Journal of Universal Computer Science, vol. 16, no. 17 (2010), 2333-2352
submitted: 15/2/10, accepted: 30/8/10, appeared: 1/9/10 © J.UCS

Developing a Secure Mobile Grid System through a UML Extension

David G. Rosado
(UCLM. Alarcos Research Group-Information Systems and Technologies Institute, Spain
David.GRosado@uclm.es)

Eduardo Fernández-Medina
(UCLM. Alarcos Research Group-Information Systems and Technologies Institute, Spain
Eduardo.FdezMedina@uclm.es)

Javier López
(University of Málaga. Computer Science Department, Spain
jlm@lcc.uma.es)

Mario Piattini
(UCLM. Alarcos Research Group-Information Systems and Technologies Institute, Spain
Mario.Piattini@uclm.es)

Abstract: The idea of developing software through systematic development processes to improve software quality is not new. Nevertheless, there are still many information systems such as those of Grid Computing which are not developed through methodologies that are adapted to their most differentiating features. A systematic development process for Grid systems that supports the participation of mobile nodes and incorporates security aspects into the entire software lifecycle will thus play a significant role in the development of systems based on Grid computing. We are creating a development process 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 process is that of analysis which is focused on ensuring that the system's security and functional requirements are elicited, specified and modelled. In our approach, this activity is driven by use cases and supported by the reusable repository. This obtains, builds, defines and refines the use cases of the secure Mobile Grid systems which represent the functional and non-functional requirements of this kind of systems. In this paper, we present the proposed development process through which we introduce the main aspects of the UML profile defined for building use case diagrams in the mobile Grid context through which it is possible to represent specific mobile Grid features and security aspects, showing in detail how to build use case diagrams for a real mobile Grid application by using our UML profile, denominated as GridUCSec-Profile.

Keywords: UML extension, Security, Use Cases, secure mobile Grid, secure development
Categories: C.2.4, D.2.1, K.6.5, L.4, L.7

1 Introduction

The growing need to construct secure systems, principally as a result of the new vulnerabilities caused by the use of the Internet and that of applications distributed in heterogeneous environments, has encouraged the scientific community to demand a

clear integration of security into the development processes [Bass, Bachmann et al. (2004); Breu, Burger et al. (2003); Haley, Moffet et al. (2006); Jürjens (2005); Lodderstedt, Basin et al. (2002); Mouratidis and Giorgini (2006); Rosado, Gutiérrez et al. (2006)]. Systems based on Grid Computing are a type of systems that have clear differentiating features of which security is an extremely important aspect. The Grid enables resource sharing and dynamic allocation of computational resources, thus increasing access to distributed data, promoting operational flexibility and collaboration, and allowing service providers to scale efficiently in order to meet variable demands [Foster and Kesselman (2004)].

In the purview of Grid and Mobile Computing, Mobile Grid is an heir of the Grid, which addresses mobility issues, with the added elements of supporting mobile users and resources in a seamless, transparent, secure and efficient way [Guan, Zaluska et al. (2005); Jameel, Kalim et al. (2005); Park (2009)]. Mobile Grid environments have special features that make them different from other systems and which must be considered throughout the entire development lifecycle. Furthermore, as is described in [Giguhre (2001)], mobile computing imposes a degree of complexity inherent to the environment, such as dynamic environments, mobility, computational resource limitations, latency and instabilities in data transfer, energy supply limitations, and input/output interface limitations. This degree of complexity makes security more difficult to implement in a mobile platform as a result of the limitations of resources in these devices [Bradford, Grizzell et al. (2007)], and is even more critical owing to the open nature of wireless networks.

As is well known in the scientific community, the best way to achieve secure software is to incorporate security aspects at an early stage of the software development [Artelsmair and Wagner (2003); Mouratidis and Giorgini (2006)]. Considering the security aspects from the beginning of the development ensures that security requirements are fully coupled with the design, and that the other system requirements and incompatibilities and errors that may occur once the system has been built are significantly reduced. Thus, although some of the security requirements specified in the analysis activity cannot be fully detailed until the next stages of development (design and construction), it is important to capture them in the analysis activity to ensure that they are considered from the beginning, and to obtain a robust and reliable final product.

The majority of existing mobile Grid applications have been built without a systematic development process and are based on ad-hoc developments [Dail, Sievert et al. (2004); Kolonay and Sobolewski (2004)]. The lack of adequate development methods for this kind of systems has encouraged us to build a methodology with which to develop them [Rosado, Fernández-Medina et al. (2008a); Rosado, Fernández-Medina et al. (2008b)], offering a detailed guide to their analysis, design and implementation. The analysis activity of this methodology is focused 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. The design activity is focused on the design of a secure software architecture which is the software architecture of the system with the incorporation of a specific security architecture for these environments. Finally, the construction activity is oriented

towards the implementation and tests of the final system using the various tools, technologies and standards in Mobile Grid computing.

UML use cases [OMG (2007)] have become a widely used technique for the elicitation of functional requirements [Alexander and Maiden (2004)] 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 [Alexander (2003); Firesmith (2003); Sindre, Guttorm and Andreas L. Opdahl (2001); Sindre, G. and A.L. Opdahl (2001); Sindre and Opdahl (2005)]. 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 [Alexander (2003)].

