ISSN 2320 - 2602
Volume 3, No.2, February 2014
International Journal of Advances in Computer Science and Technology
Available Online at http://warse.org/pdfs/2014/ijacst10322014.pdf

Improving Grid Networks Security by One-time Password Security Mechanism

Aida Kazemi
Islamic Azad University of Central Tehran Branch, Iran, A.Kazemii@hotmail.com

ABSTRACT

The goal of grid networks is to integrate all of hardware and software capabilities of the different sets of computers as a comprehensive system, in order to calculate and process the data. Data has play key role in Grid computing. Support of distributed resources and prevent any unauthorized access to data, require a secure access control system to grid network. In this article with use of OTP security mechanism by workflow, we present a mechanism for controlling allowed access to grid networks for increasing security, to envelope all of security services such confidentiality, collectivity, identification and as Non-repudiation and prevent any security threats.

Keyword: Authentication, Grid computing, Hash Algorithm, One-time password(OTP), Security

1. INTRODUCTION

Grid computing is a distributed computing model that is used to solve computational problems or data and was first presented in 1998 by Kesselman and Foster [1][2]. Grid computing technique has been used in various fields such as electronics, biology, astronomy, etc. [3][4]. An example of using this technique is to create virtual observatory and astronomical use. In fact the grids need to coordinate with workflow for secure its security. Given that the data plays an important role in distributed systems, including the grids, so their security is considered as an important issue. In fact, data is the main object in processing and grid computing [5]. However, the security implications are important in processing and data access. Type of credit control and data integrity is a problem and a lot of research has been done in this area. For example, for data protection four solutions is suggested [6]: Preventing the system calls in application level: to ensure no invalid code enforcement, a transfer code is generated based on the arguments.

To avoid system calls at the user level: in this way the user access to file system objects, such as directories, directory trees, etc. Monitoring and relevant calls are evaluated and reviewed.

Flexible Core: Here implementing resources have access to the core and sent hardware resources to lower levels to library systems and supports each source separately. This solution is solvable in extremely complex manner and sometime is system dependent .

Virtualization: a way of isolating systems is virtualization that produces the illusion of a single, integrated system. Basic techniques of virtualization include: Virtualized grouped models Para-virtual Model

In virtualized grouped models, multiple operating systems, which are called guest operating systems run as a user on the host operating system. In general, this method does not need to change the host operating system. One of the most popular of these methods is VMWare GSX Server that use various optimization to reduce virtualization overheads. Para-virtual model use storing of hardware modes for memory and resources management and overhead is very small in performance. In Para-virtual model because of the performance boost, changes takes place in the operating system and in this method has higher performance compared with the grouped case. In conjunction with the para-virtualisation Xen provides very good performance. In addition to these two virtualization model, another model of virtualization has been suggested in [7] that is using share core based on virtualization techniques and in this technique kernel has been used shareable and user space segmented for using on different set of applications. One example of these shared kernel is used on Linux Vserver [8]. Overall in grid computing to provide security there is two layers of hierarchy: The top layer is layer of protective supervision and is a virtual organization and the bottom layer consists of Grid enabled resources. Grid workflow is used to provide security for Grid computing. Workflow can be used to reduce the risk of the user dataset. Safety requirements in this case are:

1. Data Confidentiality: To ensure that unapproved principles of work data don't read
2. Finishing the work data: To ensure that unapproved changes are detected.
3. Confidentiality of data workflow: To ensure that unapproved principles of data don't read workflow.
4. Complete data of workflow: to ensure that unapproved changes in workflow are identified [9].

In Grid networks, for controlling of allowed accesses to the system, the authentication method is used by the X.509 digital certificate authentication. However discovering of it and using it to logging to system by invaders is possible. In this paper, we present a method to enhance the security authentication that in every access to the system a disposable password (encryption key) is used for user authentication. This approach reduces the chances of theft and reuse by the attacker.

