IST-2001-32133
GridLab - A Grid Application Toolkit and Testbed

D6.1 "Requirements Document"

Author(s):	Marcin Adamski, Michal Chmielewski, Sergiusz Fonrobert, Adam Gowdiak, Bartosz Lewandowski, Jarek Nabrzyski, Tomasz Ostwald, Juliusz Pukacki
Document Filename:	
Work package:	WP6 Security
Partner(s):	
Lead Partner:	Poznan Supercomputing and Networking Center
Config ID:	GridLab-6-D1-0001-1
Document classification:	INTERNAL

Abstract: This document is the initial version of design requirements for security workpackage (WP6) in the GridLab project. As such, this document is not intended to be any binding version but should rather be considered as a material for discussion and further work.

Version: 1.0
Updated: April 1st 2002

Contents

1 The goals of WP6

The goal of WP6 is to provide an acceptable level of security to virtual organizations created within the GridLab project. This goal requires creating appropriate security infrastructure covering all aspects of operating in the grid environment.

Based on users and developers requirements, the following main properties of such an infrastructure can be specified:

- it should be a base for a trustable and secure environment,
- should support various types of resources,
- should enable to define multiple collaborative groups within the virtual organization,
- should support multiple credentials (originating from various trusted parties),
- should be possibly transparent to users and applications,
- should use the existing security mechanisms, wherever possible,
- should allow to interoperate with other VOs.

The mentioned requirements can be fulfilled only through defining the global security policy for the grid environment and enforcing it through appropriate authorization infrastructure.

Currently, most of security mechanisms available in grid systems refer to the authentication problems. There are in fact very few or even no components supporting the authorization process. Creating such components is the main practical goal of WP6.

In its context, the authorization services may be considered as the secure and flexible infrastructure for managing virtual organization, with special support of managing trust relations.

2 The Authorization Service

Currently, one of the main security problems within grid environments is lack of mechanisms for defining and implementing grid security policies. In order to solve this problem an appropriate authorization service has to be introduce.

The present requirements for authorization services are generally similar to

those defined for the Community Authorization Service[1]. The security components of

the GridLab middleware are obviously about to be built with scalability, flexibility and fault-tolerance.

Yet, a set of requirements for authorization service should be

emphasized:

- authorization policy is always based upon mutual authentication,

[1] http://www.globus.org/research/papers/CAS_2002_Submitted.pdf

- objects of policy definitions (e.g. subject↦object relation) should include users, general resources, services, data entities, processes and other (user defined),
- the authorization services should accept credentials from various parties, which are defined as trusted (appropriate definitions should be included in the security policy),
- resource stakeholders should be able to define usage restrictions; however, they should be included into the global security policy (concept of producer-community agreement),
- security policies should be created in a hierarchical structure with special support on creating collaborative groups.

3 Security of the GridLab

There are some differences in terms and definitions while looking at architecture with security in mind. From WP6 point of view, a grid is considered

as the set of resources to which access (in any defined form) is granted _through_ the grid middleware services.

Such understanding of the grid concept has several consequences:

- security policy covers interactions between various trust domains; defined security rules are applied when access to remote resources is requested,
- security policy, therefore, does not apply directly to applications or users,
- local (not network enabled) services cannot be covered by the security infrastructure,
- to be fully interoperable with the security infrastructure, middleware service must be designed and implemented according to provided guidelines.

An additional assumption of the project is the lack of modifications of local security mechanisms of resources. The consequence is the lack of direct support for

security of resources, which are completely delegated to their stakeholders.

4 Security infrastructure

The security infrastructure is located in the GridLab middleware layer. In the consequences, the security policy will be enforced only when user will request access (in any defined form) using a grid service.

The key element of security infrastructure is an authorization service, which expected to be based or compatible with Community Authorization Service, which is being developed as a part of Globus. The security

infrastructure will be built upon trust to appropriate authorizations services, which therefore should be considered as its critical components. From security point of view, grid services are do not considered as trusted parties.

The part of authorization serivce will therefore be to verify (i.e. grant or deny) if action which service attempts to perform on behalf of the user is exactly what user requested.

