A Secure Environment for Grid-Based Supply Chains

Lorenzo BLASI[1], Alvaro ARENAS[2], Benjamin AZIZ[2], Paolo MORI[3], Umberto ROVATI[1],
Bruno CRISPO[4], Fabio MARTINELLI[3], Philippe MASSONET[5]
[1]*Hewlett-Packard Italiana S.r.l., Via G. di Vittorio 9, Cernusco sul Naviglio, 20063, Italy*
Tel: +39 02 92121, Email: lorenzo.blasi@hp.com; umberto.rovati@hp.com
[2] *e-Science Centre, STFC Rutherford Appleton Laboratory, Didcot, OX11 0QX, UK*
Tel: +44 1235 778840, Email: A.E.Arenas@rl.ac.uk, B.Aziz@rl.ac.uk
[3]*Istituto Informatica e Telematica CNR, via Moruzzi 1, Pisa, 56124, Italy*
Tel: +39 050 3152069, Fax: +39 050 3152593,
Email: paolo.mori@iit.cnr.it, fabio.martinelli@iit.cnr.it
[4]*Vrije Universiteit Amsterdam, De Boelelaan 1081a, Amsterdam, 1081HV, The Netherlands*
Tel: +31 20 5987829, Fax: + 31 20 5987653, Email: crispo@cs.vu.nl
[5]*CETIC, Rue des Frères Wright, 29/3, B-6041 Charleroi, Belgium*
Tel: +32 71 490 744, Email: phm@cetic.be

Abstract: This paper introduces a transportation supply chain which exploits Grid services for optimizing both the delivery and cost of each customer order. The proposed case study focuses on an auction-based model to select transporters for given transportation tasks in a generic supply chain. Each transporter uses a Grid-based computing service to re-optimize the routes of its vehicles after the addition of each new transportation task. The main objective of this paper is to describe a secure environment for the transportation supply chain by identifying its security issues and developing security components that help to solve these issues. These components are currently under implementation in the EU GridTrust project.

1. Introduction

Logistics is a service that moves its customer's products from one place to another. Big transporter companies may be chosen for their brand, but at the end what makes the difference is the quality and price of the service; thus competition in the transport sector is driven by the two main factors of delivery time and price.

A characteristic of current logistic systems is that only a few big players make use of global optimization techniques. Improving transporters fleets' utilization is an environment-friendly activity because it lowers the number of circulating trucks, but small transporters rarely apply operating-research techniques, as usually they don't have enough customers at the same time.

But how can a small transporter improve its operations to compete with big players? How can a transporter find enough transportation tasks to improve its own fleet utilization? And how can a customer find the best transporter for each given transportation task?

The proposed case study tries to answer the questions above with a solution based on two main ideas. The first is to use an auctioning system that exploits competition between transporters and allows customers to find the best provider for each task. The second idea is to have route computing services, i.e. computational services that provide maps and libraries to execute applications solving the logistic optimization problem, to allow even small (SME) transporters to optimize their routing. Both the auctioning system and the routing computing service will be hosted on Grid resources. This solution raises several security challenges such as selection of services with compatible security policies or continuous control of the execution of unknown applications, among others.

2. Objectives

The main objective of this paper is to describe a secure inter-enterprise Grid environment for a business case such as a transportation supply chain. The same secure environment can be widely applied to other scenarios as well, be they Grid- or SOA-based.

This paper identifies some security issues of the case study and introduces security components that help solving them, components such as a service for measuring and keeping track of users' trust level or a service providing continuous control to prevent malicious activities. These and other components described below are currently under implementation in the EU GridTrust project [1].

3. Methodology

The methodology we adopted in GridTrust follows these lines:

- Perform a security analysis of the scenario to define security requirements for the application using the KAOS goal-oriented requirements-engineering methodology [4], as well as to identify use cases and mis-uses cases.
- Identify and develop architecture components that could contribute to meet the main security challenges identified. These components are described in the next section;
- Evaluate how the architecture helps in solving the security challenges of the case study.

Currently GridTrust is in the implementation phase and the evaluation will be carried out in the next year. Our plan is to have a running version of the GridTrust Security Framework components by September 2008.

