Lecture Notes in Computer Science

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

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

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

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

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

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

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

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

ISSN 0302-9743

ISBN 978-3-642-04946-0

9 783642 049460

Lecture Notes in Computer Science
LNCS LNAI LNBI

springer.com

Heuser • Pernul (Eds.)

LNCS 5833

Advances in Conceptual Modeling – Challenging Perspectives

ER Workshops 2009

Carlos Alberto Heuser
Günther Pernul (Eds.)

LNCS 5833

Advances in Conceptual Modeling – Challenging Perspectives

ER 2009 Workshops CoMoL, ETheCoM, FP-UML, MOST-ONISW, QoIS, RIGiM, SeCoGIS Gramado, Brazil, November 2009, Proceedings

Springer

Lecture Notes in Computer Science 5833

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

Carlos Alberto Heuser Günther Pernul (Eds.)

Advances in Conceptual Modeling - Challenging Perspectives

ER 2009 Workshops CoMoL, ETheCoM, FP-UML, MOST-ONISW, QoIS, RIGiM, SeCoGIS
Gramado, Brazil, November 9-12, 2009
Proceedings

Springer

Volume Editors

Carlos Alberto Heuser
Federal University of Rio Grande do Sul
Instituto de Informática
Porto Alegre, Brazil
E-mail: heuser@inf.ufrgs.br

Günther Pernul
University of Regensburg
Department of Management Information Systems
93053 Regensburg, Germany
E-mail: guenther.pernul@wiwi.uni-regensburg.de

Library of Congress Control Number: 2009935903

CR Subject Classification (1998): D.2, D.3, D.2.2, D.3.2, F.3.3, H.2.8, D.1.2

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

ISSN 0302-9743
ISBN-10 3-642-04946-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-04946-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12775286 06/3180 5 4 3 2 1 0

Preface

This book contains the papers accepted for presentation and publication in the workshop proceedings of the 28th edition of the International Conference on Conceptual Modeling (ER Conference), held during November 9–12, 2009, in Gramado, Brazil. The ER workshops complement the main ER conference and are intended to serve as an intensive collaborative forum for exchanging late-breaking ideas and theories in an evolutionary stage and related to conceptual modeling.

For the 2009 edition the workshop committee received 14 excellent proposals from which the following were selected:

- ACM-L: Active Conceptual Modeling of Learning
- CoMoL: Conceptual Modeling in the Large
- ETheCoM: Evolving Theories of Conceptual Modeling
- FP-UML: Workshop on Foundations and Practices of UML
- MOST-ONISW: Joint International Workshop on Metamodels, Ontologies, Semantic Technologies, and Information Systems for the Semantic Web
- QoIS: Quality of Information Systems
- RIGiM: Requirements, Intentions and Goals in Conceptual Modeling
- SeCoGIS: Semantic and Conceptual Issues in Geographic Information Systems

These workshops attracted 100 submissions from which the workshop program committees selected 33 papers, maintaining a highly competitive acceptance rate of 30%.

The workshop co-chairs are highly indebted to the workshop organizers and program committees for their work.

July 2009

Carlos A. Heuser
Günther Pernul

Organization

ER 2009 Workshops Chairs

Carlos A. Heuser	Universidade Federal do Rio Grande do Sul, Brazil
Günther Pernul	Universität Regensburg, Germany

CoMoL 2009 Program Chairs

Stefan Jablonski	University Bayreuth, Germany
Roland Kaschek	Kazakhstan Institute of Management, Economics and Strategic Research, Kazakhstan
Bernhard Thalheim	Christian-Albrechts-University Kiel, Germany

CoMoL 2009 Program Committee

Sabah S. Al-Fedaghi	Kuwait University, Kuwait
Karen C. Davis	University of Cincinnati, USA
Valeria De Antonellis	Brescia University, Italy
Lois Delcambre	Portland State University, USA
Ulrich Frank	University Duisburg-Essen, Germany
Nicola Guarino	LOA-CNR, Italy
Klaus P. Jantke	Fraunhofer IDMT, Germany
John Krogstie	Norwegian University of Science and Technology, Norway
Sebastian Link	Victoria University of Wellington, New Zealand
Heinrich C. Mayr	Alpen-Adria University Klagenfurt, Austria
Andreas Oberweis	University Karlsruhe, Germany
Antoni Olive	UPC Barcelona Tech, Spain
Andreas L. Opdahl	University of Bergen, Norway
Erich Ortner	Technical University of Darmstadt, Germany
Fabian Pascal	Database Debunkings, USA
Oscar Pastor	DSIC - Universidad Politécnica de Valencia, Spain
Klaus Pohl	University Duisburg-Essen, Germany
Klaus-Dieter Schewe	Information Science Research Centre, New Zealand
Michael Schrefl	Johannes Kepler University Linz, Austria
Markus Stumptner	University of South Australia, Australia
Yuzuru Tanaka	Hokkaido University, Japan
Susan Urban	Texas Tech University, USA
Mathias Weske	HPI University Potsdam, Germany
Roel Wieringa	University of Twente, The Netherlands

