CAiSE'07
Trondheim, Norway

The 19th International Conference on
Advanced Information Systems Engineering

11–15 June 2007, Trondheim, Norway

Theme: Ubiquitous Information Systems Engineering

Editors: Barbara Pernici and Jon Atle Gulla

Proceedings of Workshops and Doctoral Consortium

Vol. 1
EMMSAD, BPMDS, BUSITAL

Barbara Pernici
Jon Atle Gulla (Eds.)

CAiSE'07

19th International Conference on Advanced Information Systems Engineering

Trondheim, 11—15 June, 2007

Proceedings of the Workshops and Doctoral Consortium

AOIS'07
BPMDS'07
BUSITAL'07
EMMSAD'07
UMICS'07
WISM'07
Doctoral Consortium

Preface

These proceedings include the papers from six workshops and the doctoral consortium held in conjunction with the 19th International Conference on Advanced Information Systems Engineering (CAiSE'07) in Trondheim.

The workshops at CAiSE'07 form an important complement to the conference and provide a forum for researchers and practitioners to exchange ideas and share results in an atmosphere that fosters interaction and problem solving. They have a tighter focus than the main conference and also tend to address emerging trends and technologies.

The workshops were selected based on quality, relevance, and reputation. Many of them have had a long history with CAiSE, on topics related to modelling and to designing innovative systems within organizations.

The two-day workshops in these proceedings are:

- BPMDS'07 – Eight International Workshop on Business Process Modeling, Development, and Support
- EMMSAD'07 – Twelfth International Workshop on Exploring Modelling Methods in Systems Analysis and Design
- UMICS'07 – Fifth International Workshop on Ubiquitous Mobile Information and Collaboration Systems

There are also three one-day workshops:

- BUSITAL'07 – Second International Workshop on Business/IT Alignment and Interoperability
- AOIS'07 – Seventeenth International Workshop on Agent-Oriented Information Systems
- WISM'07 – Fourth International Workshop on Web Information Systems Modeling

The proceedings also includes the papers from the CAiSE Doctoral Consortium.

We are grateful to the workshop organizers who took responsibility as program chairs for their workshops and managed the process from issuing call for papers to preparing their respective parts of the workshop proceedings. We would also like to thank all members of the various program committees and all other referees that devoted their time to review papers and help us put together a very exciting workshop program at CAiSE'07.

Enjoy the workshops and doctoral consortium in Trondheim!

May 2007   Barbara Pernici
                                                                   Jon Atle Gulla

Gold Sponsors

Insitutional Sponsor

Local Sponsors:

Additional Collaborators

Table of Contents

Selmin Nurcan
Gil Regev
Rainer Schmidt
Pnina Soffer

BPMDS'07

8TH International Workshop on Business Process Modeling, Development, and Support

Workshop at

CAiSE'07

The 19th International Conference on
Advanced Information Systems Engineering
Trondheim, 11-15 June, 2007

Selmin Nurcan, Gil Regev, Rainer Schmidt and Pnina Soffer (Eds.)

Organization

BPMDS'07 Workshop Organizers

Selmin Nurcan - University Paris 1 Panthéon Sorbonne, France
Gil Regev – Ecole Polytechnique Fédérale, Lausanne, Switzerland
Rainer Schmidt - University of Applied Sciences, Aalen, Germany
Pnina Soffer – University of Haifa, Israel

BPMDS'07 Program Committee

Wil van der Aalst - Eindhoven University of Technology, The Netherlands
Ian Alexander – Scenario Plus, UK
Ilia Bider– IbisSoft, Stockholm, Sweden
Signe Ellegaard Borch - IT University of Copenhagen, Denmark
Stewart Green - University of the West of England, UK
Elke Hochmüller - Carinthia Tech Institute, Austria
Paul Johannesson - Royal University of Technology, Stockholm, Sweden
Marite Kirikova - Riga Technical University, Latvia
Nikolaus Kleiner, DaimlerChrysler Research, Berlin, Germany
Agnes Koschmider, University of Karlsruhe, Germany
Peri Loucopoulos - University of Manchester, UK
Jan Mendling - Vienna University, Austria
Murali Mohan Narasipuram, City University of Hong Kong
Selmin Nurcan - University Paris 1 Pantheon Sorbonne, France
L.F. Pau - Erasmus University, Netherlands
Jan Recker - Queensland University of Technology, Brisbane, Australia
Gil Regev – Ecole Polytechnique Fédérale, Lausanne, Switzerland
Manfred Reichert - University of Twente, Enschede, The Netherlands
Peter Rittgen - University College of Borås, Sweden
Michael Rosemann - Queensland University of Technology, Brisbane, Australia
Rainer Schmidt - University of Applied Sciences, Aalen, Germany
Pnina Soffer – University of Haifa, Israel
Markus Strohmaier – University of Toronto, Canada
Lars Taxén - Linköping University, Sweden
Jelena Zdravkovic - Royal University of Technology, Stockholm, Sweden
Michael zur Muehlen - Stevens Institute of Technology, USA