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 [Alexander (2003)].

The proposal as a whole is rather wide-ranging, and it is for this reason that, in this paper, we shall focus solely on the analysis activity of the process in which 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 which are necessary for the subsequent activities in the process.

The remainder of the paper is organized as follows: In [Section 2], we summarize the development process which we are elaborating. In [Section 3], we present the UML extension used to build use cases diagrams for secure mobile Grid environments. In [Section 4], we apply this UML extension in depth in order to build use case diagrams in a specific mobile Grid application, and provide a detailed description of the possible values of the tagged values of the stereotypes defined in the UML profile. In [Section 5] we explain how we continue through the process from the use case diagrams to the design and implementation of the system. Finally, we propose our conclusions and future work.

2 Overview of the proposed development process

The Secure Mobile Grid development process (SecMobGrid) has been designed to build software systems based on Mobile Grid computing with security aspects. It is a process which builds a secure software product from initial requirements and needs of Mobile Grid systems. This process not only includes security in a development process but is a development process in itself, which incorporates security aspects

throughout the entire process. The process is specially designed for this kind of systems since we have considered the particular aspects and features in each of the phases and activities of the process (planning, analysis, design, construction and maintenance).

This process is different from others owing to the fact that we define tasks and activities that are specific to Mobile Grid systems in which the reuse of elements (such as use cases, security use cases, reference security architecture, etc., available in the repository) is a key aspect in their development, and both the features and details of the Grid technological environment and mobile computing are considered and are present in each task and activity of the process.

Firstly the "*Secure Mobile Grid System Planning*" activity, in the planning phase, carries out an initial capture of requirements and necessities (basic functionality of the system, the domains and organizations involved, the risks to the system, the main security aspects, and so on) in order to create a development plan.

The development phase is composed of three activities: analysis, design and construction, and the principal ideas of these activities are as follows:

- The "*Secure Mobile Grid System Analysis*" activity is focused on identifying and analyzing the requirements and security requirements of Grid systems from a reusable use case model in which the use case and security use case diagrams for this kind of systems are defined. A UML profile called *GridUCSec-profile* is built in which new stereotypes for use cases, actors and associations are defined to capture the behaviour of Mobile Grid systems.
- The goal of the "*Secure Mobile Grid System Design*" activity is to define a secure software architecture from which we should select the structural elements that the system is composed of and the behaviour and interfaces between them. A software architecture is defined by using the typical techniques of the traditional development processes (for example, the Unified Process) and, moreover, the security aspects must be added through a security architecture which is integrated with software architecture, thus obtaining a secure software architecture specified for Mobile Grid systems, which is the main artifact of the design model generated in this activity.
- In the "*Secure Mobile Grid System Construction*" activity, the final system is implemented by considering the Grid technological platform which will be used, and the artifacts of the design model generated in the previous activity. All components (classes, interfaces, services, mechanisms, protocols, etc.) defined in the secure software architecture are implemented and integrated in a single final software product.

The maintenance phase has only one activity: "*Secure Mobile Grid System Maintenance*" and this is a typical maintenance activity in any development process, in which a maintenance plan of the system for its later modification is defined according to the client's new necessities.

Therefore, the main block of the SecMobGrid process consists of a requirements analysis activity driven by use cases, a design activity that focuses on architecture, and a construction activity oriented towards implementation. All these activities are supported by a repository in which different reusable elements that can be used in the different activities and tasks of the SecMobGrid process are stored.

Finally, we have developed a prototype tool called SMGridTool (Secure Mobile Grid Environments Tool) which provides a simple, automatic and intuitive means of building use case diagrams especially designed for Secure Mobile Grid systems by following the UML extension defined in this paper (GridUCSec-profile), and which assists developers and analysts to build use cases diagrams. This tool is focused on the construction and definition of secure Grid use case diagrams, and on the management of the repository that stores reusable artifacts which can be reused in the construction of diagrams. It also permits use case diagrams to be defined by establishing relationships between all the use cases defined in an easy and automatic manner. The tool also facilitates the management of the repository of use case diagrams which enables the stakeholders to reuse diagrams (or parts of them), in addition to maintaining different versions of the same diagram. SMGridTool also automatically performs the validation of the use case diagrams, checking the constraints defined by the GridUCSec-profile for each use case and relationship.

