A New Research and Design for Grid Portal Security System

Alireza Souri

Department of Computer Engineering, East Azarbaijan Science and Research Branch, Islamic Azad University, Tabriz, Iran

Alireza.souri@iauasrb.ac.ir

ABSTRACT

Grid security problem is one of the core issue of grid portal only provides strong grid security system, grid portal can have continuous growth, just have a certain application value, can guarantee the grid users who use various resources and services safely which the grid provided. This paper first analyzes the grid portal security demand, and then design a grid portal security system, finally we research and design its realization technology based on the user login security, resource scheduling security, data transmission safety and data safety operation the four aspects.

KEYWORDS

Grid Portal Security, Node authentication, User Login, System structure

1. INTRODUCTION

Grid portal system has large quantities and dynamic variable process. Various resources need different authentication and authorization mechanism. The task execution by a large process component, and there are different communication mechanism, resource and user could belong to multiple organizations, grid belongs to distributed. The attributes which related to the user are managed by more than one organization space [1]. Grid portal safety feature described above illustrate it's the problem of security needs is very complex, so we should consider its security needs.

1.1 Basic Security Needs

Grid portal system security elements include: integrity, access control, privacy, identification, usability, non-repudiation.

Integrity is to ensure that the grid data cannot be inserted, malicious modifying and deleted etc. Access control is to control and restrict user's ability to access the grid resources. Confidentiality refers to protecting the grid data from attacking during the transmission process. Identification is that we identify authentication to the interactive objects of grid system, preventing personate making false services. Usability is to prevent the usability of grid portal to reduce and prevent other attacks.
1.2 Special Security Needs

The user group is huge and has an imperfect authentication. Grid portal resources and organization are large, to facilitate the huge number set of relation between the organization and account management, each user must have an identity. A local user identity and the grid portal identity, and user appointed the identity of the remote resources, which all to match, still need to building trust relationship, these are all very difficult.

Authorization mechanism is imperfect. Agent mechanism is without good scalability, too weak, it is difficult to support dispersive and the huge number of usem and service resources. Security mechanism is diversified. The grid enterprise each has different security mechanism. Each enterprise should make its resource adapted to grid environment, when the user access, security architecture should verify user data, and translated into the required form. Safety measures lack adaptability. Grid trusting relation is dynamic; it will also affect resource safety [2].

2. Grid Portal Safety Design

2.1. Grid Security Architecture Design

Through analysis and study of above security needs, this article designs the grid security architecture, and it is divided into four layers as Figure I shows:

![Grid security architecture diagram]

Figure 1. Grid security architecture

1. The bottom is a node safety autonomous management layer. Based on node security service in global identity authentication and global access control it provides node identity authentication
and access control services. Grid node access control strategy management can realize the independent authorization management to local resources.

2. Centralizing management platform security infrastructure layer that it includes security agreement, PKI certificate management, and grid trusting model management. Global strategy, especially access control strategy definition, exchange, management, etc. Related units in a grid management include grid users, roles, and organization and so on.

3. Centralized management platform for global security service layer. Based on grid global management security infrastructure layer, it provides several global security services, including the identity authentication services, access control services, audit service, etc.

4. Application-oriented security services entrance. Grid Security Services portal to accept service requests, call the security service, or application start agent service requests, and sometimes the grid need to make cross domain service requests.

Meanwhile, there’s a supporting environment in the GSec (Grid Security) architecture, the supporting environment in GSec whole hierarchy can be used as GSec technical support, including Internet / Intranet / Extranet network environment, GSec basic agreements (such as grid protocol, network protocols, etc.), standards and norms (such as the enterprise standard, national standard, international standards and norms, network and information security standards, grid standards and grid, etc), development platforms (such as GSI, Tomcat, etc.), providing basic operating environment for the realization of security service in GSec. 

Grid security system structure (Figure 1) features as follows:

1. using the node layer, base layer, service layer and application layer four-story structure, and rely on the existing platform, standards and norms as a support environment; the node layer realization services for local security management; global security services layer provides global security services, including authentication, the global authorization, etc; base layer to provide security for the security services infrastructure; application layer, requests for an interview; supporting environment provides a unified norms, standards and existing technology platforms.

2. Centralized, management and autonomous control: grid with a global centralized, management and local self-control security system framework. Grid service node after the service encapsulated, the service registers in the grid virtual domain and even the whole world grid in order to achieve shared. Grid management platform provide centralized management. Middleware of centralized management platforms provides task decomposition, workflow management and other services, besides it provides security services. Centralized management platform infrastructure provides third-party security intermediary, to achieve the certificate, strategy and organization and management, global security services to enhance authentication and access control. But the grid node can control the local shared services independently. Shared services require authorized by the local node before they can use [3].