4. Technology and Business Case Description

This section describes the Virtual Organisation (VO) model adopted by the GridTrust project, our supply-chain case study, security issues related to the case study, GridTrust architecture, and its application to the case study.

4.1 A Model of Virtual Organisations

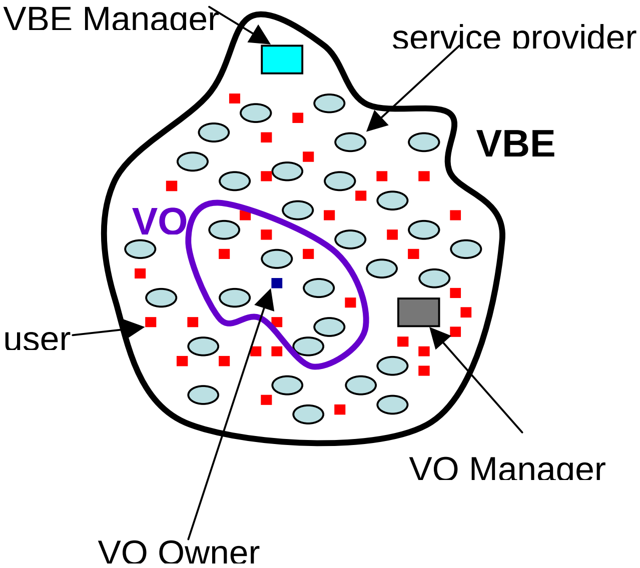

Figure 1: Organisations and Users in a VBE

In order to support rapid formation of VOs, we use the concept of virtual breeding environment (VBE) [3]. 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, as illustrated in Figure 1. Such organisations may provide resources/services (ovals), and include users that utilise VO resources (small squares).

4.2 A Grid-Based Supply Chain for Transportation

We have developed a supply chain based on auctions in order to find the best offer for a transportation task. The auctioning system, which runs reverse auctions of type First-Price Sealed-Bid [2], allows producers to propose Requests for Quotation (RfQ) for transportation tasks (such as “move N units of P from A to B”). Each Transporter who wants to make a competitive offer should recalculate its routing with the added transportation task; routing recalculation is performed on Grid resources using the routing computational services. After recalculation each transporter$_i$ can make its offer. Choice of the best offer may be based on price, planned delivery time and transporter’s reputation, depending on customer requirements.

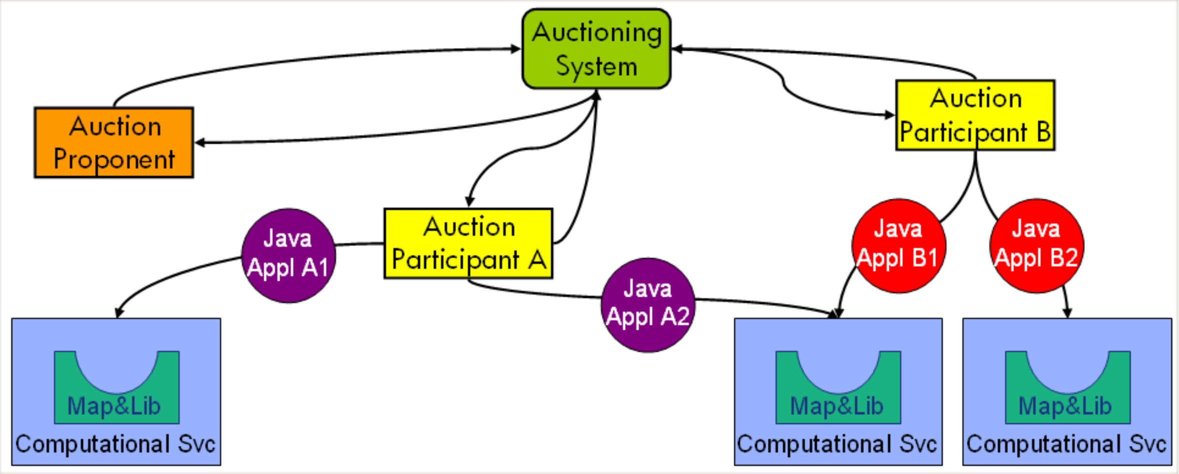

Figure 2 - Full Auctioning Scenario

The components of this business scenario are the following (see Figure 2):

