PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices

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

(1) Group Research Alarcos, Information Systems and Technologies Department UCLM-Indra Research and Development Institute. ESI. University of Castilla-La Mancha Ciudad Real, Spain
{David.GRosado, Eduardo.Fdez-Medina,Mario.Piattini}@uclm.es
(2) Computer Science Department University of Málaga 29071, Málaga, Spain
jlm@lcc.uma.es

***Abstract*— A Grid computing system is defined as a platform that supports distributed system applications which require fast access to a large quantity of distributed resources in a coordinated manner. With the development of wireless technology and mobile devices, the Grid becomes the perfect candidate so that mobile users can make complex works that add new computational capacity to the Grid. Security of these systems, due to their distributed and open nature, receives great interest. The growing size and profile of the grid require comprehensive security solutions as they are critical to the success of the endeavour. A formal approach to security in the software life cycle is essential to protect corporate resources. However, little thought has been given to this aspect of software development. Due to its criticality, security should be integrated as a formal approach in the software life cycle. A methodology of development for secure mobile Grid computing based systems is defined, that is to say, an engineering process that defines the steps to follow so that starting from the necessities to solve, we can design and construct a secure Grid system with support for mobile devices that is able to solve and cover these necessities.**

***Index Terms*— Grid computing, Security Architecture, Mobile Devices, Secure Development Process**

I. Introduction

THE Grid idea is mainly focused on the remote access to computational resources, thus solving the problem of coordinating the resources shared between virtual, multi-institutional and dynamic organizations. When talking about sharing, we refer not only to files interchange but also to direct access to computers, software, data and other resources that are required by multiple applications in the fields of industry, science or engineering [1].

Mobile Computing is a generic term describing the application of small, portable, and wireless computing and communication devices. The Mobile Computing focuses on the requirement of providing access to information, communications and services everywhere, anytime and by any available means. The technical solutions for achieving this are not always easy to implement [2].

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. It has the ability to deploy underlying ad-hoc networks and provide a self-configuring Grid system of mobile resources (hosts and users) connected by wireless links and forming arbitrary and unpredictable topologies [2].

Security has been a central issue in grid computing from the outset, and has been regarded as the most significant challenge for grid computing [3]. The characteristics of computational grids lead to security problems that are not addressed by existing security technologies for distributed systems [4, 5]. But now the growing size and profile of the grid require comprehensive security solutions as they are critical to the success of the endeavour [6]. So, the grid must have mechanisms and security policies that are in charge of checking out that only authorized users have access to the resources provided by it [7, 8, 9].

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. These constraints introduce significant challenges that have to be addressed in order to maintain a secure network [10]. 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. Therefore, a Grid infrastructure that supports the participation of mobile nodes will play a significant role in the development of Grid computing.

On the other hand, 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 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 [11, 12]. 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, from the initial state to the final state, all the requirements related to Mobile Grid systems are analyzed and integrated. This process must make it easier for developers the analysis and characterization of all functional and security necessities during all stages of the development cycle of the software based on Grid technology as well as support the mobile devices.

In this paper, we will begin to construct the foundations of a process or ordered methodology of systematic development that serves as guide for the development of any Grid system with mobile devices, considering all the aspects of security during all phases of development obtaining, as a result, a secure, robust and scalable Mobile Grid system.

In next section, the importance of mobile Grid computing will be described. In section 3, we give a brief overview of the wireless and mobile environment. Section 4 is the main contribution of the paper, and the initial proposal of the process of systematic development to construct a secure Grid system that supports the mobile devices will be stated. We will finish by putting forward our conclusions as well as some research lines for our future work.

II. Mobile Grid Computing

At first glance, it seems that the marriage of mobile wireless consumer devices with high-performance grid computing would be an unlikely match [13]. 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. Both sides benefit from this fact since, on the one hand, the Grid offers its services to the mobile users to complete their works in a fast and simple way and on the other hand, the mobile devices offer their limited resources, but million 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 the mobile technology.

There are certain researches in the field of Grid environments with mobile devices [14, 15, 16, 17], that deal with the problem and the difficulty to incorporate into the existing Grid systems, mobile devices and terminals that can consume services and share their resources since they are flexible, heterogeneous and limited. This fact makes their incorporation into a fixed platform even more difficult.

