Secure access to grid information service using shibboleth and PERMIS

Secure Access to Grid Information Service Using Shibboleth and PERMIS

Wei Jie[#*1] Zhenghong Huang[#2] Michael Daw[*3] Rob Procter[*4]
Xiaorong Li[+5] Lianggui Tang[#6] Sheng Lu[#7]
[#]*Chongqing Technology and Business University, China*
{[2]hzh, [6]tlg, [7]lusheng}@ctbu.edu.cn
[*]*University of Manchester, UK*
{[1]wei.jie, [3]michael.daw, [4]rob.procter}@manchester.ac.uk
[+]*Institute of High Performance Computing, Singapore*
[5]lixr@ihpc.a-star.edu.sg

Abstract

Grid Information Service (GIS) is a core functional component of a Grid that provides information about various resources and their status. Security underpins a GIS making secure access to a GIS an important issue. On the basis of our existing work on a GIS architecture, we further propose a security framework which leverages Shibboleth as the authentication infrastructure and combines PERMIS authorization technology. As a result, this security framework integrates the advantages of both Shibboleth cross-domain identity federation and PERMIS policy driven role based access control, thus presenting a new security model for secure access to a GIS.

1. Introduction

A Grid is a distributed system that may contain numerous scattered domain sites that form Virtual Organizations (VOs) [1]. In Grid environments, users rely on a Grid Information Service (GIS) [2, 3] to provide information about various kinds of resources and their status. However, each participating domain site may wish to have ultimate control of its own resources, and may not want to disclose all information about resources to certain users. Therefore a GIS should incorporate proper security infrastructure and mechanisms to protect information access. Generally the security requirements for a GIS may include the following:

- Authentication – Authentication will take place before a user gains access to a GIS. That is, the GIS will check the identity of the user ensuring the user is allowed to query the GIS and retrieve information from it. A challenge that comes with user authentication is that some domain sites may wish to keep their own authentication systems, so the security infrastructure of a GIS needs to reconcile with existing authentication systems and make them interoperable.
- Authorization – The security infrastructure of a GIS should implement information access control mechanisms which reflect resource or information owners' privileges, and protect information by only allowing authorized accesses. Besides, the security infrastructure should provide resource or information owners flexibility to define their information access control policy (be it coarse-grain or fine grain policy), as well as modify or extend their current policy with ease.
- Independence – The security infrastructure and mechanisms incorporated into a GIS should not interfere with the GIS's own functionality, nor should the security procedures incur considerable overheads upon the performance of the GIS. On the other hand, it is expected that the security infrastructure could be integrated with a GIS in a seamless way.
- Scalability – The security infrastructure of a GIS should work well with the growing size of a GIS-monitored Grid, for example, with more users issuing queries to the GIS or more domain sites joining the Grid VO, the security infrastructure of a GIS should still be expected to perform well.
- Confidentiality – Information communication between a GIS and its clients must be carried out using encryption. Through some well-established

The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services(CEC-EEE 2007)
0-7695-2913-5/07 $25.00 © 2007 IEEE

cryptographic technologies like TLS [4] and MLS [5], confidentiality on GIS communication could be achieved.

- Manageability – The security infrastructure of a GIS may consist of many sub-components. The management of such a complex service (e.g. installation, deployment, etc) may incur a lot of administrative overheads. Some tools will be helpful in order to automate the management of the security infrastructure.

Among the above security requirements for a GIS, authentication and authorization are two of the most critical. There has been substantial work on authentication and authorization technologies in the context of Grid. A typical example is the GSI (Grid Security Infrastructure) [6] in the Globus Toolkit [7]. The GSI is a security framework in which authentication is performed using PKI based X.509 end-entity certificate [8]. A certificate asserts a user's identity which is expressed as a unique Distinguished Name (DN). The GSI also allows for the creation of delegated privileges by issuing proxy certificates [9] and brings added benefits of single sign-on over distinct domains. Whilst the GSI addresses user identity issues, obtaining X.509 certificates from a trusted Certification Authority (CA) can be a demanding job, especially for inexperienced users, requiring them to follow a detailed process for obtaining the certificates and converting them into appropriate formats before they are then able to access the Grid resources. There are also likely to be issues of scalability and flexibility with the expansion of Grid VOs, as it is unable to cope with dynamically changing users, along with management of their rights and permissions. In addition, it also raises privacy concerns due to the release of personal information for user authorization.