BPMDS'07 Industrial Advisory Board

Ian Alexander – Scenario Plus, UK
Ilia Bider– IbisSoft, Stockholm, Sweden
Lars Taxén - Linköping University, Sweden

Preface

The coordinated design of business processes and their support systems became a strategic issue for all enterprises, which identified information as an essential resource for creating value. BPMDS'04 was devoted to this subject. During the last two workshops (BPMDS'05, BPMDS'06), we focused on the issue of flexibility in business processes and their support systems. In this workshop we will discuss the broader issue of what it means to design an adequate process and its support systems. Adequacy can be measured with respect to the goals of the stakeholders of the business process. Typical goals that are named in connection with business process (support) design are productivity, quality, efficiency, flexibility and conformance with formal and legal rules such as ISO 20000 or SOX. Are they the only ones? Typical means that are named in this context are "best practices", reuse and theoretical approaches. Are they the right means for achieving these goals?

The main issues that are addressed in the workshop are:
A. What does adequate design mean?
B. How to determine whether a design is adequate or not?
C. What means can be employed to achieve adequate design?

In particular, we want to examine typical concepts used in relation with process design, such as, reuse, theoretical approaches and even buzz-words for instance, "best practices". Reusability is often considered as a highly desired property of the designed processes and their support systems. "Best practices" are often used by practitioners to promote design techniques that are supposed to have been proven in practice, but it is not clear why they are "the best" as their name may suggest, and whether they can be transferred from one organization to another. The need to have the "right" theoretical approach represents the other extreme promoted by researchers who advance theoretical frameworks for design. These often suffer from being impractical and unscaleable.

The 24 papers accepted to BPMDS'07 out of 37 papers submitted cover various areas of adequate business process design. They are organized under the following section headings.

Opening

Process and enterprise architectures: The papers of this session explore the relationship between adequacy and process and enterprise architectures.

Design adequacy: In this group of papers, the influence of the design of business processes on adequacy is investigated.

Process and context modeling: In this session the theoretical foundations for the modeling of adequate business processes are given.

Selmin Nurcan, Gil Regev, Rainer Schmidt and Pnina Soffer (Eds.)

Collaboration, Coordination and Processes: This session contains papers which investigate means for achieving the adequacy of processes containing collaborative and coordinative elements.

Requirements and processes: The fulfillment of requirements is essential of the adequacy of processes. Therefore, the papers of this session investigate means for the fulfillment of requirements.

Reuse and Generic models: Reuse of process models and their parts which have already proven their appropriateness in such or such situation is an important means for reducing the effort to achieve adequacy. The papers in this group present approaches to achieve such a reuse.

Adequacy evaluation: The various means for achieving adequacy also need methods to evaluate the adequacy achieved. Different approaches are presented in this session.

 "Best practices": Adequacy and "best practices" show a complicate relationship. On one hand, best practices facilitate adequacy. On the other hand, best practices obstruct the achievement of adequacy. The papers of this session reflect on this strained connection.

Finally, we wish to thank all the people who submitted papers to the workshop for having shared their work with us, as well as the members of the BPMDS'07 program committee and the workshop organizers of CAiSE'07 for their help with the organization of the workshop.

Table of Contents

"Best practices"

Using QVT to obtain Use Cases from Secure Business Processes modeled with BPMN

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,
University of Castilla-La Mancha
Ciudad Real, Spain.
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es

Abstract. Nowadays, enterprises are aware of the importance that business processes and security have in relation to their competitive position and performance. In previous works, we have proposed a BPMN extension which allows us to capture security requirements from the business analyst's perspective. In this paper, we will show a set of rules described with QVT, refinement rules and checklists which permits us to obtain UML use cases from a business process specification that considers security requirements.

