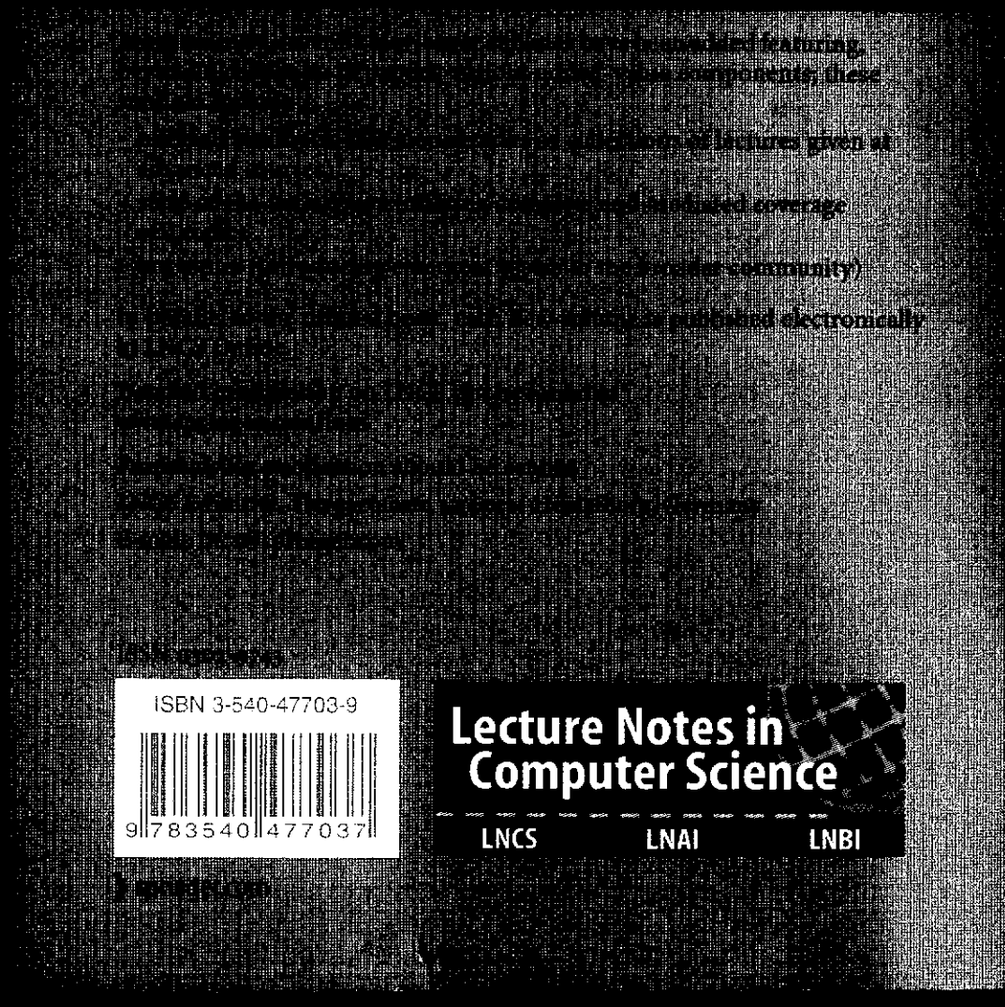
Lecture Notes in Computer Science

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.)



Roddick et al. (Eds.)

LNCS 4231

ER 2006 Workshops BP-UML, CoMoGIS, COSS, ECDM, OIS, QoIS, SemWAT

ER 2006 Workshops BP-UML, CoMoGIS COSS, ECDM, OIS, QoIS, SemWAT Tucson, AZ, USA, November 2006, Proceedings

Springer

Lecture Notes in Computer Science 4231

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

John F. Roddick V. Richard Benjamins
Samira Si-Saïd Cherfi Roger Chiang
Christophe Claramunt Ramez Elmasri
Fabio Grandi Hyoil Han Martin Hepp
Miltiadis Lytras Vojislav B. Mišić
Geert Poels Il-Yeol Song Juan Trujillo
Christelle Vangenot (Eds.)

Advances in Conceptual Modeling – Theory and Practice

ER 2006 Workshops BP-UML, CoMoGIS
COSS, ECDM, OIS, QoIS, SemWAT
Tucson, AZ, USA, November 6-9, 2006
Proceedings

Springer

Volume Editors

John F. Roddick E-mail: roddick@infoeng.flinders.edu.au
V. Richard Benjamins E-mail: rbenjamins@isoco.com
Samira Si-Saïd Cherfi E-mail: sisaid@cnam.fr
Roger Chiang E-mail: roger.chiang@uc.edu
Christophe Claramunt E-mail: claramunt@ecole-navale.fr
Ramez Elmasri E-mail: elmasri@cse.uta.es
Fabio Grandi E-mail: fgrandi@deis.unibo.it
Hyoil Han E-mail: hyoil.han@ischool.drexel.edu
Martin Hepp E-mail: martin.hepp@deri.org
Miltiadis Lytras E-mail: mdl@aueb.gr
Vojislav B. Mišić E-mail: vmisic@cs.umanitoba.ca
Geert Poels E-mail: Geert.Poels@UGent.be
Il-Yeol Song E-mail: songiy@drexel.edu
Juan Trujillo E-mail: jtrujillo@dlsi.ua.es
Christelle Vangenot E-mail: christelle.vangenot@epfl.ch