CoMoL 2009 External Reviewers

Tayyeb Amin
Devis Bianchini
Bernd Neumayr

EThecoM 2009 Program Chairs

Markus Kirchberg	Institute for Infocomm Research, A*STAR, Singapore
Klaus-Dieter Schewe	Information Science Research Centre, New Zealand

EThecoM 2009 Program Committee

Sabah S. Al-Fedaghi, Kuwait	Sebastian Link, New Zealand
Shawn Bowers, USA	Chengfei Liu, Australia
Stefan Brass, Germany	Hui Ma, New Zealand
Andrea Calì, UK	Wilfred Ng, Hong Kong
Gill Dobbie, New Zealand	Jaroslav Pokorny, Czech Republic
David W. Embley, USA	Letizia Tanca, Italy
Flavio A. Ferrarotti, Chile	James F. Terwilliger, USA
Aditya K. Ghose, Australia	Bernhard Thalheim, Germany
Guido Governatori, Australia	Alex Thomo, Canada
Sven Hartmann, Germany	Thu Trinh, Germany
Roland Hausser, Germany	Millist Vincent, Australia
Edward Hermann Haeusler, Brazil	Junhu Wang, Australia
Stephen Hegner, Sweden	Qing Wang, New Zealand
Henning Koehler, Australia	Jeffrey Xu Yu, Hong Kong
Leandro Krug Wives, Brazil	

EThecoM 2009 External Reviewers

Henrik Björklund
Fernando Bordignon
Thomas Packer

FP-UML 2009 Program Chairs

Juan Trujillo	University of Alicante, Spain
Dae-Kyoo Kim	Oakland University, USA

FP-UML 2009 Program Committee

Doo-Hwan Bae	KAIST, South Korea
Michael Blaha	OMT Associates Inc., USA
Cristina Cachero	Universidad de Alicante, Spain
Brian Dobing	University of Lethbridge, Canada
Joerg Evermann	Victoria University Wellington, New Zealand
Eduardo Fernández	Universidad de Castilla-La Mancha, Spain
Robert France	Colorado State University, USA
Irene Garrigos	Fernandez University of Alicante, Spain
Jens Lechtenböorger	Universität Münster, Germany
Pericles Loucopoulos	University of Manchester, UK
Hui Ma Massey	University, New Zealand
Oscar Pastor	Universidad Politècnica de València, Spain
Jose Norberto Mazon Lopez	University of Alicante, Spain
Heinrich C. Mayr	Universität Klagenfurt, Austria
Sooyong Park	Sogang University, Korea
Jeff Parsons	Memorial University of Newfoundland, Canada
Colette Rolland	Université Paris 1-Panthéon Sorbonne, France
Matti Rossi	Helsingin kauppakorkeakoulu, Finland
Manuel Serrano	Universidad de Castilla-La Mancha, Spain
Keng Siau	University of Nebraska-Lincoln, USA
Il-Yeol Song	Drexel University, USA
Ling Tok Wang	National University of Singapore, Singapore
Ambrosio Toval	Universidad de Murcia, Spain
Panos Vassiliadis	University of Ioannina, Greece

FP-UML 2009 External Reviewers

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

MOST-ONISW 2009 Program Chairs

Martin Doerr	Foundation for Research and Technology, Greece
Fred Freitas	Federal University of Pernambuco, Brazil
Giancarlo Guizzardi	Federal University of Espírito Santo, Brazil
Hyoil Han	Drexel University, USA

MOST-ONISW 2009 Program Committee

Mara Abel	Federal University of Rio Grande do Sul, Brazil
Jinli Cao	La Trobe University, Australia
Oscar Corcho	Universidad Politécnica de Madrid, Spain
Stefan Conrad	Heinrich-Heine-Universität Düsseldorf, Germany

Table of Contents

FP-UML 2009 – Fifth International Workshop on Foundations and Practices of UML

Dependability and Agent Modeling

Semantics Representation and Tools

MOST-ONISW 2009 – The Joint International Workshop on Metamodels, Ontologies, Semantic Technologies, and Information Systems for the Semantic Web

QoIS 2009 – The Fourth International Workshop on Quality of Information Systems

Assessment of Data Quality Factors

Tools for Information System Quality Assessment

RIGiM 2009 – Third International Workshop on Requirements, Intentions and Goals in Conceptual Modeling

Modelling

Elicitation Issues

SECOGIS 2009 – Third International Workshop on Semantic and Conceptual Issues in Geographic Information Systems

Foundational Aspects

Semantical Aspects

Applying a UML Extension to Build Use Cases Diagrams in a Secure Mobile Grid Application

David G. Rosado[1], Eduardo Fernández-Medina[1], and Javier López[2]

