ENHANCEMENT OF A SIMPLE USER AUTHENTICATION SCHEME FOR GRID COMPUTING

VIKNESH A/L RAMAMOORTHY

UNIVERSITI TEKNOLOGI MALAYSIA

ABSTRACT

Grid computing means a multiple independent computing, because it is composed of resource nodes not located within a single administrative domain. The goal of grid is to only provide secure grid service resources to legal users. Even though grid computing is more than just a technology to abet high performance computing, it is still have some issues to concerns and cares. One of the issues is security issues. Authentication is important part in grid security. Other process in grid are depends on authentication. The aim of this project is to enhance the method of password based authentication scheme and to get better password based authentication scheme in grid computing environment through its time complexity. In this project, the study is done on the existing grid security infrastructure and existing password based authentication scheme. Password Enable Certificate Free Grid Security Infrastructure (PECF-GSI) and A Simple User Authentication Scheme has been selected as the reference for the enhanced authentication scheme. Comparative study and pre-lab testing on A Simple User Authentication Scheme and PECF-GSI has been done in the research methodology. Finally, the enhanced authentication scheme has been designed, developed and tested based on four time complexity notations that are time for modular multiplication, time for multiplication of a number and an elliptic curve point, time for hashing operation and time for inversion. This project has achieved the aim, the scope and the objectives of the project by showing a good performance in terms of time complexity.

ABSTRAK

Pengkomputeran grid bermaksud pelbagai pengkomputeran yang tidak bersandar, ini kerana grid mempunyai pelbagai nod sumber yang tidak terletak hanya dalam suatu domain pentadbiran. Matlamat grid adalah memberikan perkhidmatan sumber grid yang selamat kepada pengguna yang sah. Walaupun pengkomputeran grid jauh lebih hebat berbanding pengkomputeran keberkesanan tinggi, ia masih mempunyai isu-isu yang perlu diambil kira. Salah satu isu adalah isu keselamatan. Pengesahan merupakan isu yang penting dalam keselamatan pengkomputeran grid. Proses lain di dalam grid bergantung kepada pengesahan. Matlamat kajian ini adalah melakukan penambahan keatas kaedah metod skim pengesahan berasaskan katalaluan dan mendapatkan skim pengesahan berasaskan katalaluan yang lebih baik bagi pengkomputeran grid menerusi masa kerumitannya. Dalam kajian ini, carian dan perbandingan dilakukan terhadap infrastruktur keselamatan grid yang sedia ada dan juga skim pengesahan berasaskan katalaluan yang sedia ada. Infrastruktur keselamatan grid yang membenarkan katalaluan dan tidak perlukan sijil (PECF-GSI) dan Sebuah Skim Pengesahan Pengguna yang Mudah bagi Pengkomputeran Grid dipilih sebagai rujukan bagi skim yang hendak ditambah. Kajian perbandingan dan pra-ujian makmal terhadap Skim Pengesahan Pengguna yang Mudah dan PECF-GSI telah dilaksanakan dalam metodologi kajian. Akhir sekali, model skim penambahan direka, dibangunkan dan diuji mengunakan empat notasi kompleksiti masa. Iaitu, masa untuk modular pendaraban, masa untuk pendaraban suatu nombor dengan lengkungan elliptic, masa untuk operasi hash, dan masa untuk operasi penyongsangan. Projek ini telah mencapai skop dan objektif dengan menunjukkan prestasi yang baik.

TABLE OF CONTENTS

2 LITERATURE REVIEW

CHAPTER 1

INTRODUCTION

1.1 Introduction

Grid computing in general is a special type of parallel computing which relies on complete computers with onboard Central Processing Unit (CPU), storage, power supply, network interface and more connected to a network like private, public or the Internet by a conventional network interface, such as Ethernet. The analogy of grid can described as below.

When user plug an appliance or other object requiring electrical power into a receptacle, user expect that there is power of the correct voltage available, but the actual source of that power is not known. Any local utility company provides the interface into a complex network generators and power sources and provides the public with an acceptable quality of service for public energy demands. Rather than each house or neighborhood having to obtain and maintain its own generator of electricity, the grid infrastructure provides a virtual generator and it is highly reliable generator.

Grid technology also enables complex interactions among computational and data resources. The sharing of the resources in grid computing will increase the range of computer applications. This sharing may involve not only file exchange but also direct

access to computers, software, data, and other resources, as is required by a range of collaborative problem solving and resource-brokering strategies emerging in industry, science and engineering. When a user wants to request some computing and data resources, the grid can seamlessly, transparently and dynamically supply the resources over Internet.

1.2 Problem Background

The sharing process in grid is necessarily and highly controlled with resource providers and users or consumers defining clearly and carefully just what is shared, who is allowed to share, and the conditions under which sharing occurs. The controlling process is important because the goal of grid computing is to only provide secure grid service resources to legal users (Lu. R. *et al,* 2007). This statement clears out that, the security issues becomes an important concern of grid computing.

To prevent the illegal users from visiting the grid resources, it should be guaranteed that strong mutual authentication needed for users and servers. Authentication is believed, as a cornerstone service, since other services depend on the authentication of communication entities. As mentioned above, the grid systems should be guaranteed that stronger authentication needed for users and servers and ensure that resources and data not provided by an attacker. Generally, the authentication in the grid computing aims to:-

1. 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. Guarantee the safety of the information in grid.

