Implementation of Access Control Models Based on Key Pre-Distribution Schemes

Sergey V. Belim [1,2]
[1]Omsk State Technical University
11 Mira avenue, 644050, Omsk, Russia
[2]Siberian State Automobile
and Highway University
5 Mira avenue, 644080, Omsk, Russia
sbelim@mail.ru

Svetlana Yu. Belim
Omsk State Technical University
11 Mira avenue, 644050, Omsk, Russia
svbelim@gmail.com

Abstract

The paper proposes the implementation of discretionary access control in distributed systems. Modification the pre-distribution scheme for symmetric encryption keys is performed. Discretionary security policy is implemented as a ban on some information channel. Blom's and KDP key pre-distribution schemes are modified to implement ban channels. The developed scheme allows to calculate the encryption key for permitted channels. The encryption key is zero for disallowed channels.

1 Introduction

In distributed information systems, secure communication between subscribers is implemented using encryption of communication channels. The encryption key exchange problem occurs in this case. Public key encryption algorithms can provide such secure communication. But they require more computing resources and work slowly.Therefore, symmetric encryption schemes are very common. Pairwise key schemes are used to maximize information protection. These schemes use their own key for each subscriber pair. This approach creates additional difficulties in storing and using keys for systems with a large number of subscribers. There are also problems with the scalability the network. Key pre-distribution schemes are used for such systems. In these schemes, the key distribution server sends private key materials to network subscribers via secure channels. Additional subscriber information is in the public domain. Encryption keys are computable. The encryption key is calculated on the basis of closed key materials and open information about subscribers.

The existing key pre-distribution schemes are based on the principle of enabling each subscriber to interact with each. However, in most distributed systems, there are restrictions on the transmission of information. As a rule, such restrictions are presented in the form of a ban on the interaction for some subscriber pairs. Such a security policy may be represented as a discretionary access control access matrix.

Two key pre-distribution schemes have become most common: the Blom's scheme [1] and the KDP-scheme [2]. These two schemes use a different mathematical approach. The Blom's scheme is based on calculating the values for symmetric polynomial over a finite ring. The KDP-scheme uses finite sets. Blom's scheme is widely

In: Sergei S. Goncharov, Yuri G. Evtushenko (eds.): Proceedings of the Workshop on Applied Mathematics and Fundamental Computer Science 2020 , Omsk, Russia, 30-04-2020, published at http://ceur-ws.org

used to secure wireless networks [3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. The KDP-scheme is mainly used in networks that allow subnetwork partitioning [13, 14, 15].

The authors have previously modified the key pre-predistribution scheme for mandatory access control [16, 17] and for system with simplex information channels [18, 19, 20].

2 The Blom's scheme modification

We are looking at a distributed network with n subscribers. Setting of task consists in organization of secure interaction of network subscribers. Additional conditions are imposed on the interaction of network members. Some subscribers pairs are not allowed to exchange information. For allowed subscriber pairs, messages are exchanged using data encryption. All authorized information channels are two-way. Strict recording this access control is carried out using the access matrix. Rows and columns correspond to network subscribers. The access matrix cells contain one if the channel is allowed and zero if the channel is denied. The task is to generate and distribute closed key materials in such a way that for allowed channels both parties can calculate a common encryption key, and for banned channels the encryption key is zero. We're putting a limit on the length of the key. The key must be m bits long.

In the basic Blom's scheme [1], the key distribution server generates a symmetric polynomial $f(x, y)$ of degree $2l$ with random coefficients. All calculations are performed on the deduction ring Z_M. This polynomial is stored in secret on the key generation server and is used to generate key materials. Polynomial degree restrictions are associated with the number of subscribers in the network. If the number of participants is n, then inequality must be performed for the polynomial degree $l < n$. In addition to secret key materials, the scheme uses open information that is provided by the key distribution server at the subscribers request. The server generates a unique number r_i $(i = 1, ..., n)$ for each network subscriber. The numbers r_i $(i = 1, ..., n)$ are open. Secure key materials are produced individually for each subscriber. In this scheme, the key materials for the user u_i is the polynomial coefficient vector $g_i(x) = f(x, r_i)$. Secret key materials are transmitted via a secure channel. The value for the function $g_i(x)$ is calculated at the point r_j to generate the encryption key k_{ij} between the subscribers u_i and u_j $(k_{ij} = g_i(r_j))$. Subscriber u_j performs similar operation $(k_{ji} = g_j(r_i))$. The equality $k_{ij} = k_{ji}$ is executed because the polynomial $f(x, y)$ is symmetric. Both members of the information channel receive the same encryption key.

The main security problem of the key pre-distribution scheme is resistance to compromising. ompromising is the ability to obtain the remaining keys by a limited set of known pair encryption keys. The usual Blom scheme is resistant to compromising l keys[1].

