Different Aspect Grid Security; based on User Authenticity and Message-based Security Service: A Review

Prasenjit kumar Patra
Department of Computer Science
Lovely Professional University, Jalandhar India

Pranshu Saxena
Department of Computer Science
Lovely Professional university, Jalandhar India

Rajwinder Singh
Department of Computer Science
Lovely Professional university, Jalandhar India

ABSTRACT

Today, individuals and institutions in science, research organization and industry are increasingly forming virtual organizations to pool resources and tackle a common objective. Massive amount of information has been passed not only confined into particular country but also spread out across the globe. Participants in virtual organizations commonly need to share resources such as data archives, computer cycles, and networks resources usually available only with restrictions based on the requested resource's nature and the user's identity. Thus, any sharing mechanism must have the ability to authenticate the user's identity and determine whether the user is authorized to request the resource. Moreover polices regarding message integrity also a great impediment while passing through scalable region (possible active attacks). This paper described a draft over view of different security polices for achieving confidentiality, authenticity, authorization, and integrity as well. So in this study we account for the possible strain to get over above discussed security issues.

Keywords

Grid computing, message based security, active attacks, Grid Security Infrastructure, authentication.

1. INTRODUCTION

Basically, Grid computing is concerned how to share and coordinated use diverse resources in distributed environments. Subjective aspect of different researcher on grid as follows; in 1998, I. Foster and C. Kesselman defined Grid in his book, "The: 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 [3]. Later in 2000 I. Foster *et al.* [4] refine the definition of grid and summarize as follows, "it coordinates resources that are not subject to centralized control, it uses standard, open, general-purpose protocols and interfaces, and it delivers nontrivial quality of service". Whereas Kon *et al*. [15] define grid computing as, "coordinated resource sharing and problem solving in dynamic, multi-institution virtual organizations". The dynamic and multi-institutional nature of these environments introduces challenging security issues, which include integration with existing systems and technologies, interoperability with different "hosting environments" and trust relationships among interacting hosting environments. These security issues become more brutal while active intruder takes part in communication scenario. This paper we are reviewing two aspects of security policies *First*, ability to authenticate the user's identity later conclude about authorization to request and response as virtual organizations tend to be fluid, however, so authentication mechanisms must be flexible and lightweight, allowing administrators to quickly establish and change resource-sharing arrangements. Nevertheless, because virtual organizations complement rather than replace existing institutions, sharing mechanisms cannot change local policies and must allow individual institutions to maintain control over their own resources. *Second*, to maintain the integrity of message which has been passed over wide area from the active intruders, idea is that there should not be any concealment of data while transferring over network resources.

For thoughtful discussion about the security essentials, let consider a scenario of two research organizations (A & B), disperse over a wide area, working on a same project, sharing the common data base located at different location (C). Mammoth amount of important information transferred via networks in order to compare the experimented results, but the constraint is that security is prime issue while transferring the information.

This example can dig out following distinctive characteristics of the grid computing respective of information security;

- Resources may require different authentication and authorization mechanisms and policies, which we will have limited ability to change. Later we indicate this situation by showing the local access control policies that apply at the different sites. These include

Kerberos, plaintext passwords, Secure Socket Library (SSL), and secure shell.

- An individual user will be associated with different local name spaces, credentials, or accounts, at different sites, for the purposes of accounting and access control. At some sites, a user may have a regular account. At others, the user may use a dynamically assigned guest account or simply an account created for the collaboration.
- Resources and users may be located in different countries a message based security is required grounded on confidentiality so we review different encryption standard in further discussion of this paper.

2. SECURITY PREREQUISITE

Successful deployment of Grid systems and applications may require any or all of the standard security functions, including authentication, authorization, message digest, message encryption, access control, integrity, privacy, and nonrepudiation. In this section, we focus primarily on issues of authentication and access control. Specifically, we seek to:

(1) provide authentication solutions that allow a user, the processes that comprise a user's computation, and the resources used by those processes, to verify each other's identity;

(2) message digest so that outside the world cannot access the data.

