A SECURE KEY COMPUTATION PROTOCOL FOR SECURE GROUP COMMUNICATION WITH PASSWORD BASED AUTHENTICATION

[1]Velumadhava Rao R*, [2]Vikhnesh ma*, [3]Kailash B*, [4]Selvamani K, and [5]Elakkiya R

[1,2,3]Department of Computer Science,
Rajalakshmi Institute of Technology, Chennai, India
velu_b4u@yahoo.com,
{vikhneshiva19,kailashdaskd}@gmail.com
[4]Department of Computer Science,
Anna University, CEG, Guidny, Chennai, India
smani@cs.annauniv.edu
[5]Department of Computer Science,
Jerusalem College of Engineering, Chennai, India
elakkiyaceg@gmail.com

ABSTRACT

Providing security in group communication is more essential in this new network environment. Authentication and Confidentiality are the major concerns in secure group communication. Our proposed approach uses an authenticated group key transfer protocol that relies on trusted key generation center (KGC). KGC computes group pair for each individual and transport the pair of values to all group members in a secured manner. Password based authentication mechanism is used to avoid the illegal member access in a group Also, the proposed approach facilitates efficient key computation technique such that only authorized group members will be able to computer and retrieve the secret key and unauthorized members cannot retrieve the key. The proposed algorithm is more efficient and relies on NP class. In addition, the distribution of key is also safe and secure. Moreover, the pair generated for the computation of key is also very strong since the cryptographic techniques are used which provides efficient computation.

KEYWORDS

Authentication, Confidentiality, Key Generation, Key Distribution

1. INTRODUCTION

Security in group communication encompasses authentication and confidentiality. To avoid the illegal users from accessing the group resources strong mutual authentication between entities should be guaranteed. Password-based authentication is extensively used because of its simplicity. Authorization provides a specific permission to a particular user on a specified resource. Message Authentication and Message Confidentiality are the two important security functions considered in most of the secure communication. Message Authentication ensures the sender that the message was sent by a specified sender and the message was not altered anywhere in the transmission path. Message confidentiality ensures that the sender confidential data can be

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 175–182, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3619

read only by an authorized and intended receiver. Hence, the confidential data is secured in an efficient way which is not tampered by unauthorized users.

To provide a secure group communication, it is necessary to manage the keys for creating, updating and distribution. Moreover, before exchanging the confidential data, the key establishment protocol has to distribute the group key to all participating entities in a secured and effective manner. The two important types of key establishment protocols are namely key transfer protocols and key agreement protocols. Key transfer protocols rely on KGC to select group key for communicating information with the group members by sharing one or more secret key during registration. But in key agreement protocols, the group key is determined by exchanging public keys of two communication parties with the presence of communication entities.

The most commonly used key agreement protocol is Diffie-Hellman (DH) key agreement protocol [4]. However, the Diffie Hellman key distribution algorithm can provide secret key only for two entities, and cannot provide secret keys for the group that has more than two members. When there are a more number of members in a group the time delay for setting up the group key will take longer time. Hence, it is necessary to propose a new technique to avoid this type of constraints in group communication. In this proposed work, group communication applications will make use of key transfer protocol to transmit data to all the group members with the minimum resources needed for this group communication.

In this work, a cryptographic technique for secure key distribution and key management in the group environment is proposed. The algorithms are analyzed with suitable samples. The remaining paper is organized as follows. Chapter 2 surveys about the existing work in this area. Chapter 3 explores the proposed work and the implementation details. Chapter 4 and Chapter 5 analyzes and discusses the results obtained from the work. Chapter 6 discuss about the security analysis. Chapter 7 concludes the proposed and implemented work and suggested some possible enhancements.

2. LITERATURE SURVEY

There are many works pertaining to the secure Group Communication and that have been carried out, but some of the important works has been surveyed and cited here. Among them, Mike Burmester and Yvo Desmedt [3] presented a Group Key Exchange protocol which extends the Diffie-Hellman protocol [2]. The protocol is scalable and secure against passive attacks. But, Diffie Hellman public key distribution algorithm is able to provide group key only for two entities. Bohli [4] developed a framework for robust group key agreement that provides security against malicious insiders and active adversaries in an unauthenticated point-to-point network. Bresson et al. [13] constructed a generic authenticated group Diffie-Hellman key exchange algorithm which is more secure. Katz and Yung [5] proposed the first constant-round and fully scalable group Diffie-Hellman protocol which is provably secure. There are many other works related to group key management protocols based on non-DH key agreement approaches. Among them, Tzeng [9] presented a conference key agreement protocol that relies on discrete algorithm assumption with fault tolerance. This protocol establishes a conference key even if there is several numbers of malicious participants in the conference. Hence, this method is not suitable for group communication.

