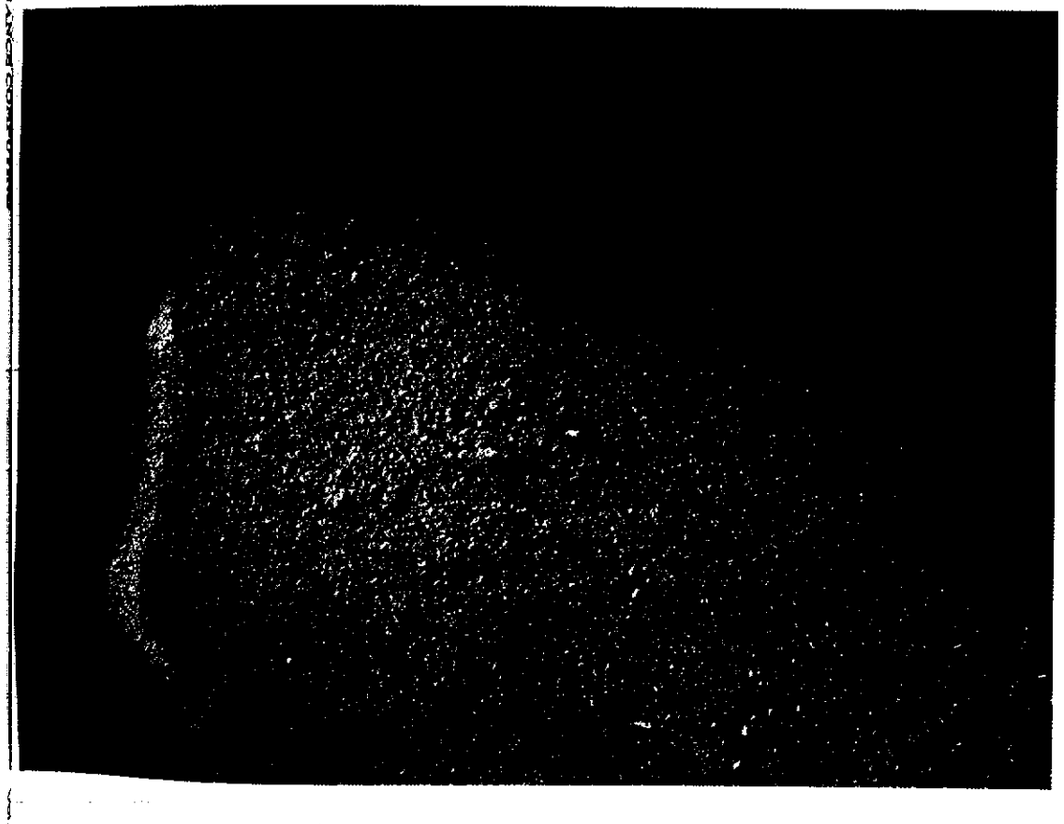
ISSN 1935572-6

Vol.1, No. 3
July - September 2009

An official publication of
the Information Resources
Management Association

INTERNATIONAL JOURNAL OF GRID AND HIGH PERFORMANCE COMPUTING

INTERNATIONAL JOURNAL OF
Grid and High Performance Computing



International Journal of Grid and High Performance Computing, 1(3), 1-17, July-September 2009 1

Obtaining Security Requirements for a Mobile Grid System

David G. Rosado, University of Castilla-La Mancha, Spain
Eduardo Fernández-Medina, University of Castilla-La Mancha, Spain
Javier López, University of Málaga, Spain
Mario Piatini, University of Castilla-La Mancha, Spain

ABSTRACT

Mobile Grid includes the characteristics of the Grid systems together with the peculiarities of Mobile Computing, with the additional feature of supporting mobile users and resources in a seamless, transparent, secure and efficient way. Security of these systems, due to their distributed and open nature, is considered a topic of great interest. In this article we present the practical results of applying a secured methodology to a real case, specifically the approach that define, identify and specify the security requirements. This methodology will help the building of a secured grid application in a systematic and iterative way. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Misuse and Use-Case Model; Mobile Grid Computing; Security; Security Requirements Analysis; Software Development Methodologies*

INTRODUCTION

Grid computing is concerned with the sharing and coordinated use of diverse resources in distributed "Virtual Organizations (VO)" (Ian Foster, Kesselman, Nick, and Tuecke, 2002). Grid manages resources and services distributed across multiple control domains (Ian Foster and Kesselman, 1999; Ian Foster et al., 2002).

Mobile computing is pervading our society and our lifestyles with a high momentum. Mobile computing with networked information systems help increase productivity and operational efficiency. This however, comes at a price. Mobile

computing with networked information systems increases the risks for sensitive information supporting critical functions in the organization which are open to attack (Talukder and Yavagal, 2006).

Mobile Grid, in relevance to both Grid and Mobile Computing, is a full inheritor of Grid with the additional feature of supporting mobile users and resources in a seamless, transparent, secure and efficient way (Litke, Skoutas, and Varvarigou, 2004). Grids and mobile Grids can be the ideal solution for many large scale applications being of dynamic nature and requiring transparency for users.

