Access Control System for Grid Security Infrastructure

Conference Paper · December 2007

DOI: 10.1109/WI-IATW.2007.45 · Source: IEEE Xplore

CITATIONS
6

READS
90

2 authors:

Mayphyo oo
University of Computer Studies, Yangon
7 PUBLICATIONS **12** CITATIONS
SEE PROFILE

Thinn Thu Naing
University of Computer Studies, Yangon
26 PUBLICATIONS **76** CITATIONS
SEE PROFILE

Access Control System for Grid Security Infrastructure

May Phyo Oo, Thinn Thu Naing
University of Computer Studies, Yangon, Myanmar
mayphyooo@gmail.com, ucsy21@most.gov.mm

Abstract

Grid access control mechanism is aimed at verifying the identity of an entity, controlling certificates and to restrict from unauthorized accesses to grid resources. Hence, it plays a vital role to get the system availability as well as to prevent the attackers who tries to get the unauthorized accesses to resources. In fact, this paper proposes the system that provides the secure certificate framework to offer access control. The main contribution of this paper is creating two types of certificate and using counting process to secure Authorization, Authentication and Access Control service that is adapted to traditional RSA algorithm for Grid Application.

1. Introduction

In a grid, member machines are configured to execute programs rather than just to move data. This makes an unsecured grid potentially fertile ground for viruses and Trojan horse programs [3]. For this reason, sharing of resources is important to control them strongly. Resource providers and resource consumers need to negotiate resource sharing arrangements, defining the conditions of sharing, such as what is shared and who is allowed to access the shared resources. A set of individuals and institutions participating in such sharing relationships are referred to as a Virtual Organization (VO) [5]. The Certificate Authority (CA) is one of the most important aspects of maintaining strong grid security. A CA is used to hold these public keys and to guarantee who they belong to [14]. Authorization is needed to allow legitimate grid users to access confidential grid information and resources. Thus, Access Control System for grid security infrastructure using community authorization service (CAS) [6], matching method and counting method is developed. It is the new managing certificate scheme for grid environment. In this system, Certificate Authority (CA) performs two types of certificate and limits the range of using certificate counts for grid users by using counting process. In order to put much more trust among sender, receiver and CA, the frequency of certificates including time stamps are restricted by counting method. Counting service of CA can protect attacks to have trusted certificate by controlling the range of using counts. These approaches will be applied into RSA [14] public key algorithm for encryption/decryption function in our system. This paper focuses on access control, authorization, authentication, certificates formats and how security has been made for the benefit of grid users.

The remainder of this article is organized as follows. In section 2 related work and problem issues are described. In section 3 proposed framework and models for authorization, authentication and access control system assumption are introduced. In section 4 the performance evaluation of ACS-GSI system is presented. Section 5 concludes with a brief discussion and future work.

2. Related work and Problem Issues

Every user and service on a Grid is identified via a certificate, which contains information vital to identifying and authenticating the user or service [4]. A GSI certificate includes four primary pieces of information: A subject name, issuer (identity of CA), public key (belonging to the subject) and the digital signature of the named CA [8]. CA is used to certify the link between the public key and the subject in the certificate[1]. GSI certificates are encoded in the X.509 certificate format, a standard data format for certificates established by the Internet Engineering Task Force (IETF) [2]. Authorization is important for authentication, confidentiality, auditing, and access control. Authentication aims at verifying the identity of an entity [4]. If the CA's private key is compromised, the digital certificates will not be reliable anymore [13]. In addition, existing certificates rely on private key, public key, and validity of the expiration. If attackers get user private key, they can make false certificates and can access resources without registration till it expires. Moreover, there is another problem-- when grid users request to CA to issue new certificate for their expired certificates, CA may face

0-7695-3028-1/07 $25.00 © 2007 IEEE
DOI 10.1109/WI-IATW.2007.45

connection failure. So CA's reply may delay for important users. If a user wants to send important message, he can face delaying process while waiting for the reply from CA [9].

