Development of new security infrastructure design principles for distributed computing systems based on open protocols

Yu. Yu. Dubenskaya[a], A. P. Kryukov, A. P. Demichev

Skobeltsyn Institute of Nuclear Physics, M.V.Lomonosov Moscow State University (SINP MSU), 1(2), Leninskie gory, GSP-1, Moscow, 119991, Russia

E-mail: [a] dubenskaya@theory.sinp.msu.ru

The report presents our current work on design and development of security infrastructure of modern kind that is intended for different types of distributed computing systems (DCS). The main goal of the proposed approach is to provide users and administrators with transparent, intuitive and yet secure interface to the computational resources. The key points of the proposed approach to security infrastructure development are listed as follows:

All the connections in the DCS must be secured with SSL/TLS protocol.

Initial user authentication is performed using a pair of login and password with the use of multi-factor authentication where necessary. After successful login a user obtains a special session key with a limited validity period for further password-free work.

Every single computational request is protected by the individual hash which is not limited in time.

These hashes are registered by the special authentication and authorization service, and states of the hashes are tracked on real time. The service also provides online requests authorization for delegation of user rights to the other services in the DCS.

A prototype of the proposed security infrastructure was deployed on a testbed. It includes an authentication and authorization service, an execution service, a storage management service, and a user interface. Various tests have shown that the proposed algorithm and architecture are competitive in terms of functionality, usability, and performance. The results can be used in the grid systems, cloud structures, large data processing systems (Big Data), as well as for the organization of remote access via the Internet to supercomputers and computer clusters.

Keywords: security infrastructure, distributed computing systems, authorization, authorization

The work was supported by the Ministry of Education and Science of the Russian Federation, agreement No.14.604.21.0146 (RFMEFI60414X0146).

Introduction

Distributed computing systems (DCS) are widely used by the engineers and scientists to solve different computational problems in various fields of natural sciences. One of the most remarkable examples of DCS is the Worldwide LHC Computing GRID (WLCG) [Sciaba, Andreeva, …, 2010], which is used for reduction and processing of huge amount of experimental data derived from the Large Hadron Collider (LHC).

One of the most significant issues that faces developers and administrators of a DCS is to provide an appropriate security level during data processing and calculations. On the one hand, DCS users need to be sure that the results of data processing and calculations are protected from unauthorized access and would not be passed to the illegal intruder. On the other hand, owners of the computational resources that form the DCS want to have guarantees that only the authorized users will be able to submit computational requests to the system and to obtain the results.

Consequently, the security infrastructure of a DCS is to provide strong authentication and authorization of the users and services of the DCS, and also is to guarantee privacy, integrity and availability of processed and transmitted data. Moreover, integrity of the DCS itself should be assured as well as real-time availability of both user and auxiliary services.

Currently in most DCSs (including WLCG) security is based on the public key infrastructure (PKI) [Buchmann, Karatsiolis, Wiesmaier, 2013]. Additionally, in most of the GRID systems the proxy certificates [Tuecke, Welch, …, 2004] are used. 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 certificates is due to security reasons. If the request processing takes too long and the corresponding proxy certificate expires, an end user has to interact with special services that support prolongation of proxy lifetime [Kouril, Basney, 2005].

Analysis of experience of existing DCS operation reveals that PKI-based security infrastructure along with proxy certificates provides very high security level, but is difficult to understand and to interact with for the end users of the system. Furthermore, a contradiction between the limited lifetime of the proxy certificates and the unpredictable time of the request processing makes the security infrastructure overcomplicated, and is a big issue for the end users of the system. Thereby, along with the incontestable benefits of strong security the mentioned approach has serious usability issues. In practice, the researcher that acts as a DCS user can face serious problems trying to legally gain remote access to computing resources. 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 the users have. The need to use proxy lifetime prolongation services does more harm than good in that it makes the computation request submitting and processing still more complicated.

In this paper we propose an alternative approach to development of the security infrastructure for a DCS with no use of the proxy certificates with short lifetime. The main goal of the work is to improve usability and facilitate access to the DCS for the end users, provided that security level of the DCS still remains high.

In the next section the proposed approach is presented in more detail, including suggested architecture for the security infrastructure (that is considered as a part of the overall DCS architecture) and itemized step-by-step authentication and authorization algorithms. In Discussion we consider possible shortcomings of the proposed security infrastructure and some solutions recommended to avoid them. In Conclusion the advantages of the proposed approach are analyzed in brief.

Proposed approach to security infrastructure development

Providing of the intuitive, user-friendly, and yet secure interface can attract to a DCS a lot of new end users who are non-specialists in the field of computer science and information security, and who

want to get access and perform calculations in the DCS. The proposed approach to development of the security infrastructure primarily addresses a challenge of the DCS usability improving.

One of the main principles of the proposed approach is intentional complication of the security infrastructure by adding a special auxiliary service, that would be a trusted third party for all the DCS actors (users and services). This new auxiliary service is destined for authentication and authorization of the DCS actors, hereinafter to be referred to as AA-service. Within the framework of the proposed approach all the interaction requests between the DCS actors must be verified and approved by the AA-service. This solution allows to hide difficult cryptographic operations from the end users, ensuring that interface to DCS becomes more intuitive and usable.

