A Composite-Service Authorization Prediction Platform for Grid Environment*

Chuanjiang Yi, Hai Jin, and Sheng Di

Services Computing Technology and System Lab
Cluster and Grid Computing Lab
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
hjin@hust.edu.cn

Abstract. In workflow and grid environment, the security challenges with the appearance of composite service increasingly become more severe than before especially to the traditional static access control model and dynamic authorization model. To solve these challenges, we presented a Dynamic Access Control Prediction mechanism for service workflow on the basis of Markov Chain. In fact, this prediction mechanism is only one part of the larger system, *Composite-Service Authorization Prediction* platform (CAP), which is totally composed of three key modules---- composite-service pre-processing, result feedback, and authorization prediction. In this paper, we present the design of its architecture as a whole.

1 Introduction

With the Internet and business globalization substituting the separation which used to be a typical role in the traditional business paradigm [1], some problems to the traditional static and dynamic access control model occurred, especially in the workflow [1][2] and grid environment [3]. According to the background knowledge of workflow and grid, we can find a common range in which subjects and objects belong to different organizations and finally condense them into a composite service model. So, it is probable that the sub-elements of composite service belong to completely different organizations, or limited by various policies.

The appearance of composite service causes three challenges to static access control model:

- The relations between subjects and objects cannot maintain a fixed connection, in that they are constrained by their respective security rules and can be added or deleted anytime.
- The previous simple static access control policy on objects is not able to distinguish diverse access requests from various organizations submitted by one and the same subject.

* This paper is supported by National Science Foundation under grant 90412010 and China CNGI project under grant CNGI-04-15-7A

Y. Luo (Ed.): CDVE 2007, LNCS 4674, pp. 217–225, 2007.

- When a subject belongs to varied real organizations, an object will be put into different VOs in different jobs. If the rules to control the access of the object are all static, it is probable that a static access control policy would be used in different VOs. This will cause confusion in managing VO.

In addition, it also causes another two challenges to dynamic access control model:

- Different dynamic authorization policies on different services may conflict each other. Thus it may cause failures of executing jobs.
- The authorization policy may be changed temporarily and dynamically just before the service is called, and this unexpected state will cause the job failure either.

To solve all the challenges mentioned above, we focus on the dynamic creation of access control policy for grid environment based on the CGSP project [4] and present a Dynamic Authorization Prediction mechanism for service workflow on the basis of Markov Chain. Consequently, we develop *Composite-Service Authorization Prediction* platform (CAP) to help achieve flexible and reliable access control.

The remainder of this paper is organized as follows. Section 2 describes our motivating scenario. We review related authorization research in section 3. Section 4 presents the architecture of CAP and the modules function. In section 5, we introduce key methods used in CAP. Conclusions and our future work are given in Section 6.

2 Scenario

The underlying common grid computing platform in ChinaGrid project is called *ChinaGrid Supporting Platform* (CGSP) [4]. One important characteristic of CGSP 2.0 is that the Job Manager module can parse, schedule, execute and monitor composite services. After modeling a composite service as an Ordered Service Sequence, we develop a new approach to calculate the conditional probability of one service execution in a set of service sequence in Markov Chain. We create access control rules dynamically according to these calculated values.

Imagine such a scenario: the CGSP environment has deployed a composite service , *CS* for short, which is composed of 4 atomic services named *a, b, c* and *d*. Assume that a legal user of CGSP, called Alice, wants to access *a*. Not only has the *CS* job been successfully submitted, but its first three services, *a, b* and *c*, have also been finished. Unfortunately, the job may still fail just because Alice does not own the access to the last atomic service, *d*.

Consider another scenario: Alice, via role *r*, calls service *a* for a computational fluid dynamics job, *J1*, at 9:00, and at 14:00, she calls *a* again to finish an image-processing job, *J2*, through the same role *r*. These two requests are plausibly the same (just the original data are different), but in fact they are submitted for two different jobs. This situation will cause two potential security problems. One is that the static access control policy can not distinguish the difference between these two service calls. The other is that the same static access control policy will be used in different VOs. This situation will cause confusion on the management of VO. Therefore, when the two jobs belong to two different organizations, the service *a* will be put into