2. One-time password technology (OTP)

Currently there are various ways to attack computer systems in networks. Some types of attacks are guessing weak and inappropriate passwords, testing all possible states and dictionary attacks. One way to avoid this problem is to use disposable passwords or dynamic (One Time Password) as passwords. One of the main advantages of dynamic passwords as compared to traditional password is their robustness against attacks, Because each password is used only in one work session, there is no possibility of hearing and reuse of password, so it is more important than static passwords and is suitable for high security applications in the virtual world. One Time Password or OTP is one of the authentication methods. Authentication is done in three ways, namely:

1. What You Know Authentication (such as a password)
2. What You Have Authentication (eg, token or card)
3. What You Are Authentication (eg, corneal scans or fingerprinting)

The first authentication method has long been used and in this manner there is always concerns about disclosing and forgetting the password. The third type of authentication being used vastly but it does not operate in virtual environment, because in this way the user needs different equipment such as cameras, scanners, as well as fingerprint, that is not possible for all users. But the second authentication method that is the main topic of this paper provides the best method and producer tool to generate OTP to us. This method is usually used with the first method of authentication and called two-factor Authentication [10].

Devices that could produce disposable password is called OTP Token and have various varieties.

2.1 Categorizing types of OTP Token

In order to generate disposable passwords a tool called OTP Token is used. This tool can either used as hardware or software for the user. In Two-factor authentication simultaneously two factor is used for user authentication [10]. One of these factors can be fixed password and other factor usually is a device, software or a tool that the user owns. The second factor can be used in two forms: hardware and software. The hardware form is usually took the form of hardware devices that have a unique ID and each person should have one of these devices that is different from the rest. The software form also, as the name suggests is a unique software program that give to the user and is different with other users software. (Nayeb and Sharifi, 1391).

2.2 System features

Software architecture:

OTP Tokens are not independent system and What they do is completed with other systems, in other words passwords that they are generated is checked by another system, called AA Server (Authentication, Authorization Server) or central authentication server. Overview of the software architecture of this system is shown in the following figure:

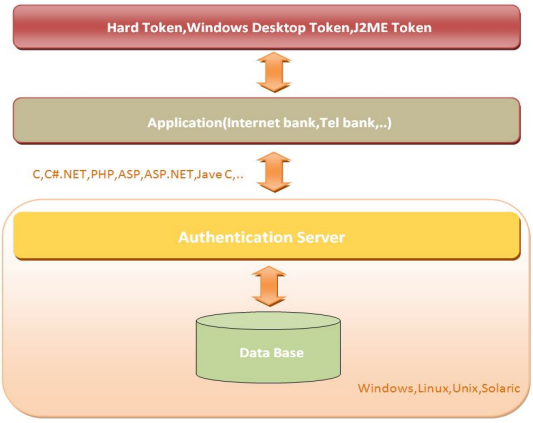

Figure 1: The software architecture(OTP Token System)

2.2.1 Authentication Server (AA Server) and its features:

AA server is a centralized authentication system that performs authentication of all users centralized. This system has the capability to communicate with other systems such as the Internet banking and could authenticate users of these systems. Thus, these systems may also transfer their user authentication to AA Server.

The overall structure of the system is as follows:

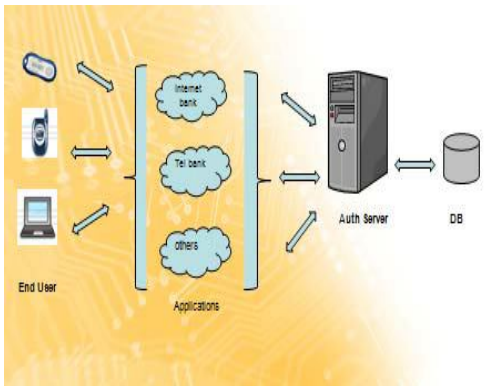

Figure 2: Central Authentication System(AA Server)

Authentication server capabilities includes the following:

1. User Authentication
2. Members Management
3. assigning OTP Token to the user
4. changing OTP Token settings
5. Synchronization of OTP Token with server

2.2.2 System Security

Because of using the password created by the user only once the other users logging to the system by previous password to steal information or access to the information is not possible.