2.1 Previous works

A preliminary publication of the process has been presented in [Rosado, Fernández-Medina et al. (2008b)] in which we describe a first general approach of our development process. An informal presentation of the first steps of our process is also provided in [Rosado, Fernández-Medina et al. (2008a)], 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 [Rosado, Fernández-Medina et al. (2009b)] from which we obtain the security requirements for a specific application by following the steps described in our process. 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 [Rosado, Fernández-Medina et al. (2009c); Rosado, Fernández-Medina et al. (2008a)]. A detailed description of this UML profile for building use case diagrams is provided in [Rosado, Fernández-Medina et al. (2010b)]. Finally, a formal description of the analysis activity using SPEM 2.0 [OMG (2008)] and in which this UML profile is used to build use cases diagrams has been defined in [Rosado, Fernández-Medina et al. (2010b)]. This paper is an extension of [Rosado, Fernández-Medina et al. (2009a)] in which we provide an in depth and detailed description of the different values and aspects considered when use case diagrams are built by applying the UML extension (called GridUCSec-profile) to a real mobile Grid system. The difference between our previous works and this paper is that here, once we have defined our UML profile and it has been validated with a case study, we present how we can use it, manage it, reuse the repository of elements built, assign values and establish relationships with all the elements of the profile until a final use case diagram is obtained which captures all the features, specifically the security features, of these environments. Moreover, the previous publication of the formal description of the aforementioned analysis activity, despite using the same use case diagram, only indicates the final diagram as a result of one of the tasks in the analysis activity. However, in this paper we have built the final diagram by assigning values and establishing relationships with all the elements of our profile from the beginning.

3 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 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. A UC diagram metamodel in UML 2.0 extended with the new stereotypes of GridUCSec-profile is shown in [Fig. 1].

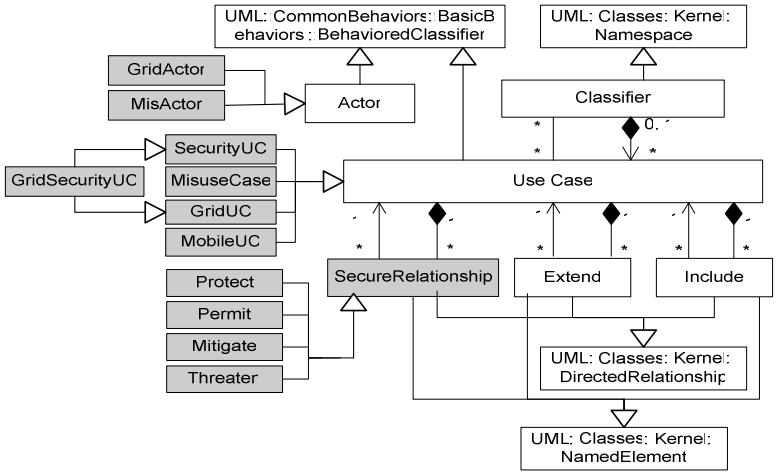


Figure 1: The concepts used for modeling secure mobile Grid UCs in UML 2.0

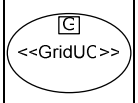
For the representation of Grid use cases, security use cases and misuse cases, a set of stereotypes have been defined, which have been grouped into packages, *GridUCSec* and *TypesGridUCSec* that are part of the GridUCSec-Profile. The GridUCSec package imports data types and their values from the TypesGridUCSec package for assigning the types of the tagged values defined in the GridUCSec package.

The *GridUCSec* package is composed of Grid use cases, security use cases, misuse cases, associations of permission, protection, threaten and mitigation, together with the involved actors. This package has 12 stereotypes ([see Fig. 1]): 5 specialize to UseCase (from UseCases), 2 specialize to Actor (from UseCases), and 5 specialize to DirectedRelationship (from Kernel) and NamedElement (from Kernel and Dependencies).

In this package we have defined two new stereotypes for the Actor class, one of which represents an actor in Grid systems and the other of which represents a bad actor that initiates attacks on the system. We have also defined 5 stereotypes of a Use Case class which will be used to represent specific use cases in this kind of systems, such as the security use cases that capture the security aspects of the system, misuse cases that capture the attacks and threats to the system, grid use cases that define the common features of the Grid systems and mobile use cases that define the mobile behavior. Finally, we have defined the relationships (protect, permit, mitigate and threaten) which are necessary to establish associations with the new uses cases defined in our profile and with the generic use cases of UML. A more detailed description can be found in [Tab. 1].

The *TypesGridUCSec* package defines the types of data for the tagged values of the stereotypes of the GridUCSec-Profile, such as level of protection and of risk, types of permission, of requirement, of asset, of attack, etc. This package is composed of 9 stereotypes which specialize to the Enumeration class (from Kernel) which are: AssetType, AttackType, AttackerType, CredentialType, FrequencyType, GridActorType, LevelType, PermissionType and RequirementType. These types of data have a set of possible values that the tagged values of the stereotypes defined in the GridUCSec package must select.

In [Tab. 1], we briefly define the stereotypes for the GridUCSec-profile based on thec UML 2.0 specification [OMG (2007)]. 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.

«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.	
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.	
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.	
Tagged Values	InvolvedAsset, SecurityRequirement, SecurityDegree,	

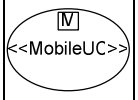
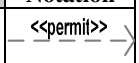
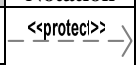
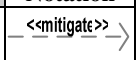
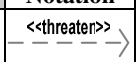
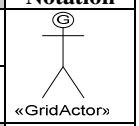
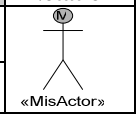
	SecurityDependence, SecurityDomain	
«MisuseCase»		**Notation**
Description	A sequence of actions, including variants, that a system or other entity can perform, interacting with misusers of the entity and causing harm to certain stakeholders if the sequence is allowed to be completed.	
Tagged Values	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.	
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.	
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.	
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.	
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.	
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.	
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	
Tagged Values	KindMisActor, HarmDegree	

Table 1: Detailed description of Stereotypes for the GridUCSec package

4 Applying GridUCSec-profile to a real case

GridUCSec-profile has been 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 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.

