Gaining Secure Assets using Integrated Components of Grid Security Infrastructure (GSI) Creating inside Grid Environment

Maath.Kamal.Al-anni/Msc

Computer Science Department Pune University, Pune, India

Summary
The existence of grid computing in the near future is an admitted reality. The ubiquity of the grid computing connection to desktops has brought both boon to scientists as well as a cause of concern due to the security of digital assets that may be unknowingly exposed[1,3]. Grid Security Infrastructure (GSI), with all its components, has been the most commonly deployed solution to secure corporate assets against external and not internal attacks [7]. In other words, certificates are the way users authenticate themselves in grid-network activates that perform identity verifications [4]. The certification methods are supported as an instance of SSL/TSL (Secure Socket Layer/Transport Layer) security that implements authentication through the exchange of certificates based on public/private keys according to the X509 standard [9]and also with help of DS(digital signature)[7]. The present paper intends to demonstrate briefly the grid access by users and secure tunnels (like virtual private network (VPN)) [8], then to show practically some intruders which can penetrate the security system while delegation processes are taken place. So far all of appointed procedures are looking elegant, still there are some drawbacks, if one look at grid security from a side of internal attacks that absolutely gives a real depicture of threats. this paper will summarize a problem with a case study of Globus toolkit 4.x (a type of middleware software) in which delegation has to be applied Within a grid set up, GSI is well-configured security stages which has the completed components for helping grid users and administrators getting a benefit from security tools before running any job with Globus toolkits, generating a proxy is a last step before firing Globus run command (globus-run command Executable file)[6]. Although it is passed all these security requirements, still there is a fault of internal attacks on it. Therefore, when delegation process has taken place the supper-user i.e. administrator of proxy's node or successive machines of delegated machine can access its Proxy's private key and x509 certificate meanwhile contacting business under its name.Input here the part of summary. As it mentioned above a problem with this assumed work will have a suggestion for solving the mentioned problem by using N.N (Neural Network with Artificial approaches) with IDS (Intrusion Detection System). It could be helpful to solve such a problem using learning phrases to train N.N about three patterns (Normal, Abnormal, and Random Behaviors). Later on the network being able and ready to classify patterns in related with previous learning stages, Finally, it is suggested to work as a package within targeted server's machine to prevent most possible penetrations.

Key words:
Input here the part of 4-5 keywords.

1. Security Preamble

Security requires the three fundamental services of authentication, authorization, and delegation, all of these supposed to have been successively done. If one fails, grid users cannot proceed to next subsequent stages [7]. Based on this concept, inventors of middleware have generated tools/components that can help grid users to perform these services easily.
Grid security infrastructure (GSI) is one of these components which can be helpful in securely accomplishing work within grid environments. GSI is based on two approaches: digital signature (DS) and public key infrastructure (PKI) [11]. DS is working appropriately with Message Digestible 5 (MD5), a Hash function [5], whereas PKI depends on "Ron Rivest, Adi Shamir, and Len Adlemen" (RSA) in encrypting and decrypting processes of electronic message between authentic users. These are known as asymmetric methods of authentication, latter techniques are quite good to authenticate users remotely [12, 7, and 8], If it is supposed that every stage has to completely finish before successive stages start, then during the time of any transaction between either grid users or grid nodes has to get authentic specific participants within grid environments, and grid user or node have to obtain authentication at every stage. This scenario helps authentic-grid members to empower each other remotely with the help of digital signature. Simply it means that the particular users will be able to perform this mechanism perfectly. All these mechanisms are performed by using DS and PKI which is called as authentication stage. The next stage is a message exchange between two or more authenticated users through session ID [8, 3, And 2], it will be in a codified message to ensure that only particular users who has private key got it.
This stage is performed by encrypting/decrypting message using one-key pad leading to faster performance. This process is known as symmetric methods of encryption/decryption, however the grid security is concerned with a first stage which has to be the authentication process with help of the PKI and DS which can help delegator and services provider authentically trusted, a following stage of next session which can be

