12-3-2012

Implementing a Secure Academic Grid System - A Malaysian Case

Mohd Samsu Sajat
Universiti Utara Malaysia

Suhaidi Hassan
Universiti Utara Malaysia

Adi Affandi Ahmad
Universiti Utara Malaysia

Ali Yusny Daud
Universiti Utara Malaysia

Amran Ahmad
Universiti Utara Malaysia

IMPLEMENTING A SECURE ACADEMIC GRID SYSTEM – A MALAYSIAN CASE

Mohd Samsu Sajat, Suhaidi Hassan, Adi Affandi Ahmad, Ali Yusny Daud, Amran Ahmad, Mohamed Firdhous
InterNetWorks Research Lab, School of Computing, UUM CAS,
Universiti Utara Malaysia, Malaysia
{mohdsamsu, suhaidi, adi, aliyusny, amran}@uum.edu.my, mfirdhous@internetworks.my

Abstract

Computational grids have become very popular in the recent times due to their capabilities and flexibility in handling large computationally intensive jobs. When it comes to the implementation of practical grid systems, security plays a major role due to the confidentiality of the information handled and the nature of the resources employed. Also due to the complex nature of the grid operations, grid systems face unique security threats compared to other distributed systems. This paper describes how to implement a secure grid system with special emphasis on the steps to be followed in obtaining, implementing and testing PKI certificates.

Keywords
Grid computing, grid security, virtual organization, A-grid, Sintok-grid.

INTRODUCTION

The Computational Grid has been defined as a system of hardware and software that work together to provide dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities (Foster & Kesselman, 1999). Grid systems carry out coordinated resource sharing for solving problems in dynamic, multi-institutional virtual organisations. They can negotiate and renegotiate resources sharing arrangements among the participating entities in order to carry out the task at hand in the most efficient manner (Al-iesawi & Samat, 2010). Due to the advantages of grid computing systems over isolated computing servers and other distributed systems, several countries have been promoting the implementation academic and national grid computing systems. In this line, Malaysian government embarked on implementing two grid systems under KnowledgeGrid and AcademicGrid (A-Grid) initiatives. The KnowledgeGrid initiative expects to interconnect all the government institutions including ministries, departments and other statutory bodies for the purpose of sharing resources and information while the objective of the A-Grid initiative is to interconnect the universities in Malaysia. Ultimately these grid systems would be connected to other regional and international grid systems in order to become the part of the single global grid system.

Security plays a major role in the successful implementation of any distributed system including grid systems. Due to the complex nature of grid systems compared to other distributed systems, new and unique security threats have emerged (Li, Cui, Tian, Wang, & Yan, 2006). Various grid security models and architectures such as Open Grid Forum (OGF), Alternative Security Architecture for OGSA (ASA-OGSA), Integrated Site Security for Grid (ISSeG) and Single Sign-on Infrastructure (SSI) have been proposed by several researchers and reported in literature (Demchenko, de Laat, Koeroo, & Groep, 2008; Li et al., 2006; Hoeft & Epting, 2007; Qiang & Konstantinov, 2010). These models and architectures are discussed in detail with specific reference to their strengths and weaknesses in the related work section. In this paper the authors have presented the case study of how a practical grid system has been implemented with special emphasis on security implementation. The paper describes every step to be followed when adding a Virtual Organisation to an existing grid system.

RELATED WORK

Demchenko et al. (2008) have commented that the Open Grid Forum (OGF) had been concentrating on short term security goals of achieving interoperability between presently deployed grid systems. They have further indicated that the main focus of the OGF had been on the primary security services and mechanisms such as authentication, authorization and web service protocol security. They have also shown that there is a gap between the Open Grid Security Architecture (OGSA) security model and services definition of the OGF and the practical grid implementations such as LCG/EGEE (LHC Computing Grid /Enabling Grids for E-Science), OSG (Open Science Grid) etc. The main reason for these gaps has been identified as the use of different grid middleware implementations.

