EasyChair Preprint

№ 706

Research on security communication and access control of grid service

Yu-Bo Wang, Cai-Sen Chen, Xi-Ren Wang, Xiang-Liang Ma and Lei-Ze Xue

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

December 29, 2018

Research on security communication and access control of grid service

Yu-Bo Wang[1], Cai-Sen Chen[2*],Xi-Ren Wang[1] Xiang-liang Ma[3] Lei-Ze Xue[4]

[1] Teaching and Research Support Center, Army Academy of Armored Forces, Beijing 100072, China.

355094556@qq.com,1418116241@qq.com

[2] Military Exercise and Training Center, Army Academy of Armored Forces, Beijing 100072, China.

caisenchen@163.com,

[3] Institute of Software, Chinese Academy of Sciences, Beijing 100049, China

maxiangliang@163.com

[4] 66184 Armed Forces, HeBei 071000, China

270963268@qq.com

Abstract. With the development of science and technology, grid technology has played an increasingly important role in people's lives. Grid technologies prospects has also been given great expectations. However, due to the platform of grid feature relies the Internet and its characteristics in use will encounter a range of security issues, and as an emerging technology, it also will face a variety of challenges, so the research of the problems of grid security communication becomes practical significance. In this article, it will be focused on security communication of grid services and grid access control, and put forward the own points idea.

Keywords: Grid technologies, Security Communications, Access control, grid services

1 Introduction

1.1 Research purpose and research significance

The computer is hailed as the greatest invention of the 20th century, and then humans have fully utilized their ingenuity and constantly improved computer technology. Today, people use a variety of services provided by Internet resources and networks to meet their diverse needs.

Generally speaking, the grid uses the Internet to connect a wide variety of resources (including computing resources, storage resources, bandwidth resources, software resources, data resources, information resources, knowledge resources, etc.) into a logical whole. Just like a supercomputer, providing users with integrated information and application services (computing, storage, access, etc.),

[*] Corresponding Author

the virtual organization finally realizes resource sharing and collaborative work in this virtual environment, completely eliminating resources "islands", most Fully achieve information sharing. The whole network is like a super huge computer. On this super huge computer, all the integrated resources are fully shared.

Some people have compared the grid to the "power grid". In contrast, the power station bears the role of the power resource provider, while the provider of the grid resource is the computer, and the consumer is our vast number of users. Like the power grid, the coverage of the grid is very wide, but although users share their resources for the sake of their own interests, they sometimes cannot trust the security of such resource sharing. For example, confidentiality of communication, integrity of resources, privacy of information of users, and the like. On the other hand, grid is an emerging technology after the Internet and the Web. Based on the current research results, grid computing is considered to be a solution to the grid problem. However, because the grid is based on the Internet, and the Internet is an open information platform, it is vulnerable to threats from outside. I believe that computer viruses such as "hackers" and "panda burning incense" are no strangers. Security issues have also become severe. Therefore, it is very important to study the grid communication security communication problem.

There are many factors that affect grid security, including identity authentication, trust relationships, and access control. The traditional approach to grid security is to establish a single user identity authentication strategy. Most organizations today deploy network firewalls around their computer networks to protect their critical data. But this single measure has its own huge information limitations. We are waiting for improvement. The access control mechanism is a line of defense against grid security based on identity authentication. By establishing certain rules to restrict user access to resources, security issues can be controlled. How to make good use of access control technology to reduce the risk of grid service security communication, so as to better improve the security performance of grid services. Research on this issue has become practical.

1.2 Status of Grid Security Research

As mentioned earlier, grid users cannot trust the grid environment. Therefore, the purpose of grid security implementation is to make the resources of grid integration, and the feasibility of grid users in the grid environment. At present, the research on grid security is mainly focused on security architecture. Includes GSI for the Globus project and OGSA-based grid security architecture. On the other hand, the security level of the grid environment is improved by means of security authentication, access control, data integrity, communication confidentiality, and single sign-on. Based on the traditional grid security architecture, this paper proposes some techniques to improve security communication. Based on the access control and trust mechanism, an access control model is established. Thereby to strengthen the strength of grid security communication.