1 Introduction

In a highly competitive environment where enterprises must adapt themselves in order to maintain their position, business processes (BP) have become crucial. This is due to the fact that they allow us to describe, standardize, and adapt the way in which they react to certain types of business events. At the same time, due to the intensive use of communication and information technologies, security has been transformed into a highly important aspect in the majority of the common areas of an enterprise.

In previous works [7] we have proposed an extension orientated towards capturing security requirement (SR) in a business process description. We believe that considering security from the business analyst's perspective will be useful in confronting this new scenario. Also, these specifications are a good starting point for software construction.

Model transformation is focused on solving the problems of time, cost and quality associated with software creation. The Object Management Group (OMG) proposal to solve this problem is composed of: Model Driven Architecture (MDA); a framework for software development, and Query/View/Transformations (QVT); a standard for model transformation.

In our proposal we transform a computation independent model (CIM) into a platform independent model (PIM). We start from a business process with security requirement description, CIM-level, and obtain use cases and security use cases at PIM-level. Both models can be used in a software development process.

2 Security in Business Processes

In spite of the importance of security in business processes, its modeling has not been adequate since, generally, those who specify SR are requirements engineers who have accidentally tended to use architecture specific restrictions instead of security requirements. Moreover, security has been integrated into applications in an ad-hoc manner, often during the actual implementation process or during the system administration phase.

However, at present it is possible for those who model BP to capture easily identifiable SR at a high level because: (i) BP representation has improved in the Business Process Modeling Notation-Business Process Diagram (BPMN-BPD), (ii) the SR will tend to have the same basic kinds of valuable and potentially vulnerable assets, and (iii) empirical studies show that it is common at the BP level for customers and end users to be able to express their security needs. Therefore, we have approached the problem of including security in BP by extending BPMN-BPD. The proposed extension, called BPSec, basically considers the graphical representation of SR taken from the taxonomy proposed in [4]. We consider the following SR; Attack Harm Detection, Access Control, Audit Register, Integrity, Privacy and Non Repudiation. We have used a padlock, *de facto* standard, to graphically represent SR.

3 Use Case and Security Use Case from Secure Business Process

In our proposal we use BPMN-BPD and BPSec to describe a Secure Business Process (SBP). We have applied a set of transformation rules, refinement rules and checklists to obtain a subset of use cases and security use cases that facilitate the understanding of the problem. SBP is used in "Business Modeling" and use cases are used in the "Requirement" and "Analysis & Design" disciplines of the Unified Process (UP).

In the works related to security and use cases (or misuse case) [1, 3, 5, 9], these are used to capture SR but unlike of our proposal, they are not directly obtained from BPMN-BPD security specifications. In the works related to the attainment of use cases from BP specifications, we have found that in [8], the possibility of obtaining use cases from a BP specification made with BPMN is suggested, and in [6], the automatic obtention of UML artifacts from a BP description made by using BPMN is proposed. The authors extend BPMN (Extension Level-1) to add information about the sequence and the input and output flows. This allows them to apply rules from which use cases, state diagrams, sequence and collaboration are achieved. In [10], a transformation performed from a BP described with UML 2.0 activity diagrams to use cases is stated and finally, in [2], use cases are obtained from BP models which are not represented by activity diagrams.

In our proposal we consider that: (i) previous manual intervention is not required, ii) transformations are described by using special languages (QVT) iii) the result of transformations is linked to a software process development (UP), and iv) we consider security aspects. The use cases are derived from BPMN-BPD by applying a set of rules described in QVT (see Table 1), refinement rules and checklists (Table 2).

Table 1: Mapping between SBP and Use Case elements

transformation BusinessProcessDiagram2UseCaseDiagram	

top relation R1 // from Pool to Actor
{ checkonly domain bpmn_BusinessprocessDiagram p:Pool {name=n}
 enforce domain uml_UseCaseDiagram a:Actor{name=n}
  where { ap.containedNode → forAll(cn:Activity|R4(cn))} }
	top relation R2 // from Lane to Actor
	{ checkonly domain bpmn_BusinessprocessDiagram l:Lane {name=n}
	 enforce domain uml_UseCaseDiagram a:Actor{name=n}
	  where { ap.containedNode → forAll(cn:Activity|R4(cn))}}