Library of Congress Control Number: 2006934617

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 3-540-47703-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-47703-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11908883 06/3142 5 4 3 2 1 0

Foreword to ER 2006 Workshops and Tutorials

Welcome to the workshops and tutorials associated with the 25th International Conference on Conceptual Modeling (ER 2006). As always, the aim of the workshops is to give researchers and participants a forum to discuss cutting-edge research in conceptual modeling, both in theory and, particularly this year, in practice.

The change in the nature of the ER workshops to be a balance between research theory and practice has been apparent for a number of years and shows the continual maturing of conceptual modeling over the past 25 years. Now in its silver anniversary year, the ER series continues to be the premier conference in conceptual modeling and the interest shown in the workshops is testament to this. In all, 39 papers were accepted from a total of 95 submitted, an overall acceptance rate of 41%.

The focus for this year's seven workshops, which were selected competitively following a call for workshop proposals, ranges from practical issues such as industrial standards, UML and the quality of information systems, through to workshops focused on managing change in information systems, geographic systems, service-oriented software systems and the Semantic Web. Four have been run previously at an ER conference, three were new this year.

- Best Practices of UML (BP-UML 2006)
- Conceptual Modeling for Geographic Information Systems (CoMoGIS 2006)
- Conceptual Modeling of Service-Oriented Software Systems (COSS 2006)
- Evolution and Change in Data Management (ECDM 2006)
- Ontologizing Industrial Standards (OIS 2006)
- Quality of Information Systems (QoIS 2006)
- Semantic Web Applications: Theory and Practice (SemWAT 2006)

This volume contains the proceedings from the seven workshops. Also included are the outlines for the three tutorials:

- Conceptual Modeling for Emerging Web Application Technologies - Dirk Draheim and Gerald Weber.
- State of the Art in Modeling and Deployment of Electronic Contracts - Kamalakar Karlapalem and P. Radha Krishna.
- Web Change Management and Delta Mining: Opportunities and Solutions - Sanjay Madria.

Although there was a lot to see, the scheduling of the workshops and the main conference were organized so as to maximize the opportunity for delegates to attend sessions of interest.

Setting up workshops such as these takes a lot of effort. I would like to thank the PC chairs and their Program Committees for their diligence in selecting the

papers in this volume. I would also like to thank the main ER 2006 conference committees, particularly the conference Co-chairs Sudha Ram and Mohan Tanniru and the conference Publicity Chair and Webmaster, Huimin Zhao, for their support in putting this programme together.

John F. Roddick
Flinders University
PO Box 2100, Adelaide
South Australia
roddick@infoeng.flinders.edu.au

ER 2006 Conference Organization

Honorary Conference Chair

Peter P. Chen (Louisiana University, USA)

Conference Co-chairs

Sudha Ram (University of Arizona0, USA, ram@eller.arizona.edu)
Mohan R. Tanniru (University of Arizona, USA, mtanniru@eller.arizona.edu)

Program Committee Co-chairs

Dave Embley (Brigham Young University, USA, embley@cs.byu.edu)
Antoni Olive (Universitat Politecnica de Catalunya, Spain, olive@lsi.upc.es)

Workshop and Tutorial Chair

John F. Roddick (Flinders University, Australia, roddick@infoeng.flinders.edu.au)

Panel Co-chairs

Uday Kulkarni (Arizona State University, USA, uday.kulkarni@asu.edu)
Keng Siau (University of Nebraska,Lincoln, USA, ksiau@unlnotes.unl.edu)

Industrial Program Co-chairs

Arnie Rosenthal (Mitre Corporation, arnie@mitre.org)
Len Seligman (Mitre Corporation, seligman@mitre.org)

Demos and Posters Co-chairs

Akhilesh Bajaj (University of Tulsa, USA, akhilesh-bajaj@utulsa.edu)
Ramesh Venkataraman (Indiana University, USA, venkat@indiana.edu)

Publicity Chair and Webmaster

Huimin Zhao (University of Wisconsin, Milwaukee, USA, hzhao@uwm.edu)

Local Arrangements and Registration

Anji Siegel (University of Arizona, USA, asiegel@arizona.edu)

Steering Committee Liaison

Bernhard Thalheim (Christian-Albrechts-Universiät zu Kiel, Germany, thalheim@is.informatik.uni-kiel.de)

ER 2006 Workshop Organization

ER 2006 Workshop and Tutorial Chair

John F. Roddick (Flinders University, Australia, roddick@infoeng.flinders.edu.au)

BP-UML 2006 - Second International Workshop on Best Practices of UML

BP-UML 2006 was organized within the framework of the following projects: METASIGN (TIN2004-00779) from the Spanish Ministry of Education and Science, DADASMECA (GV05/220) from the Valencia Ministry of Enterprise, University and Science (Spain), and DADS (PBC-05-012-2) from the Castilla-La Mancha Ministry of Science and Technology (Spain).