2.3 Methods to produce OTP

Note that as we intended in this paper to control secure access to grid networks with workflow, user authentication and verification, we need mention production methods of OTP. As can be seen in Figure 3, to generate OTP the following methods performed:

Scratch List: The easiest mode of OTP that the list of codes is given in the paper to the client that the server is informed of these codes and client use those codes either in order or with index.
Short Time: In this method, the server and client are shared with one or more passwords and disposable code produced with the help of this code and the current time. The main problem is that in this method server and the client should be synchronized with each other. It should be noted that the procedure is similar to Token.
Challenge / Response: This method improves the previous method in which instead of using time, a unique number generated by the server (Challenge) is used [11][12].

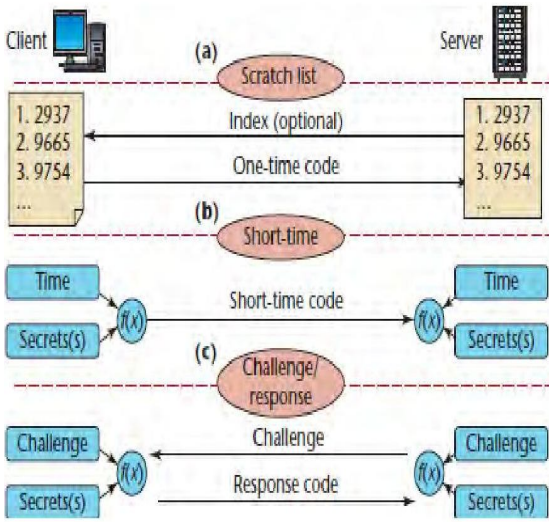

Figure 3: Authentication methods[12]

Here, we use Challenge / Response and Hash Algorithm to generate the OTP or one-time password. In the authentication process there is only one value that its sameness is to be checked between the two systems, so we use one-way encryption algorithm of Hash.
All of these algorithms are one-way, so main information could not be obtained from the original data source after coding of information and it could be decoded only if these codes are in hand [13].
The hash used primarily to ensure that both sides are using the same encryption key, without requiring the key to be exchanged between the two sides.
The most popular methods of Hashing are:
_Message Digest algorithm 5 (MD5)
_Secure Hash Algorithm (160 bits) (SHA_1)
_SHA_256
_SHA_384
_SHA_512

3. PROPOSED SOLUTION

In this paper, for authentication we use software type (software pattern) that is unique to produce disposable password. User register through the site or by entering his personal details and according to input data (unique) such as name, surname, date of birth, and ... and with using the SHA1 (based on [14] and [15]) password generated and stored in the database server. Using the Software Pattern has this advantage that any software can be used only for a single user. In this proposed method, user that need to enter grid network or use resources firstly enter in a workflow and with password that is produced by OTP security mechanism and Hash algorithm (Figure 4) checked by workflow or central authentication system and if confirmed by the identity authentication center, the user is allowed to enter to system and indirectly will access the desired data through a single server.

