Research Journal of Applied Sciences 9 (11): 771-773, 2014
ISSN: 1815-932X

Analysis of the Single Session Access Model in the Distributed Portal Network of the Interacting Parties of the Informational Space

[1]Igor Sergeevich Konstantinov, [1]Sergej Aleksandrovich Lazarev,
[1]Oleg Vladimirovich Mihalev and [2]Vladimir Leonidovich Kurbatov
[1]Belgorod State National Research University, St. 85 Pobedy, 308015 Belgorod, Russia
[2]North Caucasian Branch Bstu after V.G. Shukhov, St. 24 Zheleznovodskay, Mineral Water, 357202 Stavropol Territory, Russia

Abstract: This study considers the mechanism of a single session of access by a particular user within the entire distributed network of the enterprise portals. The implementation of this model of the session access ensures the single user authentification in the portals network no matter which nodes were accessed at first and further on. Therefore, only a single random point is determined for the user access to the portals network.

Key words: Portals network, session access model, user authentification, single session of access, access control, information associations

INTRODUCTION

The research in the area of designing of information associations within the global informational space on the basis of enterprise portals (Lazarev, 2012) which includes solving the tasks of designing the automated information systems for industrial complexes management (Konstantinov and Ivaschuk, 2013) determined the necessity of implementation of the single model of the session access within the specified network. The concept of constructing a network of portals and its distributed nature suggest the secured authorized information exchange (Lazarev and Demidov, 2010, 2012) between the users belonging to the different domain groups and different information portals integrated in a network. This is why by accessing to resources of the different information sites (portals) the access control subsystem of the relevant site needs to identify the user for the purpose of authorization (Konstantinov *et al*., 2013). Consequently, the information site shall ask the user to enter his authentification data which is quite natural at the primary access to the network resources but is totally unacceptable with regard to convenience of the use, for an already authorized user if each addressing to another network information site will require re-authentification. An alternative solution is the mechanism of validation of the user session from the other information site that had authenticated this user before. But in order to do that it is needed to maintain interactions with all the other network nodes by implementing the full-mesh logical topology which takes much efforts and costs (Tagger *et al*., 2013; Olifer and Olifer, 2002; Wiesmann *et al*., 2000) with regard to the use of the computing and network resources. It is obvious that some centralized mechanism of implementation of the single user session in the portals network and unambiguous user identification in each of its segments is required. These requirements determine the urgency of the specified issue.

PROCEDURE

Traditionally, the session access (user session) mechanisms are used for control of the user activity in the multi-user software systems which includes the user identification and authentification within the frameworks of the session running (Konstantinov *et al*., 2014; Gutzmann, 2001). A user session is a virtual connection that is accurately attached to a definite system user. Each session has a temporary identifier a name that is used in order to obtain the system user identifier and additional session information and certain lifetime a period during which the session is considered to be active and participates in coordination of the system operation. For the assignment of the session identifier the authentification process shall be completed.

By designing of the mechanisms of the user session support within the enterprise portals network it was observed that implementation of the procedure of the compulsory user authentification at the stage of establishing connection with each new network node is

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

an inefficient and inconvenient solution with regard to the end user and the information exchange process itself. Therefore, we have examined the possibility of centralizing the user authentification process with the further replication of the session data. In the simplest case authentification is performed at the central node and the dataset containing the user session record is replicated to the other read-only network nodes. Such, method is called replication and is used in the most information systems where the writing operations are quite rare as compared to the data retrieval operations (Birget *et al*., 2001).

It should be noted that such model features an apparent error: In case of non-availability of the central server as the result of the hardware or software failure the system is unable to accept the new connections, the denial of service takes place.

Another possible approach to the organization of the data replication model and topology of connections between the system nodes is the active replication which suggests that the session data may be recorded at the few peer nodes of the distributed network. In the last case the fully connected interaction with the degree that equals to N(N-1)/2 takes place which requires extensive resources for arrangement of the relevant logical topology (Taggera *et al*., 2013). It is obvious that the most rational in terms of reliability and fault tolerance of the portals network as well as in terms of the costs required will be some hybrid engineering solution using the mechanisms of both the passive and active replication of session data, as well as communication between the nodes of the network performing recording, storage and reading of this information.

MAIN PART

From the formal perspective a network of portals may be defined as:

$$P=\langle A, C, D\rangle \quad (1)$$

Where:

A = $\{a_i\}$ set of the access control nodes, $i=\overline{1,n}$

C = $\{c_j\}$ set of the network control nodes, $j=\overline{1,m}$

D = $\{d_i\}$ is the set of the user network domains

A uniquely named user group is described by a domain represented by a tuple:

$$d_i=\langle U_i, D_i'\rangle \quad (2)$$

Where:

U_i = Set of users of the i-th domain, $i=\overline{1,n}$

D_i' = Subset of the networks domains which the domain d_i, $D_i'\subseteq D$ and $d_i\in D_i'$ trusts

At the same time each user domain corresponds to a particular network access control node and vice versa, $A\leftrightarrow D$ and in d_i there is a subset of the users $U_i'\subseteq U_i$ authorized at the current moment t. The network control node is represented by the tuple:

$$c_j=\langle S^0, R^0, D\rangle \quad (3)$$

Where:

S^0 = Set of all active user sessions in the portals network

R^0 = Set of all identified requests in the network

The equality $c_1 = c_2 = ... = c_m$ ensures the replication and distribution of the network control functions between the nodes. The access control node is represented by the tuple:

$$a_i=\langle S_i, R_i, D_i'\rangle \quad (4)$$

where,

S_i = Set of active user sessions at the access control node

R_i = Set of the identified requests to the access control node

Implementation of the mechanism of the single user session within a portal network suggests that at the access control node a_i there is a session $s_{ik}\,(k=\overline{1,l})$ by which the authorized user u_{qz}' is identified that belongs to the domain d_q included in the list of the trusted domains of this node, i.e., the session access model satisfies the following condition:

$$\forall a_i:\exists s_{ik}\in S_i; u_{qz}'\in U_q'; d_q\in D_i'\Rightarrow T: s_{ik}\rightarrow u_{qz}' \quad (5)$$

Where:

u_{qz}' = The zth authorized user of the q-th domain, $z=\overline{1,l}, q=\overline{1,n}$

T = The user-to-the-session function

Similarly, the unauthorized users of the q-th domain $\overline{U_q}\,(U_q')$ may also be authorized only at the network node a_i that trusts the domain $d_q\in D_i'$. A request by the portal network user is considered to be identified if it is possible to identify the requester on the basis of (Eq. 5) by the active session:

$$\forall r_{ikx}\in R_i:\exists s_{ik}\in S_i\Rightarrow E: r_{ikx}\rightarrow s_{ik} \quad (6)$$

Where:

r_{ikx} = The xth request to the i-th node containing the tag of the kth user session, $x=\overline{1,y}$

E = The function of the user session identification by the request

Otherwise in respect of the unidentified requests a user needs to pass the authentification. The distributed structure of the system and peculiar features of the construction thereof suggest that for the support of the user session and unambiguous identification of his requests the session data corresponding to the request shall be available either at the node addressed or at the central node of the system. This is why a user session at the access node s_{ik} may represent a replica of the user session at the network control node s^0_{jk}, since:

$$S^0 = \bigcup_{i\in I} S_i, R^0 = \bigcup_{i\in I} R_i \Rightarrow \exists s_{ik} S_i \equiv s^0_{jk} \in S^0, \quad \exists r_{ikx} \in R_i \equiv r^0_{jkx} \in R^0 \tag{7}$$

Thus, upon unavailability of the portal network control nodes for the purpose of identification of the user session (Eq. 6) the session data available at the access control node processing the request suffices. According to the specifics of operation of the portal network and user session management (prevalence of the reading operations) the hybrid approach to the session data propagation management is implemented active replication from the common nodes to the central one and the passive replication in the opposite direction. At the same time the sessions at the common network nodes may only be created in case of failure of the central node in the mode of hot swapping of the authentification source. Such, configuration assures the fast and effective propagation of the session data and high accessibility of the system as a whole.

DISCUSSION

It should be noted that this study substantiates the necessity of constructing a single model of session access in a distributed portal network. Various approaches to the session data management in distributed networks have been considered. The hybrid approach to the user session management has been proposed and the formal description of the single session access model for a distributed portal network has been provided.

CONCLUSION

Implementation of the proposed session access model enables the single user authentification and using a single random point of access to the distributed portal network no matter which network nodes were accesses at first and further on, even upon non-availability of the central network node.

REFERENCES

Birget, J.C., X. Zou, G. Noubir and B. Ramamurthy, 2001. Hierarchy-based access control in distributed environments. Proceedings of the IEEE International Conference on Communications, Volume 1, June 11-14, 2001, Helsinki, Finland, pp: 229-233.

Gutzmann, K., 2001. Access control and session management in the HTTP environment. IEEE Internet Comput., 5: 26-35.

Konstantinov, I.S. and O.A. Ivaschuk, 2013. Approaches to creating environment safety automation control system of the industrial complex. Proceedings of the IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, Volume 2, September 12-14, 2013, Berlin, Germany, pp: 828-832.

Konstantinov, I.S., S.A. Lazarev and O.V. Mihalev, 2014. [Realization of a single model session access in the distributed network portals]. Herald Comput. Inform. Technol., 6: 44-49, (In Russian).

Konstantinov, I.S., S.A. Lazarev and P.P. Silaev, 2013. [Multifactor security user authentication subsystem in the enterprise portals using universal digital access key]. Herald Comput. Inform. Technol., 11: 55-60, (In Russian).

Lazarev, S.A. and A.V. Demidov, 2010. [The concept of construction of a control system of an information exchange in the network of corporative portals]. Inform. Syst. Technol., 4: 123-129, (In Russian).

Lazarev, S.A. and A.V. Demidov, 2012. [The features of building access control subsystem of management information exchange network for corporate portals]. Inform. Syst. Technol., 4: 103-110, (In Russian).

Lazarev, S.A., 2012. [Some aspects of the information associations creation in the global networks based on a network of corporate portals]. Inform. Syst. Technol., 1: 103-106, (In Russian).

Olifer, V.G. and N.A. Olifer, 2002. [Network Operating Systems]. Peter Publisher, St. Petersburg, Russia, ISBN: 5-272-00120-6, Pages: 544, (In Russian).

Tagger, B., D. Trossen, A. Kostopoulos, S. Porter and G. Parisis, 2013. Realising an application environment for information-centric networking. Comput. Networks, 57: 3249-3266.

Wiesmann, M., F. Pedone, A. Schiper, B. Kemme and G. Alonso, 2000. Understanding replication in databases and distributed systems. Proceedings of the IEEE 20th International Conference on Distributed Computing Systems, April 10-13, 2000, Taipei, Taiwan, pp: 464-474.