The GSI also provides a server-side authorization framework which evaluates a chain of authorization scheme, i.e., Policy Decision Points (PDPs) [10], in order to determine the access rights of a user making a request for Grid services. However, authorization in the GSI is by default based on Access Control Lists (ACLs) [3]. This approach provides very limited functionality and is inconvenient for large-scale Grid VOs as it lacks the necessary scalability and flexibility in describing Grid users' rights and privileges.

Other typical Grid authorization technologies include Community Authorization Service (CAS) [11] and the Virtual Organization Membership Service (VOMS) [12]. The central idea behind CAS is that while service providers can specify a coarse-grained policy, the fine-grained security policy decisions can be delegated to the administrator of the community that is served by the CAS. Particularly, the CAS will decide whether a user has sufficient privileges and give the user the right to perform the requested actions; the local service provider then applies its own local policy to determine the amount of access granted. The VOMS is a system for managing authorization data within Grid VOs. The VO administrator maintains a centralized database to add each VO user and give users appropriate attributes needed to access resources across the VO. However, these authorization infrastructures are based on centralized models and thus raise scalability issues.

In this work, we propose a security framework that is incorporated into our existing GIS architecture and aims to address the aforementioned security requirements. This security framework leverages the widely accepted Shibboleth [13] as the authentication infrastructure and combines PERMIS (PrivilEge and Role Management Infrastructure Standard) [14] authorization technology to provide scalable and flexible Grid VO-wide authentication as well as policy driven, role based, multi-grained authorization for access to and usage of the GIS. Before the discussion of the security framework for our GIS, we will briefly introduce Shibboleth and PERMIS technologies in order to better understand the security framework.

1.1. Shibboleth and PERMIS

Shibboleth is an architecture and open-source implementation for federated identity-based authentication and attribute-based authorization infrastructure based on the SAML (Security Assertion Markup Language) specification [15]. Federated identity allows for information about users in one security domain to be provided to other organizations in a common federation (a federation is a collection of domains that have agreed trust relationships to authenticate their respective users properly). Shibboleth basically defines a set of protocols for the passing of identity information and attributes between domains and service providers in a privacy-preserving way. However, how authentication is carried out by the domains and how access rights management is carried out by the service providers is left up to the respective parties. In other words, Shibboleth separates the user authentication that is performed by users' respective home domains, and the authorization that is performed by the service providers to be accessed based on users' attributes that have been passed to it.

The PERMIS is an authorization infrastructure that provides all the necessary facilities to manage user

privileges and authorization policies, and to make authorization decisions. The PERMIS is based on the Privilege Management Infrastructure (PMI) [16] which uses PKI principles of operation. Central to the PMI is the Attribute Certificates (ACs) [17] which maintain a binding between a user's unique identifier and one or more of privilege attributes. The PMI uses the ACs issued to a user as a basis to determine the access rights of the user. This is the central idea behind Role Based Access Control (RBAC) [14] – attributes / roles describe a user's rights and the target services will then read the user's AC to see if s/he is allowed to perform the action being requested. This de-couples the user's privileges from their local identity and allows a more dynamic and flexible approach to access control. The PERMIS uses XML policies which define the rules by which a service makes authorization decisions to the users.

The rest of the paper will focus on the security framework for the GIS. It starts with an introduction to background work of our GIS architecture. Then we discuss the architecture of the security framework, the Shibboleth-based authentication as well as the PERMIS based authorization. Finally we conclude the paper and outline the future work direction.

