Towards CIM to PIM Transformation: From Secure Business Processes Defined in BPMN to Use-Cases

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 software community is currently paying attention to model transformation. The MDA approach is particularly orientated towards solving the problems of time, cost and quality associated with software creation. Enterprises are, moreover, aware of the importance that business processes and security have in relation to their competitive position and performance. In our previous work, we have proposed a BPMN extension which can be used to define security requirement in business process specifications. A Secure Business Process description is that of computation independent models in an MDA context. In this paper we propose a CIM to PIM transformation composed of QVT rules. Various UML use cases, which will be part of an information system, are obtained from the secure business process description.

Keywords: MDA, Business Processes, Security Requirement, BPMN, QVT.

1 Introduction

In recent years, enterprise performance has been linked to the capability that each enterprise has to adapt itself to the changes that arise in the business market. In this context, Business Processes (BP) have become valuable resources in the maintenance of competitiveness.

Furthermore, economic globalization, along with the intensive use of communication and information technologies, have given rise to the situation of enterprises not only expanding their businesses but also increasing their vulnerability. As a consequence of this, and with the increase in the number of attacks on systems, it is highly probable that sooner or later an intrusion may be successful.

Although the importance of business process security is widely accepted, the business analyst perspective in relation to security has hardly been dealt with until now. In the majority of cases, the identification of security requirements has been somewhat confused. In general, there has been a tendency to identify functional

G. Alonso, P. Dadam, and M. Rosemann (Eds.): BPM 2007, LNCS 4714, pp. 408–415, 2007.

security requirements. This type of requirements varies according to the type of application, whilst the security requirements do not vary at a high level of abstraction [6]. In previous work [18] we introduced security representation into business processes. To do so, we extended the BPMN-BPD (Business Process Modeling Notation - Business Process Diagram) [3]. A BPSec extension was created which allowed us to capture those security requirements which had been expressed by the business analyst. Such a specification gave origin to a Secure Business Process (SBP).

Moreover, software engineering is currently greatly influenced by MDA, a new paradigm that claims to work at a model and metamodel level. The MDA approach is composed of the following perspectives: the computation independent viewpoint (CIM, Computation Independent Model), the platform independent viewpoint (PIM, Platform Independent Model) and the platform specific viewpoint (PSM, Platform Specific Model) [14]. Since these models represent a different abstraction of the same system, an integration/transformation mechanism is required to establish *how* to move from one level to another. The OMG proposal for a transformation language is QVT (Query/View/Transformation) [17].

In this paper, we demonstrate how a set of UML Use Cases [15] which are considered to be a PIM can be obtained from the specification of an SBP, which is considered to be a CIM. The transformations have been described as a set of QVT rules, checklists and refinement rules. Both the description of the SBP and the use cases can be used in the software development process. We have chosen to use the UP (Unified Process) [9].

The structure of the remainder of the paper is as follows: in Section 2, we shall summarize our proposal and related work. In Section 3 we shall present the main issues concerned with security requirement specification in business processes. In Section 4, we shall describe the way in which use cases can be obtained. Finally, in Section 5, we shall put forward an example and in Section 6 our conclusions will be drawn.

2 Our Proposal and Related Work

A business process which has been constructed by a business analyst is useful in the business environment and can also be used in the software construction process. A BP description contains important system requirements (a starting point for all development processes in modern software). In this work, we have paid special attention to the attainment of more concrete models derived from the BP specification which are, in particular, related to the security requirements specification in BP.

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. In the last column we can see the UP disciplines. The central part shows our proposal and the artifacts which are derived from its application. The SBP specification is made by using the BPMN-BPD and BPSec extension. The transformation is made by using QVT rules, checklists and refinement rules (in dark grey). If Figure 1 is observed horizontally it will be noted that an SBP description corresponds with a CIM model and can be used as a complement to the *Business Modeling* discipline of the UP. In addition, the Use Cases, which form a part of a PIM model, will complement the *Requirement* and *Analysis & Design* disciplines.