The aim of this paper is to present how a UML profile of use cases for mobile Grid applications is applied to a real case, and how we can assign different values and build use case diagrams to capture the security requirements and needs for this kind of systems.

Before obtaining the results presented in this paper, this profile has obviously been defined and refined by adding all those new use cases and relationships that needed to be applied to the case study. The case study has therefore served to improve and modify our UML profile with new elements, which were not initially considered, and which were necessary to capture the presence of certain behavior and security aspects that have been discovered upon their application to the case study. Early versions of the methodology and model have been published previously, as indicated in this paper, but nothing has been published in relation to the main contribution of this paper, which is the practical implementation of the final UML profile in a case study.

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.

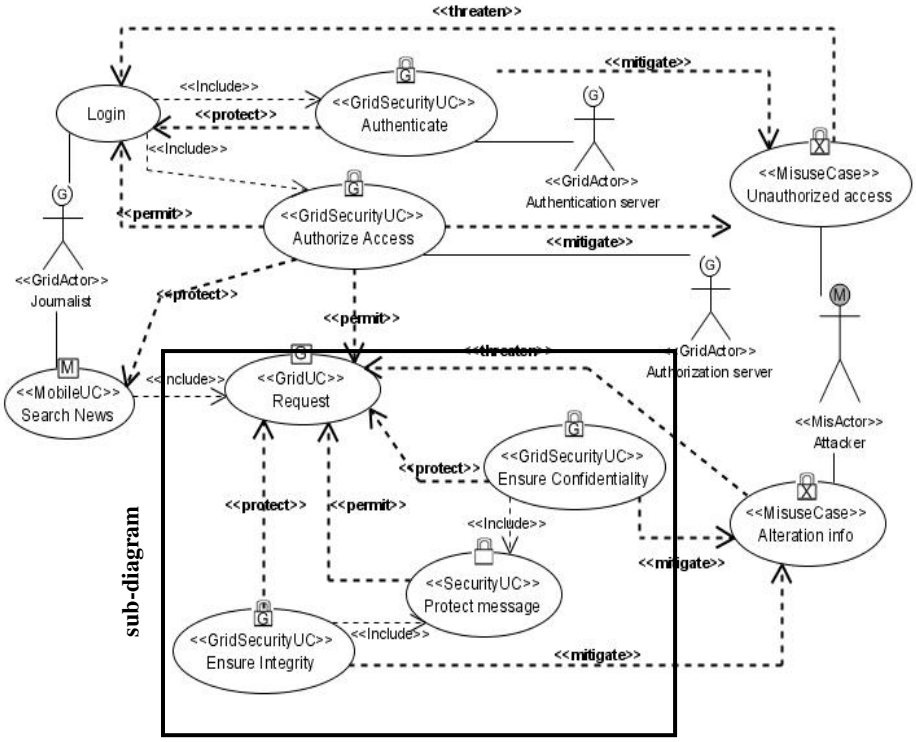


Figure 2: Main diagram of the application with reusable UCs and reusable sub-diagram [Rosado, Fernández-Medina et al. (2010b)].

The detailed information of the reusable sub-diagram stored in the repository according to GridUCSec-profile is shown in [Tab. 2]. 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.

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}	
	InvolvedAsset: {Message}	ProtectionLevel: {Medium}
«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}	

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

The values in the other stereotypes shown in [Tab. 2] are assigned by following the same criteria. So, for example, for the "*«Protect» EC - R*" relationship type, we define the following values:

- *InvolvedAsset: {Message, Data}*. This indicates that this relationship protects assets such as message and data, thus establishing protection in both messages and data with the security UC which owns this relationship. These values should coincide with some of the assets involved in the origin UC and destination UC.

- *ProtectionLevel: {High}*. This indicates that this relationship offers the destination UC a high level of protection through the security UC "*«GridSecurityUC» Ensure Confidentiality*".
- *KindAttack: {MasqueradingAtt}*. This identifies the kind of attack that we wish to protect and is carried out in the destination UC of this relationship. This attack is of a masquerading type in which a possible disclosure or modification of information in a request to the Grid system can be carried out.

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. Now, 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.
- *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.

This misuse case threatens the "*«GridUC» Request*" use case, establishing a "*threaten*" relationship («Threaten» AI – R) with the following values:

- *KindVulnerability: messages by wireless network*. This indicates that messages exchanged by wireless are vulnerable to possible attacks (disclosure, modification, alteration, etc.) on the requests of the system.
- *SuccessPercentage: {High}*. This indicates that this attack has a high percentage of success in attacking the request to the Grid system.

- *KindAttack: {MasqueradingAtt, EavesdroppingAtt}*. This indicates the possible attack types which may occur in the system initiated by the origin misuse case (Alteration info) towards a destination UC (Request).