. It is necessary that for permitted information channels $k_{ij} \neq 0$, and for banned $k_{ij} = 0$. A zero key encryption ban is set on the system. This automatically results the discretionary security policy.

We use the list L of subscriber pairs numbers (i, j), for which a ban on creating information channels has been introduced. The total number of ban information channels is denoted s. We are modifying the symmetric polynomial used to produce key materials. We use a polynomial $F(x, y)$ equal to the product of two symmetric polynomials.

$$F(x, y) = d(x, y)f(x, y). \tag{1}$$

$f(x, y)$ is arbitrary symmetric polynomial with degree $2l$.

The symmetric polynomial $d(x, y)$ satisfies a set of requirements.

$$d(r_i, r_j) = 0,\ d(r_j, r_i) = 0,\ for\ (i, j) \in L,\ and\ d(r_i, r_j) \neq 0,\ d(r_j, r_i) \neq 0, for\ (i, j) \notin L. \tag{2}$$

The polynomial $d(x, y)$ is equal to the product of the polynomials $d_{ij}(x, y) = 0$.

$$d(x, y) = \prod_{(i,j)\in L} d_{ij}(x, y). \tag{3}$$

The equality $d_{ij}(x, y) = 0$ is performed only under the condition $((x = r_i) \wedge (y = r_j)) \vee ((x = r_j) \wedge (y = r_i)) = 1$. From the requirement of symmetry for polynomials $d_{ij}(x, y)$ it follows that they are representative through elementary symmetric polynomials.

$$\sigma_1(x, y) = x + y, \quad \sigma_2(x, y) = xy. \tag{4}$$

A quadratic function with two roots satisfies the necessary requirements.

$$d_ij(\sigma_1, \sigma_2) = (\sigma_1(x, y) - \sigma_1(r_1, r_2))^2 + (\sigma_2(x, y) - \sigma_2(r_1, r_2))^2, \tag{5}$$

Substituting expressions for elementary symmetric polynomials, we obtain the representation the polynomial through the original variables.

$$d_{ij}(x, y) = (x + y - r_i - r_j)^2 + (xy - r_i r_j)^2. \tag{6}$$

We write an expression for the polynomial $d(x, y)$.

$$d(x, y) = \prod_{(i,j)\in L} \left((x + y - r_i - r_j)^2 + (xy - r_i r_j)^2\right). \tag{7}$$

Further work is carried out according to the usual Blom's scheme algorithm with the replacement the polynomial $f(x, y)$ to the polynomial $F(x, y)$. The degree of the polynomial $d(x, y)$ is determined by the total number banned information channels s.

$$deg\ d(x, y) = 4s. \tag{8}$$

Theorem 1. If the key pre-distribution scheme is based on the polynomial $f(x, y)$ of degree $2l$ and the number of banned information channels is s, then the scheme is resistant to compromising $l + 2s$ key materials.

Theorem 2. If the key pre-distribution scheme is based on the polynomial $f(x, y)$ of degree $2l$ and the number of banned information channels is s, then compromising the list of protected information channels is possible when compromising at least $l + 2s$ key materials.

3 The KDP-scheme modification

We consider solving the same problem using a modified KDP-scheme. In a common KDP scheme, the key distribution server sends out a key set $K = \{k_1, ..., k_m\}$ to all participants over secure channels. This key set is kept secret. A family of subsets $S = \{S_1, ..., S_n\}$ sets $\{1, 2, ..., n\}$ is stored in open form. Each member of this set family is mapped to one subscribers. If the user u_i initiates an information channel with the user u_j, then he asks the server subsets S_i and S_j. User u_i defines the set of elements included in the intersection of sets.

$$S_{ij} = S_i \cap S_j. \tag{9}$$

The set S_{ij} defines the element numbers of the set K used to calculate the pair encryption key. The encryption key is defined as a bitwise XOR operation applied to selected elements of the set K.

$$k_{ij} = \bigoplus_{l\in S_{ij}} k_l. \tag{10}$$

All operations are symmetrical, so both participants will receive the same pair key.

The discretionary security policy is described using the access matrix M. Rows and columns of this matrix are associated with network subscribers. The allowed data channels correspond to the unit values in the cells of the access matrix, and the forbidden values are zero. The elements of the subsets family S are selected so that at $M[i, j] = 0$, the equality $S_{ij} = \emptyset$ is fulfilled, and at $M[i, j] = 1$, $Sij \neq \emptyset$ is performed.