Another important principle of the proposed approach is in replacement of proxy certificates with special hashes that are used to ensure that the request was not changed (further we will call them request hashes). To confirm the legality of the request in the DCS the AA-service uses specially generated unique hashes with unlimited lifetime. After receiving a computational request every execution service (that is installed on the computational resource) checks the request hash via the AA-service, and executes the request only if the AA-service responds that the hash is valid and has not been used yet. Thus the use of request hashes, on the one hand, makes it possible to solve the problem of request integrity protection during processing in the DCS, and on the other hand, eliminates the problem of the short lifetime of the regular proxy certificates. Online registration of the request hashes in the database of the AA-service provides strong authentication and authorization during requests processing in the DCS.

To increase usability the third principle is used that is intended to simplify the user experience, and is in use of the login/password pair for user authentication, while service-to-service interaction should pass only using proven solutions based on asymmetric cryptography and PKI. Thus, the AA-service is a key element of the proposed security infrastructure of the DCS, as all the system actors interact with it. The authorization is also performed by the AA-service with the use of request hash verification and online access rights check.

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

- All the connections in the DCS must be secured with SSL/TLS protocol.
- 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 (e.g. one-time-valid dynamic pass-code sent via SMS, e-mail, and so on.).
- After successful login a user obtains a special session key (lifetime of the key is called session and is defined by the DCS administrator) for further work with no need to enter login/password pair over and over again during the session (when the session expires a user will have to enter login/password pair anew). Each next user request is implicitly supplied by the previously obtained session key that is used for password-free access to the AA-service.
- Each request should be protected by the individual hash which is not limited in time. This request hash is generated 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 will be different. The request hash is generated by the AA-service at the moment when a user finalizes the request. All the request hashes are registered by the AA-service in the special database, and states of these hashes are tracked on real time. That is a consideration, as request hashes are one-time-valid, so a user will not be able to submit the same request twice using the same request hash.
- At the moment when a user submits its request to the execution service appropriate request hash is implicitly sent also.
- Having received a computational request every execution service checks against the AA-service if the request hash is valid, correct and has not been used yet, and if the user is authorized to pass the request, and if the AA-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 (S1) generates a new sub-request (R1) from the initial user request (R0).
- AA-service generates a request hash (H1) for the new sub-request R1, and registers H1 in its database.
- The first service S1 passes the sub-request R1 to the second service (S2) for processing. The second service S2 examines the received sub-request hash H1 via AA-service.
- If AA-service responds OK the second service S2 will continue sub-request processing otherwise the sub-request will be rejected.

Thanks to this approach an end user has even no need to know what a X.509 certificate and/or proxy certificate is, much less there is no need to install special cryptographic libraries on the user's local computer. All the cryptographic entities, such as session keys and request hashes are generated implicitly and are hidden from the user as well as details of the service-to-service interactions. Thus, thanks to intentional complication of the security infrastructure by adding the AA-service both high level of security along with seamless and easy access to the computational resources of the DCS for the end users are achieved. Thereby end users can concentrate on their computational needs.

The proposed approach is universally applicable and architecture-independent. It can be used in the GRID systems, cloud structures, large data processing systems (Big Data), as well as for the remote access via the Internet to supercomputers and computer clusters.

A prototype of the proposed security infrastructure was deployed on a testbed. It includes an AA-service, an execution service, a storage management service, and a user interface. Various tests have shown that the proposed algorithm and architecture are competitive in terms of functionality, usability, and performance.

Discussion

One of the possible shortcomings of the proposed architecture of the security infrastructure is the requirement to have on-line access to the AA-service for all end users and auxiliary 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 twenty user requests per second. For the critical high-availability systems it is possible to introduce two parallel AA-services with on-line master to slave database replication. For example, to address the issue a replication system for PostgreSQL database management system – Slony-I [Marcotte, 2005] can be used. At this case one of the AA-services acts as a master service that processes requests and another acts as a slave (an inactive full copy of the master). Only the master service is allowed to modify the data. If the master service crashes it would be easy for the administrator of the DCS to switch to the slave service immediately with almost no loss of information.

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

Conclusion

The proposed approach allows to enhance user's operational performance and greatly increases the competitive advantage for scientific and industrial research organizations that use DCSs. Scientific and technical teams, individual researchers and technology developers, as well as educators, graduate assistants and students have the great opportunity to accelerate their practical results through the use of a simplified remote access to DCS computational resources for data processing and calculations in various fields of natural sciences and technology.

References

Buchmann J. A., Karatsiolis E., Wiesmaier A. Introduction to Public Key Infrastructures. // Springer-Verlag Berlin Heidelberg, 2003.

Kouril D., Basney J. A credential renewal service for long-running jobs. // Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing. — 2005. — Vol. 2005. — P. 63–68.

Marcotte L. Database replication with Slony-I // Linux Journal. — 2005. — No.134. [Electronic resource]. URL: http://www.linuxjournal.com/article/7834 (accessed 18.11.2016).

Sciaba A., Andreeva J., Campana S., Donno F., Litmaath M., Magini N., Moscicki J. T., Renshall H. Computing at the Petabyte scale with the WLCG. Worldwide LHC Computing Grid Tech. Rep. CERN-IT-Note-2010-006. [Electronic resource]. URL:

http://cds.cern.ch/record/1302999/files/SCALE2010-WLCG-V2.pdf (accessed 18.11.2016).

Tuecke S., Welch V., Engert D., Pearlman L., Thompson M. Internet X.509 Public Key Infrastructure Proxy Certificate Profile. Tech. Rep. RFC 3820. [Electronic resource]. URL: https://www.ietf.org/rfc/rfc3820.txt (accessed 18.11.2016).