In order to solve the above problems, an access control system for grid users using counting process and creating two types of certificate is proposed. That is one reason why two types of certificate are needed to use for reducing those above risks. According to this idea, issuing two types of certificate is intended to use between Certificate Authority and Authentication Service. Counting Process might also manage the range of using counts to control their certificates among CA and grid nodes. The CA makes two types of certificate with the range of using counts to check the true identity of a grid user and their grid requests. Moreover it plays the important role of access control in order to complete jobs in time. So we can recover exactly whether delaying events in time by creating two types of certificate and using the counting process for grid users.

3. System Framework

In this system, there are six main components. They are Virtual Organization, Grid Authorization, Authentication, Access control, Certificates and Counting Process. The security aspects of using counting process and creating two types of certificate for grid users are proposed and an access control method for authentication and authorization within grid environment is built. The secure method of Grid Security Infrastructure for authorization, authentication and access control is an extension of GSI. In order to recover and control Certificates, we should be aware of not only access control method but also some of the other resources and policies defined in GSI.

3.1 Work Mechanism of ACS_GSI System

In ACS_GSI system, the counting process (CP) plays the role of the restricting frequency of Certificate in the responsibilities of Certificate Authority. This system's work mechanism is illustrated in the algorithm that follows. Firstly grid application client creates certificate request and sends to CA. Next, CA replies to client giving certificate. Client sends his primary certificate to the CAS server. The latter CAS verifies Client's certificate, checks the range of using counts allowed from CA, matches Client's outgoing frequency of certificate and incoming frequency of certificate in CAS's incoming count table and fetches Client's right, granted by the policy database. If Client's primary certificate is valid, the CAS server creates and sends a restricted proxy certificate by Client in order to access the requested resource. This certificate contains the name of the CAS server in the subject name field, limited the range of using counts of CA and the restrictions in the policy field. After that, Client authenticates to the resource with the proxy certificate as an authorized user. The resource on Grid Server checks whether the request is authorized by the local policy of the organization. Later on, it matches the outgoing frequencies of certificate from Client's sent folder and the incoming frequencies of certificate from Server's inbox folder. Finally, when these checks are successful, the request is processed on the remote resource of Grid Server.

ACS_GSI Algorithm

Begin
s ← user data from RA
c ← data of user certificate
p ← data in proxy certificate
a ← data allowed by CA
M_e ← encrypted random message of client
M_d ← decrypted random message of server
1. Request Certificate to CA
If s=c, then
A: Creates C_{pri} , C_{sec} $\{F_c , Sig\}_{CP,RSA}$
B: Issues C_{pri} and C_{sec} (to client)
C: Client request $_{proxy}$ C to CAS
If C_{pri} valid then issues $_{proxy}C_{Restric}$ from CA
2. Client sent $_{proxy}C_{Restric}$ to Server
Increase outgoing count
If p=a then
A: Accept proxy $C_{Restric}$
B: Increase incoming count
If incoming count > limited count then
reject: go to 1
apply C_{sec}
C:match outgoing count and incoming count
If outgoing count=incoming count then
C1: Allow access resources
Else reject: go to 1
Apply C_{sec}
If $M_e = M_d$ then go to C1
Else reject and exit
End

3.2 Access Control Model and Assumption

In this secure model, it could prove the secure authorization, authentication and access control system as follows.