Moreover, in a centralized group key management, there is only one trusted entity responsible for managing the entire group. Hence, the group controller need not depend on any auxiliary entity to perform key distribution. Harney et al. [10] proposed a group key management protocol that requires O(n) where n is the size of group, for encrypting and update a group key when a user is evicted or added in backward and forward secrecy.

Eltoweissy et al.[6] developed a protocol based on Exclusion Basis Systems (EBS), a combinatory formulation for the group key management problem. Lein Harn and Changlu Lin [1] introduced a group key transfer protocol where members of the group fully rely on Key Generation Center (KGC). They proposed an authenticated key transfer protocol based on secret sharing scheme that KGC can broadcast group key information to all group members at once. Chin-Yin Lee et al. [7] addressed the security issues and drawback associated with existing group key establishment protocols. They have also used secret sharing scheme to propose a secure key transfer protocol to exclude impersonators from accessing the group communication. Their protocol can resist potential attack and also reduce the overhead of system implementation. Burmester et.al [11] has presented a practical conference key distribution systems based on public-keys and also authenticates the users.

3. PROPOSED WORK

Based on the above survey in this secure group communication, it is necessary to propose a new model to solve the identified issues. The proposed model consists of four processes namely the User Registration, Group key generation based on prime numbers, Key generation and Key distribution, Group re-keying. The four main processes are explained as below.

3.1. User Registration

This module explains the process of User Registration. Each user has to register their identity at KGC for subscribing the key distribution service. While legitimate entities register to KGC, the encrypted hash value of their password is stored in the authentication server. Hence, this approach initially authenticates the user by matching its encrypted hash value with that of the stored value. The hash value of the password is calculated using Message Digest (MD5) algorithm and the encrypted password is stored in the authentication file. KGC keeps track of all registered users and removes any unsubscribed users in the group. During registration process, each user m_i is required to share a random secret value S_i with the KGC. Once user registration process is completed, KGC assigns a permanent secret id, denoted by Pi for each member m_i in the group

3.2. Group Key Generation and Distribution

Whenever there is a group of users participating in a group communication, the Key Generation Center (KGC) will select a random group key $K > (P_i \oplus S_i)$ for all i of Group G and computes the message (X_i, Y_i) pairs in the following manner.

$$X_i = K / (P_i \oplus S_i) \quad (1)$$

$$Yi = K \bmod (P_i \oplus S_i) \quad (2)$$

Once the pair is generated, KGC published (X_i, Y_i). From this public information, each group member mi can able to retrieve the key by computing

$$K = X_i * (P_1 \oplus S_1) + Y_i \quad (3)$$

Only authorized member can able to retrieve the hidden key using this pair (X_i, Y_i).

3.3 Group Re-keying

Scalable group re-keying is the important task to be performed when user joins or leaves the group in the secure group communication. The group keys needs to be updated to maintain the forward and backward secrecy. To achieve this, the two important tasks namely members join and members leave operation is performed.

3.3.1 Member Join

When a member wants to join the system, the new member will register with the KGC. KGC will share a prime number P_{n+1} and the member will provide the secret id S_{n+1} where $K >(P_{n+1} \oplus S_{n+1})$. KGC generates the new pair of values (X_i, Y_i) by using equation (1) and (2). After receiving the (X_i, Y_i) pairs, the newly joined member can use the prime number along with his secret id to derive the key K from equation (3).

3.3.2 Member Leave

When a member leaves the system, the member should inform to the KGC. Now KGC generates a new group key as follows. Step 1. KGC selects a new prime number K' (where $K' > (P_1 \oplus S_1)$ for all i).

Step 2. New pair of values (X_i, Y_i) are generated with the new Key K and distribute it to all the group members.