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

named as exchanging the information with the secure way using session ID which is widely used In SSL/TSL, this becomes the catch word in recent technology of security issues [11, 8, and 10].
The asymmetric process using PKI approaches is preferred because it is managed by public/private key pairs in attesting/rejecting (authenticate) grid users/nodes. However, asymmetric process is faster because it reduces user authentication only to use encryption/decryption of messages with the help of a single session ID only (one-key for both process)[7].
The two procedures mentioned above are extremely systematic. Additionally, there is a further policy which is more essential and known as mapping-file, it is responsible of achieving users scrutiny to access local resources or not [12].
Definitely, this as we have tried to explain in preceding paragraphs is true when security is only refining external attacks or troublesome-problems, wherefore it is quite good for preventing an external attacker but what about its internal attacker that a current article will try to treat its external vulnerabilities in this paper.
From this section, input the body of your manuscript according to the constitution that you had. For detailed information for authors, please refer to [1].

2. Grid Technologies for Security Layout

HPC (High performance computer) and Grids can significantly help because a single application would be run by multiple powerful resources that are not available in a single organization, heterogeneity, availability, security, and fault tolerance and other issues arise, Grid Technology takes care of all these issues by using what is called “middleware “[14] [17]. The architecture of a typical grid shown in fig -1- .
The Grid Fabric consists of distributed resources such as computer, networks, storage devices and scientific instrument. The distributed resources could be logical or physical clusters, supercomputers, servers and ordinary PCs which run a variety of operating systems(as Unix variants or windows)[13].
The core Grid Middleware sits on top of this fabric and provides services such as remote process management, co-allocation of resources, storage access, information registration and discovery, security, and some aspects of Quality of Service (QoS) such as resource reservation and trading, therefore, the complexity and heterogeneity of distributed resources can be hidden by these services by providing a uniform and consistent access to them. A popular Grid Middleware which supports many of these core services is Globus[14]developed by researchers from the Argonne National Laboratory and University of Southern California, USA, Alchemy [15] is another Middleware which is predominately focuses on supporting enterprise Grid and it is alter Web-Services-Based remote job management services.
User-level Grid Middleware provides abstractions to the services provided by the Low-level (core) Middleware these include application development environments, programming tools and security components.
The most important component in this layer which is concerning in our research paper works is Security which is used to Authentication process, delegations, and access rights and gathers different users across Grids.
A popular user-level Grid Middleware providing Utility-user Grid Middleware security and delegation is Grid Security Infrastructure(GSI)[14] developed by researchers from the university of Melbourne, Australia.
Several applications can be constructed on top of grid middleware, developed using Grid – enabled language and utilities such as HPC++ or MPI.

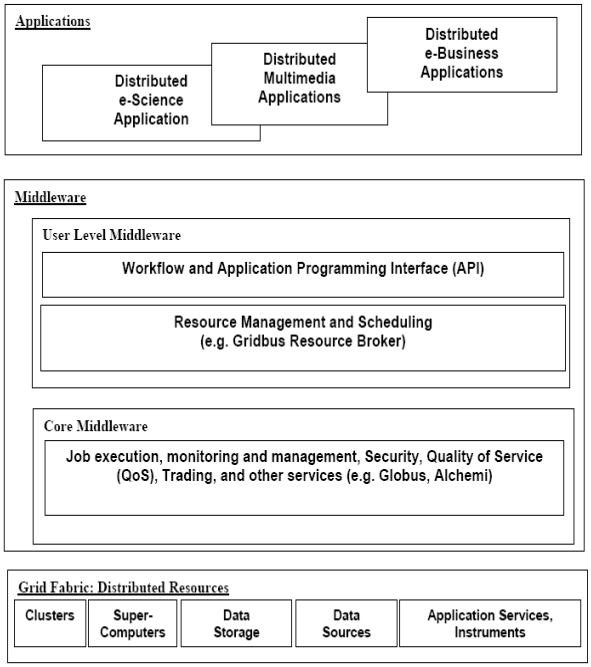

Fig. 1: The Architecture of Grid.

