SECURITY IN GRID COMPUTING

Kusum Yadav Ph.D Research Scholar, JJT University Jhunjhunu
Dr Rakesh Kumar, Director, KSJIET, Modinagar, Uttar Pradesh,India

ABSTRACT

Grid computing started out as the simultaneous application of the resources of many networked computers to a single (scientific) problem. A grid is a collection of machines, sometimes referred to as "nodes," "resources," "members," "donors," and many other such terms. They all contribute any combination of resources to the grid as a whole. The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files. Grid computing is concerned with the sharing and coordinated use of diverse resources in distributed "virtual organizations." Today in grid systems more and more organizations are involved. Sensitive data in one department may need to be protected from access by jobs running for other departments. Some resources may be used by all users of the grid while others may have specific restrictions. The dynamic and multi-institutional nature of these environments introduces challenging security issues that demand new technicalapproaches

Keywords: *Grid Computing; Distributed Systems; Security in Grids; Donors, Resources in Distributed Virtual Organizations.*

INTRODUCTION

The term grid computing originated in the early 1990s as a metaphor for making computer power as easy to access as an electric power grid in Ian Foster's and Carl Kesselman's seminal work, "The Grid: Blueprint for a new computing infrastructure" (2004). Ian Foster and Carl Kesselman defined Grid in their book "The Grid: Blueprint for a New Computing Infrastructure": "A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities[1]."

Grid computing is concerned how to share and coordinated use diverse resources in distributed environments. Grid computing is about several processors distributed globally and sharing the computational resources to solve various problems. One of the main strategies of grid computing is

to use middleware to divide and apportion pieces of a program among several computers, sometimes up to many thousands. Grid computing involves computation in a distributed fashion, which may also involve the aggregation of large-scale cluster computing-based systems. Though traditional virtual machines (e.g. clusters) have been designed for a local area network, the exponential growth of the Internet allows this concept to be applied on much large scale. ATM banking, automated check-out counters, and other services which require a computer terminal to communicate with a central processing machine utilize grid computing services. While these services are used for very basic transactions, the range of the grid computing network extends much farther. The communication channel principle makes it possible for applications of grid computing processes to be designed for economically priced Internet services based on usage amounts. Among the other applications of grid computing, this programming structure can also be useful in forming P2P file sharingnetworks.

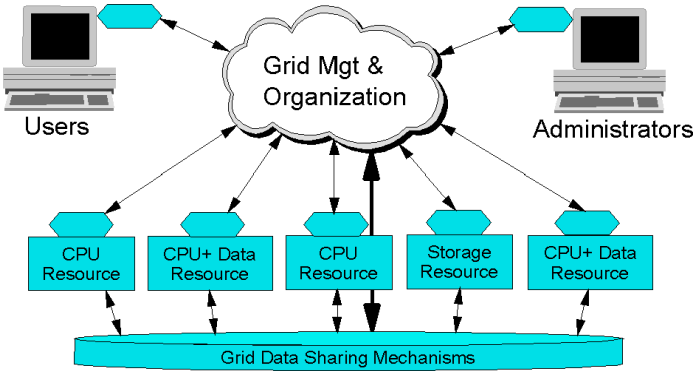


Figure 1: A Simple Grid

As present in Figure 1 the simplest grid consists of just a few machines, all of the same hardware architecture and same operating system, connected on a local network. This kind of grid uses homogeneous systems so there are fewer considerations and may be used just for experimenting with grid software. The machines are usually in one department of an organization, and their use as a grid may not require any special policies or security concerns.