Finally, the misuse case is initiated by an attacker which is represented by a MisActor stereotype (*"«MisActor» Attacker*") and whose values are:

- *KindMisActor: hacker*. This indicates that a possible attacker of the system is a hacker.
- *HarmDegree: {Medium}*. This indicates that a hacker can cause a medium degree of harm to the system and that we must protect it.

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. The values assigned to *"«GridSecurtyUC» Authorize access*" UC are:

- *SecurityRequirement: {Authorization}*. This indicates that this UC establishes authorization in the system, accepting or denying the requests of access to the system, resource or service.
- *InvolvedAsset: {Identity, Resource}*. This indicates that the important assets in this UC are identity and resource, thus establishing authorization decisions from the user's identity and the resource access policy.
- *SecurityDomain: SecNews*. This identifies the security domain of the application in which security controls are carried out. This application contains SecNews.
- *SecurityDegree: {VHigh}*. This adds a very high degree of security to the system, establishing authorization to access Grid services and resources.
- *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 UC therefore defines 4 types of relationships. We have defined for these 4 types, 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.
- *«Permit» Authorize Access – Request (AA – R).* This relationship defines values for the tagged values:
  - *PermissionCondition: check privileges*. This indicates that it is necessary to check the privileges of the user or service that makes the request to the system to permit the realization of the *"«GridUC» Request*" UC.
  - *KindPermission: {CheckExecute}*. This indicates the type of permission granted for the realization of the *"«GridUC» Request*" UC. This permission is of the execution type.
- *«Permit» Authorize Access – Login (AA – Login).* This relationship defines values for the tagged values:

  - *PermissionCondition: check access rights*. This indicates that it is necessary to check the access rights of the user or service that wishes to access the system to permit the realization of the *"Login*" UC.
  - *KindPermission: {CheckExecute, Protect}*. This indicates the types of permissions granted for the realization of the *"Login*" UC. These permissions are of the execution and protection types.
- «Mitigate» *Authorize Access – Unauthorized Access (AA–UA)*. This relationship defines values for the tagged values:
  - *SuccessPercentage: {VHigh}*. This indicates that the *"«GridSecurtyUC» Authorize access*" security UC has a very high percentage of success in mitigating the attack of unauthorized access to the system.
  - *KindCountermeasure: check privileges*. This indicates that, by checking the privileges of the user or service involved in the system, we can protect security and privacy from the "unauthorized access" attack.

Finally, this UC is related to an actor which is represented by a GridActor stereotype (*"«GridActor» Authorization Server*") and whose values are:

- *KindGridActor: {Service}*. This indicates that the type of Grid actor that interacts with the *"«GridSecurtyUC» Authorize access*" security UC is a service.
- *KindRole: security server*. This indicates the type of role that the service plays in the system, signifying that the privileges associated with the authorization server are known from its role. This role is of the security server type.
- *DomainName: SecNews*. This indicates that the authorization server belongs to the SecNews security domain.
- *KindGridCredential: {X509}*. This indicates that the type of credential exchanged with the authorization server is the X.509 certificate. It is necessary to know this when we implement the authorization service.
- *Site-Credential: {(SecNews, X509)}*. This indicates that the type of credential exchanged with the SecNews domain is the X.509 certificate.

The remaining values for the tagged values of the stereotypes of the diagram in [Fig. 2] are obtained as we have shown previously and that we have omitted by constraints space.

5 Towards the Design and Construction

As we have seen in [Section 2], the proposed development process contains three activities in the development phase in which, in the analysis activity, we build use case diagrams to identify the requirements of the mobile Grid system, in the design activity we design a secure software architecture that fulfils the requirements identified in the analysis activity, and finally, in the construction activity we implement the services of the architecture designed in the design activity using the Grid tools and libraries to build Grid computing based systems.

Therefore, from the security use cases defined in the use case diagrams built in the analysis activity according to a UML extension presented in this paper, we can identify and specify the security requirements necessary in the Grid application which are defined thanks to the tagged values of the stereotypes of our UML profile (GridUCSec-profile). These requirements permit our process to continue through the design and implementation of the security architecture which covers all these security

requirements. For our case study, we have the following security UCs: Authenticate, Authorize access, Ensure Confidentiality and Ensure Integrity [see Fig. 2]. The security requirements defined in the tagged values of the «GridSecurityUC» stereotype of our profile are extracted from these security UCs. These requirements are: Authentication, Authorization, Confidentiality and Integrity.

We have also elaborated a service-oriented security architecture [Rosado, Fernández-Medina et al. (2010a)] in which we have defined a complete set of security services and interfaces which cover the majority of security requirements specified in the analysis activity for Mobile Grid systems. This security architecture protects the Grid system and offers the necessary support to ensure that the security requirements and needs are fulfilled. The set of security services that will take part in the security architecture and which we consider to cover the security requirements for these systems are: Integrity, Confidentiality, Authentication, Authorization, Non-repudiation, Delegation, Anonymity, Privacy, Trust Management, Credential Management, Identity Management, Mobile Policy, Grid Security Policy and Audit. From security UCs and with the associated security requirements, we can identify the subset of security services of the reference security architecture for a specific application through association rules between security requirements and security services. These association rules indicate what the most appropriate security services of the security architecture are, depending on the security requirements captured and specified in the analysis activity through use cases with the new UML profile.

