6th INTERNATIONAL
INFORMATION SECURITY & CRYPTOLOGY
CONFERENCE

ISCTurkey

6. ULUSLARARASI
BİLGİ GÜVENLİĞİ ve KRİPTOLOJİ
KONFERANSI

Security Challengers in Grid Operating Systems

Farhad Soleimanian Gharehchopogh, Neda Jabbari, and Nima Hojjati

Abstract—Vast nature of internet causes creation an environment "grid" for a developable system creation with high effectiveness, distributing and reliability. In a distributed system like grid, information safe transfer and duties services security guarantee is an important subject. Different architectures are proposed for creating security in grid that the most important one is a grid operating system (GOS). GOS is trying to create security in transferred information, shared resources by security module and security of each node in grid computational environment. In this paper, we describe a little about GOS and then, we review about security components in grid especially security in GOS.

Index Terms—Grid Operating System, Security, System, Distributed

I. INTRODUCTION

GRID term is proposed as a distributed computational infrastructure for developed science and engineering in 1990 [1]. Grid is a distributed computational infrastructure that causes more usage of computational resources by sharing a lot of heterogeneous resources in outspread geographical distances. Sharing and resource selection are based on their user accessibility, capacity, ability, cost and need to service quality [2]. Grid computational environment is a distributed computational infrastructure that support of virtual organizations creation and exploit with control mechanisms and polar organizational resource sharing [1]. Global registration center is a central storage that grid service creators maintain a database of resources are useful for users admission, recognizing them, dynamic services creation and representation [3]. Because, public operating systems are designed for using in personal level, they can reply to grid need level, so, middle wares came to this area. But, middle wares couldn't solve all problems that it caused creation of GOS. The main and primary idea of GOS came from Faster and et al. [4]. GOS can cause services presentation for sharing function ease in grid environment. In this paper, firstly, we review grid component in section 2 and we continue speaking about security in grid and GOS in section 3.

Farhad Soleimanian Gharehchopogh is with the Department of Computer Engineering, Urmia Branch, Islamic Azad University, Iran (corresponding author to provide phone: 00989141764427 and 00905544040942; e-mail: bonab.farhad@gmail.com).

Neda Jabbari is with the Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran (e-mail: nedajabbari.nj@gmail.com).

Nima Hojjati is with the Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran (e-mail: n.hojjati@gmail.com).

II. GRID OPERATING SYSTEM

A. Grid Networks

In the last of 1990s, grid computational networks are created as proposed supersede for common super computers to solve problems that need a lot of computations and high content of data and relations. Grid computing by using internet creates use of other system's hardware resources. Use up resource in grid computing, contain huge computers, storage systems which are virtual organizations data resources with different politics that use by scientific, engineering and other computations in a large scale [5]. Virtual organization is a set of distributed resources that searches resources need for users and also share their resources. Although, it is more than a decade that grid is created but because of it doesn't present its acceptable solutions, couldn't find his situation in global area. In recent years, grid middle ware [6, 7] is emerged for more and simpler usage from grid software infrastructure such as, Globus [9], Legion [8], Condor [10] and UNICORE [11] that a lot of distributed computational problems use these tools with good base for writing application and focus on develop grid environment and computational resources but because of that grid developing by grid middle ware need more software layers, so, they aren't safe for information transfer [14]. For representing a safe distributed control, with satiability and high quality of services based on flexibility, nodes heterogeneous in grid cause problem in grid. For aiming to these goals, grid middle ware is classified to these components:

- Middle ware base
- Identity system and justification
- Job management and schedulers
- Data management
- Unblock management
- Information systems

Grid doesn't have any limitation in subject geographical area and also contains heterogeneous resources but it unblock because of transparent in distributed systems from user view. It is used of current computers without additional costs and can include a lot of cluster in geographical areas. Computational resources have big peace of resources that include processors and their relations. In this regard, data resource can be a memory of a processor or secondary memory for saving processed data in grid.

B. Grid Operating System

GOS is proposing for supporting local resource efficient management or grid environment remote resources for a system that is connected with this environment [17]. Grid base operating system play virtual machine role as a layered

6th INTERNATIONAL
INFORMATION SECURITY & CRYPTOLOGY
CONFERENCE

ISCTurkey

6. ULUSLARARASI
BİLGİ GÜVENLİĞİ ve KRİPTOLOJİ
KONFERANSI

interface in grid environment that the most important role of this interface is information safe transferring between connected nodes to grid and it has dynamic resources. In [17], a GOS should contain:

- Creation a simple connection in grid, endurable error in nodes, giving justification for survey applications
- Proposing a platform for user access to grid resources and transparent distributed resources, process access proposition to all resources and resources that are shared between resource and process
- Policies appointment to create local resource in grid
- High efficiency and high accessibility
- High scalability, dynamic system further configuration, omission and adding node and transparent for applications.