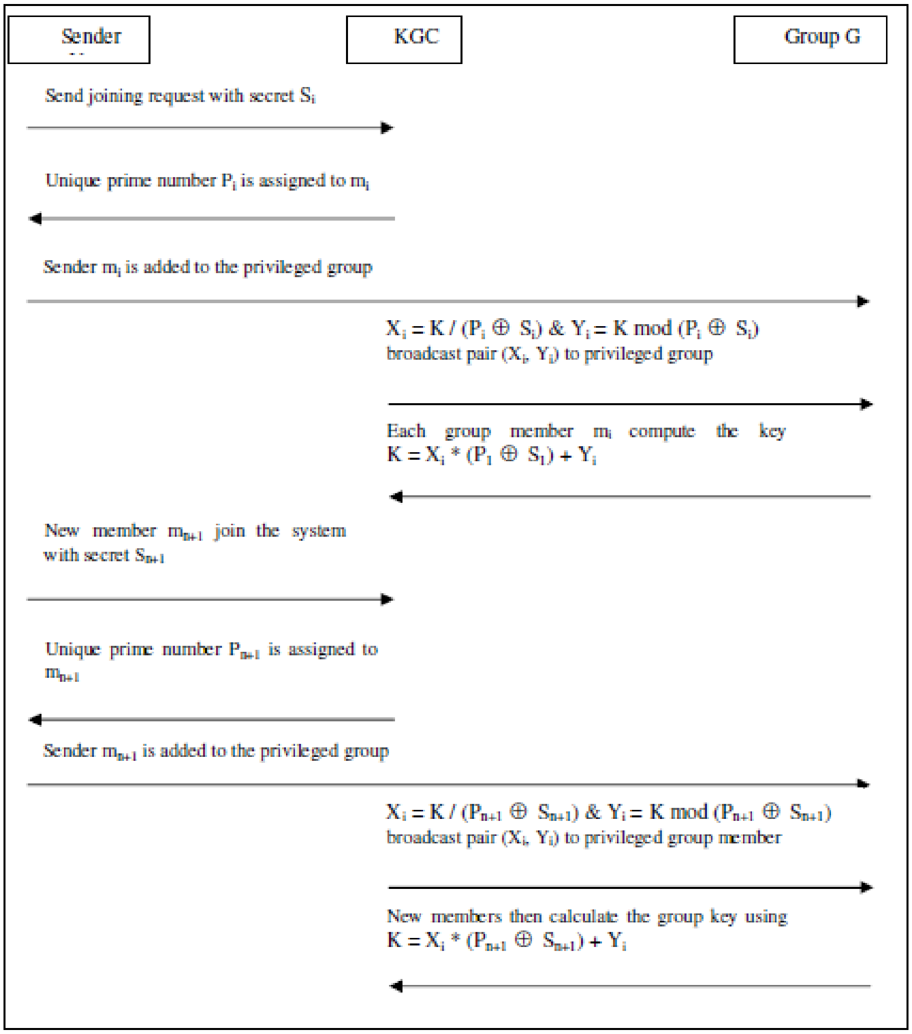
Sender
KGC
Group G
Send joining request with secret S_i
Unique prime number P_i is assigned to m_i
Sender m_i is added to the privileged group
$X_i = K / (P_i \oplus S_i)$ & $Y_i = K \bmod (P_i \oplus S_i)$
broadcast pair (X_i, Y_i) to privileged group
Each group member m_i compute the key
$K = X_i * (P_1 \oplus S_1) + Y_i$
New member m_{n+1} join the system with secret S_{n+1}
Unique prime number P_{n+1} is assigned to m_{n+1}
Sender m_{n+1} is added to the privileged group
$X_i = K / (P_{n+1} \oplus S_{n+1})$ & $Y_i = K \bmod (P_{n+1} \oplus S_{n+1})$
broadcast pair (X_i, Y_i) to privileged group member
New members then calculate the group key using
$K = X_i * (P_{n+1} \oplus S_{n+1}) + Y_i$

Fig 1. Process of Key Generation

4. EXPERIMENTAL SETUP

The proposed password based authenticated system is tested with five valid and five invalid users. Each of the five valid users has their own username and password. Initially, the users have created their username and password (Table 1). The authentication server stores the encrypted hash values of the passwords. As the hash values of the passwords are different it ensures uniqueness.

For key generation and key extraction mechanism, we considered a group with M=3 members. Member1 has permanent secret id (Prime), P1=55837, Member2 has P2=55603, Member3 has P3=35353, and key K= 65585.