[1] UCLM. Alarcos Research Group-Information Systems and Technologies Institute. Information Systems and Technologies Department, ESI, 13071 Ciudad Real, Spain
{David.GRosado, Eduardo.FdezMedina, Mario.Piattini}@uclm.es
[2] University of Málaga, Computer Science Department, Málaga, Spain
jlm@lcc.uma.es

Abstract. Systems based on Grid computing have not traditionally been developed through suitable methodologies and have not taken into account security requirements throughout their development, offering technical security solutions only during the implementation stages. We are creating a development methodology for the construction of information systems based on Grid Computing, which is highly dependent on mobile devices, in which security plays a highly important role. One of the activities in this methodology is the requirements analysis which is use-case driven. In this paper, we build use case diagrams for a real mobile Grid application by using a UML-extension, called GridUCSec-Profile, through which it is possible to represent specific mobile Grid features and security aspects for use case diagrams, thus obtaining diagrams for secure mobile Grid environments.

Keywords: UML extension, Security, Use Cases, secure mobile Grid, secure development.

1 Introduction

With regard to the overall lack of software security in industry, many efforts are currently being made to integrate security into software and software development [1-5]. Systems based on Grid Computing are a type of systems that have clear differentiating features of which security is an extremely important aspect. Grids are centred on sharing resources between dynamic collections of individuals, institutions and resources in a flexible, secure and coordinated manner [6]. Grid environments have special features that make them different from other systems and which must be considered throughout the entire development lifecycle.

The lack of adequate development methods for this kind of systems has encouraged us to build a methodology with which to develop them [7, 8], offering a detailed guide to their analysis, design and implementation. The analysis activity of this methodology is centred on use cases (hereafter UCs) in which we define the behaviour, actions and interactions with those implied in the system (actors), thus obtaining a first approach towards the needs and requirements (functional and non-functional) of the system to be constructed.

C.A. Heuser and G. Pernul (Eds.): ER 2009 Workshops, LNCS 5833, pp. 126–136, 2009.

UML use cases [9] have become a widely used technique for the elicitation of functional requirements [10] when designing software systems. One of the main advantages of UCs is that they are easy to understand with only a limited introduction to their notation, and are therefore very well-suited to the communication and discussion of requirements with system stakeholders. Misuse cases, i.e. negative scenarios or UCs with a hostile intent, have recently been proposed as a new avenue through which to elicit non-functional requirements, particularly security requirements [11-15]. UCs have proved helpful in the elicitation of, communication about, and documentation of functional requirements. The integral development of use and misuse cases provides a systematic way in which to elicit both functional and non-functional requirements [13].

Security requirements exist because certain people and the negative agents that they create (such as computer viruses) pose real threats to systems. Security differs from all other specification areas in that someone is deliberately threatening to break the system. Employing use and misuse cases to model and analyse scenarios in systems under design can improve security by helping to mitigate threats [13].

In the analysis activity of the methodology we use security UCs and misuse cases together with UCs as essential elements of the requirements analysis. These elements must be defined for the context of mobile Grid, and we have therefore extended UML in order to define new UCs, security UCs and misuse cases for mobile Grid systems as a single package (called GridUCSec) of UCs for the identification and elicitation of both functional and non-functional requirements for mobile Grid environments.

A preliminary publication of the methodology has been presented in [8] in which we describe our general approach. [7] provides an informal presentation of the first steps of our methodology which consists of analyzing the security requirements of mobile grid systems directed by misuse cases and security UCs, and which is applied in an actual case study in [16] from which we obtain the security requirements for a specific application by following the steps described in our methodology. We have then gone on to elicit some common requirements of these kinds of systems, and these have been specified to be reused through a UML extension of UCs [17-19]. This paper shows how to apply the UML extension, called GridUCSec-profile, to a real mobile Grid system in order to build UC diagrams, with the help of the reusable UCs available in the repository, using the stereotypes and relationships defined in this profile. One task of the analysis activity of our methodology builds UC diagrams. In this paper we explain how this is achieved.

The remainder of the paper is organized as follows: In section 2, we present the UML extension for secure mobile Grid UCs. In section 3, we apply this UML extension to build UCs diagrams in a mobile Grid application. Finally, we propose our conclusions and future work.