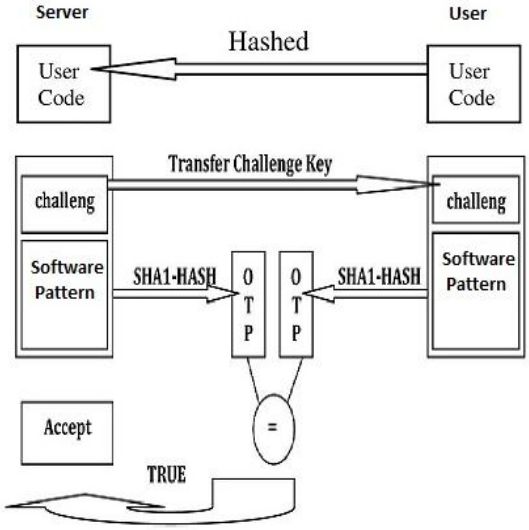

Figure 4: Production process & Authentication One-time password

In this method the user for receiving grid network services, or by introducing himself to the appropriate agency, after confirming the identity and authenticity of the user, a software pattern and a unique ID is assigned to the user. This ID has encrypted with Hash algorithms and provided to the user along with software pattern. For each network user login, user enters his ID code and receives a Challenge from server. By Challenge code and software pattern and with using the Hash, disposable password that is a symmetric disposable key is generated; This password is authenticated via workflow by AA Server that is a centralized authentication and if user authenticated he allowed to enter into grid network and user passed to server unit. Here the user passed his request to server unit and unit gives requested resources or data to the user. Thus access to grid network and resources is indirectly and through the central authentication system. This produce a secure channel to access resources and data and will increase the safety and efficiency of grid networks.

4. CONCLUSION

From above the results :
Authentication of user performed by OTP that is a disposable symmetric OTP and each entering to system is different from previous enters and leakage of it will not cause any breach in

the system. Grid network entry and access to resources takes place after authentication by authentication center. Using Hash algorithm to encrypt the password on OTP process, it has the added bonus that with leakage of it basic information could not be obtained. To fix it, simply change the hash function. These things results more complex grid network and resources access by intruders.

This method covers all the security services such as confidentiality, integrity, authentication and Non-repudiation and prevents any security threat. All above cases contribute to increasing safety and efficiency in the grid networks.

REFERENCES

1. I.foster "*Blueprint for a new computing infrastructure*" 2nded.sanfransisco: Morgan Kaufmann, 2004.
2. I.foster, C.Kesselman and S.tuecke,"*The anatomy of the grid: enabling scalable virtual organization*", international journal of high performance, vol.15, no3, pp 200-222, 2001.
3. AstroGrid,"Virtual Observatory Software for Astronomers", vol.2009, 2009.
4. NVO."National virtual observatory", vol.2009, 2009.
5. F.Wang, J.LVO, H.deng, B.liang, and K.Ji,"*C-SWF: A Lightweight Scientific Workflow System for Astronomical Data Processing*", in second international workshop on computer science and engineering Qingdao,2009,pp.64-67.
6. "*Grid computing security (A taxonomy)*", published by the Computer Society, 2007.
7. A.Bendahmane, M.Essaaidi, A.EIMoussaoui, A.Younes,"*Grid Computing Security mechanisms*", 2009.
8. Vserver,http://linux vserver.org/documentation,accessed on 13th July, 2006.
9. Enhancing Grid Security Using Workflows, Trusted Computing and VirtualizationAMD64 Virtualization Codenamed &Pacificate Technology, Secure Virtual Machine Architecture Refrence Manual Publication no.33047, Revision 300, Advanced Microdevices Inc.april 2005.
10. F. Aloul, S. Zahidi ,W. El-Hajj, "Two Factor
11. Authentication Using Mobile Phones" ,Proceedings OF IEEE International Conference on Mobile Technology, 2009.
12. M. AlZomai, A. Jøsang, A. McCullagh, E. Foo: "Strengthening SMS-Based Authentication through Usability", 2008 International Symposium on Parallel and Distributed Processing with Applications.
13. Thomas Weigold, Thorsten Kramp, and Michael Baentsch, "Remote Client Authentication", IEEE Security & Privacy journal Published by the IEEE Computer Society, 2008.
14. Gupta, Alok, " Digital signature: use and modification to achieve success in next generational e-business processes", February 2003.
15. N.R. Potlapally, S. Ravi, A. Raghunathan," Analyzing the energy consumption of security protocols", Princeton University, ACM Digital Library, 2003.
16. C. H. Gebotys," Low Energy Security Optimization in Embedded Cryptographic Systems", University of Waterloo, ACM Digital Library, 2004.