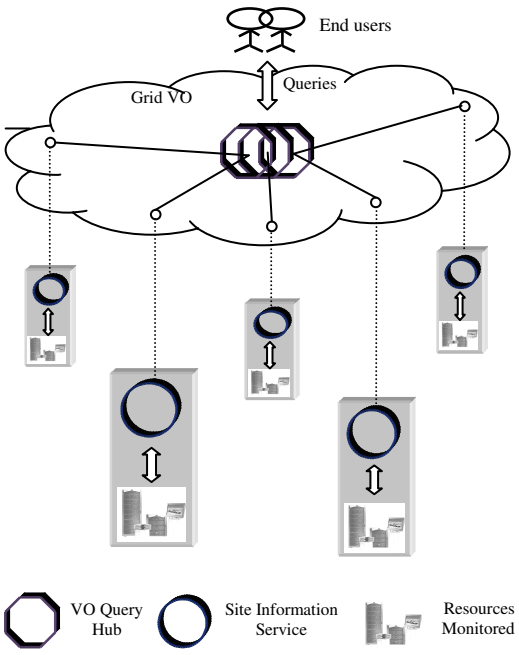

Figure 1. Overall architecture of the GIS

2. Security framework

In our earlier work [18], we presented an architectural model of GIS for large scale Grid VOs. The proposed GIS is an integrated Grid service that comprises of a set of components/services working at three different layers, i.e. resource layer, site layer, and VO layer (as illustrated in Figure 1). This hierarchical framework matches the structure of a Grid VO in a natural way, allowing efficient management of information at different levels of the Grid infrastructure. For the benefit of describing the security framework that is incorporated into the GIS architecture, the main function and features of each layer of the GIS can be summarized as follows:

- The resource layer is the underlying layer of the GIS, and physically it consists of all the resources being monitored in a Grid VO. The major components of the GIS at the resource layer are the Information Sensor and Information Agent. Information Sensors are our basic mechanism for capturing information about the resources being monitored. Information Sensors are runtime pluggable and can be integrated dynamically into the Information Service architecture. An Information Agent is a daemon running on each resource being monitored by the GIS. Each Information Agent invokes and monitors the Information Sensors deployed on the same resource to obtain up-to-date information about the resource being monitored.
- The site layer comprises a set of Site Information Services (SISs) each running in an administrative domain site that participates in a Grid VO. By talking to the underlying Information Agents, an SIS aggregates information on the resources being monitored in its domain. Meanwhile, the SIS maintains a data cache in order to reduce query response time and improve the throughput of queries. The SISs are implemented as WSRF-compliant [19] Web services.
- The VO layer has one or more VO Query Hubs that processes users' queries (we design a set of SQL-style query interface hiding the complexity of Grid from the end users and providing user-friendly access to resource information via the GIS). The VO Query Hub uses a Distributed Hash Table (DHT) based peer-to-peer approach to track the resource information within all the domain sites and redirects users' queries to appropriate SISs. The DHT is involved in the storing of the information classes of the resources being monitored as keys and the URIs of the SISs that contain the given

The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services(CEC-EEE 2007)
0-7695-2913-5/07 $25.00 © 2007 IEEE

information classes as values into the DHT nodes. This method enables us to efficiently manipulate a large amount of resource information distributed across multiple domain sites and brings the benefit of scalability and reliability.

We conducted a set of experiments to evaluate the performance of the GIS and the results indicate that the GIS presents satisfactory scalability in handling information for large scale Grids. In the following, we will discuss a security framework that enhances the GIS with security features, and is seamlessly incorporated into the current GIS without interfering with the functionality and architecture of the GIS. The core idea behind this security framework is that it integrates Shibboleth as the authentication infrastructure and PERMIS as the authorization infrastructure.

2.1. Security architecture

The security framework of the GIS integrates the identity federation and attribute assignment function of Shibboleth with the policy-based enforcement function offered by the PERMIS access control infrastructure to enable secure access to the GIS. Figure 2 illustrates the architecture of this security framework. In our scenario of GIS security, the following entities are involved in the security framework:

- *Users*: users are from the domain sites participating in a Grid VO, and they are the principal actors who access the GIS for information query through a GIS portal.
- *VO administrator*: a VO administrator has the privileges to manage the membership of a Grid VO by enrolling or removing domain sites.
- *Site administrator*: each domain site participating in the Grid VO has a site administrator. In terms of security management, a site administrator is responsible for creating authorization policies, specifying what roles have which privileges and what kind of ACs will be recognized by the PERMIS. The authorization policies will be used by the PERMIS for all reasoning regarding authorization to access the SIS.
- *Attribute manager*: each domain site has an attribute manager issuing attributes to users in that domain site, determining roles for users. Attributes will be managed in the form of Attribute Certificates. The certificates can be stored locally in an LDAP server [20].