3. Combination of professional and versatility: grid-based security architecture analysis of the characteristics of the grid, according to the security needs of the grid and provide new features or enhance existing security services. Based on universal grid security infrastructure, strengthen the professionalism of the field grid.

4. Comprehensive and comprehensive combination: to provide a full range of security, focus on improving and strengthening authentication and access control security services. According to the characteristics and needs of the grid, the grid security research focuses on basic authentication
and authorization services. Others, such as auditing, data encryption and so on, because there is no special needs, using the basic grid security technology.

2.2. User Login Security Design

Enterprises authorized provider permission to use the application service; grid security system must meet the "single sign-on (SSO)". Users login grid system, and see the authorized content. User need only once authentication in the initial login, access to and use of resources, and free resources, internal communication to the user without further authentication. The user's password, keys, etc. must be protected, requiring security measures to ensure that login is real suppliers, so requiring authentication and access control.

Figure 2 is user login authentication. In grid portal, in order to ensure user login security, requiring prior completion of application and issuance of identify documents in the authentication institutions CA. When the user login, based on digital certificate by SSL/TLS security agreement, completed identity authentication and making users have lawful access user login system.

![User entity certification and agent certification](image)

Grid portal identity authentication implementation process is based on authentication protocol, that different contexts match the different authentication process [4]. Through research, design their implementation process as Figure.3 shows.
The first step, determine authentication subject categories, authentication subject is users or nodes. If it is a node, it must provide node certificate to pass identify authentication. Node certificate for special occasions, such as signed an agreement can use such node certificate. The second step, determine the object of user access. If the object is node, then use the certificate authentication method. If the object is a centralized management platform, then search dynamic organization. If the user’s dynamic organization is running, state needed to further determine the user's access object security level.

The third step, according to the object security level to determine the identity of the user authentication method.

Figure. 3: Grid portal identity authentication execution
2.3. Research on Resource scheduling and security of data Transmission

Enterprise applies services through the Grid portal, the system schedule grid resources; complete a grid Service dynamically, in the process should ensure the resource scheduled safely. When apply grid services, firstly, register enterprises user identity in the certification authority CA achieve an identity certificate, and then in the registration system, the appropriate allocation of resources to the enterprise access, dynamic allocation of resource to complete security properties verification, so that resources scheduling process of the access control can be realized.

After enterprise applied the grid system service application, we need to use automatic data extraction synchronous and interface entry tool these two methods to transfer and saved data to the grid system, involved some of core data transmission from the enterprise to the grid, and should be transparent and secure storage to the appropriate resources in this series of processes require security measures. In order to solve these problems, you can use security protocol which is based on SSL/TLS in client or storage terminal , which work between the application layer, and transport layer, after certificated, provide a secure channel for data communications to ensure security of data transmission.

2.4. Data Safety Design

In the grid portal, customer data is stored on his computer, the client keep a part of the data, during the actual use, these data are combined together, it is necessary to ensure that client data cannot be used by other customers, therefore, requiring to solve data manipulation security problems. Response to these security issues, combined with the security needs of the grid portal, this paper to designed grid business process security scheme shown in Figure 4.

![Figure 4: Grid business process security scheme](image)

Figure 4 is the grid operation flow diagram, picture includes four entities.  
- Service terminal users: grid portal enterprise or individual;  
- Identity providers: management domain users of the system in;  
- Service provider :provides grid for data and business services;
After users login the grid portal, they will go to step-1 to access services. Access control center of service provider side will check if it's authenticated. If it is, turn to step 6 to access resources directly, if not return to the step-2 service discovery access, redirect users to discovery service providers, then step-3 is the certification redirection is to redirect the user to the identity providers SSO authentication services, after move to step-4, If certified it will submit to the service provider authentication assertion response. If the service provider requires more information, they can achieve through step-5 properties assertion request and response. When a user requests the service, since all data is managed through the encryption and decryption driven, so the user data is secure, which were to step-7 secure transmission of data.

3. CONCLUSIONS

This paper first analyzes the grid portal security demand, and then design a grid portal security system, finally we research and design its realization technology based on the user login security, resource scheduling security, data transmission safety and data safety operation the four aspects.

REFERENCES


Authors

Alireza Souri received his B.Sc. in Computer Engineering University College of Nabi Akram, Iran in 2011. Currently, he is receiving M.Sc. in Software Engineering from East Azarbaijan Science and Research Branch, Islamic Azad University in Iran. His main interest is in the formal verification, modeling and analyzing Network systems, Multilayer systems, Antivirus systems, Grid computing, and Real-time systems. He is member of The Society of Digital Information and Wireless Communications.