Security Issues in Grid Computing

R. Geetha
M.phil Research Scholar
Department of Computer Science
Bharathiar University, Coimbatore.

D. Ramyachitra
Assistant Professor
Department of Computer Science
Bharathiar University, Coimbatore.

ABSTRACT
Grid computing combines the computer resources from various administrative domains to reach a main objective. In grid computing, the computers in the network can work together to solve large scale computational problem, thus functioning as a supercomputer. Grid computing is used to complete complicated or tedious mathematical or scientific calculations. Some research areas were identified in the classes of the literature survey where more study is necessary. The avenues for future research are also discussed in this paper. Some types of grid systems exist currently and the security needs and solutions to address those needs for each type vary. This paper describes an overview of different types of the security issues in grid computing and also provides an effort to define, analyze and grid security problems for different types of grid setups and security situation that are faced by grid computing.

Keywords
Grid, grid computing, security issues, Globus Toolkit.

1. INTRODUCTION
A computational grid is hardware and software structure that provides reliable, responsible, persistent and economical access to high-end computational capabilities. Though grid computing has become the buzzword in both industry and educational community it is not a technology which has been developed from scrape. To a certain extent, it is a conglomeration of different existing technologies like cluster computing, peer-to-peer (p2p), end web service technologies [1].

Grid computing is a powerful and efficient computational technology which is represented as an advanced step for the previous distributing computing. Alongside with the high network communication speed and high technical specified machines that are shared still suffers from some limitations because of the way and the percentage of using these resources. Grid computing as a new computing generation uses the resources of many divided computers linked by a network for solving such great computation problems by making use of the underutilized resources or grid shared resources.

Grid computing is emerging as a promising technology for three reasons: (i) its capability to make more cost-efficient utilization of a given amount of computing resources, (ii) as a way to solve large scale problems that cannot be solved without an huge amount of computing power, and (iii) because it proposes that the resources of many computers can be controlled and managed towards a common objective [2].

During the last decade, different technology elements like cluster computing and peer-to-peer computing (p2p) have evolved from the distributed and high performance computing. In cluster computing, different computing resources like machines, server, etc. are connected together by high-speed inter-connects like communications, Gigabit Ethernet, etc. to provide high performance. Grid computing is a wide area parallel distributed computing environment where idle processor cycles and underutilized storage of geographically dispersed resources are utilized in an optimum way which acts as a supercomputer [1].

Security is defined in the resource layer of grid architecture. The resource being used may be valuable and the problems being solved or task being attempted sensitive. The security problems in grid environment are complex because resources are located in different administrative domains with each resource potential having its own policies and procedures.

The security service is a processing or communication service provided by a system to give a specific kind of protection to system resources. Security services implement security plans and are implemented by security mechanism. Security concerns are difficult by the fact that there are different requirements by users, resource owners, designers who are creating or adapting their current products and tools to take pro of the grid technology [3].

The rest of the paper is organized as follows: Section 2 describes the issues in grid computing and their concerns. Section 3 describes various authorization systems in grid computing. Section 4 describes the taxonomy of grid security issues. Section 5 describes the security authentication schemes in grid computing and Section 6 describes the security in Globus toolkit. Finally Section 7 gives conclusion.

2. GRID COMPUTING ISSUES AND CONCERNS
In Grid computing environment mainly three types of security issues are challenged: integration with their existing systems and technologies, interoperability with dissimilar service providers like J2EE technology based systems, .NET based systems, and Linux based systems and trust formation among service providers and users of Grid environments. There are a large number of technology providers, users and academicians who are working at different levels of grid computing stack to make the technology usable omnipresent [4].

Application and Data Engineering
Though grid computing is more than presently a technology to abet high presentation computing, most of the early adopters of the grid are users in the areas where there are large amounts of data and computation involved like life sciences, finance, automotive and aerospace energy [5].

Grid manageability

The systems where besotted with problems planning, management, security and other challenges. To solve these problems, large work has been accepted out at different levels. For example, in the form of structure management systems, job schedulers, methods for implementing security, etc [5].

