Chapter 12
Identifying Secure Mobile Grid Use Cases

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 Piattini
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. We are elaborating a process of development to build secure mobile Grid systems considering security on all life cycles. In this chapter, we present the practical results applying our development process to a real case, specifically we apply the part of security requirements analysis to obtain and identify security requirements of a specific application following a set of tasks defined for helping us in the definition, identification, and specification of the security requirements on our case study. The process will help us to build a secure Grid application in a systematic and iterative way.

INTRODUCTION

Grid computing has emerged to cater the need of computing-on-demand (Jana, Chaudhuri, & Bhaumik, 2009) due to the advent of distributed computing with sophisticated load balancing, distributed data and concurrent computing power using clustered servers. 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 & Kesselman, 2004).
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 & Yavagal, 2006).

At first glance, it seems that the marriage of mobile wireless consumer devices with high-performance Grid computing would be an unlikely match. After all, Grid computing to date has utilised multiprocessors and PCs as the computing nodes within its mesh. Consumer computing devices such as laptops and PDAs are typically restricted by reduced CPU, memory, secondary storage, and bandwidth capabilities. However, therein lies the challenge. The availability of wirelessly connected mobile devices has grown considerably within recent years, creating an enormous collective untapped potential for resource utilisation. To wit, recent market research shows that in 2008, 269 million mobile phone and 36 million smartphone (Gartner, 2009) were sold worldwide, and that in 2006, 17 million PDAs (Gartner, 2007) were sold worldwide. Although these individual computing devices may be resource-limited in isolation, as an aggregated sum, they have the potential to play a vital role within Grid computing (Phan, Huang, Ruiz, & Bagrodia, 2005).

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, & 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, & Jackson, 2005). The characteristics of computational grids lead to security problems that are not addressed by existing security technologies for distributed systems (Foster, Kesselman, Tsudik, & 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, & Jenkins, 2007).

The reasons that led us to focus on this topic are several: Firstly, the lack of adequate development methods for this kind of systems since the majority of existing Grid applications have been built without a systematic development process and are based on ad-hoc developments (Dail et al., 2004; Kolonay & Sobolewski, 2004), suggests the need for adapted development methodologies (Giorgini, Mouratidis, & Zannone, 2007; Graham, 2006; Jacobson, Booch, & Rumbaugh, 1999; Open Group, 2009). Secondly, due to the fact that the resources in a Grid are expensive, dynamic, heterogeneous, geographically located and under the control of multiple administrative domains (Bhanwar & Bawa, 2008), and the tasks accomplished and the information exchanged are confidential and sensitive, the security of these systems is hard to achieve. And thirdly, because of the appearance of a new technology where security is fundamental together with the advances that mobile computation has experienced in recent years that have increased the difficulty of incorporating mobile devices into a Grid environment (Guan, Zaluska, & Roure, 2005; Jameel, Kalim, Sajjad, Lee, & Jeon, 2005; Kumar & Qureshi, 2008; Kwok-Yan, Xi-Bin, Siu-Leung, Gu, & Jia-Guang, 2004; Sajjad et al., 2005).

In this paper, we will apply the activity 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
Related Content

Fault Detection and Recovery Mechanisms and Techniques for Service Oriented Infrastructures
www.igi-global.com/chapter/fault-detection-recovery-mechanisms-techniques/55252?camid=4v1a

An Architectural Overview of the GReIC Data Access Service
www.igi-global.com/chapter/architectural-overview-grelc-data-access/64500?camid=4v1a

Fast Paxos Made Easy: Theory and Implementation
www.igi-global.com/article/fast-paxos-made-easy/120458?camid=4v1a

Custom-Made Cloud Enterprise Architecture for Small Medium and Micro Enterprises
www.igi-global.com/chapter/custom-made-cloud-enterprise-architecture/64504?camid=4v1a