We use the auxiliary set of subsets D to build a family S with the desired properties. The number of elements in the set D is equal to half the number unit elements in the access matrix M. The matrix M is symmetric, therefore, we limit ourselves only to considering the elements above the main diagonal. The elements of the set D are constructed as disjoint subsets of the set $\{1, 2, ..., n\}$. The number of elements in $D = \{D1, ..., Dm\}$ is determined by the number of unit elements above the main diagonal in the matrix M. Enter an additional MD matrix over the set of subsets of the set $\{1, 2, ..., n\}$. The value of the elements is determined by the following rule: if $M[i, j] = 1$, then $MD[i, j] = D_k$, and $MD[j, i] = D_k$, if $M[i, j] = 0$, then $MD[i, j] = \emptyset$, and $MD[j, i] = \emptyset$. The sets S_i are determined based on the elements of the matrix MD arranged in the i-th row.

$$S_i = \bigcup_{j=1}^{n} MD[i, j], \quad (i = 1, ..., n). \tag{11}$$

A family of sets S built using such an algorithm meets the security policy requirements.

4 Conclusion

Modifications the Blom's and KDP key pre-distribution schemes allow the discretionary security policy implementation for distributed systems. The rights to create information channels are checked automatically when calculating encryption keys and do not require activation the centralized server. The disadvantage of the proposed system is an increase the key materials size in the Blom's scheme. Key materials contain additional information about banned information channels.

References

[1] R. Blom. An optimal class of symmetric key generation systems. *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*:335-338, 1985.

[2] C.J. Mitchell, . Piper. Key storage in Secure Networks. *Discrete and Applied Math*, 21:215–228, 1988.

[3] E. Shi, A. Perrig. Designing secure sensor networks. *IEEE Wireless Communications*, 11(6):38–43, 2004.

[4] Y. Liang, H. V. Poor, S. Shamai. Information Theoretic Security. *Found. Trends Commun. Inf. Theory*, 5:355–580, 2009.

[5] A. Parakh, S. Kak. Matrix based key agreement algorithms for sensor networks. *Fifth IEEE In-ternational Conference on Advanced Telecommunication Systems and Networks (ANTS)*:1–3, 2011.

[6] A. Rasheed, R. Mahapatra. Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks," *in IEEE Transactions on Parallel and Distributed Systems*, 22(1):176–184, 2011.

[7] W. Bechkit, Y. Challal, A. Bouabdallah, V. Tarokh. A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. *in IEEE Transactions on Wireless Communications*, 12(2):948–959, 2013.

[8] H. Chan, A. Perrig, D. Song. Random Key Pre-distribution Schemes for Sensor Networks. *IEEE Symposium on Security and Privacy*:197-213, 2003.

[9] Z. Yu, Y. Guan. A key pre-distribution scheme using deployment knowledge for wireless sensor networks. *IPSN 2005*:261–268, 2005.

[10] A. Rasheed, R. Mahapatra. An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks. *2008 IEEE International Performance, Computing and Communications Conference*:264–270, 2008.

[11] M. B. Paterson, D. R. Stinson. A unified approach to combinatorial key predistribution schemes for sensor networks. *Des. Codes Cryptogr.*, 71:433-457, 2014.

[12] K. Panyim, P. Krishnamurthy. A Hybrid Key Predistribution Scheme for Sensor Networks Employing Spatial Retreats to Cope with Jamming Attacks. *Mobile Netw Appl.*, 17:327-341, 2012.

[13] Y. Liu, M. Dong, K. Ota, A. Liu. ActiveTrust: secure and trustable routing in wireless sensor net-works. *IEEE Transactions on Information Forensics and Security*, 11(9):2013–2027, 2016.

[14] D. Zhao, K.-W. Chin, R. Raad. Approximation algorithms for broadcasting in duty cycled wire-less sensor networks. *Wireless Networks*, 20(8):2219–2236, 2014.

[15] X. Zheng, J. Wang, W. Dong, Y. He, Y. Liu. Bulk data dissemination in wireless sensor networks: analysis, implications and improvement. *IEEE Transactions on Computers*, 65(5):1428–1439, 2016.

[16] S.V. Belim, S.Yu. Belim. Mandatory access control implementation in the distributed systems. *Automatic Control and Computer Sciences*, 52(8):1124–1126, 2018.

[17] S.V. Belim, S.Yu. Belim. The modification of Blom's key predistribution scheme, taken into account simplex channels. *Automatic Control and Computer Sciences*, 52(8):1134–1137, 2018.

[18] S.V. Belim, S.Yu. Belim. Implementation of simplex channels in the Blom's keys pre-distribution scheme. *Journal of Physics: Conf. Series*, 1210:012008, 2019.

[19] S.V. Belim, S.Yu. Belim. Use the keys pre-distribution KDP-scheme for mandatory access control implementation. *Journal of Physics: Conf. Series*, 1210:012009, 2019.

[20] S.V. Belim, S.Yu. Belim. Vector key pre-distribution scheme. *Journal of Physics: Conf. Series*, 1441:012033, 2020.