A NOVEL WAY OF VERIFIABLE REDISTRIBUTION OF THE SECRET IN A MULTIUSER ENVIRONMENT USING GROUP KEY

P Devaki[1], G Raghavendra Rao[2]

[1]*Associate Professor, Dept. of IS&E, NIE, Mysore*
[2]*Professor and Head, Dept. of CS&E, NIE, Mysore*

Abstract

Shamir's threshold secret sharing is one of the mechanisms to distribute the shares of a secret to a group of authorized users called access structure (m, n). But the group members may change based on the organizations needs. This change of access structure requires the redistribution of the shares of that secret to the new members of that group (m', n'). In this paper we are proposing a method to distribute without using a private channel. Also redistribute the shares of a secret on change in the access structure. The redistribution does not involve the members of the old access structure. It is also proposed to verify the shares and also the reconstructed secret by each and every member of the group.

Keywords: *Redistribution, Threshold secret sharing, Old share holders, Verification.*

----------***----------

1. INTRODUCTION

The applications which are used by a designated group of users in a multiuser environment need control in accessing the information. Examples include military information, patient's information, bank information, designs , cryptographic keys, passwords etc. these and many other information are considered as critical or sensitive data which requires utmost care in maintaining the secrecy of the information. To access the critical information, a key or password is required which also needs to be kept secret. The efficient way of maintaining the secrecy of the key or password is based on Shamir's threshold secret sharing [1] or based on Blakley's secret sharing[2]. Organizations can define the group of users who can access the critical information by obtaining the key. Let G=P= {p_1, p_2, p_3….p_n} be a group of users who are authorized to access the critical information. The users of a group will obtain a share of the key which can be used to access the information. The shares for a key will be generated by the dealer who will have higher position and who is trustworthy. The shares are generated in such a way that, the original key can be obtained by combining all the shares of that key. The purpose of dividing the key is to see that no user gets the complete key which can be compromised accidentally or intentionally. One more purpose is since the information is critical; it should not be accessed unnecessarily and get modified. With the secret sharing technique it is possible to avoid all these possibilities as no user will have the complete key at any point of time. If a user wants to access the information, he has to send a request to all the users requesting for their shares , so that once he obtains all the shares the key can be reconstructed and can be used to access the system. Threshold secret sharing is a variation of the secret sharing defined by Shamir. There are 2 aspects for using threshold secret sharing.

a. To reduce the waiting time by a requester to collect all the shares from other users.
b. To eliminate the limitation of construction of secret in case of one or more shares lost or which do not arrive in time at the requester place.

So threshold secret sharing is defined as (m,n). m is the minimum number of shares out of n shares that are required to reconstruct the key. It is not possible to reconstruct the secret with even m-1 number of shares. Here the dealer is assumed to be with the higher priority that the organization and users (employees) believe. His role is only to divide the secret and distribute the shares in a secured manner. In case of change in the group members or the change in the secret, the dealer has to regenerate the shares and distribute them to the users. In a multi user environment a group may be dynamic. A new member may be added or a member may be out of the group. If a new member is added then the dealer has to give a new share. If a member goes out of the group, his share must be invalidated so that in future he should not use that share or send that to other users so that a wrong key can be generated. To avoid the users keeping the same old shares even after one or more members leave the group, it is better to generate a new set of shares and distribute among the new set of members. This is where redistribution comes in to picture.

In this paper we are proposing a new way of redistributing the shares based on Shamir's secret sharing in case of any change in the group. The shares are also sent securely to the members of a group without any secret channel. The members of the group can easily verify the shares and the reconstructed key.

2. RELATED WORK

In Desmedt and Jajodia's redistribution protocol [3], each share holders of m out of n old shareholders distribute n' new subshares of their shares of a secret, and n new shareholders combine m' subshares (one from each old

shareholder) to generate new shares. m' new shares are required to reconstruct the original secret. Here all the old share holders are involved in the redistribution of the shares irrespective of the faulty share holder. Even if one out of m share holders is a faulty share holder who is involved in redistribution of the shares will result in generation of wrong shares and hence results in reconstruction of wrong secret.

In Keith M Martin and Rei Safavi-Naini [4], old share holders are responsible in redistributing the shares to a new access structure without the help of a trusted dealer. They have defined several protocols for conducting redistribution of a secret from one access structure to another access structure $\Gamma \rightarrow \Gamma'$.