3. Related Work

Most of the existing security is dealing with Point-to-Point security solutions. This Point-to-Point Security can be achieved by different ways, including SSL/TLS and IPSec as examples, figure-1.1- shows Point-to-Point Security establishment.

Figure -1.1-
Point-to-Point Security establishment

As shown in figure-1.2-, web services security involves achieving end-to-end message security between the initial senders of the message to the final receiver of the message. These messages may go through many intermediaries on the way.

Figure -1.2-
End - to - End Security

This message security is a combination of different levels of security requirements including end-point authentication and authorization, message integrity, message confidentiality, privacy, trust, federation among collaborators.

We know that achieving the above level of security is a challenge. The GXA (Grid extendable architecture) tries to address the previous problem of security with a set of interoperable and industry-accepted standards. The following diagram shows

The core security standards identified by GXA in order to achieve the required end-to-end security as it are mentioned in diagram -1.3-.

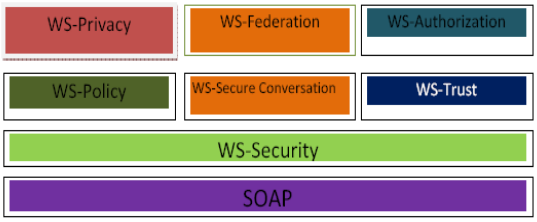

Figure -1.3-
WS-Security stack for SOAP

There are a number of distributed technologies that exist today, including Kerberos, public key, and others. The widespread acceptance of these technologies helps the creator of the WS-Security specifications decide how to use them effectively in the Web Services environment, instead of creating new security technologies.

This decision paved the way for creating XML standards that uses existing technologies and future ones. With these requirements in mind, the WS-Security standard defines a SOAP header with a number of security assertions and meta-information. This provides quality of production through message integrity and message confidentiality.

4. Grid Environment

Figure 1. Introduces a conceptual grid environment explained the layouts of a globus (A type of middleware)[10]. In this experimental environment, there are a server and two working machines:

- Certificate Authority (CA).

It is the simple certificate authority.

- Node1 (machine1) and Node2 (machine2) within a grid set up.

They are the Grid Nodes.

The user's names are different on node1 and node2, but they share the same grid user ID, which is known as the distinguished name [2]:

/O=Grid/O=Globus/OU=hostname.cs.unipune.ernet.in/CN =grid user.

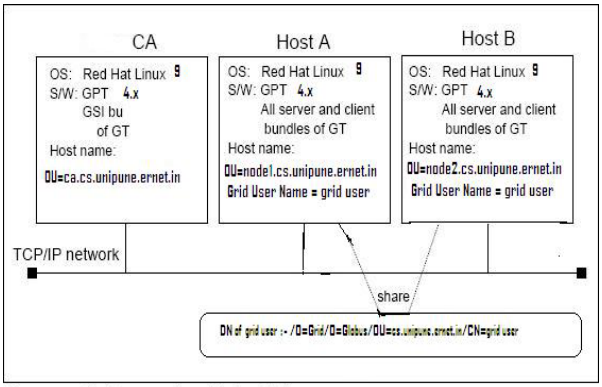

Figure 1 System overview after installation

5. Digital Certificates

Digital certificates are digital documents that associate with a grid resource with its specific public key. A certificate is a data structure containing public key and pertinent details about the key owner. A certificate is considered to be a tamper-proof electronic ID when it signed by the certificate authority for the grid environment. It is also called X.509 certificate which acts like a passport [3, 2].