Security has been a central issue in grid computing from the outset, and has been regarded as the most significant challenge for grid computing (Humphrey, Thompson, and Jackson, 2005). The characteristics of computational grids lead to security problems that are not addressed by existing security technologies for distributed systems (Ian Foster, Kesselman, Tsudik, and Tuecke, 1998; Welch et al., 2003). Security over the mobile platform is more critical due to the open nature of wireless networks. In addition, security is more difficult to implement into a mobile platform due to the limitations of resources in these devices (Bradford, Grizzell, Jay, and Jenkins, 2007).

Because of the difficulty of incorporating mobile devices into a grid environment (Guan, Zaluska, and Roure, 2005; Jameel, Kalim, Sajjad, Lee, and Jeon, 2005; Kwok-Yan, Xi-Bin, Siu-Leung, Gu, and Jia-Guang, 2004; Sajjad et al., 2005), and by adding the appearance of a new technology where security is fundamental and the advances that mobile computation has experienced in recent years, the need to define, consider and develop a methodology or process of development appears in which, within the whole software lifecycle (Anderson, 2001; Baskerville, 1993), all the requirements and security aspects related to Mobile Grid systems are analyzed and integrated obtaining as a result a secure, robust and scalable Mobile Grid system.

In this article, we will apply the stage of security requirements analysis for obtaining a set of security requirements on a mobile grid environment for a case study of media domain where the mobile devices participate as actives resources. Using misuse cases and security use cases we obtain a vision about the threats and risks of the system and about the security requirements and mechanisms that we must use to protect to our mobile grid system.

The rest of article is organized as follows: Section II will describe some of the security requirements most important on grid environments and will identify the common attacks that can appear on a on mobile grid system. In section III, we give a brief overview of our methodology of development for mobile grid systems, we will describe the analysis stage and we will study one of the activities of this stage, the Mobile Grid Security Requirement Analysis activity. In section IV, we will present a case study and we will apply the activity of security requirements analysis for obtaining a set of security requirements for our real application. We will finish by putting forward our conclusions as well as some research lines for our future work.

SECURITY REQUIREMENTS AND ATTACKS ON A MOBILE GRID SYSTEM

Defining Security Requirements

The basic security components are comprised of mechanisms for authentication, authorization, and confidentiality of communication between grid computers. Without this functionality, the integrity and confidentiality of the data processed within the grid would be at risk.

We define the basic security requirements on grid environments, but there are many other security requirements and challenges associated with grids and mobile computing (Trusted Computing Group Administration, 2006; Vivas, López, and Montenegro, 2007) that, due to space restrictions, we do not define here:

- **Authentication:** It ensures that only valid devices and users access a given service. Authentication mechanisms and policies are supposed to constitute the basis on which local security policies can be integrated within a VO (Ian Foster et al., 1998).
- **Confidentiality:** Both privacy and intellectual property concerns require confidentiality in the use of data. Encryption is one of mechanisms used to enforce confidentiality.
- **Integrity:** It ensures that message (data) communications are not tampered with while in transit or in storage (in memory on the device, for example).
- **Authorization and access control:** In grids, local access mechanisms should be applied whenever possible, and the owner of a resource should be able to enforce local user authorization.
- **Privacy:** It is the ability to avoid information being disclosed to determined actors. Privacy also involves rules about what information can be shared among users, whether messages can be exchanged "in private," and the anonymity of users (if needed and/or desired).
- **Non-repudiation:** It refers to the inability to falsely deny the performance of some action.

All these security requirements must be identified and analyzed in the analysis stage of our methodology from the mobile grid security use cases (MGSUC) defined in this stage and that we will explain further on.

Defining Attacks on Grid Environments

According to (Enterprise Grid Alliance Security Working Group, 2005), the following include some of the threats and risks based on the unique characteristics of an enterprise Grid:

- **Access control attacks:** defines risks with unauthorized entities, as well as authorized entities, bypassing or defeating access control policy.
- **Defeating Grid auditing and accounting systems:** includes threats to the integrity of auditing and accounting systems unique to an enterprise Grid environment. This may include false event injection, overflow, event modification, and a variety of other common attacks against auditing systems.
- **Denial of Service (DoS):** this describes an attack on service or resource availability. As an enterprise Grid is often expected to provide a better availability compared to a non-Grid environment,

the following DoS threats must be considered as part of a risk assessment:

- DoS attack against the Grid component join protocol to prevent new authorized Grid components/users from successfully joining.
- Authorized Grid component or user is "forced" to leave the grid.
- User or service attempts to flood the Grid with excessive workload which may cause compute, network and/or storage components to become exhausted, or the latency to access those resources significantly impacts other Grid users.
- Altering scheduling (or other Quality of Service) priorities that have been defined for Grid components to unfairly prioritize one application/service over another.

