Research Journal of Applied Sciences 10 (10): 629-632, 2015
ISSN: 1815-932X

Implementation of Unified Session Access Model in a Closed Virtual Environment of Distributed Information-Computational Resource System as a Secured Portal Network

Igor S. Konstantinov, Sergej A. Lazarev, Oleg V. Mihalev and Vladimir E. Kiselev
Belgorod State National Research University, Pobedy St. 85, 308015 Belgorod, Russia

Abstract: This study discusses the mechanism of a single access session for a particular user within a closed virtual environment system of distributed information resources as a secured portal network. The implementation of this session access model provides a user single authentication in the portal network, no matter what nodes were called firstly and subsequently. Thus, it defines only one arbitrary user entry point to the portal network.

Key words: Virtual environment, network of portals, session access model, user authentication, single session of access, access control and information associations

INTRODUCTION

The research in the field of information associations development within a global information space based on a portal network (Lazarev, 2012) to meet the challenges of a closed virtual system environment development for distributed information resources (Lazarev *et al*., 2014c), determined the need of a single session access model implementation in the network. The concept of a portal network development and its distributed nature assume a secured authorized information exchange (Lazarev and Demidov, 2010, 2012) between the users belonging to different domain groups and various information portals of a network. That is why when an access to the resources of various network information sites (portals) takes place from the access control subsystem of a corresponding node it is required to identify a user in order to check his powers (Lazarev *et al*., 2013). Thus, an information node should request a user to enter his authentication data which is quite natural during a primary call to network resources but totally unacceptable from the aspect of operation convenience for an authorized user if each call to other information network node will require a re-authentication. An alternative solution is the existence of a confirmation mechanism in respect of a user's session from another information node, which authenticated this user. To do this, it is necessary to maintain the interactions with all the other network nodes by implementing a full-mesh logical topology which is very difficult and costly (Taggera *et al*., 2013; Lazarev *et al*., 2014b; Wiesmann *et al*., 2000) from the point of computing and network resource use. It is obvious that we need a centralized mechanism for the implementation of a single user session within a portal network and uniquely identification of a user in each of its segments. This aspect determines the urgency of this problem.

MATERIALS AND METHODS

Traditionally, the session access mechanisms (user session) are used for a user work management in multi-user software systems, including a user identification and the confirmation of his powers under an active session (Lazarev *et al*., 2014a; Gutzmann, 2001). A user session is a virtual connection, strictly tied to a, particular user of a system. Each session has a temporary identifier, a name which is used to obtain a user's system identifier and additional session information and lifetime: the time moment at which a session is considered to be an active one and participates in a system operation coordination. It is necessary to pass an authentication process to set a session identifier (Fig. 1).

When you project the mechanisms of a user session support within the network of corporate portals, it was noted that the implementation of a user compulsory authentication procedure at the stage of a connection creation with each new node of a network is an inefficient and an inconvenient solution in terms of an end user and the process of information exchange. In this regard, the possibility of a user authentication centralizing was considered followed by session data replication. A simple authentication is carried out in a central node and the data

Corresponding Author: Igor S. Konstantinov, Belgorod State National Research University, Pobedy St. 85, 308015 Belgorod, Russia