2 UML Extension for Secure Mobile Grid Use Cases

We use the Unified Modeling Language (UML) as the foundation of our work for several reasons: UML is the de-facto standard for object-oriented modelling. Many modelling tools support UML and a great number of developers are familiar with the language. Hence, our work enables these users to develop access control policies

Table 1. Detailed description of Stereotypes for the GridUCSec package

«GridUC»		**Notation**
Description	Specifies requirements of the Grid system and represent the common behaviour and relationships for this kind of systems. It specializes the UseCase within the Grid context defining the behaviour and functions for the Grid system.	<<GridUC>>
Tagged Values	GridRequirement, ProtectionLevel, SecurityDependence, InvolvedAsset	
«SecurityUC»		**Notation**
Description	Specifies security requirements of the system, describing security tasks that the users will be able to perform with the system.	<<SecurityUC>>
Tagged Values	SecurityRequirement, InvolvedAsset, SecurityDegree, SecurityDomain	
«GridSecurityUC»		**Notation**
Description	This represents specific security features of Grid systems. It adds specific special security features which are covered by this stereotype, and specializes to common security UCs of other applications.	<<GridSecurityUC>>
Tagged Values	InvolvedAsset, SecurityRequirement, SecurityDegree, SecurityDependence, SecurityDomain	
«MisuseCase»		**Notation**
Description	A sequence of actions, including variants, that a system or other entity can perform, interacting with misusers of the entity and causing harm to certain stakeholders if the sequence is allowed to be completed [12, 21].	<<Misuse>>
Tagged Values	InvolvedAsset, ImpactLevel, RiskLevel, ThreatLikelihood, KindAttack	
«MobileUC»		**Notation**
Description	This represents mobile features of the mobile devices within Grid systems. It defines the mobile behaviour of the system and specializes UseCase within the Grid context and mobile computing defining the behaviour and functions for the mobile Grid system.	<<MobileUC>>
Tagged Values	MobileRequirement, ProtectionLevel, SecurityDependence, InvolvedAsset, NetworkProtocol	
«Permit»		**Notation**
Description	This relationship specifies that the behaviour of a UC may be permitted by the behaviour of a security UC.	<<permit>>
Tagged Values	PermissionCondition, KindPermission	
«Protect»		**Notation**
Description	This relationship specifies that the behaviour of a UC may be protected by the behaviour of a security UC.	<<protect>>
Tagged Values	InvolvedAsset, ProtectionLevel, KindAttack	
«Mitigate»		**Notation**
Description	This relationship specifies that the behaviour of a misuse case may be mitigated by the behaviour of a security UC.	<<mitigate>>
Tagged Values	SuccessPercentage, KindCountermeasure	
«Threaten»		**Notation**
Description	This relationship specifies that the behaviour of a UC may be threatened by the behaviour of a misuse case.	<<threaten>>
Tagged Values	SuccessPercentage, KindVulnerability, KindAttack	
«GridActor»		**Notation**
Description	This actor specifies a role played by a Grid user or any other Grid system that interacts with the subject.	«GridActor»
Tagged Values	KindGridCredential, KindGridActor, KindRole, DomainName, Site-Credential	
«MisActor»		**Notation**
Description	This actor specifies a role played by a attacker or misuser or any other attack that interacts with the subject	«MisActor»
Tagged Values	KindMisActor, HarmDegree	

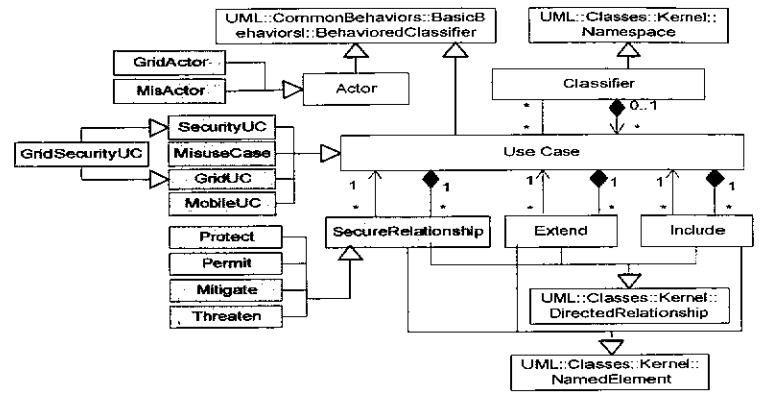

Fig. 1. The concepts used for modeling secure mobile Grid UCs in UML 2.0

using an intuitive, graphical notation. UML offers the possibility of extending the modeling language using well-defined extensibility constructs that are packaged in a so-called UML Profile. In our work, we use *stereotypes* to define new types of model elements and *tagged values* to introduce additional attributes into metamodel types.

In order to define reusable UC diagrams, which are specific to mobile Grid systems, it is necessary to extend the UML 2.0 metamodel and define stereotypes. A stereotype is an extension of the UML vocabulary that allows us to create new building blocks derived from the existing ones but which are specific to a concrete domain, in our case, the Grid computing domain. In this section we present the GridUCSec-Profile extension through which it is possible to represent specific mobile Grid features and security aspects for UC diagrams, thus obtaining UC diagrams for secure mobile Grid environments. This extension has been built as a UML profile which is an extensibility mechanism that allows us to adapt the metaclasses of a model thus making the incorporation of new elements into a domain possible. Fig. 1 shows a UC diagram metamodel in UML 2.0 extended with the new stereotypes of GridUCSec-profile.