In Theodore M. Wong and Jeannette M. Wing [5] is also based on Shamir's threshold secret sharing. Apart from redistribution the new share holders can verify the validity of their shares after redistribution between different access structures. New shareholders can generate valid new shares if they can both verify the validity of the old shares and that of the sub shares.

In all the above mentioned papers, the old share holders are responsible for redistribution of the shares.

Limitations in normal redistribution protocols:

1. Use of private channels to distribute the shares
2. Each old user is involved in generating the sub shares
3. Some users may be faulty users due to which wrong shares may be generated
4. Computation time required is more, as each original share needs to be shared among the new set of users.
5. Computation is involved in verification of the shares as it involves exponentials.

3. PROPOSED WORK

Here we are proposing algorithms to distribute the shares, redistribute as well as to verify the shares.

3.1 Sharing the Secret

Based on the Shamir's secret method, a dealer (D) is responsible in dividing the secret in to shares and distributes it to the authorized members of a group. Addition to this in our protocol a group manger (G_m) is included who is responsible for verifying the membership of members in a group. Any changes in the group, the G_m will inform the dealer after verification.

Dealer holds the set of secrets (S) which need to be divided in to shares.

$$S = \{S_1, S_2, S_3 \ldots\ldots\ldots S_k\}$$

Where S_1, S_2 $\ldots S_k$ are the different secrets for different applications/systems.

Following table shows the details which will be maintained by the dealer.

Table – 1

Secret	Group ID	Members ID	H
S_1	G_1	p_1, p_2, p_4, p_5, p_7	H (S_1)
S_2	G_2	p_2, p_3, p_6, p_8	H (S_2)
.			
.			
S_k	G_k	$p_9, p_{10}, p_{11}, p_{12}, p_{13}$	H (S_k)

The above table shows that which group is authorized to use which secret, the members of the group, and the compressed value of the secret which cannot be reversed.

When a group is authorized to access the application/system, then the dealer selects the corresponding secret and applies the Shamir's threshold secret sharing mechanism to divide the secret in to shares equal to the number of users present in that group.

Example:

$S_{1\,i} = S_1 + C_{1i} + C_2\, i^2 + \ldots. C_{m-1}\, i^{m-1}$

$S_1 = \{S_{11}, S_{12}, S_{13}, S_{14}, S_{15}\}$ for each share S_{1i} hash code h_{1i} will be generated by the dealer, where i = 1 to 5.

$H = \{h_{11}, h_{12}, h_{13}, h_{14}, h_{15}\}$

3.2 Distribution of Shares

Our protocol is based on the following features:

a. Dealer has the public keys of all the members of a group
b. Dealer and the group manager G_m share a secret key $K_{D,Gm}$
c. G_m will participate in generating the group key G_k along with the members of a group

Distribution Protocol (VSS):

1. Group manager G_m verifies the members of a group and sends the list to the dealer. $G = \{ p_1, p_2, p_4, p_5, p_7\}$
2. G_m participates in generation of the group key G_k for the members of the group G
3. Dealer D divides the secret S_1 in to number of shares, S_{11} , S_{12} , S_{14}, $S_{15}\ldots$ S_{17}
4. Dealer encrypts each share with the corresponding public key of members of the group

$E_{pu1}(S_{11}) + E_{pu2}(S_{12}) + E_{pu4}(S_{14}) + E_{pu5}(S_{15}) + E_{pu7}(S_{17})$

5. Dealer then encrypts the above shares along with the members ID with the secret key of group manager and sends it to the G_m.

$E\ K_{D,Gm}\ [\{E_{pu1}(S_{11}) + E_{pu2}(S_{12}) + E_{pu4}(S_{14}) + E_{pu5}(S_{15}) + E_{pu7}(S_{17}) \}\ p_1,p2,p_4,p_5,p7]$

6. Dealer calculates the hash code for each share of the secret and sends all the hash codes in a separate file to each member of the group.