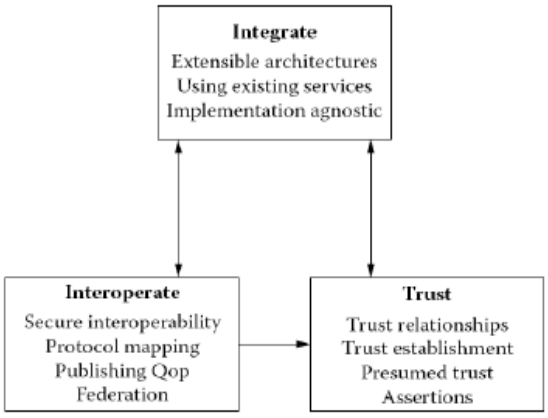

Fig 1: Security challenges in Grid Computing [4]

Grid Licensing

Large level information technology systems are undergoing transformation changes in the wake of technological developments and their adoption in scientific and business applications [7].

Grid Security

In addition to the normal security challenges like authentication, confidentiality, and truth, the grid offers several other single security challenges [7].

3. DIFFERENT AUTHORIZATION SYSTEMS IN GRID COMPUTING

Scalability

Push based system are generally more scalable than their pull based counterparts. Also, for administrators, it is more scalable to have the policy in a centralized system rather than in each and every node of the Grid system. In both these count, both Community Authorization Service (CAS) and Virtual Organization Membership Service (VOMS) score highly [5].

Security

Most of the systems mentioned in these are immune to masquerade attack as they support authentication of several type. Certificates are most prevalent means of authentication while Enterprise Authorization and Licensing System (EALS) supports passwords, certificate, or other types of credentials like bio matrices. However most of the push based system are prone to DOS attacks as most of them depend on a centralized database for storing policies [6].

Revocation

CAS and VOMS do not have explicit revocation mechanisms. Therefore once adversary gains access to the system then it can access all the resources based on the obtained credentials [8].

Inter-Operability

Another characteristic which is important to the Grid authorization systems is how inter-operable the systems are. CAS and privilege and role management infrastructure standards (PERMIS) have been made to inter-operate using Security Assistance Management Manual (SAMM) standards. However, if they are to be used extensively in the enterprises policies need to be exposed as Extensible Access Control Markup Language (XACML) standards and exchanged using Security Assertions Markup Language (SAML) [15].

4. TAXONOMY OF GRID SECURITY ISSUES

Architecture Related Issues

These issues address the affairs pertaining to the architecture of the grid. The users of the grid are concerned about the data powdered by the grid and hence there is a need to protect the data confidentiality and integrity as well as the user validation [7].

Architecture level issues may include issues like information security, authorization and service level security which destabilize the whole system and hence an architectural level solution is needed to prevent those [16].

Information security deals with the information exchange between different hosts and users. The solutions to these issues are communication in a secured way, authentication, single sign on and delegation.

Grid systems require resource specific and system specific authorizations. It is important mainly for systems where the resources are shared between multiple departments or organizations. The authorization systems are of two types: Virtual organization level systems and resource level systems. Virtual organization level systems have a centralized authorization system which provides credentials for the users to access the resources and resource level systems allow the users to access the resources based on the credentials presented by the users.

The grid service level security issues are of two types: QoS Violation Issues and DOS (Denial-of-Service) related issues. The QoS violation issue is about the forced Qos violation by the adversary through congestion, slowing or dropping packets or through resource hacking. The Denial-of-Service is more dangerous where the access to a certain service is denied.

Infrastructure Related Issues

These issues are related to the network and host which are found in the grid infrastructure. Host level security issues are individual's issues that make a host apprehensive about affiliating itself to the grid system. The issues that are related to the infrastructure may include data protection, job starvation, and host accessibility [5].

Grid computing infrastructure must address several potentially complicated areas in many stages of the implementation. These complications arise in the areas of security, resource management and information services and data management.

The infrastructure related issues are of two types: host security issues and network security issues. The host level security issues are those issues that make a host comprehensive about affiliating itself into the grid system.

The main subissues include data protection issues and job starvation [16].

The network security issues arise mainly due to the heterogeneity and high speed requirements of many grid applications. Many of the grid network issues are active areas of research and are most developed in labs and not yet commercialized.

