Chapter 5.2
Trust Management for Grid Systems

Benjamin Aziz
STFC Rutherford Appleton Laboratory, UK

Alvaro Arenas
STFC Rutherford Appleton Laboratory, UK

Fabio Martinelli
Istituto di Informatica e Telematica, CNR, Italy

Paolo Mori
Istituto di Informatica e Telematica, CNR, Italy

Marinella Petrocchi
Istituto di Informatica e Telematica, CNR, Italy

Michael Wilson
STFC Rutherford Appleton Laboratory, UK

ABSTRACT

Grid computing is a paradigm for distributed computation on shared resources. It uses a large-scale, highly decentralized infrastructure, in which a huge number of participants share heterogeneous resources for a given purpose. Each participant both provides their own resources and exploits others' resources, combining them to solve their own problems. Trust management is a major issue in the shared Grid environment because Grid participants are usually unknown to each other and usually belong to separate administrative domains, with little or no common trust in the security of opposite infrastructures. The standard security support provided by the most common Grid middleware may be regarded as one means through which such common trust may be established. However, such security solutions are insufficient to exhaustively address all the trust requirements of Grid environments. In this chapter, the authors survey proposals for enhancing trust management in Grid systems.

INTRODUCTION

Innovations in information technology and business models are creating new security issues which require designs beyond those of traditional security solutions. In particular, the problem of guaranteeing that only authorized users have access to sensitive resources and data has been traditionally solved by adopting access control techniques. In these techniques the decision process is based on the identity or the role of the user. Since, in distributed environments with no central authority, the resource owner and the user that accesses the resource are often unknown to each other, traditional access control techniques cannot be applied. Consider an example in which a

DOI: 10.4018/978-1-4666-0879-5.ch5.2

research institute adopts the policy of granting the right to execute applications on the computational resources shared by the institute, to professors of accredited universities. Although one authority may assert that the requestor's identity is Alice Black, if this identity is unknown to the research institute, this does not help in making a decision whether she is entitled to use the resources or not. The crucial information needed in such scenario is the set of rights and qualifications of the requestor asserted by recognized authorities (i.e., the university she attends) together with trust information about the authorities themselves (is that university accredited for the research institute?). Trust management (Blaze et al., 1996), was born to implement distributed access control in decentralized systems, where access control decisions are based on statements called credentials made by multiple principals.

Grid is a distributed computing environment where each participant shares a set of his resources with others (Foster et al, 2001). This environment may group participants into virtual organizations. A virtual organization is a set of individuals and/or institutions (e.g. companies, universities, research centres, industries and so on) who share their resources. A Grid user exploits this environment by searching among the available resources for a set that can be exploited to solve his problem. These resources are heterogeneous in that they could be computational, storage, software repositories and so on. The Open Grid Forum community has developed a standard to share resources on the Grid called the Open Grid Service Architecture (OGSA) (Foster et al, 2006), which defines the concept of Grid services and it is based on the Web Service Resource Framework (WSRF) (Banks, 2006). The Globus Toolkit 4 (Foster, 2005), is the reference implementation of the OGSA standard, and in this paper we refer to this implementation as the Grid environment (although the model developed applies to any possible implementation). Security is a very important issue for the Grid, because the participants are probably unknown to each other, and they belong to distinct administrative domains that adopt different security mechanisms and apply distinct security policies. Moreover, some participants can join or leave the virtual organisation during its lifecycle.

This chapter shows how trust management techniques can be successfully applied to support and enhance Grid security mechanisms. We will describe models, architectures, and implementations of trust management systems for the Grid, especially tailored for virtual organizations deployment. We review the existing models and the proposed architectures, as well as some prominent implementations for existing Grid toolkits (e.g., Globus). Both researchers and practitioners may benefit from this survey, which provides the state of the art at a glance and hints for future research and development.

The structure of the chapter is as follows. The next section gives an overview of the paradigm of virtual organizations, commonly used to model resource sharing in Grid systems. The third section gives an overview of some popular Grid security models and architectures as a means for establishing trust. In the following section, we discuss a couple of trust models and architectures; one for enhancing a role-based and trust management language with weights and the other for utility-based reputation management in Grids. Finally, we conclude the chapter with a discussion on possible future trends for Grid trust management.

VIRTUAL ORGANIZATIONS IN GRID COMPUTING

Overview

Grid computing is a term often used to describe the amalgamation of several existing technologies such as cluster computing, Peer-to-Peer (P2P) computing and Web services technologies. In order to understand the behavior of such a heterogeneous blend of technologies, Grid systems are