Chapter 6

Single Attestation Image for a Trusted and Scalable Grid

Yuhui Deng
Jinan University, P. R. China

Na Helian
University of Hertfordshire, UK

ABSTRACT

Traditionally, Grid users are forced to trust the Grid platforms, but the users are not always regarded as trustworthy. This trust asymmetry hinders the commercializing of Grid resources. Trusted Grid is proposed to tackle this challenge by leveraging Trusted Computing (TC). However, the TC relies on a microcontroller Trusted Platform Modules (TPM) which has limited computing power and is doomed to be a system bottleneck. This paper constructs a trusted Grid as a flat ring and decentralizes the functionalities of TPM across the ring. This architecture offers a single attestation image which provides a transparent attestation to a scalable, large-scale, and dynamic trusted Grid. The architecture also significantly reduces the frequency of attestations, thus alleviating the TPM bottleneck. Furthermore, the architecture can avoid the potential system bottleneck and single point of failure of the centralized architecture or the root node of the hierarchical architecture.

INTRODUCTION

Grid is a flexible, secure, and coordinated resource sharing among dynamic collections of individuals, institutions, and resources (Foster, Kesselman, & Tuwcke, 2001). The main issue of Grid security in the past works is achieving authentication and authorization of Grid users and their programs (Basney, Humphrey, & Welch, 2005; Chadwick, 2005; Cody, Sharman, Rao, & Upadhyaya, 2008; Martin & Yau, 2007; Welch, 2004). The open source Globus Toolkit (GT) (The Globus Alliance, 2009a) has been employed worldwide as a middleware to develop Grid platforms and support Grid applications. Grid Security Infrastructure (GSI) (Welch, 2004) is adopted by GT to offer fundamental security services which enable secure authentication and communication over an
open network channel. For example, secure communication between elements of a Grid, security across organizational boundaries, single sign-on for Grid users, and so forth. In the GSI-like security mechanisms, Grid users are forced to trust the Grid platforms, but the users are not always regarded as trustworthy (Hwang et al., 2005; Löhr, Ramasamy, Sadeghi, Schulz, Schunter, & Stüble, 2007). The mechanisms do not consider trust from users’ standpoint. This trust asymmetry could potentially result in a situation that the Grid users worry about the security of their jobs, tasks, confidential data, and so forth. This is because the resource providers in a Grid platform could cause damages to the users with little risk of detection or penalty. For example, an attacker hiding in a Grid platform might publish confidential data, or destroy the entire computation by providing false results. Due to this reason, companies hesitate to utilize the available Grid resources for confidential and important tasks (Löhr et al., 2007). Therefore, symmetrical trust between Grid users and the Grid platform is crucial for a successful Grid.

Trusted Grid is proposed to tackle this challenge of asymmetrical trust by leveraging Trusted Computing (TC) (Löhr et al., 2007; Martin & Yau, 2007). TC is defined and developed by the Trusted Computing Group (TCG) to ensure that a system will behave in specific ways, and those behaviors will be enforced by hardware and software (TCG Specification, 2007). Trusted Platform Module (TPM) is designed by TCG to ensure that the ownership of a platform can be asserted by asset managers, while allowing users to perform jobs. A TPM contains a set of Platform Configuration Registers (PCRs) to securely store a representation of the platform’s configuration information. Therefore, the TPM can be employed to guarantee that each computer will report its configuration parameters in a trustworthy manner. TC can not only be maintained in a single platform (e.g., endorsement key, memory curtaining, and sealed storage), but also provide attestation to a remote challenger. Attestation indicates that a trusted platform attests and reports its integrity state recorded in the PCRs. If a Grid platform can offer remote attestation to Grid users to ensure that the platform is trusted, the users would be very happy to use the Grid resources, thus improving the resource utilization. The reader is referred to (Trusted Computing Group, 2007) for a comprehensive understanding of the TC related knowledge.

The objective of Grid is to virtualize the geographically distributed resources and allow users and applications to access resources as a single machine (Deng & Wang, 2007). A large-scale and complex Grid application could involve hundreds or thousands of geographically distributed resources. With the growth of application requirements, a Grid system should have the ability to continue to provide satisfied capabilities including resources, performance, and fault tolerance in a transparent manner when the system is increased in size. Monitoring and Discovery System (MDS) (The Globus Alliance, 2009b; Deng, Wang, & Ciura, 2009) is a key component to provide basic mechanisms for resource discovery and monitoring in a typical Grid environment. If Grid users want to validate the integrity of a Grid platform, they have to verify the MDS through remote attestation, since all resources are registered in the MDS. However, the TPM is a secure microcontroller with limited computing power. If hundreds or thousands of Grid users perform the remote attestation simultaneously, a single MDS equipped with TPM is doomed to be a system bottleneck. Furthermore, the MDS has to provide resource query, store-and-forward of the submitted jobs and job results. Therefore, a distributed policy consisting of multiple TPM-equipped MDSs is required to deal with this challenge.

Traditional approaches maintain a centralized MDS or a set of hierarchically organized MDSs to index resource information in a Grid. However, three reasons limit the efficiency of the traditional approaches. The first, the centralized approach, and the root node of the hierarchical method have the inherent drawback of a single
Related Content

Resource Management in Real Time Distributed System with Security Constraints: A Review
[www.igi-global.com/article/resource-management-real-time-distributed/53851?camid=4v1a](www.igi-global.com/article/resource-management-real-time-distributed/53851?camid=4v1a)

The Development of a Parallel Ray Launching Algorithm for Wireless Network Planning
[www.igi-global.com/chapter/development-parallel-ray-launching-algorithm/72247?camid=4v1a](www.igi-global.com/chapter/development-parallel-ray-launching-algorithm/72247?camid=4v1a)

CAPM Indexed Hybrid E-Negotiation for Resource Allocation in Grid Computing

OBIRE: Ontology Based Bibliographic Information Retrieval in P2P Networks
[www.igi-global.com/article/obire-ontology-based-bibliographic-information/47427?camid=4v1a](www.igi-global.com/article/obire-ontology-based-bibliographic-information/47427?camid=4v1a)