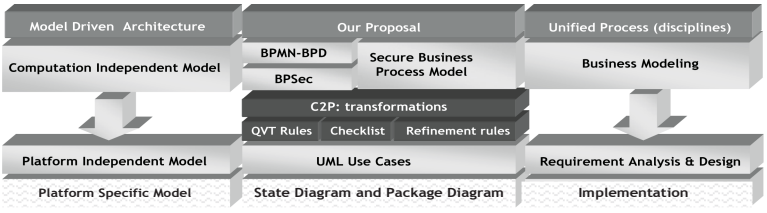

Fig. 1. An overview of our proposal

In related works we found that use cases (or misuse cases) [1, 5, 10, 16, 20], have been used to capture security requirements. However, unlike our proposal, they are not directly derived from BPMN-BPD security specifications.

In related works to the attainment of use cases from BP specifications, we have discovered that in [19], the possibility of obtaining use cases from a BP specification made with BPMN is suggested, and in [11], the automatic attainment of UML artifacts from a BP description that was made using BPMN is proposed. The authors extend the BPMN 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 [21], a transformation which was made from a business process described with UML 2.0 Activity Diagrams to use cases is stated and finally, in [4], use cases are obtained from business process models that are not represented by activity diagrams. Our proposal differs to the above works in that: (i) the business process specification includes security requirements, (ii) we have used the QVT for the specification of the transformations, and (iii) we have related the resulting artifacts to a software development process.

3 Security in Business Process

The works which are related to the specification of security requirements in business processes [2, 7, 8, 13] all coincide in the idea that it is necessary to capture the point of view of the business expert with regard to security, and to include these specifications within the software development process.

At present, security requirements are easy for business analysts to identify because: (i) business process representation has improved in BPMN, (ii) the security requirement tends to have the same basic kinds of valuable and potentially vulnerable assets [6], and (iii) empirical studies show that it is common at the business process level for customers and end users to be able to express their security needs [12].

Consequently, we have approached the problem of including security requirements in business processes by extending the BPMN-BPD. The proposed extension, which we have called BPSec, considers the graphical representation of security requirements; a non-limited list, taken from the taxonomy proposed in [6].

In our proposal we have used a padlock (see Figure 2a), standard *de facto*, to represent security requirements. The same symbol, the padlock, but with a twisted corner (see Figure 2b) is used to represent a Security Requirement with Audit Register. The set of security requirements are shown in Figure 2.

Fig. 2. Icons to represent security requirements in BPSec

4 Rules and Checklists to Obtain Use Cases from an SBP Model

A business process, built by a business analyst, is also very useful in a software construction process since it can be used to obtain numerous kinds of system requirements. Use cases and security use cases are derived from the SBP specification using BPMN-BPD by applying a set of QVT rules, checklists and refinement rules.

The QVT rules are orientated towards identifying actors and related use cases from Pools, Lanes, Groups, Activities, and security requirement specifications. In Table 1, rules expressed in textual QVT are described.

