ENGINEERING PROCESS BASED ON GRID USE CASES FOR MOBILE GRID SYSTEMS

David G. Rosado, Eduardo Fernández-Medina, Mario Piattini
University of Castilla-La Mancha, Alarcos Research Group – Institute of Information Technologies & Systems
Dep. of Information Technologies & Systems – Escuela Superior de Informática, Ciudad Real, Spain

Javier López
Computer Science Department, University of Málaga, 29071, Málaga, Spain

Keywords: Development process, Use cases, Security Use cases, Security Service Oriented Architecture, Grid computing, Mobile computing.

Abstract: The interest to incorporate 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 own Grid infrastructure. Security of these systems, due to their distributed and open nature, is considered a topic of great interest. A formal approach to security in the software life cycle is essential to protect corporate resources. However, little attention has been paid to this aspect of software development. Due to its criticality, security should be integrated as a formal approach into the software life cycle. We are developing a methodology of development for secure mobile Grid computing based systems that helps to design and build secure Grid systems with support for mobile devices directed by use cases and security use cases and focused on service-oriented security architecture. In this paper, we will present one of the first steps of our methodology consisting of analyzing security requirements of mobile grid systems. This analysis will allow us to obtain a set of security requirements that our methodology must cover and implement.

1 INTRODUCTION

Grid computing is already a mainstream paradigm for resource-intensive scientific applications, but it also promises to become the future model for enterprise applications. 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 to meet variable demands (Foster and Kesselman, 1999).

Today, the development of wireless technology and mobile devices enables us to access the network service from anywhere at any time (Bruneo, Scarpa et al., 2003). Provided that mobile devices have limited computing capacity, the Grid becomes an important computation service provider that enables mobile users to perform complicated jobs (Trung, Moon et al., 2005). On the other hand, the performances of current mobile devices have significantly increased, reason why laptops and PDAs can provide aggregated computational capability when gathered in hotspots, forming a Grid on site. 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 et al., 2004; Guan, Zaluska et al., 2005; Jameel, Kalim et al., 2005).

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 et al., 2005). 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 et al., 2007). Therefore, a Grid infrastructure that supports the participation of mobile nodes will play a significant role in the development of Grid computing.

G. Rosado D., Fernández-Medina E., Piattini M. and López J. (2008).
ENGINEERING PROCESS BASED ON GRID USE CASES FOR MOBILE GRID SYSTEMS.
In *Proceedings of the Third International Conference on Software and Data Technologies - SE/GSDCA/MUSE*, pages 146-151
DOI: 10.5220/0001879901460151

A Grid system is a software that has been developed by means of a certain technology and that fulfills a set of characteristics and own functionalities of the Grid. As it is a software, the problems that have arisen and given rise to numerous researches in the last years are those of considering and integrating security into the whole software lifecycle (Baskerville, 1993; Anderson, 2001). In addition, if we add the appearance of a new technology where security is fundamental and the advance that mobile computation has experienced in the last years, it appears the need to define, consider and develop a methodology or process of development in which security is integrated from the first stages of development, obtaining as a result, a secure, robust and scalable Mobile Grid system.

In this paper we want to describe a development process directed by special use cases for mobile grid systems that will help us to identify the necessities and requirements of these environments from initial states and that they will guide us toward the construction of secure service oriented architecture supporting mobile devices and offering security grid services. This methodology has two (general and security) reusable repositories containing artefacts, elements, diagrams of use cases, mechanisms, patterns, templates, and so on, both general and security aspects, that we can use in any stages or activities of our methodology making the development easier.

The rest of paper is organized as follows: In section 2, we will show an overview of our development methodology for secure mobile grid systems. Section 3 will present the main contribution of the paper, which is the analysis process of our methodology of development. We will explain the analysis stage and we will describe in detail one of the activities of this analysis stage, the activity of building security use cases. We will finish by putting forward our conclusions as well as some research lines for our future work in section 4.