Users are issued certificates using authorization function.

$$z(x) = \sum_{i=1}^{n} s_i - c_i \begin{cases} \text{accept, if } z(x)=0 \\ \text{reject, otherwise} \end{cases}$$

Let z (x) =authorization function
s = user's attributes from registration process
c = attributes on user's certificate

If the user's attributes such as registration number, user name and so on, are the same as the attributes of the registration process, then CA accepts the user as an authorized user and issues two types of certificate. Otherwise the user's request will be rejected.

$$v(x) = \sum_{i=1}^{n} g_i - u_i \begin{cases} \text{accept, if } v(x)=0 \\ \text{reject, otherwise} \end{cases}$$

Let v(x) = certificate verification function
u = attributes of user's primary certificate
g = policy information agreed from CA

After getting certificates from CA, user can access resources submitting primary certificate to grid server. When grid server receives client's primary certificate, server verifies attributes of user's primary certificate matching with agreed policy information of CA. If the attribute of user's primary certificate is the same as information agreed from CA, certificate revocation function reports to grid server like a true certificate. Hence, grid server accepts it as a real certificate. Otherwise server assumes it as a false one and rejects the certificate.

In addition, errors are checked by using the matching function.

$$f(x) = b_i - a_i \begin{cases} \text{accept, if } b_i - a_i = 0 \\ \text{reject, otherwise.} \end{cases}$$

f (x) =matching function
a=number of frequency of outgoing certificate
b =number of frequency of incoming certificate

There are two facts in this model: If the difference between the number of frequency of outgoing certificate and the number of frequency of incoming certificate is equal to zero, there is no error. So both the user and grid server will continue communicating and trust each other. Otherwise there is an error. If that happens, both the user and the grid server understand that it is an invalid event. Depending on the result of matching function, grid server decides whether to allow resources for the user or not.

Again, the counting method has been built for checking restricted frequency of certificate as shown in the following secure simulation model.

$$g(x) = r - \sum_{i=1}^{n} i \begin{cases} \text{accept, if } g(x)=0 \\ \text{reject, otherwise} \end{cases}$$

g (x) = counting function of using certificate
n= the sum of using counts from grid user
r=the restricted range of using counts from CA

In this secure counting model, two facts are found out. If the difference between the total frequencies of using certificate from the user and the restricted range of using counts from CA is greater than or equal to zero, there is no error. So both the client and the server will continue to communicate and trust each other. Otherwise there will be invalid events.

4. Performance Evaluation

This system contributes two approaches such as (i) two types of certificates are used as primary and secondary certificate.(ii) it restricts not only the range of using counts but also time validity. In this section, performance evaluation of ACS_GSI is presented.

4.1 Mechanism using Counting Process

ACS_GSI system can analyze the statistics of over counts that are shown in Figure 1.

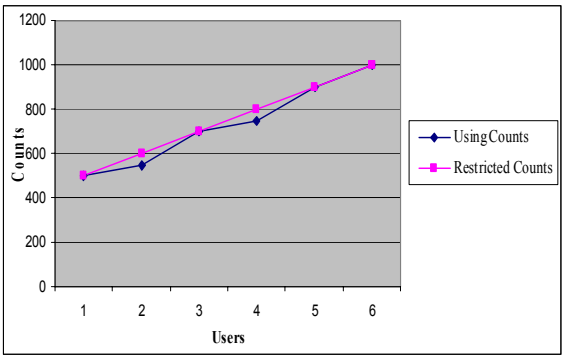

Figure1.Used Counts and Restricted Counts

According to the result of this figure, the system detects when users exceed their limited counts using counting algorithm as well as it gives message as user's certificate is expired. When users know their expired certificates, users can use secondary certificates immediately. Counting service of CA can protect attacks to have trusted certificate by controlling range of using counts.

4.2 Mechanism using Matching Function

Performance evaluation results of access control system using matching algorithm is shown in Figure 2. Whenever users send their certificates to Grid Server, user's outgoing count table records user's certificate counts. On the other hand, frequency of certificate are also recorded by incoming count table of Grid Server. In fact the frequency of user's certificate can not be known by anyone. Whenever a hacker tries to access resources using user's certificate, he will face access denied from server due to the result of matching algorithm and counting algorithm. Even if he gets the user's private key and he can access resource; users can know their certificates have encountered some problems due to the result of matching algorithm. If so occurs, user can request a new certificate by changing key. Hence, these results detect the invalid events and protect unauthorized users to access resources.

