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

Lecture Notes in Computer Science

LNCS LNAI LNBI

❯ springer.com

Fischer-Hübner et al. (Eds.)

LNCS 4083

Trust, Privacy, and Security in Digital Business

TrustBus 2006

LNCS 4083

Simone Fischer-Hübner
Steven Furnell
Costas Lambrinoudakis (Eds.)

Trust, Privacy, and Security in Digital Business

Third International Conference, TrustBus 2006
Kraków, Poland, September 2006
Proceedings

Springer

Lecture Notes in Computer Science 4083

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

Simone Fischer-Hübner Steven Furnell
Costas Lambrinoudakis (Eds.)

Trust, Privacy, and Security in Digital Business

Third International Conference, TrustBus 2006
Kraków, Poland, September 2006
Proceedings

Springer

Volume Editors

Simone Fischer-Hübner
Karlstad University
Department of Computer Science
Universitetsgatan 2, 651 88 Karlstad, Sweden
E-mail: simone.fischer-huebner@kau.se

Steven Furnell
University of Plymouth
School of Computing, Communications and Electronics
Network Research Group, Plymouth, PL4 8AA, UK
E-mail: sfurnell@plymouth.ac.uk

Costas Lambrinoudakis
University of the Aegean
Department of Information and Communication Systems Engineering
Karlovassi, 83200 Samos, Greece
E-mail: clam@aegean.gr

Library of Congress Control Number: 2006931261

CR Subject Classification (1998): K.4.4, K.4, K.6, E.3, C.2, D.4.6, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-37750-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-37750-4 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11824633 06/3142 5 4 3 2 1 0

Preface

This book presents the proceedings of the Third International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2006), held in Kraków, Poland, September 5-7, 2006. The conference continues from previous events held in Zaragoza (2004) and Copenhagen (2005), and maintains the aim of bringing together academic researchers and industry developers to discuss the state of the art in technology for establishing trust, privacy and security in digital business. We thank the attendees for coming to Kraków to participate and debate the new emerging advances in this area.

The conference programme included two keynote presentations, one panel session and eight technical papers sessions. The keynote speeches were delivered by Jeremy Ward from Symantec EMEA on the topic of "Building the Information Assurance Community of Purpose", and by Günter Karjoth from IBM Research - Zurich, with a talk entitled "Privacy Practices and Economics — From Privacy Policies to Privacy SLAs."

The subject of the panel discussion was "Is Security Without Trust Feasible?" chaired by Leszek T. Lilien from Western Michigan University, USA. The reviewed paper sessions covered a broad range of topics, from access control models to security and risk management, and from privacy and identity management to security protocols. The conference attracted 70 submissions, each of which was assigned to four referees for review. The Programme Committee ultimately accepted 24 papers for inclusion, which were revised based upon comments from their reviews.

We would like to express our thanks to the various people who assisted us in organizing the event and formulating the programme. We are very grateful to the Programme Committee members, and external reviewers, for their timely and rigorous reviews of the papers. Thanks are also due to the DEXA Organizing Committee for supporting our event, and in particular to Mrs. Gabriela Wagner for her help with the administrative aspects. We would also like to thank Sokratis Katsikas, Javier López and Günther Pernul for their past efforts in establishing the conference series, and their valuable advice and assistance in enabling us to take it forward.

Finally we would like to thank all of the authors who submitted papers for the event, and contributed to an interesting set of conference proceedings.

September 2006
Kraków, Poland

Simone Fischer-Hübner, Karlstad University, Sweden
Steven Furnell, University of Plymouth, UK
Costas Lambrinoudakis, University of the Aegean, Greece

Programme Committee

General Chair

Simone Fischer-Hübner	Karlstad University, Sweden

Programme Committee Co-chairs

Steven Furnell	University of Plymouth, UK
Costas Lambrinoudakis	University of the Aegean, Greece

International Programme Committee Members

Alessandro Acquisti	Carnegie Mellon University, USA
Marco Casassa Mont	HP Labs, Bristol, UK
David Chadwick	University of Kent, UK
Nathan Clarke	University of Plymouth, UK
Frederic Cuppens	ENST Bretagne, France
Ernesto Damiani	University of Milan, Italy
Ed Dawson	Queensland University of Technology, Australia
Claudia Eckert	Darmstadt Technical University, Germany
Hannes Federrath	University of Regensburg, Germany
Eduardo B. Fernandez	Florida Atlantic University, USA
Elena Ferrari	University of Insubria at Como, Italy
Juan M. González-Nieto	Queensland University of Technology, Australia
Rüdiger Grimm	University of Koblenz , Germany
Dimitrios Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Ehud Gudes	Ben-Gurion University, Israel
Sigrid Gürgens	Fraunhofer Institute for Secure Information Technology, Germany
Marit Hansen	Independent Center for Privacy Protection, Germany
Audun Josang	School of Software Engineering & Data Communications, QUT, Australia
Tom Karygiannis	NIST, USA
Sokratis Katsikas	University of the Aegean, Greece
Dogan Kesdogan	RWTH Aachen University, Germany
Hiroaki Kikuchi	Tokai University, Japan

