Controlling Certificates for Grid Security Authentication and Authorization System

May Phyo Oo; Thinn Thu Naing

Abstract—*Grid authentication and authorization services are aimed at verifying the identity of an entity, managing 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 gain the unauthorized accesses to resources. In fact, this paper proposes the secure certificate framework to improve the security of the certificates based on Grid Security Infrastructure by making each server and each client keep track of how many times a certificate is used and accepted. The main contribution of this paper is using the counting process to secure Authorization and Authentication service for Grid Application.*

Index Terms—*Counting Process, Certificate, Authentication, Authorization and Grid Security Infrastructure*

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 [15]. Authorization is needed to allow legitimate grid users to access confidential grid information and resources. Thus, Controlling Certificates for Grid Security Authentication and Authorization System (CC_GAA) using matching method and counting method are 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. In order to put much more trust among sender, receiver and CA, the frequencies of certificates including time stamps are restricted by counting method. These approaches will be applied into Grid Security Infrastructure (GSI) in our system. This paper focuses on authorization, authentication, certificates formats and how security has been made for the benefit of grid users.

There are many benefits in this secure system due to the result of advanced counting service. When a grid user enters

Manuscript received January 29, 2007.

May Phyo Oo is with the University of Computer Studies, Yangon, Myanmar (e-mail: mayphyooo@gmail.com).

Thinn Thu Naing is with the University of Computer Studies, Yangon, Myanmar (e-mail: ucsy21@most.gov.mm).

grid logon, counting service counts the number of units using user certificate and checks either invalid or valid account. Moreover, CC_GAA calculates the limiting counts from CA and returns to the grid user. When grid users face invalid events, they can recover themselves by changing new certificate from CA. So the proposed secure system can control valid certificates regularly in time by replacing counting service in grid logon service. CC_GAA can reduce the risks of stealing certificates. Authentication service as well as authorization in Grid can be supported by adding this counting service in grid logon service. If the attackers enable to get user private key, they can make invalid certificates and they can get other's certificates. And they can use these certificates and access resource until expiration of time. This is the important fact in the role of using certificate. Counting service controls the frequency of using certificate between sender and receiver and restricts the frequency of using certificate among CA, Client and Server. Moreover grid users can check using time of their certificates according to the facility of CC_GAA. To have trust Certificate Authority (CA) of the security infrastructure, counting service is used in the responsibility of CA. Limiting the frequency of Certificates can protect unauthorized access of masquerading attackers because both client and server can check their frequency of using certificates each other vice visa. When they know errors among them as the result of counting process, they can recover themselves by using secondary certificates instantly. So we develop secure certificates in authentication and authorization acceptable to virtual organizations rather than existing certificates.

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 and authentication assumption are introduced. In section 4 the performance evaluation of CC_GAA 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]. Authentication is important for authorization, 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 the bottle neck of network connection. 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 [14].

In order to solve the above problems, an authentication and authorization system for grid users using counting process and creating two types of certificate are 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 named primary and secondary 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 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 like figure 1. 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 controlling certificates for authentication and authorization system within grid environment is built. The secure method of Grid Security Infrastructure for authorization and authentication is an extension of GSI. In order to recover and control Certificates, we should be aware of not only using counting process, creating two types of certificate but also some of the other resources and policies defined in GSI.

3.1 Virtual Organizations

In this system, a typical scenario of a Grid application is a military environment. We describe the following facts:

[1] How the members of VO are interacted in subsystems.

[2] According to the system assumption, each military command is performed as virtual sub organization nodes such as Army, Air Force, Navy and Police.

[3] In Army nodes, there are some branches employed such as Central Command, Eastern Command, Western Command, and Southern Command and so on.

[4] In Air Force (AF) Node, there are some branches employed such as AF1, AF2 and etc.

[5] In Navy Node, it also consists of some branches command.

[6] In Police Node, police command is also organized by some branches such as Special Bureau Command (SB1), SB2 and so on.

3.2 Process Flow of VO Members

In this section, we describe the process flow of VO members for CC_GAA system as following algorithm.

