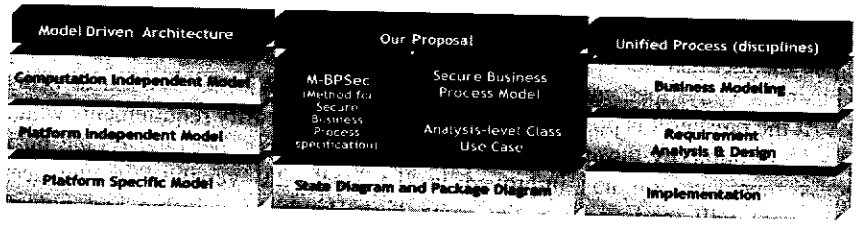

Fig. 1. Overview of our proposal

uses QVT rules, refinement rules and checklists. If Figure 1 is observed horizontally it will be noted that there is a correspondence between the elements presented in our proposal and the MDA models and UP disciplines. Thus, an SBP description corresponds with a Computation Independent Model (CIM). Said model can be used as a complement in the "Business Modeling" discipline of the UP. The Use Cases, which form a part of a Platform Independent Model (PIM), will complement the "Requirement" and "Analysis & Design" disciplines.

In related work dealing with security requirement elicitation methods we found in [6] a comparative analysis of nine elicitation methods. The author has used the following comparison criteria: adaptability, a computer-aided software engineering (CASE) tool, stakeholder acceptance, easy implementation, graphical output, quick implementation, a shallow learning curve, high maturity and scalability. In [7] the authors analyzed seven proposals orientated towards establishing security requirements in the development of an information system scope. The comparative criteria are: degree of agility, help support, degree of integration with other software requirements, user friendliness and contributions of the proposal as regards security. And finally, a comparative evaluation of three approaches: common criteria, misuse cases and attack trees which take into account learnability, usability, solution inclusiveness, clarity of output and analyzability criteria is carried out by [2].

However, none of the proposals for the acquisition of security requirements which we have reviewed consider the acquisition of these requirements by using a business process described with UML 2.0-AD as a starting point. Our proposal considers this situation, and also the possibility of automatically obtaining other UML artifacts which contain security requirements and which complement the traditional stages in a software creation process.

3 M-BPSec: A Security Requirement Elicitation Method

In this section we show our proposal, a security requirements elicitation method (see Figure 2). In Section 3.1 we shall describe the workers who participate in M-BPSec, the tools and models which are used and the artifacts which are generated. The *Construction*, *Security requirement incorporation*, *Refining* and *Transformations* stages are described in Sections 3.2, 3.3, 3.4, and 3.5 respectively. Besides having defined each stage of the M-BPSec, we have also used an example which allows us to relate the *workers*, *tools*, *models*, and *artifacts* which form a part of each stage.

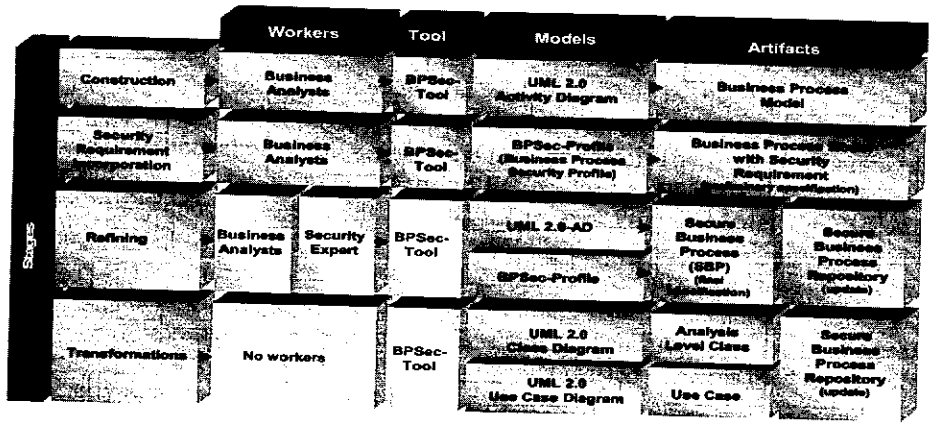

Fig. 2. M-BPSec: A method for security requirement elicitation

3.1 Workers, Tool, Models and Artifacts

Two types of workers are involved in M-BPSec: business analysts and security experts. The *business analyst* is responsible for the specifications related to the business itself as well as for incorporating (from his/her point of view) security requirements into the specifications by considering a high level of abstraction. The *security expert*: is the person responsible for refining the security specifications indicated by the business analyst. Such refinement considers the verification of the validity and the completeness of the specifications.