- **Malicious code/"malware":** This describes any code that attempts to gain unauthorized access to the Grid environment, to subsequently elevate its privileges, hide its existence, disguise itself as a valid component, or propagate itself in clear violation of the security policy of the enterprise Grid.
- **Object reuse:** This describes how sensitive data may become available to an unauthorized user, and used in a context other than the one for which it was generated. In the enterprise grid context, this is a risk if a Grid component is not properly decommissioned.
- **Masquerading attacks:** describes a class of attacks where a valid Grid component may be fooled into communicating or working with another entity masquerading as valid Grid component. Such an attack could permit the disclosure or modification of information, the execution of unauthorized transactions, etc.
- **Sniffing/snooping:** involves watching packets as they travel through the network. An enterprise Grid potentially introduces additional network traffic between applications/services, the system and grid components that should be protected. Failure to address this threat may result in other types of attacks including data manipulation and replay attacks.

In addition to these, it is also necessary to adopt the general security mechanisms applicable in any enterprise scale IT infrastructure, and includes physical security to protect against threats from humans (either malicious or accidental) as well as man-made and natural catastrophes.

OVERVIEW OF OUR METHODOLOGY

Methodology of Development

Our methodology of development (Rosado, Fernández-Medina, López, and Piattini, 2008) is a systematic process that must be iterative and incremental. An iterative approach proposes an incremental understanding of the problem through successive refinements and an incremental growth of an effective solution through several versions.

The methodology to develop a systematic process will consist of different phases; each one of them will also be divided into stages, and these, in turn, into activities and tasks. This methodology has been modified and improved with regard to a first approach (Rosado et al., 2008). In this new approach we have added two repositories (general and security) where

we can include and update with artifacts, templates, patterns, elements, diagrams that are common in these environments and that we can use for future developments. Also, our methodology will be guided by specials use cases (mobile Grid use cases) with new constraints, behavior and characteristics that are compatibles with known use cases. Diagrams of mobile grid use cases will be added in our repository. A third aspect is that we build a security service oriented architecture with services, mechanisms and technologies needed for mobile grid systems.

Our methodology will initially consist of 3 phases:

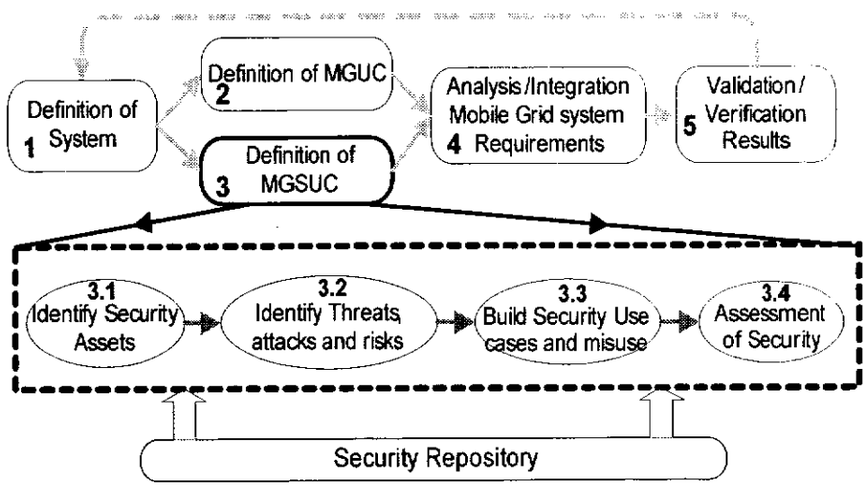
- **Planning phase:** secure mobile grid system planning stage.
- **Development phase:** secure mobile **grid system analysis stage** (Figure 1, up), secure mobile grid system design stage and secure mobile grid system construction stage.
- **Maintenance phase:** secure mobile grid system maintenance stage.

In this article, we study one of the activities of the secure mobile grid system analysis stage, the Definition of Mobile Grid Security Use Cases activity whose tasks can be seen in Figure 1 (bottom). In this activity (activity 3 of Figure 1) we identify threats and risks related to mobile grid environments which attack assets that we want to protect, and we build the diagrams of security use cases and misuse for mobile grid environments considering these assets, threats and attacks.

Secure Mobile Grid System Analysis Stage

In this subsection, we will describe the analysis stage, enumerating and describing briefly what activities are parts of this stage. This analysis stage is composed of five activities (see Figure 1):

Figure 1. Tasks of the "mobile Grid security requirements analysis" activity



- **Definition of Mobile Grid System.** It describes the system by adapting the previous results and limiting the reach of it to identify standards, norms and tools.
- **Definition of Mobile Grid Use Cases (MGUC).** The purpose of this activity is to build a diagram of use cases where we can identify the necessities and requirements of both users and the mobile Grid environment. There are diagrams of use cases in the general repository that we can use for building our diagram.
- **Definition of Mobile Grid Security Use Cases (MGSUC).** It builds diagrams of security use cases and misuse for identifying the security requirements of our system, analyzing the threats that the attackers can carry out and assessment risks for the mobile Grid system. We will define this activity in the next subsection.
- **Mobile Grid System Requirements Analysis.** It specifies both functional and non-functional (excluding security) requirements from MGUC. Also, it specifies security requirements from MGSUC and integrates them into a specification of requirements of the final application.
- **Validation and Verification of Results.** During the course of some designs, requirements can change at the last minute or may go undiscovered. Requirements also have a way of changing when you least expect them to, so it is always a good idea to validate them before you proceed. This activity validates the results obtained from the analysis as well as approves the analysis of the system.

