Grid Security Framework for Managing the Certificate

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

Abstract

The certificate is a central concept in Grid Security Infrastructure authentication. The certificate guarantees the authenticity of the data, thus effectively authenticating the sender. In this paper, we propose a secure certificate authentication framework using Counting Process to interact trusty for Grid users .We intend to apply this approach in secured performance on Grids as well as in grid application for authenticating users, protecting attacks, and recovering failed systems. The main idea presented in this paper is to add counting process and matching method into RSA algorithm to apply in Grid certificate authentication.

Key Words: *Counting Process, RSA public key, Certificate, Authentication method and Authorization method*

1. Introduction

Security is a much more important factor in planning and maintaining a grid than in conventional distributed computing, where data sharing comprises the bulk of the activity. The computing resources are hosted in differing security domains and heterogeneous platforms. In a grid, the member machines are configured to execute programs rather than just move data. This makes an unsecured grid potentially fertile ground for viruses and Trojan horse programs. For this reason, security infrastructure is important to understand the issues involved in authenticating users and properly executing the responsibilities of a Certificate Authority (CA) [3]. The Certificate Authority is one of the most important aspects of maintaining strong grid security. An organization may choose to use an external Certificate Authority or operate one itself. A CA is used to hold these public keys and to guarantee who they belong to [11]. When a user uses his private key to encrypt something, the receiver uses the corresponding public key to decrypt it. The receiver knows that only that user's public key can decrypt the message correctly [8]. However, anyone could intercept this message and decrypt it because anyone can get the originator's public key. If the originator instead doubly encrypts the message with his private key and the intended recipient's public key, a secure communication link is formed. The receiver uses his private key to decrypt the message and then uses the sender's public key for the second decryption. Now the recipient knows that if the message decrypts properly, then only the sender could have sent it and furthermore, the sender knows that only the intended receiver can decrypt it [1].

We intend to apply this system in grid application for military environment. A grid login is usually more convenient for grid users and it could eliminate the ID matching problems among different machines. It makes grid user look more like one large virtual computer rather than a collection of individual machines like Globus, for instance, some grid system like implements a proxy login model that keeps the user logged in for a specified amount of time. To go against masquerading attackers and tampering attackers, digital certificates have to be used. The counting process will perform two types of certificate for every grid user. In order to put much more trust among sender, receiver and CA, frequency of certificates including time stamp are restricted by counting method. Moreover a matching method is applied in the grid authentication system which grants sender and receiver by controlling the frequency of incoming and outgoing certificate. Counting service of CA can protect attacks to have trusted certificate by controlling the range of using counts. We will apply these approaches into RSA public key algorithm for encryption/decryption function in our system. This paper focuses on Authentication, Certificate Authorization and how security has been made to the benefit of Grid users. Managing the frequency of certificates as well as the development of a new authentication system, leads to security and protects threats.

The remainder of this article is organized as follows. In Section 2 we describe related work and problem issues. In Section 3 we describe the reason for using Counting Process in grid logon Service. In Section 4 we introduce our proposed framework and models for authentication system assumption. We conclude in Section 5 with a brief discussion of conclusion and future work.

Proceedings of the 2006 IEEE/WIC/ACM International Conference
on Web Intelligence (WI 2006 Main Conference Proceedings)(WI'06)
0-7695-2747-7/06 $20.00 © 2006 IEEE

2. Related work and Problem Issues

Every user and service on the Grid is identified via a certificate, which contains information vital to identifying and authenticating the user or service[5]. 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[9]. A third party (a CA) is used to certify the link between the public key and the subject in the certificate. In order to trust the certificate and its contents, the CA's certificate must be trusted. 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]. Authentication becomes a challenging problem because of the different organizations involved. Authentication [4, 12] is paramount to Grid Security. Authentication is important to authorization, confidentiality and auditing. Authentication aims at verifying the identity of an entity [4]. Authentication is needed because the user identity is a parameter in most access control (authorization) solutions used on the Grid [4]. Finally, authentication is crucial to accountability, because user’s identity is part of security events logged in the audit trail [4]. If the CA’s private key is compromised, this means the digital certificates will not be reliable anymore. As a result: authentication failure will trigger authorizations failure because authorizations are based on the subject name in the certificate. Finally the whole Grid System will fail. Moreover existing certificates rely on expiration of time to valid. There is a problem when the expired certificate request to CA to change new certificate, CA may face connection failure. So CA’s reply may delay for an important user. If the user wants to send an important message, he can face a delaying process due to waiting the reply of CA.

In order to solve the above problems we proposed the managing frequency of certificates in the authentication system with the counting process. Our motivation for this decision was to make secured certificates with counting process in authentication acceptable to virtual organizations rather than the existing certificate.