Program Chairs

Juan Trujillo (University of Alicante, Spain)
Il-Yeol Song (Drexel University, USA)

Program Committee

Doo-Hwan Bae (KAIST, South Korea)
Michael Blaha (OMT Associates Inc., USA)
Cristina Cachero (Universidad de Alicante, Spain)
Tharam Dillon (University of Technology Sydney, Australia)
Dirk Draheim (Freie Universität Berlin, Germany)
Gillian Dobbie (University of Auckland, New Zealand)
Jean-Marie Favre (Université Grenoble, France)
Eduardo Fernández (Universidad de Castilla-La Mancha, Spain)
Jaime Gómez (Universidad de Alicante, Spain)
Anneke Kleppe (Universiteit Twente, The Netherlands)
Ludwik Kuzniarz (Blekinge Tekniska Högskola, Sweden)
Jens Lechtenböorger (Universität Münster, Germany)
Tok Wang Ling (National University of Singapore, Singapore)
Pericles Loucopoulos (University of Manchester, UK)
Hui Ma (Massey University, New Zealand)
Andreas L. Opdahl (Universitetet i Bergen, Norway)
Jeffrey Parsons (Memorial University of Newfoundland, Canada)
Óscar Pastor (Universitat Politècnica de València, Spain)
Witold Pedrycz (University of Alberta, Canada)
Mario Piattini (Universidad de Castilla-La Mancha, Spain)

Ivan Porres (Åbo Akademi University, Finland)
Colette Rolland (Université Paris 1-Panthéon Sorbonne, France)
Matti Rossi (Helsingin kauppakorkeakoulu, Finland)
Manuel Serrano (Universidad de Castilla-La Mancha, Spain)
Bernhard Thalheim (Universität zu Kiel, Germany)
A Min Tjoa (Technische Universität Wien, Austria)
Ambrosio Toval (Universidad de Murcia, Spain)
Antonio Vallecillo (Universidad de Málaga, Spain)
Panos Vassiliadis (University of Ioannina, Greece)

Referees

F. Molina
J. Lasheras
Ki Jung Lee
S. Schmidt
A. Sidhu

CoMoGIS 2006 - Third International Workshop on Conceptual Modeling for Geographic Information Systems

Workshop Chairs

Christelle Vangenot (EPFL, Switzerland)
Christophe Claramunt (Naval Academy Research Institute, France)

Program Committee

Masatoshi Arikawa (University of Tokyo, Japan)
Natalia Andrienko (Fraunhofer Institute AIS, Germany)
Michela Bertolotto (University College, Dublin, Ireland)
Patrice Boursier (University of La Rochelle, France and Open University, Malaysia)
Elena Camossi (IMATI-CNR Genova, Italy)
James Carswell (Dublin Institute of Technology, Ireland)
Maria Luisa Damiani (University of Milan, Italy)
Thomas Devogele (Naval Academy Research Institute, France)
Max Egenhofer (University of Maine, USA)
Andrew Frank (Technical University of Vienna, Austria)
Bo Huang (University of Calgary, Canada)
Zhiyong Huang (National University of Singapore, Singapore)
Christian S. Jensen (Aalborg University, Denmark)
Ki-Joune Li (Pusan National University, South Korea)
Dieter Pfoser (CTI, Greece)
Martin Raubal (University of Münster, Germany)
Andrea Rodriguez (University of Concepcion, Chile)

Sylvie Servigne (INSA, France)
Kathleen Stewart Hornsby (University of Maine, USA)
George Taylor (University of Glamorgan, UK)
Nectaria Tryfona (Talent Information Systems, Greece)
Agnes Voisard, (Fraunhofer ISST and FU Berlin, Germany)
Nico van de Weghe (University of Gent, Belgium)
Nancy Wiegand (University of Wisconsin-Madison, USA)
Stephan Winter (University of Melbourne, Australia)
Ilya Zaslavsky (San Diego Supercomputer Center, USA)
Esteban Zimanyi (Free University of Brussels, Belgium)

CoSS 2006 - International Workshop on Conceptual Modeling of Service-Oriented Software Systems

Workshop Chairs

Roger Chiang, (University of Cincinnati, USA)
Vojislav B. Mišić, (University of Manitoba, Canada)

Advisory Committee

Wil van der Aalst, (Technische Universiteit Eindhoven, The Netherlands)
Akhil Kumar, (Penn State University, USA)
Michael Shaw, (University of Illinois at Urbana-Champaign, USA)
Keng Siau, (University of Nebraska at Lincoln, USA)
Carson Woo, (University of British Columbia, Canada)
Liang-Jie Zhang, (IBM, USA)
J. Leon Zhao, (University of Arizona, USA)

