New security infrastructure model for distributed computing systems

J Dubenskaya¹, A Kryukov¹, A Demichev¹ and N Prikhodko²

¹Skobeltsyn Institute of Nuclear Physics, Lomonosov State University, Moscow, Russia
²Yaroslav-the-Wise Novgorod State University, Veliky Novgorod, Russia

E-mail: dubenskaya@theory.sinp.msu.ru

Abstract. At the paper we propose a new approach to setting up a user-friendly and yet secure authentication and authorization procedure in a distributed computing system. The security concept of the most heterogeneous distributed computing systems is based on the public key infrastructure along with proxy certificates which are used for rights delegation. In practice a contradiction between the limited lifetime of the proxy certificates and the unpredictable time of the request processing is a big issue for the end users of the system. We propose to use unlimited in time hashes which are individual for each request instead of proxy certificate. Our approach allows to avoid using of the proxy certificates. Thus the security infrastructure of distributed computing system becomes easier for development, support and use.

1. Introduction

Distributed computing systems (DCSs) are widely used by the researchers to solve different computational problems in various fields of natural science. DCS’s are especially popular in the computer simulation in physics. Perhaps one of the most significant examples of DCS is the European GRID infrastructure (EGI) [1], including the Worldwide LHC Computing GRID (WLCG) [2], which is used for processing and simulation of experimental data from the Large Hadron Collider (LHC). The brilliant result of the LHC experiments is the discovery of Higgs boson, which could not be reached without the WLCG.

For the purpose of this paper we will consider a DCS as a set of interacting Web services which send requests to each other. Access points for such a system are user Web interfaces or command line interfaces installed on users’ personal computers.

One of the most important parts of the DCS is a security infrastructure that provides: authentication and authorization, data integrity, encryption and so on. Information security is particularly important in such areas of science and technology as medicine, biological research, and engineering development. On the one hand, researchers need to be sure that the results of data processing and simulation are protected from unauthorized access; on the other hand, owners of the computational resources that
make up the DCS want to have guarantees that only the authorized users will be able to submit computational requests to the system.

The security infrastructure for the DCS is to provide users with a comfortable and secure access to the remote resources. Currently in most DCSs security is based on the public key infrastructure (PKI) [3] in conjunction with proxy certificates [4]. Proxy certificate is a special short time living certificate used for the purpose of providing restricted rights delegation within a PKI based authentication system. The short lifetime of the proxy certificate is due to security reasons. In DCSs proxies are used in several cases:

- To grant the rights between users and services to access to computing resources.
- While processing a composite computational task. A composite task is a regular task that needs to be processed by several services successively (i.e. the second service receives requests from the first service directly). In this case rights delegation between services takes place.

Along with the incontestable benefits of strong security the mentioned approach has also some disadvantages. First of all it is about the usability issues. The fact is that requesting and management of the X.509 certificates and proxies requires deep understanding of the basic concepts of the PKI that not all users have. The second problem with proxies is a short lifetime, while one cannot predict how much time would take request processing. There are special services to support prolongation of proxy lifetime [5], and all this make the security infrastructure overcomplicated and difficult to interact with. For example, the security infrastructure of EGI/WLCG is shown on figure 1.

![Figure 1. The security infrastructure of EGI/WLCG with proxy renewal procedure.](image)

In this paper we propose an alternative approach to building of the security infrastructure for the DCSs with no use of the proxy certificates with short lifetime. The main idea is to generate a separate individual hash for each request and to register the request along with the corresponding hash in the new specially introduced infrastructure entity called 'validation service'. This service should be trusted by the other services of the DCS and should act on-line. Upon getting computational request each service checks its hash against the validation service and continues only if the hash is correct and is not yet used. Unlike proxy certificate, such a hash is not limited in time. This feature is not a big issue as the unlimited lifetime of the hash is compensated by the fact that it can be used only once and only for a specific request.

In the next section we present the detailed description of the proposed approach including step-by-step authentication, authorization, and delegation algorithms. In Discussion we consider possible weak
points of the proposed security infrastructure and some solutions recommended to avoid them. In Conclusion the advantages of the proposed approach are analyzed in brief.

2. Proposed approach to security infrastructure building

Providing of the user-friendly, intuitive and yet secure interface can attract to the DCS lots of new users who are not experts in the field of computer science. To improve usability and facilitate access to the DCS we propose an alternative approach to building of the security infrastructure for the DCSs.