In developing a security architecture that meets these requirements, we also choose to satisfy the following constraints derived from the characteristics of the grid environment and grid applications:

- 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.
- Protection of credentials: User credentials (passwords, private keys, etc.) must be protected.
- Encrypted message: Actual data should be digested into another form to deal with unwanted concealment. Hash code should be required to deal with active modification attack, maintain the integrity.
- Uniform credentials/certification infrastructure: Inter domain access requires, at a minimum, a common way of expressing the identity of a security principal such as an actual user or a resource. Hence, it is imperative to employ a standard (such as X.509v3) for encoding credentials for security principals.

3. SECURITY DEPLOYMENT: A REVIEW

In this section we are introducing some of the techniques; those are helpful on the above scenarios. In the concern User site, primary constraint is simplicity, program processing at user site should possess a subset of the user's rights and have access to the permitted resources. More over solution must be transparently interface with common remote access tools: remote login via Telnet, file access via FTP, Web browsers, and programming libraries as Common Object Request Broker Architecture (CORBA) and Message Passing Interface (MPI). It must also allow implementation of new inter site applications by providing standardized APIs for accessing security functions. For example, a group developing collaborative design tools should be able to easily integrate authentication and authorization mechanisms.

In the context of Sites, those are responsible for providing the resources, require authentication and authorization infrastructure as well, this secured infrastructure is provided as follows;

- Typically sites can't easily replace or modify their intra-domain security solution, so we need a distinct inter-domain solution that interoperates with local security solutions, is at least as strong as local solution so that it does not weaken site security, and is easy to understand so that site administrator can trust it.
- Site administrators must have tight control over policies governing access to their resources; including how users established their identity and which user access which resources.

The "Technical Alternatives for Multisite Authentication," sidebar explains why the two most popular authentication approaches- Secure shell and Kerberos- did not meet these requirement prompting us to develop GSI.

Two widely used authentication approaches—Kerberos and secure shell—do not meet our requirements.

3.1. Kerberos

Kerberos—used alone or under the distributed computing environment authenticates users through a secure transaction with a centrally maintained key server. Kerberos achieves inter organizational, or cross-realm, authentication by designating trustworthy key servers in other organizations. Kerberos meets many of the basic requirements for virtual organization authentication, but it presents two problems:

- Using Kerberos for inter-site authentication also means using it for intra-site authentication, which is often not feasible because of equipment and staffing costs.

- Sites must negotiate many cross-realm authentication agreements, and many sites resist surrendering too much control over local policy.

3.2. Secure shell

Secure shell (SSH), a widely used login technology, meets a number of our requirements: It is based on public-key authentication technology, uses link encryption to protect user credentials, and is easily deployed. Users like SSH because it provides basic remote login and file copy capabilities without a lot of complexity. SSH, however, have two significant drawbacks:

- It requires users to manage their own cross-site authentication relationships by copying public keys (or keeping track of passwords) for all sites they access, a task that can be burdensome if they access many sites. Moreover, SSH does not give sites control over authorization, so they cannot, for example, deny access to a particular user without invading user privacy.

- SSH supports only limited capabilities—remote shell and file transfer but not others that require authentication, such as collaborative environments and Web browsers.

So need a more robust system that will out performs the previously deployed security algorithms rely on authenticity, integrity and algorithm.

R. Butler *et al.* [1] proposed new Grid Security Infrastructure (GSI) for inter-site security purpose that deals with inter-domain operations, bridging the different local security solutions of essential sites. That proposed GSI infrastructure has following capabilities and significant features:

- Credentials using standard X.509v3 system i.e. certification authority issues a certificate binding a public key to a particular distinguished name in the X.500 tradition and a certification authority (CA) a trusted third party, ties and identity to a public private key pair by singing a certificate.
- Secured Socket Layer (SSL) is used to express the authentication (checks the entity identity) algorithm, this is done by local admin by installing these certificates, which are then used to verify the certificate chain.
- Finding an original certificate is heuristic process that begins with the CA and growing, as first the user, then the user's proxies, sign certificate. By checking this certificate chain, processes started on separate sites by the same user can authenticate to one another by tracking back along the certificate chain.
- GSI contains an Access Control list (ACL) which are used to account for polices that determine which request should be accepted or not.
- Local subject name such as Kerberos principal or login name is the principle advantage over the authentication protocol that is used global identification for involving parties.