Program Committee

Fabio Casati, (HP Labs, USA)
Dickson K. W. Chiu, (Dickson Computer Systems, Hong Kong)
Cecil Eng Huang Chua, (Nanyang Technological University, Singapore)
Haluk Demirkan, (Arizona State University, USA)
Stephane Gagnon, (New Jersey Institute of Technology, USA)
Patrick Hung, (University of Ontario Institute of Technology, Canada)
Qusay H. Mahmoud, (University of Guelph, Canada)
Hye-young Helen Paik, (University of New South Wales, Australia)
Venkataramanan Shankararaman, (Singapore Management University, Singapore)
Benjamin B. M. Shao, (Arizona State University, USA)
Vladimir Tosic, (Lakehead University, Canada)
Harry J. Wang, (University of Delaware, USA)
Lina Zhou, (University of Maryland at Baltimore County, USA)

ECDM 2006 - Fourth International Workshop on Evolution and Change in Data Management

Workshop Chair

Fabio Grandi (University of Bologna, Italy)

Program Committee

Alessandro Artale (Free University of Bolzano-Bozen, Italy)
Sourav Bhowmick (Nanyang Technical University, Singapore)
Michael Böhlen (Free University of Bolzano-Bozen, Italy)
Carlo Combi (University of Verona, Italy)
Curtis Dyreson (Washington State University, USA)
Shashi Gadia (Iowa State University, USA)
Kathleen Hornsby (University of Maine, USA)
Michel Klein (Vrije Universiteit Amsterdam, The Netherlands)
Richard McClatchey (University of the West of England, UK)
Federica Mandreoli (University of Modena and Reggio Emilia, Italy)
Torben Bach Pedersen (Aalborg University, Denmark)
Erik Proper (University of Nijmegen, The Netherlands)
John Roddick (Flinders University, South Australia)
Nandlal Sarda (IIT Bombay, India)
Myra Spiliopoulou (Otto-von-Guericke-Universität Magdeburg, Germany)
Carlo Zaniolo (UCLA, USA)

Additional Referees

M. Golfarelli
P.S. Jørgensen

OIS 2006 - First International Workshop on Ontologizing Industrial Standards

Workshop Chairs

Martin Hepp (University of Innsbruck, Austria)
Miltiadis Lytras (Athens University of Economics and Business, Greece)
V. Richard Benjamins (iSOCO, Spain)

Program Committee

Chris Bizer (Free University of Berlin, Germany)
Chris Bussler (Cisco Systems, Inc., San Francisco, USA)
Jorge Cardoso (University of Madeira)
Oscar Corcho (University of Manchester, UK)
Jos de Bruijn (DERI Innsbruck, Austria)

Doug Foxvog (DERI Galway, Ireland)
Fausto Giunchiglia (University of Trento, Italy)
Karthik Gomadam (LSDIS Lab, University of Georgia, USA)
Michel Klein (Free University of Amsterdam, The Netherlands)
Paavo Kotinurmi (Helsinki University of Technology, Finland)
York Sure (University of Karlsruhe, Germany)

QoIS 2006 - Second International Workshop on Quality of Information Systems

Workshop Chairs

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

Steering Committee

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

Program Committee

Jacky Akoka (CEDRIC - CNAM and INT, France)
Laure Berti (IRISA, France)
Mokrane Bouzeghoub (PRISM, University of Versailles, France)
Andrew Burton-Jones (University of British Columbia, Canada)
Tiziana Catarci (Università di Roma "La Sapienza," Italy)
Isabelle Comyn-Wattiau (CNAM and ESSEC, France)
Corinne Cauvet (University of Aix-Marseille 3, France)
Marcela Genero (Universidad de Castilla-La Mancha, Spain)
Paul Johannesson (Stockholm University, Sweden)
Jacques Le Maitre (University of Sud Toulon-Var, France)
Jim Nelson (Southern Illinois University, USA)
Jeffrey Parsons (Memorial University of Newfoundland, Canada)
Óscar Pastor (Valencia University of Technology, Spain)
Houari Sahraoui (Université de Montréal, Canada)
Farida Semmak (Université Paris XII , IUT Sénart Fontainebleau)
Keng Siau (University of Nebraska, USA)
Guttorm Sindre (Norwegian University of Science and Technology, Norway)
Monique Snoeck (Katholieke Universiteit Leuven, Belgium)

Il-Yeol Song (Drexel University, USA)
David Tegarden (Virginia Polytechnic Institute, USA)
Bernhard Thalheim (University of Kiel, Germany)
Dimitri Theodoratos (NJ Institute of Technology, USA)
Juan Trujillo (University of Alicante, Spain)

SemWAT 2006 - First International Workshop on Semantic Web Applications: Theory and Practice

Workshop Chairs

Hyoil Han (Drexel University, USA)
Ramez Elmasri (University of Texas at Arlington, USA)