In Table 1, we briefly define the stereotypes for the GridUCSec-profile based on the UML 2.0 specification [20]. Three elements are shown in the definition: 1) *Description*: This indicates the purpose and significance for the different users of stereotypes. 2) *Notation*: This corresponds with an icon that it is associated with the stereotype for its graphic notation. 3) *Tagged Values*: This identifies the attributes associated with the stereotype.

3 Applying GridUCSec-Profile to a Real Case

GridUCSec-profile is being validated through a real case application, a business application in the Media domain, defined within the GREDIA European project (www.gredia.eu). This profile will help us to build UC diagrams for a Mobile Grid

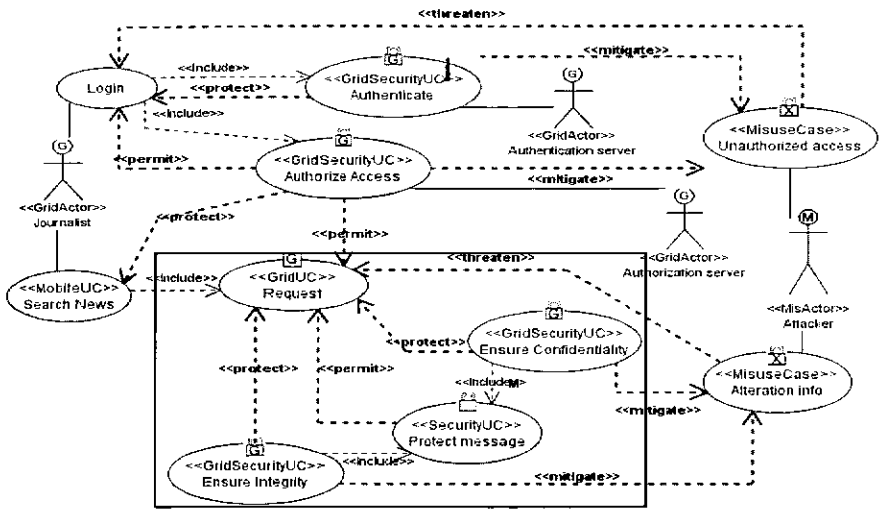

Fig. 2. Main diagram of the application with reusable UCs and reusable sub-diagram

application, which will allow journalists and photographers (actors in the media domain) to make their work available to a trusted network of peers at the same instant as it is produced, either from desktop or mobile devices. We wish to build a system that will cater for the reporter who is on the move with lightweight equipment and wishes to capture and transmit news content.

First, we must identify the functional UCs of the application, but due to space constraints only consider two of them (Login and Search news) are considered here. Second, we must define the possible security needs for these functional UCs (authentication, authorization, confidentiality and integrity). Third, we must identify the possible threats that may attack the system and represent them as misuse cases (unauthorized access and alteration info). Finally, we use the GridUCSec-profile to relate the UCs between them and describe the relevant security aspects that will be necessary in the next activities of the methodology. The resulting diagram is shown in Fig. 2.

The "*«GridSecurityUC» Authenticate*" models the authentication service of the application and is responsible for protecting the "*Login*" UC and for mitigating the "*«MisuseCase» Unauthorized access*" misuse case which threatens the "*Login*" UC. The "*«GridSecurityUC» Authorize access*" models the authorization service and is responsible for protecting the "*«MobileUC» Search news*" UC, for mitigating the "*«MisuseCase» Unauthorized access*" misuse case and for permitting the execution of "*Login*" and "*«GridUC» Request*". We also have the "*«MisuseCase» Alteration info*" misuse case that threatens the modification or alteration of the information exchanged in the messages every time that a request is sent to the system. This threat is mitigated by the "*«GridSecurityUC» Ensure Confidentiality*" and "*«GridSecurityUC» Ensure Integrity*" UCs which are part of the reusable sub-diagram stored in the repository. Finally, the "*«MobileUC» Search News*" UC is identified as a mobile UC due to the

possible mobility of the user who requests information from the system from the mobile devices. This mobile UC includes the "*«GridUC» Request*" UC which is responsible for making the request in a secure manner.

In order to build the resulting diagram, we have used a reusable UCs diagram (sub-diagram shown in Fig. 2) which is availability in the repository and is defined by using our UML profile, to model a common scenario that ensures confidentiality and integrity of a request in Grid environments, which is required of our application. This sub-diagram shows how the "*«GridUC» Request*" UC is protected, through «protect» relationships, by the "*«GridSecurityUC» Ensure Confidentiality*" and "*«GridSecurityUC» Ensure Integrity*" security UCs which mitigate the "*«MisuseCase» Alteration info*" misuse case that threatens "*«GridUC» Request*". It also establishes a «permit» relationship from the "*«SecurityUC» Protect message*" security UC, meaning that once the message is protected, the request can be carried out.