Some GOS are same with public operating system in personal computers such as modularity that is one of the important rules in GOS, having politics dispassionate and free mechanisms, having universality in infrastructure for better programs and software's implementation, having low changes in operating system core [5]. GOS project is a GOS that support grid middle ware infrastructure. In [3], GOS made of these components:

GOS Core: In [19], GOS core has very low content and it is so soft that contains all services that are in high layer. Indeed, core is an interface between local operating systems users and grid computational environment. Keeping of core creates a security infrastructure for grid computations that can simply influence by users. Although service developing base on their unblock structure is hard but GOS addressing these problems by preparing a modularity architecture that needs a little changes in core [5].

Resource Management: Operating system uses from resource management modules for proposing related services that contain these components: resource registration, resource search, resource scheduler and devotion, error tolerance and services provider.

Node Description and Using of Resources: Nodes in grid is selected by that node efficiency. The use nodes resources maintains for computing for account of a node separately.

Grid Security: we can arise grid security by two methods: firstly, use of justifications admission before users inter to grid global environment. Secondly, it's done by GOS by using manual control that includes node admission and users identity.

Network Management: Traffic in grid computations makes it better controllable for services better representing by network management. The architecture [5] that is proposed for GOS includes three main parts that each of them has more pieces:

- Grid applications
- Grid middle ware

There are several project for GOS like Vigne [10], XtreemOS [20] and Apple xgrid [21]. XtreemOS is based on Linux and purpose of it is a distributed physical resource underside layer abstract liaison in an open source grid environment [22]. This GOS proposes

a set of system services and developing of them in Linux old version for users that we can use all of grid availability. Vigne is a GOS that its purpose is programmers and users escape from shared resources and removing grid computational resources [23]. Apple XGrid is a part of Apple Mac OSX that let an organization to create grid componental or cluster computational.

III. SECURITY IN GRID-BASE OS

For network manager, one of the most important activities is network resources security guarantee. Illegal access to network resource or intentional and unintentional information blemish make network unsafe. This topic in grid network has more importance because of its distributed structure. Grid security infrastructure and its related application software need security module like identity recognizing, access control, unblock independence and lake of denial efficiency. In grid computing for establish security should be a powerful infrastructure in low levels. Security architecture in grid should be useful, developable and unblock. Security in grid is for three groups of grid environment parts:

- A nod of grid that gets present resources and uses it
- Virtual organization
- A user that gives his/her resources to other users

In [23], three main component of security are: privately, integrity and accessibility. In [24], firstly security grafts in grid are:

- **Identity preparation**: identity preparation means we give justification to users for activity that surveys all procedures that includes user computations and resources that use them and justifies their safety [14]. Identity preparation gives this confidence that corporative entity is free. This entity can be a person, tool, service or installed application in network. The user allows ability means user can receive services from network.

- **Single sign on**: for orchestrate different resources that do a single job in grid computational environment, this security module used for identity preparation high suppression in such systems [19]. Indeed, user gets his/her first enter from admission justification module and after that he/she can enter without additional surveys.

- **Credential span and renewal**: different activities in grid componental environment have different longevity and running time and as lots of activities longevity isn't given at the start of the process, so, if they didn't end after a period of time their run time should be extended. Thus, these activity attendance authorities extend in system means risk reduces in identity preparation and single sign-on [1].

- **Justification**: justification is like identity preparation. At first, a user needs justification for access to services in grid. In grid, justification politics should have these forms: both of service

6th INTERNATIONAL
INFORMATION SECURITY & CRYPTOLOGY
CONFERENCE

ISC turkey

6. ULUSLARARASI
BİLGİ GÜVENLİĞİ ve KRİPTOLOJİ
KONFERANSI

receiver and service sender should export justification.

- **Representation:** Virtual organizations effective function in grid componental environment that are grid services infrastructure is based on trust. For create and manage this trust it needs a representation that has needed justification for survey services from a node to another one and setback their imports to each other's procedures. This deputation is needed for dynamic and static service creation warranty [1, 22].

- **Private sanctum preservation**: in Private sanctum preservation, both of service requester and service replier should require justifications for personal sanctum preservation politics appointment and implementation [17].