Each security service will have an interface through which to interact with other services both within and outside the architecture. The interfaces have been defined in a specific manner in order to focus on and identify the objective that we wish to achieve, and in a manner that is sufficiently generic for it not to depend on any technological platform.

Each security UC is therefore associated with one or more security requirements, and the security services associated with these security UCs cover the security requirements represented by these security use cases. Thus, the aim is to obtain a set of security services which cover and take into account the security requirements represented by the four security use cases. By following the association rules between security requirements and security services, we obtain that the security services to consider for the security architecture of this application from the security use cases identified in the analysis activity are: Authorization, Authentication, Credential Management, Identity Management, Trust Management, Confidentiality and Integrity. We should not omit the Grid Security Policy service and the Mobile Policy service which are needed to manage the different policies of the system. These security services are obtained from the relationship with the security requirements which are defined as tagged values in the GridUCSec-profile and are shown in [Fig. 3].

Finally, and after carrying out a set of tasks in the design activity, we obtained the design model which is the output artifact of this activity and will be the input artifact for the construction activity which is focused on the configuration and implementation of the elements contained in the design model. In this activity we define the technological environment that we must use in order to implement the system with the help of tools and libraries oriented towards Grid computing. The selected tool is the Globus toolkit which provides software tools that facilitate the construction of computational grids and grid-based applications. PERMIS and VOMS

can also be used as a security infrastructure for authorization and access control, along with Java CoG kits, which is a tool that provides the implementation in Java of some components of the Globus toolkit. It is necessary to implement the interfaces of the security services selected and identified in the design activity in the Globus platform.

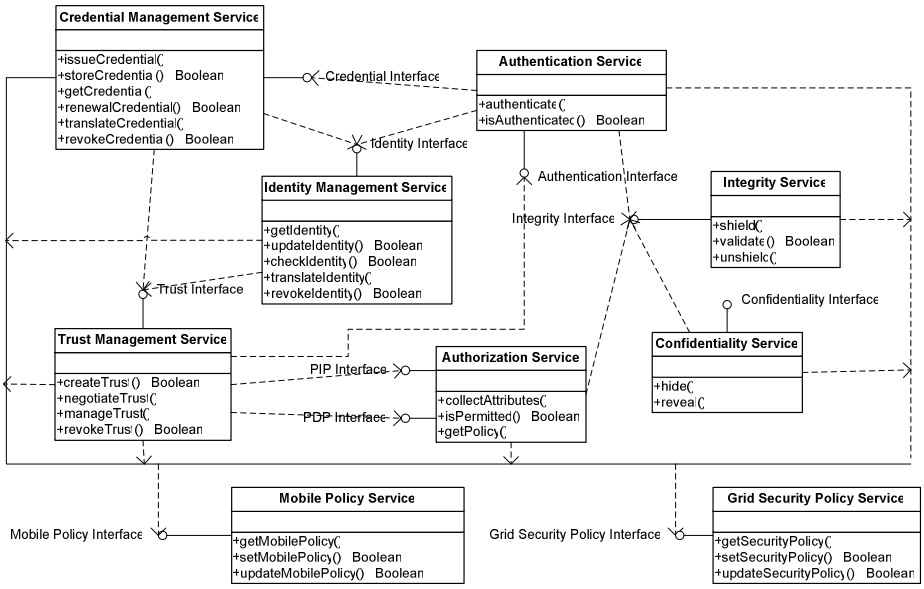


Figure 3: Services and interfaces of Security Architecture instantiated for this case study

6 Lessons Learned

The development of the case study has enabled us to apply the SecMobGrid process to a real environment and to verify in practice that the process allows the development of a secure Mobile Grid system from the initial needs and requirements.

The lessons learned from the implementation of this process in the case study have been:

- The application of this case study has allowed us to improve and refine several tasks in the process, essentially by adding new artifacts that were necessary or removing others that were not used. A series of steps and the use of certain techniques, along with the repository of reusable elements, have also been updated and refined.
- It has been shown that the support of a tool is crucial for the practical application of this process, specifically in the analysis activity owing to the large number of use cases managed and the numerous security relationships and attributes which have to be defined for a complete analysis of system requirements.

- We were also able to identify aspects for improvement in the prototype tool, principally with regard to repository management since, as different applications are being developed, the number of use cases and diagrams stored in the repository grows.
- Prior to the application of the process, we identified a set of possible values that could be assigned to the use cases defined in the GridUCSec-profile, indicating specific values that appear in most Mobile Grid systems as being the set of assets to be considered, the set of requirements to consider, all the possible attacks on the system, etc. These values are very useful for building Grid use case diagrams and are taken into consideration in the entire development process.