Table 2 shows the detailed information of the reusable sub-diagram stored in the repository according to GridUCSec-profile. In this table we can see the different values for the tagged values of the stereotypes used in the sub-diagram. So, for example, we assign the following values to the "*«GridSecurityUC» Ensure Confidentiality*" UC:

- *SecurityRequirement: {Confidentiality}*. This indicates that this UC establishes confidentiality in the diagram, incorporating this security requirement in the application.
- *InvolvedAsset: {Message, Data}*. This indicates that the important assets in this UC are message and data, thus establishing confidentiality in both messages and data.
- *SecurityDomain: SecNews*. This identifies the security domain of the application in which security controls are carried out. This application contains SecNews.
- *SecurityDegree: {High}*. This is used to establish confidentiality in messages. It adds a high degree of security to the message exchanges and communication in the system.
- *SecurityDependence: {VLow}*. This value indicates that this UC has a very low risk level and does not, therefore, need to be protected by others.

This security UC protects the "*«GridUC» Request*" UC and mitigates the "*«MisuseCase» Alteration info*" misuse case. Many values of the tagged values of these stereotypes must therefore coincide, indicating the relationships between them to fulfil their purposes. The "*InvolvedAsset*" tagged value for the "*«GridUC» Request*" UC is therefore "Message", indicating that messages are the asset to be protected from threats and attacks which may damage them. This protection is carried out by both "*«GridSecurityUC» Ensure Confidentiality*" and "*«GridSecurityUC» Ensure Integrity*". The value for the "*InvolvedAsset*" tagged value of the *«protect»* stereotypes must also coincide and are assigned the "Message" value. The message is also one of the assets that may be threatened by the "*«MisuseCase» Alteration info*" misuse case, which we shall deal with next. The values in the other stereotypes shown in Table 2 are assigned by following the same criteria.

Table 2. Detailed definition for the reusable subdiagram using GridUCSec-profile

Stereotype	Tagged Values	
«GridSecurityUC» Ensure Confidentiality (EC)	SecurityRequirement: {Confidentiality}	
	InvolvedAsset: {Message, Data}	SecurityDomain: SecNews
	SecurityDegree: {High}	SecurityDependence: {VLow}
«GridSecurityUC» Ensure Integrity (EI)	SecurityRequirement: {Integrity}	
	InvolvedAsset: {Message, Data}	SecurityDomain: SecNews
	SecurityDegree: {High}	SecurityDependence: {VLow}
«SecurityUC» Protect Message (PM)	SecurityRequirement:{Confidentiality, Integrity, Privacy}	
	InvolvedAsset: {Message}	SecurityDomain: SecNews
	SecurityDegree: {High}	
«GridUC» Request (R)	GridRequirement: {Interoperatibility}	SecurityDependence: {Medium}
	ProtectionLevel: {Medium}	InvolvedAsset: {Message}
«Protect» EC – R	InvolvedAsset: {Message, Data}	ProtectionLevel: {High}
	KindAttack: {MasqueradingAtt}	
«Protect» EI – R	InvolvedAsset: {Message, Data}	ProtectionLevel: {High}
	KindAttack: {EavesdroppingAtt, MasqueradingAtt}	
«Permit» PM - R	PermissionCondition: messages encrypted and signed	
	KindPermission: {Execute, Include, Protect}	

It is next necessary to define the relationships between all the UCs that are part of the main diagram (reusable or not) and their relationships with the UCs from the sub-diagram to be integrated into the main diagram. In Table 3, we define these relationships and any relevant information that it is necessary to obtain for the following activities or tasks of the methodology. In the reusable sub-diagram, we have defined security UCs which permit us to establish «*mitigate*» relationships with misuse cases. So, for example, the confidentiality of messages can mitigate and prevent the modification or alteration of the messages that are exchanged in the system, and this is represented with the «*mitigate*» relationship between the "*«GridSecurityUC» Ensure Confidentiality*" UC and the "*«MisuseCase» Alteration info*" misuse case. The values defined for this relationship are the following:

- *SuccessPercentage: {High}*. This indicates a high percentage of attack mitigation with message confidentiality.
- *KindCountermeasure: encrypt message*. This indicates the countermeasure that it is recommendable to take to protect the security against this attack.

For the "*«MisuseCase» Alteration info*" misuse case it is necessary to define the values which detail the main features of the attack, and which assist us towards a better knowledge of this type of attacks in order to make decisions regarding how to protect to our system from them. The values assigned to this misuse case are:

- *InvolvedAsset: {Message, Identity, Data}*. This indicates the assets that may be attacked by this UC. In this case, the alteration of information affects messages, data and identity stored in the mobile device. The message is the asset to be protected by the security UCs and which is threatened by the misuse cases in this application.
- *ImpactLevel: {High}*. This threat produces a high impact level in the system if the alteration of the messages is carried out successfully.