top relation R3 // from Group to Actor
{ checkonly domain bpmn_BusinessProcessDiagram g:Group {name=n}
 enforce domain uml_UseCaseDiagram a:Actor {name =n}
  where { ap.containedNode → forAll(cn:Activity|R4(cn))}}
	relation R4 // from Activities to UseCase
	{ checkonly domain bpmn_BusinessProcessDiagram ac:Activity {name=n,
	inPartition=ap}
	 enforce domain uml_UseCaseDiagram uc:UseCase {name=n, subject=
	ACTORS: Set(Actor)};
	  where {ACTORS→including (a:Actor{name=ap.name})}}

transformation BPSec2UseCaseDiagram	
top relation R5 // from Security Requirement to subject { checkonly domain bpsec_BPSec sr:SecurityRequirement {requirementtype = n} enforce domain uml_UseCaseDiagram c:Clasifier {name=n}}	top relation R6 // from Security Requirement to subject { checkonly domain bpsec_BPSec sr:SecurityRequirement enforce domain uml_UseCaseDiagram a:Actor {name="Security Staff"}}

The refinement rules aim to complete the QVT rules by adding; subject names, group names, main actor identification, actor generalization and redundancies which have to be eliminated.

Table 2: Checklist with which to obtain security use cases

Access Control
«Preconditions»: Secure Role, and Permissions for the objects in the secure role scope and «Postconditions»Secure role validated to access to resources, Permissions for the validated objects, and Audit Register (optional)
– Assign secure role to the partition, region or action
– Validate the secure role. This task is divided into: identify, authenticate and authorize the secure role
– Verify permissions for the objects in the secure role field. This implies a review of the permissions granted to the objects that are within the field of access control specification
– If audit register has been specified, then the information related to the security role, the security permissions and the objects in the access control specification field must be stored

AttackHarmDetection
«Preconditions» Secure Role and «Postconditions»   Audit Register
– Assign secure role (origin and destination in the case of ObjectFlow).
– Register the type of element for which security requirements and date and time when access to that element was produced were specified

Integrity
«Preconditions» Secure Role and «Postconditions»   Audit Register
– High specification implies: ask for permissions, verify permissions, make security copies, and produce audit register
– Medium specification implies: send a warning message, make security copies, and produce audit register
– Low specification implies produce audit register

NonRepudiation
«Preconditions» Secure Roles (origin and destination) and «Postconditions» Valid roles, and Audit Register (optional)
–   Assign origin and destination roles
–   Validate roles: This task is divided into: identify, authenticate and authorize the secure role

Privacy
«Preconditions»   Secure Role and «Postconditions» Audit Register (optional)
– Assign a secure role (if anonymity was specified, then the role is generic and expires together with the session)
– Validate roles: This task is divided into: identify, authenticate and authorize the secure role
– Verify revelation permissions (anonymity and confidentiality)
– Verify storage permissions (anonymity only)
– Verify audit register specification
– If audit register has been specified, then the information related to the security role must be stored

4   Example

Our illustrative example, Figure 1 describes a typical BP for the admission of patients to a health-care institution. The business analyst identified "Patient" (individual who receives medical care), "Administration Area" where the medical institution records details about costs and insurance, and finally, "Medical Area" where pre-admission tests, examinations, evaluations and complete clinical data collection are carried out. The business analyst has considered the following aspects of security: Non

Repudiation for "Admission Request" message flow, Access Control and Privacy (confidentiality) have been defined for "Administration Area" and Integrity (high) requirement has been specified for "Clinical Information".
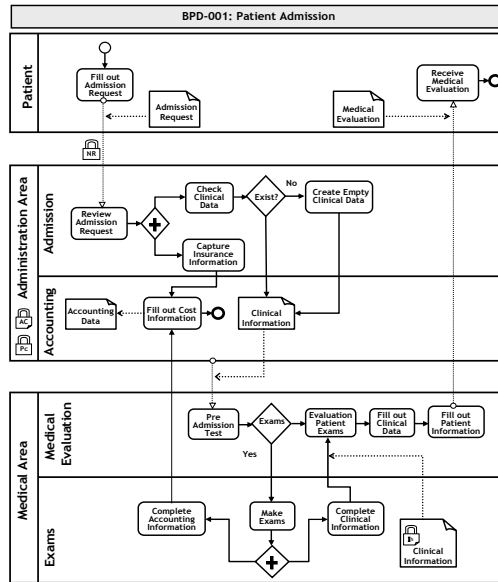