Today, the development of wireless technology and mobile devices enables us to access the network service from anywhere at any time [18]. Although mobile devices promote mobile communication and flexible use, they still bring problems such as unpredictable quality of the network, low confidence, limited resources (energy, bandwidth, etc.) and periods of disconnections [19]. Provided that mobile devices have limited computing capacity, the Grid becomes an important computation service provider that enables mobile users to perform complicated jobs [20]. 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. This capability can improve the use of Grid applications even in places where this would be imaginary.

In mobile environments the context is extremely dynamic and it cannot be managed by a priori assumptions. For that reason, these Grid systems must provide the mobile software necessary to be able to handle all the questions related to mobile environments. The mobile Grid will introduce changes to the general Grid concept. New functionalities of the Grid will be needed since the old ones will not make use of all the capabilities that will be available. These functionalities will involve end-to-end solutions with emphasis on Quality of Service (QoS) and security, as well as interoperability issues between the diverse technologies involved. Enhanced security policies and approaches to address large scale and heterogeneous environments will be needed [2].

Grids and mobile Grids can be the ideal solution for many large scale applications that are of dynamic nature and require transparency for users. Grid will increase the job throughput and performance of the involved applications and will increase utilization rate of resources by applying efficient mechanisms for resource management in the vast amount of its resources. It will enable advanced forms of cooperative work by allowing the seamless integration of resources, data, services and ontologies [2].

III. Wireless and Mobile Computing

One of the main problems of wireless technologies is that the provided bandwidth is, in terms of magnitude, lower than in wired networks and, as a consequence, the signal loss is very frequent and the noise level is influenced by the external conditions. A second aspect is related to mobile devices themselves which are characterized by a scarce amount of resources in terms of CPU, RAM, display, storage and, in particular, the fact that they are equipped with small batteries that limit power consumption and affect both the wireless transmission and the access to services that require a high computational load. Finally, a third aspect that is necessary to consider is user mobility since it causes problems related to signal loss during the movement in a new cell (handoff), to the address management due to the crossing of different administrative domains as well as to the need of adapting services to the real position of the user [21].

Mobile computing is characterized by four constraints: Mobile elements are resource-poor relative to static elements. Mobility is inherently hazardous. Mobile connectivity is highly variable in performance and reliability. Mobile elements rely on a finite energy source. These constraints are not artifacts of current technology, but are intrinsic to mobility. Together, they complicate the design of mobile information systems and require us to rethink traditional approaches to information access [22].

IV. Methodology of development

A. Overview

Our objective is to provide developers with firstly a methodology or development systematic process that will include the complete development of Grid systems of whatever complexity and magnitude, where models, processes, methods, mechanisms, techniques, tools and documentary support are defined, and secondly an architecture that helps them develop a secure Grid system where support for mobile devices is defined, and that, considering the needs or requirements of the initial system, gives place to the design and implementation of a secure mobile Grid system in an ordered and systematic way.

This systematic engineering process will mainly face two great challenges: On the one hand, to establish a methodology for the secure development of the Grid systems, not only considering the functional needs, but also the non-functional ones, especially security not only of the system to be constructed but also of the necessities arising when implementing it using the Grid technology. On the other hand, the second challenge to solve is the use of mobile devices in Grid systems, with all the difficulties that constructing a Grid infrastructure that supports mobile devices entails, due to the limitations and characteristics of these devices.

For that reason, having a methodology of development centered in Grid systems, that provides a secure development and supports mobile devices is a great advance in the field of Grid systems and mobile devices. Simultaneously, it supposes a powerful tool for the developers of these systems.

B. Main Roles

The main roles defined here constitute the roles that are part of anything methodology of development software adding roles especially focused on security: Customer, Project Manager, Business modeler, Requirements engineer, Security requirement engineer, Systems Analyst, Security Analyst, Risk expert, Security developer, Auditor, System Architect, Security Architect, Test Engineer, Maintenance Team, Designer, Integrator Engineer, Programmer, External entity.

Also we need to describe the roles that are focused on mobile Grid systems and security on these environments: Grid Computing expert and mobile technology and mobile devices expert.