2 METHODOLOGY OF DEVELOPMENT

Our objective is to provide developers with firstly, a methodology or development systematic process that will include the complete development of Mobile Grid systems of whatever complexity and magnitude, and secondly, an architecture that helps them to develop a secure mobile Grid system in an ordered and systematic way. The systematic process that we have developed is an iterative, incremental and reusable process. This methodology has been modified and improved with regard to a first approach (Rosado, Fernández-Medina et al., 2008), and it will consist of 3 phases (see Figure 1): planning, development and maintenance of a secure mobile Grid system. In all of them we use elements of the repositories for completing each phase or stage. We briefly describe the phases of our methodology emphasizing the features of mobile grid that are necessary in each phase:

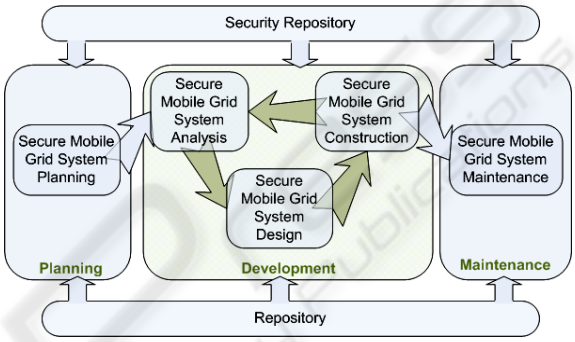

Figure 1: Methodology of development for secure mobile grid systems.

The planning phase is composed of the *Secure Mobile Grid System Planning stage*, where it is important to understand exactly which components of the grid must be rigorously secured to detect any kind of attack. Technology considerations are important in deploying a grid and it is essential to understand how the departments within an organization interact, operate, and contribute to the whole.

The development phase is composed of three stages: analysis, design and construction.

- The *Secure Mobile Grid System Analysis stage* is centred in building diagrams of use cases and security use cases of our system identifying and analyzing requirements and security requirements of our systems to build. These use cases must be defined for mobile grid applications (stereotypes, constraints, relations, behaviour, etc.). This stage will be described in detail in section 3.
- In the *Secure Mobile Grid System Design stage*, we must build a security architecture offering the necessary security services that fulfill and cover the security requirements identified in the previous stage. This architecture will be a service-oriented architecture where we define a collection of basic security services

supporting the security requirements of mobile devices in Grid environments. Moreover, we need to identify what security mechanisms, protocols and policies will be used for designing the basic security services.

- In the *Secure Mobile Grid System Construction stage*, we must implement the basic security services together with security mechanisms and protocols for our secure service-oriented architecture. We must study the Grid Security Infrastructure (GSI) that provides methods for authentication of Grid users and secure communication. It is based on SSL (Secure Sockets Layer), PKI (Public Key Infrastructure) and X.509 Certificate Architecture. The system to be developed is composed of mobile devices and resources which altogether set up a mobile grid system. The wireless technology will be essential for the communication between devices.

The maintenance phase is composed of the *Secure Mobile Grid System Maintenance stage*, where a plan of maintenance of the system for its later modification is defined according to the new necessities of the client. If a new organization want to take part of system, or if someone wants to add or to eliminate resources of Grid, the viability of the proposed change must be studied identifying which part of the system is affected and who must take part in its correction, being this change able to be accepted or denied depending on the reach of it.

3 SECURE MOBILE GRID SYSTEM ANALYSIS STAGE

In this section, we will analyze the most common security requirements and challenges associated with the above-defined mobile grids. Applications and their requirements should be analyzed to understand how they could be designed and developed to reap the benefits of a mobile grid. We propose an analysis stage oriented by Grid use cases which are special use cases (stereotypes) where we define constraints and properties that are necessary to define when we are working with mobile devices in Grid environments. This analysis stage will use a reuse repository where diagrams of Grid use cases for Grid applications (CPU intensive, data intensive, collaborative, and so on) are defined and prepared to be used in the design of the diagram of use cases for any mobile Grid application. We define six types: <<Grid: sch>> indicating that the use case belong to the scheduler package; <<Grid: res>> indicating that the use case belong to the resource package; <<Grid: data>> indicating that the use case belong to the data package; <<Grid: manage>> indicating that the use case belong to the management package; <<Grid: secur>> indicating that the use case belong to the security package; and <<Grid: info>> indicating that the use case belong to the information package. The relations between use cases are defined in the repository and we can add new relations or add new actors or constraints for building our own diagram for our application.

This stage analyzes security requirements through grid use cases that we must build for our application using the diagrams of grid use cases of the repository and defining the interfaces and relations between use cases until a full diagram of grid use cases for our application is built. We will describe the analysis stage in a general way and we will study in depth one of the activities of this stage related to the analysis of security requirements that will be explained in the following subsection. Now we will explain the most important (see Figure 2):

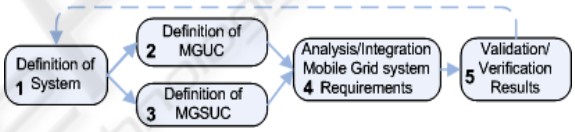

Figure 2: Activities of the Secure Mobile Grid System Analysis stage

- *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.
- *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. 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 defining security use cases for the mobile grid system.