The Tool is the *BPSec-Tool*, which is used to design the SBP, to automatically transform models and to update the data contained in the secure business process repository. The BPSec-Tool was built by using a 3-tiered architecture to separate the presentation, application, and storage components, using MS-Visio, C#, and MS-Access technology respectively.

The Models employed are: (i) *UML 2.0-AD*, used for business process specification; (ii) *BPSec-Profile* used for security requirement specification; (iii) a *Class Diagram* and a *Use Case Diagram*, which both contain the specifications which will be automatically obtained from the SBP specification.

The artifacts are: (i) a *Business Process Model* described with UML 2.0-AD in which the business process is modelled without security requirements; (ii) a *Business Process Model with Security Requirement* and a *Secure Business Process*, both of which are described with UML 2.0-AD and BPSec-Profile. The first of these corresponds with a preliminary specification and the second corresponds with the final specification; (iii) *Secure Business Process Repository* (see Figure 3) in which the SBP, analysis-level class and use case are stored, and (iv) *Analysis-Level Class* and *Use Case*, both of which are automatically created and contain security specifications.

The repository contains information about the secure business process specification. Information concerning the activity diagram, security requirements specification, analysis-level classes and use cases are stored here. The repository is

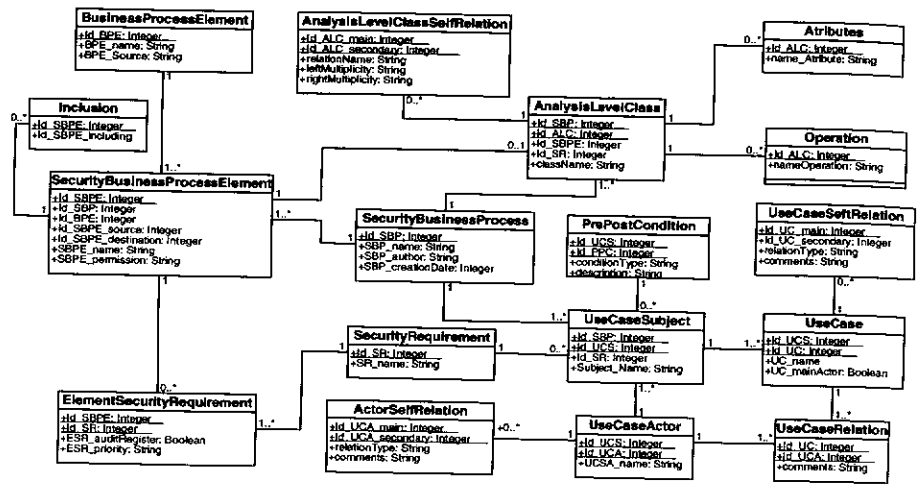

Fig. 3. Secure Business Process Repository

automatically created from the SBP specification. It is completed with the information from the analysis-level classes and the use cases which are obtained automatically. The repository can additionally be used to obtain historical information in order to make the business process specifications secure.

In the following sections we shall explain each stage in the M-BPSec. The stages will be described through the worker, tool, model and output artifacts that are used in each stage. We shall additionally use the example of a business process which is related to the admission of patients to a medical institution (see Figure 4).

3.2 *Construction* Stage

In this stage the objective is to build the business process model. To attain this objective, the UML 2.0-AD must be used. The *Construction* stage is carried out by the business analyst, who sets the time and place of the work activities, ensures that they have a beginning and an end, and who clearly explains the business view point. The BPSec-Tool is used to make a business process design with UML 2.0-AD. The final result of this stage is a Business Process Model.

In our example the business process is initiated with an admission request which is filled in by the *Patient*. This document, called an *Admission Request*, is sent to the *Administration Area*. In this area, information related to insurance is captured, and the existence of the patient's medical file is verified.

Once the patient's documentation has been validated and completed, it is sent to the *Medical Area*. The *Medical Evaluation* area uses a set of pre-admission tests to determine the patient's medical condition. If necessary, additional examinations are carried out, and these must be registered from both the clinical and the economic point of view. Finally, the *Medical Evaluation* document is filled in with information about the patient, and this is then sent to him/her. The business process is completed when the patient receives his/her *Medical Evaluation*.

3.3 Security Requirement Incorporation Stage

In this stage the security requirements can be added to the business process description from the business analyst's viewpoint. The business analyst must able to identify the potential threats in the business process model. The security requirements must subsequently be incorporated, using BPSec-Profile (supported by the BPSec-Tool). The output artifact in this stage is a Business Process Model with Security Requirement.

