

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, Tsodik, 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 active 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 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.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/obtaining-security-requirements-mobile-grid/3967

Related Content

Modeling Scalable Grid Information Services with Colored Petri Nets

Vijay Sahota, Maozhen Liand Marios Hadjinicolaou (2012). *Evolving Developments in Grid and Cloud Computing: Advancing Research* (pp. 169-184).

www.irma-international.org/chapter/modeling-scalable-grid-information-services/61990

An Osmosis-Based Intelligent Agent Scheduling Framework for Cloud Bursting in a Hybrid Cloud

Preethi Sheba Hepsibaand Grace Mary Kanaga E. (2020). *International Journal of Distributed Systems and Technologies* (pp. 68-88).

www.irma-international.org/article/an-osmosis-based-intelligent-agent-scheduling-framework-for-cloud-bursting-in-a-hybrid-cloud/256207

Trust, Virtual Teams, and Grid Technology

Genoveffa Jeni Giambona, Nicholas L.J. Silburnand David W. Birchall (2009). *Grid Technology for Maximizing Collaborative Decision Management and Support: Advancing Effective Virtual Organizations* (pp. 131-146).

www.irma-international.org/chapter/trust-virtual-teams-grid-technology/19342

Grid Workflows with Encompassed Business Relationships: An Approach Establishing Quality of Service Guarantees

Dimosthenis Kyriazis, Andreas Menychtasand Theodora Varvarigou (2012). *Grid and Cloud Computing: Concepts, Methodologies, Tools and Applications* (pp. 1332-1348).

www.irma-international.org/chapter/grid-workflows-encompassed-business-relationships/64542

Ambiance Intelligence Approach Using IoT and Multi-Agent System

Meftah Zouai, Okba Kazar, Guadalupe Ortiz Bellot, Belgacem Haba, Nadia Kabachianand M. Krishnamurthy (2019). *International Journal of Distributed Systems and Technologies* (pp. 37-55).

www.irma-international.org/article/ambiance-intelligence-approach-using-iot-and-multi-agent-system/218825