Security and Trust Management for Virtual Organisations: GridTrust Approach

Syed Naqvi and Paolo Mori

Abstract The GridTrust Security Framework (GSF) offers security and trust management for the next generation Grids (NGG). It follows a vertical approach for Grid security from requirements level right down to application and middleware levels. New access control models for collaborative computing, such as the usage control model (UCON), are implemented for securing the Grid systems. The GSF is composed of security and trust services and tools provided at the middleware and Grid foundation middleware layers. GSF addresses three layers of the NGG architecture: the Grid application layer, the Grid service middleware layer, and the Grid foundation layer. The framework is composed of security and trust services and tools provided at the middleware and Grid foundation middleware layers. GSF provides policy-driven autonomic access control solutions that provide a continuous monitoring of the usage of resources by users.

1 Introduction

A secure Virtual Organisation (VO) requires that security objectives and requirements have been defined and are enforced throughout the VO lifecycle. GridTrust has employed a goal oriented requirements engineering method that is tailored for defining VO security objectives and refining them into enforceable security policies. An Eclipse-based policy design tool is developed that allows specifying and refining security objectives into requirements.

Syed Naqvi
Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC), 29/3 Rue des Frres Wright, 6041 Charleroi, Belgium e-mail: syed.naqvi@cetic.be

Paolo Mori
Istituto di Informatica e Telematica Consiglio Nazionale delle Ricerche (IIT-CNR), 1 Via G. Moruzzi, 56124, Pisa, Italy e-mail: paolo.mori@iit.cnr.it

The usage control model (UCON) is a new access control paradigm proposed by Park and Sandhu [4] that encompasses and extends different existing models. Its main novelty, in addition to the unification view, is based on continuity of usage monitoring and mutability of attributes. This model is employed in the GridTrust project due to its suitability for managing access/usage control in Grid systems. GridTrust defines a policy specification language, POLPA, which is a process description language that is able to express the basic policy models defined by UCON.

GridTrust explored a utility-based model for reputation, which in contrast to most other reputation models that require direct feedback from users, builds the reputation from information provided by monitoring systems, making it suitable for Grids.

2 The GridTrust Project

The GridTrust framework (as depicted in Fig. 1) addresses three layers of the NGG architecture: the Grid application layer, the Grid service middleware layer, and the Grid foundation layer. The framework is composed of trust and security services and tools as indicated in the figure. The trust and security services are provided at the Grid service middleware and Grid foundation middleware layer. The services all use usage control policies. The services at the service middleware layer are the following: a Secure Resource Broker, a Reputation service, and a Service Level Usage Control Service. At the Grid foundation middleware layer fine grained continuous computational Usage Control service is provided.

2.1 Technical Approach

The Secure Resource Broker is invoked by the VO owner to retrieve the set of resources required to set up his VO. The VO owner also specifies the security requirements of the services he needs. The Reputation service keeps track of the past behaviour of VO users. This service is exploited by other GSF services that need the current reputation of a VO user to perform the decision process. The Service Level Usage Control Service is a coarse grained authorization service that enforces XACML security policies to regulate the access to Grid services. The Computational Usage Control Service, instead, monitors the behaviour of the Java applications executed on computational services on behalf of remote VO users. This service is an implementation of the UCON framework proposed by Sandhu [4] adapted for the Grid necessities, and enforces a security policy written in POLPA, a process algebra based security policy language [2]. The service evaluates the security policy to decide whether each security relevant action performed by the application is permitted on the computational resource, and revokes actions in progress when the right does not hold anymore. To evaluate the security policy, the Computational Usage Control service interacts with the Reputation service, in order to get the current value of