3.3. Message Based Security Services

In this section we are describing message based security on the basis of message digest. *First*, message is digested with MD5/SHA.X and refine into new size based on digestion algorithm (128/160), later digested message fed to various authentication scheme which we discuss above, this scheme intended to provide such a form that will become impediment for active intruders, and moreover it will be vigorous from the brute force attack due to digesting the message into to fixed length from the arbitrary length input.

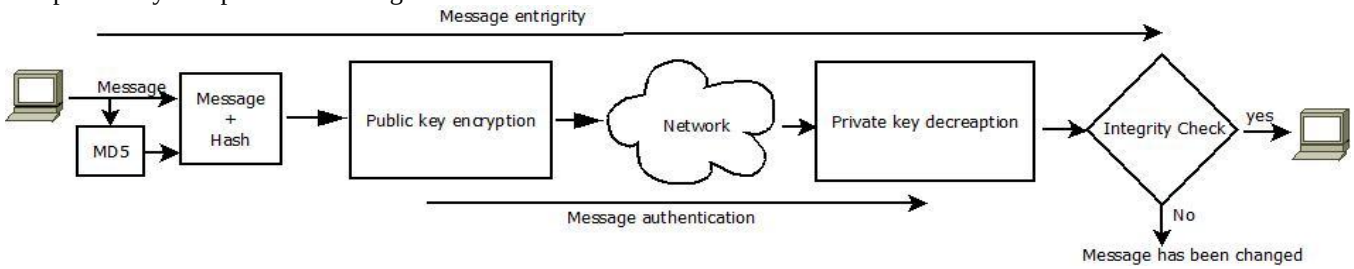

Fig 1: Message Based Security Services.

3.4. Advantages of GSI model over traditional Model

GSI is more Adaptable to handle in the dynamic environment in following manners;

- For users, the global name and proxy credentials mean the user needs only one authentication to access all resources, and proxy credentials and delegation allow programs running on a user's behalf to access resources. The use of X.509, SSLv3, and GSS-API standards facilitates the development of common GSI-enabled tools and more complex applications.
- For sites, the architecture does not require changing the local security infrastructure; instead, sites can

simply install relatively simple GSI-enabled servers that use well-known standards. Sites control policy through the access control list and map file, so administrators feel comfortable with the code and are willing to deploy it alongside SSH and other remote access mechanisms.

In her research paper, she has provided various aspects of security criterion like System solution, Hybrid solution, Behavioral solution, and related technology. These solutions collectively secure grid computing environment.

Ali Raza Butt [12] proposed a method to address the problem of malicious code of users. De-coupling of grid user management from the physical entities and guaranteeing safe grid usage in the absence of user accountability. They used two methods to overcome grid security issues in their approach; providing a private and anonymous account for every job submitter. The standard user account is a unique numeric identifier. They only maintain Grid user data in logical use accounts. Because the account is not tied to a specific numeric identifier, the system could dynamically manager the permission of the account.

After getting the job from users we put the job into one queue with security priority that is the reason system knows the application should run on which security level .Based on the security priority, Two-level motioning process approach Runtime process monitoring can provide control all-over the system, but this method has extra overheads. System cannot monitor every process from starting to ending. In the first level, they provide a restricted shell to enforce the host security policy. The restricted shell decides whether the application should be monitored. Before execution an application, the restricted shell informs level-two to monitor the applicant at runtime.

4. CONCLUDING REMARKS & FUTURE ASPECTS

Grid computing is a very intensive research topic and security issue is very important in Grid while we are talking about geographically dispersed resources. Several Grid security architectures have been deployed in last ten years for the purposed of three challenges that grid environment have; integration with existing system, interoperability with different environment and trust relationship among domains.