Spyros Kokolakis	University of the Aegean, Greece
Klaus Kursawe	Philips Research, Eindhoven, The Netherlands
Leszek Lilien	Western Michigan University, USA
Antonio Lioy	Politecnico di Torino, Italy
Javier López	University of Malaga, Spain
Peter Lory	University of Regensburg, Germany
Olivier Markowitch	Université Libre de Bruxelles, Belgium
Fabio Martinelli	National Research Council – CNR Pisa, Italy
Fabio Massacci	University of Trento, Italy
Jose A. Montenegro	University of Malaga, Spain
Eiji Okamoto	University of Tsukuba, Japan
Martin S. Olivier	University of Pretoria, South Africa
Rolf Oppliger	eSecurity Technologies, Switzerland
Maria Papadaki	University of Plymouth, UK
Ahmed Patel	Centre for Applied Research in Information Systems, Kingston University, UK
Günther Pernul	University of Regensburg, Germany
Andreas Pfitzmann	Dresden University of Technology, Germany
Hartmut Pohl	University of Applied Sciences, FH Bonn-Rhein-Sieg, Germany
Karl Posch	University of Technology, Graz, Austria
Torsten Priebe	Capgemini, Austria
Gerald Quirchmayr	University of Vienna, Austria
Kai Rannenberg	Goethe University of Frankfurt, Germany
Christoph Ruland	University of Siegen, Germany
Pierangela Samarati	University of Milan, Italy
Matthias Schunter	IBM Zurich Research Lab., Switzerland
Mikko T. Siponen	University of Oulu, Finland
Adrian Spalka	University of Bonn, Germany
Leon Strous	De Nederlandsche Bank, The Netherlands
Stephanie Teufel	University of Fribourg, Switzerland
Jianying Zhou	I2R, Singapore

External Reviewers

Isaac Agudo	University of Malaga, Spain
Manos Antonakakis	NIST, USA
Aimilios Apostolopoulos	NIST, USA
Giampaolo Bella	University of Catania, Italy
Rainer Böhme	Dresden University of Technology, Germany
Katrin Borcea-Pfitzmann	Dresden University of Technology, Germany
Colin Boyd	Queensland University of Technology, Australia
Andrew Clark	Queensland University of Technology, Australia
Sebastian Clauß	Dresden University of Technology, Germany
Nora Cuppens-Boulahia	ENST Bretagne, France
Wiebke Dresp	University of Regensburg, Germany
Ludwig Fuchs	University of Regensburg, Germany
Dimitris Geneiatakis	University of the Aegean, Greece
Juhani Heikka	University of Oulu, Finland
Christos Kalloniatis	University of the Aegean, Greece
Costas Karafasoulis	University of the Aegean, Greece
George Karopoulos	University of the Aegean, Greece
Maria Karyda	University of the Aegean, Greece
Tobias Koelsch	RWTH Aachen University, Germany
Stefan Köpsell	Dresden University of Technology, Germany
Hristo Koshutanski	Create-Net, Italy
Ponnurangam Kumaraguru	Carnegie Mellon University, USA
Dimitris Lekkas	University of the Aegean, Greece
Mink Martin	RWTH Aachen University, Germany
Patrick Sinclair Merten	University of Fribourg, Switzerland
Nicola Mezzetti	Università di Bologna, Italy
Björn Muschall	University of Regensburg, Germany
Andriy Panchenko	RWTH Aachen University, Germany
Lexi Pimenidis	RWTH Aachen University, Germany
Carsten Rudolph	Fraunhofer Institute for Secure Information Technology, Germany
Rolf Schillinger	University of Regensburg, Germany
Christian Schläger	University of Regensburg, Germany
Sandra Steinbrecher	Dresden University of Technology, Germany
Martin Steinert	University of Fribourg, Switzerland
Daniela Wanner	University of Fribourg, Switzerland
Andreas Westfeld	Dresden University of Technology, Germany
Nicola Zannone	University of Trento, Italy

Table of Contents

Session 1: Privacy and Identity Management

Session 2: Security and Risk Management

Session 3: Security Requirements and Development

Session 4: Privacy Enhancing Technologies and Privacy Management

Session 5: Access Control Models

Session 6: Trust and Reputation

Session 7: Security Protocols

Session 8: Security and Privacy in Mobile Environments

References

[1] Castro-Rojo, R., Lopez, D. R.: The PAPI system: point of access to providers of information. In: Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 37. Elsevier, Amsterdam (2001) 703-710

[2] Cavusoglu, H., Mishra, B., Raghunathan, S.: A Model for Evaluating IT Security Investments. In: Communications of the ACM, Volume 47. ACM Press, New York (2004) 87–92