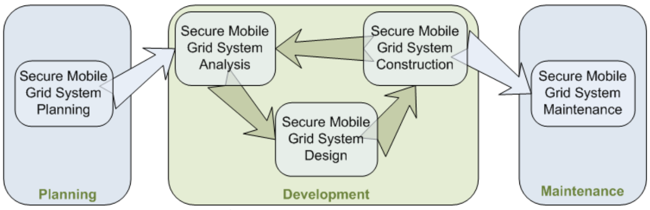
Secure Mobile Grid System Planning
Secure Mobile Grid System Analysis
Secure Mobile Grid System Construction
Secure Mobile Grid System Design
Secure Mobile Grid System Maintenance
Planning
Development
Maintenance

Fig. 1. Phases and stages of our methodology.

C. Development Process Approach

The development process starts from the necessities that the system to construct must fulfill, considering the specific characteristics of mobile devices. These necessities are the inputs to the development process in which, through a series of stages, a secure Mobile Grid system will be designed and constructed where all the initial necessities will be covered following the models defined by the methodology.

The systematic process of development is an iterative and incremental process. An iterative approach proposes an incremental understanding of the problem through successive refinements and an incremental growth of an effective solution through several versions. Thus, in each iteration of the process, new and necessary characteristics can be added and extended so that a complete final design is obtained covering the initial necessities. In this first proposal, and following some methodologies of software development like the Unified Process [23], we will present a general vision of the development methodology, leaving a more detailed study for future researches.

The methodology to develop a systematic process will consist of different phases, each one of them will also be divided into stages, and these last ones into activities and tasks. Our methodology will initially consist of 3 phases (see Fig. 1): planning, development and maintenance of a secure Grid system.

In all phases and stages we must take into account many features associated with grid environments [5] during the life cycle: user population, resources pool, and the group of processes running on different sites are potentially large and dynamic; processes may communicate by a variety of mechanisms such as unicast or multicast; different authentication and authorization mechanisms can be present in a single job computation, according to the local security policies of the sites involved; a user may be associated with different local name spaces or credentials; local authentication, authorization and access control may apply at different sites; individual users may be associated with different local name spaces, credentials and accounts at different sites.

D. Stages of the Methodology

1) Planning Stage

Apart from the typical aspects of any planning stage, other aspects related to the mobile grid described here, are taken into account. Security is a much more important factor in planning and maintaining a grid than in conventional distributed computing, where data sharing comprises the bulk of the activity. 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. However, organizational and business issues can be equally important. It is important to understand how the departments within an organization interact, operate, and contribute to the whole. While a grid-based environment may offer many advantages, any given application may not necessarily benefit from a grid. For example, some personal productivity applications are tightly coupled with a user's interface and do not consume a large amount of computing resources. Running them on a grid may not provide significant benefits. However, other applications may be very suited for exploiting a grid. To determine if existing or planned applications that are CPU intensive can take advantage of a grid environment requires many considerations. In this stage, we must describe some aspects to be considered related to the possible applicability of a grid to these applications, for example, to determine whether calculations can be performed parallely, to consider the amounts of data needed to be sent to the node performing a calculation and the time required to send it, etc. Both portability and the capability to take advantage of virtual resources are key attributes of an application that can take advantage of grid computing.

Activities: This stage is composed the following activities (see Fig. 2):

- A1: Initial Study. It collects data and organizes them so that they can be used, identifying the objectives, reach and scope of the mobile grid system.
- A2: Identification of Necessities. It identifies the necessities that are due to cover, taking into account the user's necessities, the grid considerations and the limitations of the mobile devices
- A3: Definition of the Virtual Organization. To identify the group of the implied ones that they will take part in the development process, to determine the functions to carry out, and necessary and final products.
- A4: Study of current Mobile Grid systems. It selects and studies the currents mobile Grid systems, valuing their characteristics and deficiencies to take them into account in later steps.
- A5: Definition of the technologic mobile Grid Architecture. The administrator should understand the organization's requirements for the mobile grid to better choose the grid and mobile technologies that satisfy those requirements.
- A6: Study of viability. It studies the different solutions alternatives considering the products to develop or use, the necessities, dates, costs, risks, scope and to study the impact of the solution with Grid technology.
- A7: Definition of Planning. It defines the plan of the project indicating the objectives and necessities that cover, the implied ones in each stage, intermediate and final obtained results, technical and human resources to use, documentation to elaborate, obtained benefits, etc.
- A8: Checking and Approval of the Planning. It reviews the results of the planning as well as those of approving the final result if all the people in charge are in agreement.