The secret shared by each users are S1=28931, S2=37123, S3=12347. By applying equation (1) of the pair generation by KGC, we generated the pair as

$X_1 = K / (P_1 \oplus S_1)$ i.e 65585 / (55837 ⊕ 28931) = 1
$Y_1 = K \bmod (P_1 \oplus S_1)$ i.e 65585 mod (55837 ⊕ 28931) = 21779

$X_2 = K / (P_2 \oplus S_2)$ i.e 65585 / (55603 ⊕ 37123) = 3
$Y_2 = K \bmod (P_2 \oplus S_2)$ i.e 65585 mod (55603 ⊕ 37123) = 10145

$X_3 = K / (P_3 \oplus S_3)$ i.e 65585 / (35353 ⊕ 12347) = 1
$Y_3 = K \bmod (P_3 \oplus S_3)$ i.e 65585 mod (35353 ⊕ 12347) = 17935

The generated pairs for the three members are (1, 21779), (3, 10145), (1, 17935). These pairs are distributed to each member of the group. After receiving this message each member in the group computes the key by using its pair as follows.

$K_1 = X_1 * (P_1 \oplus S_1) + Y_1$ i.e., 1 * 43806 + 21779 = **65585**
$K_2 = X_2 * (P_2 \oplus S_2) + Y_2$ i.e., 3 * 18480 + 10145 = **65585**
$K_3 = X_3 * (P_3 \oplus S_3) + Y_1$ i.e., 1 * 47650 + 17935 = **65585**

We have taken K (Key) sizes as 64,128, 512, 1024 bits and the value of S (prime) has been taken has 64, 128, 512 and 1024 bits. When a non-group member M_k attempts to compute the group key with a unknown value pair it will not be able to retrieve the correct key.

5. PERFORMANCE ANALYSIS

The performance analysis for the password based authenticated module is analyzed with respect to the number of valid and invalid users. The analysis of the work has been done under the following heads

5.1 Md5 Analysis

The probability of two messages having the same message digest is on the order of 2^64 operations. The probability of coming up with any message having a given message digest is on the order of 2^128 operations. This ensures uniqueness of the message digest.

5.2 Replay Attack

Usually replay attack is called as ‘man in the middle’ attack. Adversary stays in between the user and the file and hacks the user credentials when the user contacts file. As key matching between the users is checked before file transfer and the information is encrypted before transfer, the probability of this attack is minimized.

Table 1. Authentication files with unique hash value passwords

S.no	Username	Password	Hash Value
1	user1	admin	4c56ff4ce4aaf9573aa5dff913df913d
2	user2	Test2	Dfg45f4ce4aaf9573aa5dff913df913e
3	user3	test5	dddd6ffsdfdfdffffff913df997art567fg
4	user4	test8	4c56ff4ce4aaf9573aa5dff913df913d
5	user5	test10	sfggce4aaf9573aa5dff913df913fget

5.3 Guessing Attack

Guessing attack is nothing but the adversaries just contacts the files byrandomly guessed credentials. The effective possibility to overcome this attack is to choose the password by maximum possible characters, so that the probability of guessing the correct password can be reduced. As the proposed approach uses random generation of key, it is more difficult to guess the password.

5.4 Stolen Verifier Attacks

Instead of storing the original password, the verifier of the password is stored. As the encrypted hash value of the password is stored, the proposed protocol is also more robust against the attack.

6. Security Analysis

Given K , P and S, it is easy to compute
$X = K / (P_1 \oplus S_1)$ and $Y = K \bmod (P_1 \oplus S_1)$.

But given X and Y it is very difficult to compute K, in polynomial time, without knowing P and S such that $K = X * (P_1 \oplus S_1) + Y$, and it is NP hard for large size of K. Even if several pairs (X_i, Y_i) are known, it is very difficult to compute K, unless the corresponding P_i's and S_i's are known.

Suppose,

$K = X_1 * (P_1 \oplus S_1) + Y_1$ (P_1 and S_1 not known) (1)
$K = X_2 * (P_2 \oplus S_2) + Y_2$ (P_2 and S_2 not known) (2)
$K = X_3 * (P_3 \oplus S_3) + Y_3$ (P_3 and S_3 not known) (3)
$K = X_4 * (P_4 \oplus S_4) + Y_4$ (P_4 and S_4 not known) (4)

From the first of two equations, we get

$X_1 * (P_1 \oplus S_1) + Y_1 = X_2 * (P_2 \oplus S_2) + Y_2$
$X_1 * (P_1 \oplus S_1) - X_2 * (P_2 \oplus S_2) = Y_2 - Y_1$ (say $Y_2 > Y_1$)

$X_1 * (P_1 \oplus S_1) - X_2 * ((P_1 \oplus S_1) + R_1) = C_1$
Where ($Y_2 - Y_1 = C1$, $(P_2 \oplus S_2) = (P_1 \oplus S_1) + R_1$)