Management Related Issues

The third set of issues relate to the management of the grid. Managing pass is absolutely important in grid systems because of the mixed nature of the grid frame and applications. Like any distributed system, managing belief is also serious and falls below the purview of management related issues.

The different management issues are credential management, trust management and monitoring related issues [16].

Management of credentials is very important in grid context as there are multiple different systems which varied credentials to access them. Management of trust is very difficult in a dynamic grid scenario where grid nodes and users join and leave the system. Monitoring of resources consists of different stages such as collection, processing, transmission, storage and presentation of the data.

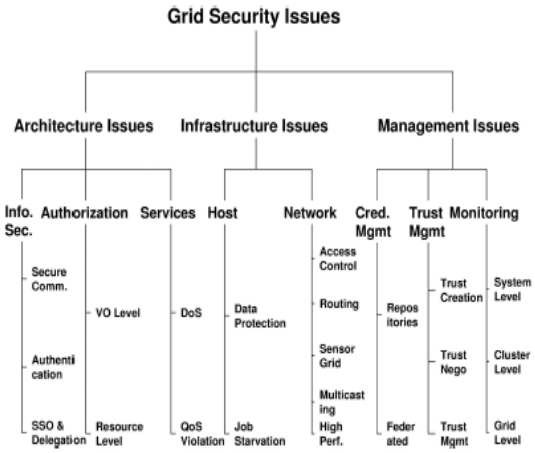

Fig 2: Taxonomy of grid security issues [16]

5. SECURITY AUTHENTICATION SCHEMES IN GRID COMPUTING

The goal of grid computing is to provide secure grid service resources to legal users and therefore the security issue becomes an important concern of grid computing. To avoid the illegal users from visiting the grid resources, it should be sure that strong mutual authentication needed for users and server. To access any resource over any network, authentication process is essential at first. Since, Grid is network based architecture, there must be a strong authentication procedure for the sake of security of resources.

Accordingly, the Grid provides open and standard protocols and application interfaces to build up all the measures for resource sharing [4]. Authentication is to ensure that the communication is established from that entity.

Mutual Authentication

Mutual authentication is the key concept of Grid computing model. A user is allowed to access certain resource of Grid environment providing the user is authorized entity. On the basis of the dependence relationship mutual authentication takes place to avoid replacement source to restrict [14].

User Proxies

A user proxy is a conference manager process that provides consent to proceed on behalf of a user for a limited phase of time. User proxy mechanism is a substitute for the user. It has got the unique feature to prevent repetitive password typing by the user for offering its service [1].

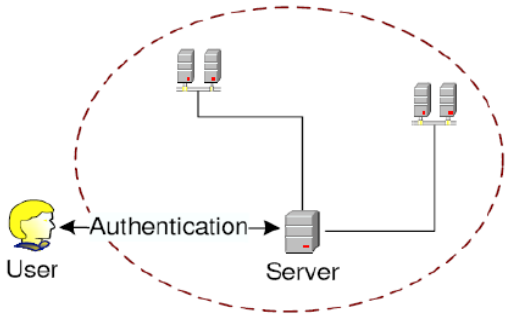

Fig 3: Simple user authentication [13]

Shared secret based authentication

The first mechanism is through sharing a secret. Most of the digital systems also work by the principle of shared secret [14]. One way to implement such a user system would be share a password between the authenticator and the user. In this form of system, the authenticator asks the user for a password which when disclosed will allow the user entirely [4].

Public Key Based Authentication

Public-key cryptography is cryptographic system that needs two part keys one of which is secret and one of which is public. One key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions [7].

The visibly available encrypting-key is usually distributed, while the private decrypting-key is known only to the recipient. Messages are encrypted with the receiver's public key, and can be decrypted only with the equivalent private key. The keys are related mathematically, but the parameters are selected so that determining the private key from the public key is either impossible or prohibitively expensive [1].

Third Party Authentication Schemes

When a person tries to enter a new country, the immigration department of the country mandates that the person possesses valid passport and visa to enter the nation. In this case, the immigration department does not know the person entering the country.

However the department believes some third party like the person's own country issuing the passport and the consulate issuing the visa. This is a classic case of third party verification where the authenticator does not identify the user, however uses a third party credential (in this case

passport/visa) for authentication purposes. In digital system also this type of authentication is very popular [10].

