International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **4**, April **2009**

 ISSN 1349-4198
pp. 1125–1136

A QUANTITATIVE METHOD FOR EVALUATING THE SECURITY THREATS OF GRID SYSTEM TO TASKS

Jianwei Ye, Binxing Fang

School of Computer Science and Technology
Harbin Institute of Technology
No.92, West Da-Zhi Street, Harbin Heilongjiang, P. R. China
{ yjw; bxfang }@pact518.hit.edu.cn

Yongzheng Zhang and Zhihong Tian

Institute of Computing Technology
Chinese Academy of Sciences
No.6 Kexueyuan South Road, Haidian District, Beijing, P. R. China
{ zhangyongzheng; tianzhihong }@software.ict.ac.cn

Received November 2007; revised July 2008

Abstract. *This paper proposes a new method to protect the confidentiality and integrity of grid tasks, in Open Grid Services Architecture. Our method identifies actual effective attacks against tasks, and quantitatively evaluates the risks that every grid service will attack the tasks based on the identified attacks. Further, our method quantitatively evaluates the risks that the confidentiality and integrity of given tasks will be attacked by the whole grid system. The identification of attacks and risk evaluation are based on the analysis of the past actions of grid services, and consider the protection mechanisms employed by tasks well. The prototype implementation of our method shows that our method is feasible and applicable in stock grid systems with little modification.*
Keywords: Grid, Task, Evaluate, Risk, Confidentiality and integrity

1. **Introduction.** Summarily, there are two types of security threats introduced by grid systems: One from malicious tasks and the other from potential malicious grid nodes. The malicious task problem that the malicious tasks would attack the grid nodes has been studied for a long time. Many effective protection mechanisms have already been proposed for it and work well. Comparatively, the malicious grid node problem that the malicious or compromised nodes would attack the tasks is more difficult.

The ultimate causes of malicious node problem are: 1) the malicious or compromised grid nodes are entirely able to control the tasks that have moved into them and have enough time and resources to attack these tasks; 2) the task owners are incapable of foreseeing and dominating the actions of the remote grid nodes. Correspondingly, there are two approaches to protect tasks: to add protection mechanisms into tasks to prevent them from being attacked; or to avoid moving tasks into the malicious nodes.

Unfortunately, so far no protection mechanisms belonging to the first approach are sound and practical. So, it is a good choice that: first to identify the attack actions of the malicious nodes and evaluate their risks; and then to selectively move the tasks into the nodes as secure as possible by the evaluation results, or employ proper mechanisms to protect the tasks. Our work is just absorbed in the attack actions identification and risk evaluation.

Our method aims at the popular application layer attacks against the security of tasks, which are the maximal threats to tasks, in popular Open Grid Services Architecture