Once we have described the activities of the analysis stage, we will explain activity 3, which is in charge of analyzing security requirements for the mobile grid system, and we apply the tasks of this activity in a case study.

Activity 3: Definition of Mobile Grid Security Use Cases (MGSUC)

The aim of this activity is to obtain a set of security requirements, validated and specified that we will have to use and to manage in the next stages or activities of the methodology. This analysis is centered on the specific security requirements of Grid and mobile computing (section 2.A) which are requirements with special characteristics and poorly studied. For this reason, we aim to analyze the security requirements that we can find when we build a secure mobile grid system. A set of tasks (see Figure 1) will serve as a guide for defining and specifying security requirements for mobile grid systems:

- **Task 3.1: Identify Security Assets**: The security assets for a grid with mobile devices depend on the characteristics and type of system to be built. The CPU-intensive applications will consider resources as main assets while data-intensive applications will consider data as main assets to protect.
- **Task 3.2: Identify Threats, Attacks and Risks**. The threats analysis is the process of identifying, as many risks that can affect the assets as possible. A well-done threat analysis performed by experienced people would likely identify most known risks, providing a level of confidence in the system that will allow the business to proceed.

In section 2.B we defined the most important threats and attacks for these environments.

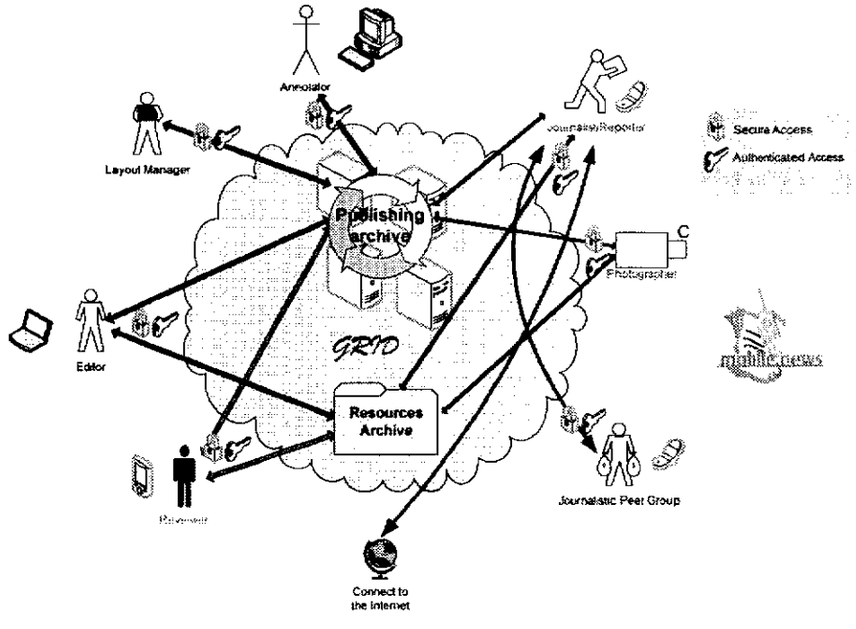
- **Task 3.3: Build Security Use Cases and Misuse**: Once we have identified the threats and vulnerabilities for Grid environments and mobile computation, we can build, using security use cases and misuse cases, a diagram of mobile Grid security use cases where threats, attacks and security are expressed and represented in the diagram indicating the assets to protect, the security objectives to achieve and the security requirements that the system must fulfill (defined in section 2.A).
- **Task 3.4: Assessment of Security**: It is necessary to assess whether the threats are relevant according to the security level specified by the security objectives. Then, we have to estimate the security risks based on the relevant threats, their likelihood and their potential negative impacts, in other words, we have to estimate the impact (what may happen) and risk (what will probably happen) which the assets in the system are exposed to. We have to interpret the meaning of impact and risk.

The aim of this activity is build diagrams of security use cases correctly defined where all security requirements of our system are represented and identified.

CASE STUDY

Our development methodology will be validated with a business application in the Media domain (see Figure 2) attempting to solve existing problems in this domain.

Figure 2. Mobile Grid computing system for media application



The methodology will help us to build a Mobile Grid application, which will allow journalists and photographers (actors of media domain) to make their work available to a trusted network of peers the same instant it is produced, either from desktop or mobile devices.

With the explosion of ultra portable photo/video capture media (i.e. based on mobile phones, PDAs or solid state camcorders) everyone can capture reasonably good quality audiovisual material while on the move. We want 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. This user needs to safely and quickly upload the media to a secure server to make it easier for others to access, and to avoid situations where his device's battery dies or another malfunction destroys or makes his media unavailable.

In the media domain, both the distributions of content, and the need for rapid access to this content, are apparent. News is inherently distributed everywhere and its value falls geometrically with time. These two reasons make the need for Grid technology evident in both scenarios which represent, however, a plethora of relevant business cases which share these two common characteristics: the need for fast access to distributed content.

Following the process of analysis defined in the definition of mobile grid security use cases activity aforementioned, we will identify and analyze security requirements involved in this case study helping of security repository and mobile grid security uses cases. For all possible use cases defined for this application, we are only going to consider three use cases (due to space constraints), defined in Table 1, which we are going to work with in the following tasks.]