A digital certificate is made up of a unique distinguished name (DN) and certificate extensions that contains the information about the individual or host that is being certified. Some information in this section may contain the subject's e-mail address, organization unit or location and so on. Below in figure -2- a graphical depiction of the digital certificate is presented [5, 6]. Figure -2- a graphical depiction of the digital certificate source

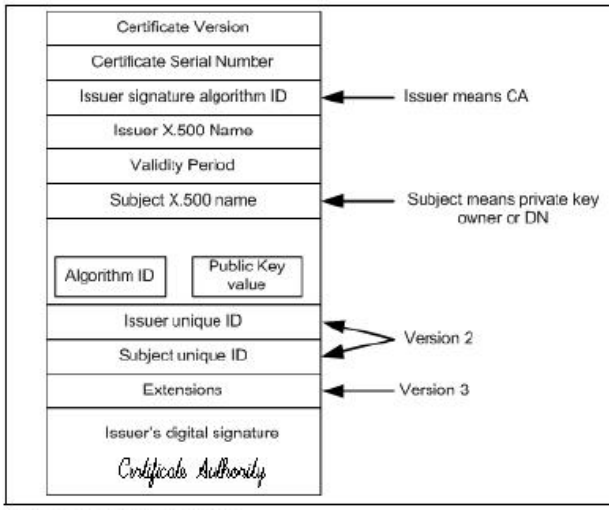

Figure -2 Digital certificate

The authentication described above is a one–time authentication for the purpose of certificate issuance. This can be compared to the processes when a government authority issues a passport to an individual [10, 11].

There are two different types of certificates that are used within a grid environment:

- User (as a grid user, you will need a user certificate to identify yourself within the grid).
  "/O=Grid/O=Globus/OU=domain name.com/CN=user name"
- Server (if you plan on running PKI enabled programs on your server, you will need to register a server certificate).
  "/O=Grid/O=Globus/OU=domain name.com/CN=server name"

Certificate revocation lists (CRLs) are issued to mark some certificates unusable, even though their expiration has not come yet. Path validation is especially important when explaining why delegated certificates are valid within the grid, as long as the path is valid within the delegated certificate [4, 5]; the following sections explain virtually obtained certificates during different requested issues. Moreover, they describe ways of showing unsigned and signed requests from actual certificate authority. Below there are two diagrams in figure 3.

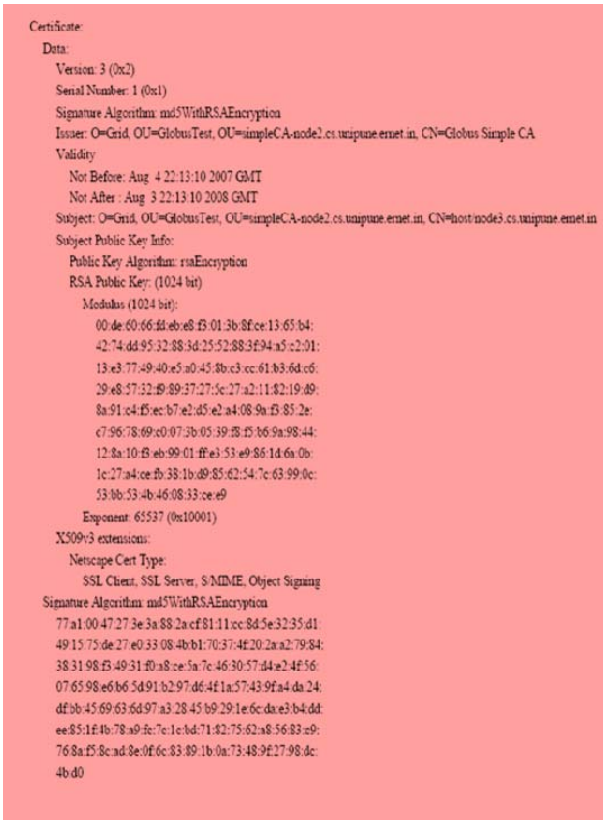

Figure-3-diagram-1- a signed certificate of a host or user by CA.

This is a Certificate Request file:

It should be mailed to mkalanni@cs.unipune.ernet.in

Certificate Subject:

/O=Grid/OU=GlobusTest/OU=simpleCA-node2.cs.unipune.ernet.in/CN=host/node3.cs.unipune.ernet.in

The above string is known as your host certificate subject, and it uniquely identifies this host.