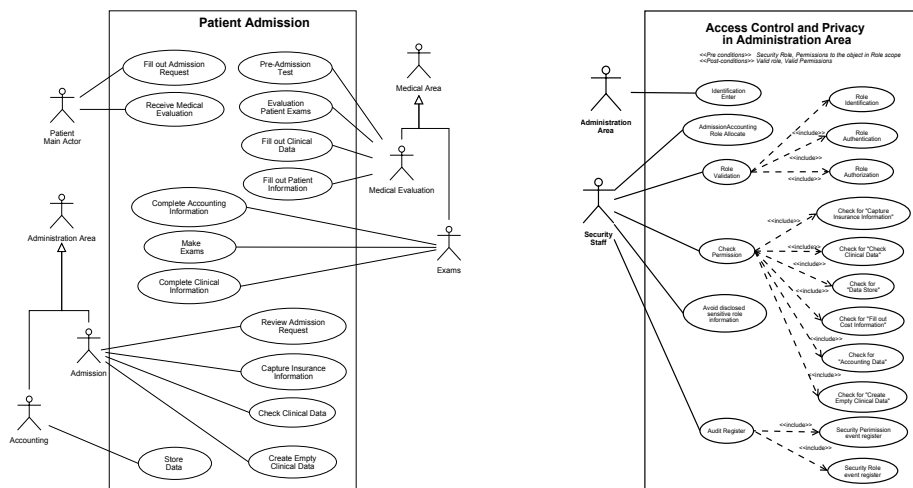**Figure 1:** Patient Admission to a Medical Institution

Figure 2: Patient Admission and Access Control/Privacy use cases specification

In Figure 2 (left-hand side), the use case related to the "Patients Admission" BP is shown. On the right-hand side, the security use case related to the specification of Access Control and Privacy for the "Administration Area" pool is presented.

5 Conclusions

In our work, we have gone a little further, given that we have gone beyond the business analyst's perspective (CIM level), in relating security to more concrete models (PIM level) which are orientated towards software construction. Additionally, we have established a link between two widely used notations, not only in the business field but also in software engineering. The result is a set of use cases and security use cases which have been achieved from the specification of a secure business process. Such UML artifacts, together with SBP, can be used in the first stages of a consolidated software development process such us UP. Future work is orientated towards enriching transformations to thus make it possible to obtain more complete use case models.

References

1. Alexander, I. F.; *Misuse Cases: Use Cases with Hostile Intent*, IEEE Software. Vol. 20 (1). (2003). pp.58-66.
2. Dijkman, R. M. and Joosten, S. M. M.; *An Algorithm to Derive Use Cases from Business Processes*, 6th International Conference on Software Engineering and Applications (SEA). Boston, USA,. (2002). pp.679-684.
3. Firesmith, D.; *Security Use Case*, Journal of Object Technology. V. 2 (3). (2003). pp.53-64.
4. Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.
5. Jürjens, J.; *Using UMLsec and goal trees for secure systems development*, ACM Symposium on Applied Computing (SAC). Madrid, Spain. (2002). pp.1026-1030.
6. Liew, P., Kontogiannis, P. and Tong, T.; *A Framework for Business Model Driven Development*, 12 International Workshop on Software Technology and Engineering Practice (STEP). (2004). pp.47-56.
7. Rodríguez, A., Fernández-Medina, E. and Piattini, M.; *A BPMN Extension for the Modeling of Security Requirements in Business Processes*, IEICE Transactions on Information and Systems. Vol. E90-D (4). (2007). pp.745-752.
8. Rungworawut, W. and Senivongse, T.; *A Guideline to Mapping Business Processes to UML Class Diagrams*, WSEAS Trans. on Computers. Vol. 4 (11). (2005). pp.1526-1533.
9. Sindre, G. and Opdahl, A.; *Capturing Security Requirements through Misuse Cases*, Norsk informatikkonferanse (NIK). Trondheim, Norway. (2001). pp.219-230.
10. Štolfa, S. and Vondrák, I.; *A Description of Business Process Modeling as a Tool for Definition of Requirements Specification*, Systems Integration 12th Annual International Conference. Prague, Czech Republic. (2004). pp.463-469.