Beside these aims, two main issues of authentication process must be considered. First is the security of the authentication and second is the time complexity of the authentication. The security of the authentication can be found by analyze the security properties which consist of some security attacks. The authentication process must resist some security attack to fulfill the grid's aims.

Authentication process must control the time complexity, whereby the time complexity is important to have efficient authentication process. The time consuming of authentication can be found by analyze the time of complexity and the types of computation.

1.3 Problem Statement

Grid computing, as a distributed computing model, stands for the new kind of systems that combine heterogeneous computational resources, such as computers, storage space, sensors, application software, and experiment data, connected by the Internet and make them easy access to a wide user community.

From the problem background for flexibility in grid computing the authentication framework should strike a proper balance between the entirely demands of the security and the access speed. Fluent choosing different security mechanisms based on different demands is a powerful solution. The authentication framework also should be designed to have the interoperability with local security solutions, and apply the local access control mechanism without change to get lightweight grid environment.

Beside that, the authentication should not be bundled with any concrete and fixed mechanism of security, because of the dynamic nature of the grid (Chen.J. 2006), even though certificate based authentication more appropriate and secure than password based authentication (Chakrabarti.A. 2007).

1.4 Project Aim

This project aimed to enhance the method of password based authentication scheme and to get better password based authentication scheme in grid computing environment through its time complexity.

1.5 Project Objectives

To achieve the aim of the project, there are three major objectives have to be fulfilled:

1. To analyze the characteristics of grid computing environments, the security challenges in grid computing, the existing password based authentication scheme, the existing grid security infrastructure.

2. To design and develop the enhanced password based authentication scheme that will secure the grid computing environment using selected existing authentication scheme.

3. To test and implement the enhanced authentication scheme using lab testing.

1.6 Project Scope

1. The study focused on the existing authentication scheme and especially on password based authentication scheme.

2. The features selection of password based authentication scheme done by comparative studies and lab experiment.

3. The grid security infrastructure involve in this study should support password based authentication.

4. The development is using C++ programming language.

REFERENCES

Aura T, Roe M. *Strengthening Short Hash Values,* Microsoft Research

Bagwell P. *Ideal Hash Trees,* Es Grands Champs, Switzerland

Butt. A. R., Adabala, S., Kapadia, N.H., Figueiredo, R. J., Fortes, J.A.B. *Grid Computing Portals and Security Issues*. Journal of Parallel and Distributed Computing. 2003. 63: 1006 – 1014

Cai Z. A Password based Grid Security Infrastructure. *Second International Conference on the Digital Society*.IEEE Computer Society 2008

Certicom, *The Elliptic Curve Cryptosystems,* Updated 2000, published 1997.

Chakrabarti, A. *Grid Computing Security.* Berlin Heidelberg N.Y.: Springer-Verlag. 2007

Chakrabarti, A., Damodaran, A., Sengupta, S. *Grid Computing Security : A Taxonomy*. IEEE Security & Privacy. IEEE computer society. 2007

Chivers, H. Grid Security: *Problems and Potential Solutions Computing.* International Journal of Network Security. 2007 Vol.7 No.2 202–206

Crampton, J., Lim, H.W., Paterson, K.G., Price, G. *A Certificate Free Grid Security Infrastructure Supporting Password Based User Authentication*.UK Engineering and Physical Sciences Research Council (EPSRC). 2008

Foster I,Kesselman C,Tuecke S, Tsudik G. *A security Architecture for Computational Grids.* Conference on Computer & Communication Security. San Francisco CA USA 1998

Hu, H., Yao, H. *A scheme for Authentication and Authorization in a Grid Application*. Conference on Advanced Information Networking and Application. IEEE. 2005

Koblitz N, Menezes A, Vanstone S, *The State of Elliptic Curve Cryptography*, Designs, Codes and Cryptography. 2000. Kluwer Academic Publishers, Boston.

Lu, R., Cao, Z., Chai, Z., Liang, X., *A Simple User Authentication Scheme for Grid Computing.*

Manish Mehta, *Authentication services in Open Grid Services*. Ph.D. University of Missouri, USA:2004

Saeki M, (1997) *Elliptic Curve Cryptosystems,* School of Computer science, McGill University, Montreal.

Shamus Software Ltd, *MIRACL User Manual,* Ballybough, Ireland.

Thompson, M. R., Jackson, K. R. *Security Challenges in Supporting Grid Computing and Collaboration*. Distributed System Department - Lawrence Berkeley National Laboratory

Welch V., Siebenlist, F., Foster I., Bresnahan J., Czajkowaki K., Gawor J., Kesselman C., Meder S., Pearlman L., Tuecke S. Security for Grids Services.

Welch V.,Pearlman L.,Foster I.,Kesselman C.,Tuecke S. *A Community Authorization Service for Group Collaboration*

Wu, R., Li, R., Yu, F., Yue, G., Xu, C. *Research on User Authentication for Grid Computing Security*. Second International Conference on Semantics, Knowledge, and Grid. 2006. IEEE Computer Society. 2006.

Yoon, E.J., Yoo, K.Y., (2005) *An Efficient Password Authentication Schemes Without Using the Server Public Key for Grid Computing.* In Zhuge H and Fox G.C Grid and Cooperative Computing (149-154). Berlin Heidelberg: Springer-Verlag.