Hoeft and Epting (2007) have discussed the Integrated Site Security for Grid (ISSeG) project carried out by the European Union in detail. ISSeG has been carried out as a part of the EU Framework Programme 6 by CERN of Switzerland, Forschungszentrum Karlsruhe GmbH (FZK) of Germany and STFC of the United Kingdom with specific responsibilities assigned to each partner. The ISSeG project aims to fulfil two main objectives. They are namely; to retain the site security for an effective working environment, while maintaining sufficient openness for scientific research and to ensure the three pillars of security confidentiality, integrity and availability of research and personal data. ISSeG proposes to have centralised resource management for faster detection and management of security breaches, integrated identity and resource management, and enhanced network connectivity management. It will develop and deploy security mechanisms and tools to implement effective security training, best practices and administrative procedures among all the stakeholders of the project. It can be seen that the ISSeG project focuses solely on centralized resource and event management. Though, centralised resource and event management has its own advantages in terms of efficient utilization of resources, performance will suffer when the system grows large and also limits the independence of partners. Also, ISSeG require all the sites and VOs to be homogeneous severely restricting the innovation within systems.

Qiang and Konstantinov (2010) have described a single sign-on infrastructure developed as a part of the NorduGrid Advanced Resource Connector (ARC) Grid middleware. They propose that the single sign-on with identity federation that can facilitate cross domain access would be more suitable for non-IT users than Public Key Infrastructures (PKI) to support mutual authentication using X.509 certificates. The proposed infrastructure totally eliminates the use of X.509 credentials and the users will need only their username/password combination to access any resource within the grid system. It also proposes to use Short Lived Credential Services (SLCS) for accessing grid systems that require X.509 credentials to access resources within their domains. The temporary certificates issued by SLCS have a life time of 12 hours and hence it is proposed to use only local file permissions to protect the private keys instead of encrypting them using passphrases. This is one of the main shortcomings of this propsed mechanism as it can be exploited by IT users to attack the entire system including the ones that are protected using PKI.

Li et al. (2006) have proposed an alternative security architecture that can be implemented in place of OGSA. They have also proposed that the grid security system is composed of two main components, namely; security rule definition and security rule implementation. The proposed framework can be extended easily compared to the GSI as it is developed independent of the grid system and loosely coupled to it. However the proposed mechanism suffers from the shortcoming that it stores the security data outside the grid system and hence can be attacked by malicious users easily.

DESIGN AND IMPLEMENTATION OF GRID SYSTEM

The basic architecture of the Sintok-Grid implemented at the Universiti Utara Malaysia is shown in Figure 1. The Figure shows the main nodes in the network and how they are connected together and to the public network. The architecture shown in Figure 1 consists of two network segments, namely the internal network and the external (public) network. The internal network hosts all the servers of the Sintok-Grid and the public network hosts the other grid sites in the Academic Grid Malaysia.

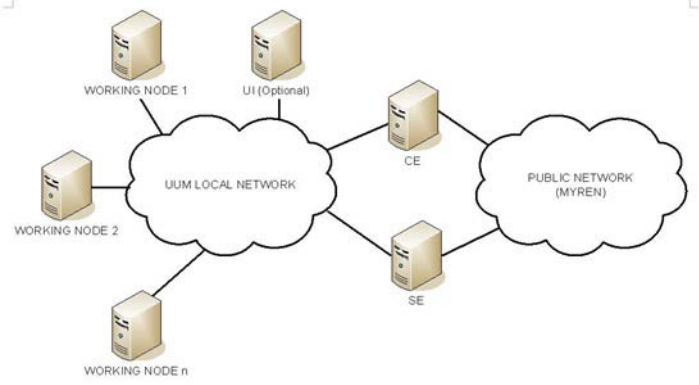

Figure 1: Architecture of the Sintok-Grid

The grid site currently hosts only the minimum number of servers necessary for a grid site. They are namely User Interface (UI), Berkeley Database Information Index Site (BDII), Storage Element (SE), Computing Element (CE) and MON. The UI is the service that provides users access to grid resources including management of tasks and data. The BDII is the grid information system consisting of a standard LDAP server

which is updated by an external process. The update process obtains LDIF from a number of sources and merges them. It then compares this to the contents of the database and creates an LDIF file of the differences. This is then used to update the database. BDII uses an LDAP implementation of the Grid Laboratory Uniform Environment data model while the accounting management is provided by the MON. The CE provides the task management control at the cluster node that handles all the workers in the cluster. The SE is the storage provider for the grid system. For a foundation level academic grid at least two special class servers are required, one for running the CE, SE and the MON and the other one hosting the BDII. Optionally the UI must also be run in a third server. The servers except the UI must be fitted with a minimum of two Network Interface Cards (NICs). One NIC will connect the server to the local network while the other one would connect it to the public network.