[3] Chadwick, D., Otenko, A.: The PERMIS X.509 role based privilege management infrastructure. In: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT '02). ACM Press, New York (2002) 135-140

[4] Cremonini, M., Martini, P.: Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In: Proceedings of the Fourth Workshop on the Economics of Information Security. Harvard (2005)

[5] Jøsang, A., Pope, S.: User Centric Identity Management. In: Clark, A., Kerr, K., Mohay, G. (eds.): Proceedings of AusCERT Asia Pacific Information Technology Security Conference 2005. Gold Coast (2005) 77-89

[6] Katsikas, S. K., Lopez, J., Pernul, G.: Trust, Privacy and Security in E-business: Requirements and Solutions. In: Proc. of the 10th Panhellenic Conference on Informatics (PCI'2005). Lecture Notes in Computer Science. Springer-Verlag, Berlin Heidelberg New York (2005) 548-558

[7] Kormann, P., Rubin, A.: Risks of the Passport single sign-on protocol. In: Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 33. Elsevier, Amsterdam (2000) 51-58

[8] Liberty ID-FF Bindings and Profiles Specification, Liberty Alliance Project, 2003. Accessible at http://www.projectliberty.org/specs/liberty-idff-bindings-profiles-v1.2.pdf

[9] Lopez, J., Oppliger, R., Pernul, G.: Authentication and authorization infrastructures (AAIs): a comparative survey. In: Computers & Security, Volume 23. Elsevier, Amsterdam (2004) 578-590

[10] Microsoft Passport Review Guide. Accessible at http://download.microsoft.com/download/a/f/4/af49b391-086e-4aa2-a84b-ef6d916b2f08/ passport_reviewguide.doc

[11] Nowey, T., Federrath, H., Klein, C., Plössl, K.: Ansätze zur Evaluierung von Sicherheitsinvestitionen. In: Proc. 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics, P-62, Köllen-Verlag, Bonn (2005) 15-26

[12] Pfleeger, S.L.: Risky Business: what we have yet to learn about risk management. Journal of Systems and Software, Volume 53. Elsevier, New York (2000) 265-273

[13] Pfleeger, C.P., Pfleeger, S.L.: Security in Computing. 3rd edn. Prentice Hall, New Jersey (2002)

[14] Schlaeger, C., Nowey, T., Montenegro, J.A.: A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce. In: Proc. of the First International Conference on Availability, Reliability and Security (ARES '06). IEEE Computer Society, Los Alamitos (2006) 709-716

[15] Schlaeger, C., Pernul, G.: Authentication and Authorisation Infrastructures in b2c e-commerce. In: Bauknecht, K., Pröll, B., Werthner, H. (eds.): Proc. of the Sixth International Conference on Electronic Commerce and Web Technologies - EC-Web '05. Lecture Notes in Computer Science, Vol. 3590. Springer Verlag, Berlin Heidelberg New York (2005) 306-315

[16] Tanenbaum, A.S., van Stehen, M.: Verteilte Systeme. Grundlagen und Paradigmen. Prentice Hall, München (2003)

[17] Vidalis, S.: A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. School of Computing Technical Report CS-04-03, University of Glamorgan (2004)

Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes

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

[1] Departamento de Auditoría e Informática, Universidad del Bio Bio,
La Castilla S/N, Chillán, Chile
alfonso@ubiobio.cl

[2] ALARCOS Research Group, Information Systems and Technologies Department,
UCLM-Soluziona Research and Development Institute,
University of Castilla-La Mancha, Ciudad Real, Spain
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract. Security is a crucial issue for business performance, but usually, it is considered after the business processes definition. Many security requirements can be expressed at the business process level. A business process model is important for software developers, since they can capture from it the necessary requirements for software design and creation. Besides, business process modeling is the center for conducting and improving how the business is operated. This paper contains a description of our UML 2.0 extension for modeling secure business process through activity diagrams. We will apply this approach to a typical health-care business process.

1 Introduction

The new business scene, where there are many participants and an intensive use of communications and information technologies, implies that enterprises not only expand their businesses but also increase their vulnerability. As a consequence, with the increase of the number of attacks on systems, it is highly probable that sooner or later an intrusion can be successful [19]. This security violation causes losses. For this reason, it is necessary to protect computers and their systems in the best possible way. Best possible security does not necessarily mean absolute security, but a reasonable high security level in relation to the given limitations [25].

On the other hand, business processes are key to maintain competitiveness. Since, they are the ability of an enterprise to describe, standardize, and adapt the way it reacts to certain types of business events, and how it interacts with suppliers, partners, competitors, and customers [21].

Regardless of the importance of the security notion for companies, this is often neglected in business process models, which usually concentrate on modeling the process in a way that functional correctness can be shown [2] mainly due to the fact that the expert in the business process domain is not an expert in security [9]. Typically, security is considered after the definition of the system. This approach often leads to problems, which most of the times are translated into security

S. Fischer-Hübner et al. (Eds.): TrustBus 2006, LNCS 4083, pp. 51 – 61, 2006.

vulnerabilities [17], which clearly justify the need of increasing the effort in the pre-development phases, where fixing the bugs is cheaper [14].