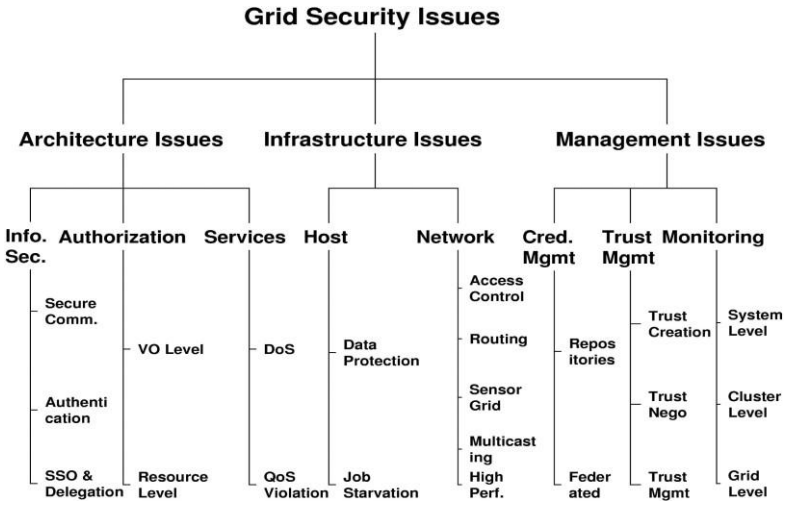


Figure 2: Taxonomy of grid security issues[2]

Need of Security in Grid System

Though traditional virtual machines (e.g. clusters) have been designed for a local area network, the exponential growth of the Internet allows this concept to be applied on much large scale. A grid system also is a mechanism to pool resources on-demand to improve the overall utilization of the system. The issues and concerns for grid systems are protection of applications and data from system where computation executes, stronger authentication policies and procedures are required for both users and code, protection of local execution of code from remote systems and management of different administrator domains and security policies. That's why a grid system also requires a monitoring system in place to monitor the resource usage, trust management system to create, negotiate, and manage trust between other systems or "strangers," and an authorization system to authorize the users to a access certain set ofresources.

Grid Architecture

The Grid architecture is composed of following layers:

Fabric Layer: Provides the local services of a Resource.
Connective Layer: Core communication and authentication protocols.
Resource Layer: Enables resource sharing.
Collective Layer: Coordinates interactions across multiple resources

Application Layer: User applications use collective, resource, and connective layers to perform grid operations in virtual organizations.

Grid Computing Security Issues and Challenges

Security requirements within the Grid environment are driven by the need to support scalable, dynamic, distributed virtual organizations (VOs) [2]—collections of diverse and distributed individuals that seek to share and use diverse resources in a coordinated fashion.

Marty Humphrey, Mary R. Thompson[4] defined various scenarios and gave various clues on how Grid security should be managed and what are its problems. The main challenges and their possible solutions are discussed as under:

Challenge: A machine is sharing its resources and the user is running applications. Then it has to be needed to assure that the machine has not beencompromised**.**

Solution: Specialized scheduler which ensures allows users with enough rights to run applications.

Challenge: Local user ID and Grid user ID must bemapped.

Solution: It can be done through the use of centralized domain controllers, for instance, OpenLdap, that provide user authentication and authorizationmethods.

Challenge: Determine access policies to services either locally or remotely.

Solution: The authorization policy must locally be digitally signed by the owner and kept securely. Remotely, the owner must be able to have a secure connection and authenticatehimself.

Challenge: Data integrity and confidentiality should be achieved.

Solution: Integrity is achieved through MAC algorithms. Confidentiality is achieved through encryption methods and keys with a limited lifetime.

Challenge: Properkey management.

Solution: One possibilityisto use smartcards.

Challenge: Trust relationships between users and domains/hosts becomeimperative.

Solution: Authentication is achieved by SSL credentials or secure DNS andIPSec.

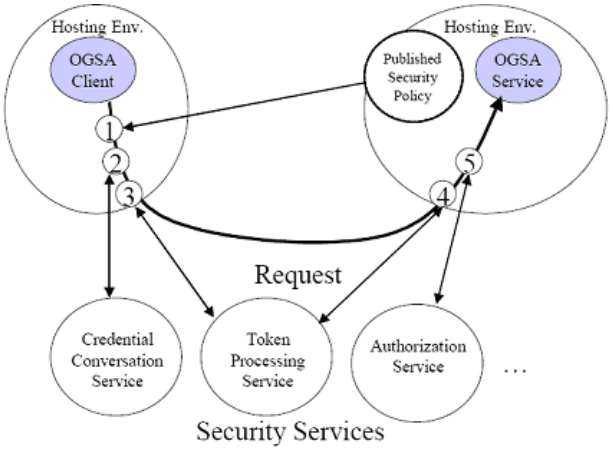
Challenge: Informationmustbe available and canberequested from everywhere.

Solution: So in order to have availability, information services are used. LDAP can be used to thesepurposessince it givesuserandpassword access controland can map the user's identificationdetailsto his service'sdirectory.