Program Committee

Palakorn Achananuparp (Drexel University, USA)
Yuan An (University of Toronto, Canada)
Paul Buitelaar (DFKI GmbH, Germany)
Stefania Costache (University of Hannover, Germany)
Vadim Ermolayev (Zaporozhye National University, Ukraine)
Fabien Gandon (INRIA, France)
Raul Garcia-Castro (Universidad Politecnica de Madrid, Spain)
Peter Haase (University of Karlsruhe, Germany)
Kenji Hatano (Doshisha University, Japan)
Stijn Heymans (Vrije Universiteit Brussel, Belgium)
Istvan Jonyer (Oklahoma State University, USA)
Esther Kaufmann (University of Zurich, Switzerland)
Christoph Kiefer (University of Zurich, Switzerland)
Beomjin Kim (Indiana University - Purdue University, USA)
SeungJin Lim (Utah State University, USA)
Jun Miyazaki (Nara Advanced Institute of Science and Technology, Japan)
JungHwan Oh (University of Texas at Arlington, USA)
Byung-Kwon Park (Dogna University, Korea)
Xiaojun Qi (Utah State University, USA)
Lawrence Reeve (Drexel University, USA)
York Sure (University of Karlsruhe, Germany)
Davy Van Nieuwenborgh (Vrije Universiteit Brussel, Belgium)
Mikalai Yatskevich (University of Trento, Italy)

Table of Contents

CoMoGIS 2006 - 3rd International Workshop on Conceptual Modeling for Geographic Information Systems

Keynote

Spatial and Spatio-temporal Data Representation

Optimizing Representation and Access to Spatial Data

Spatio-temporal Data on the Web

CoSS 2006 - International Workshop on Conceptual Modeling of Service-Oriented Software Systems

ECDM 2006 - 4th International Workshop on Evolution and Change in Data Management

Keynote

Accepted Papers

OIS 2006 - 1st International Workshop on Ontologizing Industrial Standards

Accepted Papers

QoIS 2006 - 2nd International Workshop on Quality of Information Systems

Introduction to QoIS06

Information System Quality

Data Quality

SemWAT 2006 - 1st International Workshop on Semantic Web Applications: Theory and Practice

Semantic Web Applications (I)

Semantic Web Applications (II)

Capturing Security Requirements in Business Processes Through a UML 2.0 Activity Diagrams Profile

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

Abstract. Security has become a crucial aspect for the performance of present organizations since the protected object is the mission of them. Therefore, the management approach oriented to business processes has been a good answer for the current scenarios, changing and complex, where organizations develop their task. Both subjects form a basic requirement to reach not only the mission but also the organizational objectives in a strongly connected global economy. In this work, we will show a microprocess through which it is possible to specify and refine security requirements at a high level of abstraction, in a way that they can be incorporated into the development of a software system. In addition, an extension of UML 2.0 activity diagrams will be presented through which it is possible to identify such requirements.

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 [22].

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 [3] mainly due to the fact that the expert in the business process domain is not an expert in security [10]. 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 vulnerabilities [19], which clearly justify the need of increasing the effort in the pre-development phases, where fixing the bugs is cheaper [16].

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 [16], 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 [2], 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 [6].

In our proposal, we consider the definition of a microprocess that complements the requirements capture defined in the Unified Software Development Process [11] and we have defined a UML 2.0 activity diagrams profile to capture security requirements.

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 profiles. In Section 4, we will propose a microprocess for the security requirements specification and a UML 2.0 profile that allows the business analyst to carry out this task. Finally, in Section 5, we will present an example and in Section 6 our conclusion will be drawn.

J.F. Roddick et al. (Eds.): ER Workshops 2006, LNCS 4231, pp. 32–42, 2006.

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 [7]. And in the second place, security has been integrated into an application in an ad-hoc manner, often during the actual implementation process [3], during the system administration phase [15] or it has been considered like outsourcing [18].

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 [16]. Consequently, we believe that business analysts can integrate their view on business security into the business process perspective. In addition, 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 [8].

In the review of related works, we have had the possibility to check that not only in those works directly referring to security regarding business processes [3, 10, 17, 23, 24, 27] but also in those that have to do with security and information systems [1, 2, 4, 12, 15, 19, 25, 28], security specifications made by the business analyst are absent. Moreover and in spite of the fact that in some of these works, UML is used for security specifications, none of them use the activity diagrams available in UML 2.0.

3 UML 2.0 Activity Diagrams and UML 2.0 Profiles

Activity diagrams are the UML 2.0 elements used to represent business processes and workflows [13]. 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 [5]. 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 [20]. 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 metaclasses from existing metamodels to be extended to adapt them for different purposes. The profiles mechanism is consistent with the Meta Object Facility (MOF) [20]. 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. invariants). They can be expressed in natural language, programming language or through Object Constraint Language (OCL). Tagged values are additional metaattributes 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 [14], Data Warehouse and its relation to business process dynamic structures [26] or they add semantics to the activities considering organizational aspects that allow us to express resource restrictions during the execution of an activity [13].

4 Microprocess and UML 2.0 Profile for Security Requirements

Requirements specification is a stage that has been taken into account in the most important software construction models such as the traditional waterfall model, the prototype construction, the incremental model, and the spiral model, among others. [21]. In these models, it is considered a stage in which we should obtain the system requirements either from the client or from the interested people in order to start the software construction from that point.