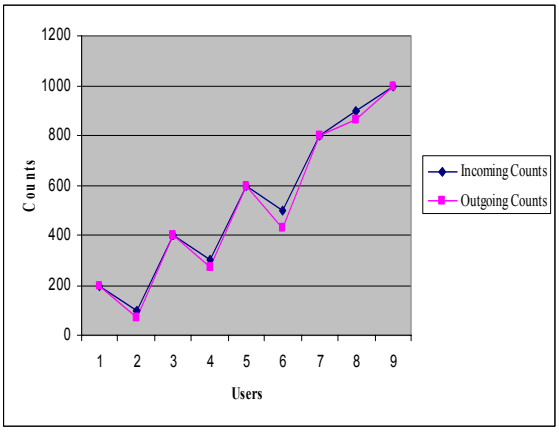

Figure2. Matching Incoming Counts and Outgoing Counts

5. Conclusion and Future Work

This paper presents an access control system creating two types of certificates that based on Grid. The Certificate of the secure Authorization service, thorough research on access control in the Grid environment has been developed. Grid security authenticated standardization and methods and how to improve authorization with trust managing certificate on Grid are being focused. The certificate of this secure system is certainly more reliable than existing certificates for Grid Users. The counting process could manage which secured credentials make it easier for authorized user to use their certificates. It can also be argued that when users face invalid events, they can use secondary certificates to access resources for recovering themselves. With the result of ACS_GSI, this system can be applied not only in grid environment but also in other applications such as Sensor Networks, Mobile Computing and so on in the future.

References

[1] S. Farrell, and R. Housley." *An Internet Attribute Certificate Profile for Authorization".* Internet Engineering Task Force, RFC 3281, 2002

[2] L.Ferreira, Viktors Berstis, Jonathan Armstrong. "*Introduction to Grid Computing with Globus".*

[3] I.Foster, C.Kesselman, G.Tsudik, and S.Tuecke. „*Security Architecture for Computational Grids",*. 5th ACM Conference on Computer and Communications Security, 1998

[4] I. Foster, C. Kesselman. *"The Grid Blueprint for a New Computing Infrastructure"*, Morgan Kaufmann, 1999

[5] I. Foster, C. Kesselman, S. Tuecke. *"The Anatomy of the Grid: Enabling Scalable Virtual Organizations"*, International Journal of Supercomputer Applications and High Performance Computing, 2001, 200-222.

[6] I. Foster, L. Pearlman, V. Welch, C. Kesselman, S. Tuecke "*A Community Authorisation Service for Group Collaboration*", in Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks. Washington, DC, USA: IEEE Computer Society, 2002, p. 50

[7] M. D. Harper, Herald information Systems. "*Trust, Security and ConfidenceOnline: The verifier's perspective*". Current development in e-commerce, Lecture Notes, RHUL, 2003.

[8] H. Mack. *"Public Key Infrastructure in E-Commerce Environments"*, Ecommerce Infrastructure, Lecture notes, Royal Holloway, University of London, 2003.

[9] M.P.Oo, N.L.Thein, T.T.Naing , *"Grid Security Framework for Managing the Certificate"* Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence, p-166

[10] M.P.Oo and T.T.Naing , "*Controlling Certificate to Authenticate Grid Users"*, Proceeding of the International Conbference on Internet Information Retrieval , Hankuk Aviation University of Korea, 2006

[11] F. Piper. *"Introduction to cryptography"*, Lecture Notes, RHUL, 2003.

[12] http://www.rsa.com

[13] M. Surridge, "*A rough Guide to Grid Security*". Issue 1.1a, IT-Innovation centre, 2002-2003. development in E-commerce, Lecture Notes, RHUL, 2003.

[14] V.Welch, F. Siebenlist, I.Foster, *"Security for grid services,"*in HPDC'03: Proceeding of the 12thIEEE International Symposium on High Performance Distributed Computing, DC, USA:IEEE Computer