Towards Developing an Authentication Framework for Securing GUISET Infrastructure

Noluthando B. Mhlongo, Edgar Jembere and Matthew Adigun
Department of Computer Science
University of Zululand, Private Bag X1001, KwaDlangezwa, Empangeni 3880
Tel: +27 35 9026393, Fax +27 35 9026569
thandomhlongo4@gmail.com , ejembere@gmail.com and madigun@pan.uz.ac.za

Abstract-Grid Computing has come out to be a significant field considering its focus on large scale resource sharing. There are many grid infrastructures that have been developed. Within these infrastructures, users may utilize processing, storage, software, and data resources from any interconnected computers leading to greater resource sharing and utilization ratio. Such dynamic and multi-institutional natures of grid environments introduce challenging security issues that require technical approaches. To ensure no unauthorized access to such an infrastructure, this work proposes an authentication framework. We intend to adopt a certificate enabled Grid Security Infrastructure (GSI), which will thus assist the password based mutual authentication between the grid infrastructure users that request resources and the server granting access to the users.

Index Terms---Grid Computing, Security, Mutual Authentication Framework.

I. INTRODUCTION

Grid was defined in the mid 90's as a "hardware and software infrastructure that provides dependable, consistent, pervasive and inexpensive access to high computational capabilities" [1]. This definition has now broadened with more focus on "coordinated resource sharing and problem solving in multi-institutional virtual organizations" [2]. Basically, a grid computing infrastructure supports the sharing and coordinated use of resources in dynamic global, heterogeneous distributed environments. A known example of a grid-based infrastructure is the -Grid-based Utility Infrastructure for Small, medium, and micro enterprises Enabled Technology (GUISET) [3], which is a typical grid service provisioning environment. GUISET was developed to enhance business operations where SMMEs need not own the infrastructure but could pay for what they use [4]. The main idea of GUISET is to provide an e-infrastructure where SMME's are able to pool their resources and expertise together for sharing and collaboration among themselves and their external business partners.

With the open resource sharing paradigm and the provisioning of unlimited access to end users by GUISET, security challenges arise. This paper seeks to secure the shareable resources in the GUISET infrastructure by authenticating every user that requires access to them. It should thus be noted that, not only does a server need to authenticate a user's identity to ensure that there is no unauthorized usage of resources, but also the server must be authenticated by the user to assure that the resources received can be trusted. We refer to this as mutual authentication. So the adoption of a certificate enabled Grid Security Infrastructure will thus enable the mutual authentication.

The rest of the paper is structured as follows: section II explores the related work, section III discusses the framework, and section IV concludes the paper.

II. RELATED WORK

Due to the increase in the usability and sharing of resources, the resources become vulnerable to security threats. These resources need to be protected. The confidentiality, integrity of resources and privacy of the user information need to be maintained. Currently, the Grid Security Infrastructure [5] plays a vital role in securing the grid resources. With the GSI's capability of supporting single sign-on, mutual authentication and delegation, GSI will be essential when developing our security framework. GSI, Developed as part of the Globus toolkit (http://www.globus.org/toolkit) [12], is based on Public key Infrastructure which uses X.509 certificates as the way in which users authenticate themselves in grid-network activates that perform identity verification.

In the past, many systems have relied on a simple password for authentication; this is still true of many web interfaces used today. Crampton et-al [6] proposed a security infrastructure for grid applications, in which users are authenticated using passwords only. His work might have been very effective since it supported many essential grid security services which add value to our work e.g. single sign on, mutual authentication and the use of public key cryptographic techniques. But there are a number of problems with this type of authentication. Firstly knowing a password is not a full proof mechanism to authenticate an individual [14]. In theory they can be a strong authentication mechanism, but in practice passwords get mislaid or the management of password files can easily become compromised by user or external forces. As such passwords by themselves are inadequate as a primary line of defense.

There are many other solutions for the grid security systems. Notable examples are Kerberos [7], CRISIS [8] etc. Kerberos has been widely used for its provision of mutual authentication between the requestor and servers, but has a disadvantage of relying heavily on cryptography which may lead to performance issues.

CRISIS is the security component of Web-OS; an operating system designed for use in wide area distributed computing. Web-OS and Globus are Similar in that they both aim to provide seamless access to files and computational resources distributed throughout a wide-area network. CRISIS, like GSI, employs X.509 for certificates.