- **Privacy**: for maintaining privacy in grid, we need a safe transmission and also message safe encryption and decryption in return way on grid end point [23, 24].

- **Message Integrity**: It guarantees that if a message or a document is changed illegally. It will be recognizing in [18].

- **Exchange Policy**: related policies to service providers and service receivers are for safety from exchange and the change of identity preparation qualification, limitations and ability and security maintain rules support.

- **Secure entry to system**: entry to system should be done safety, as this entry uses in computation so it should be include an entry to secure system by any type of functional information or procedure.

- **Confidence**: It means that require conditions is proposed for security level from a web host environment by each node that include security actions running mechanisms and usage policy of them such as keeping via virus, using of firewall for accessing to internet and use of virtual private network [10, 24].

- **Management**: to have security in grid we need a management that this management contains high level of requirements like antivirus, dominance recognizing and prevention.

- **Firewall**: we can use firewall in grid for security creation without used local control in firewall politics. Access control and identity proportion have a relation between themselves and we can make it that people could access to network services by access level identifying and have some ability such as data repairing and changing, position removing and changing and data storage way. Indeed, access control specifies that who can use some types of services. Lack of denial is preventing and keeping nodes in a service representation relationship compare of other current nodes [24]. To have a safety grid, we should have a safety virtual organization. So, grid security should create a safety virtual organization. Virtual organization has life cycle [23]: recognition, formulization,

function, completion and destroy. Now, to have a secure virtual organization, security should be in every point. For users and resource better control in grid network, GOS created a dynamic virtual machine and maintained security of computational resources by virtual machine [17].

In [24], security in GOS can establish in three levels: grid level, grid application and host grid:

- **Grid level**: contains set of joint nodes that main topics on it are needed resource finding, trust of free node access and prohibition of other nodes accessing to that resource. In this level, for creating require safety, identity proportion should be active in each grid node, thus, free node access is successful and illegal node access is unsuccessful. A grid network is formed of connected nodes to this network that security establishes for a node is so important on it. Users let other nodes to access to their resources by connecting to grid network but, this access can be dangerous and reduce security of service providers and even service providers. Therefore, one of the security problems in GOS is creating security in each node. In grid, a node should be accessible completely or not (all or nothing) [17]. This means that when a node is prepared to survey services for one of the members, another node couldn't use that node services.

- **Application level**: this level includes all nodes that implement a part of grid-base program. If a node GOS procedure has a connection with another node GOS procedure, it should be establishment by service provider and receiver public application. In application level prevents intractable relations creation between nodes and these relations should be accessible by current relation liaison to avoid repugnance among similar nodes. For preventing security in this level we should stop illegal user's intervention in program management. Thus, grid network manager should exports access limitations and justifications for creating safety in this important level.

- **Host level:** for preventing information privacy and unblocking, information security should be in servers.

For creating exchanged information security among service provider and receiver in grid network, GOS stores information in secret and unblock forms and for creating these two needs, it surveys user justifications in grid level.

One of the basic topics in each operating system to create security is having every service justification for users that GOS has it and is one of the most important security creation components. Indeed, users can use of protected resources that have required justification in operating system from resource manager. For example, XtreemOS needs information storage privacy and unblock for having a justification [22]. These represented in XtreemOS GOS [19].

Main security components for XtreemOS are:

- **Privacy**: It represented by ISO (International Standard Organization). Privacy is one of the basic topics in security.
- **Unblocking:** unblocking guarantees that in data transferring, exchanged information are valid and complete. For example, when we want have a copy from a sensitive and important document; information valid and complete transfer is very important, because there is information change probability in transfer.
- **Availability:** availability points to information using ability. Security concept in availability relates to this topic that maybe a person denial access to data or a specific service intentional that is free for users.

GOS implements access control for each node require justification trust attaining for service receive or represent. Single sign-on is another security creator components that it creation, users should have particular and valid identity.

Installed GOS in each system can enter to global grid and use its services after identity acknowledgment that it's arise users safety. Indeed, users should use of GOS permissive copies and updated for arising security coefficient.

IV. RESULTS AND FUTURE WORKS

GOS is in lower level of host operating system, consequently, security component control done near user that it cause represent higher level in security by flexibility creation in grid services. Grid computational environment is a platform for users benefit from other nodes resources in needed time but this array or service receive not only can transfer unsecure information, also can be dangerous for nodes shared resource. So, it is important to have a powerful and safe infrastructure for data transferring. If a user doesn't have trust to grid computational environment, it wouldn't represent its resource and also wouldn't use other resources. We should have a GOS to attain a safe platform in grid that has a light core but with its specific security module. In this paper, we survey researcher's proposed needed security modules, although, we should survey more a lot of security hole that are in GOS.