Each grid server requires a public Internet Protocol (IP) address and also, if the WNs need to be accessed directly by servers from other connected grid systems, they also need public IP addresses (Schmidt, Fallenbeck, Smith & Freisleben, 2009). The Sintok-Grid is a part of the larger A-Grid system, so the nodes especially the servers need to be visible and accessed from networks outside Sintok-Grid. Hence the servers were configured with public IP addresses. The other requirement for making the grid system accessible from outside is enabling them to be identified using hostnames rather than IP addresses. Hence the Domain Name Server (DNS) in the grid system must be fully configured such that forward and reverse lookups are supported for each public IP address. Reverse lookups enables the resolution of fully qualified domain names from IP addresses (Taddia & Mazzini, 2005; Jung, Sit, Balakrishnan & Morris, 2002). Also reverse lookups can be used to detect intrusions thus protecting the servers from attacks (Erbacher, Walker & Frincke, 2002). Hence DNS system was setup in order to make the Sintok-Grid seamlessly integrate with the A-Grid. The link capacity or bandwidth between the WNs and the network, or WAN cloud, plays a major role in the overall performance of the system. The network bandwidth used must be able to accommodate the data and the command requests and responses transferred between the public network and the local network to be processed by WNs. In the case of Sintok-Grid, the bandwidth of the UUM Internet link is sufficiently large enough to handle the expected traffic.

Once the hardware of the grid system and the network has been installed the system must be installed with the right software especially the operating system, middleware and virtualization software. In order to minimize the cost of the overall implementation, it is possible to use open source software for all the components. In the current implementation of the Sintok-Grid, Scientific Linux 5.x, gLite 3.2 and Proxmox 1.8 have been selected as the operating system, middleware and virtualization platform respectively. Specific elements of the grid system such as CE, SE, UI and IS require specific installation process to be followed. The following sections briefly explain the steps to be followed when implementing these systems.

Installation of Computing Element

The CE is one of the main components of the grid system. The CE is the element that interfaces with both the public network and the internal network where the WNs are connected. The items required to be installed are the operating system (Scientific Linux 5.x) and Host certificate. The steps to be followed are:

- Enable the reverse lookup for CE IP address on the DNS server.
- Stop yum autoupdate service
- System time must be synchronised using an NTP server
- Install YUM Repository (EMI Release)
- Install CA Certificates
- Update YUM Database
- Install Package, CA, CREAM CE and TORQUE
- Install Host Certificate
- set the right permissions

Installation of User Interface

UI is a client suite and API that can be used by applications and users to access gLite services. The UI components available in gLite include:

- VOMS command-line tools

- Workload Management System clients and APIs
- Logging and Bookkeeping clients and APIs
- Data Transfer command-line clients and APIs
- Data Catalog command-line clients and APIs
- gLite I / O client and APIs
- R-GMA client and APIs

The steps to be followed are:

- Add the YUM repository UI
- Install glite-UI RPMs and configuration tool YAIM
- Configure the User Interface
- Determine the Grid Services to be used by the UI
- Define Parameters of Virtual Organization (VO)
- Use the YAIM to configure the UI
- Test the UI

Installation of Storage Element

Storage Element (SE) and the Information System (IS) were co-hosted on the same computer to reduce cost. Hence prior to installing the SE, the platform was virtualized using Proxmox 1.8. The SE and IS were then installed independently on the two separate virtualized systems. The components o be installed include the operating system (Scientific Linux 5.x), Host certificate and MySQL database. The steps to be followed are as follows:

- Enable the reverse lookup for CE IP address on the DNS server.
- Stop yum autoupdate service
- System time must be synchronized using an NTP server
- Install YUM Repository
- Install CA Certificates
- Update YUM Database
- Copy the Host Certificates to Grid Security Folder and Set the Permissions
- Install DPM MySQL
- Configure Users and Groups

SECURITY INSTALLATION AND TESTING

This section explains the security installation and testing carried out in the Sintok-Grid a VO in the Academic Grid Malaysia. The security of the Sintok-Grid is based on PKI and user certificates along with username password combination for users. The reasons for adopting PKI for Sintok-Grid security include the following considerations. The most common security infrastructure for grid computing namely the Grid Security Infrastructure (GSI) is also based on Public Key Infrastructure (PKI) (Heo & Hwang, 2012; Pala, Cholia, Rea, & Smith, 2011). The grid systems require an authentication mechanism that inter-operates across domain boundaries. PKI is well suited for such situations as it provides sufficient flexibility to allow resource managers to securely grant access to their systems in such distributed environments (Pala, Cholia, Rea, & Smith, 2008). Also in many countries there are national PKIs which are government organizations that have a very rigours procedure for issuing certificates. Hence the certificates issued by these national PKIs can be trusted with relative ease as they are guaranteed by governments. Certification Authority (CA) is the main component in a PKI. The CA verifies and confirms the identities of entities involved in a communication similar to a notary. In a national PKI, a government agency plays the role of a CA, hence the communication between two validated