Table 3. Detailed description of the elements of the main diagram using GridUCSec-profile

Stereotype	Tagged Values	
«MobileUC» Search News (SN)	MobileRequirement: {Integrity, Delegation}	
	SecurityDependence: {High}	InvolvedAsset: {Message}
	NetworkProtocol: {WAP}	ProtectionLevel: {VHigh}
«MisuseCase» Alteration info (AI)	InvolvedAsset: {Message, Identity, Data}	
	ImpactLevel: {High}	RiskLevel: {High}
	ThreatLikelihood: {Frequent}	KindAttack: {MasqueradingAtt}
«MisuseCase» Unauthorized access (UA)	InvolvedAsset: {Message, Identity, Data}	
	ImpactLevel: {High}	RiskLevel: {High}
	ThreatLikelihood: {Frequent}	KindAttack: {MasqueradingAtt}
«GridSecurityUC» Authorize Access (AA)	Securityrequirement: {Confidentiality}	
	SecurityDegree: {High}	InvolvedAsset: {Message}
	SecurityDependence: {VLow}	SecurityDomain: SecNews
«GridSecurityUC» Authenticate (Auth)	Securityrequirement: {Confidentiality}	
	SecurityDependence: {VLow}	InvolvedAsset: {Message}
	SecurityDegree: {High}	SecurityDomain: SecNews
«Threaten» AI – R	KindVulnerability: messages by wireless network	SuccessPercentage: {High}
	KindAttack: {MasqueradingAtt, EavesdroppingAtt}	
«Threaten» UA – Login	KindVulnerability: identity and credential stored	SuccessPercentage:{VHigh}
	KindAttack: {AccessControlAtt, MaliciousAtt}	
«Mitigate» EC – AI	SuccessPercentage: {High}	KindCountermeasure: encrypt message
«Mitigate» EI – AI	SuccessPercentage: {High}	KindCountermeasure: digital sign
«Mitigate» AA–UA	SuccessPercentage: {VHigh}	KindCountermeasure: check privilegies
«Mitigate» Auth – UA	SuccessPercentage: {VHigh}	KindCountermeasure: check identity
«Protect» Auth - Login	InvolvedAsset: {Credential, Identity}	ProtectionLevel: {High}
	KindAttack: {AccessCOntrolAtt, IntruderAtt}	
«Protect» AA – SN	InvolvedAsset: {Identity, Resource}	ProtectionLevel: {VHigh}
	KindAttack: {MaliciousAtt, AccessControlAtt}	
«Permit» AA – R	PermissionCondition: check privilegies	KindPermission: {CheckExecute}
«Permit» AA - Login	PermissionCondition: check access rights	
	KindPermission: {CheckExecute, Protect}	
«GridActor» Journalist	KindGridActor: {Mobile User}	DomainName: News
	KindRole: journalist	KindGridCredential: {UserPass, X509}
	Site-Credential: {(News, UserPass),(SecNews,X509)}	
«GridActor» Authentication server	KindGridActor:{Service}	KindRole: security server
	KindGridCredential:{X509}	DomainName: SecNews
«GridActor» Authorization server	KindGridActor:{Service}	KindRole:security server
	KindGridCredential:{X509}	DomainName: SecNews
«MisActor» Attacker	KindMisActor: hacker	HarmDegree: {Medium}

- *RiskLevel: {High}*. With regard to the assets involved in this misuse case, this attack produces a high risk level of damage to the assets.
- *ThreatLikelihood: {Frequent}*. This specifies a frequent (monthly) likelihood that this threat will occur in the system to alter information in the messages.
- *KindAttack: {MasqueraddingAtt}*. The masquerading attack could permit the disclosure or modification of information.

The UC that has most relationships with the other UCs is the "*«GridSecurtyUC» Authorize access*" which protects "*«MobileUC» Search News*", grants permission for the realization of "*«GridUC» Request*" and "*Login*" UCs, and mitigates the

"*«MisuseCase» Unauthorized access*" misuse case. This UC therefore defines 4 types of relationships, which are shown in Table 3. For example, for the *«Protect»* relationship, we have defined the following values:

- *«Protect» Authorize Access – Search News (AA – SN).* This relationship defines values for the tagged values:
  - *InvolvedAsset: {Identity, Resource}.* This indicates that the assets which should be protected by authorization rules are the identity of the user and the resource owned by this identity.
  - *ProtectionLevel: {VHigh}.* This relationship specifies a very high protection level that the origin UC offers to the destination UC.
  - *KindAttack: {MaliciousAtt, AccessControlAtt}.* This relationship can protect UCs from malicious and access control attacks.

Table 3 shows the remaining values for the tagged values of the stereotypes of the diagram in Fig. 2. Each value is obtained as we have shown previously.

4 Conclusions and Future Work

In order to study the needs and particularities of mobile Grid systems, it was necessary to define an extension of UML UCs that would capture the performance, functions, properties and needs that arise in this kind of systems. The UML extension for UCs makes it possible to analyse the system's security requirements from the early stages of development, to enrich UC diagrams with security aspects and to define values that are essential if we are to interpret and capture what will be required in the following activities of our development process.