3.1 Definition of Mobile Grid Security Use Cases (MGSUC)

The analysis stage of our methodology has a set of activities (see Figure 2) analyzing the requirements of mobile grid systems. One of them (activity 3) is devoted to define and build a diagram of security use cases that will serve to specify the security requirements for this kind of systems. A study of security requirements in the analysis stage is necessary for building a secure system, identifying and analyzing security from early stages of life cycle. Once the diagram is built, we can formally specify the security requirements that we can extract from the security use cases. A set of tasks will serve us as a guide for defining and building the security use cases and misuse cases for mobile grid systems:

3.1.1 Identify Security Assets: Task 3.1

The security assets for a grid with mobile devices depend on the characteristics and type of system to build, but the most important assets to protect will be exchanged data, resources of each participant organization, communication between mobile devices and the grid, and personal information. The CPU-intensive applications will consider resources as main assets while data-intensive applications will consider data as main assets to protect.

3.1.2 Identify Threats, Vulnerabilities and Risks: Task 3.2

We can consider the security threats related to any open network and others related to the mobile communications. The security threats that are usually present in the mobile and open networks are the following: eavesdropping, communication jamming, injection and modification of data, interruption, unauthorized access, repudiation, shoulder surfing, lost mobile terminal, stolen mobile terminal, unprepared communication shutdown, misreading and input error. The most important security attacks for Grid are as follows: user credentials attacks, man in the middle, credentials compromise and/or replay, session hijack, SOAP routing detour, attributes/credentials probing and brute force attacks, improper key and privileges management and control, etc.

In the security repository there are a set of threats, vulnerabilities and risks either identified from the beginning or that have been added during the development. These vulnerabilitities and risks are well-known for mobile computing and Grid computing. If there are new threats for this application, we must define them and update the repository with these new threats extending and improving the security repository for future developments.

3.1.3 Build Diagrams of Security Use Cases and Misuse Cases: Task 3.3

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.

In this task, we can use artifacts from our security repository such as reference diagrams of security use cases and misuse cases for Mobile Grid system that have been built in initial phases of development or updated in several activities and tasks of our methodology. These reference diagrams are general diagrams for any mobile Grid application therefore, we must adapt them to our necessities modifying, adding or deleting relations, constraints and security cases until obtaining a diagram of security use cases for our application that serves for specifying security requirements in next tasks or activities of this stage.

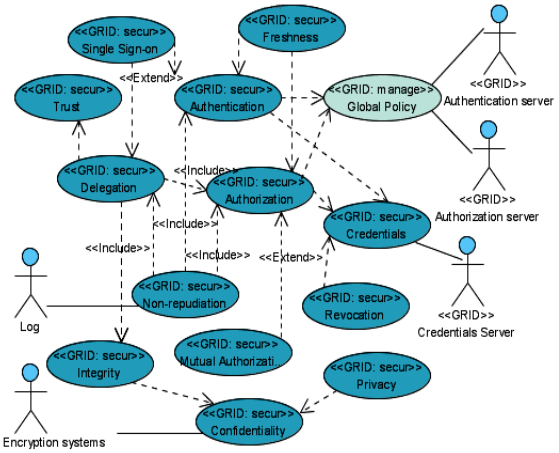

Figure 3: Grid Security Use Cases inside of the security repository

In figure 3, we can see the general diagram for Mobile Grid security use cases with the external

actors implicated and the security use cases that we believe fundamental. Based on this information, we use the use cases and their relations and constraints for building our diagram of security use cases covering the initial necessities and requirements, and the resultant diagram integrates them into the final diagram of use cases for the secure mobile Grid application.

3.1.4 Assessment of Security (Threats, Risks and Countermeasures): Task 3.4

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. In order to carry out this task, we will use a technique proposed by the guide of techniques of MAGERIT (MAP, 2006) and which is based on tables to analyze impact and risk of threats.

For example, if an alteration of information occurs, we must analyze if the information that has been modified implies low impact and risk, or on the contrary it implies high impact and risk.

3.2 Analysis/Integration of Mobile Grid Systems Requirements

This activity will have as result a security requirements specification for our application and they have been obtained from use cases and security use cases that we have build using components and models of repositories (general and security) where we can update and add with news elements that we believe important for future developments of this kind of applications. So, for example, we must obtain a set of security requirements that will be some of the most important security requirements and challenges associated with grids and mobile computing (ITU, 2004; Trusted Computing Group Administration, 2006; Vivas, López et al., 2007): Authentication, Confidentiality, Integrity, Authorization and access control, Trust, Single sign-on, privilege delegation, Non-repudiation, interoperability, Usability, Availability, and so on.