- Auctioning system (a custom Grid service)
- Auction Proponent, it’s the Producer application (creates auction, receives result, creates Delivery VO)
- Auction Participant, is the Transporter application (notified of an auction, creates Routing VO, invokes routing calculation, sends an auctioning offer)
- Map&Lib, are Routing support services, (maps, map access library, base routing functionality) made available by the Computational Service provider
- Java Appl, is the Routing application (executed on Computational Service) which may be different for each Auction Participant

The Auction Proponent plays the role of a producer in a supply chain, creating a Delivery VO to manage the whole auctioning and delivering process. Each transporter participating in the auction (i.e. in the Delivery VO) creates its own Routing VO in order to calculate best routes to participate in the auction.

The Grid computational service provider(s) may offer several maps with different levels of accuracy for the underlying distance-time (DT) matrix and libraries implementing different algorithms for solving base routing problems.

In general the transporter already has a certain set of transportation tasks to be performed and already calculated a sequence minimizing the path length for each of its vehicles. Adding the requested transportation task this sequence has to be reoptimized. To perform such a reoptimization, calculating the added cost and thus creating an offer for the new task, the transporter will send to the computational service provider an application exploiting some of the provided maps and libraries.

When either auction time expires or offers are available from all invited bidders, the closing phase starts and the auctioning system selects the winning offer based on the optimization criterion defined at auction creation time.

A future implementation of the system will allow monitoring the whole delivery phase and verifying transporter's compliance with the offered terms of service (considering the offer as a SLA). The reputation index of a transporter is based on a history of its accomplishments; with the current implementation it lowers if the transporter's behaviour is not in line with VO security policies, but using a SLA monitor the reputation can be increased with successful shipments and lowered if the transporter doesn't fully comply with the terms agreed in the SLA.

4.3 Security Issues in a Grid-Based Transportation Supply Chain

The main security issues for the auctioning service are summarized as follows: secure identification of auction participants, secrecy of offers at least until auction closure, data integrity and non-repudiation of both offers and RfQs.

Routing services also raise important security issues, mainly originating from the fact that they execute unknown applications on behalf of potentially unknown or not trusted users. Hence, a security support is required to control that these applications do not perform actions meant to steal valuable data or to gain unauthorized accesses. For example, if a transporter is paying a monthly subscription for using map A, it cannot use map B.

The use of reputation information as one of the parameters for selecting transporters is a fundamental part of the proposed model. Transporters' reputation can be measured with respect to their complying with global and local security policies defined for Grid resources. In the future it will be measured also with respect to the transporters' ability in honouring the agreed SLAs for delivering goods.

4.4 GridTrust Architecture

In this section we describe the main components of the GridTrust Security Framework (GSF) that contribute to meet security challenges identified in the previous section. GSF services are developed at the Grid middleware layer and as Globus has been chosen as reference Grid middleware, they are developed as additional Globus services.

- The **VBE Manager** acts as a service registry, where service providers register their services and other GSF services can retrieve them given abstract service descriptions. Each Virtual Organization (VO) will be created within a specific Virtual Breeding Environment (VBE); a VBE may contain several different VOs.
- The **VO Manager Service (VOM)** coordinates all other security services and is the single point of access for users and service providers participating in the VO. The VO Manager is responsible for handling several functionalities. These include VO creation, populating VOs with services required by VO owners to achieve their goals, updating VO policies, evolving the VO by allowing its member service providers to subcontract part of their services to other service providers and finally, terminating the VO.
- The **Policy and Profile Manager (PPM)** keeps all the knowledge bases needed by GSF services: VBE and VOs users, with security preferences and their trust and

reputation credentials; VOs with their owner and security policies; service providers with their services and security policies regulating access and usage of the services.