With the security framework in place, any user who needs to access the GIS must go through the security enforcement – authentication first, followed by authorization. The general process for a user to access the GIS can be described as follows (as illustrated in Figure 2):

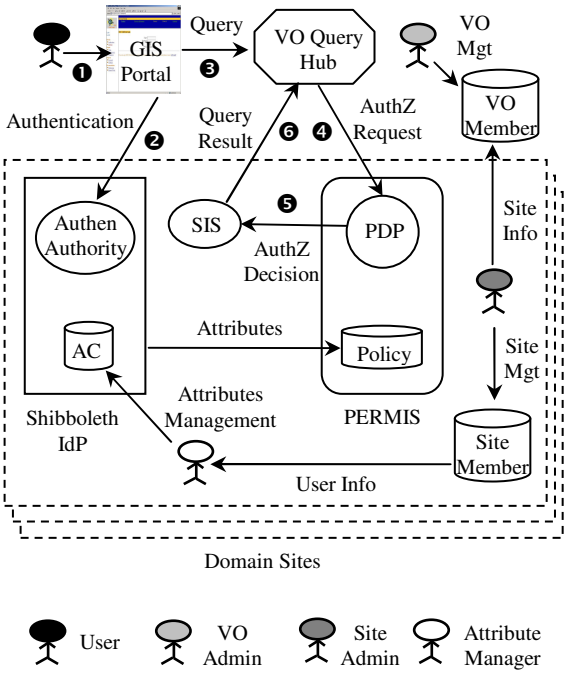

Figure 2. Architecture of the security framework of the GIS

(1) The user logs on to the GIS portal with his/her username/password registered at the authentication system of his/her domain site.
(2) The user is authenticated by his/her home domain site's IdP's authentication service as per the Shibboleth authentication model (the authentication process will be discussed later in Section 2.2).
(3) Once authentication is granted, the user can issue a query which will be handled by the VO Query Hub. The VO Query Hub will firstly check whether the query complies with the pre-defined query interface and then perform DHT operations. As a result, the query is only forwarded to the SISs that meet the criteria of the query.
(4) For each domain site that receives the query, before its SIS is invoked, an authorization request to access the SIS is passed to the PERMIS based authorization system.
(5) The PERMIS based authorization system will make decisions on whether the user has the rights to access the SISs. The decisions are based on the authorization policies written by the site

administrator (the authorization process will be discussed later in Section 2.3).

(6) If access is granted, the SIS will process the user's query and return the results to the VO Query Hub. Then the VO Query Hub merges the results returned from all the SISs and finally sends this back to the user.

This security architecture provides benefits to the security management of the GIS. First, since Shibboleth utilizes local login information of the domain sites, it allows for cross-domain single sign-on to the GIS and removes the need for a GIS to maintain a centralized authentication system to store usernames and passwords. This brings more flexibility for user authentication. It also makes the security system of the GIS easily scalable with a larger-scale Grid VO. Second, domain sites can establish their own trust federations and define their own policies on user attribute release. Most importantly, without the need for a centralized authorization system for the GIS, site administrators have the freedom to define their own authorization policy and decide upon what attributes and attribute values are needed for authorization decision to access the SISs. It also makes authorization management more flexible over the traditional approach of using users and group identifiers.

In the following sections we will discuss the Shibboleth-based authentication and the PERMIS based authorization in detail to elaborate the benefits offered by the security framework.

2.2. Authentication via Shibboleth

The first step in the user to the GIS security flow is user authentication. We now discuss the issues involved in the Shibboleth-based user authentication within the security framework, in particular, the authentication model, user attribute management, as well as VO and site membership management.

2.2.1. Authentication model. The adoption of Shibboleth technology in our GIS security framework requires that each domain site in a Grid VO has its own authentication system. To achieve seamless integration of these separate authentication systems, an IdP component of the Shibboleth is deployed in each domain site. The IdP creates and manages user identities and supplies user information. In addition, a WAYF (Where-Are-You-From) service is deployed that maintains participating domain sites within the Grid VO. The authentication process conforms to the standard Shibboleth model and can be described as follows:

(1) When a user logs on to the GIS portal, it is redirected to the WAYF service.

(2) The user chooses his/her home domain site, and then the user is redirected to his/her home domain site's authentication system.

(3) The user is authenticated by his/her home domain site's authentication system (e.g. GSI, Kerberos, One Time Password, etc).

(4) The IdP redirects the user to the GIS portal. A signed SAML authentication assertion is passed in this redirect containing a unique handle for the user and demonstrating that the user has been authenticated.

Once the user is authenticated, the PERMIS based system will take over authorization. The authorization process will be discussed in a later section.