7. The G_m will decrypt the above message, verifies the second part of the message which indicates the members of that group.
8. After the verification the G_m will encrypt the above decrypted message with the group key G_k
9. The encrypted message is braodcast in the network
10. The members of the group receive the message, using the G_k they can decrypt the message to get the following message.

$$[\{E_{pu1}(S_{11}) + E_{pu2}(S_{12}) + E_{pu4}(S_{14}) + E_{pu5}(S_{15}) + E_{pu7}(S_{17})\}\ p_1,p_2,p_4,p_5,p_7]$$

11. Each member can extract its share by decrypting the corresponding encrypted share by using its private key.
12. Each user verifies the share with its corresponding hash code to confirm that the share has not been modified during transmission and stores that share. $E_{pui}(S_{1i})$

3.3 Redistribution of the Secret

If a member of a group leaves the group, then the share of that member must become invalid in future so that, the member should not participate in the reconstruction of the secret.

If a share of one or more members get compromised, then it is necessary to generate a new set of shares and redistribute to the users.

If a new member joins a group then a new share must be given to the new member so that, the new member can participate in the reconstruction of the secret.

In the above cases, it is necessary to generate a new set of shares and distribute it to the members of the group.

Redistribution of the shares has been defined by various researchers. In our paper we are defining the redistribution process, in which there is no involvement of the old members. Here the dealer only will generate the new set of shares for the new set of users and distributes to the members.

3.3.1 Protocol for Redistribution of the Shares (VSR)

1. Any change in the group will be notified to the G_m.
2. G_m will verify the new members joining the group and sends that information to the dealer
3. In case of a member withdrawn from a group, after updating its list by eliminating the member from that group G_m will inform the dealer.
4. In both the above cases, G_m will send the information about the members and their group to the dealer.
5. Once the dealer receives the updated information from the G_m, it will select a new set of coefficients for the same secret and generates the shares.
6. The hash codes will be generated for each of the newly generated share, and send it as a separate file.
7. Once the shares are generated, it makes use of the above distribution protocol to distribute the shares.
8. Each member will get a new share and can be verified with the hash codes sent by the dealer.

3.4 Strengths of our Protocol:

1. No need of private or secret channels to distribute the secrets.
2. No old member is involved in regeneration and redistribution of the shares.
3. No chance of reconstructing a wrong secret, as the shares will be verified every time, whenever they are being used.
4. Less computation time, as the distribution will be done by the dealer.
5. No calculations for verifying the shares by the members.

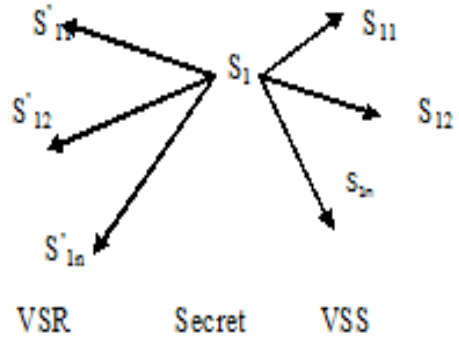

Fig – 1

Fig -1 shows that secret S_1 has been distributed using our verifiable secret sharing (VSS), and also using verifiable secret redistribution (VSR).

4. CONCLUSIONS

In this paper we have shown that, the redistribution is done with the help of dealer only. As the old share holders are not involved in the redistribution of the new shares, there is no chance of generating the wrong shares. computation expenses are also reduced as only the new set of shares will be generated instead of sub shares out of old shares. But here the redistribution is done only in case of change in the access structure from (m,n) to (m',n'). Since the dealer is a trusted entity the shares generated by the dealer can also be trusted. Our method doesn't require secret channel to distribute the new shares. It is also possible to verify the new shares without exponentiation which is computationally expensive. As the validity of users are verified by the G_m every time, the chances of having faulty users are nil or very rare.

REFERENCES

[1]. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[2]. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the Natl. Computer Conf.*, vol. 48 of *American Federation of Information Processing Societies Proceedings*, 1979

[3]. Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications *Technical Report ISSE TR-97-01, George Mason University, Fairfax, VA*, July 1997.

[4]. Keith M Martin and Rei Safavi-Naini, Bounds and techniques for efficient redistribution of secret shares to new access structure, *The Computer Journal* , Vol. 42, No. 8, 1999.

[5]. Theodore M. Wong and Jeannette M. Wing , Verifiable Secret Redistribution for Threshold Sharing Schemes, *CMU-CS-02-114R* , October 2002.