Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A secure collaboration service for dynamic virtual organizations

Jianxin Li[a,*], Jinpeng Huai[a], Chunming Hu[a], Yanmin Zhu[b]

[a] School of Computer Science & Engineering, Beihang University, Beijing, China
[b] Department of Computer Science & Technology, Shanghai JiaoTong University, Shanghai, China

ARTICLE INFO

Article history:
Received 7 July 2009
Received in revised form 4 May 2010
Accepted 8 May 2010

Keywords:
Virtual organization
Distributed computing
Security policy
Secure collaboration
Privacy
Policy evaluation

ABSTRACT

Nowadays, various promising paradigms of distributed computing over the Internet, such as Grids, P2P and Clouds, have emerged for resource sharing and collaboration. To enable resources sharing and collaboration across different domains in an open computing environment, virtual organizations (VOs) often need to be established dynamically. However, the dynamic and autonomous characteristics of participating domains pose great challenges to the security of virtual organizations. In this paper, we propose a secure collaboration service, called PEACE-VO, for dynamic virtual organizations management. The federation approach based on role mapping has extensively been used to build virtual organizations over multiple domains. However, there is a serious issue of potential policy conflicts with this approach, which brings a security threat to the participating domains. To address this issue, we first depict concepts of implicit conflicts and explicit conflicts that may exist in virtual organization collaboration policies. Then, we propose a fully distributed algorithm to detect potential policy conflicts. With this algorithm participating domains do not have to disclose their full local privacy policies, and is able to withhold malicious internal attacks. Finally, we present the system architecture of PEACE-VO and design two protocols for VO management and authorization. PEACE-VO services and protocols have successfully been implemented in the CROWN test bed. Comprehensive experimental study demonstrates that our approach is scalable and efficient.

1. Introduction

There is an increasing demand for resource sharing and cooperation to support complex business processes and agile applications. Many promising paradigms of distributed computing, such as grid computing, peer-to-peer computing, pervasive computing [29,30] and cloud computing [2], have recently emerged for resource sharing and aggregation across multiple administrative domains. A virtual organization (VO) [4,7] is a dynamic coalition of geographically dispersed resources and users from different domains, which are unified by a common goal. Even in a centralized cloud computing environment, more and more users tend to build virtual organizations to aggregate the capabilities of both private cloud resources (e.g., the resources provided by local enterprises) and public cloud resources (e.g., the resources provided by Amazon EC2 or S3) in order to achieve collaborating goals.

There is a great security challenge for such virtual organizations. First, collaborating domains may join and leave dynamically during a business collaboration process. Second, to build a virtual organization, a participating domain may be required

[*] Corresponding author.
E-mail addresses: lijx@act.buaa.edu.cn, lijx@buaa.edu.cn (J. Li), huaijp@buaa.edu.cn (J. Huai), hucm@act.buaa.edu.cn (C. Hu), ymzhu@stju.edu.cn (Y. Zhu).

0020-0255/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2010.05.014

to disclose sensitive policies. It has become a fundamental problem how to create a secure collaboration environment for virtual organizations.

We look at a motivating example as follows.

Example 1. A national disease research centre encounters an epidemic disease and is not able to treat it. Thus, it needs cooperation from several other hospitals. In this case, a virtual organization comprising the national center and the hospitals should be established for the temporal cooperation. However, it is a key issue to create security policies for the new VO based on the security policies of the local domains. At the same time, the security policies of a domain is concerning privacy and therefore the domain's autonomy must be retained while the users of every domain in this VO can access a wide range of special services.

A number of approaches to security management of virtual organizations have been proposed. These approaches can be classified into two categories: *general approach* and *federation-based approach*.

A *general approach* completely creates a new set of policies for the virtual organization, and assigns new identities or attributes to all users or services in the virtual organization. It is an easy-to-implement approach and has been adopted by most grid systems. This approach, however, cannot fully accommodate the dynamism of virtual organizations in which collaborators may join or leave frequently. This implies that the security policy for local domain users and services cannot be fully utilized, and it introduces a heavy management burden. It is overwhelming for the system to assign identities to all the potential users or services. Moreover, the policies of the virtual organization have to be updated whenever the access control policy of a domain resource changes.

A *federation-based approach* reuses the original security policies of participating domains by defining their trust relationships through identity mapping, role mapping or delegation policies. This is an efficient approach, but we have found that collaboration policies defined by this approach may have possible conflicts. Policy conflicts lead to a potential security threat to local domains. For example, a user with a lower privilege may gain a higher privilege through an identity mapping loop. In this paper, we illustrate some examples through the role-based access control (RBAC) model [22], where a role is associated with permissions.

Notation statement: a role is denoted by r, with or without subscript. If role r_{A2} is senior to role r_{A1}, this inheritance relationship is denoted by $r_{A2} \prec r_{A1}$. If a user u is a member of role r_{A1}, then u acquires the permissions of role r_{A2}. A role mapping policy is denoted by m. We also denote this hierarchy relation with a role mapping policy m: (r_{A1},r_{A2}).

As shown in Fig. 1, there are two role mapping policies: m_2: (r_{C1},r_{B1}) and m_4: (r_{B2},r_{C2}) between domain C and domain B with a role hierarchy relation $r_{B2} \prec r_{B1}$. Based on these polices, we derive a new relation (r_{C1},r_{C2}) which brings on a conflict with the original role hierarchy relation $r_{C1} \prec r_{C2}$ in domain C. Thus, the security of local policies in domain C will be violated.

Traditional federation systems have different assumptions on virtual organizations. For example, secure interoperation is merely used to coordinate existing polices among security domains. In a virtual organization, new roles and policies should be defined for common tasks. Similarly, the policy conflict problem also exists in a virtual organization using federation policies. Unfortunately, such a serious problem is neither recognized nor addressed by existing work. Next, let us consider the following example.

Example 2. A federation-based virtual organization scenario shown in Fig. 2. Domain A and domain B form a virtual organization VO. The administrator of this virtual organization defines a role hierarchy relation $r_{VO3} \prec r_{VO1}$ and a task policy m_1: (r_{B1},r_{VO1}) which means r_{B1} in domain B has the permissions of r_{VO1}. In domain B, it has $r_{B1} \prec r_{B2}$, and also defines a mapping policy m_2: (r_{VO3},r_{B2}).

As illustrated in Fig. 2, we can also derive a new relation (r_{B1},r_{B2}), similar to the scenario in Fig. 1, through three policies m_1, m_2 and $r_{VO3} \prec r_{VO1}$. However, this relation also violates the role hierarchy relation of domain B. Thus, such conflicts should be detected during the creation of VO collaboration policies.

Several methods have been proposed for detecting policy conflicts in a federation-based VO management system. Some novel approaches [11,23] to deal with policy conflicts. The main idea is that all participating domains first submit their local

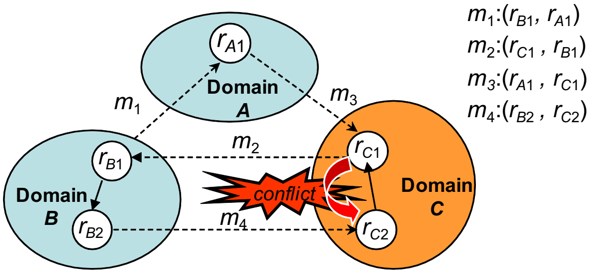

Fig. 1. Example for federation-based collaboration.