ISSN 0146-4116, Automatic Control and Computer Sciences, 2018, Vol. 52, No. 8, pp. 1124–1126. © Allerton Press, Inc., 2018.
Original Russian Text © S.V. Belim, S.Yu. Belim, 2018, published in Problemy Informatsionnoi Bezopasnosti, Komp'yuternye Sistemy.

Implementation of Mandatory Access Control in Distributed Systems

S. V. Belim[a], * and S. Yu. Belim[a]

[a] *Dostoevsky Omsk State University, Omsk, 644077 Russia*

**e-mail: BelimSV@omsu.ru*

Received March 12, 2018

Abstract—The implementation of mandatory distribution of access in distributed systems taking into account a user hierarchy is considered. The access control is based on the scheme of preliminary key distribution similar to KDP-scheme. The algorithm of building a family of subsets taking into account a user hierarchy was developed.

Keywords: mandatory access control, preliminary key distribution, KDP-scheme, user hierarchy

DOI: 10.3103/S0146411618080357

1. INTRODUCTION

The mandatory access control is widespread in computer systems and is more reliable than discretionary access control, as it makes it possible to block the channels of information leakage "by memory." However, implementation of this security policy in distributed systems faces a number of difficulties [1]. In a local computing system it is sufficient to appropriate to each user a label of access level, which is then written into the attributes of generated by him processes and files that he creates. When a request for access comes, the security subsystem compares the labels of access levels. In the distributed computing system, such scheme turns out to be inoperative due to ideology of a system building, as there is no a centralized scheme of access permission [2, 3]. In this regard, it is necessary to develop distributed algorithms of access control. The approach based on access certificates is one of the possible decisions. In this case, the server of release and validation of certificates plays a role of security subsystem. However, when there are a large number of accesses, the server load increases that leads to system retardation and reduction of its stability.

Qualitatively different algorithms can be built based on the schemes of preliminary key distribution. In this case, the server role is reduced to release of key materials. The network subscribers generate the keys of information exchange independently. The main problem is that the widely known schemes of preliminary key distribution [4, 5] provide a polygrid information exchange. To take into account the security policy of the system, it is necessary to make a modification of such schemes. The modification of Blom's scheme of preliminary key distribution taking into account forbidden channels was proposed in [6]. The arrangement of simplex channels for the same scheme is implemented in [7]. The decision of similar problem based on a KDP-scheme was proposed in [8, 9]. These works are aimed at implementing a discretionary security policy. A mandatory security policy requires taking into account the hierarchy of both subjects and objects. One of the decisions based on hash-functions was proposed in [10–12]. However, this approach does not make it possible to implement the exchange between users taking into account the hierarchy.

The objective of this work is development of a scheme of preliminary key distribution, which makes it possible to implement the mandatory security policy in distributed computing systems.

2. PROBLEM STATEMENT AND KEY DISTRIBUTION SCHEME

Let us consider the distributed system with a set of users U. We will assume that at set U an ordering relation is given, leading to user hierarchy, which has a tree structure. If the hierarchy of user u_i is higher than the hierarchy of user u_j, then we will write $u_i > u_j$. It should be noted that the tree hierarchy of users implies the possibility of situation, in which two users are not comparable, as they are at different branches

of hierarchical tree. In this case, we will write $u_i <> u_j$. The mandatory security policy permits information flows only upwards. This means that for two users $u_i > u_j$, the information flow is possible only from u_j to u_i, but in the opposite direction it is impossible. If two users are incomparable, then the information flow between them is also impossible.

Thus, it is stated the problem of building such a key scheme, which would make it possible to exchange information only between users merely in accordance with the hierarchical subordination. To decide this problem, we will build the scheme of preliminary key distribution, which makes it possible to generate the key of message transmission only for permitted directions of information flows.

We will try the solution of this problem by analogy with KDP-scheme of preliminary key distribution. The usual KDP-scheme is that there is a common set of key materials $K = \{k_1, ..., k_n\}$ that is sent out to all users by secure channel before the scheme starts to operate. Next, a system of subsets $S = \{S_1, ..., S_m\}$ of set $\{1, ..., n\}$ is formed, where m is the number of users of the system. Set S is stored in a public access. If user u_i wants to connect with user u_j then he extracts subsets S_i and S_j from set, then he computes their intersection $S_{ij} = S_i \cap S_j$. The common exchange key is generated based on the elements of set of key materials K, the numbers of which place within S_{ij}:

$$k_{ij} = \oplus k_l \ (l \in S_{ij}).$$

User u_j in order to read the message performs the same set of operations and receives the identical key.

This scheme cannot be used directly, as it makes it possible to connect each user with each user, and that the information exchange channels will be bilateral. At first, we modify the scheme so that the information transmission channels are unilateral. For that, it is necessary to require the asymmetry of paired keys by the permutation of indices $k_{ij} \neq k_{ji}$. We will use, as in the usual KDP-scheme, a set of key materials K, and some set of subsets S. The key of transmission of information from user u_j to user u_i we will calculate based on the difference of sets:

$$\Delta S_{ij} = S_i \backslash S_j.$$
$$k_{ij} = \oplus k_l \ (l \in \Delta S_{ij}).$$

The requirement of asymmetry of the keys, obviously, will be fulfilled. Each user u_i ($i = 1, ..., m$) to reading the messages uses keys k_{ij} ($j = 1, ..., m$), and to encrypt the messages he uses keys k_{ji} ($j = 1, ..., m$). At that, the symmetric encryption algorithms are used.