Lim and Paterson [9] recently proposed a fully identity-based security infrastructure for grid application using identity-based public key cryptography. Key management in this approach is simpler that in the PKI-based GSI because it does not use certificates and key sizes are relatively small. This strategy may be disadvantageous since key revocation can be a bit complicated. To enhance this, Boneh and Franklin [10] proposed the use of a date concatenated with a user's identifier to achieve automated key expiry. However, this approach has the disadvantage of increasing the workload of a private key generation, since the PKI is required to regularly issue private key to its users.

Laganier [11] believes that security mechanisms used currently do not scale well with most participating domains and entities and all this is due to the use of the public key infrastructure global to the grid environments. His work proposes an approach in which he combines the network and operating system virtualization with the Host Identity Protocol (HIP) and a simple public key infrastructure (SPKI) delegation/ authorization certificate. This method is believed to be efficient because it allows for the maximum of generality, because its lowest layer implementation allows it to contribute a least common denominator to deployed security infrastructure. And differs from the GSI from an implementation point of view.

In a broader sense, any system's security goal is to prevent users who do not have proper privileges from accessing resources and information organizations participating in grids must use appropriate policies to harden their infrastructures while enabling interaction with the outside resources. So, drawing inspiration from these existing security systems, we intend to fill the gap of securing the grid infrastructure (GUISET) from intruders who do not have proper privileges to access the GUISET resources. We intend to mutually authenticate both GUISET service requestors and providers, making sure that sensitive and proprietary data/resources are secured.

III. PROPOSED RESEARCH APPROACH

This research intends to investigate the usage scenarios in the GUISET infrastructure and the security requirements of such scenarios. We want to formulate/ develop a mutual authentication framework to secure the GUISET resources from being accessed by unauthorized users. The framework will be inspired by the existing grid security infrastructure, which uses the certificates to assist password based mutual authentication. The proposed authentication framework will then be evaluated as a GUISET broker capability.

IV. CONCLUSION

The provision of fast and flexible information/resource sharing to Small, Medium, and Micro Enterprises by GUISET has resulted into resources being exposed to security threats and vulnerabilities. Based on existing security infrastructures for grid environments, this paper proposes an authentication framework to secure these shared resources. We want to authenticate both requesters and providers before access to GUISET resources is granted.

REFERENCES

[1] Foster I. and Kesselman C, editors. (1999):" *The Grid: Blueprint for a New Computing Infrastructure"*, 1999. Morgan Kaufmann Publishers, Inc.

[2] Foster I. (2002), "What is the Grid: A Three-PointChecklist", 2002. Online at: wwwfp.mcs.anl.gov/~foster/Articles/WhatIsTheGrid.pdf.

[3] Adigun M., Emuoyibofarhe O., Migira S. (2006) "Challenges to Access and Opportunity to use SMME enabling Technologies in Africa" 1st All Africa Technology Diffusion Conference. Johannesburg South Africa, June 12-14, 2006.

[4] Sibiya M.G., Jembere E., Xulu S.S., Adigun M.O. (2008) "A Web Services based e-Commerce Business Model for Resource Constrained SMMEs" Proceedings of the 2008 SATNAC Conference.

[5] Foster I., Kesselman C., Tsudik G., Tuecke S. (1998) "Security Architecture for Computational Grids" 5th ACM conference on Computer and Communications Security, 1998.

[6] Crampton J., Lim H., Paterson K., Price G. (2007) "A Certificate-Free Grid Security Infrastructure Supporting Password-Based User Authentication" In Proceedings of the 6th Annual PKI R&D Workshop, 2007.

[7] Neuman C.,Yu T., Hartman S. (2005) "The Kerberos Network Authentication Service (V5)" RFC 1510, 1993.

[8] Belani E., Vahdat A., Anderson T., Pahlin M. (1998) "The CRISIS Wide Area Security Archiecture" In Usenix Security Symposium, Jan 1998.

[9] Lim W., Paterson G. (2005) "Identity-based cryptography for grid security. Proceedings of the 1st IEEE International Conference on e-Science and Grid Computing, pages 395-404, 2005.

[10] Boneh D., Franklin M. (2001) "Identity-based encryption from the Weil pairing" Advances in Cryptology Proceedings of CRYPTO 2001, pages 213–229. Springer- Verlag LNCS 2139, August 2001.

[11] Laganier J.,Primet P. (2005) "HIPernet: A Decentralized Security Infrastructure for Large Scale Grid Environments" Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, 2005.

[12] http://www.globus.org/toolkit. (last accessed 04 June 2010)

Noluthando Mhlongo received her undergraduate degree from the University of Zululand in 2008 and is currently studying towards her Masters of Science degree at the same institution. Her research interests include security in grid computing infrastructures.