In [12] we have proposed the following types of security requirements: Access Control, Attack Harm Detection, Security Auditing, Non Repudiation, Integrity and Privacy. In our proposal we have used a padlock, standard *de facto*, to represent security. The same symbol, the padlock, but with a twisted corner is used to represent a Security Requirement with Audit Register.

In the "Admission of Patients" business process specification, the business analyst has specified «Privacy» (anonymity) for the *Patient* ActivityPartition, with the aim of preventing the disclosure and storage of sensitive information about Patients. «Nonrepudiation» has been defined for the control flow that goes from the *Fill Admission Request* action to the *Capture Insurance Information* and *Check Clinical Data* actions with the aim of avoiding the denial of the *Admission Request* reception. «AccessControl» and «Privacy» (confidentiality) have been defined for the Interruptible Activity Region. A «SecurityRole» can be derived from this specification. *Admission/Accounting* will be another role. All objects in an interruptible region must be considered for permission specification. The Access Control specification has been complemented with an audit requirement. This implies that it must register information about the security role and security permissions. An «Integrity» (high) requirement has been specified for the *Clinical Information* DataStore and finally, the business analyst has specified «AttackHarmDetection» for the *Medical Evaluation* DataStore, so that, all events related to the attempt or success of attacks or damages are registered. The graphic specification of the business process which has been carried out by using the BPSec-Tool, is shown in Figure 4.

Additionally, the priority attribute, according to that established in [1], and the permission for the actions, data store and object flows in access control scope, must be specified.

3.4 *Refining* Stage

In the *Refining* stage the security requirement specified in the business process description must be reviewed and complemented. The workers, the business analyst and the security expert, work together and the specifications that will finally be incorporated into the business process are agreed. The BPSec-Tool must be used to achieve a Secure Business Process (final specification). The repository which contains information about the secure business process specification is also automatically generated.

The priority specification of each security requirement and security permissions associated with the access control specification are also refined in this stage. The *must be* priority was assigned to Privacy (anonymity) and AuditRegister, and to

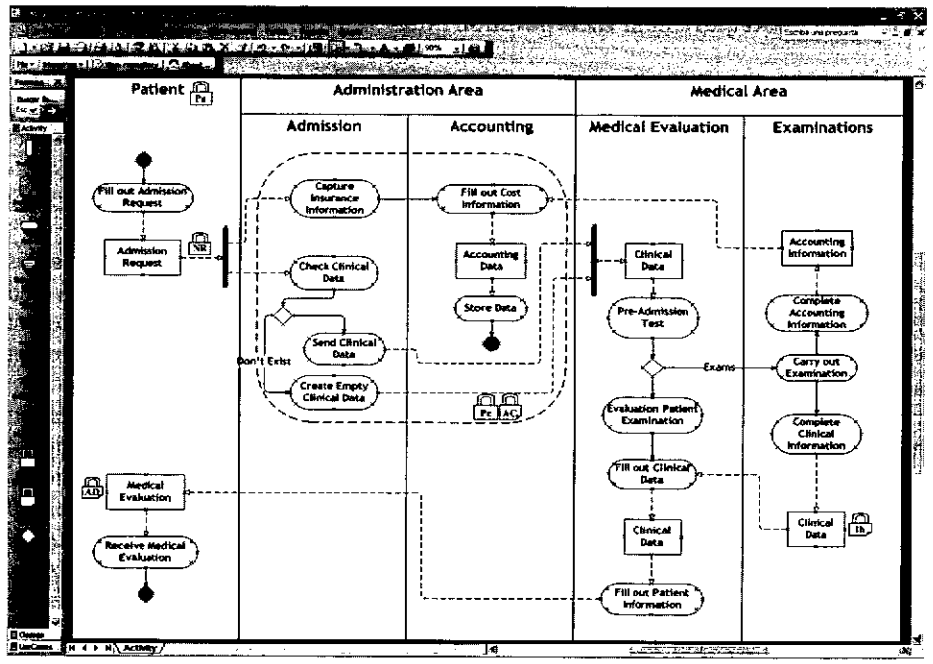

Fig. 4. Admission of Patients to a Medical Institution with security requirement

Nonrepudiation, *should have* was assigned to Access Control, and to Privacy (confidentiality), and *could have* was assigned to Integrity (high).

The *execution* permission was assigned to *Capture Insurance Information*, *Check Clinical Data*, *Store Data*, and *Create Empty Clinical Data*. The *CheckExecution* permission was assigned to *Fill out Cost information*. And the *Update* permission was assigned to *Accounting Data*.

3.5 Transformation Stage

Finally, in the *Transformation* stage, the analysis-level classes and use cases are obtained and are stored in the repository. This stage does not require workers because the artifacts and the repository are generated automatically.