Our proposal studies a microprocess that complements the specification of the system context defined in the Unified Process [11] paying special attention to security requirements capture. To do so, a UML 2.0 activity diagrams profile is proposed.

4.1 SeReS4BP Microprocess

We have considered the use of the Unified Software Development Process stated by Jacobson, Booch y Rumbaugh (2000) since it is a quite consolidated and successful software construction method [9]. This process is composed by a set of activities that allow us to transform a user's requirements into a software system.

In the Unified Process, requirements capture is mainly done during the inception and elaboration stages. The objective of this task is to make a good enough description of the system's requirements (conditions and capabilities that must be fulfilled by the system) to determine what the system must or must not do. To do so, it is considered the performance of an enumeration of the requirements of the candidates, the understanding of the system context, and the capture of both functional and non functional requirements.

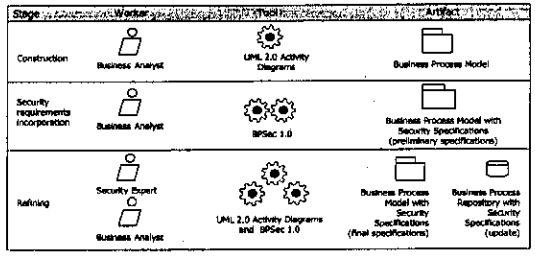


Fig. 1. Complete view of the SeReS4BP microprocess

The security requirements specified in the business process can be perfectly linked to the Unified Process. To do so, we propose to complement the task "to understand the system context" with specifications of the domain built by the business analyst. Our proposal is a microprocess that considers the necessary activities that allow us to specify requirements (particularly, security requirements) taking into account the business analyst's perspective. This microprocess is called SeReS4BP (Security Requirement Specification for Business Process). Figure 1 shows us a view of the main activities performed in this microprocess and Table 1 shows us a details description.

Table 1. SeReS4BP activities

Stages: *Construction*: whose objective is the business process model construction. To reach this objective, the UML 2.0 activity diagram must be used. *Security requirements incorporation*: this stage consists of incorporating security requirements, from the business analyst viewpoint, into the business process model that was specified in the previous stage. *Refining*: This stage corresponds to the review and complementing of the security specifications that have been incorporated into the business process. At this stage, the business analyst and the security expert work together. The specifications that will be finally incorporated into the business process will be agreed at this stage.
Workers: *Business Analyst*: he/she will be 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 considering a high level of abstraction. *Security Expert*: he/she will be the responsible for refining the security specifications indicated by the business analyst. Such refining considers the verification of the specifications validity and complementation.
Tools: *UML 2.0 Activity Diagrams* for the business process specification. *BPSec 1.0* for security requirements specifications
Artifacts: *Business process model*: This artifact is the result of the construction stage. It contains the business process specifications and it can be built using UML. It does not contain security specifications. *Business Process Model with Security Specifications*. This artifact is the result of the stages of incorporation of security requirements and refining. The first stage contains security preliminary specifications that, after refining, will be converted into definitive security specifications. *Business Process Repository* that contains security specifications. This repository is composed of a set of business processes that have security requirements already incorporated. This repository must be updated with the business process resulting from the refining stage.

4.2 BPSec Version 1.0 for Modeling Security Requirements in Business Processes

In this section, we will present the main aspects of our profile for representing security requirement in business process. Our proposal allows business analysts to specify security requirements in the business process by using activity diagrams. We have considered the security requirements identified in the taxonomy proposed in [8]. Later on, these requirements will be transformed, by the security experts, into technical specifications including all necessary details for their implementation.

Our Profile will be called BPSec (Secure Business Process) and will be represent as a UML Package. This profile will incorporate new data types, stereotypes, tagged value and constrains. In Figure 2, a high level view is provided.

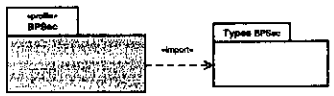


Fig. 2. High level view of BPSec Profile

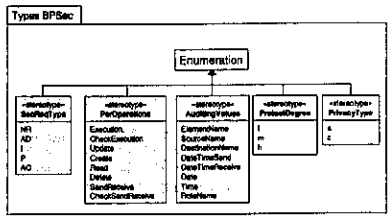


Fig. 3. Value associated to new data type

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.

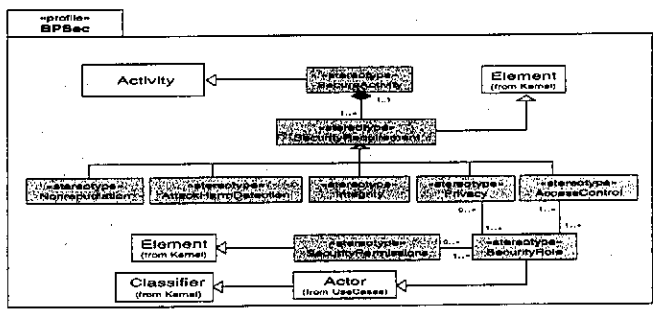


Fig. 4. New Stereotypes

In Figure 3, we can observe the values associated to each one of the necessary type. All the new type must be considered when the business analysts to specify security requirements in business process. We have defined a package that includes all stereotypes that will be necessary in our profile. In Figure 4 we show the stereotypes (in dark) for Secure Activity specifications.