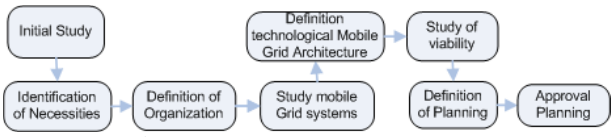
Initial Study
Identification of Necessities
Definition of Organization
Study mobile Grid systems
Definition technological Mobile Grid Architecture
Study of viability
Definition of Planning
Approval Planning

Fig. 2. Activities of Planning stage

Input Artifacts: Business description (strategy, principles, goals and drivers), Time limits, Organizational constraints, Budget information, financial constraints, Current architecture/IT system description, Description of developing organization, Description of resources available to the developing organization, Technology specification (Grid computing, wireless and mobile devices)

Output Artifacts: Problem description (purpose of scenario), Detailed objectives, Actors and their roles and responsibilities, Project description and scope, Project plan and schedule, Architecture vision, Technical requirements, Refined statements of business goals and strategic drivers, Catalogue of necessities and requirements of system, Catalogue of necessities and requirements of the Grid system and of the mobile devices identified, norms and standards to use, Security necessities for the system, grid environment and mobile devices, work plan structured.

Techniques, Practices and Reference guides: Cataloguing, Grid design workshops, UML (Diagrams, Use cases, models, etc.), Interviews, project Planning, Study of Cost-benefit, Impact on the Organization, Risk Management, Change Management, Documentation, Tests

Main Roles: Customer experts, Project Manager, Business modeler, Project team, Analysts, Security experts, Grid Computing experts, Mobile technology and Mobile devices experts, External entities

2) *Analysis Stage*

Apart from the typical aspects of any analysis stage, other aspects related to the mobile grid described here, are taken into account. We should define the most common general security requirements and challenges associated with grids [24] Among them, we can find the following ones: Authentication; Confidentiality; Integrity; Authorization and access control; Revocation; Distributed trust; Freshness; Scalability; Trust; Single sign-on; Delegation; Privacy; Non-repudiation; Credentials; Exportability; Multiple implementations; Interoperability; Interoperability with local security solutions; Integration; Uniform credentials and certification infrastructure. For mobile computing, there are five fundamental requirements for any type of data security,

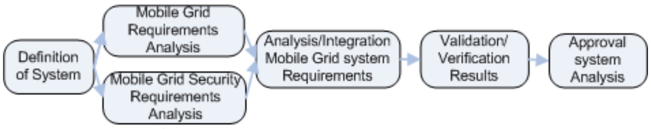
Definition of System
Mobile Grid Requirements Analysis
Mobile Grid Security Requirements Analysis
Analysis/Integration Mobile Grid system Requirements
Validation/ Verification Results
Approval system Analysis

Fig. 3. Activities of Analysis stage

including wireless Authentication, authorization and accounting (AAA); Data integrity; Privacy; Non-repudiation; Security policies. All of these factors are at play in the wireless and mobile device world [25].

Applications and their requirements should be analyzed to understand how they could be designed and developed to reap the benefits of a grid. To properly secure your grid environment, there are many different tools and technologies available. This stage analyzes some of those technologies. 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 proceeding.

Activities: This stage is composed of the following activities (see Fig. 3):

- A1: Definition of Mobile Grid System. It describes the system adapting the previous results and limiting the reach of the system to identify standards, norms and tools to use and describe all the relevant information to consider in this stage. It identifies the grid components as well.
- A2: Mobile Grid System Requirements Analysis. It defines and analyzes general both functional and non-functional requirements of the mobile grid system, for example, heterogeneity of the computing resources, geographical and organizational distribution of the resources, scalability, availability, mobile accessibility, mobility restrictions, limited resources, disconnections, QoS, distributed storage, job execution, autonomy, and so on.
- A3: Mobile Grid System Security Requirements Analysis. It defines and analyzes the security requirements of the mobile Grid system, for example, trust, single sign-on, delegation, privacy, non-repudiation, credentials, confidentiality, integrity, authentication, encryption, certificates, keys, and so on.
- A4: Mobile Grid System Requirements Integration. It integrates all the requirements analysis identified in previous stages obtaining a full analysis of all requirements of secure mobile grid system and an analysis model.
- A5: Validation and Verification of Results. During the course of some designs the 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 proceeding.
- A6: Approval of System Analysis. It validates the obtained results and the analysis. It approves the analysis of the system.

