Journal of Engineering and Applied Sciences 11 (Special Issue 2): 3290-3293, 2016
ISSN: 1816-949X

Group Policies Control of Access in the Closed Virtual Environment of the Distributed Information Resources Organization

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

Abstract: In this study, the description of the implementation mechanism for access control model (user authorization) is provided to resources of the closed distributed information environment in the form of enterprise portal network on the basis of group policies and a uniform user session.

Key words: Access control, group policies, access models, user authorization, the distributed information resources, a portals network, the closed virtual environment

INTRODUCTION

The task of creating safety infrastructure of the Distributed Information Environment (DIE) in the form of enterprise portal network assumes implementation of a uniform access control policy for resources on the basis of forming uniform hierarchy of user groups.

Portals network as the mechanism having uniform entry point and providing a uniform policy of access demarcation for users and administrators is described in operations (Lazarev and Demidov, 2010; Konstantinov *et al*., 2014a, b; Konstantinov *et al*., 2015) and represents set of the access monitoring nodes integrated in a single network with the control center of portals (TUS). Within TUS the uniform control policy of information exchange including a possibility of the authorized access to the protected information resources of all network, the uniform mechanism of control of the user session providing the necessary security level is implemented.

In operations (Lazarev and Demidov, 2012; Lazarev *et al*., 2015a, b) applicable models of access to information resources were analyzed. As the fundamental mechanism it was offered to use modification of discretionary model of access.

MATERIALS AND METHODS

Problem definition (model of access to resources): The traditional discretionary model of access control to information resources conforms to the following requirements:

- All entities (including subjects) shall be identified, i.e., the unique identifier shall be appropriated to each entity
- The access matrix which every line corresponds to the subject, cell is set contains the access rights list of the subject to an entity representing a subset of a set of the exercised access rights
- The subject has right of access to an entity only in that case when the cell of a matrix of accesses to the appropriate subject and an entity, contains this right of access

Being repelled from listed, we will create model of an access control system of safety infrastructure of the distributed information resources. The access control system can be defined as:

$$S = (C, N, R, U, D, G) \quad (1)$$

Where:

$C = \{C_K\}, k \in (l, n_C)'$ = Set of control centers

$N = \{N_K\}, k \in (l, n_N)'$ = Set of nodes of a network and specific node of a network

$$N = (R', U', D', G') \quad (2)$$

Let us, define the basic concepts within implementation for access control model to information resources according to the leading document of the state technical commission in case of the Russian president "protection against illegal access to information. Terms and determination".

Corresponding Author: Igor S. Konstantinov, Belgorod State University, Pobeda St., 85, 308015 Belgorod, Russia

The access object is unit of an information resource of automated system, access to which is regulated by rules of access demarcation. The subject of access is the person or process which actions are regulated by rules of access demarcation. Within model of access control it is necessary to define couple authorization relation the subject of access-access object, the setting explicit and unambiguous compliance. Objects of a group policy of access are provided by a set of information resources:

$$R = \{r_k\}, k \in (1, n_R)' \quad (3)$$

Where:

r_k = Information resource

n_R = Quantity of information resources with which the system operates

Subjects of a policy are defined by a great number of users of system:

$$U = \{u_k\}, k \in (1, n_U)' \quad (4)$$

Where:

u_k = User

n_U = The number of the users registered in system

RESULTS AND DISCUSSION

The user of system the person or the technical device which can send system requests through telecommunication channels traditionally is considered and receive from it the response in the form of provision of access to a certain resource or a failure in that. Within system it is considered that the user is a member of one (and only one) the organization which is a part of a portals network. For the external users who aren't belonging any of such organizations the additional dummy organization is entered. Each unregistered user in system is considered the member of this dummy organization and all such users are equivalent and have the lowest access level. The great number of the users registered in system as members of one of the supported organizations form the domain of users. The domain of users is fixed behind the control center and is operated by his administrator. In essence control centers play a role of the AAA servers providing storage of authentication and other these users of the domain. Each user of system is associated with the user domain from a set:

$$D = \{d_k\}, k \in (1, n_D)' \quad (5)$$

Where:

d_k = User domain

n_D = The number of the user domains registered in system

For control of access rights users shall be integrated in groups according to organizational hierarchy of the enterprise on departments, branches, services, etc., and nodes of a network are obliged to support an urgent status of information on these communications. Following this purpose, each information resource and each user domain are associated with specific group of privileges of a set:

$$G = \{g_k\}, k \in (1, n_G)' \quad (6)$$

Where:

g_k = Group of privileges

n_G = The number of groups of the privileges registered in system

Then subjects and access objects can be determined by tuples:

$$\forall u_k \in U: u_k = (i_k^U, d_i, g_j) \quad (7)$$

where, $I_U = \{i_k^U\}, k \in (1, n_U)'$ set of identifiers of users:

$$\forall r_k \in R: (i_k^R, g_i) \quad (8)$$

where, $I_R = \{i_k^R\}, k \in (1, n_R)'$ set of identifiers of information resources of system. At the same time there is a relation F_A, defining address enable of the user to a resource:

$$\exists F_A: U \times R \rightarrow \{true, false\} \quad (9)$$

The model of selective access control (Discretionary Access Control, DAC) allows operation of the user u over an information resource r, if the group $g_i \in u$ coincides with the group $g_j \in r$.