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, CheckSendReceiv
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

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 can be added to activity diagram elements (see Table 3). 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 3). 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 5).

Table 3. 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 Store Node	Object Flow
Nonrepudiation						✓
AttackHarmDetection	✓	✓	✓	✓	✓	✓
Integrity					✓	✓
Privacy		✓				
AccessControl	✓	✓	✓			
Security Role	✓	✓	✓			
SecurityPermissions				✓	✓	✓

In Table 4 we show the stereotypes for secure activity specifications extensively. Each stereotype specification contains: name, base class, description, notation (optional), constrains and tagged values (optional).

Table 4. Stereotypes specifications for security requirement

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	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 ="Create" 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	SecurityRole
Base Class	Actor (from UseCases)
Description	It contains a role specifications. This roles must be obtained from access control and/or privacy specifications

Table 4. (*continued*)

Constrains	The role in the security role stereotype can be derived from: Activity, ActivityPartition and/or InterruptibleActivityRegion 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
Name	SecurityRequirement — Notation: 
Base Class	Element
Description	Abstract class containing security requirements specifications. Each security requirement type must be indicated in some of its subclasses
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
Name	Nonrepudiation — Notation: NR
Base Class	SecurityRequirement
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 3.
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"
Name	AttackHarmDetection — Notation: AD
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
Constrains	It can be only specified in the diagram elements indicated in Table 3.
Tagged Values	AvAD: AuditingValues context AttackHarmDetection Inv: self.AvAD="ElementName" or self.AvAD="Date" or self.AvAD="Time"
Name	Integrity — Notation: I_x
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.
Constrains	It can be only specified in the diagram elements indicated in Table 3. 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: P_x
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.
Constrains	It can be only specified in the diagram elements indicated in Table 3. 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: AC
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.
Constrains	It can be only specified in the diagram elements indicated in Table 3. 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 5) 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).

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" with the aim of avoiding the denial of the "Admission Request" reception. «AccessControl» has been defined over the Interruptible Activity Region.

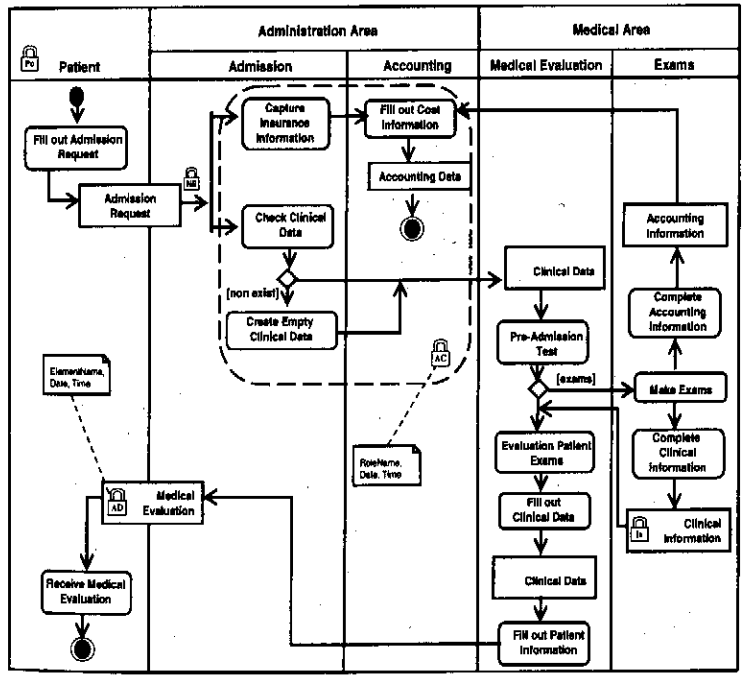


Fig. 2. Admission of Patients in a Medical Institution

Table 5. «SecurityRole» and «SecurityPermission» specifications

Role	Permissions → Objects		Permissions → 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

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).

6 Conclusions and Ongoing Work

The advantage of early representing requirements, in this case, security requirements, favours the quality of the business process since it provides it with more expressivity and improves the software quality since it considers characteristics that, in other way, would have to be incorporated late. So, we can save on maintenance costs as well as on the total cost of the project. We have defined a microprocess that complements the requirements stage defined in the Unified Process and we have used UML 2.0 to represent security requirements.

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) and MISTICO, both supported by FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", and COMPETISOFT granted by CYTED.

References

1. Abie, H., Aredo, D. B., Kristoffersen, T., Mazaher, S. and Raguin, T.; *Integrating a Security Requirement Language with UML*, 7th International Conference, The UML: Modelling Languages and Applications. Vol. 3273. Lisbon, Portugal. (2004). pp.350-364.
2. 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.
3. Backes, M., Pfitzmann, B. and Waider, M.; *Security in Business Process Engineering*, International Conference on Business Process Management (BPM). Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). pp.168-183.