Input Artifacts: Output artifacts of the Planning stage, the Validation report and the modifications (of the construction stage), Business domain, Use cases models, Use cases of security models, Reports of threats and risks, List of Requirements and Security Requirements (of generic system, of Grid systems and of mobile devices), Specific standards, Policies of security, Manuals, System Constraints.

Output Artifacts: Catalogue of requirements and security requirements of the system on a Grid environment with mobile devices, Specification of Requirements and Security requirements of the final system, Analysis model, Report of analysis validation, Report of failures or errors found.

Techniques, Practices and Reference guides: Meeting and interviews, UML, UMLSec, Analysis of cost-benefit, abuse cases, tree of threats, security use cases.

Main Roles: Project Manager, Business modeler, Requirements engineer, Security requirement engineer, Systems Analyst, Security Analyst, Risk expert, System Architect, Security Architect, Grid Computing expert, Mobile technology and mobile devices expert.

3) Design Stage

Apart from the typical aspects of any design stage, other aspects related to the mobile grid described here, are taken into account. The participants and users of the grid can be members of several real and virtual organizations. The grid can help in enforcing security rules among them along with in implementing policies, which can resolve priorities for both resources and users. Many or most of the grid middleware, technologies, and system components are probably new to many people within the design team and it is always a good idea to hear firsthand experience. Once the functional and non-functional requirements are known, the architect should readily be able to select the type of grid and the best topology required to satisfy the majority of the business requirements.

Given that grid solutions are adaptable to meet the needs of various business problems, different types of grids are designed to meet specific usage requirements and constraints. Any design will require a basic set of system management tools to help determine availability and performance within the grid. A design without these tools is limited in how much support and information can be provided about the health of the grid infrastructure. The storage possibilities are endless within a grid design. How that storage will be secured, backed up, managed, and replicated are some of the questions that the grid design will try to answer. In this world of mobile broadband, IT managers have several primary concerns about wireless security. Namely, they want to make certain that their current, wired networks remain secure, and they want to ensure that only authorized and authenticated users are accessing that network [25].

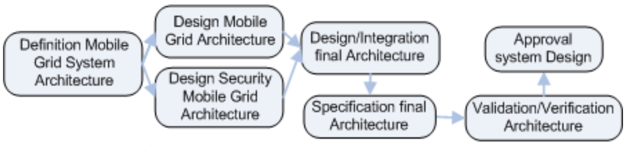
Definition Mobile Grid System Architecture
Design Mobile Grid Architecture
Design Security Mobile Grid Architecture
Design/Integration final Architecture
Specification final Architecture
Validation/Verification Architecture
Approval system Design

Fig. 4. Activities of Design stage

Activities: This stage is composed of the following activities (see Fig. 4):

- A1: Definition of the Mobile Grid System Architecture. It describes the generic architecture, elements, grid components, subsystems, security services, mechanisms, patterns, etc. Besides, it describes the generic Mobile Grid architecture and its technological environment.
- A2: Design of the Mobile Grid System Architecture. It designs and analyzes the mobile grid architecture obtaining an architecture that covers all the necessities of the system (generic, grid and mobile necessities).
- A3: Design of the Security Mobile Grid Architecture. It designs and analyzes the security mobile grid architecture obtaining a security architecture that covers all the security necessities of the system (security generic, security grid and security mobile).
- A4: Integration and Design of the final Architecture. It designs and analyzes the resulting architecture relating and integrating the previous architectures to obtain a final architecture of reference that covers all the necessities of the secure Grid system with mobile devices.
- A5: Specification of the final Architecture. It specifies the final architecture in a coherent way, by precisely describing the grid components, elements and relations and all the details of the designed architecture, using some ADL, design models and views and points of view with security aspects.
- A6: Validation and Verification of the final Architecture. It verifies that in the designed architecture, all the elements that appear to be correct are justified and it validates that the design covers the initial necessities of the system.
- A7: Approval of the System Design. It presents and approves the design of the final architecture.