Table 1. Mapping between BPMN-BPD 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"}
  }
```

A set of checklists has been created through which to obtain the security related use cases. Each checklist contains a set of generic tasks that must be applied to a specific SBP specification. A selection of these checklists is shown in Table 2.

Table 2. Checklist through which to obtain security use cases

Access Control
«Preconditions» Secure Role, and Permissions over the objects in the secure role scope
«Postconditions» Secure role validated to access to resources, Permissions over the validated objects, and Audit Register (optional)
– Assign secure role to the partition, region or action
– Validate the secure role (this task is complemented with misuse cases described in [5]). This task is divided into:
• Identify the secure role. This implies recognizing roles before starting the interaction
• Authenticate the secure role: This task implies the verification of the role identity before starting the interaction
• Authorize the secure role. This implies assigning privileges to roles that were duly authenticated
– Verify permissions over the objects in the role secure 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
Privacy
«Preconditions» Secure Role
«Postconditions» Audit Register (optional)
– Assign a secure role (if anonymity was specified, then the role is generic and expires together with the session)
– Validate the role. This task is divided into:
• Identify the secure role. This implies recognizing the role before starting the interaction
• Authenticate the secure role. This task implies verifying the role identity before starting the interaction
• Authorize the secure role. This implies assigning privileges to the role that was duly authenticated
– 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

Finally, the refinement rules (see Table 3) are focused upon enriching the specifications obtained through the application of the QVT rules and checklists.

Table 3. Use case Refinement Rules (RR)

Rule	Description
RR1	Subject name (not related to security specification) is obtained from the business process name
RR2	Subject name for security requirement must be complemented with the name of the BPMN-BPD element
RR3	Group Name is obtained by linking the Pool or Lane names in which Group is contained
RR4	Main Actor corresponds to the Pool, Lane or Group name in which Start Event is present
RR5	Actor Generalization is obtained from Pool and Lane
RR6	Redundant specifications must be eliminated

5 Example

Our illustrative example (see Figure 3) describes a typical business process for the admission of patients to a health-care institution. In this case, the business analyst has identified the Pools: “Patient”, “Administration Area” (divided into “Accounting” and “Admission” lanes), and “Medical Area” (divided into “Medical Evaluation” and “Examination” lanes).

The business analyst has specified «Privacy» (anonymity) for the “Patient” Pool, with the aim of preventing the disclosure of sensitive information about Patients. S/he has specified «Nonrepudiation» for the Message Flow that goes from the “Fill out Admission Request” activity to the “Review Admission Request” activity with the aim of avoiding the denial of the “Admission Request” reception. And finally, «AccessControl» has been defined in a Pool called “Administration Area”. A «SecurityRole» can be derived from this specification. All objects in a Pool region must be considered for permission specification. Access control specification has been complemented with Audit Register requirement. This implies that information about the security role and security permissions must be registered.