Initially our security repository contains several generic security use cases that we can adapt to our necessities (behavior, relations, restrictions, etc.), set of diagrams of security use cases and misuse which we can reuse modifying the relations, adding news security use cases and restrictions until adapting to the application requirements. Also, in the security repository, templates of threats, attacks, vulnerabilities, risk scenarios, and other security elements are defined. For example, the diagram of security use cases that we can use for building our own diagram of security use cases is shown in Figure 3 (an analysis more detailed as future work).

We describe a security scenario where we present use cases, misuse cases that can attack to the identified use cases, and the security use cases associated both with use cases and misuse cases for protecting the system of these misuse cases, using the security use cases defined in the security repository.

Having identified these use cases, we can carry out a first iteration of our methodology, identifying the security requirements associated with these use cases and identifying and defining the rest of them in later iterations where a new refinement will be realized. Next, we will execute this process or set of tasks for analyzing all security requirements for the media domain in this case study.

Task 3.1: Identify Security Assets

On mobile Grid environments we can identify a set of assets that we must protect for obtaining a secure grid system, which are the following: User and system data (stored, transmitted); Identity information;

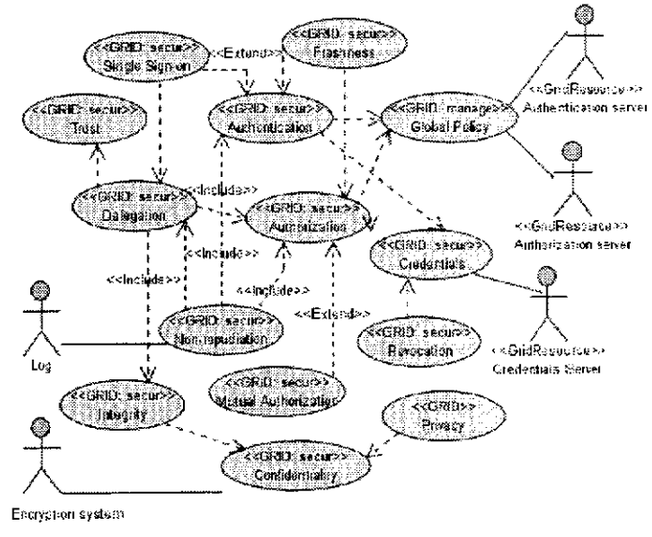
Table 1. Use cases

Use Case Name	**Login to the system**
Goals/Description	Provide authentication mechanisms
Scenario example	All users log in to the grid system
Description	- A user launches the Grid application - The user provides username and password - The system checks the user data and permits or denies entry to the system

Use Case Name	**Search for news**
Goals/Description	A journalist can search for news material through the system interface in: 1. public sources 2. his organisation's historical archive 3. trusted commercial portals according to the subscriptions paid-for.
Scenario example	The journalist familiarizes himself with the topic
Description	- A user formulates a search query - The user selects sources to search from a list - The user submits the query

Use Case Name	**Get query results**
Goals/Description	Receive query results from available repositories
Scenario example	The Journalist receives a list with the results of the search query
Description	- The system returns results based on the metadata description of the stored material. - Results can be sorted according to the journalist's needs, such as thematic groups. - Visualization of results is based on the end user device capabilities (low resolution video for mobile devices)

Figure 3. Example of Grid security use cases inside of the security repository



Credentials (private keys, passwords); Accounting; CPU-/Storage-/Mobile devices-/ Network-resources; General system.

In a first iteration of our case study, we define the most important assets related to use cases aforementioned that we must protect and that are the reference for the identification of threats, attacks and security use cases. These assets are:

- Personal information about the journalist or editors: name, age, address, subscriptions, salaries.
- Media information used: photos, articles, recordings, videos, intellectual property rights.
- Exchange information: messages, queries, transactions.

Task 3.2: Identify Threats, Attacks and Risks

Examples of threats are unauthorized disclosure of information, attacks to the content of a message through wireless links, denial-of-service attacks, network authentication related attacks, physical node attacks, alteration of information, and so on. In Table 2 we can see the threats considered for the assets identified on mobile grid environments.

For our case study we can identify threats associated with security assets identified in previous task. The threats and attacks can be described with misuse cases as shown in Figure 4.