1. Army.Defence→Rg:{VO}
2. VO → Defence{Verify :Army.Defence}
3. SC.Army: Confirm $\{Id\}_{Army.Defense}$,
   where SC is site contact.
4. VO→ CA {issue Cer $_{Army.Defence}$ }
5. PL→Contact {Police.Home Affair}:
   Create $\{_{SubN}$Account $_{Cer}\}_{Army.Defence}$
   where PL is project leader.
6. VO→Army.Defence{Account.Police}

In step 1, Army Command registers with the VO to get a certificate. In step 2, the VO will contact Army Command in order to verify that the information of Army Command is true or not. In step 3, the site contact in Army confirms the Army Command's identity. And the VO asks the CA to issue a digital certificate for Army command in step 4. Then the project leader contacts all VO sites to create a local account for Army command based on the Subject name in his Certificate like an account of Police. Later, Army Command is sent to a confirmation that his account with the VO has been established according to step 7. In this way, Army Command becomes a Virtual Organization member. This is a component of our system.

3.3 Authorization and Authentication Model and Assumption

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

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

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

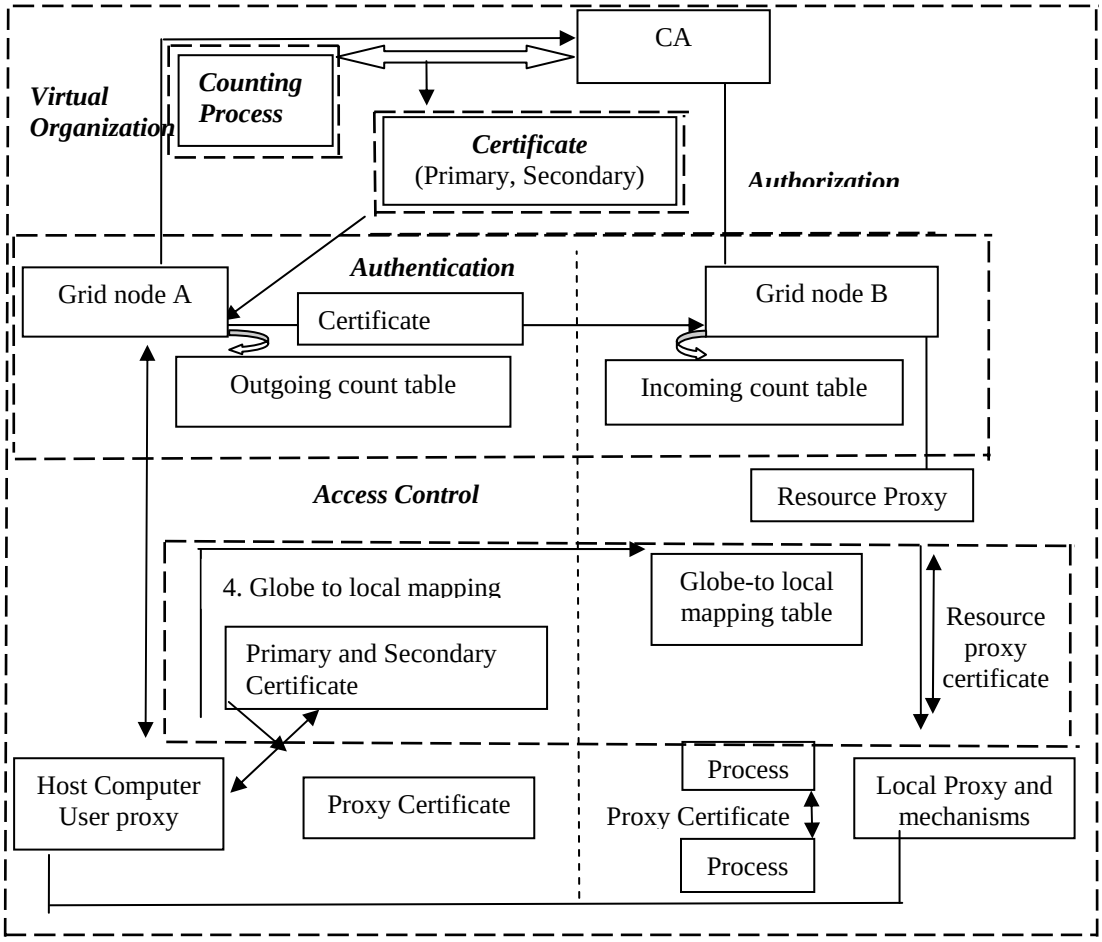
u = attributes of user's primary certificate

g = policy information agreed from CA

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.

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

Figure1: Components of CC_GAA System



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.