Input Artifacts: Output artifacts of Analysis stage, Best practices, Technological environment, reference architecture, security architecture, design constraints, grid characteristics and mobile functionalities.

Output Artifacts: Architecture design, Description of the architecture, Specification of the architecture with ADL, Detailed specification of components, elements, relations, etc., Design models, Report of fulfilment of requirements in the architecture, Report of validation of design.

Techniques, Practices and Reference guides: Walkthroughs, Design Patterns, Security patterns, UML UMLSec, Revisions, Monitoring, Documentation.

Main Roles: Project Manager, Systems Analyst, Security Analyst, Risk expert, Security developer, System Architect, Security Architect, Security Designer, Integrator Engineer, Grid Computing expert, Mobile technology and mobile devices expert.

4) Construction Stage

Apart from the typical aspects of any construction stage, other aspects related to the mobile grid described here, are taken into account. The degree of security involved is based on the type of grid topology as well as on the data that the security will be protecting. The security requirements for a grid design within a bank will be completely different from those of an academic institution doing research. Grids can be built in all sizes, ranging from just a few machines in a department to groups of machines organized as a hierarchy spanning the world. We must define the grid system topologies (intragrid, extragrid or intergrid) that we are aimed at building as a means for identifying the necessary technical, infrastructural, and other middleware components and subsystems for a grid infrastructure. The infrastructure represents the physical hardware and software components used to interconnect different grid computers. These components help support the information flow between grid systems and provide the basic set of services for connectivity, security, performance availability, and management. While many of these infrastructure components supply basic functionality to the grid, many others are optional. It will be up to you to decide on the requirements and how well these components match up to the needs of your design.

There are numerous software-based ways to safeguard mobile devices, virtual private networks (VPNs), firewalls, on-device data encryption software and device management solutions, to name just a few.

Activities: This stage is composed of the following activities (see Fig. 5):

- A1: Environment Preparation. It assures that all the tools and equipment are available for the construction of the mobile grid system.
- A2: Implementation of the Mobile Grid System Architecture. It identifies the significant components of the architecture and implements these components using the means available, mechanisms and services, as many of the Grid technology as of the mobile devices.
- A3: Implementation of the Security Mobile Grid Architecture. It implements the grid components or security elements of the architecture using not only the tools available from the technological platform Grid but also from well-known software tools of security.
- A4: Integration and Implementation of the final Mobile Grid Architecture. It integrates all the components implemented in the previous stages to give rise to the construction of a stable architecture and that can be proven.
- A5: Design and Execution of tests. It designs and defines

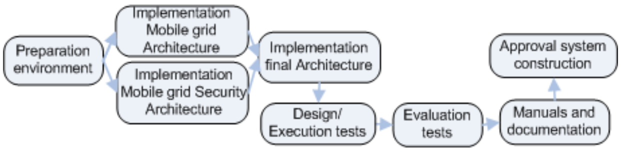
Preparation environment
Implementation Mobile grid Architecture
Implementation Mobile grid Security Architecture
Implementation final Architecture
Design/ Execution tests
Evaluation tests
Manuals and documentation
Approval system construction

Fig. 5. Activities of Construction stage

the tests verifying that the requirements, the grid components and the complete system are correct. The different tests and results will be handled, so that it is possible to go back to the previous stages if defects important to be fixed appear.

- A6: Evaluation of tests. It analyzes the test results and evaluates them according to the awaited results. It also determines the reach of the possible modifications, costs, resources, etc.
- A7: Elaboration of Manuals and Documentation. It elaborates the necessary documentation necessary to provide the user with. Furthermore, it deals with the preparation and formation of the user, the definition of the delivery formats, supports, etc.
- A8: Approval of System Construction. It approves and accepts the constructed system studying the results obtained in the previous stages and making sure that the system is correct and stable to be given to the user.

Input Artifacts: Output artifacts of the Design stage, specification of technological environment, implementation standards, technology grid, wireless and mobile technology, security mechanisms and procedures test environments, relevant technical requirements.

Output Artifacts: Built Secure Grid system with mobile devices, Result of tests, Report of test evaluation, documentation and manual of user, Plan of trainers, Evaluation of errors and changes.