All these factors are at play in the Grid, wireless and mobile device world. There are many shared security requirements both grid environments and mobile computing, and there are others one that are exclusives and depend of our application, depending of the point of view that we consider (see Table 1).

Table 1: Security requirements from several points of view.

Security Requirements	Points of View			
	Grid	Mobile computing	Mobile user	Grid service provider
Authentication	X	X		X
Confidentiality	X	X	X	X
Message Integrity	X			
Data Integrity		X	X	X
Access Control	X	X	X	X
Single sign-on	X			
Delegation	X			
Non-repudiation	X	X	X	X
Trust	X	X		
Availability		X	X	X
Anonymity			X	
Privacy	X		X	
Identity Management	X		X	
Accounting	X	X		
Credentials	X			
Interoperability	X	X		
Usability	X		X	

We have the purpose of developing and building a secure mobile grid system, we must consider these security factors within our methodology, identifying and analyzing them in the analysis stage, which will be shown below, extracting them from the security use cases and integrating security mechanisms, protocols and policies into our security architecture that covers all these requirements. ITU_T X.800 Recommendation provides not only a general description of security services but also the related mechanisms that may be used to provide these services. These services will be the security services of our service-oriented architecture (design stage of our methodology) where are well-defined obtaining a reference security architecture that offers security services to mobile users aimed at using grid services sharing and coordinating mobile resources for all members of the Grid.

4 CONCLUSIONS

In mobile environments the context is extremely dynamic and it cannot be managed by a priori assumptions. A methodology is necessary to build this mobile software incorporating security from the first phases of the life cycle obtaining a secure

mobile grid system. It is difficult to incorporate safely existing mobile devices into the Grid, so that the impact is minimum and transparent to the user. That's the reason why the necessity to elaborate and define a process of development of a system based on the Grid and mobile technology and, considering the peculiarities and necessities of this type of systems arises. This process must be always flexible, scalable and dynamic, so that it adapts itself to the necessities, always changing, of the mobile Grid systems.

An important phase of the methodology is the security requirements analysis which we have proposed with a set of task identifying assets to protect, threat and vulnerabilities of our application and building a diagram of security use cases and misuse cases from which we can specify security requirements for our application in next stages of our methodology. These security requirements must be analyzed, specified and validated ensuring that all requirements obtained are complete, consistent and easily understandable and analyzable by the different actors involved in the development.

As a future work we will analyze in depth the proposed methodology making a special effort in describing each stage in detail and applying all the stages to a case study to obtain a real mobile grid system. Also, we will complete our initial repositories with all use cases and security use cases, relations, constraints, actors, and any other information important and we will specify them formally.

ACKNOWLEDGEMENTS

This research is part of the following projects: MISTICO (PBC-06-0082) 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).

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., B. M. Grizzell, et al. (2007). Cap. 4. Pragmatic Security for Constrained Wireless Networks. Security in Distributed, Grid, Mobile, and Pervasive Computing. A. Publications. The University of Alabama, Tuscaloosa, USA: 440.

Bruneo, D., M. Scarpa, et al. (2003). Communication paradigms for mobile grid users. 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'03).

Foster, I. and C. Kesselman (1999). The Grid: Blueprint for a Future Computing Infrastructure. San Francisco, CA, Morgan Kaufmann Publishers; 1ST edition.

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

Humphrey, M., M. R. Thompson, et al. (2005). "Security for Grids." Lawrence Berkeley National Laboratory. Paper LBNL-54853.

ITU (2004). ITU_T Recommendation X.1121. Framework of security technologies for mobile end-to-end data communications.

Jameel, H., U. Kalim, et al. (2005). Mobile-To-Grid Middleware: Bridging the gap between mobile and Grid environments. European Grid Conference EGC 2005, Amsterdam, The Netherlands, Springer.

Litke, A., D. Skoutas, et al. (2004). Mobile Grid Computing: Changes and Challenges of Resourse Management in a Mobile Grid Environment. 5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004).

MAP (2006). Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2), Ministry for Public Administration of Spain.

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

Trung, T. M., Y.-H. Moon, et al. (2005). A Gateway Replication Scheme for Improving the Reliability of Mobile-to-Grid Services. IEEE International Conference on e-Business Engineering (ICEBE'05).

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

Vivas, J. L., J. López, et al. (2007). Cap. 12. Grid Security Architecture: Requirements,fundamentals, standards, and models. Security in Distributed, Grid, Mobile, and Pervasive Computing. A. Publications. Tuscaloosa, USA: 440.