parties are authenticated by the government itself. Also the PKI certificate contains a pair of public and private keys for validation along with extensible attributes for additional information. Public private key pair provides the maximum protection possible as the private key is never transmitted or disclosed to anybody under any circumstance.

Certificate Installation on Clients

Figure 2 shows the process that needs to be followed when a user needs to access the grid system. Every user needs to possess a valid user certificate obtained from a CA in order to access the grid system. Also every host computer except for the Worker Nodes (WN) and User Interface (UI) must also have a certificate of the host to operate. In Malaysia, both user certificates and host certificates can be obtained from Academia Sinica Grid Computing Certification Authority (ASGCCA) in headquartered Taiwan or the Malaysian Identity Federation and Management Certification Authority (MYIFAM) or headquartered in Malaysia. The Malaysian grid community is very familiar with both the CAs. Figure 3 shows the flow diagram of the ASGCCA user certification request process.

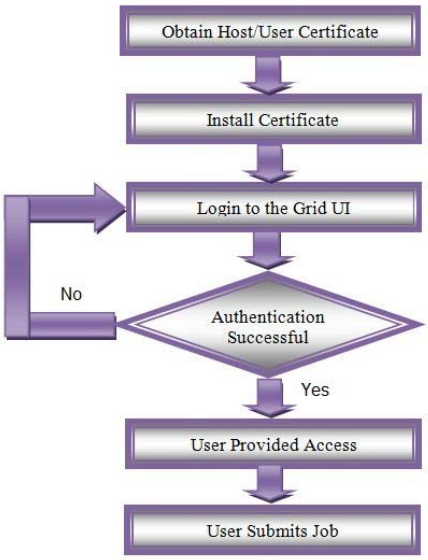

Figure 2: Process of Accessing Grid System

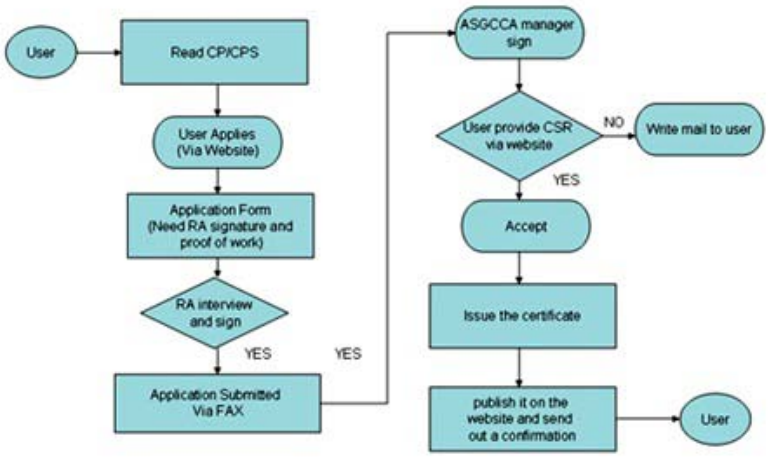

Figure 3: Certification Request Process at ASGCCA

To obtain the digital certificate files, the following steps should be strictly followed:

1. Complete the following forms:
    - OPR/iDEC/BR05/Biruni Grid Computing,

- OPR/iDEC/BR03/Sokongan ICT and
- ASGC CA User Certificate Form.

2. Apply online by submitting the duly completed forms at http://ca.grid.sinica.edu.tw/certificate/request/cert.php.

3. Once the application has been approved, obtain the digital certificate from http://ca.grid.sinica.edu.tw/certificate/request/import_cert.html by entering the certificate number.

4. Create a backup of the Digital Certificate.

5. Copy the User Certificate to grid UI.

User must store the files associated with the Digital Certificate in a folder in their home directories and change the file permission. The *userkey* file must be disabled all permission except for read for the owner and the *usercert* file must have only read access for all and read/write access for owner. Once the certificate has been installed on the client computer, users can log in to the grid UI by supplying the username/password pair supplied by the CA. If the username/password pair supplied is correct, the user will be authenticated and provided access to the grid resources. Then the user can submit jobs to the grid. Usually users are given a maximum of 12 hours continuous access including any job completion time except when long term proxy certificate has been specifically applied.