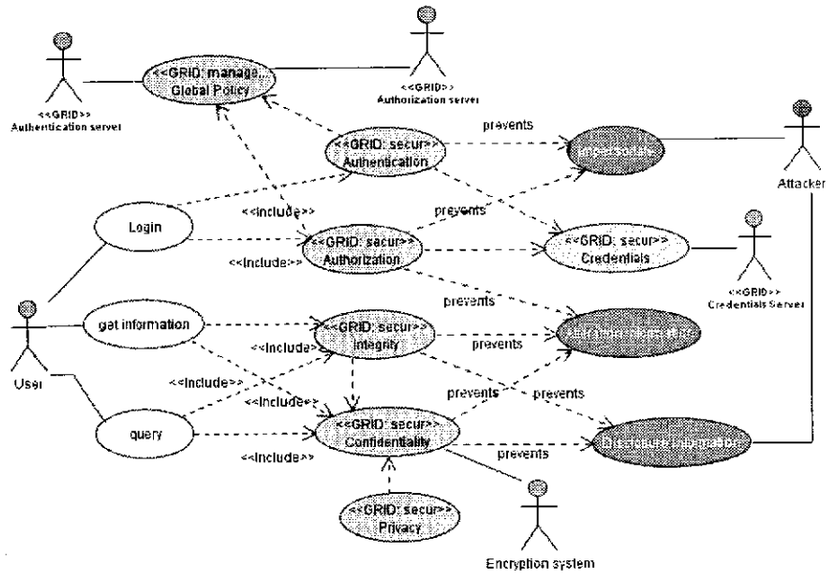
In our first iteration, we identify several possible types of threats to Information:

- Unauthorized access to grid system. In this scenario, the user wants login to the system, so that we must ensure authorized access.
- Unauthorized disclosure and alteration of information. The user can send information to the system or receive from the system, so that we must protect the information both transmitted or storage. Also we must protect the personal information that is transported through credentials.
- Unauthorized unavailability to resources. The user must have available resources anytime and anywhere.

Table 2. Security threats on mobile grid environments

Assets	Threats
User and system data (stored, transmitted)	- Unauthorised access (stored data) - Eavesdropping (transmitted data) - Unauthorised publishing - Manipulation - Erroneous data
Identity information	- Eavesdropping - Manipulation
Credentials (private keys, passwords)	- Theft / Spoofing (masquerade as a certain user, illegal use of software) - Publishing
Accounting	- Manipulation of log entries, CPU/memory usage, number and size of processes - Acquire information about competitor's work
CPU-/Storage-/Mobile devices-/ Network-resources	- Misusage (e.g. Spambot) - Denial of Service
General System	- Security holes / exploits - Malicious / compromised resources - Backdoors, viruses, worms, Trojan horses

Figure 4. Use cases, misuse cases and security use cases for the case study



In a first iteration we are going to consider these threats for the assets identified in task 3.1 as the most important that they damage and attack to our assets. We can show these threats in form of misuse cases and as these threats and misuse cases are common to grid environments and mobile computing, in our security repository will be defined and we can use for our application.

Task 3.3: Build Security Case Use and Misuse

Once we have identified and defined the treats, attacks, risks, and once we have a detailed definition of misuse cases and security use cases in our security repository, we can start to build the diagram of security use cases and misuse cases (diagram reduced) for this application. The Figure 4 shows the diagram of security use cases and misuse cases together with use cases defined in Table 1. We can see how a subset of the diagram of Mobile Grid security use cases shown in Figure 3 is used.

In Table 3 (stored in security repository) we can see the misuse cases specification for unauthorized modification of information which occurs, for example, when a mis-user attacks the content of a message,

Table 3. Misuse cases

Misuse Case	Modification of information
Attack	Attack on the content of a message (integrity).
Summary	The external attacker type gains access to the message exchanged between the journalist and the Grid system, and modifies the part of the message that contains the media information with the intention of changing its meaning by modifying some aspect of the information like authors, dates, or secrecy information.
Preconditions	
1)	The external attacker has physical access to the message.
2)	The external attacker has a clear knowledge of where the secrecy information is located within the message.
Interactions	
1 User Interactions	The journalist sends a query message for obtaining media information
2 Misuser Interactions	The external attacker intercepts it and identifies the part of the message to modify the media information and he/she forwards it on to media Grid
3 System Interactions	Media Grid receives the corrupted message and processes it incorrectly due to its altered semantic content. That is, it establishes that the journalist wishes as new media information that media information which had been modified by the attacker
Postconditions	
1)	Media grid will remain in a state of error with regard to the original intentions of the journalist.
2)	In the register of the system in which media grid was executed, the request received with an altered semantic content will be reflected.

Misuse Case	Interception of information
Attack	Attack on the confidentiality of a message from grid system to user
Summary	The external attacker type gains access to the message exchanged between the journalist and the Grid system, and reads a specific piece of information.
Preconditions	
1)	The external attacker has physical access to the message.
Interactions	
1 User Interactions	The journalist sends a query message for obtaining media information
2 System Interactions	Grid system receives the query message and processes it. Grid system returns the media information related with the query to the journalist
3 Misuser Interactions	The external attacker intercepts it and reads the part of the message that contains the media information and he/she forwards it on to journalist
4 User Interactions	The journalist wishes as new media information that media information which had been intercepted by the attacker.
Postconditions	
1)	Grid system will remain in a normal state and the journalist continues without realizing the interception of information by the attacker

and also the misuse case specification for unauthorized interception of information which occurs when a misuser attacks the confidentiality of a message. These misuse cases have associated security use cases that define the sequence of steps that should be carried out to avoid misuse cases that they are associated with. Table 4 describes these security use cases that ensure message integrity preventing a misuser from corrupting a message and, message confidentiality preventing a misuser from having the means to intercept a message, respectively.

Once the diagram is built and the relations, constraints, stereotypes and tagged values are defined, we can obtain and specify the security requirements for this application.