If we consider that empirical studies show that it is common at the business process level that customers and end users are able to express their security needs [14], then it is possible to capture at a high level, security requirements easily identifiable by those who models business processes. Besides, requirements specification usually results in a specification of the software system which should be as exact as possible [1], since, effective business process models facilitate discussions among different stakeholders in the business, allowing them to agree on the key fundamentals and to work towards common goals [5].

For business process modeling, there are several languages and notations [8], however, UML (Unified Modeling Language) is a widely accepted standard notation. The most important change of UML 2.0 version with respect to the previous ones has been that of the activity diagrams which improve the business process representation. Our work considers a UML 2.0 extension that allows us to incorporate security requirements into activity diagrams from the perspective of the business analyst. We have considered the security requirements identified in the taxonomy proposed in [7].

Our proposal is based on the MDA (Model Driven Architecture) approach. We will define early requirements identification using UML and this will make it possible to perform independent specifications of the implementation. Moreover, we believe that it is possible to have two different perspectives about security requirements at a high level of abstraction. One of them related to business analysts and the other associated with security experts. In this paper we have deepened in the first perspective.

The structure of the rest of the paper is the following: in Section 2, we will summarize the main issues about security in business processes. In Section 3, we will present a brief overview of UML 2.0 activity diagrams and extensions. In Section 4, we will propose a UML 2.0 extension to represent security requirements. Finally, in Section 5, we will present an example and in Section 6 our conclusion will be drawn.

2 Security in Business Process

In spite of the importance of security for business processes, we have found out two problems. The first one is that modeling has not been adequate since, generally, those who specify security requirements are requirements engineers that have accidentally tended to use architecture specific restrictions instead of security requirements [6]. And in the second place, security has been integrated into an application in an ad-hoc manner, often during the actual implementation process [2], during the system administration phase [13] or it has been considered like outsourcing [16].

An approach to model security considering several perspectives is presented in [9]. Authors take into consideration the following perspectives: *static*, about the processed information security, *functional*, from the viewpoint of the system processes, *dynamic*, about the security requirements from the life cycle of the objects involved in the business process, *organizational*, used to relate responsibilities to acting parties within the business process and the *business processes* perspective, that provides us with an integrated view of all perspectives with a high degree of abstraction. Moreover, capturing the security requirements of a system is a hard task that must be established at the initial stages of system development, and business spruces offer a view of business structure that is very suitable as a basis for the elicitation and specification of security requirements. Business process representations may in this way present in all stages of system development different levels of abstraction appropriate for each stage [14]. Consequently, we believe that business analysts can integrate their view about business security into the business process perspective.

On the other hand, functional security requirements tend to vary depending on the kind of application. This cannot be said about security requirements since any application at the highest level of abstraction will tend to have the same basic kinds of valuable and potentially vulnerable assets [7].

The research works related to security specifications carried out by business domain experts are; (i) scarce [2, 9, 15], (ii) oriented to transaction security [20], (iii) directly oriented to information systems in general [23] or (iv) thought for security and software engineers [16]. Moreover, several works [10, 13, 14, 24] have used UML to perform the specification of security requirements. In these works, activity diagrams have not been used to capture security requirements. However, we believe that it is possible that business analysts can express their security requirements through activity diagrams.

3 UML 2.0 Activity Diagrams and UML 2.0 Extensions

UML 2.0 is divided into structural and behavioral specifications. Behavior models specify how the structural aspects of a system change over time. UML has three behavior models: activities, state machines, and interactions. Activities focus on the sequence, conditions, and inputs and outputs for invoking other behaviors, state machines show how events cause changes of object state and invoke other behaviors, and interactions describe message-passing between objects that causes invocation of other behaviors [4].

Activity diagrams are the UML 2.0 elements used to represent business processes and workflows [11]. In UML previous versions, expressivity was limited and this fact confused users that did not use the orientation to objects as an approach for modeling. Now, it is possible to support flow modeling across a wide variety of domains [3]. An activity specifies the coordination of executions of subordinate behaviors, using a control and data flow model. Activities may form invocation hierarchies invoking other activities, ultimately resolving to individual actions [18]. The graphical notation of an activity is a combination of nodes and connectors that allow us to form a complete flow.

On the other hand, the Profiles package contains mechanisms that allow meta-classes from existing meta-models to be extended to adapt them for different purposes. The profiles mechanism is consistent with the OMG Meta Object Facility (MOF) [18]. UML profiles consist of Stereotypes, Constraints and Tagged Values. A stereotype is a model element defined by its name and by the base class to which it is assigned. Constraints are applied to the stereotype with the purpose of indicating limitations (e.g. pre or post conditions, invariants). They can be expressed in natural language, programming language or through OCL (Object Constraint Language).