2.2.2. Attribute management. Shibboleth requires agreed sets of attributes that have been negotiated between domain sites. To achieve this, we have identified a core set of attributes to describe the users in which some key attributes are listed as follows:

- userSite: this attribute indicates the domain site to which a user belongs.
- userName: this attribute uniquely identifies a user within a domain site.
- userType: this attribute categorizes users within a domain site in terms of their system rights, e.g. a standard user or a site administrator.
- userGroup: a user can be assigned to some featured groups, for example, grid user group, non-grid user group, etc.

The above is just an initial set of user attributes which is recommended for the IdPs of each domain site that the authorization systems can subsequently use for authorization decisions to access the SISs. It is important to note that these user attributes are statically defined and agreed between the domain sites of a Grid VO which the GIS is monitoring. If the attribute managers of some domain sites need to extend the attribute set, they have to make sure that the interoperability exists between the new user attributes.

2.2.3. Membership management. A Grid VO is a dynamically established organization composed of a group of administrative domain sites that may join or leave. In accordance with the hierarchical structure of the GIS, the security framework uses a two-layer scheme to manage the membership of a Grid VO. At VO layer, the VO administrator can add/remove a domain site to/from a Grid VO upon site administrators' requests. The membership information

is stored in a database as shown in Figure 2. Meanwhile, any changes on the VO membership can be supplied to the WAYF service so that the service could maintain the latest information about the participating domain sites.

Similarly, at the site layer, we utilize a database system to store the user and group information. With database manipulation, a site administrator can add/remove users to/from his domain site, or assign / remove user to/from a group. Meanwhile, an attribute manager can retrieve the information that is provided by the database, and issue proper attribute certificates to users (as illustrated in Figure 2). The attribute certificates are in the format of X.509 certificate, and can be stored in an LDAP server.

2.3. Authorization via PERMIS

After authentication, the following step in the user to the GIS security flow is user authorization. We now discuss the issues involved in the PERMIS-based user authorization within the security framework, in particular, the authorization model and policy management.

2.3.1. Authorization model. We are motivated by the principle of the Access Control Framework [10] and thus designed an authorization engine based on PERMIS to control the access to the SISs. The structure of the authorization engine is depicted in Figure 3. In this structure, the SISs are Grid services implemented on Globus Toolkit 4 and the Globus Toolkit itself is the PEP (Policy Enforcement Point) that enforces the decisions made by the PDPs. The PDP is realized in the form of PERMIS. The authorization engine uses the API provided by the GGF SAML AuthZ specification [21] to facilitate the communication between the PEP and the PDP. This approach enhances the authorization options of the SISs through the use of PERMIS.

The authorization process is on the basis of the standard PERMIS model and can be simply described as follows:

(1) The authorization engine firstly asks the Shibboleth component responsible for retrieving the user's AC to pass on the user's AC.
(2) The user's AC will be analyzed by the credential validation component of PERMIS, and only those attributes that can be validated by the credential validation rules in the policy will be recognized as valid.
(3) Then PERMIS will use the association of attributes and privileges as specified in the policy to render an authorization decision for the user's request. That is, the user is either granted or denied access to the GIS.

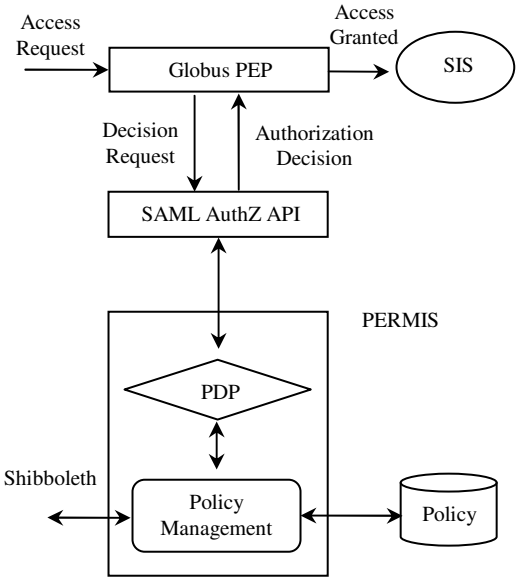

Figure 3. The authorization engine of the GIS

2.3.2. Policy management. Site administrators may need to protect information about their resources via authorized access to the GIS. Meanwhile, site administrators may also wish the security framework of the GIS to provide flexibility for them to define multi-grained policies for information access control. The policy management in the security framework for the GIS is based on RBAC in which policies are defined stating the rules for assigning roles to users and permissions to roles. The policies are represented by X.509 certificates which mainly include role specification attribute certificates and role assignment attribute certificates. The role specification attribute certificates holds the permissions granted to each role, and the role assignment attribute certificates assign various roles to users. Here we mainly discuss four kinds of policies that embody the main aspects of policy management, i.e. subject policy, role assignment policy, target policy and target access policy.