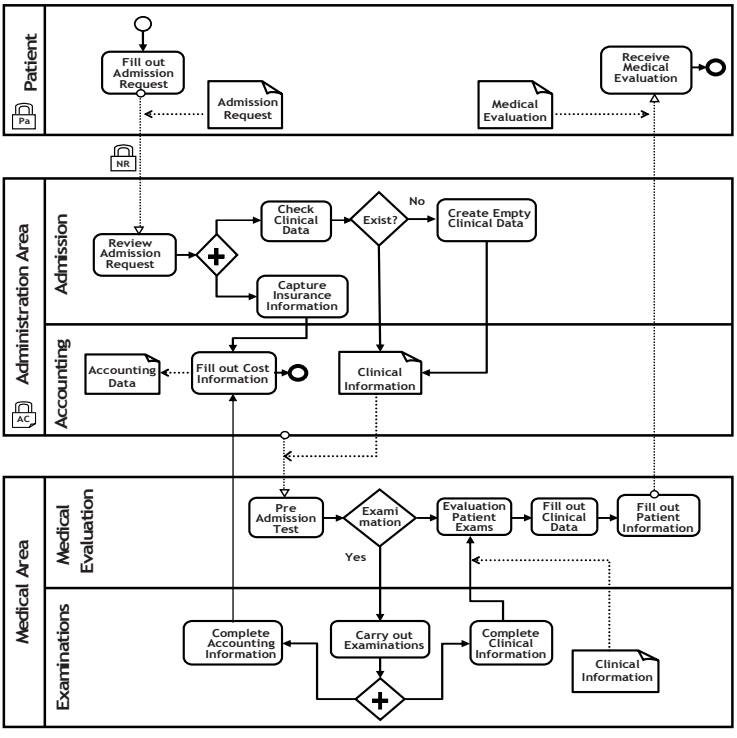

Fig. 3. Patient Admission to a Medical Institution

In Table 4 both the results of the application of the transformations defined with QVT and the application of the refinement rules are described.

Table 4. QVT and refinement rules applied to Patient Admission Business Process

Rule	Use Case element
R1	Actors: Patient, Administration Area, and Medical Area
R2	Actors: Admission, Accounting, Medical Evaluation and Examinations
R3	Actor: ---
R4	Use Case: Fill out Admission Request, Receive Medical Evaluation, Review Admission Request, Capture Insurance Information, Check Clinical Data, Create Empty Clinical Data, Fill out Cost Information, Pre-Admission Test, Evaluate Patient Examinations, Fill out Clinical Data, Fill out Patient Information, Complete Accounting Information, Carry out Examinations, and Complete Clinical information
R5	Subjects: Privacy, Non Repudiation, and Access Control
R6	Actor: Security Staff
RR1	Subject: Patient Admission
RR2	Subjects: Privacy in Patient, Non Repudiation in Admission Request, and Access Control in Administration Area
RR3	Actor: ---
RR4	Main Actor: Patient
RR5	Actor: Administration Area (Admission and Accounting) and Medical Area (Medical Evaluation and Exams)
RR6	Use cases: Review Admission Request, Capture Insurance Information, Check Clinical Data, Create Empty Clinical Data, and Fill out Cost Information can be excluded from the subject “Access Control in Administration Area”

In Figure 4, some use cases derived from the SBP for the admission of patients are graphically shown. The general use case is shown on the left-hand side and two use cases derived from security requirement specification (Privacy and Non Repudiation) are shown on the right-hand side.

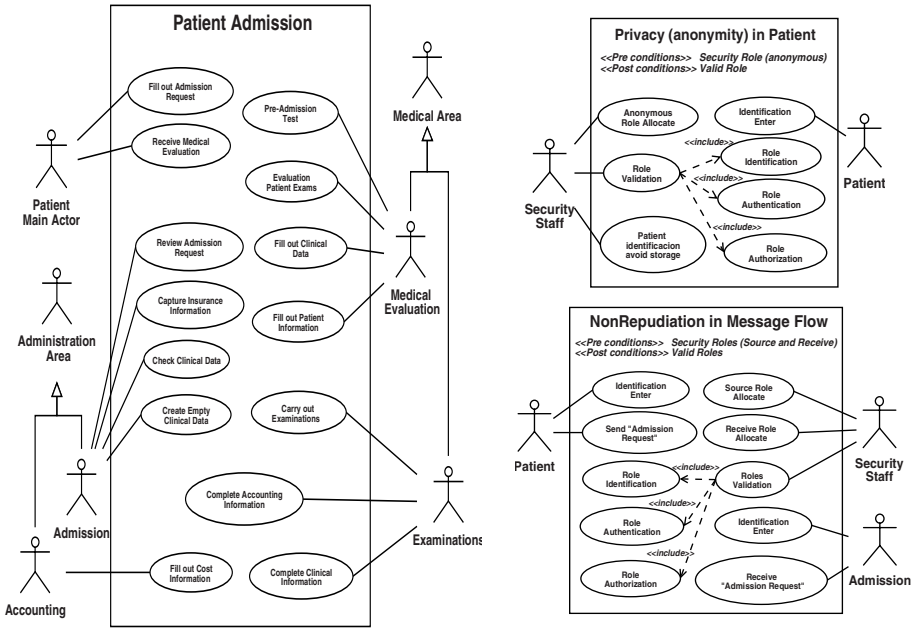

Fig. 4. Patient Admission, Privacy, and Non Repudiation use cases specification

6 Conclusion

One means by which to confront the problem of security consists of incorporating it into the business process specifications at an early stage. At this level, it is possible to capture security requirements which take the business analysts' viewpoint into account. In previous works, we have proposed a BPSec extension through which it is possible to specify security requirements at a high level of abstraction. Nevertheless, it is necessary to enable these specifications to form part of more concrete solutions. With this purpose in mind, we have used the MDA focus and QVT rules to specify the rules which allow us to pass from CIM to PIM. The result has been a set of UML Use Cases which have been obtained from the SBP specification described with BPMN-BPD.

Ongoing work is orientated towards enriching transformations in order to make it possible to obtain more complete models of use cases. Furthermore, in our future work we intend to optimize the prototype that we have created to carry out the transformations.