Challenge: Delegation of rights to one or multiple persons is a problem with no clear solution yet.

SECURITY SERVICES

Security requires the three fundamental services: authentication, authorization, and encryption. A grid resource must be authenticated before any checks can be done as to whether or not any requested access or operation is allowed within the grid. The security service to insure that this does not happen is encryption. The Grid Security Infrastructure (GSI) of Globus and a Public Key Infrastructure (PKI) provide the technical framework (including protocols, services, and standards) to support grid computing with five security capabilities: user authentication, data confidentiality, data integrity, non-repudiation, and keymanagement.



4. Role of Globus Toolkit in Security

At the root of any grid environment, there must be mechanisms to provide security, including authentication, authorization, data encryption etc. The Grid Security Infrastructure (GSI) component of the Globus Toolkit provides robust security mechanisms. The Grid Security Infrastructure (GSI)[4] provides functions of single/mutual authentication, encrypted communication and credential delegation in grid interactions. These functions are essential for security as well as for accounting that a job is associated clearly with the user who submitted it. User access rights and permissions will be used to determine whether and with what priority a job is executed on the machine selected by the user or by a scheduler. The Grid Security Infrastructure includes an OpenSSL[5] implementation. It also provides a single sign-on mechanism, so that once a user is authenticated, a proxy certificate is created and used when performing actions within the grid. When

designing your grid environment, you may use the GSI sign-in to grant access to the portal, or you may have your own security for the portal. The portal will then be responsible for signing in to the grid, either using the user's credentials or using a generic set of credentials for all authorized users of the portal. Most distributed computing systems use identity-based authentication and authorization control. As the typical case, a user is given a username and password for accessing a computing system; when she is ready to launch her applications, she logs into the system and submits the application jobs. In a grid environment, users or their agents simultaneously need accesses to multiple resources from different administrative domains that have different security mechanisms. This requirement creates several security issues. The two typical ones are: Single sign-on: A user should be able to authenticate once (e.g., when starting a computation) and initiate computations that acquire resources, use resources, release resources, and communicate internally, without further authentication of the user. Interoperability with local security solutions: While the grid security solutions may provide inter-domain access mechanisms, an access to a resource will typically be determined by a local security policy that is enforced by local security mechanisms. It is impractical to modify every local resource to accommodate inter-domainaccesses.

A number of organizations are using the Globus Toolkit, including Brookhaven National Lab, Phillips, and the Texas Advanced Computing Center. It includes a wide variety of native connectors for third-party workload management systems and Grid service providers, which increases interoperability between existing systems and vendors and reduces Grid integration effort and cost. Globus Toolkit will also include extensions to support execution within Kerberos security infrastructures. It is also revamping its integrated and OGSI-compliant Platform LSF family, with new reports, analytics and license optimization offerings to provide customers with comprehensive functionality beyond core workload management. Globus has also announced a new contract win with the US Department of Defense, which will utilize Platform LSF HPC to further its high performance computing program.

CONCLUSIONS

Lots of technologies are nowadays on the market and some of them share their features. In this case, as it has been demonstrated, already existing security solutions can be used for other technologies. In addition, in some specific issues, new technologies can be more secure than older ones due tothat

the design of new solutions can be more suitable to avoid security problems and will make this task much easier.

REFERENCES

1) I. Foster and C. Kesselman (editors), The Grid: Blueprint for a Future Computing In Infrastructure, Morgan Kaufmann Publishers, San Fransisco, USA,1999.
2) Foster, I., Kesselman, C. and Tuecke, S, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International Journal of High Performance Computing Applications, 15 (3). 200-222.2001.
3) Chakrabarti, Anirban , ""Grid Computing Security" 2007, XIV, 332 p. 87illus.
4) Marc-Elian Begin. Comparative Study: Grids and Clouds, Evolution or revolution. May 2005. CERN https://edms.cern.ch/file/925013/4/EGEE-Grid-Cloud-v1_2.pdf.
5) The Globus Project,http://www.globus.org
6) The Global Grid Forum,http://www.gridforum.org/
7) Grid Benchmarking Research Group,http://nas.nasa.gov/GGF/Benchmarks/

Authors would like to extend their heartfelt thanks to the academic and infrastructural support received from their respective Dept./University.