6. SECURITY IN GLOBUS TOOKIT 4.0 (GT4)

The Globus Toolkit (GT) [8] is an open source middleware developed as a collection of loosely coupled components and it has become facto pioneer of grid development. These components compose of services, programming libraries and development tools designed for building Grid-based application.GT components fall into five wide domain parts: Security (GSI-Grid Security Infrastructure), Data management, Execution Management, Data and Information Services, and regular runtime, fault detection, portability [15]. A simplified view of the main components for the Globus toolkit is shown in figure3 [7].

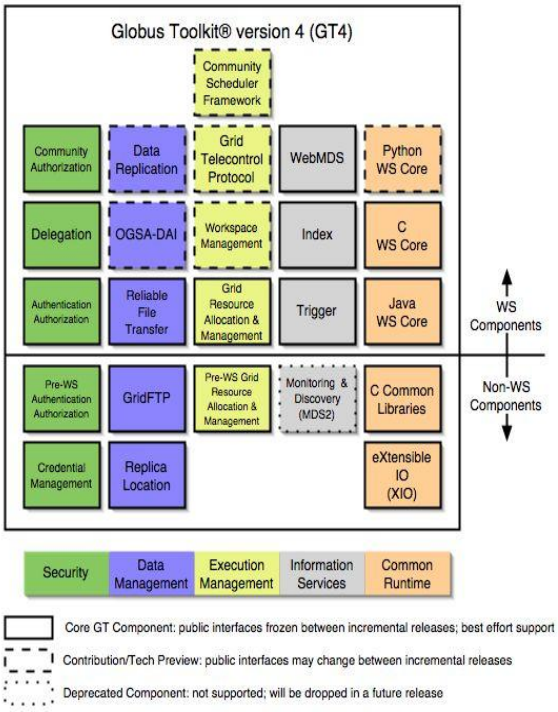

Fig 4: Globus Toolkit version 4.0 [18]

The security implementations of the Globus Toolkit 4.0 are discussed below:

Message protection in GT4

GT4 uses two mechanisms to protect the SOAP message being transferred between the special components, viz. Transport-level security and message level security. Transport-level security protects the records transferred at the transport layer using standards like Transport Layer Security (TLS). Message level security, on the other hand, works at a high layer and uses web services based standers like WS-security, WS-secure conversation by protecting the SOAP messages that are being transferred over the transport channel [8].

Transport-level security

Transport level security in GT4 is implemented using the transport layer security (TLS) standards. GT4 implements the transport security using a secure socket implementation which is able to provide the security properties [4]. The transport level security in GT4 is the default security mechanism used in GT4. The major reason for that is the performance overhead introduced by message level security mechanisms [7].

Message-level security

GT4 also uses message level security (MLS) as an alternative to transport level defense, where encryption, authentication and integrity mechanisms are employed at the message layer, rather than at the transport layer by means of web service standards like WS-Security and WS-Secure conversation. WS-Security standard provide mechanisms to provide privacy, authentication and integrity to the SOAP messages [1].

Message level and transport level security approaches

When the two mechanisms message level and transport level security are compared, two main points are need to be considered. They are end-to-end security and performance.

End-to-end security

The transport level security works as a point-to-point mechanisms and does not work across multi-hop link. This is one of the benefits of message level security. It works across hops and is a complete end-to-end solution [9].

Performance

The performance overhead associated with the web services based security mechanisms is quite significant. The stream based pipelining is used at each period in order to improve the performance [14].

Delegation in GT4

GT4 supports delegation through the use of X.509 based proxy certificate. Proxy certificates allow the bearers of X.509 certificate to delegate their privileges temporarily to another entity. GT4 supports the delegation to process through the components: a delegation factory service (DFS) and a delegation service (DS) [8].

GT4 COMPONENTS

The GT4 components include

- Common runtime
- Security
- Data Management
- Information Services
- Execution Management

Common Runtime

The common runtime components deliver a set of fundamental and tools libraries which are needed to build all WS and non-WS services [17].

Security

Using the Security components, established on the grid security infrastructure (GSI), it is assured that the communications are securing [6].