The subject policy specifies the category of users who may be granted roles in each domain site. Each category is specified as an LDAP subtree, using Include and Exclude statements with optional layering. For example, if taking the 'useType' attribute defined in Section 2.2.2 as the main criteria to categorize users, a site administrator at the Institute of High Performance

Computing (IHPC) in Singapore could make the following subject policy for two categories of users within the domain site, i.e. standard users and site administrators:

```
<SubjectPolicy>
 <SubjectDomainSpec ID="standardUsers">
  <Include LDAPDN="ou=standarduser, dc=ihpc,
                   dc=edu, dc=sg"/>
 </SubjectDomainSpec>
 <SubjectDomainSpec ID="siteAdministrators">
  <Include DAPDN="ou=administer, dc=ihpc,
                  dc=edu, dc=sg"/>
 </SubjectDomainSpec>
</SubjectPolicy>
```

The role assignment policy specifies which roles can be assigned to which subjects. For example, the following policy assigns the subjects above to two kinds of roles, i.e. restrictedAccess and fullAccess.

```
<RoleAssignmentPolicy>
 <RoleAssignment>
  <SubjectDomain ID="standardUsers"/>
  <Role Type="permisRole"
        Value="restrictedAccess"/>
 </RoleAssignment>
 <RoleAssignment>
  <SubjectDomain ID="siteAdministrators"/>
  <Role Type="permisRole"
        Value="fullAccess"/>
 </RoleAssignment>
</RoleAssignmentPolicy>
```

We also need to define the target policy that specifies the target domains which is information categories in the context of GIS. In the following example, the site administrator defines two target domains, i.e., the hardware information and software information.

```
<TargetPolicy>
 <TargetDomainSpec ID="HWinfo">
  <Include LDAPDN="dc=cpu, dc=hardware,
                   dc=ihpc, dc=edu, dc=sg"/>
  <Include LDAPDN="dc=memory, dc=hardware,
                   dc=ihpc, dc=edu, dc=sg"/>
    …
 </TargetDomainSpec>
 <TargetDomainSpec ID="SWinfo">
  <Include LDAPDN="dc=os, dc=softwareware,
                   dc=ihpc, dc=edu, dc=sg"/>
      …
 </TargetDomainSpec>
</TargetPolicy>
```

Finally, a site administrator needs to define target access policy which grants the GIS users with respective role permissions to carry out the specified actions on the specified lists of targets. In the following example, site administrators with 'fullAccess' role are granted to access all information, while standard users with 'restrictedAccess' role can only access hardware information.

```
<TargetAccess>
 <RoleList>
  <Role Type="permisRole"
        Value="restrictedAccess"/>
 </RoleList>
 <TargetList>
  <Target Actions="Access">
  <TargetDomain ID="HWinfo"/>
  </Target>
 </TargetList>

 <RoleList>
  <Role Type="permisRole"
        Value="fullAccess"
 </RoleList>
 <TargetList>
  <Target Actions="Access">
  <TargetDomain ID="HWinfo"/>
  <TargetDomain ID="SWinfo"/>
  </Target>
 </TargetList>
</TargetAccess>
```

By defining the policies, a site administrator can decide which users are allowed to access the SIS in the domain site. The site administrator may only allow certain users to access all or partial information on some resources in the domain site. This indicates that the PERMIS based authorization system for the GIS provides the site administrators with great flexibility to define multi-grained polices for information access control.

4. Conclusions and Future Work

A Grid Information Service monitors geographically distributed resources scattered in different domain sites within a Grid VO, and provides information to users on request. Some domain sites may need the Information Service to protect the information from unauthenticated and unauthorized access. To enable users to access our GIS in a secure way, we propose a security framework incorporated into our GIS. This security framework leverages Shibboleth as an authentication infrastructure and PERMIS as an authorization infrastructure.

Shibboleth provides a simple and flexible way to access the GIS, and PERMIS allows site administrators to define their own policies on the information access control and the authorization decisions are made based on the roles of the GIS users. We believe that this security framework may also apply for other Grid services which have a need for security.