3. Using Counting Process in Grid Logon Service

A user first must enroll as a grid user. Enrolling in the grid may require authentication for security purposes. The user establishes his/her identity with a Certificate Authority (CA). The CA makes the certificate with a range of using counts to check the true identity of a grid user and their grid requests. Within a grid environment, we need to consider the locations of the private key and thefts of certificates. That is one reason why counting process is needed to reduce these risks such as impersonation, theft of private key, and compromise of CA private key. Counting Process will manage certificates among CA and grid nodes. In order to protect certificates, the counting process can check the frequency of using certificates. According to this idea, the counting process is intended to add between Certificate Authority and Grid logon service. So we can know sure invalid events in time by replacing counting process in grid logon service. Therefore grid logon service adding counting process could support Authentication service as well as Authorization in Grid. There are many benefits in this secure system due to the result of the advanced counting process. When a grid user enters grid logon, the counting process counts the number of units using user certificate and checks either invalid or valid certificate. Moreover Counting Process calculates the limiting counts from CA and returns to the grid user.

4. Proposed Framework

In this system, the security aspects of using the counting process for grid authentication users are proposed. We propose in some detail a method for authentication within grid environment by managing certificates. The proposed architecture is described in Figure 1 and the procedures are described as following assumptions:

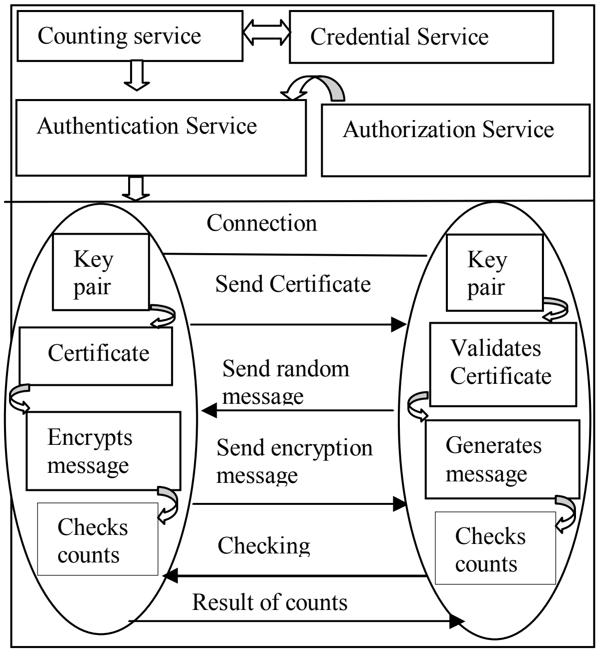

Figure1. Grid Credential Logging Service added Counting Service

- •Socket Secure Layer Protocol is used to connection establishment and user’s private key and the CA’s private key must be protected with the high degree of security.
- • Public key of the CA must be securely communicated to

Virtual Organization (VO) users and VO sites [6]. For example, a user to access the Grid is to be a member of a VO.

- CA controls the number of frequency of certificate by using the counting process and allows clients to use resources by defining the number of frequency including secondary certificate.
- Clients can use resources within the limited number of times by using primary certificate and Server allows resources to use only a limited amount of certificate for each client.
- When Grid Users face the invalid events, CA changes the new certificate for grid users although previous certificate doesn't expire. If Grid user's certificate has problem, Grid user can communicate by using the secondary certificate before getting a new certificate.
- When client uses the secondary certificate, server validates client's secondary certificate and accepts it.

4.1 Process Diagram of Security Framework

We describe the security framework in figure2. Suppose there are an application Client, four grid nodes and a Certificate Authority in our scenerio. Assume four grid nodes are Army, Air force , Navy and State affairs. And application Client is Central office.When application client needs to perform secret jobs and to send important messages, the headquarters must enter grid logon service including counting process with certificate. When Central office has authenticated these army nodes, Central office invokes a job and grid controller schedules a job on the grid server. And grid controller divides the task into subtasks and assigns it to Army, Air force, Navy and State affairs. Then the result from them would be collected by the result collector. The result collector returns the result of the job invoked to the grid controller. Finally, the grid collector returns the results back to the Central office. CA will generate the two types of certificates by using the counting process for the grid user. They are primary certificate and secondary certificate. Primary certificate includes eight major: Subject name, Public key of the grid user, serial number, validity (Restricted Range of Using Counts), Signature Algorithm, Possible extension fields, identity of (CA) and Digital Signature of the Third Party. Secondary certificate includes public key of the server and allowing range of using counts at least. Compared to the traditional authentication system, our certificates depend on the range of using counts. So Grid users can check invalid access and know the invalid certificate by managing certificates. In this way Grid users can communicate and access trust each other.

4.2 Model for Authentication System Assumption

In the proposed secure model, the authentication system can be proved as follows. Errors are also checked by using the matching function.

For matching the frequency of using certificate,

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

Let $R= B \backslash A \neq \Phi$

A= number of frequency of outgoing certificate

B= number of frequency of incoming certificate

f(x)=Matching function of using frequency of certificate.