REFERENCES

[1] I. Foster, C. Kesselman, The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufman Publishers, 2nd edition, 2004.
[2] A. Iamnitchi, D. Talia, P2P Computing and Interaction with Grids, Future Generation Computer Systems, North-Holland, Vol. 21, No.3, pp. 331-332, 2005
[3] S. Ahmed, P. Mahmood, Architecture for Grid Enhanced Operating System, International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, 2007.
[4] I. Foster, C. Kesselman, Steven Tuecke, The Anatomy of the Grid Enabling Scalable Virtual Organizations, International Journal Supercomputer Applications, 2001.
[5] T.M. Pinkston, V.K. Prasanna, GridOS: Operating System Services for Grid Architectures, HiPC 2003, LNCS2913, pp. 353–362, Springer-Verlag, Berlin Heidelberg, 2003.
[6] E. Laure, Middle Ware for the Next Generation Grid Infrastructure, Proceedings of the Computing in High Energy Physics Conference, pp. 826, 2004.
[7] I. Foster, C. Kesselman., Globus: A Meta-Computing Infra-structure Toolkit, Intl J. Supercomputer Applications, Vol. 11, No. 2, pp.115-128, 1997.
[8] V. Huber, UNICORE: A Grid Computing Environment for Distributed and Parallel Computing, Lecture Notes in Computer Science, pp.258–266, 2001.
[9] G. Shaw, A.S. Wulf, The legion Vision of a Worldwide Virtual Computer, Communications of the ACM, Vol. 40, pp. 39-45, 1997.
[10] B. Gleeson, A. Lin, J. Heinanen, T Finland, G. Armitage, A. Malis, IP based Virtual Private Networks, Technical report, Internet Engineering Task Force, 1975.
[11] B. Aziz, A. Arenas, J. Bicarregui, B. Matthews, E. Yang, A Formal Security Requirements Model for a Grid-based Operating System, STFC e-Science Centre, Rutherford Appleton Laboratory, UK Available at: www.e-science.stfc.ac.uk, Last Access: 2013.5.15.
[12] B. Mathews, "Towards a Knowledge Grid: Requirements for a Grid OS to support Next Generation Grids",Core Grid Work- shop on NGN, Belgium, 2005
[13] The Globus Project, Introduction to Grid Computing, Argonne National Laboratory, 2002.
[14] S.Puri,Q.Abbas," Grid Operating System: Making Dynamic Virtual Services in Organizations" International Journal of Computer Theory and engineering, Vol. 2, No. 1 February, 2010.
[15] Burke, S. Campana, S. Lorenzo, P.M. Nater, C. Santinelli, R. Sciaba, A: User Guide, Members of the EGEE-II Collaboration, April 2008.
[16] XtreemOS, Integrated Project, Security Requirements for a Grid-based OS.
[17] Karen Kent Frederick. Ronald W. Ritchey Stephen Northcutt. Lenny Zeltser. Scott winters. INSIDE - Network Perimeter Security. New-Riders, 2003
[18] I. Foster, C, Kesselman. G. Tsudik, S. Tuecke, A Security Architecture for Computational Grids Technical Report, The Globus Alliance, 1998.
[19] J. Belass, Measuring security in a Grid Computing Environment, Master's Thesis, Department of Computer Science and Media Technology, University College, 2005.
[20] S. William, Cryptography and Network Security Principles and Practices, Fourth Edition, 2005.
[21] V. Welch, J. Novotny, S. Tuecke. An Online Credential Repository for the Grid: My Proxy, Technical Report, The Globus Alliance http://www.globus.org, 2001.
[22] M. Adamski. M. Chmielewski, S. Fonrobert, A. Gowdiak, B. Lewandowski. J. Nabrzyski, T. Ostwald, J. Pukacki, Technical report, Available at: http://www.gridlab.org, Last Access: 2013.5.14.
[23] E. Jeanvoine, Using Overlay Networks to Build Operating System Services for Large Scale Grids, The Fifth International Symposium on Parallel and Distributed Computing, pp. 191–198, 2006.
[24] C. Morin, XtreemOS: A Grid Operating System Making Your Computer Ready for Participating in Virtual Organizations", 10th IEEE International Symposium on Object/component/service-Oriented Real-time Distributed Computing (ISORC), 2007.