Task 3.4: Assessment of Security

In Table 5 we define the impact and risk for two of these threats. For the time being, we are going to evaluate risk and impact with five possible values: Very Low, Low, Medium, High and Very High. The likelihood of a threat could be: Very Frequent (daily event), Frequent (monthly event), Normal (once a year), Rare (once in several years).

For alteration and disclosure of information we can see that if the information is sensitive (personal data, bank data), these treats represent a high risk for our system and we must ensure that attacks (modifying or altering information) do not attain their objectives. In this case we must strongly protect the information stored and transmitted between user and system. This assessment must be present in the next stages and activities and it must take into account when we design the security service oriented architecture.

CONCLUSION

The interest in incorporating mobile devices into Grid systems has arisen with two main purposes. The first one is to enrich users of these devices while the other is that of enriching the Grid's own infrastructure. Both benefit from this fact since, on the one hand, the Grid offers its services to mobile users to complete their work in a fast and simple way and, on the other hand, the mobile devices offer their limited resources, but millions of them, in any place and at any time, endorsed by the fast advance in the yield and capacity that is being carried out in mobile technology.

In many cases, constrained wireless networks are made up of devices that are physically constrained and therefore have little room for memory, batteries, and auxiliary chips. Security over the mobile platform is more critical due to the open nature of wireless networks. In addition, security is more difficult to implement into a mobile platform due to the limitations of resources in these devices.

Due to this difficulty when we want to incorporate mobile devices into a grid system and due to the fact that we must take into account security aspects throughout the life cycle, it is necessary to provide a systematic process to developers for building this kind of system considering grid characteristics, mobile computing and security aspects throughout the development process. This process must always be flexible, scalable and dynamic, so that it adapts itself to the ever-changing necessities of mobile Grid systems.

In this article we have presented a methodology for designing and building a secure mobile grid system based on an iterative and incremental process. This

Table 4. Security use cases

Security Use Case		Ensure Integrity
Use Case Path		System Message Integrity
Security Threat		A misuser corrupts a message from the system to a user.
Preconditions		
1)	The misuser has the means to intercept a message from the system to a user.	
2)	The misuser has the means to modify an intercepted message.	
3)	The misuser has the means to forward the modified message to the user.	
Interactions		
1	System Interactions	The system sends a message to a user.
	System Actions	The system ensures that modifications to the message will be obvious to the user
2	Misuser Interactions	The misuser intercepts and modifies the system's message and forwards it on to the user.
3	User Interactions	The user receives the corrupted message.
	System Actions	The system will recognize that the message was corrupted.
4	System Interactions	The system will notify the user that the message was corrupted
Postconditions		None

Security Use Case		Ensure Confidentiality
Use Case Path		User Message Privacy
Security Threat		Misuser accesses private message from the user to the system
Preconditions		
1)	The misuser has the means to intercept a message from the user to the system	
2)	The system has requested private information from the user.	
Interactions		
1	User Interactions	The user sends a private message to the system.
2	System Actions	The system makes the private message illegible while in transit.
3	Misuser Interactions	The misuser intercepts the user's private message.
Postconditions		The misuser cannot read the user's private message

methodology is composed of several stages and activities and in each one of them the stakeholders carry out their tasks. An important phase of the methodology is the security requirements analysis which we have proposed with a set of tasks to obtain security requirements for mobile grid systems based in security use cases. Considering a case study for media domain, we have applied the analysis activity for analyzing security requirements in this real application using techniques of uses cases,

Table 5. Threats, attacks and risks

Threat	Unauthorised alteration of information	
Impact	LOW if there is no personal information modified	HIGH if the opposite is the case
Attack	Modification of information	
Probability	Frequent	Frequent
Risk	LOW	HIGH
Threat	Unauthorised disclosure of information	
Impact	LOW when the disclosed information is not sensitive or important	HIGH if the opposite is the case
Attack	Interception of information	
Probability	Frequent	Very Frequent
Risk	LOW	HIGH

misuse cases, security use cases and risk assessment where we obtain a specification of security requirements of our system analyzed on several refinements.

Applying this set of tasks we have been able to incorporate security requirements into our analysis and into our system. The application of this case study has allowed us to improve and refine some tasks of the security requirements analysis activity.

As a future project we will define in depth all stages of the methodology and we will use our case study to apply the activities and tasks to analyzing and studying the obtained results so that they will be validated with the expected outcome. Also we will define the diagrams of security use cases that serve us as templates in our own diagrams of security use cases and misuse.

ACKNOWLEDGMENT

This research is part of the following projects: MISTICO (PBC-06-0082) and QUASIMODO (PAC08-0157-0668) financed by FEDER and by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha" (Spain), and ESFINGE (TIN2006-15175-C05-05) granted by the "Dirección General de Investigación del Ministerio de Educación y Ciencia" (Spain). Special acknowledgment to GREDIA (FP6-IST-034363) funded by European Commission.

REFERENCES

Anderson, R. (2001). *Security Engineering - A Guide to Building Dependable Distributed Systems*: John Wiley&Sons.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys, 25*(4), 375 - 414.