From the users point of view, the main goal is to simplify use of security infrastructure, however without lowering the security level. The communication between clients (users and services) and authorization

service will be perfomed through well defined API. The requirement of usage simplicity will also refer to resource administrators - to add the resource to the grid will require only installing of standard CAS-enabled

components and defining trust to appropriate GridLab authorization service(s).

The detailed security architecture will be presented in the Technical Specification Report, which will be delivered at the end of 6th month of the project.

5 The system layer components

Obviously, the design and implementation of the GridLab security infrastructure has

appropriate requirements for specific workpackages as well as for components

residing in the system layer.

As for the system layer components (i.e. not assumed as implemented in the GridLab

project), the following requirements can be specified:

- should provide methods for security communication between resources (e.g. TSL or GSI components),
- should provide infrastructure for authenticating various parties within the virtual organization (i.e. PKI with fail-safe infrastructure of CAs),
- should provide more flexible and dynamic components for mapping (translation) the global security policy into local ones (rigid requirement!).

Among the mentioned requirements, the most significant seems to be the last one, mainly because currently there is no fully operational solution fulfilling this

requirement. It should be clearly stated that using of the improved component(s) for security policy translation is a rigid requirement for

introducing global security policy[2].

Currently, it is assumed that translation between grid and local security policy will be performed using CAS-enabled components developed as a part of Globus.

[2]The other issue is that such components should have much more extended functionality. See draft of Requirements for Grid Security

6 Failure handling scenarios

One of the best ways to illustrate requirements for Security Workpackage in the GridLab project is to present some hypothetical consequences of security compromise at various components. Obviously, no system can be considered completely secured. The actual level of security can be often established through analysis of potential consequences in case of security system's failure.

Below, examples of such scenarios are presented. Please note, that they should be considered just as illustrations of security architecture concept not the descriptions of its actual characteristics.

- **User compromise** is the case when intruder was able to gain unauthorized access to his system or his private keys. In such a case, an intruder should be able to perform operations on GridLab resources in the range of specific user's privileges, which are defined in the grid security policy.

  After reporting an incident, the privileges for compromised user should be immediately withdrew.

- The case of **service compromise** refers to situations, when vulnerability (design or implementation one) in legitimate grid service is exploited, and unauthorized access is gained. An intruder has therefore full access to a system hosting service and to data being processed. However, intruder cannot be able to access any other resources due to lack of privileges, which will not be granted without appropriate requests from a privileged user. Especially, a compromised service cannot pretend any privileged user and without appropriate private keys, intruder is not able to fake user's requests.

  Compromising the service system should allow intruder only to monitor or block incoming requests.

- In the case of grid **resource compromise** (for example computational system), it should be assumed that using currently available technologies, an intruder will get complete access to data stored and processed in the system. However, he will not be able to get access to any other resource systems directly through grid infrastructure.

  The security of resources can be increased only through extending capabilities of components for enforcing grid security policy at local systems or through using operating systems with special capabilities.

- The last case is a **compromise of authorization service**. When such incident occurs, it should be assumed that intruder gains indirect access to all grid resources (defined within specific trust domain), as he is able to perform actions as any defined user and accept any actions, as it would be acceptable in the grid security policy.

  Therefore, the system (or usually systems) hosting the authorization service should be considered as its most critical component, which requires additional security.

7 Issues beyond the scope

It should be clearly stated that it is not possible to achieve high security

level in grid environments, using only currently available technologies and

security mechanisms.

The security is often discussed using three main terms: confidentiality, integrity and availability. The overall problems with the security of a grid infrastructure will be discussed using these three terms.

- The aspect of **confidentiality** - it cannot be provided without modification to the operating systems of resources. Applications are about to be executed in unrestricted environments, which are highly susceptible to direct attacks. What is more important, attacks can also be performed using grid infrastructure. In consequence, data (e.g. calculation results) stored in the systems' resources should not be considered as secured.
- The requirement of **integrity** - it is often discussed in the context of the communication process only, which is a significant simplification. The attacks against data being transferred are relatively rare and real threats to data integrity are located at resources and application client systems. The problem is the same as in the case of confidentiality.
- The last but not least is requirement of **availability** - it is often defined as resistance of the system against various accidental conditions as well as direct denial of service attacks. The availability of infrastructure strongly depends on the consistency of its architecture and design of specific services and protocols. An appropriate analysis of the GridLab architecture in the context of denial of service threats should be performed in the future.