available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Daonity – Grid security from two levels of virtualization☆

Haibo Chen[a], *Jieyun Chen*[b], *Wenbo Mao*[c,*], *Fei Yan*[d]

[a]*Fudan University, Department of Physics, Shanghai 200433, China*
[b]*Huazhong University of Science and Technology, Wuhan 430074, China*
[c]*Hewlett–Packard Laboratories China, Beijing 100022, China*
[d]*Wuhan University, Wuhan 430072, China*

Keywords:
Grid computing
Grid security infrastructure (GSI)
Behavior conformity
Trusted computing (TC)
Virtual organization (VO)
Platform attestation
Resource virtualization
Platform virtualization
Secure operating systems

ABSTRACT

The service oriented architecture of grid computing has been thoughtfully engineered to achieve a service level virtualization: not only should a grid be a virtual machine (also known as a virtual organization, VO) of unbounded computational power and storage capacity, but also should the virtual machine be serviceable in all circumstances independent from serviceability of any of its component. At present, a grid VO as a result of service level virtualization only is more or less confined to participants from scientific computing communities, i.e., can have a limited scale. It is widely agreed that for a grid to pool resources of truly unbounded scale, commercial enterprises and in particular server-abundant financial institutions, should also "go for the grid," i.e., open up their servers for being used by grid VO constructions. We believed that it is today's inadequate strength of the grid security practice that is the major hurdle to prevent commercial organizations from serving and participating the grid.

This article presents the work of Daonity which is our attempt to strengthening grid security. We identify that a security service which we name *behavior conformity* be desirable for grid computing. Behavior conformity for grid computing is an assurance that ad hoc related principals (users, platforms or instruments) forming a grid VO must each act in conformity with the rules for the VO constitution. We apply trusted computing technologies to achieve two levels of virtualization: resource virtualization and platform virtualization. The former is about behavior conformity in a grid VO and the latter, that in an operating system. With these two levels of virtualization working together it is possible to build a grid of truly unbounded scale by VO including servers from commercial organizations.

1. Introduction

Virtualization of resources is the key element in grid computing. Viewed by a user, a computational grid (Bair, 2004; Foster and Kesselman, 1999; Foster et al., 2001) should be a "virtual machine" of unbounded resources. In reality, this virtual machine is ad hoc constructed for the user, comprising a number – possibly very large – of physically separate resources to combine to a federated or collaborated computing environment called *virtual organization* (VO). Fig. 1 illustrates a typical VO structure in a high performance computing setting which comprises of one user (whose platform is in the left),

☆ Work funded by Hewlett–Packard Company. Part of work by Huazhong University of Science and Technology was also supported by the Chinese Natural Science Foundation's "Research Projects of Great Importance" Grant no. 90412010.

* *Corresponding author*. Fax: +86 21 651 04 949.
E-mail addresses: haochen@fudan.edu.cn (H. Chen), Mao_Wenbo@emc.com (W. Mao).

1363-4127/$ – see front matter © 2007 Published by Elsevier Ltd.
doi:10.1016/j.istr.2007.05.005

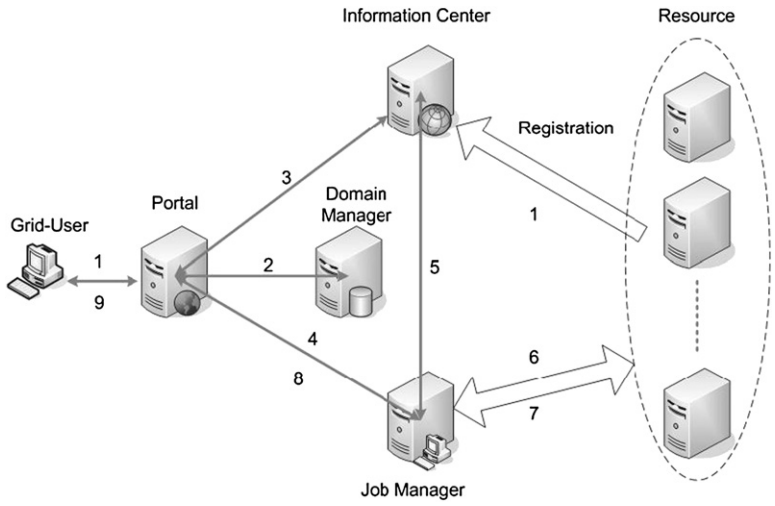

Fig. 1 – A typical grid computing virtual organization.

brokerage servers (Portal, Domain Manager, Information Center and Job Manager in the middle) and job execution farm (resource in the right). This grid VO model depicts typical steps of how grid jobs are submitted and executed. The following enumeration corresponds to the numbered steps in Fig. 1:

1 User begins by logging onto Portal. Independently, resources, which are formed by principals are willing to lease computing/storage resources, register resources to Information Center. The latter will play the role of a resource broker.
2 Domain Manager verifies user's legitimacy of using the grid services. The verification can be based on a prearranged relationship between these two principals (e.g., a credential of user on the basis of a shared secret), or based on a trusted third party's certification (e.g., a credential of user on the basis of a public-key certification). Domain Manager is in a security server's position in a VO.
3 User, having logged onto Portal, can check, by interacting with Information Center, service state and obtain the state information to match his/her jobs' requirement.
4 After obtaining satisfactory service state information, user submits jobs to Job Manager.
5 Job Manager cooperates with Information Center and obtains the addresses of the resources which can satisfy user's job requirements.
6, 7 Job Manager works on user's jobs with selected resources. It supplies user's data to resources, and stores returned computing results for user.
8, 9 Upon completion of jobs execution, Job Manager flags up for user to fetch the results.

The principals in the middle of Fig. 1 (Portal, Domain Manager, Information Center and Job Manager) play important roles to achieve resource virtualization. The organization of these principals in Fig. 1 achieves a service oriented architecture (SOA) for grid computing. A characteristic feature in the SOA can be referred to as a high degree of dependability which covers desirable services collectively in terms of reliability, availability, privacy and scalability. A grid VO can typically execute jobs for a user in a streamlined manner: the user submits a batch of jobs to the middle principals in Fig. 1 in one go and comes back to fetch the result only after the jobs are done. It should be possible that, after the submission of a user's jobs, the jobs must be processed without requiring any further intervention by the user. Moreover, the continuation in the execution of the jobs should not depend on the continuation of serviceability of any component of the VO. We shall see in Section 3 how this property is realized by the leading grid architecture Globus Toolkit Version 4 (GT4). GT4 has several thoughtful designs to virtualize resources with an intension to achieve high dependability for grid computing. Among other means in the architectural design, the security part of the grid architecture plays an enabling role for achieving grid resource virtualization.

However, in Section 3 we will also see through in-depth analyses and discussions a (hidden) point that grid resource virtualization in GT4 is done in a trade-off by working with a weakened notion of trust, even though a strong notion of trust is needed among grid VO participants in order to build a VO of large scale. Our discussions will reveal that the trade-off turns out to be responsible for a limited benefit we can gain from resource virtualization of GT4 as a result of a lowered quality of resource virtualization we have at present.

Therefore the work presented in this article has the following goal: to retain the property of high dependability of, at the same time to strengthen trustworthiness for, the leading grid architecture.

1.1. *Our approach: trusted computing for two levels of virtualization*

We consider that *Trusted Computing Group* (TCG) technologies (Trusted Computing Group; Trusted Computing Group, 2001, 2003; Pearson, 2003) developed by TCG form a practical and readily applicable technical means to serving the need of grid security. TCG is an important industrial initiative for improving computer security by means of a hardware supported security architecture. TCG uses a hardware module *Trusted*