Tagged values are additional meta-attributes assigned to a stereotype, specified as name-value pairs.

Research works related to UML 2.0 profiles and business processes refer to aspects of the business such as Customer, kind of Business Process, Goal, Deliverable and Measure [12], Data Warehouse and its relation to business process dynamic structures [22] or they add semantics to the activities considering organizational aspects that allow us to express resource restrictions during the execution of an activity [11].

4 UML 2.0 Extension for Modeling Business Process with Security Requirement

Our proposal allows business analysts to specify security requirements in the business process by using activity diagrams. It is the first part of a security requirements specification that will have later to be complemented by a security analyst. Both perspectives let us enrich the security requirements specifications in business processes.

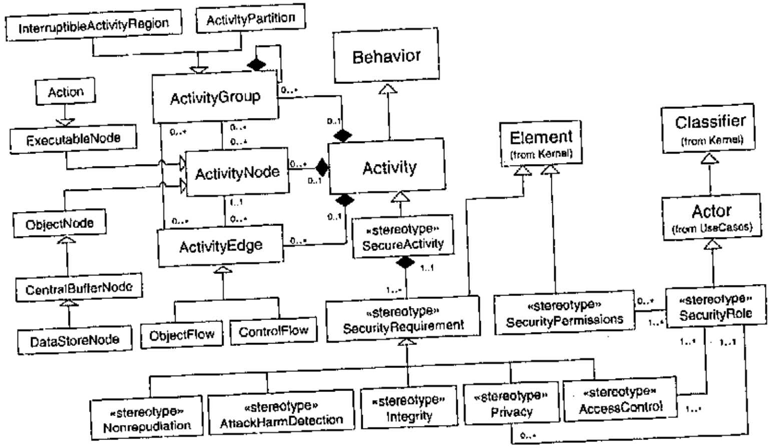

Fig. 1. Extending the UML 2.0 meta-model with security stereotypes

Figure 1 shows the UML 2.0 meta-model extended with stereotypes (in dark) for Secure Activity specifications. A Secure Activity is a stereotype derived from Activity. «SecureActivity» is strongly associated with security requirements stereotypes. «SecurityRequirement» has a composition relationship with «SecureActivity». The proposed notation for «SecurityRequirement» must be complemented by adding it letters that will allow us to identify the type of requirement that is specified.

The stereotypes derived from «SecurityRequirement» can be *added* to activity diagrams elements. Any security requirement (NR, AD, I, P or AC) can be added to activity diagram elements (see Table 1). For example, an «Integrity» requirement can be specified over data store, control flow or object flow.

«SecurityRole» and «SecurityPermissions» are related in different ways, because both can be *obtained* from the UML 2.0 element of activity diagrams (see Table 1). For example, «SecurityRole» can be obtained from activities, partitions or regions specifications, but it is not specified in an explicit way over these activity diagrams elements. «SecurityPermission» is a special case, because, permissions depending on each activity diagram element which they are related to. For example, for Actions object, Execution or CheckExecution operations must be specified (see Table 3).

Table 1. Security Requirements and Activity Diagram Elements

	UML 2.0 element for containment in activity diagrams					
Stereotypes for secure activity specification	Activity	Activity Partition	Interruptible Activity Region	Action	Data StoreNode	Object Flow
Nonrepudiation (NR)						✓
AttackHarmDetection(AD)	✓	✓	✓	✓	✓	✓
Integrity (I)					✓	✓
Privacy (P)		✓				
AccessControl (AC)	✓	✓	✓			
Security Role	✓	✓	✓			
SecurityPermissions				✓	✓	✓

In addition, we need the definitions of some new data types to be used in tagged value definitions. In Table 2, we will show the new data type stereotypes definitions. All new data types have been derived from the Enumeration Class.

Table 2. New data types

Name	Description	Values associated
SecReqType	It represents a type of security requirement. It must be specified for Non Repudiation, Attack/Harm Detection, Integrity, Privacy or Access Control.	NR, AD, I, P, AC
PerOperations	It is an enumeration for possible operations over objects in activity diagrams. These operations are related to permissions granted over the object	Execution, CheckExecution, Update, Create, Read, Delete, SendReceive, CheckSendReceive
ProtectDegree	It is an abstract level that represents criticality. This degree can be low (l), medium (m) or high (h).	l, m, h
PrivacyType	It consists of anonymity (a) or confidentiality (c).	a, c
AuditingValues	It represents different security events related to the security requirement specification in business processes. They will be used in later auditing	ElementName, SourceName, DestinationName, DateTimeSend, DateTimeReceive, Date, Time, RoleName

Next tables will show the stereotypes for secure activity specifications extensively. Each stereotype specification contains: name, base class, description, notation, constrains and tagged values.