- The **Secure Resource Broker (SRB)** is called by VOM with a list of services, needed by the VO Owner to form its VO, and the associated security requirements. It returns the list of providers offering the requested services and also satisfying all the specified security requirements. One of those requirements is the reputation of a service in a VBE.
- The **Trust and Reputation Service (TR)** keeps track of the past and current behavior of VO owners, users and service providers and transforms it into trust and reputation credentials that can be considered by other users, service providers and GSF services when making decisions.
- The **Continuous Usage Control Service (C-UCON)** is an implementation of the UCON policy framework [5], where it is deployed on each service provider and is responsible for the evaluation and runtime enforcement of policies about resource usage in VOs. It also reports feedback to the TR service about users violating these UCON policies.

Each of these services can be invoked only by mean of the API it exports, hiding all the implementation details on how the service is implemented. The framework is flexible so during the project we provide instance implementations for each service, but implementations developed by third parties can easily replace ours. Besides, the framework is modular so it allows the possibility of adding future new security services if needed.

4.5 Applying GridTrust Services in the Transportation Supply Chain

To satisfy the identified security issues a secure Grid environment is needed. When the Producer in the supply chain scenario receives an order from a Customer, it utilizes GSF components to construct a secure Delivery VO whose members are shown in Figure 3.

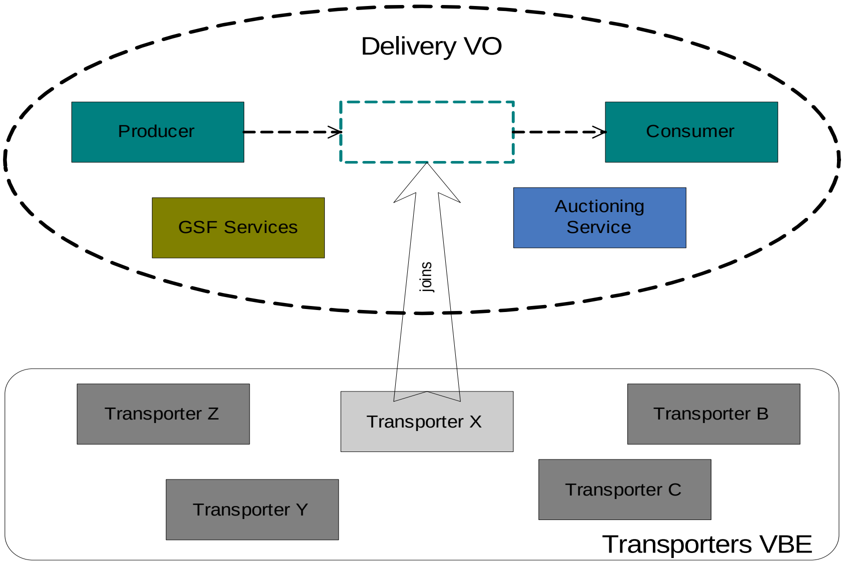

Figure 3: The Delivery VO and its Transporters VBE

This is done over several phases. In the first phase, the producer requests from the VOM service the creation of a Delivery VO. In the next phase, the Producer registers with the PPM service (through the VOM) the list of VO users and their security profiles. Then the Producer requests from the VOM to search for a suitable auctioning service by including the abstract description of the service and of security requirements (e.g.

reputation level). The VOM utilizes the SRB service in its search and once the right candidates are reported back to the Producer, the Producer will inform the VOM of its selection and SRB will negotiate and schedule the selected candidate. The operational phase now commences with the Producer sending to the auctioning service a Request for Quotation (RfQ) for delivering the ordered goods. This triggers each transporter to start a new Route-Calculation VO as shown in Figure 4, which will include Computational Services (CS) needed to compute the route and the bid. The route-calculation services will be derived from a Computational Services VBE. Each transporter chooses the most suitable set of CSs depending on the maps and the libraries offered, and also taking into account the security features, and it will submit its route calculation application to these services. The result returned by the route calculation application executed on the computational services is a new sequence of paths, one for each vehicle, paired with its incremental cost that allows the transporter to define its bid. The winning transporter with the best bid is then reported back to the Producer, which requests from the VOM the addition of that transporter to the delivery VO. The delivery VO is now fully operational.