Techniques, Practices and Reference guides: Tests, revisions, Implementation methods, security verification, Monitoring

Main Roles: Test Engineer, Trainers, Technical team, Systems Analyst, Security Analyst, Security expert, Security developer, Integrator Engineer, Programmers, Architects Team, Grid Computing expert, Mobile technology and mobile devices expert.

5) *Maintenance Stage*

Apart from the typical aspects of any maintenance stage, other aspects related to the mobile grid described here are taken into account. A plan of maintenance of the system for its later modification is defined according to the new necessities of the client. Once the system has been put into the hands of the end users, often we have to face questions that require an additional development to fit the system, to correct some non detected problems or to finalize some characteristics that had been postponed. Depending on the received request of maintenance, we must study the viability of the proposed change to identify 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.

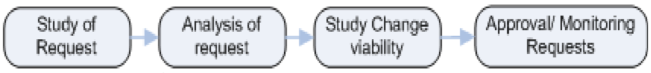

Fig. 6. Activities of Maintenance stage

Activities: This stage is composed of the following activities (see Fig. 6):

- A1: Study of Requests. It studies the change request and defines a system of control and request registry.
- A2: Analysis of Requests. It analyzes the request to establish the reach to carry out the request. It allocates the people in charge and studies the possible solutions. Also, it determines if the request is accepted or rejected.
- A3: Study of Change Viability. It studies the modifications to carry out, defining the resources, personnel, cost and time affected by the request and evaluating the propose complexity of the change and solutions.
- A4: Approval and Monitoring of Requests. It establishes a request monitoring plan. The changes will be made and if the results of the previous activities are favourable and the people in charge agree, the request will be approved.

Input Artifacts: Output artifacts of the construction stage, maintenance request.

Output Artifacts: Report of impact of change, Acceptance or rejection of the request, Personnel, cost and time required, List of elements to change.

Techniques, Practices and Reference guides: Monitoring, Cost/benefit analysis, Estimation of resources, personnel and time, Interviews and meeting.

Main Roles: Customers experts, Project Manager, Maintenance Team, Analysts, Requirements engineer, Designers team.

V. CONCLUSIONS

The Grid connects groups of PCs, storage units and nets, allowing research centers and enterprises to dynamically assign resources according to the business necessities. These resources are distributed on the net in a transparent way but keeping a high security level and a correct management policy that takes into consideration technical as well as economic parameters. It is a new computation paradigm, a shared model that allows not only communication and storage but also information processing all over the world. In this new shared model, security plays an essential role for the success of this new paradigm, assuring access to the resources, the information, the users and the organizations that put their resources at the disposition of the world.

It is difficult to incorporate, safely existing mobile devices into the Grid, so that the impact is minimum and transparent to the user. At the moment, there are many technologies and tools available that cause that the Grid applications are secure, but at the time of incorporating mobile devices (PDA, mobile telephones, etc.) the possibilities of implementing security are reduced, mainly due to the limitations of these mobile devices and to their technologies (wireless, WAP, etc.).

There are numerous referring studies to incorporate security into the whole life cycle of software in order to obtain an end product that fulfills the required security requirements. In the case of the life cycle of a mobile Grid system, the same situation occurs; it is necessary to incorporate security from the first stages of development, by defining a process or a methodology that, besides developing a mobile Grid system, incorporates all aspects of Grid security and mobile devices into the life cycle and obtains, consequently, a secure end product. That’s the reason why the necessity to elaborate and define a process of development of a system based on Grid and mobile technology and, considering the peculiarities and necessities of this type of systems arises. This process must always be flexible, scalable and dynamic, so that it adapts to the necessities, always changing, of the Grid systems.

As future work we will analyze in depth the proposed methodology, making a special effort in describing each stage in detail and defining a scenario or study case where we apply our methodology obtaining a real mobile grid system.

Acknowledgment

This research is part of the following projects: DIMENSIONS (PBC-05-012-2) and 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

[1] Foster, I., C. Kesselman, and S. Tuecke. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. 7th International Euro-Par Conference Manchester on Parallel Processing. 15(3): pp. 1 - 4. 2001.