7 Conclusions and future work

The systematic engineering process that we are elaborating will principally confront two great challenges, the first of which is to establish a process for the secure development of Grid systems, considering both the functional and non-functional needs, and particularly the security not only of the system to be constructed but also the needs that arise when it is implemented using Grid technology. The second challenge is that of solving the use of mobile devices in Grid systems, with all the difficulties that constructing a Grid infrastructure that supports mobile devices entails, owing to the limitations and features of these devices. This is why the need exists to develop and define a process for developing a system based on Grid and mobile technology, considering the security peculiarities and needs for this kind of systems from the early stages of development.

In order to study the needs and particularities of mobile Grid systems, it was necessary to define an extension of UML use cases that would capture the performance, functions, properties and needs that arise in this kind of systems. The UML extension for use cases makes it possible to analyse the system's security requirements from the early stages of development, to enrich use case 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 Grid needs to build a unified security system that supports all security functions, signifying that a service oriented security architecture that defines a wide set of security services and covers all the security requirements for the mobile Grid environments captured by Grid use cases is fundamental for building a security model for this kind of systems. The application of this profile to a real case has helped us to refine and improve all artifacts of the process (UML profile, security architecture, repository, association rules, etc.) by adding or changing new values, properties, constraints, parameters, services, interfaces, and so on that were not initially considered. It has also allowed us to complete and improve the activities and tasks of the development process.

As future work, we shall complete the formal development process to describe the phases, activities and tasks with the SPEM specification and we shall define the process with a tool that supports the SPEM notation, such as EPF (Eclipse Process

Framework), and enables its automated integration with the processes of other methodologies based on UML as UP, OPEN, OpenUP, etc. We shall also refine and improve the parameters and tagged values of the GridUCSec-profile in order to capture the most important aspects and features of Mobile Grid systems to enable them to be taken into account in the design and construction activities of the process. We shall complete the real case by describing all the application's functional UCs with GridUCSec-profile, and we shall apply our process and the UML profile to a new case study according to the electronic bank. An adaptation of this proposal to Cloud computing, which is a technology which provides computer services through the Internet, may also be studied.

Acknowledgements

This research is part of the following projects: QUASIMODO (PAC08-0157-0668) and SISTEMAS (PII2I09-0150-3135) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain), MEDUSAS (IDI-20090557) financed by the "Centro para el Desarrollo Tecnológico Industrial. Ministerio de Ciencia e Innovación (CDTI)" (Spain), BUSINESS (PET2008_0136) and PEGASO/MAGO (TIN2009-13718-C02-01) financed by the "Ministerio de Ciencia e Innovación" (Spain) and FEDER. Special acknowledgment to GREDIA (FP6 34363 - Grid enabled access to rich media content) funded by European Commission.

References

[Alexander (2003)] Alexander, I., Misuse Cases: Use Cases with Hostile Intent. IEEE Software, (2003): p. 58-66.

[Alexander and Maiden (2004)] Alexander, I. and N. Maiden, Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle. (2004): John Wiley & Sons.

[Artelsmair and Wagner (2003)] Artelsmair, C. and R. Wagner. Towards a Security Engineering Process. in The 7th World Multiconference on Systemics, Cybernetics and Informatics. (2003). Orlando, Florida, USA.

[Bass, Bachmann et al. (2004)] Bass, L., F. Bachmann, R.J. Ellison, A.P. Moore, and M. Klein, Security and survivability reasoning frameworks and architectural design tactics. SEI, (2004).

[Bradford, Grizzell et al. (2007)] Bradford, P.G., B.M. Grizzell, G.T. Jay, and J.T. Jenkins, Cap. 4. Pragmatic Security for Constrained Wireless Networks, in Security in Distributed, Grid, Mobile, and Pervasive Computing, A. Publications, Editor. (2007): The University of Alabama, Tuscaloosa, USA. p. 440.

[Breu, Burger et al. (2003)] Breu, R., K. Burger, M. Hafner, J. Jürjens, G. Popp, V. Lotz, and G.Wimmel. Key issues of a formally based process model for security engineering. in International Conference on Software and Systems Engineering and their Applications. (2003).

[Dail, Sievert et al. (2004)] Dail, H., O. Sievert, F. Berman, H. Casanova, A. YarKhan, S. Vadhiyar, J. Dongarra, C. Liu, L. Yang, D. Angulo, and I. Foster, Scheduling In The Grid Application Development Software Project, in Grid resource management:state of the art and future trends. (2004). p. 73-98.

[Firesmith (2003)] Firesmith, D.G., Security Use Cases. Journal of Object Technology, (2003): p. 53-64.

[Foster and Kesselman (2004)] Foster, I. and C. Kesselman, The Grid2: Blueprint for a Future Computing Infrastructure. (2004), San Francisco, CA: Morgan Kaufmann Publishers; 2 edition.

[Giguhre (2001)] Giguhre, E., Java 2 Micro Edition: The Ultimate Guide to Programming Handheld and Embedded Devices. (2001): John Wiley & Sons, Inc.

[Guan, Zaluska et al. (2005)] Guan, T., E. Zaluska, and D.D. Roure. A Grid Service Infrastructure for Mobile Devices. in First International Conference on Semantics, Knowledge, an Grid (SKG 2005). (2005). Beijing, China.