2 Grid security communication and access control research

2.1 Understanding of Grid Security Communication

2.1.1 Grid definition and its characteristics

In general, we understand that grid is a process of integrating resources based on the Internet platform to enable users to share resources. As mentioned above, the grid is an integrated computing and resource environment that, after fully absorbing various computing resources, transforms them into a ubiquitous, reliable, standard, and economical computing power. . Ian Foster described the grid definition in "Mesh Profiling". Based on the definition of grid, grid computing is proposed. It is pointed out that the most concerned issue of grid computing is the coordination of resource sharing and collaborative problem solving in the virtual organization of multi-agency. Generally speaking, the grid contains three basic functional elements: task management, task scheduling, and resource management. The three basic functional elements are simply that the grid user submits the task resources to the grid, and then the grid technology performs scheduling management on the submitted task resources, and determines and monitors the running status of the grid resource environment. From the definition and composition of the grid, we can easily derive the first feature of the grid: resource sharing. In addition to the resource sharing in the conceptual sense, resources such as large databases distributed on the network and visualization devices can also be shared. At present, this advantage has been fully demonstrated in the industrial, scientific, and mechanical fields, such as resource agency resources and collaborative problem solving. Of course, for security reasons, the premise of such resource sharing must be based on the sharing of high-level control. The second characteristic of the grid is the distribution and dynamics. Distribution refers to a wide distribution of grids and a wide range of integrated resources. Dynamic characteristics are the higher requirements for automatic migration of grid implementation tasks. Enables grid users to respond to changing dynamic resources and functions in the grid as they use resources. Secondly, the characteristics of the grid also include system diversity. This is because the grid relies on the Internet platform to integrate various network resources, and each computer and resource's own architecture and operating system and application software have different structures. . In this way, the interconnection of communication and interoperability between different structures and different resources determines the diversity of the system of the grid. The characteristics of the grid are far from the same, including the characteristics of autonomy and multi-client-oriented, which are mainly based on different standards

2.1.2 Encryption Technology and Security Protocol

Grid security issues are much larger than network security issues. This is also determined by the nature of the grid. In general, the grid needs to perform access authorization, user single sign-on, identity authentication, auditing, intrusion detection, data confidentiality and integrity checking and other security steps. Encryption techniques are often used in these processes. Simply put, information is replaced with secret symbols. In this way, security communication in the grid service can be guaranteed, the confidentiality of the privacy of the grid user is guaranteed, and the resource integrity is not destroyed. At present, there are mainly private key cryptosystems, public key cryptosystems and hybrid cryptosystems. The first two types are distinguished according to different working principles, that is, whether different keys are used in the process of encryption and decryption, and the same key is used for encryption and decryption of the private key cryptosystem. Under this system, both of the transactions: that is, the sender and the receiver of the message must exchange keys through a security channel in advance, so as to ensure that the two have a common key in the exchange, and the latter is the opposite. The encryption key is publicly available, and the decryption key can be accessed securely.

The hybrid cryptosystem combines the first two encryption systems for operational processing. The security protocol can also be considered as a key exchange protocol, ie two entities wishing to establish a security channel should use some kind of authentication protocol, which has the task of establishing a key. Including authentication protocols, key exchange protocols, authentication and key exchange protocols. In the information network, security measures can be taken at any level of the ISO seven-layer protocol. Such as encryption and authentication at the transport layer, encryption and authentication at the network layer, etc., but the security protocols adopted by each layer are different. The common IPSec protocol serves the network encryption layer, while the SSL protocol is used. Transport layer.

2.1.3 Grid security communication requirements and threats

Since the grid environment is an open platform, and the potential exposure risks arising from the output and use of resources, it has become a problem that we need to solve in grid security communication. The basic element of grid security is to maintain data integrity and Confidentiality. A security mechanism must be established in this process to organize unauthorized access. The non-repudiation of grid security is used as evidence to prove that grid users have performed or manipulated a specific task. This will help to resolve the dispute well in the future. Relying on the characteristics of these components of grid security, it can be seen that grid requirements mainly include the following aspects. The first is the authentication problem, which provides access points for multiple authentication authorities. This access point is unknown to any type of access mechanism. The second one is the single sign-on problem. He actually solves the problem that the grid user can obtain resources and use resources after performing identity authentication with the resource manager, but does not need to be in the subsequent shared resources. Perform secondary authentication. The third is the problem of proxy and authorization in grid security. The agent should be based on the principle of minimizing the rights of the agent, and at the same time strictly control the agent's authorized subject and give the life cycle. Authorization is to determine under what conditions the service can be accessed and who decides which access. In addition, the confidentiality of communications, message integrity, policy exchange, exportability, and unified credentials are all areas of security communication requirements.

Ensuring that each resource's visitors to each of the grids are authenticated is a challenge to our grid security. As I said above, in practical applications, the integrity and confidentiality of communication should also be considered. For virtual organizations (VOs), it is possible to share the traditional available resources among all members, and must rely on a dual trust relationship between local users and their organizations and between VOs and users. . But we cannot assume this trust relationship. In addition, there are still many potential dangers in grid security, which will not be repeated here.

2.2 Grid access control research

2.2.1 Overview of Grid Access Control

The grid access mechanism is also called authorization. The simple one is to authorize the information access of legitimate users and information service requests. User access to a resource will be controlled by rules set by the access control mechanism. Access violations of the rule will not be allowed.