Table 3. Security activity and security requirement stereotypes

Name: SecureActivity Base Class: Activity	Description: A secure activity contains security specification related to requirements, role identifications and permissions.	
Constrains	• It must be associated at least with one SecurityRequirement **context** SecureActivity **inv**: self.SecurityRequirement->size()>=1	
Name: SecurityRole Base Class: Actor (from UseCases)	Description: It contains a role specifications. This roles must be obtained from access control and/or privacy specifications	
Constrains	• The role in the security role stereotype can be derived from: Activity, ActivityPartition and/or InterruptibleActivityRegion (see Table 1) • It must be associated with an access control specification and can be associated with privacy and security permissions **context** SecurityRole **inv**: self.AccessControl -> size() >= 1 **context** SecurityRole **inv**: self.Privacy -> size()>= 0 **context** SecurityRole **inv**: self.SecurityPermission -> size()>= 0 **context** SecurityRole	
Name: SecurityPermission Base Class: Element (from Kernel)	Description: It contains permission specifications. A permissions specification must contain details about the objects and operations involved	

Constrains	• It must be associated with security role specification
	context SecurityPermission **inv**: self.SecurityRole ->size()>= 1
	• It must be associated with Actions, DataStoreNode or ObjectFlow
	context SecurityPermissions **inv**:
	self.Actions.size+self.DataStoreNode.size+self.ObjectFlow.size=1
	• It must be specified such as Objects and Operations pairs.
	context SecurityPermissions **inv**:
	if self.Actions->size()=1 then
	self.SecPerOperations="Execution" or
	self.SecPerOperations="Checkexecution"
	endif
	if self.Datastorenode->size()=1 then
	self.SecPerOperations="Update" or
	self.SecPerOperations ="Ceate" or
	self.SecPerOperations="Read" or
	self.SecPerOperations ="Delete"
	endif
	if self.Objectflow->size()=1 then
	self.SecPerOperations="Sendreceive" or
	self.SecPerOperations="Checksendreceive"
	endif	

Tagged Values	SecurityPermissionOperation: SecPerOperations	
Name: SecurityRequirement Base Class: Element (from Kernel)	Description: Abstract class containing security requirements specifications. Each security requirement type must be indicated in some of its subclasses.	**Notation**
Constrains	• A security requirement must be associated with a secure activity **context** SecurityRequirement **inv**: self.SecureActivity ->size()=1 • The notation must be completed in the subclass specification for each security requirement. It must be used one security requirement type.	🔒
Tagged Values	SecurityRequirementType: SecReqType	**Notation**
Name	Nonrepudiation	
Base Class	SecurityRequirement	🔒 NR
Description	It establishes the need to avoid the denial of any aspect of the interaction. An auditing requirement can be indicated in Comment	
Constrains	• It can be only specified in the diagram elements indicated in Table 1.	

Tagged Values	AvNr: AuditingValues
	context Nonrepudiation **inv**:
	self.AvNr="ElementName" or
	self.AvNr="SourceName" or
	self.AvNr="DestinationName" or
	self.AvNr="DateTimeSend" or
	self.AvNr="DateTimeReceive"	

Table 4. Stereotypes specifications for security requirements

Name	AttackHarmDetection	***Notation***
Base Class	SecurityRequirement	
Description	It indicates the degree to which the attempt or success of attacks or damages is detected, registered and notified. An auditing requirement can be indicated in Comment	🔒 AD
Constrains	• It can be only specified in the diagram elements indicated in Table 1.	
Tagged Values	AvAD: AuditingValues **context** AttackHaarmDetection **inv**: self.AvAD="ElementName" or self.AvAD="Date" or self.AvAD="Time"	
Name	Integrity	**Notation**
Base Class	SecurityRequirement	
Description	It establishes the degree of protection of intentional and non authorized corruption. The elements are protected from intentional corruption. An auditing requirement can be indicated in Comment.	🔒 Ix
Constrains	• It can be only specified in the diagram elements indicated in Table 1. • The Protection Degree must be specified by adding a lower case letter according to PDI tagged value.	
Tagged Values	PDI : ProtectDegree AvI: AuditingValues **context** Integrity **inv**: self.AvI="ElementName" or self.AvI="Date" or self.AvI="Time"	
Name	Privacy	**Notation**
Base Class	SecurityRequirement	
Description	It indicates the degree to which non authorized parts are avoided to obtain sensitive information. An auditing requirement can be indicated in Comment.	🔒 Px
Constrains	• It can be only specified in the diagram elements indicated in Table 1. • A privacy requirement has one security role specification **context** Privacy **inv**: self.SecurityRole -> size() = 1 • The Privacy Type must be specified adding a lower case letter according to Pv tagged value. If privacy type is not specified then anonymity and confidentiality are considered.	
Tagged Values	Pv: PrivacyType AvPv: AuditingValues **context** Privacy **inv**: self.AvPv="RoleName" or self.AvPv="Date" or self.AvPv="Time"	
Name	AccessControl	**Notation**
Base Class	SecurityRequirement	
Description	It establishes the need to define and/or intensify the access control mechanisms (identification, authentication and authorization) to restrict access to certain components in an activity diagram. An auditing requirement can be indicated in Comment.	🔒 AC
Constrains	• It can be only specified in the diagram elements indicated in Table 1. • It is valid only if it is specified at least one security role. **Context** AccessControl **inv**: self.SecurityRole -> size() >= 1	
Tagged Values	AvAC: AuditingValues **context** AccessControl **inv**: self.AvAC="RoleName" or self.AvAC="Date" or self.AvAC="Time"	