Data management

These components allows to access the large set of data in a virtual organization.

Information services

The Information Services includes a set of components to discover and monitor resources in a virtual organization. GT4 also consist of a non-WS version for legacy purposes. This component is deplored and will certainly dissolve in future releases of the toolkit.

Execution management

Execution management constituents deal with the initiation, monitoring, management, planning and coordination of executable programs, usually called jobs, in a grid.

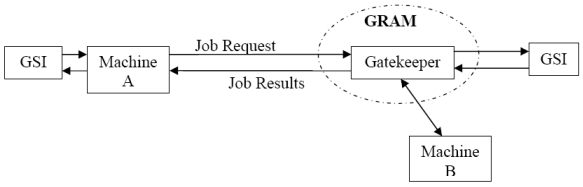

Fig 5.Components of Globus Toolkit [19]

7. CONCLUSION

Grid computing has become a hopeful way for distributed supercomputing from its very beginning and attracts many attentions worldwide. There are many ways to access the resources of a computational grid and each method is associated with a unique security requirement and it also has implications for both the resource user and the resource provider. Although this computing technology has been accepted worldwide, still it has got a lot of problems mainly regarding with different security issues. The security in grid environment is achieved through the implementation of various security measures such as authentication, authorization and data integrity. This study provides an overview of security issues concerned mainly with authentication and presented various schemes in authentication. Further strong authentication procedures must be developed in future for the sake of security of resources in the grid environment.

REFERENCES

[1] I. Foster, C. Kesselman, and S. Tuecke, 2001. The Anatomy of the Grid - Enabling Scalable Virtual Organizations. International Journal of Supercomputer Applications.

[2] R. Al-Khannak, B. Bitzer, 2008. SouthModifying Modern Power Systems Quality by Integrating Grid Computing Technology.

[3] R.Kalaisevi Dr.V.Kavitha ,2012. “Authentication in grid security infrastructure- A Survey” Procedia Engineering, Pages 4030-4036.

[4] Avijit Bhowmick and C.T. Bhunia, 2012. Analysing Grid Security Issues and Some PreliminaryApproaches for Secure Environment in Grid, International Journal of Computer Science and Telecommunications Volume 3, Issue 5, (May 2012).

[5] Anirban Chakrabarti, 2010. Grid Computing Security (GCS) .

[6] Chakrabarti,A., Damodaran, A., Sengupta S. 2008. Grid computing security: A taxonomy.IEEE Security and Privacy, Pages 44–51.

[7] Globus Alliance: 2008. GT 4.0 Reliable File Transfer (RFT) Service. (March 2008).

[8] 3. Welch, V. 2005. Globus toolkit version 4 grid security infrastructure: A standards perspective. Technical report, Globus Alliance.

[9] Jerome H. Saltzer, David P. Reed, and David D. Clark. 1984. End-to-End Arguments in System Design. *ACM Transactions in Computer Systems*, (November 1984), Pages 277–288.

[10] B. Atkinson, 2002. et. al. Specification: Web Services Security (WS-Security),Version 1.0, 05 (April 2002).

[11] R.Buyya, 2006. Grid computing info centre: frequently asked questions (FAQ) http://www.gridcomputing.com/gridfaq. html (Document view: (March 28, 2006).

[12] M. Humphrey, M.R. Thompson, K.R. Jackson, 2005. Security for grids, Proc. of IEEE (March 2005) 644–652.

[13] Rongxing Lu, Zhenfu Cao, Zhenchuan Chai, and Xiaohui Liang. 2007. A Simple User Authentication Scheme for Grid Computing (Received July 6, 2005; revised and accepted Apr. 30, 2007)

[14] http://www.globus.org/security/overview.html

[15] Security Issues in Grid Computing for ppt.

[16] Taxonomy of grid security issues

[17] www.globusconsortium.org/news/GT4available.pdf

[18] Mark P.Wachowiak, Ph.d.Febrary 2, 2007.

[19] Ian Foster. A Globus Toolkit Primer. (Draft). 2005 http://www.globus.org/toolkit/docs/4.0/key/GT4_Primer 0.6. Pdf. (April 26, 2005).