To install this host certificate, please save this e-mail message into the following file.

/etc/grid-security/hostcert.pem

You need not edit this message in any way. Simply save this e-mail message to the file.

If you have any questions about the certificate contact the Globus Simple CA at mkalanni@cs.unipune.ernet.in

Figure-3-digram-2-is a request certificate for user/node from CA.

6. Getting Access to the Grid

In order to build a grid environment using GSI components, one has to create a set of keys for public key cryptography and request his/her certificate from the certificate authority and a copy of the public key of the CA [8]. Figure 4 describes the way to establish the GSI communication.
When that procedure has been completed and the person receives his signed digital certificate, he will have three important files on his grid host [10, 9].

The CA's public key.
The grid host's private key.
The grid host's digital certificate.

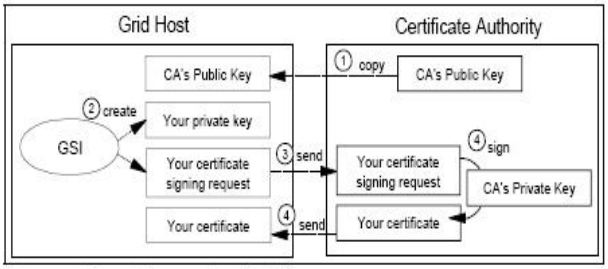

Figure 4 Preparation procedure for GSI

7. Authentication and Authorization

Imagine a scenario where users need to communicate with another grid computer's application and they want to ensure that the data from the host is really from the host. Furthermore, they should make sure that they can trust the grid host and they can use the authentication function of GSI [5, 7]. It is shown in figure 5. It has authenticated with the remote grid resource.
The subject is in the form of Distinguished Name (DN)-like.
"/O=Grid/O=Globus/OU=hostname.cs.unipune.ernet.in/CN=your name".

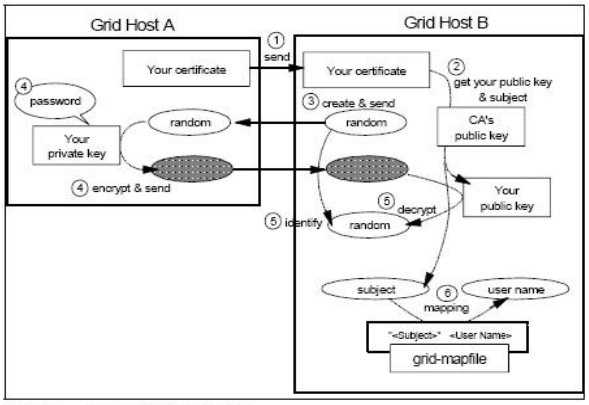

Figure 5 Authentication procedure

To put it in nutshells, authentication is the process of sharing public keys securely with each other, and authorization is the process that maps your DN to a local user/group of a remote host [6].

8. Delegation Process

Imagine a situation where you distribute jobs to remote grid machines and let them distribute their child jobs to other machines under your security policy. In this situation, your possibility can use the delegation function of GSI, as shown in figure-6-.
If you are on the side of host A, you can create your proxy at host B to delegate your authority. This proxy acts as yourself, and submits a request to host C on your behalf.

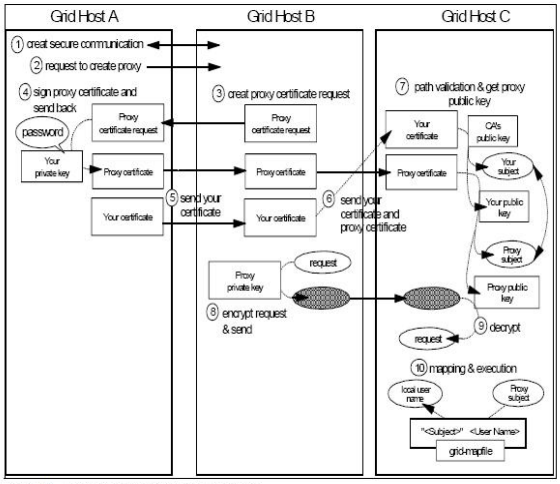

Figure 6 Delegation procedure of user's proxy

The procedure in Figure-6- represents remote delegation, where a user creates a proxy at a remote machine. There is also a local delegation, where a user creates a proxy certificate at the local machine: for that task, Globus Toolkit uses the grid-proxy-init command and gatekeeper daemon mechanism.