However, for the organization of opportunities of control of group policies of access it is expedient to define an order of inheritance of access between groups of privileges. For this purpose it is necessary to present their hierarchy in the form of the oriented graph in which each group of privileges corresponds to peak and arcs define hereditary communications:

$$\forall g_k \in G: g_k = (i_k^G, G_k) \quad (10)$$

Where:

i_G = $\{i_k^G\}$

$k \in (1, n_G)$ = Set of identifiers of groups of privileges

$G_k \subset G$ = Great number of heritable groups of privileges

Bypass of a graph will create a set $G\sim \subseteq G$. Access for the user u to an information resource r it will be resolved if a product of sets G~i, the graph of hierarchy of group of privileges received in case of bypass $g_i \in u$ and G~j, the graph of hierarchy of group of privileges received in case of bypass $g_j \in r$, isn't an empty set.

In view of the distributed nature of system it is necessary to enter a row of restrictions into the concept of inheritance of groups of privileges. Besides, having an ultimate goal creating a flexible access control mechanism, it is necessary to select distinction of hereditary communications between groups:

$$\forall g_k \in G: g_k = \{i_k^G, D_k, G_k, G'_k\} \quad (11)$$

Where:

$D_k \subseteq D$ = Set of the user domains resolved for group

$D_k \subseteq D$ = Great number of groups of privileges, switched on in inheritance hierarchy

$D'_k \subseteq G$ = Great number of the groups of privileges excluded from an inheritance hierarchy

The including communications allow to inherit address enables of groups of privileges, switched on in hierarchy. The excluding communications realize a possibility of an exception of groups of privileges of an inheritance hierarchy without the need for modification of parent peaks. In a general view it is possible to describe the relation F_G, defining finite subset $G^{\sim} \subseteq G$:

$$\frac{k\ (G_i F_G(g_k)}{F_G(g_i) = \{g_i\} U\left(k|G'_i\ F_G(g_k)\right)} \quad (12)$$

Then relation F_A, defining address enable of the user u to an information resource r is:

$$F_A(u, r) = \begin{cases} \text{true, } \Pi p N И F_G(g_u) \bigcap F_G(g_r) \neq \phi И d_u \in D_r; \\ \text{false, } \Pi p И F_G(g_u) \bigcap F_G(g_r) \neq \phi И Л \pi d_u \in d_r \end{cases} \quad (13)$$

By means of introduction of binary coding of elements, resource-intensive operations over sets can be reduced to operations over tag values (Lazarev *et al*., 2014). Using character representation of tag functions and having taken the user's belonging to group of privileges for some predicate $\varepsilon(u, g)$ and the user's belonging to the user domain for some predicate $\delta(u, g)$, let us make the logic diagram defining address enable according to the described principles:

$$\begin{aligned} F^{\sim}_G(u_i, g_j) &= \varepsilon(u_i, g_j) V (G_j F^{\overset{k}{\sim}}_G (u_i, g_k) \\ &\quad \Lambda(\square)' G'_j F^{\sim}_G (u_i, g_k)), \\ F^{\sim}_A(u_i, r_i) &= (D_r, \delta(^k u_i, d_k)) \Lambda F^{\sim}_G (u_i, g_r) \end{aligned} \quad (14)$$

Summary: The approach considered in article formed a basis for implementation of an algorithm of user authorization of the closed distributed information environment in the form of a portals network. As the fundamental implementation mechanism of an algorithm of user authorization modification of discretionary model of access is used. Development of an effective algorithm of user authorization demanded adaptation of an algorithm of the simplified authentication of users for implementation of group policies of access control.

CONCLUSION

Access for the user to an information resource will be allowed if it belongs to one of groups of the privileges which are present at an inheritance hierarchy and its user domain is the allowed for group of privileges of a root of a graph.

ACKNOWLEDGEMENTS

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

REFERENCES

Konstantinov, I.S., S.A. Lazarev and O.V. Mihalev, 2014a. [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, 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: 771-773.

Konstantinov, I.S., S.A. Lazarev and P.P. Silaev, 2015. Safety mechanism for multi-factor authentication with digital access key use in closed virtual environment of distributed information resources. Intl. J. Appl. Eng. Res., 10: 44927-44932.

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. Features of a subsystem development for the system access management in respect of information exchange of corporate portal network. Inf. Syst. Technol., 4: 103-110.

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev and V.E. Kiselev, 2015a. Implementation of unified session access model in a closed virtual environment of distributed information and computing resource system as a secured portal network. Res. J. Applied Sci., 10: 629-632.

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev, A.V. Demidov and R.V. Shateev, 2015b. The development of infrastructure security for distributed information computer environment based on secured portal network. Int. J. Applied Eng. Res., 10: 38116-38120.

Lazarev, S.A., O.A. Ivashchuk, I.S. Konstantinov and K.A. Rubcov, 2014. Mechanism of information exchange management within portal network of environmental monitoring subjects. Int. J. Appl. Eng. Res., 9: 16789-16794.