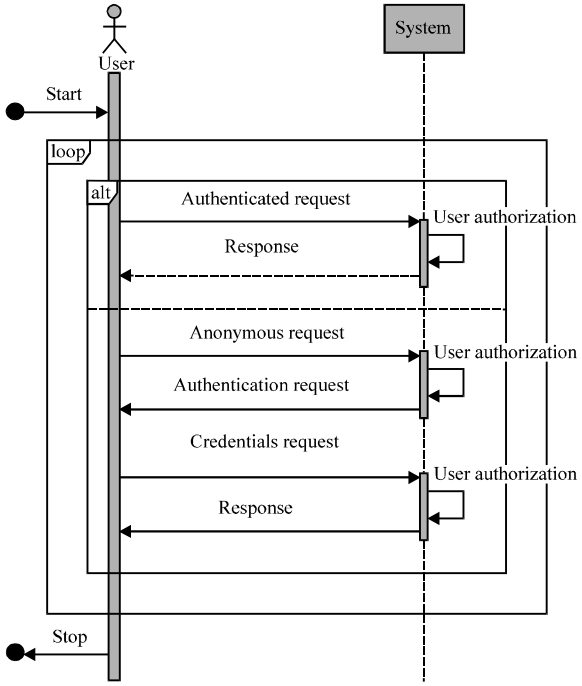

Fig. 1: System and user interaction scheme in a session access model

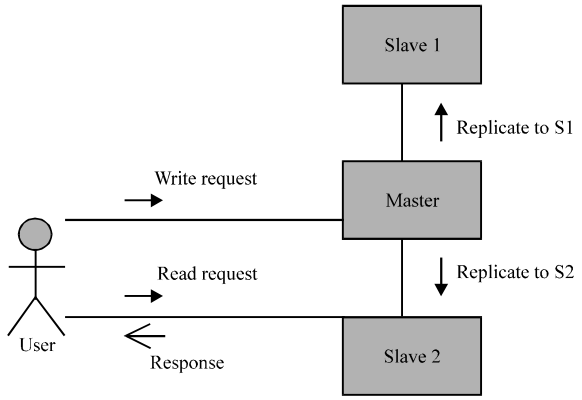

Fig. 2: Passive replication mechanism

array of a user session recording is replicated to other network nodes which are read-only. This approach is called a passive replication (Fig. 2) and is used in most information systems, where the recording operations are relatively rare in relation to the data extraction procedures (Birget *et al*., 2001).

It should be noted that such a scheme has an obvious disadvantage: when a central server is unavailable due to a hardware or a software failure, the system loses its ability to accept new connections, a service denial takes place.

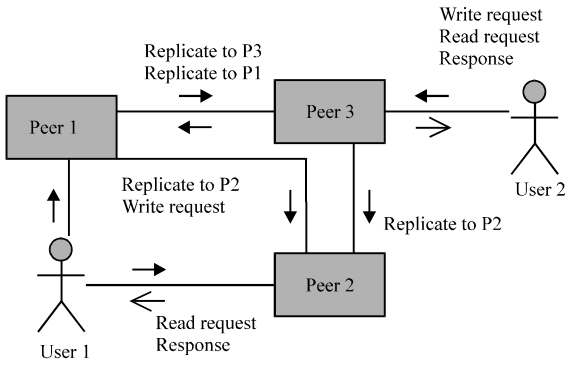

Fig. 3: Active replication mechanism

Another possible approach to the organization of the data replication scheme and the connection topology between network nodes is an active replication which suggests that session data record may be carried out on several equal nodes of a distributed network (Fig. 3). In extreme cases, a fully-coherent interaction with the amount of bonds equal to N (N-1)/2 takes place. It will require substantial resources for the organization of this logical topology (Taggera *et al*., 2013). Obviously, the most efficient in terms of reliability and fault tolerance of a portal network as well as the required costs will be a hybrid technical solution using the mechanisms of both passive and active replication for session data as well as the organization of network nodes interaction performing the record, the storage and the retrieval of this information (Chashin *et al*., 2014).

RESULTS AND DISCUSSION

Main part: A portal network is a set of access control nodes, the nodes of network management, custom network domains. A uniquely named user group is characterized by a domain. At that each user domain corresponds to a specific network access control node and vice versa.

The implementation of a single user session mechanism in a portal network suggests that some access control node has a session according to which an authorized user is identified, belonging to a definite, included in the list of this node "trusted" domains. Similarly unauthorized users of a domain may also be authorized only on a network node which trusts a domain.

A portal network user request is considered as an identified when it is possible to determine its initiator by an active session. Otherwise, a user must be authenticated for unidentified requests.

The distributed nature of a system and the peculiarities of its development suggest that the

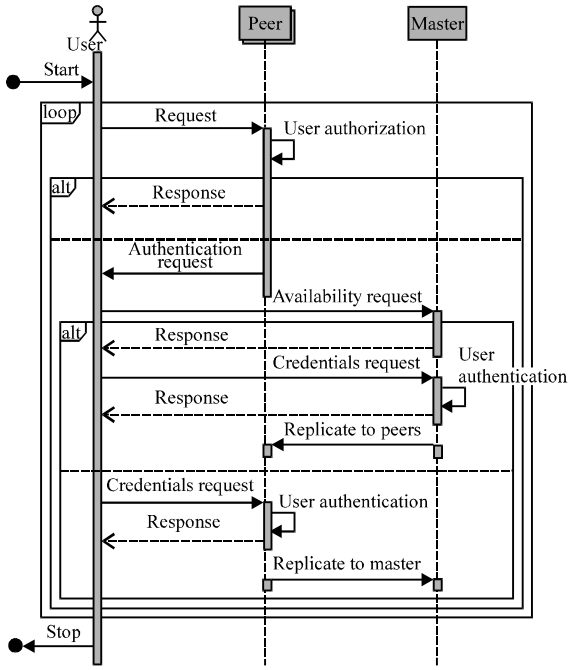

Fig. 4: The mechanism of a session access single model implementation in the network of corporate portals

maintaining of a user's session and an unambiguous identification of its requests should have the session data corresponding to a request or on the node where the request took place or at a central node of a system. Therefore, a user session on an access node may be a replica of the user session for a network control node.