Our survey mainly focuses on secure grid challenge. Due to bulk amount of important information has been passed across widely dispersed resources. Participants in virtual organizations commonly need to share resources such as data archives, computer cycles, and networks resources usually available only with restrictions based on the requested resource's nature and the user's identity and integrity of data as well. Several researchers trying to make more secure environment by investigating issues like as inter-Grid interoperability, policy express, access control for Web services and security Grid environment.

Grid computing already has history for more than ten years. Although, many grid security software services have been developed very well, for example, Global Security Infrastructure, GRIP for interoperability, the research of Grid security just starts. Grid security still is one of the most crucial and difficult research topics. Based on the analysis to research of Grid computing in research institutes, Universities and industry companies, we should focus on following research topics in Grid security:

- Virtual Organization based interoperability, and security policies justify the legitimate user and their authorization.
- Policy express and exchange in inter-Grid and intra-Grid
- Policy based Access control for distinct user
- Local and Globus Security Grid environment for all organization.
- Certification authority and dynamically secure delegation for service requester.
- Adaptive trust relationship management.
- Message-based security service in Protocol level and policy level for the purpose of no concealment of the data.

5. REFERENCES

[1] Randy Butler Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Carl Kesselman, "A National-Scale Authentication Infrastructure," IEEE Transaction grid society 2000.

[2] Zphre Zare, "Security in grid computing," 5th SASTech 2011, Khavaran Higher-education Institute, Mashhad, Iran. May 2012.

[3] I. Foster and C. Kesselman, "Globus: A Toolkit-Based Grid Architecture," *The Grid: Blueprint for a Future Computing Infrastructure*, I. Foster and C. Kesselman, eds., Morgan Kaufmann, San Francisco, 1999, pp. 259-278.

[4] I. Foster et al., "A Security Architecture for Computational Grids," *Proc. ACM Conf. Computers and Security*, ACM Press, New York, pp. 83-91, 1998.

[5] R. Barbera, "The GENIUS Grid Portal," 2003

[6] F. Donno, V. Ciaschini, D. Rebatto, L. Vaccarossa, M. Verlato, "The World GRID transatlantic test bed: a successful example of Grid interoperability across EU and US domains," Computing in High Energy and Nuclear Physics, 24-28 March 2003.

[7] M. Thomas, J. Boisseau, "Development of NPACI Grid Application Portals and Portal Web Services," Cluster Computing, 2003.

[8] Gurmeet Singh, Ewa Deelman, Gaurang Mehta, Karan Vahi, Mei-Hui Su, "The Pegasus Portal:

Web Based Grid Computing," ACM Symposium on Applied Computing, 2005.

[9] M. Li, P. van Santen, D. W. Walker, O. F. Rana, M. A. Baker, "Portal Lab: A Web Services Toolkit for Building Semantic Grid Portals," proceedings of the 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2002.

[10] Toyotaro Suzumura, Hidemoto Nakada, Satoshi Matsuoka, Henri Casanova, "Grid Speed: A Web-based Grid Portal Generation Server," Proceedings of the Seventh International Conference on High Performance Computing and Grid in Asia Pacific Region, 2004.

[11] Unicore, "Unicore -Globus Interoperability of Grid Infrastructures," 2005.

[12] Ali Raza Butt, Sumalatha Adabala, Nirav H. Kapadia, Renato J. Figueiredo, and Jose A.B. Fortes, "Grid computing portals and security issues," Parallel and Distributed computing, 2003.

[13] Rafae Bhatti, Elisa Bertino, Arif Ghafoor, "A Trust-based Context-Aware Access Control Model for Web-Services," Proceedings of the IEEE International Conference on Web Services, 2004.

[14] Globus project, http://www.globus.org. (June. 2006).

[15] The Globus Security Team, "Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective," 2005.

[16] Fabio Kon, "Grid computing as coordinated resource sharing and problem solving in dynamic multi-institution virtual organizations," Dec 2008.