5 Example

Our illustrative example (see Figure 2) describes a typical business process for the admission of patients in a health-care institution. In this case, the business analyst identified the following Activity Partitions: Patient, Administration Area (which is a top partition that is divided into Admission and Accounting middle partitions), and the Medical Area (divided into Medical Evaluation and Exams).

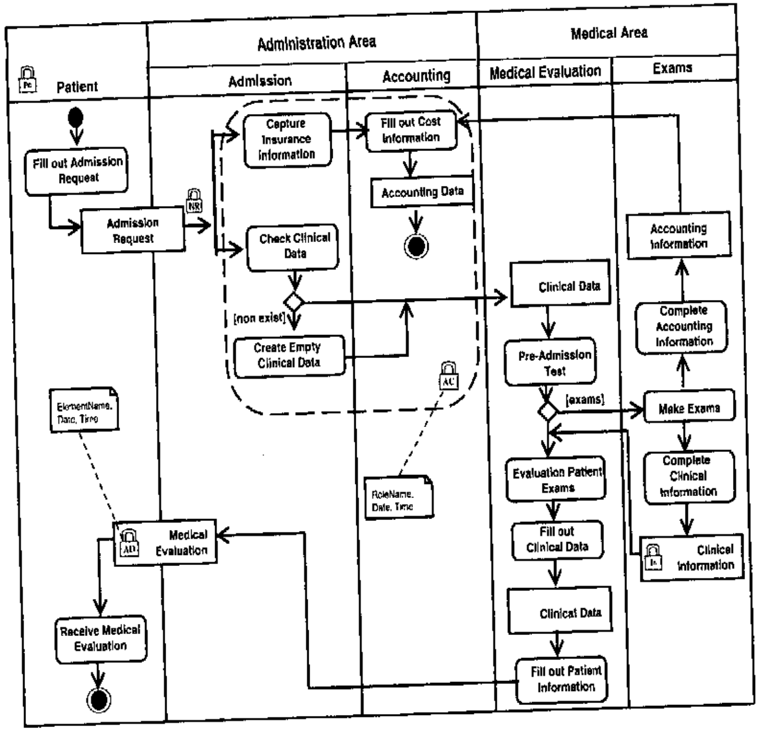

Fig. 2. Admission of Patients in a Medical Institution

The business analyst has considered several aspects of security. He/she has specified «Privacy» (confidentiality) for Activity Partition "Patient", with the aim of preventing the disclosure of sensitive information about Patients. «Nonrepudiation» has been defined over the control flow that goes from the action "Fill Admission Request" to the actions "Capture Insurance Information" and "Check Clinical Data" withthe aim of avoiding the denial of the "Admission Request" reception. «AccessControl» has been defined over the Interruptible Activity Region. A «SecurityRole» can be derived from this specification. Admission/Accounting will be a role. All objects in an interruptible region must be considered for permissions specification (see Table 5). Access control specification has been complemented with audit requirement. This implies that it must register role name, date and time of all events related to the region interruptible. Integrity (high) requirement has specified for Data Store "Clinical Information". Finally, the business analyst has specified Attack Harm Detection with auditing requirement. All events related to attempt or success of attacks or damages are registered (names in this case are clinical information, date and time).

Table 5. «SecurityRole» and «SecurityPermission» specifications

	Permissions		
Role	Objects		Operations
Admission/Accounting	Action	Capture Insurance Information Fill out Cost information Check Clinical Data Create Empty Clinical Data	Execution CheckExecution Execution Execution
	DataStoreNode	Accounting Data	Update

6 Conclusions and Ongoing Work

The UML 2.0 version, particularly improved for business process representation through activity diagrams, opens an opportunity to incorporate security requirements that allow us to increase this aspect of the systems from early stages in software development. In this paper, we have presented a UML 2.0 extension that allows us to incorporate security requirements into activity diagrams that will increase the scope of the expressive ability of business analysts.

The next step should be that of applying an MDA approach to transform the model (including the security requirements) into most concrete models (i.e. execution models). Therefore, future work must be oriented to enrich the security requirements specifications, improving the UML extension specification to complement it with Well-Formedness Rules and OCL.

Acknowledgements

This research is part of the following projects: DIMENSIONS (PBC-05-012-1), supported by FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", COMPETISOFT (granted by CYTED) and RETISTIC (TIC2002-12487-E) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (Spain).