2.2.2 The main mode of access control and its existing problems

At present, there are three modes of access control: First, the first mode is the autonomous access control mode (DAC). This mode is based on the agent mentioned in the discussion of grid security requirements. This mode is also called resource proxy resource. That is: the principal can autonomously grant a subset of access rights to other principals. At present, the methods implemented are mainly based on row and column-based autonomous access control [1]. However, due to the flexibility of autonomous access control, it is said that in the process of information transmission, real security cannot be guaranteed. Because in the actual operation, once the user owner passes the access right to the user who does not have access rights, the user who does not have the access right of a certain resource can access the resource through the autonomous access control, which obviously brings about A big security risk. Secondly, the second mode enforces access control (MAC). It is a hierarchical mandatory control mechanism to achieve information shunting. Under the mandatory access control mechanism, when a process accesses a file, access can be allowed only when the security attribute of the object matches the security attribute of the process. One of the obvious features of this access control is to ensure communication security by granting a corresponding security certificate to each subject in the system. However, there is a rule in this mechanism that does not read or write, and the direction of information flow can only be from low security level to high security level . Therefore, its scope of application is limited, and some departments that require a high level of security cannot adopt this mechanism. Finally, role-based access control is currently the popular security access control method. He is also a form of mandatory access control, but unlike the mandatory access control described above, he is not based on multi-level security requirements. He completes the granting and cancellation of user rights by assigning and canceling roles. And provide role assignment rules. Under this rule, access rights are tied to roles, and roles are associated with users. This is a good solution to the DAC problem, objectively separating users from access rights.

3 Some ideas on grid security communication and control research

3.1 Establish a grid security authentication model

The first is the establishment and management of the trust model. Grid users, applications, and resources should be established with a good trust relationship. Although the establishment of this trust relationship requires the cooperation of various participants, under the existing high-performance computer system, this security authentication mode still plays an important role. This includes user trust mechanisms and application trust mechanisms. The user trust mechanism is a trust based on identity relationship. The access authority of the resource is controlled by the system administrator. When the user identity reaches the set rule standard, the access permission is allowed. At this stage, the PKI user authentication method is used 3]. PKI is a security authentication technology that assigns accounts based on trust relationships and specifies access resources. This mechanism can well cope with the shortcomings of dynamic, temporary, and uncertainties of trust. The application trust mechanism is a requirement for system administrators.

3.2 Support single sign-on

Single sign-on support Virtual organization members only need to verify identity once to use the various resources of the grid computing environment. This advantage should be fully utilized. This requires a space to save user login information. This will provide a strong proof that you will not be able to log in here. We know that members of a virtual organization have the right to access multiple administrative domain resources, but the legal identity and role requirements of the resources within the administrative domain are different. The simple single sign-on feature determines that members cannot use the latter-scoped identity to authenticate each time.

3.3 Establishing an Access Control Service for Virtual Organizations

Traditional GSI has some shortcomings in the access control mechanism in the grid environment. This lack of response depends on the entire resource server for each account that the user requests to access the resource. This limits the permissions of grid users to access resources. In response to these shortcomings, it is necessary to establish a virtual organization (VO), which is a collection of certain entities in some organizations that have some common characteristics, and they have a consistent pattern when sharing and using various resources. The management of traditional security policies cannot meet the needs of dynamics. The VO technology is compatible with security technologies in different regions, and users in the VO can dynamically create and revoke resources. And the members and resources in the virtual organization have their own rules to comply with, so that you don't have to rely on the whole organization for execution, you only need to decide for yourself. This will solve the shortcomings of traditional security strategies.

4. Conclusion

The continuous development of grid technology has made people realize the importance of grid architecture. The grid uses internet as the communication support platform, which makes grid operations face various security threats. Therefore, grid security research requires: support security communication between entities in the network environment, prevent subject counterfeiting and data leakage; support security across virtual enterprise boundaries, and avoid the use of centralized management security systems. In the future work, the following aspects should be strengthened: first, to strengthen the research on the fault-tolerant mechanism of the safety channel; second, to strengthen the research to prevent the repeated attack mechanism; third, to strengthen the prediction of the composite service access control.

5 Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments. This research was supported by the National Natural Science Foundation of China under Grant No. U1836101.

References

[1] Du Zhihui, Chen Wei, Liu Peng. Grid computing [M]. Beijing: Tsinghua University Press, 2002-11.

[2] Huang Daming, Li Guodong. Research on Grid Monitoring System [J]. Computer Science Research. 2003, 30 (9): 144-147, 151.

[3] Wang Qingrong. Research on Grid Security Architecture and Certificate Management Technology [D]. Lanzhou: Lanzhou University, 2005.

[4] Gao Hongqing. Grid-based distance learning research [D]. Changchun: Northeast Normal University, 2004.

[5] Li Wei, Xu Zhiwei, Bu Siying, Charlie. An Effective Resource Search Method in Grid Environment[J]. Journal of Computer Science. 2003, 26(11): 1546-1549.

[6] Wu Xiaonian. Research and implementation of key technologies for security authentication and access control of data grid [D]. Changsha: National University of Defense Technology, 2004

[7]Dawn. Research on access control mechanism in grid security interoperability [D]. Wuhan: Huazhong University of Science and Technology, 2007

[8]Zou Deqing.Grid security interoperability and its application research[J]. Chinese Journal of Computers, 2010, 33(3): 514-525