$(X_1 - X_2) (P_1 \oplus S_1) - X_2R_1 = C1$ (5)

Similarly from 1 and 3, we get

$(X_1 - X_3)\ (P_1 \oplus\ S_1)\ - X_3R_2 = C2$ (6)

From 2 and 3, we get

$(X_2 - X_3)\ (P_2 \oplus\ S_2)\ - X_3R_3 = C3$

$(X2 - X3)\ ((P_1 \oplus S_1) + R_1) - X_3R_3 = C3$

$(X_2 - X_3)\ (P_1 \oplus\ S_1) + (X_2 - X_3)\ R_1 - X_3R_3 = C3$ (7)

Thus, there only 3 equations (5 – 7) to determine 5 unknowns (R_1, R_2, R_3, P_1 and S_1), Therefore one of the values R_1, or R_2 or R_3 or P_1 or S_1will be left arbitrary, hence the value of K cannot be determined easily and correctly.

The strength of the RSA algorithm relies on the fact that the given M (product of two large prime numbers), it is not possible to find the two factors in polynomial time (It is NP-hard). In our algorithm, we have more complex message M, than what is used in RSA algorithm. Therefore, it is very difficult to find any of the prime numbers P1, P2,.., Pn is NP-hard. Thus the Key K is more secure and safe preventing it from man-in-the-middle attack and brute-force attack. To maintain secrecy, KGC generates a new pair message and broadcast it everytime when a member leaves the system.

7. CONCLUSION AND FUTURE ENHANCEMENT

Key transfer protocol relies on a trusted Key Generation Center (KGC) to select group key and to distribute group keys to all group members in a secret manner. KGC assign a large prime number to each member in the group. Our proposed algorithm is efficient both in terms of message generation and key extraction. In future, we wish to implement our design for communication in dynamic and hierarchical groups. Also we wish to compare our algorithm with the dual-level key management for secure group communication.

REFERENCES

[1] Lein Harn and Changlu Lin. Authenticated Group Key Transfer Protocol Based on Secret Sharing. IEEE Trans.Computers; Vol.59, no.6, 2010, pp.842-846.

[2] W. Diffie and M.E. Hellman. New Directions in Cryptography. IEEE Trans. Information Theory; Vol. IT-22, No. 6, 1976, pp.644-654.

[3] Mike Burmester and Yvo Desmedt. A Secure and Scalable Group Key Exchange System," Information Processing Letters; 94(3), 2005, pp. 137—143.

[4] Bohli. A Framework for Robust Group Key Agreement. In Computational Science and Its applications - ICCSA 2006 (3), Lecture Notes in Computer Science; vol. 3982, Springer 2006, pp. 355-364.

[5] J. Katz and M. Yung. Scalable Protocols for Authenticated Group Key Exchange. J Cryptology; Vol. 20, 2007, pp. 85-113.

[6] M. Eltoweissy, M.H. Heydari, L. Morales, and I.H. Sudborough, "Combinatorial Optimization of Group Key Management," J. Network and Systems Management, Vol. 12, No. 1, pp. 33-50, 2004.

[7] Chia-Yin Lee, Zhi-Hui Wang, Lein Harn, Chin-Chen Chang. Secure Key Transfer Protocol Based on Secret Sharing for Group Communications. IEICE Transactions; 94-D(11), 2011,pp. 2069-2076.

[8] E. Bresson, O. Chevassut, and D. Pointcheval. Provably-Secure Authenticated Group Diffie-Hellman Key Exchange. ACM Trans. Information and System Security; Vol. 10, No. 3, Aug 2007, pp. 255-264.

[9] Tzeng. A Secure Fault-Tolerant Conference-Key Agreement Protocol. IEEE Trans. Computers; 51(4), 2002, pp 373-379.

[10] H. Harney, C. Muckenhirn, and T. Rivers. Group Key Management Protocol (GKMP) Architecture; RFC 2094, July 1997.

[11 .M. Burmester and Y.G. Desmedt. A Secure and Efficient Conference Key Distribution System. Proc. Eurocrypt '94 Workshop Advances in Cryptology;1995, pp. 275-286.

[12. M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman Key Distribution Extended to Group Communication. Proc. Third ACM Conf. Computer and Comm. Security (CCS ’96), 1996, pp. 31-37.

[13. E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater. Provably Authenticated Group Diffie-Hellman Key Exchange. Proc. ACM Conf. Computer and Comm. Security (CCS ’01), 2000, pp. 255-264.