There are two facts in this model: If the difference between the frequencies of the user A's outgoing certificate and the user B's incoming certificate is equal to zero, there is no error.. So both the user A and the user B will continue to communicate and trust each other. Otherwise both user A and user B understand that it is an invalid event.

For checking restricted frequency of certificate,

$$g(x)= \begin{cases} \text{reject, if count} < 0 \\ \text{accept, if otherwise.} \end{cases}$$

Let $\text{Count}=| B | \backslash | A | < 0$

g(x)= Counting function of using certificate.

A=the sum of the frequency of certificate by using user A

B=the restricted range of using counts from certificate authority

If A difference from B is greater than or equal to zero, there is no error. So both the user A and the user B will continue to communicate and trust each other. Otherwise there is an error.

For recoverying the failed certificate,

$$h(x)= \begin{cases} \text{accept, if } s = t \\ \text{reject, if otherwise} \end{cases}$$

h(x)=Recovery function of secondary certificate

s=decrypted random message by public key of user B and secondary private key of user A

t=encrypted random message by private key of user B and secondary public key of user A..

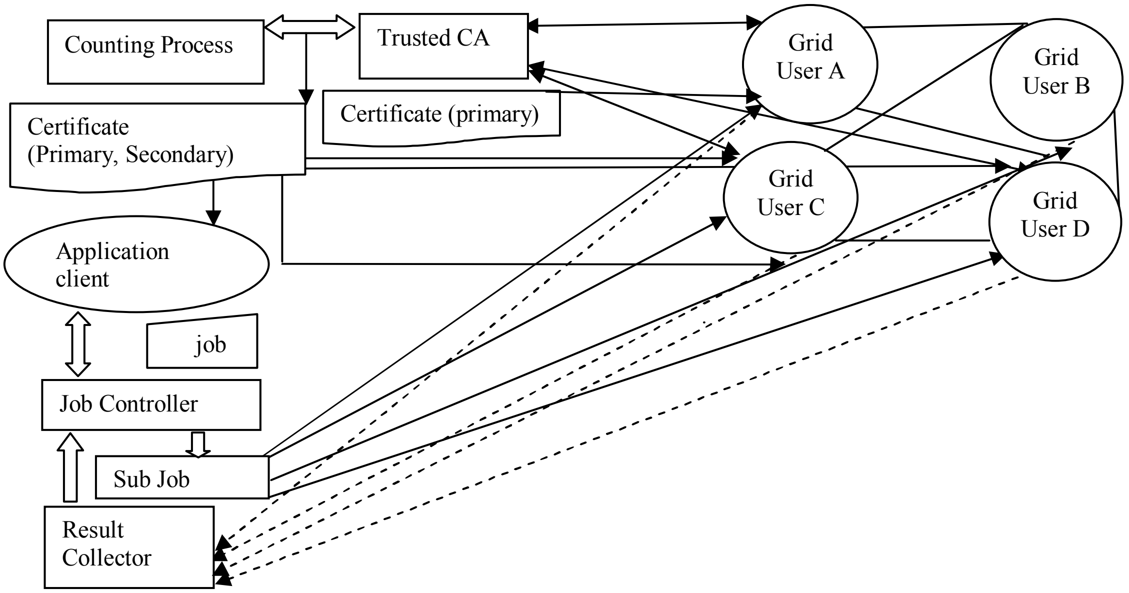

Figure2. Process Diagram of Security Framework

According to this result, we suggest the following fact: If the encrypted random message by private key of user B and secondary public key of user A is equal to the decrypted random message by public key of user B and secondary private key of user A, the user B accepts it. So both the user A and the user B can interact truly although primary certificate invalid. Otherwise the user B will reject the user A to access resources absouletely.

6. Conclusion and Future Work

This paper proposes a recovering certificate authenticating framework on Grid. We present the certificate of the secure Authentication model. This proposed secure certificate is more efficient using counting process rather than existing certificates for Grid Users. The counting process controls the secure credentials for authenticated user. It can also be argued that when users face invalid events, they can use secondary certificates to access the resource by recovering themselves. We intend to explore the access control in the Grid environment. We are also focusing on Grid security authorized standardization and methods about how to improve authentication with trust controlling certificate on Grid.

References

[1] S. Chokhani. *"Public Key Infrastructures and Certificate Authorities",* Chapter 23, Computer Security Hand book, Fourth Edition, Wiley, 2002.

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

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

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

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

[6] 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.

[7] http;//www.globus.org/mds

[8] http;//www.rsa.com

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

[10] A. Martin and M. Hopcroft. " *A Critical Survey of Grid Security Requirements and Technologies"*, Technical Report PRG-RR-03-15, Oxford University Computing Laboratory, August 2003

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

[12] G. Price, *"Public Key Infrastructure: Challenges and Challengers"*, Current

[13] M. Robshaw, S. Murphy. *"Advanced Cryptography"*, Lecture Notes, RHUL

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