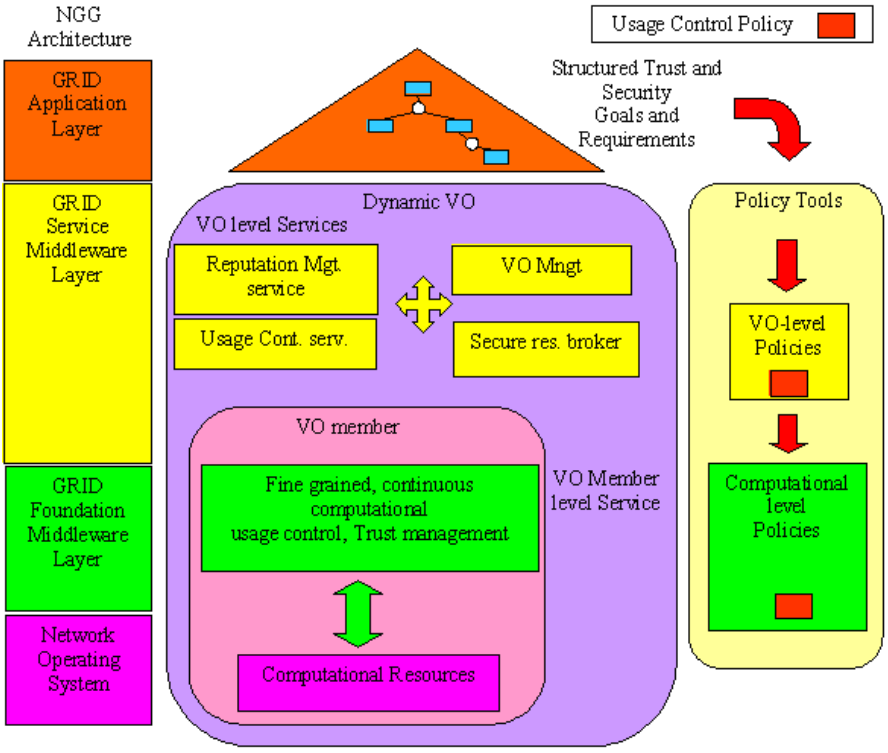

Fig. 1 GridTrust framework

the user's reputation attribute. Moreover, this service also reports to the Reputation service a feedback about the user behaviour on the computational resource.

The GridTrust framework policy tools aim to produce the security and trust policies needed by the different services. At the application level a requirements tool helps analysts define security and trust goals and requirements, and produces high-level security and trust policies. A policy refinement tool takes the abstract security and trust policies as input and refines them into service and computational level usage control policies. These usage control policies are used by the different trust and security services.

2.2 Innovation

The innovation of the GridTrust project is its integrated framework that provides a set of services performing the main Grid interactions in a secure way. These tools allow the Grid participant to create and manage VOs, to select resource providers having certain security requirements, to manage users' mutable attributes such as

the reputation, and to execute Java applications on behalf of remote Grid users in secure way, i.e. performing a fine-grained and continuous monitoring of computational services according to the UCON model. The cutting edge advantage of the GridTrust framework is that it consists of not only a simple authorization system but it provides a set of services that, exploiting the usage control model, enhances the security of the whole Grid lifecycle, starting from the VO formation, including the execution of Java applications on the VO computational services, until the VO dissolution.

3 Impact and Perspectives

The GridTrust project aims to enable companies to set up and operate dependable VOs that are secure and trusted. The demonstration will exhibit the various functioning of GridTrust tools for the security design and trust requirements of the VO. VOs will allow companies to provide and to access Grid resources to achieve common goals. VOs are also valuable in the larger context of Service Oriented Architectures to set up ”virtual” markets and to support collaboration between different units of a corporation or between cooperating players in the same market [3].

In order to support rapid formation of VOs, we use the concept of Virtual Breeding Environment (VBE). A VBE can be defined as an association of organisations adhering to common operating principles and infrastructure with the main objective of participating in potential VOs. We have adopted the view that organisations participating in a VO are selected from a VBE [1].

Acknowledgements The research leading to the results presented in this paper has received funding from the European Union’s sixth framework programme (FP6) Project GRIDTRUST under grant agreement number 033817.

References

1. L. Blasi, A.Arenas, B. Aziz, P. Mori, U. Rovati, B. Crispo, F. Martinelli, P. Massonet. A Secure Environment for Grid-Based Supply Chains. Proc. eChallenges Conference 2008. In: Collaboration and the Knowledge Economy: Issues, Applications, Case Studies, Paul Cunningham and Miriam Cunningham (Eds), IOS Press, 2008 Amsterdam, ISBN 978-1-58603-924-0
2. F. Martinelli, P. Mori. A Model for Usage Control in GRID Systems. In: Proceeding of GridSTP 2007, International Workshop on Security, Trust and Privacy in Grid Systems at SecureComm 2007. IEEE Computer Society, (2007), ISBN: 1-4244-0975-6.
3. S. Naqvi, P. Massonet, B. Aziz, A. Arenas, F. Martinelli, P. Mori, L. Blasi, G. Cortese. Fine-grained continuous usage control of service based Grids the GridTrust Approach. Lecture Notes in Computer Science, Vol.5377/2008, pp.242-253
4. R. Sandhu, J. Park. The UCONABC Usage Control Model. ACM transaction on Information and System Security, 7(1): 129-174, 2004