References

1. Artelsmair, C. and Wagner, R.; *Towards a Security Engineering Process*, The 7th World Multiconference on Systemics, Cybernetics and Informatics. Vol. VI. Orlando, Florida, USA. (2003). pp.22-27.
2. Backes, M., Pfitzmann, B. and Waider, M.; *Security in Business Process Engineering*, International Conference on Business Process Management. Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). pp.168-183.
3. Bock, C.; *UML 2 Activity and Action Models*, Journal of Object Technology. Vol. 2 (4), July-August. (2003). pp.43-53.
4. Bock, C.; *UML 2 Activity and Action Models, Part 2: Actions*, Journal of Object Technology. Vol. 2 (5). September-October. (2003). pp.41-56.

5. Eriksson, H.-E. and Penker, M., *Business Modeling with UML*, OMG Press. (2001).
6. Firesmith, D.; *Engineering Security Requirements*, Journal of Object Technology. Vol. 2 (1), January-February. (2003). pp.53-68.
7. Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.
8. Giaglis, G. M.; *A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques*, International Journal of Flexible Manufacturing Systems. Vol. 13 (2). (2001). pp.209-228.
9. Herrmann, G. and Pernul, G.; *Viewing Business Process Security from Different Perspectives*, 11th International Bled Electronic Commerce Conference. Slovenia. (1998). pp.89-103.
10. Jürjens, J.; *Towards Development of Secure Systems Using UMLsec*, Fundamental Approaches to Software Engineering, 4th International Conference, FASE 2001 at ETAPS-2001 Genova, Italy, April 2-6, 2001, Proceedings. Vol. 2029. (2001). pp.187-200.
11. Kalnins, A., Barzdins, J. and Celms, E.; *UML Business Modeling Profile*, Thirteenth International Conference on Information Systems Development, Advances in Theory, Practice and Education. Vilnius, Lithuania. (2004). pp.182-194.
12. List, B. and Korherr, B.; *A UML 2 Profile for Business Process Modelling*, 1st International Workshop on Best Practices of UML (BP-UML 2005) at ER-2005. Klagenfurt, Austria. (2005).
13. Lodderstedt, T., Basin, D. and Doser, J.; *SecureUML: A UML-Based Modeling Language for Model-Driven Security*, UML 2002 - The Unified Modeling Language, 5th International Conference. Vol. 2460. Dresden, Germany. (2002). pp.426-441.
14. Lopez, J., Montenegro, J. A., Vivas, J. L., Okamoto, E. and Dawson, E.; *Specification and design of advanced authentication and authorization services*, Computer Standards & Interfaces. Vol. 27 (5). (2005). pp.467-478.
15. Maña, A., Montenegro, J. A., Rudolph, C. and Vivas, J. L.; *A business process-driven approach to security engineering*, 14th. International Workshop on Database and Expert Systems Applications (DEXA). Prague, Czech Republic. (2003). pp.477-481.
16. Maña, A., Ray, D., Sánchez, F. and Yagüe, M. I.; *Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software*, VIII Reunión Española de Criptología y Seguridad de la Información, RECSI'04. Leganés, Madrid. España. (2004). pp.383-392.
17. Mouratidis, H., Giorgini, P. and Manson, G. A.; *When security meets software engineering: a case of modelling secure information systems*, Information Systems. Vol. 30 (8). (2005). pp.609-629.
18. Object Management Group; *Unified Modeling Language: Superstructure*, version 2.0, formal/05-07-04. In http://www.omg.org/docs/formal/05-07-04.pdf. (2005).
19. Quirchmayr, G.; *Survivability and Business Continuity Management*, ACSW Frontiers 2004 Workshops. Dunedin, New Zealand. (2004). pp.3-6.
20. Röhm, A. W., Herrmann, G. and Pernul, G.; *A Language for Modelling Secure Business Transactions*, 15th. Annual Computer Security Applications Conference. Phoenix, Arizona. (1999). pp.22-31.
21. Roser, S. and Bauer, B.; *A Categorization of Collaborative Business Process Modeling Techniques*, 7th IEEE International Conference on E-Commerce Technology Workshops (CEC 2005). Munchen, Germany. (2005). pp.43-54.
22. Stefanov, V., List, B. and Korherr, B.; *Extending UML 2 Activity Diagrams with Business Intelligence Objects*, 7th International Conference on Data Warehousing and Knowledge Discovery (DaWaK2005). Copenhagen, Denmark. (2005).

23. Tryfonas, T. and Kiountouzis, E. A.; *Perceptions of Security Contributing to the Implementation of Secure IS*, Security and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003). Vol. 250. Athens, Greece. (2003). pp.313-324.
24. Vivas, J. L., Montenegro, J. A. and Lopez, J.; *Towards a Business Process-Driven Framework for security Engineering with the UML*, Information Security: 6th International Conference, ISC 2003, Bristol, U.K. (2003). pp.381-395.
25. Zuccato, A.; *Holistic security requirement engineering for electronic commerce*, Computers & Security. Vol. 23 (1). (2004). pp.63-76.