Thus, when the nodes for portal network management are not available to identify a user session the availability of session data is necessary and enough only to at access control node, processing a request. Schematically, this mechanism is shown by Fig. 4 as an interaction sequence diagram.

Because of the portal network operation nature and user session management (the predominance of reading operations), a combined approach to the management of session information spreading is realized an active replication from ordinary nodes to a central node and a passive replication in a reverse direction. At that the ability of session creation on the general network nodes is available only in the case of a central node failure within the mode of an authentication source "hot" replacement. At the same time, this configuration provides the guarantee of a rapid and an effective dissemination of session data and a high availability of a system as a whole.

Summary: It should be noted that this study substantiates the necessity of a single model development for a session access in a distributed portal network. Different approaches to the session information management are considered in distributed networks. A combined approach to the management of user sessions is proposed and a formal description of a session access single model is provided for a distributed network of portals.

CONCLUSION

The implementation of a proposed session access model provides a single user authentication and one arbitrary entry point in a distributed portal network, no matter what network nodes were called firstly and subsequently, even when a central network node is unavailable.

ACKNOWLEDGEMENT

The research concerning this issue was sponsored by the RF Ministry of Education and Science. The project ID is RFMEFI57514X0099.

REFERENCES

Lazarev, S.A., 2012. Some aspects of the data associations development in the global information networks on the basis of a corporate portal network development. Information Syst. Technol., 1 (69): 103-106.

Lazarev, S.A., I.S. Konstantinov and O.V. Mihalev, 2014a. Realization of a single model session access in the distributed network portals. Vestnik komp'iuternykh i informatsionnykh tekhnologii (Herald of computer and information technologies), 6: 44-49.

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev and V.L. Kurbatov, 2014b. Analysis of the single session access model in the distributed portal network of the interacting parties of the informational space. Res. J. Appl. Sci., 9 (11): 771-773.

Lazarev, S.A., O.A. Ivashchuk, I.S. Konstantinov and K.A. Rubcov, 2014c. Mechanism of Information Exchange Management within Portal Network of Environmental Monitoring Subjects. Intl. J. Appl. Eng. Res., 9 (22): 16789-16794.

Lazarev, S.A. and A.V. Demidov, 2010. The concept of network information exchange management creation for corporate portals. Information Syst. Technol., 4 (60): 123-129.

Lazarev, S.A. and A.V. Demidov, 2012. Features of a subsystem development for the system access management in respect of information exchange of corporate portal network. Information Syst. Technol., 4 (72): 103-110.

Lazarev, S.A., I.S. Konstantinov, O.V. and P.P. Silaev, 2013. Multifactor security user authentication subsystem in the enterprise portals using universal digital access key. Vestnik komp'iuternykh i informatsionnykh tekhnologii (Herald of computer and information technologies), 11: 55-60.

Taggera, B., D. Trossena, A. Kostopoulosb, S. Porterc and G. Parisisa, 2013. Realizing an application environment for information-centric networking. Computer Networks, 57 (16): 3249-3266.

Wiesmann, M., F. Pedone, A. Schiper B. Kemme and G. Alonso, 2000. Understanding replication in databases and distributed systems. Proceedings 20th IEEE International Conference on Distributed Computing Systems, pp: 464-474.

Gutzmann, K., 2001. Access control and session management in the HTTP environment. IEEE Internet Computing, 5 (I.1): 26-35.

Birget, J.C., Xukai Zou, G. Noubir and B. Ramamurthy, 2001. Hierarchy-based access control in distributed environments. Proceedings ICC2001 IEEE Intl. Conferenceon Communications, 2: 229-233.

Chashin, J.G., I.S. Konstantinov and S.A. Lazarev, 2014. Simulation of the software-defined network for a high-performance computing cluster. Res. J. Appl. Sci., 9 (10): 704-706.