Acknowledgments. 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 (506PI287), 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. Alexander, I.F.: Misuse Cases: Use Cases with Hostile Intent, IEEE Software. IEEE Software 20(1), 58–66 (2003)
2. Backes, M., Pfitzmann, B., Waider, M.: Security in Business Process Engineering. In: van der Aalst, W.M.P., ter Hofstede, A.H.M., Weske, M. (eds.) BPM 2003. LNCS, vol. 2678, pp. 168–183. Springer, Heidelberg (2003)
3. BPMN: Business Process Modeling Notation Specification, OMG Final Adopted Specification, dtc/06-02-01 (2006), In http://www.bpmn.org/Documents/OMG%20Final%20-Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf
4. Dijkman, R.M., Joosten, S.M.M.: An Algorithm to Derive Use Cases from Business Processes. In: 6th International Conference on Software Engineering and Applications (SEA). Boston, USA, pp. 679–684 (2002)
5. Firesmith, D.: Security Use Case. Journal of Object Technology 2(3), 53–64 (2003)
6. Firesmith, D.: Specifying Reusable Security Requirements. Journal of Object Technology 3(1), 61–75 (2004)
7. Herrmann, G., Pernul, G.: Viewing Business Process Security from Different Perspectives. In: 11th International Bled Electronic Commerce Conference. Slovenia, pp. 89–103 (1998)
8. Herrmann, P., Herrmann, G.: Security requirement analysis of business processes. Electronic Commerce Research 6(3-4), 305–335 (2006)
9. Jacobson, I., Booch, G., Rumbaugh, J.: The Unified Software Development Process, p. 463 (1999)
10. Jürjens, J.: Using UMLsec and goal trees for secure systems development. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 1026–1030. Springer, Heidelberg (2003)
11. Liew, P., Kontogiannis, P., Tong, T.: A Framework for Business Model Driven Development. In: 12 International Workshop on Software Technology and Engineering Practice (STEP), pp. 47–56 (2004)
12. 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)
13. Maña, A., Montenegro, J.A., Rudolph, C., Vivas, J.L.: A business process-driven approach to security engineering. In: Mařík, V., Štěpánková, O., Retschitzegger, W. (eds.) DEXA 2003. LNCS, vol. 2736, pp. 477–481. Springer, Heidelberg (2003)
14. Object Management Group: MDA Guide Version 1.0.1 (2003), In http://www.omg.org/docs/omg/03-06-01.pdf
15. Object Management Group: Unified Modeling Language: Superstructure, version 2.0, formal/05-07-04 (2005), In http://www.omg.org/docs/formal/05-07-04.pdf
16. Popp, G., Jürjens, J., Wimmel, G., Breu, R.: Security-Critical System Development with Extended Use Cases. In: 10th Asia-Pacific Software Engineering Conference (APSEC). Chiang Mai, Thailand, pp. 478–487 (2003)
17. QVT: Meta Object Facility (MOF) 2.0 Query/View/Transformation Specification, OMG Adopted Specification ptc/05-11-01, p. 204 (2005)
18. Rodríguez, A., Fernández-Medina, E., Piattini, M.: A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE Transactions on Information and Systems E90-D(4), 745–752 (2007)
19. Rungworawut, W., Senivongse, T.: A Guideline to Mapping Business Processes to UML Class Diagrams. WSEAS Trans. on Computers 4(11), 1526–1533 (2005)
20. Sindre, G., Opdahl, A.: Capturing Security Requirements through Misuse Cases, Norsk informatikkonferanse (NIK). Trondheim, Norway, pp. 219–230 (2001)
21. Štolfa, S., Vondrák, I.: A Description of Business Process Modeling as a Tool for Definition of Requirements Specification. In: Systems Integration 12th Annual International Conference. Prague, Czech Republic, pp. 463–469 (2004)