TABLE1: NOTATION USED IN THIS PAPER

$C_{Restric}$, SubN	Restricted Certificate , Subject name
C_{req}, Rg, F_c	certificate request, register, frequency of using certificate
C_{pri}, C_{Sec} ,Sig	primary certificate, signing secondary certificate

4. PERFORMANCE EVALUATIONS

We evaluated the performance of CC_GAA system as the following results.

4.1 Mechanism Using Counting Process

In this system, there are the restricted counts of using certificate for each user. We analyze the statistics of over counts. We show the performance evaluating results in figure 2.

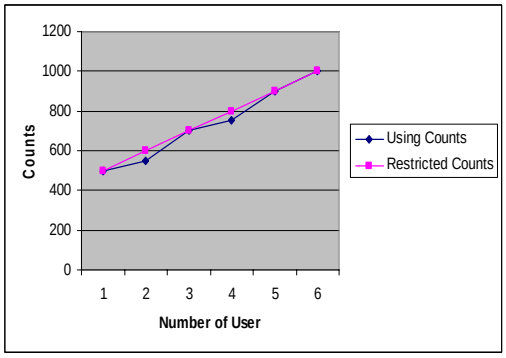


Figure2: Restricted Counts and Using Counts

According to figure 2, when users overuse their number of using counts, counting algorithm can detect over counts and give message as user's certificate is expired. As soon as users know their expired certificate, user can use secondary certificate. Counting service of CA can protect attacks to have trusted certificate by controlling the range of using counts.

4.2 Mechanism Using Matching Method

Matching method is applied in grid authentication system which grants sender and receiver by managing the frequency of incoming and outgoing certificate. We show the performance evaluation results in figure 3.

Whenever users send their certificates to Grid Server, user's outgoing count table record user's certificate counts. On other hand, the frequency of certificate is also recorded by incoming count table of Grid Server. In fact that frequency of user's certificate can not be known by any one. Whenever hacker tries to access resources using user's certificate, hacker may face access denied from server due to the result of matching algorithm and counting algorithm. Even hackers get user's private key and they can access resource; users can know that their certificates have problems due to the result of matching algorithm. Hence, user can request a new certificate by changing key. Hence, these results detect the invalid events and protect unauthorized users to access resources.

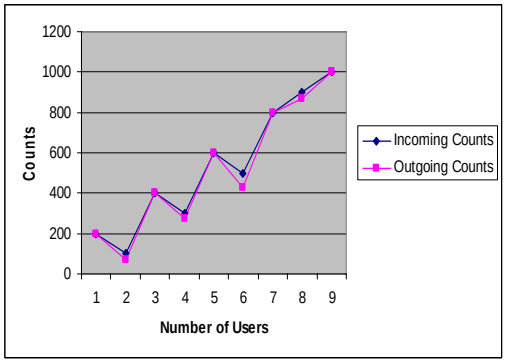


Figure 3: Incoming Counts and Outgoing Counts

5. *Conclusion and Future Work*

This paper presents a recovery method for authorization and authorization architecture that based on Grid. The Security Framework, thorough research on Certificates in the Grid environment has been developed. We are also focusing on Grid security authentication and methods about how to improve authorization with trust managing certificate on Grid. 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 the resources recovering themselves. As the result of CC_GAA, access control will also be provided in the future. This system can be applied not only in Grid environment but also in any application such as Sensor Network, Mobile Computing and so on.

References

[1] D.Chadwick, O. Otenko, "A Comparison of the AKENTI and PERMIS Authorization Infrastructures "in Ensuring Security in IT Infrastructures Proceedings of ITI First International Conference on Informatin and Communications Technology Cairo University, Ed. Mahmoud TEL-Hadidi, p5-26, 2003.

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

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

[6] I. Foster, L. Pearlman, V. Welch, C. Kesselman, S.Tuecke "A Community Authorisation Service forGroup Collaboration", in Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY'02). Washington, DC, USA: IEEE Computer Society, 2002, p. 50

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

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

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

[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, p. 110

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

[12] M.P.Oo, T.T.Naing "Access Control System for Grid Security Infrastructure", Proceeding of 2007 IEEE/WIC/ACM Web Intelligent and Intelligent Agent Technology-Workshop, p 299-302.

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

[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.

[15] V.Welch, F. Siebenlist, I. Foster,"Security for grid services," in HPDC '03: Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing (HPDC'03). Washington, DC, USA: IEEE Computer Society, 2003, p. 4