Transformations to analysis-level classes, from CIM to PIM (C2P), require a set of rules which have been specified in QVT language and also a set of refinement rules [13]. For transformations to use cases (C2P) it is necessary to specify a set of QVT rules, refinement rules and a checklist [14].

The result of the application of the QVT rules and the refinement rules in relation to the attainment of analysis-level classes can be seen in Figure 5.

The use case model derived from the business process specifications for the admission of patients (see Figure 6 on the left-hand) and the use case model derived from the Access Control and Privacy specification security requirements (see Figure 6 on the righ-hand) are graphically shown.

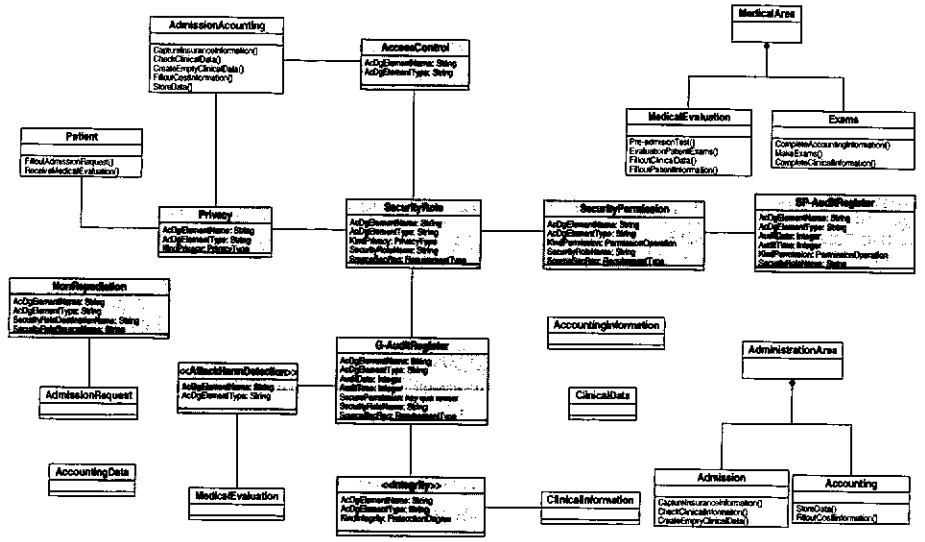

Fig. 5. Analysis-Level Class from Patient Admission

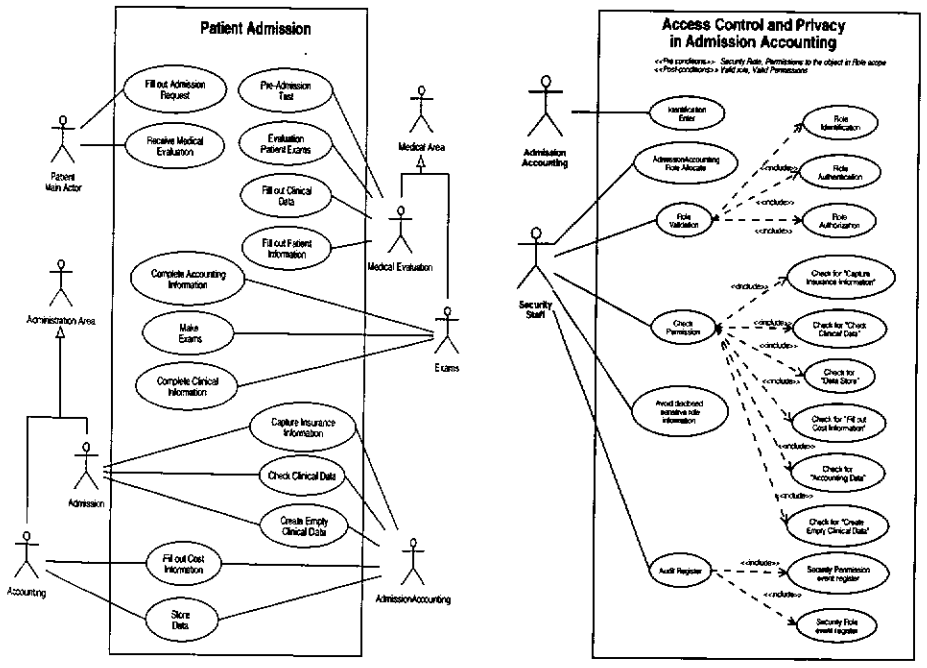

Fig. 6. Patient Admission and Access Control/Privacy use case specification

4 Conclusions

A business process specified with a UML 2.0 Activity Diagram containing security requirement allows the incorporation of a new perspective with regard to the security in a software creation process. However, this specification alone is not sufficient. The attainment of security requirements at this level of abstraction should be framed within a method which allows us to ensure both the acquisition and the adequate use of the resulting artifacts.