The main idea is in using login/password for user authentication while well tested PKI-based solutions are used for service-to-service interaction only. The authorization is implemented by using just in time approving of the rights via a special trusted validation service. The consequent security infrastructure is shown in figure 2.

![Figure 2. The proposed security infrastructure with validation service.](image)

The main points of the proposed authentication and authorization algorithm are listed as follows:

- On the first request a user have to enter a valid pair of login and password. For strong security the multi-factor authentication can be implemented.
- After successful login a user obtains a special session key for further work with no need to enter login/password pair over and over again.
- Each next user request is implicitly supplied by the previously obtained session key that is used for password-free access to the validation service.
- Each request should be protected by the individual hash which is not limited in time. This request hash is generated on the user's side for every single computational request with respect to request generation time. Due to this approach the hashes of the two completely identical successively generated requests would be different.
- These request hashes are registered by the validation service in the special database and states of these hashes are tracked on real time.
- Having received a computational request every computational service checks against the validation service if the request hash is valid, correct and is not yet used, and if the user is authorized to pass the request, and if the validation service returns OK the service executes the request. This approach ensures impossibility of request changing during its passing and processing.

Rights delegation between computational services is also implemented via request hash in the following manner:

- The first service generates a new subrequest from the initial request.
- For the new subrequest a subrequest hash is generated.
- Then the first service registers the subrequest hash in the validation service (the same as for
user's request).

- The first service passes the subrequest to the second service for processing. The second service examines the received subrequest hash via validation service.
- If the validation service says OK the second service continues processing.
- For a composite computational task a validation service collects a chain of the hashes which allow user to monitor the processing of the composite task and the status of each operation.

Thanks to this approach a user has even no need to know what a X.509 certificate and/or proxy certificate is. Session keys and request hashes are generated implicitly and are hidden from the user as well as details of the service interaction. Thus both high level of security along with seamless and easy access to the computational resources for the users are achieved thanks to intentional complication of the security infrastructure by adding a special validation service. So users are provided with seamless and easy access to the resources of the DCS and can concentrate on their computational needs.

3. Discussion

One of the possible weak points of the proposed approach is the requirement to have on-line access to the validation service for all other services of the DCS. The simulation using our prototype shows that such an infrastructure is quite stable and works fine at least for the systems with 20 user requests per second. For the critical high-availability systems it is possible to introduce two parallel validation services with on-line database replication. At this case one of the services acts as a master service that processes requests and another is a slave (an inactive full copy of the master). If the master service crashes it would be easy to switch to the slave service immediately with almost no loss of information.

An important benefit of the proposed security infrastructure is that during request processing the validation service collects all the information concerning each request in the DCS. This information can be used for monitoring purposes as well as for request revocation at any stage of processing.

4. Conclusion

The proposed approach improves user's operational performance and greatly enhances the competitive advantage for research organizations using DCSs. Scientists and engineers, as well as teachers and students can accelerate the practical results through the use of a simplified remote access to computational resources for data processing and modeling of processes in various fields of science and technology.

At the moment a prototype of the proposed security infrastructure has been developed. It includes one validation service and three other services that interact with users and with each other. The prototype is used to demonstrate the capabilities of the model and for heavy load tests.

Acknowledgments

This work is supported by the Ministry of Science and Education of Russian Federation, agreement No.14.604.21.0146.

References

[1] Kranzlmueller D, Lucas de J M, and Oster P 2010 The European Grid Initiative (EGI) Remote Instrumentation and Virtual Laboratories eds. Davoli F, Meyer N, Pugliese R, and Zappatore S (Boston Springer US) 61-66.
[2] Sciaba A, Andreeva J, Campana S, Donno F, Litmaath M, Magini N, Moscicki J T, and Renshall H 2010 Computing at the Petabyte scale with the WLCG. Worldwide LHC Computing Grid Tech. Rep. CERN-IT-Note-2010-006 (Geneva CERN).
[3] Buchmann J A, Karatsiolis E, and Wiesmaier A 2013 Introduction to Public Key Infrastructures (Springer-Verlag Berlin Heidelberg).
[4] Tuecke S, Welch V, Engert D, Pearlman L, and Thompson M 2004 Internet X.509 Public Key Infrastructure Proxy Certificate Profile Tech. Rep. RFC 3820.
[5] Kouril D and Basney J 2005 A credential renewal service for long-running jobs *IEEE/ACM International Workshop on Grid Computing* **13-14** 2-13.