[2] Litke, A., D. Skoutas, and T. Varvarigou. Mobile Grid Computing: Changes and Challenges of Resourse Management in a Mobile Grid Environment. In 5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004). December 2004, 2004.

[3] Humphrey, M., M.R. Thompson, and K.R. Jackson. Security for Grids. Lawrence Berkeley National Laboratory. Paper LBNL-54853. August 14, 2005.

[4] Welch, V., F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, and S. Tuecke. Security for Grid services. In 12th IEEE International Symposium on High Performance Distributed Computing (HPDC-12 '03): IEEE Computer Society. 22-24 June 2003, 2003.

[5] Foster, I., C. Kesselman, G. Tsudik, and S. Tuecke. A Security Architecture for Computational Grids. In 5th ACM Conference on Computer and Communications Security. San Francisco, USA: ACM Press. 1998.

[6] Kostopoulos, G., N. Sklavos, and O. Koufopavlou. Cap. 10. State-of-the-Art Security in Grid Computing. In Security in Distributed, Grid, Mobile, and Pervasive Computing, A. Publications, Editor: The University of Alabama, Tuscaloosa, USA. pp. 440. 2007.

[7] Chadwick, D.W. and A. Otenko. The PERMIS X.509 Role Based Privilege Management Infrastructure. Future Generation Computer Systems. 19(2): pp. 277–289. February 2003, 2003.

[8] Crampton, J. and H.W. Lim. Role Signatures for Access Control in Grid Computing. 2007.

[9] Pearlman, L., V. Welch, I. Foster, and C. Kesselman. A Community Authorization Service for Group Collaboration. In IEEE 3rd International Workshop on Policies for Distributed Systems and Networks. 2002.

[10] 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: The University of Alabama, Tuscaloosa, USA. pp. 440. 2007.

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

[12] Anderson, R. Security Engineering - A Guide to Building Dependable Distributed Systems. 2001: John Wiley&Sons. 640.

[13] Phan, T., L. Huang, and C. Dulan. Challenge: Integrating Mobile Wireless Devices Into the Computational Grid. In 8th annual international conference on Mobile computing and networking (MobiCom'02). Atlanta, Georgia, USA: ACM Press. 2002.

[14] 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). Beijing, China. 2005.

[15] 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. Amsterdam, The Netherlands: Springer. February 14-16, 2005.

[16] Kwok-Yan, L., Z. Xi-Bin, C. Siu-Leung, M. Gu, and S. Jia-Guang. Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes. Lecture Notes in Computer Science. 2908/2003: pp. 42-54. 2004.

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

[18] Bruneo, D., M. Scarpa, A. Zaia, and A. Puliafito. Communication paradigms for mobile grid users. In 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGrid 2003. 12-15 May 2003, 2003.

[19] Forman, G.H. and J. Zahorjan. The Challenges of Mobile Computing. IEEE Computer. 27(4). April 1994, 1994.

[20] Trung, T.M., Y.-H. Moon, C.-H. Youn, J.-J. Cho, and S.-J. Jeong. A Gateway Replication Scheme for Improving the Reliability of Mobile-to-Grid Services. In IEEE International Conference on e-Business Engineering (ICEBE'05). 2005.

[21] Puliafito, A., D. Bruneo, and M. Scarpa. Mobile Middleware: Definition and Motivations. In invited chapter in Mobile Middleware, P. Bellavista and A. Corradi, Editors. CRC Press: London. pp. 1377. 2006.

[22] Satyanarayanan, M. Fundamental Challenges in Mobile Computing. In Symposium on Principles of Distributed Computing. 1996.

[23] Kruchten, P. The Rational Unified Process: An Introduction. 2nd ed. 2000: Addison-Wesley. 320.

[24] Vivas, J.L., J. López, and J.A. Montenegro. Cap. 12. Grid Security Architecture: Requirements,fundamentals, standards, and models. In Security in Distributed, Grid, Mobile, and Pervasive Computing, A. Publications, Editor: The University of Alabama, Tuscaloosa, USA. pp. 440. 2007.

[25] Trusted Computing Group Administration, Securing Mobile Devices on Converged Networks. pp. 16. 2006. https://www.trustedcomputinggroup.org/groups/mobile/Final_iGR_mobile_security_white_paper_sept_2006.pdf