Owing to the fact that the elicitation of requirements is perhaps the most important activity in requirement engineering, in this paper we have defined a method for security requirement elicitation from a UML 2.0 Business Process specification. M-BPSec is a regular and systematic method by which to accomplish (i) security requirement specification in a business process described with UML 2.0-AD, and (ii) the attainment of the UML artifact, analysis-level classes and use cases, through which it is possible to achieve most concrete models which include security.

In M-BPSec the stages, workers, tool-models and artifacts are clearly defined and, when grouped together, allow us to elicit security requirements by using a secure business process as a starting point. We believe that M-BPSec satisfactorily fulfills the evaluation criteria of elicitation methods for requirements such as: the computer-aided software tool, easy implementation, graphical output, quick implementation, and the shallow learning curve.

The next steps in our research are orientated towards applying M-BPSec to a real case orientated towards enriching the method and the artifacts. We shall also improve the BPSEc-Tool in order to allow us to include other notations for the specification of SBP.

Acknowledgements. This research is part of the following projects: DIMENSIONS (PBC-05-012-1), and MISTICO (PBC06-0082) both partiality supported by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", Spain, COMPETISOFT (506AC087), granted by CYTED and ESFINGE (TIN2006-15175-C05-05/) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología", Spain.

References

1. Arlow, J., Neustadt, I.: UML 2 and the Unified Process: Practical Object-Oriented Analysis and Design, 2nd edn., p. 592. Addison-Wesley, Reading (2005)
2. Diallo, M.H., Romero-Mariona, J., Sim, S.E., Alspaugh, T.A., Richardson, D.J.: A Comparative Evaluation of Three Approaches to Specifying Security Requirements. In: REFSQ. 12th International Working Conference on Requirements Engineering: Foundation for Software Quality, Luxembourg (2006)
3. Firesmith, D.: Specifying Reusable Security Requirements. Journal of Object Technology 3(1), 61–75 (2004)
4. Jacobson, I., Booch, G., Rumbaugh, J.: The Unified Software Development Process, p. 463 (1999)
5. Lopez, J., Montenegro, J.A., Vivas, J.L., Okamoto, E., Dawson, E.: Specification and design of advanced authentication and authorization services. Computer Standards & Interfaces 27(5), 467–478 (2005)

6. Mead, N.R.: Experiences in Eliciting Security Requirements, CrossTalk. The Journal of Defense Software Engineering 19(12) (2006)
7. Mellado, D., Fernández-Medina, E., Piattini, M.: A Comparative Study of Proposals for Establishing Security Requirements for the Development of Secure Information Systems. In: Computational Science and Its Applications (ICCSA), Glasgow, UK, pp. 1044–1053 (2006)
8. Nuseibeh, B., Easterbrook, S.M.: Requirements Engineering: A Roadmap. In: ICSE 2000. 22nd International Conference on on Software Engineering, Future of Software Engineering Track, Limerick Ireland, pp. 35–46. ACM Press, New York (2000)
9. Object Management Group; MDA Guide Version 1.0.1(2003), http://www.omg.org/docs/omg/ 03-06-01.pdf
10. Object Management Group; Unified Modeling Language: Superstructure Version 2.1.1 (formal/2007-02-05) (2007), http://www.omg.org/docs/formal/07-02-05.pdf
11. Rational Software, Rational Unified Process, Best Practices for Software Development Teams, p.21 (2001)
12. Rodríguez, A., Fernández-Medina, E., Piattini, M.: Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes. In: Fischer-Hübner, S., Furnell, S., Lambrinoudakis, C. (eds.) TrustBus 2006. LNCS, vol. 4083, pp. 51–61. Springer, Heidelberg (2006)
13. Rodríguez, A., Fernández-Medina, E., Piattini, M.: Analysis-Level Classes from Secure Business Processes through Models Transformations. In: Lambrinoudakis, C., Pernul, G., Tjoa, A.M. (eds.) TrustBus 2007. LNCS, vol. 4657, pp. 104–114. Springer, Heidelberg (2007)
14. Rodríguez, A., de Guzmán, I.G.-R.: Obtaining Use Cases and Security Use Cases from Secure Business Process through the MDA Approach. In: Workshop on Security in Information Systems (WOSIS), Funchal, Madeira - Portugal (2007)
15. WfMC, Workflow Management Coalition: Terminology & Glossary, p.65 (1999)