9. Conclusion

As mentioned at the beginning when an original machine make a proxy on a remote machine (in remote delegation), the proxy's private key is stored on the remote machine, so the supper user of that machine can access your proxy's private key. This delegation credential can be vulnerable to attacks. In order to avoid this, it is recommended that the proxy attain restricted policies from its owner and this can be advisable as the back prop implementation provided many advantages in this work. Backprop networks are very good at classifying complex relationships, which in case of anomaly detection, is useful for classifying normal and anomalous states.

The generalized back prop neural network is good formulas along with analyzing stages. The input layer of the network governs the number of inputs and external states that the network uses in classification. Likewise the output nodes govern the total number of classes the network is classifying, the back prop is trained with supervision; thus, the desired outputs for each input pattern is supplied to the network during the training phrase.

References

[1] Foster, et al, The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, 1999, ISBN 1558604758.

[2] The Anatomy of the Grid: Enabling Scalable Virtual Organizations, found at: http://www.globus.org/research/pappers/anatomy.pdf.

[3] A brief Introduction to Grid Technology: http://www.bo.infn.it/alice/introgrd/introgrd/.

[4] Computational Grids. http://www.globus.org/research/pappers/chapter2.pdf.

[5] Internet Draft Internet X.509 Public Key Infrastructure Proxy Certificate Profile. http://www.ietf.org/internet-drafts/draft-ieft-pkix-proxy-03.txt.

[6] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. http://www.itef.org/rfc/rfc3280.txt.

[7] Grid Security Infrastructure (GSI). http://www.globus.org/security.

[8] GSI-Enable OpenSSH. http://www.grid.ncsa.uiuc.edu/ssh/.

[9] IBM Grid Computing. http://www.ibm.com/grid/.

[10] IBM Solution. http://www.ibm.com/solution/.

[11] Globus Grid Forum. http://www.gridforum.org/ http://www.ggf.org/.

[12] Globus API documentation. http://www-unix.globus.org/api/c-globus-4.3.

[13] P. Asadzadeh, R. Buyya, C.Ling Kei, D. Nayar and S. Venugopal, "Global Grids Software Toolkits: A Study of Four Grid Middleware Technologies". High Performance Computing: Paradigm and Infrastructure, Laurence Yang and Minyi Guo(editors).Wiley Press, New Jersey, USA, June 2005.

[14] A. Luther, R. BUYYA, R. Ranjan and S. Venugopal,"Alchemi: A .Net-Based Enterprise Grid Computing System", in Proceedings of the 6th International Conference on Internet Computing (ICOMP05), June 27-30, 2005, Las Vegas, USA.

[15] Foster I. and C. Kesselman. "Globus: A Met computing Infrastructure Toolkits", International Journal of Supercomputer Applications, Vol 11 No.2:pp.115-128, 1997.

[16] S. Venugopal. R. Buyya and L. Winton, " A grid Service Broker for Scheduling e-Science Applications on Global Data Grids", Concurrency and Computation: Practice and Experience, Vol. 18 No. 6,pp. 685-699,Wiley Press, New York, USA, May 2006.

Maath.K.al-Anni Received the Bsc and Msc degrees in computer science in 2003, respectively from Al-Rafedan University College, Baghdad University, Iraq, since 2005 he is a PhD scholar at Pune University, India, his research interests are Distributed Computations, Network Security, Intrusion Detection Approaches, Neural Networks, Grid Computing, parallel computing, Graphics, Networks Theory, And Computation theory.