Bradford, P. G., Grizzell, B. M., Jay, G. T., & Jenkins, J. T. (2007). Cap. 4. Pragmatic Security for Constrained Wireless Networks. In A. Publications (Ed.), *Security in Distributed, Grid, Mobile, and Pervasive Computing* (pp. 440). The University of Alabama, Tuscaloosa, USA.

Enterprise Grid Alliance Security Working Group. (2005, 8 July 2005). *Enterprise Grid Security Requirements Verison 1.0*

Foster, I., & Kesselman, C. (1999). Globus: A Toolkit-Based Grid Architecture. In *The Grid: Blueprint for a New Computing Infrastructure* (pp. 259-278): Morgan Kaufmann.

Foster, I., Kesselman, C., Nick, J. M., & Tuecke, S. (2002). Grid services for distributed system integration. *Computer, 35*(6), 37-46.

Foster, I., Kesselman, C., Tsudik, G., & Tuecke, S. (1998). *A Security Architecture for Computational Grids.* Paper presented at the 5th ACM Conference on Computer and Communications Security, San Francisco, USA.

Guan, T., Zaluska, E., & Roure, D. D. (2005). *A Grid Service Infrastructure for Mobile Devices.* Paper presented at the First International Conference on Semantics, Knowledge, an Grid (SKG 2005), Beijing, China.

Humphrey, M., Thompson, M. R., & Jackson, K. R. (2005). Security for Grids. *Lawrence Berkeley National Laboratory. Paper LBNL-54853.*

Jameel, H., Kalim, U., Sajjad, A., Lee, S., & Jeon, T. (2005, February 14-16). *Mobile-To-Grid Middleware: Bridging the gap between mobile and Grid environments.* Paper presented at the European Grid Conference EGC 2005, Amsterdam, The Netherlands.

Kwok-Yan, L., Xi-Bin, Z., Siu-Leung, C., Gu, M., & Jia-Guang, S. (2004). Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes. *Lecture Notes in Computer Science, 2908/2003*, 42-54.

Litke, A., Skoutas, D., & Varvarigou, T. (2004, December). *Mobile Grid Computing: Changes and Challenges of Resourse Management in a Mobile Grid Environment.* Paper presented at the 5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004).

Rosado, D. G., Fernández-Medina, E., López, J., & Piattini, M. (2008). *PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices.* Paper presented at the International Conference on Availability, Reliability and Security (ARES 2008), Barcelona, Spain.

Sajjad, A., Jameel, H., Kalim, U., Han, S. M., Lee, Y.-K., & Lee, S. (2005). *AutoMAGI - an Autonomic middleware for enabling Mobile Access to Grid Infrastructure.* Paper presented at the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services - (icas-icns'05).

Talukder, A., & Yavagal, R. (2006). Chapter 18: Security issues in mobile computing. In *Mobile Computing*: McGraw-Hill Professional.

Trusted Computing Group Administration. (2006). Securing Mobile Devices on Converged Networks.

Vivas, J. L., López, J., & Montenegro, J. A. (2007). Cap. 12. Grid Security Architecture: Requirements,fundamentals, standards, and models. In A. Publications (Ed.), *Security in Distributed, Grid, Mobile, and Pervasive Computing* (pp. 440). Tuscaloosa, USA.

Welch, V., Siebenlist, F., Foster, I., Bresnahan, J., Czajkowski, K., Gawor, J., et al. (2003, 22-24 June 2003). *Security for Grid services.* Paper presented at the 12th IEEE International Symposium on High Performance Distributed Computing (HPDC-12 '03).

David G. Rosado has an MSc in computer science from the University of Málaga (Spain) and currently he is a PhD student at the University of Castilla-La Mancha. His research activities are focused on security architectures for information systems and mobile Grid computing. He has published several papers in national and international conferences on these subjects. He is a member of the ALARCOS research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.

*Eduardo Fernández-Medina holds a PhD and an MSc in computer science from the University of Sevilla. He is an associate professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in databases, datawarehouses, web services and information systems, and also in security metrics. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences (DEXA, CAISE, UML, ER, etc.). Author of several manuscripts in national and international journals (*Information Software Technology, Computers and Security, Information Systems Security, *etc.), he is a member of the ALARCOS research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain. He belongs to various professional and research associations (ATI, AEC, ISO, IFIP WG11.3 etc.).*

Javier Lopez received his MS and PhD degrees in computer science in 1992 and 2000, respectively, from the University of Malaga, where he currently is a full professor. His research activities are mainly focused on network security and critical information infrastructures, and he leads national and international research projects in those areas. He is also co-editor in chief of Springer's International Journal of Information Security *(IJIS), a member of the editorial boards of international journals, and the Spanish representative on the IFIP Technical Committee 11 on security and protection in information systems.*

Mario Piattini has an MSc and a PhD in computer science from the Politechnical University of Madrid. He is a certified information system auditor from the ISACA (Information System Audit and Control Association). Full professor at the Escuela Superior de Informática of the Castilla-La Mancha University (Spain) and author of several books and papers on databases, software engineering and information systems, Piattini leads the ALARCOS research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain. His research interests are: advanced database design, database quality, software metrics, object- oriented metrics and software maintenance.