On the whole, the work we present in this paper is a general security framework for our GIS, and there are still a number of issues to be further addressed, e.g., the integration of Shibboleth with various authentication systems, the improving of policy management to support more complicated policy composition, and so on. We will also implement the security framework based on the open source packages of the Shibboleth [22] and Open PERMIS projects [23]. Some tools will also be developed to ease the deployment of the security framework and administrator work. Furthermore, we plan to deploy the GIS and the security framework on a large scale cross-domain testbed. We will conduct experiments on the testbed and investigate the scalability and performance of the security framework. This will help further optimization and enhancement of the security framework.

References

[1] I. Foster, C. Kesselman, et al, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", *International Journal of High Performance Computing Applications*, 2001, Vol. 15, pp. 200-222.

[2] S. Fitzgerald, I. Foster, et al, "A Directory Service for Configuring High-performance Distributed Computations", Proceedings of 6th IEEE Symposium on High Performance Distributed Computing, IEEE Computer Society Press, 1997, pp. 365-375.

[3] K. Czajkowski, S. Fitzgerald, I. Foster, and C. Kesselman, "Grid Information Service for Distributed Resource Sharing", Proceedings of 10th IEEE International Symposium on High Performance Distributed Computing, 2001, pp. 181 – 194.

[4] T. Dierks and C. Allen, The TLS Protocol Version 1.0, http://www.ietf.org/rfc/rfc2246.txt.

[5] MLS, http://www.globus.org/toolkit/3.0/ogsa/docs/message_security.html.

[6] I. Foster, C. Kesselman, G. Tsudik and S. Tuecke, "A Security Architecture for Computational Grids", Proceedings of the ACM Conference on Computers and Security, 1998.

[7] Globus Toolkit, http://www.globus.org.

[8] CCITT Recommendation X.509: The Directory – Authentication Framework, 1988.

[9] S. Tuecke, D. Engert, I. Foster, M. Thompson, L. Pearlman and C. Kesselman, Internet X.509 Public Key Infrastructure Proxy Certificate Profile, IETF, 2001.

[10] ITU-T Recommendation X.812 | ISO/IEC 10181-3:1996, Security Frameworks for open systems: Access control framework.

[11] L Pearlman, et al., "A Community Authorization Service for Group Collaboration", Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

[12] R. Alfieri, et al, "Managing Dynamic User Communities in a Grid of Autonomous Resources", the Conference for Computing in High Energy and Nuclear Physics, San Diego, 2003.

[13] T. Scavo and S. Cantor, Shibboleth Architecture Technical Overview, Internet 2 document: draft-maceshibboleth-tech-overview-02, June 2005. Available at http://shibboleth.internet2.edu/docs/draft-mace-shibbolethtech-overview-latest.pdf.

[14] D. W. Chadwick, A. Otenko and E. Ball, "Role-based Access Control with X.509 Attribute Certificates", IEEE Internet Computing, 2003, pp. 62-69.

[15] OASIS Security Services Technical Committee, Security Assertion Markup Language (SAML) v1.1. OASIS Standard 200308. http://www.oasisopen.org/specs/index.php#samlv1.1, 2003.

[16] D.W. Chadwick and A. Otenko, "The PERMIS X.509 Role Based Privilege Management Infrastructure", *Future Generation Computer Systems*, 2003, Vol. 19, No. 2, pp. 277-289.

[17] S. Farrell and R. Housley, "An Internet Attribute Certificate Profile for Authorization", Internet-draft 2002, http://www.ietf.org/rfc/rfc3281.txt.

[18] Wei Jie, Terence Hung, Stephen J. Turner and Wentong Cai, "Architecture Model for Information Service in Large Scale Grid Environments", Proceedings of the 6th IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2006), 2006.

[19] The WS-Resource Framework (WSRF), http://www.globus.org/wsrf/.

[20] Open LDAP, the Open Source Lightweight Directory Access Protocol (LDAP), http://www.openldap.org/.

[21] V. Welch, F. Siebenlist,, D. Chadwick, S. Meder and L. Pearlman, "Use of SAML for OGSA Authorization", Global Grid Forum, 2004.

[22] Shibboleth software package, http://shibboleth.internet2.edu/.

[23] Open PERMIS software package, http://www.openpermis.org.

0-7695-2913-5/07 $25.00 © 2007 IEEE