Host certificate Installation on Servers

Host certificates need to be installed on every server except the UI and WNs. The certificates obtained from the CA must be copied to the grid-security folder in the servers and the permissions be set accordingly. The *hostkey* file must be readable only by the administrator and all the other permissions be disabled and the *hostcert* file must have world readable and read/write for the administrator.

Security Testing

Security testing needs to be carried out in order to make sure that the security implementation is working properly and unauthorised access is detected and eliminated. First a valid user account must be created and digital certificate must be applied to it as explained before. Once the account is created, then it can be used to login to the UI server using ssh grid client or PuTTY application on Windows. If the username/password supplied is correct then the system should authenticate the user and provide permission to access the grid resources, otherwise access must be denied. The users who enter the wrong passwords are given additional opportunities to enter the password as genuine mistakes are possible.

CONCLUSION

This paper presented a case study of how a secure grid system was implemented as part of the Malaysian national grid initiative. The paper discussed the installation of the grid system briefly and the implementation of security in detail. Every step that must be followed in the installation of security certificate in both the server systems and clients was described in detail along with how to test the implementation for proper functioning of the same.

REFERENCES

Al-iesawi, A. M., & Samat, M. I. M. (2010). *A case study on implementation of grid computing to academic institution*. Paper presented at the 2010 International Symposium in Information Technology, Kuala Lumpur, Malaysia.

Demchenko, Y., de Laat, C., Koeroo, O., & Groep D. (2008). *Re-thinking grid security architecture*. Paper presented at the Fourth IEEE International Conference on eScience, Indianapolis, IN, USA.

Erbacher, R. F, Walker, K. L., & Frincke, D. A. (2002). Intrusion and misuse detection in large-scale systems. *IEEE Computer Graphics and Applications*, 22(1), 38–47.

Foster, I., & Kesselman, C. (1999). *The grid: Blueprint for a new computing infrastructure*. San Francisco, CA: Morgan Kaufmann.

Heo, D., & Hwang, S. (2012). Proposal to adapt reliability of national PKI to grid security infrastructure by credential translation and delegation with OAuth. *International Journal of Security and Its Applications*, 6(3), 65–73.

Hoeft, B., & Epting, U. (2007). *Integrated site security for grid: An initiative to cover security beyond the grid*. Paper presented at the 2007 IFIP International Conference on Network and Parallel Computing - Workshops, Dalian, China.

Jung, J., Sit, E., Balakrishnan, H., & Morris, R. (2002). DNS performance and the effectiveness of caching. *IEEE/ACM Transactions on Networking*, 10(5), 589–603.

Li, M., Cui, Y., Tian, Y., Wang, D., & Yan, S. (2006). *A new architecture of grid security system construction*. Paper presented at the 2006 International Conference on Parallel Processing Workshops, Columbus, OH, USA.

Pala, M., Cholia, S., Rea, S. A., & Smith, S.W. (2008). *Extending PKI interoperability in computational grids*. Paper presented at the 8th IEEE International Symposium on Cluster Computing and the Grid, Lyon, France.

Pala, M., Cholia, S., Rea, S. A., & Smith, S. W. (2011). Federated PKI authentication in computing grids: Past, present, and future. In E. Udoh (Ed.), *Cloud, Grid and High Performance Computing: Emerging Applications* (pp. 165-179). Hershey, PA: Information Science Reference.

Qiang, W., & Konstantinov, A. (2010). *The design and implementation of standards-based grid single sign-on using federated identity*. Paper presented at the 12th IEEE International Conference on High Performance Computing and Communications, Melbourne, Australia.

Schmidt, M., Fallenbeck, N., Smith, M., & Freisleben, B. (2009). *Secure service-oriented grid computing with public virtual worker nodes*. Paper presented at the 35th Euromicro Conference on Software Engineering and Advanced Applications, Patras, Greece.

Taddia, C., & Mazzini, G. (2005). *DNS reverse lookup statistics*. Paper presented at the International Conference on Wireless Networks, Communications and Mobile Computing, Maui, HI, USA.

Vecchio, D. D., Hazlewood, V., & Humphrey, M. (2006). *Evaluating grid portal security*. Paper presented at the 2006 ACM/IEEE Conference on Supercomputing, Tampa, FL, USA.