4. Basin, D., Doser, J. and Lodderstedt, T.; *Model driven security for process-oriented systems*, SACMAT 2003, 8th ACM Symposium on Access Control Models and Technologies. Villa Gallia, Como, Italy. (2003).
5. Bock, C.; *UML 2 Activity and Action Models*, Journal of Object Technology. Vol. 2 (4), July-August. (2003). pp.43-53.
6. Eriksson, H.-E. and Penker, M., *Business Modeling with UML*, OMG Press. (2001).
7. Firesmith, D.; *Engineering Security Requirements*, Journal of Object Technology. Vol. 2 (1), January-February. (2003). pp.53-68.
8. Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.
9. Fuggetta, A.; *Software process: a roadmap*, ICSE 2000, 22nd International Conference on Software Engineering, Future of Software Engineering. Limerick Ireland. (2000). pp.25-34.
10. Herrmann, G. and Pernul, G.; *Viewing Business Process Security from Different Perspectives*, 11th International Bled Electronic Commerce Conference. Slovenia. (1998). pp.89-103.
11. Jacobson, I., Booch, G. and Rumbaugh, J., *El proceso unificado de desarrollo de software*, . (2000). 464 p.
12. Jürjens, J., *Secure Systems Development with UML*, Springer Verlag, (2004). 309 p.
13. 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.
14. 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).
15. Lodderstedt, T., Basin, D. and Doser, J.; *SecureUML: A UML-Based Modeling Language for Model-Driven Security*, The Unified Modeling Language, 5th International Conference. Vol. 2460. Dresden, Germany. (2002). pp.426-441.
16. 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.
17. 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.
18. 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. Leganés, Madrid. España. (2004). pp.383-392.
19. 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.
20. 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).
21. Pressman, R. S., *Software Engineering: A Practitioner's Approach*, 6th Edition, (2006). 880 p.
22. Quirchmayr, G.; *Survivability and Business Continuity Management*, ACSW Frontiers 2004 Workshops. Dunedin, New Zealand. (2004). pp.3-6.
23. 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.

24. Röhm, A. W., Pernul, G. and Herrmann, G.; *Modelling Secure and Fair Electronic Commerce*, 14th. Annual Computer Security Applications Conference. Scottsdale, Arizona. (1998). pp.155-164.
25. Siponen, M. T.; *Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods*, Information and Organization. Vol. 15. (2005). pp.339-375.
26. 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).
27. 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. Bristol, U.K. (2003). pp.381-395.
28. Zulkernine, M. and Ahamed, S. I., *Software Security Engineering: Toward Unifying Software Engineering and Security Engineering*, in: Idea Group (Ed.), Enterprise Information Systems Assurance and Systems Security: Managerial and Technical Issues, M. Warkentin & R. Vaughn, 2006, p.215-232.

Finite State History Modeling and Its Precise UML-Based Semantics

Dirk Draheim[1], Gerald Weber[2], and Christof Lutteroth[2]

[1] University of Mannheim, Institute of Computer Science, A5-6
68131 Mannheim, Germany
draheim@acm.org
[2] The University of Auckland, Department of Computer Science, 38 Princes Street
Auckland 1020, New Zealand
{lutteroth, g.weber}@cs.auckland.ac.nz

Abstract. This paper discusses the notion of a state history diagram. The concept is directly motivated by a new analysis technique, form-oriented analysis, which is tailored to an important class of interactive systems including web applications. A combined UML metamodeling and framework approach is used to give precise semantics to state history diagrams and the artifacts of form-oriented analysis.

1 Introduction

In this paper we introduce a general notion of finite state modeling that has a tight integration with other modeling views, especially with class diagrams. A state transition diagram in this new notion is called a state history diagram, SHD for short. SHDs can be used in many circumstances in analysis as well as design. They are especially favorable in cases where we model a system by a finite state machine in order to capture a specific aspect, while the system as a whole is modeled by a class diagram as well. Such models are very widespread. Submit/response style interaction is a very important instance. Other examples include the state of processes in operating systems or the life cycle of components in application servers.

We give the operational semantics for general SHDs in order to clarify the general character of the introduced concept. The approach chosen here achieves a sound basis for all the special constructs introduced in form-oriented analysis in a rather short and lightweight way. This is achieved through maximal reuse, mainly because we were able to fully reuse the semantics of class diagrams for our new artifacts. Submit/response style interaction yields an appropriate abstraction from an important class of interactive systems ranging from mainframe/terminal systems to web applications. Form-oriented analysis [3,4] addresses the analysis phase of submit/response style applications. Form-oriented analysis has a special type of state history diagram called formchart. Formcharts are bipartite state transition diagrams with an OCL [9] extension DCL (dialogue constraint language).

We introduce state history diagrams in Sect. 2. We give precise semantics to state history diagrams in Sect. 3 by combining metamodeling techniques [2]

J.F. Roddick et al. (Eds.): ER Workshops 2006, LNCS 4231, pp. 43–52, 2006.