

CS590L Distributed Component Architecture

Research Project Proposal

Security Architecture in Open Grid Services

By
Manish Mehta
February 11, 2004

© 2004, Manish Mehta, University of Missouri – Kansas City, USA.

1. Introduction

The Open Grid Services Architecture (OGSA) is proposed to enable systems and applications (“services”) to run within distributed, heterogeneous, dynamic “virtual organizations” [1]. The services can be used within a single enterprise or may span over multiple organizations. The OGSA proposes to define a core Grid service semantics and integrated set of service definitions that address critical application and system management concerns. Although the Grid service specification defines essential building blocks for distributed systems, many more elements should be considered for large-scale interoperable systems. At the time of this writing, OGSA community is in very initial phase of design. However, the OGSA vision is broad covering several fields of computer science. Primarily, OGSA aims for interoperable, usable Grids for industry, e-science and e-business. The challenges in design of security architecture mainly involve Integration, Interoperability, and Building Trust Relationship. We address these challenges and propose to provide efficient solution for the problems.

1.1 Motivation and Significance

The Grid service specification developed by Open Grid Services Infrastructure (OGSI) defines, in Web Services Description Language (WSDL) interfaces and associated conventions, the mechanisms that any OGSA-compliant service must use. The security architecture being developed by OGSA Security Workgroup is intended to be consistent with the security model being defined for Web services architecture. The motivation of this research is to understand the security challenges and requirements in Grid environment. There is a need to define a unified approach to create secure, integrated and interoperable Grid services based on set of security abstractions.

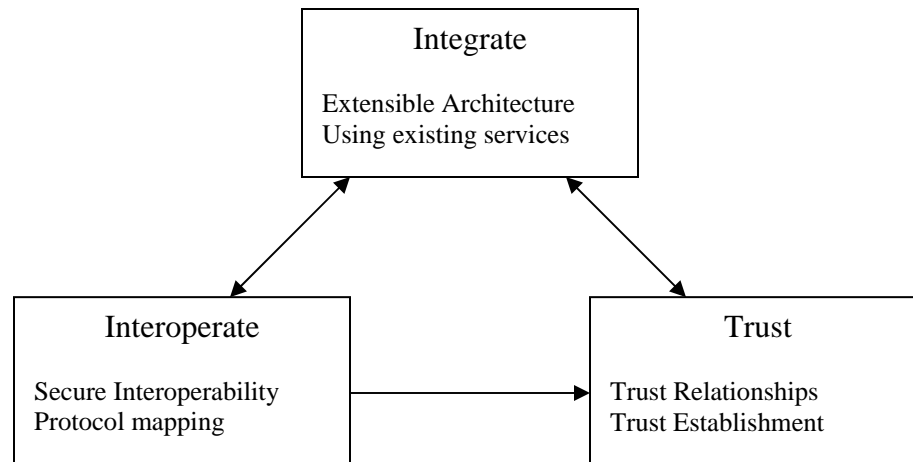
The security in Grid architecture is of major concern as the sharing the Grid environments is much more than a simple file or printer sharing in a small office environment. It is also more than sharing data or basic computing resources in large organizations. Primarily, Grid environments aim at direct access to computers, software, data, and other resources, as is required by a range of collaborative problem-solving and resource-brokering strategies. While crossing the physical and organization boundaries, Grid environment demands solutions to support security policies and management of credentials. Support for remote access to computing and data resources is to be provided. Further, Grid technology includes wide permutations of mobile devices, gateways, proxies, load balancers, globally distributed data centers, demilitarized zones etc.

Many security services are required in order to enable Grid nodes to communicate, share resources, delegate tasks, collaborate, provide brokering services etc. Following are some of the main services required in Grid environment: *Access control* to services needs to be provided via robust security protocols and comprehensive security policies. *Authentication* and *authorization* services are required to establish connection between entities. Due to distributed nature of the system, authentication services may have challenges in their design to provide *single logon* if required. *Delegation* of access rights and resources is required in distributed environment. *Privacy* policies need to be defined and enforced in order to mask personal information. *Confidentiality* and *Message Integrity* services are needed to protect the data from eavesdropping, modification, fabrication. *Information Security Assurance* is required to get certified in Grid environment to share resources securely.

1.2 Problem Description

The security challenges in Grid environment can be grouped into three main categories: Integration, Interoperability, and Trust Relationship.

- *Integration*
Practically, it is unreasonable to expect that a single security technology can be defined to address all Grid security challenges and to be adoptable in every hosting environment. Legacy infrastructure can not be changed rapidly, and hence the security architecture in Grid environment should integrate with existing security infrastructure and models.
- *Interoperability*
By definition, Grid technology is designed to operate services that traverse multiple domains and hosting environments. In order to correctly and efficiently interact with other systems, interoperability is needed at multiple levels. (Protocol level, policy level, identity level)
- *Trust Relationship*
Trust relationship among the participating domains in Grid environment is important for end-to-end traversals. This is especially important challenge as every participating domain may have different security technologies in their infrastructure.



More specifically, we can translate the Grid security challenges into Grid security requirements. The basic OGSA security model must address security disciplines. Such as authentication, delegation, single logon, credential lifespan and renewal, authorization, confidentiality, privacy, message integrity, policy exchange, secure logging, assurance, and manageability.

2. Related work

Grid technology is still a relatively young area of research. Especially, due to the complexity of concept of *virtual organizations*, the security policies and services are hard to determine and standardized. To date, there has been only [1] and [2] published on security in Grid environment.

There are other working groups working on specific security requirements like Accounting, Authorization, Authentication, Security infrastructure, and Certificate authority operations. A roadmap to Open Grid Services Architecture is given in [1]. This introductory work broadly defines the scope of the services required to support both e-science and e-business applications. Also identifies a core set of such services that are viewed as highest priority for definition. Further, it specifies at a high-level, the functionalities required for the core services and interrelationships among them. [2] proposes a strategy for addressing security within the OGSA. It defines a comprehensive Grid security architecture that supports, integrates and unifies popular security models, mechanisms, protocols, platforms and technologies to enable variety of systems to interoperate securely. [3] is a good source of white papers, design documents and message board on OGSA. [4] is official source of information on progress of OGSA security working group.

No concrete solution or architecture is provided in [1] for Grid security. It only provides a roadmap to develop a comprehensive and consistent OGSA. Security model presented in [2] describes a set of security components that need to be realized in OGSA security Architecture. However, this security model does not comprehensively address all the security challenges.

3. Proposed Solution

In this research project, we concentrate on Authentication services to be provided between virtual organizations for secure services. The proposed solution will address the problem of Authentication and Key agreement for secure data transfer between virtual organizations. We do not consider credential life span and renewal for authorized service credentials. The pre-distributed secret scheme or third-party scheme can be used to enable virtual organizations to authenticate each other and establish cryptographic keys for future secure communication.

We pick specific scenarios in Grid Environment for specific set of applications to provide authentication services. Neither the scenarios nor the specific technique has been developed yet.

4. References

- [1] OGSA-SEC-WG Draft, “*Open Grid Services Architecture: A Roadmap*”, June 2003. https://forge.gridforum.org/projects/ogsa-sec-wg/document/OGSA_Security_Roadmap/en/1
- [2] OGSA-SEC-WG Draft, “*Security Architecture for Open Grid Services*”, June 2003. https://forge.gridforum.org/projects/ogsa-sec-wg/document/Security_Architecture_for_Open_Grid_Services/en/2
- [3] Global Grid Forum, <http://www.ggf.org/>
- [4] Open Grid Services Architecture Security Working Group, <https://forge.gridforum.org/projects/ogsa-sec-wg>