For implementation of mandatory security policy it is necessary to require that for forbidden transmission channels the condition $k_{ji} = 0$ was fulfilled, i.e., $\Delta S_{ij} = \varnothing$. This requirement is a restriction on the possibility to build the set of subsets S.

The traditional KDP-scheme is built based on Sperner families. A family of subsets $D = \{D_1,...,D_n\}$ such that if $D_i \cap D_j \subseteq D_t$, then either $t = i$ or $t = j$. is named Sperner family [8]. The family of sets S is built based on the Sperner family D [9]. The elements of Sperner family D_i are used as intersections of subsets S_{ij}. We use a similar approach to solving the stated problem of arrangement of access for the systems with user hierarchy. Let us build the Sperner family by the number of users $D = \{D_1, ..., D_m\}$. We will create set S, moving over the tree of user hierarchy. Let us select the users corresponding to leaf knots of tree $u_1, ..., u_l$, where i is the number of leaf knots of tree. The corresponding elements of set S will be determined by the elements of the Sperner family:

$$S_i = D_i \ (i = 1,\ldots,l).$$

Next, we perform a recursive tree walk. If knot u_i has the nearest childrens $u_{i1}, ..., u_{ik}$, then to this user the set corresponds:

$$S_i = S_{i1} \cup S_{i2} \cup \ldots \cup S_{ik} \cup D_i.$$

With this algorithm of building, it is obviously that if u_i dominates u_j, then $S_i \supset S_j$, and therefore $S_i \backslash S_j \neq \varnothing$, whereas $S_j \backslash S_i = \varnothing$. Thus, generation of the key is possible only for one direction of information transmission. In addition, it is easy to show that in the case $u_i <> u_j$ the equalities $S_j \backslash S_i = \varnothing$ and $S_i \backslash S_j = \varnothing$ will be fulfilled too.

3. CONCLUSIONS

The proposed in this work scheme makes it possible to implement the preliminary distribution of the keys of symmetric encryption for distributed systems with user hierarchy. As in the case of KDP-scheme,

the Sperner families are used. However, usual KDP-scheme makes it possible to form bidirectional channels of information exchange, while the proposed scheme is focused to the simplex channels of information exchange. It should be noted that the proposed modification of the scheme of preliminary key distribution does not lead to increasing the amount of key materials that it is compulsory condition to using this approach to building secure systems.

REFERENCES

1. Vasiliev, Y.S., Zegzhda, P.D., and Zegzhda, D.P., Providing security for automated process control systems at hydropower engineering facilities, *Thermal Eng.*, 2016, vol. 63, no. 13, pp. 948–956.
2. Konoplev, A.S. and Kalinin, M.O., Access control method in distributed grid computing networks, *Autom. Control Comput. Sci.*, 2015, vol. 49, no. 8, pp. 679–683.
3. Kalinin, M., Krundyshev, V., Rezedinova, E., and Zegzhda, P., Role-based access control for vehicular adhoc networks, *IEEE International Black Sea Conference on Communications and Networking*, *June 4–7, 2018, Batumi*, 2018. doi 10.1109/BlackSeaCom.2018.8433628
4. Blom, R., An optimal class of symmetric key generation systems, *Proc. 84 EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, 1985, pp. 335–338.
5. Mitchell, C.J. and Piper, C., Key storage in secure networks, *Discrete Appl. Math.*, 1988, vol. 21, pp. 215–228.
6. Belim, S.V., Belim, S.Yu., and Polyakov, S.Yu., Implementation of discretionary access sharing using a modified Blom scheme for preliminary key distribution, *Probl. Inf. Bezop., Komp'yut. Sist.*, 2015, no. 3, pp. 72–76.
7. Belim, S.V. and Belim, S.Yu., Modification of the scheme for preliminary distribution of Blom keys with regard to simplex channels, *Probl. Inf. Bezop., Komp'yut. Sist.*, 2017, no. 3, pp. 82–86.
8. Belim, S.V. and Belim, S.Yu., KDP scheme of preliminary key distribution in discretionary security policy, *Autom. Control Comput. Sci.*, 2016, vol. 50, no. 8, pp. 777–786.
9. Belim, S.V. and Belim, S.Yu., The VPN implementation on base of the KDP-scheme, *CEUR Workshop Proc.*, 2016, vol. 1732. http://ceur-ws.org/Vol-1732/paper3.pdf.
10. Belim, S.V. and Bogachenko, N.F., Distribution of cryptographic keys in systems with a hierarchy of objects, *Autom. Control Comput. Sci.*, 2016, vol. 50, no. 8, pp. 773–776.
11. Dyer, M., Fenner, T., Frieze, A., and Thomason, A., On key storage in secure networks, *J. Cryptol.*, 1995, vol. 8, pp. 189–200.
12. O'Keefe, C.M., Applications of finite geometries in information security, *Australas. J. Comb.*, 1993, vol. 7, pp. 195–212.

Translated by M. Kromin