This UML profile permits us to identify features, aspects and properties that are important in the first stages of the life cycle and will be very useful when making decisions about which security mechanisms, services, etc. to use in the design activity. The application of this profile to a real case has helped us to refine and improve the definition of the profile by adding or changing new values, properties or constraints that were not initially considered. For example, we have defined mobile UCs because it is necessary to capture the mobile behaviour, and we have also defined new tagged values because we found aspects that must be included in our analysis and which were not initially included. Furthermore, this extension will permit us to build more detailed, complete and richer UC diagrams in terms of semantics.

As future work, we aim to complete the details of this methodology (activities, tasks, etc.) through the research-action method by integrating security requirements engineering techniques (UMLSec, etc.) and defining the traceability of artifacts. We will complete the real case by describing all of the application's functional UCs with GridUCSec-profile.

Acknowledgments. This research is part of the following projects: QUASIMODO (PAC08-0157-0668) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain), ESFINGE (TIN2006-15175-C05-05) granted by the "Dirección General de Investigación del Ministerio de Educación y Ciencia" (Spain), y SISTEMAS (PII2I09-0150-3135) financed by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha".

References

1. Bass, L., Bachmann, F., Ellison, R.J., Moore, A.P., Klein, M.: Security and survivability reasoning frameworks and architectural design tactics. SEI (2004)
2. Breu, R., Burger, K., Hafner, M., Jürjens, J., Popp, G., Lotz, V., Wimmel, G.: Key issues of a formally based process model for security engineering. In: International Conference on Software and Systems Engineering and their Applications (2003)
3. Haley, C.B., Moffet, J.D., Laney, R., Nuseibeh, B.: A framework for security requirements engineering. In: Software Engineering for Secure Systems Workshop, Shangai, China, pp. 35–42 (2006)
4. Jürjens, J.: Secure Systems Development with UML. Springer, Heidelberg (2005)
5. Mouratidis, H., Giorgini, P.: Integrating Security and Software Engineering: Advances and Future Vision. IGI Global (2006)
6. Foster, I., Kesselman, C.: The Grid2: Blueprint for a Future Computing Infrastructure, 2nd edn. Morgan Kaufmann Publishers, San Francisco (2004)
7. Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M.: Engineering Process Based On Grid Use Cases For Mobile Grid Systems. In: The Third International Conference on Software and Data Technologies- ICSOFT 2008, Porto, Portugal, pp. 146–151 (2008)
8. Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M.: PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices. In: International Conference on Availability, Reliability and Security (ARES 2008). IEEE Computer Society, Barcelona (2008)
9. The Object Management Group (OMG): OMG Unified Modeling Language (OMG UML). Version 2.2 (2007), `http://www.omg.org/spec/UML/2.1.2/Infrastructure/PDF/`
10. Alexander, I., Maiden, N.: Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle. John Wiley & Sons, Chichester (2004)
11. Sindre, G., Opdahl, A.L.: Templates for misuse case description. In: 7th International Workshop on Requirements Engineering: Foundation for Software Quality, Austria (2001)
12. Sindre, G., Opdahl, A.L.: Capturing Security Requirements by Misuse Cases. In: 14th Norwegian Informatics Conference (NIK 2001), Tromsø, Norway (2001)
13. Alexander, I.: Misuse Cases: Use Cases with Hostile Intent. IEEE Software, 58–66 (2003)
14. Firesmith, D.G.: Security Use Cases. Journal of Object Technology, 53–64 (2003)
15. Sindre, G., Opdahl, A.L.: Eliciting security requirements with misuse cases. Requirements Engineering Journal 10, 34–44 (2005)
16. Rosado, D.G., Fernández-Medina, E., López, J.: Obtaining Security Requirements for a Mobile Grid System. International Journal of Grid and High Performance Computing (2009) (to be published in April 1, 2009)
17. Rosado, D.G., Fernández-Medina, E., López, J.: Extensión UML para Casos de Uso Reutilizables en entornos Grid Móviles Seguros. XIV Jornadas de Ingeniería del Software y Bases de Datos - JISBD 2009, San Sebastián (2009)

18. Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M.: Towards an UML Extension of Reusable Secure Use Cases for Mobile Grid systems. IEICE Transactions on Information and Systems (2009) (submitted)
19. Rosado, D.G., Fernández-Medina, E., López, J.: Reusable Security Use Cases for Mobile Grid environments. In: Workshop on Software Engineering for Secure Systems, in conjunction with the 31st International Conference on Software Engineering, Vancouver, Canada, pp. 1–8 (2009)
20. OMG: OMG Unified Modeling Language (OMG UML), Superstructure, V2.1.2 (2007), http://www.omg.org/spec/UML/2.1.2/Infrastructure/PDF/
21. Røstad, L.: An extended misuse case notation: Including vulnerabilities and the insider threat. In: XII Working Conference on Requirements Engineering: Foundation for Software Quality, Luxembourg (2006)