Validation of a Trust Approach in Multi-Organization Environments

Khalifa Toumi, TELECOM & Management SudParis, Evry, France

Ana Cavalli, César Andrés, Universidad Complutense de Madrid, Madrid, Spain

César Andrés, TELECOM & Management SudPAris, Evry, France

ABSTRACT

A Multi-Organization Environment is composed of several players that depend on each other for resources and services. In order to manage the security of the exchange process the authors introduce the concept of trust. The authors show how adding this aspect of the cooperative work. In particular, the authors provide a framework where the concepts of trust requirement and trust evaluation play important roles for defining trust vectors. These vectors evaluate a set of requirements, under some conditions, and provide a degree of confidence. In the authors' framework they consider two different types of vectors. On the one hand a vector that relates a user to an organization and on the other hand a vector that links two organizations. Different simulations are presented in this paper in order to show this approach. Moreover, the authors show how these vectors are evaluated and shared among the different organizations. Finally, the authors propose a possible architecture to explain how to integrate their trust module in MOE in order to enhance the security.

Keywords: Experience, Knowledge, Multi-Organization Environment, Reputation, Trust Vector

1. INTRODUCTION

Currently the widespread of inexpensive communication technologies, distributed data storage and web services mechanisms urge the collaboration among organizations. A *Multi-Organization Environment*, in short MOE, consists of a set of organizations where each one acts as an O-grantee and/or O-grantor (Cuppens et al., 2006). The O-grantor is the participant which offers a resource to be used by another organization called the O-grantee. In this context an interoperability security policy defines how to control the access to shared resources. Currently, the protocols to assign these policies to the users introduce an abstraction layer and the concept of role appears (Kalam et al., 2003; Cuppens et al., 2006; Kalam et al., 2009). A role corresponds to different job descriptions in an organization. Therefore, users are assigned to different roles receiving the relevant rights to perform tasks. Usually this assignment is done based on the exchange of some credentials which allow us to introduce the concept of trust (Jiang and Baras, 2008), (Haidar et al., 2009).

The definition of a trust model (Ray & Chakraborty, 2004; Lin et al., 2005; Chakraborty & Ray, 2006; Jiang & Baras, 2008; Marmol & Perez, 2009; Wang & Li, 2011) has been widely accepted as an innovative solution to improve

DOI: 10.4018/ijsse.2014010101

the access control of resources. However, the notion of trust based on credentials implies a "strict definition" of trust. For example, previous approaches do not consider the recent experiences of the organizations with the service provider. In particular, the validity and the value of some attributes change over time which can produce a conflict evaluation (Chakraborty & Ray, 2006). Moreover, this information may be partial and incomplete in autonomic environment (Jiang & Baras, 2008). These characteristics appear in MOE arising the following issues:

1. How can trust be defined in a MOE environment?
2. How can we take into account the dynamic behavior of any organization and its users?
3. How can we provide a measure of the impact of the organizational behavior on the control access of its users?

The main contribution of this paper is to present a trust framework to answer these issues.

The Figure 1 illustrates the basic concept of our proposal. In this approach we introduce two types of trust vectors, the first one is related to users (*utv*) and the second one is related to organizations (*otv*). For instance, the organization trust vector *otv*= (*e,r,k*) means that the trust relationship between two organizations will depend on three parameters. The first one corresponds to the previous interactions between the truster and the organization; that is, the historical interaction log. The second one represents the reputation of the trustee in the MOE environment. Finally, the last one denotes the knowledge of the organization regarding the truster.

An additional contribution of this paper is to provide an evaluation method for each parameter of these vectors. In our model, these evaluations are dynamic, that is, the evaluations depend on time. Therefore, we have that trust is a relation among two entities (the trustee and the truster), related to a specific behavior of the trustee (situation), in a specific slot of time.

For instance, within this notation we are able to represent security properties that follow this pattern:

If an organization orgB is assigned to a low trust level value regarding another organization orgA, then this fact affects on the trust level of the users of the organization orgB.

A user might lose some rights if he and/or his organization performs bad behaviors, since their trust levels are not static.

The rest of the paper is structured as follows. The Section 2 studies the related work. In Section 3 some preliminary MOE concepts are introduced. Next, in Section 4 the trust model parameters experience, reputation and knowledge are presented and evaluated. Following, Section 5 details the trust vectors. Section 6 details the different components to be used in order to integrate the trust module. Finally, in Section 7 we give the conclusion and future work.

2. RELATED WORK

Several studies have investigated the control access in MOE (Cuppens et al., 2006; Kamel et al., 2008; Kalam et al., 2009; Armando et al., 2012). These approaches focus on the choice of a control access model and its adaptation to the MOE environment (dynamism, abstraction, distributed authentication, etc). However, the definition of a trust model and its integration into an access control model is not the main focus of these works.

In other research works (Ray & Chakraborty, 2004; Lin et al., 2005; Jiang & Baras, 2008; Marmol & Perez, 2009; Krautsevich et al., 2010; Agudo et al., 2010; Wang & Li, 2011; Costa et al., 2011; Moyano et al., 2012; Armando et al., 2012) the crucial concept of trust in distributed systems is widely studied. Based on these works trust depends on the *environment* and on the *evaluation* of relevant parameters. For instance, in (Krautsevich et al., 2010) a general framework for usage control on grid systems is presented. In this work three concepts: trust management, reputation and risk assessment are embedded in this framework. In addition in Costa et al. (2011) a