This flow of events highlights how the GSF components, which build on and complement consolidated Grid security techniques, can satisfy the security issues of the scenario. The SRB service, when receiving from the Producer the security requirements of the auctioning service, is able to select the suitable candidates fulfilling those requirements. Such security requirements may be, for example, that the auctioning service must maintain the integrity of bids and secrecy of offers.

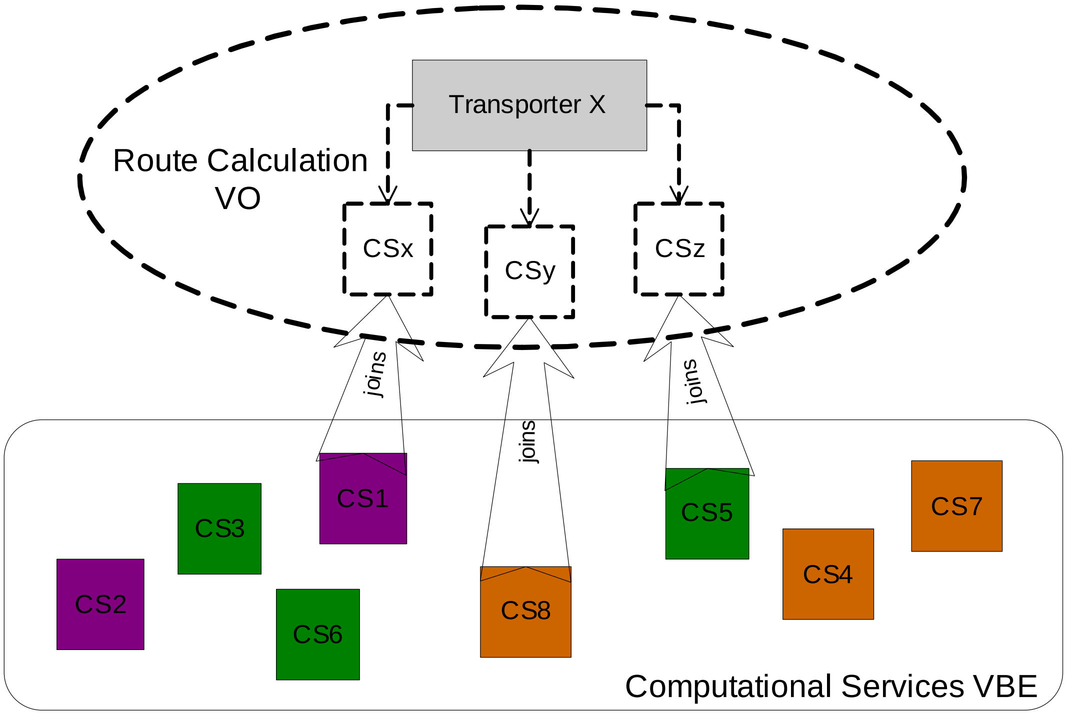

Figure 4: The Route-Calculation VO and its Computational Services VBE

The security of the CSs exploited by the transporters to compute their new paths is addressed by another GSF component, the UCON service. From their point of view, the CSs execute unknown applications on behalf of potentially unknown and untrusted users, and these applications could perform dangerous actions that could harm or damage the services. The UCON service allows to monitor the execution of these applications and to enforce a security policy preventing them from performing dangerous operations. In particular, the policy defines the admitted behaviour of the applications in terms of interactions with the underlying operating system. The CS owner could enforce also policies to regulate the usage of the maps and libraries offered by his service. As an example, the policy could state that the application can, in principle, use any map, but when it accesses one of the maps it cannot access the others anymore. The UCON service can both take into account the user reputation, computed by the TR service, to decide whether to allow a given action of the route calculation application, and can provide feedback to the TR service about the application behaviour to update the user reputation value.

5. Conclusions and Summary Recommendations

We have shown how Grid-based supply chains can be secured by associating them with trust and security management services such as VBE and VO managers, secure-aware resource brokers, reputation services, and usage control services, among others. The solution we have proposed, called the GridTrust Security Framework (GSF), incorporates these services in a manner that is modular, interoperable and security-aware.