[Haley, Moffet et al. (2006)] Haley, C.B., J.D. Moffet, R. Laney, and B. Nuseibeh. A framework for security requirements engineering. in Software Engineering for Secure Systems Workshop. (2006). Shangai, China.

[Jameel, Kalim et al. (2005)] Jameel, H., U. Kalim, A. Sajjad, S. Lee, and T. Jeon. Mobile-To-Grid Middleware: Bridging the gap between mobile and Grid environments. in European Grid Conference EGC 2005. (2005). Amsterdam, The Netherlands: Springer.

[Jürjens (2005)] Jürjens, J., Secure Systems Development with UML. (2005): Springer. 309.

[Kolonay and Sobolewski (2004)] Kolonay, R. and M. Sobolewski. Grid Interactive Service-oriented Programming Environment. in Concurrent Engineering: The Worldwide Engineering Grid. (2004). Tsinghua, China: Press and Springer Verlag.

[Lodderstedt, Basin et al. (2002)] Lodderstedt, T., D. Basin, and J. Doser. SecureUML: A UML-Based Modeling Language for Model-Driven Security. in 5th International Conference on the Unified Modeling Language (UML), 2002. (2002). Dresden, Germany: Springer.

[Mouratidis and Giorgini (2006)] Mouratidis, H. and P. Giorgini, Integrating Security and Software Engineering: Advances and Future Vision. (2006): Idea Group Publishing.

[OMG (2007)] OMG, OMG Unified Modeling Language (OMG UML), Superstructure, V2.1.2. 2007.

[OMG (2008)] OMG, Software & Systems Process Engineering Meta-Model Specification (SPEM) 2.0. 2008.

[Park (2009)] Park, J.H., USF-PAS: Study on Core Security Technologies for Ubiquitous Security Framework. Journal of Universal Computer Science (J.UCS), (2009). 15(5): p. 1065-1080.

[Rosado, Fernández-Medina et al. (2009a)] Rosado, D.G., E. Fernández-Medina, and J. López. Applying a UML Extension to build Use Cases diagrams in a secure mobile Grid application. in 5th International Workshop on Foundations and Practices of UML, in conjunction with the 28th International Conference on Conceptual Modelling, ER 2009. (2009a). Gramado, Brasil: LNCS 5833.

[Rosado, Fernández-Medina et al. (2009b)] Rosado, D.G., E. Fernández-Medina, and J. López, Obtaining Security Requirements for a Mobile Grid System. International Journal of Grid and High Performance Computing, (2009b). 1(3): p. 1-17.

[Rosado, Fernández-Medina et al. (2009c)] Rosado, D.G., E. Fernández-Medina, and J. López. 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. (2009c). Vancouver, Canada.

[Rosado, Fernández-Medina et al. (2010a)] Rosado, D.G., E. Fernández-Medina, and J. López, Security Services Architecture for Secure Mobile Grid Systems. Journal of Systems Architecture. Special Issue on Security and Dependability Assurance of Software Architectures, (2010a).

[Rosado, Fernández-Medina et al. (2008a)] Rosado, D.G., E. Fernández-Medina, J. López, and M. Piattini. Engineering Process Based On Grid Use Cases For Mobile Grid Systems. in The Third International Conference on Software and Data Technologies- ICSOFT 2008. (2008a). Porto, Portugal.

[Rosado, Fernández-Medina et al. (2008b)] Rosado, D.G., E. Fernández-Medina, J. López, and M. Piattini. PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices. in International Conference on Availability, Reliability and Security (ARES 2008). (2008b). Barcelona, Spain: IEEE Computer Society.

[Rosado, Fernández-Medina et al. (2010b)] Rosado, D.G., E. Fernández-Medina, J. López, and M. Piattini, Analysis of Secure Mobile Grid Systems: A Systematic Approach. Information and Software Technology, (2010b). 52: p. 517-536.

[Rosado, Gutiérrez et al. (2006)] Rosado, D.G., C. Gutiérrez, E. Fernandez-Medina, and M. Piattini, Security Patterns and Requirements for Internet-based Applications. Internet Research, (2006). 16(5): p. 519-536.

[Røstad (2006)] Røstad, L. An extended misuse case notation: Including vulnerabilities and the insider threat. in XII Working Conference on Requirements Engineering: Foundation for Software Quality. (2006). Luxembourg.

[Sindre and Opdahl (2001)] Sindre, G. and A.L. Opdahl. Capturing Security Requirements by Misuse Cases. in 14th Norwegian Informatics Conference (NIK'2001). (2001). Tromsø, Norway.

[Sindre and Opdahl (2001)] Sindre, G. and A.L. Opdahl. Templates for misuse case description. in 7th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'01). (2001). Austria.

[Sindre and Opdahl (2005)] Sindre, G. and A.L. Opdahl, Eliciting security requirements with misuse cases. Requirements Engineering Journal, (2005). 10(1): p. 34-44.

[WAP Forum (2001)] WAP Forum. Wireless Transport Layer Security specification. 2001; Available from: http://www.openmobilealliance.org/tech/affiliates/wap/wap-261-wtls-20010406-a.pdf.