Interoperability and Modularity. Since we are re-using an existing Grid infrastructure, which is the Globus middleware, our system components are interoperable with other Globus-based components. This facilitates future development of Globus-based solutions. In fact, the GSF components are modular in that any combination of these can exist in any Globus-based solution.

Security-aware design. The design we propose for the environment of the Grid-based supply chain case study is security-aware in that it tackles current security issues that may arise in any Grid-based system. The security requirements were elicited using a requirements-engineering methodology that has been tailored for Grid systems [4].

There are three main innovations in the GSF. First, in SOAs and Grids have been identified the need for having security into account when selecting services or brokering resources. Our Secure Resource Broker service solves this by having into consideration security information such a policies and reputation values when brokering resources. Second, we are combining in an effective way social-control mechanisms such as reputation and security, by using the Trust and Reputation service to quantify security for both Grid users and resources. Third, the Continuous Usage Control service controls the usage of Grid computational resources by applying fine-grained and history-based access control, and improves state of the art with mutable attributes, obligations and continuous enforcement. Existing authorisation systems in Grid simply check that the remote Grid user has the right to execute an application, considering applications executed on computational resources as atomic entities. Hence, once they authorise the execution of an application, no further controls are executed on the actions performed by this application on the resource. Instead, in GSF authorisation framework, the monitoring is fine grained, because the actions performed by applications on the resource are controlled, and history-based, because to decide whether an action should be allowed all the previous actions performed by the application are taken into account. Moreover, in GSF framework rights are dynamic, because attributes and conditions may vary over time. This means that, while an access is in progress, the factors that authorised it could change and the access right could not hold anymore. Consequently, in our framework, the control of the existence of a right is continuous (i.e. repeatedly performed during the access), to revoke an access that is in progress when the right does not hold anymore.

One lesson we learnt at this stage is that the complexity of Grid-based supply-chain systems (exemplified by our auctioning system and its multiple VOs) has suggested the need for lightweight and dynamic VO models. During the evaluation phase we expect discovering more insights, for example about the role of VBEs or the need for VBE federation, but also about VBE/VO design guidelines and more.

Future work includes further evaluation of the GridTrust services in other scenarios and the addition of new features to the security services such as distributed reputation management and VBE federation. Another important issue is human readability of security policies. Since the security policy enforced by the UCON service can be defined at the VO level, at the computational resource level, or can be a combination of these two, one important issue we are facing is how to express the security policies at VO level in a human readable format and how to translate these policies in an enforceable format.

References

[1] P. Massonet, A.E. Arenas, F. Martinelli, P. Mori, and B. Crispo. *GridTrust – A Usage Control Based Trust and Security Framework for Service-Based Grids*. In E. di Nitto, A.-M. Sassen, P. Traverso, and A. Zwegers, editors, “At your service: Service Engineering in the Information Society Technologies Program”. MIT Press, 2008. (To appear).

[2] Carter et al, *Reverse auctions—grounded theory from the buyer and supplier perspective* - http://www.econbiz.de/archiv/myk/whumyk/controlling/auctions_theory_perspective.pdf

[3] L.M. Camarihna-Matos, and H. Afsarmanesh, H. *Elements of a base VE infrastructure*. Journal of Computers in Industry, 51(2):139–163, 2003. (available at http://www.uninova.pt/~cam/ev/CiI.PDF)

[4] van Lamsweerde, *Requirements Engineering in the Year 00: A Research Perspective*, in Proceedings of the 22nd International Conference on Software Engineering, Limerick, Ireland, ACM, pp. 5-19, 2000. (available at http://www.sis.uncc.edu/~seoklee/teaching/Papers/lamsweerde00requirements.pdf)

[5] R. Sandhu and J. Park, *Usage Control: A Vision for Next Generation Access Control*, in Proceedings of the Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM03), Springer LNCS, 2776, pp. 17--31, 2003. (available at http://www.list.gmu.edu/park/paper/MMM03-UCON-vision.pdf)