Secret Key for Group Members

[1]SK. Abdul Rasheed, V. Kishore, [3]SK. Akbar
[1,2,3]Dept. of CSE, Sana Engineering College, Kodad, Nalgonda, AP, India

Abstract
Message passing from one source to another has become a key for many upcoming technologies. A secret sharing scheme is a method which distributes shares of a secret to a set of participants in such a way that only specified groups of participants can reconstruct the secret by poling their shares. Secret sharing is related to key management and key distribution. These problems are common to all crypto systems. Secret sharing is also used in multi-party secure protocols. Future, secret sharing schemes have natural applications in access control and cryptographic key initialization. Key transfer protocols rely on a mutually trusted key generation center (KGC) to select session keys and transport session keys to all communication entities secretly.

Keywords
Group Key Transfer Protocol, Session Key, Secret Sharing, Confidentiality, Authentication

I. Introduction

Every message under transformation ought to have security provided to it. So, for providing high security, we consider 2 issues namely (1). Message Confidentiality: Only the authenticated and intended user should read the message and (2). Message Authentication: The receiver should be assured that the sent message is from authenticated sender and the message is not altered in the middle.

Here the work of KGS starts. It should provide a one-time session key to achieve the above 2 issues of key exchange. So, KGS distributes the secret key to all intended users with confidentiality and authentication. We can see from [5] the 2 types of key establishment protocols namely Key transfer protocols, Key agreement protocols.

Apart from this the KGS helps in selecting the secret key and transport them to all communication entities secretly. These session keys are determined by all communication entities where the most commonly used is Diffie-Hellman (DH) key agreement protocol [12].

Public keys of the communication entities play a key role in this protocol. They are exchanged to fix the value of session key. As the public key itself does not provide authentication, uses a digital signature. But the only drawback is that this is on whole applicable only two 2 users but not to a group. The importance of group key is found here as everyone ought to have it. This group key management protocol can be of 2 categories. Centralize group key management protocols, where the whole group is managed by a Group Key generation. Distributed group key management, where each individual manages the generation of key rather than a group key distribution. Of the both key management protocols, we use Centralized group key management the most. It was proposed by Harney et al[5] which takes O(n) where n indicates the size of group participating in the generation of key id. In addition to this, to update this group key either adding or editing the users, we have hierarchical structure based group key protocols.

II. Related Works

We have Fiat and Naor[14] introducing a k-resistant protocol. Using this security to about k users is provided with O(k log k log n) keys and server broadcasting O(k2 log2 k log n) messages per rekeying. EBS (Exclusion Basis System) proposed by Eltoweissy et al.[10] is a combinatorial formulation which helps users to switch between number of keys needed to be stored and number of messages to be transmitted. All this is for key updating so that solution to collusion is provided.

In the previous days, this group generation management protocols involved the naturally generalized DH key agreement protocol. Many examples can be quoted like Ingemarsson et al. [1], Steer et al. [8], Burmester and Desmedt ,and Steiner et al. [9] . Later, in 1990s, Steiner et al[2] came forward with extension of DH naming it as DH key exchange[29] and in 2001, name was changed to authentication services[6].

Later from 2006, there was a drastic advancement in this group key generations. In the very year of 2006, Bohli[8] proposed a framework for group key generation agreement which is intended to provide security opposing harming participators and active unauthenticated users at every point in the network. In 2007, Katz and Yung [19] proposed the first constant round and fully scalable group DH protocol which is provably secure in the standard model. Above all, the key feature of group DH is to generate a secret group key by a standardised group like KGS other than relying on members inside.

The next advancement in providing security is identifying the intruders present inside the network. For that, Tzeng [31] provided a conference key agreement protocol with the assistance of discrete logarithm (DL). Each user in the group requires having nm power polynomials with n representing number of participants. Later,. in 2008, Cheng and Lain [11] modified Tseng"s conference key agreement protocol based on bilinear pairing. In2009, Huang et al. [16] proposed a no interactive protocol based on DL assumption to improve the efficiency of Tseng"s protocol.

III. Proposed System

- Group key transfer protocol relies on one trusted entity, KGC, to choose the key, which is then transported to each member involved.
- Each user is required to register at KGC for subscribing the key distribution service
- The KGC keeps tracking all registered users and removing any unsubscribed users. During registration, KGC shares a secret with each user.
- In most key transfer protocol, KGC encrypts the randomly selected group key under the secret shared with each user during registration and sends the ciphertext to each group member separately.
- An authenticated message checksum is attached with the ciphertext to provide group key authenticity.
- In this approach, the confidentiality of group key is ensured using any encryption algorithm which is computationally secure.
- Our protocol uses secret sharing scheme to replace the encryption algorithm. A broadcast message is sent to all group members at once.

The confidentiality of group key is information theoretically secure. In addition, the authentication of broadcasting message can be provided as a group authentication. This feature provides

efficiency of our proposed protocol.
The main security goals for our group key transfer protocol are:

- Key freshness
- Key confidentiality
- Key authentication.

A. Key Freshness

It is to ensure that a group key has never been used before. Thus, a compromised group key cannot cause any further damage of group communication.
It is ensured by KGC since a random group key is selected by KGC for each service request. In addition, the polynomial f(x) used to recover the group key is a function of random challenge selected by each group member.

B. Key Confidentiality

It is to protect the group key such that it can only be recovered by authorized group members; but not by any un-authorized user.
It is provided due to the security feature of a secret sharing scheme. KGC generates a tth degree polynomial f(x) passing through (t + 1) points,(0, k) and (xi,yi) , for i = 1 . . . , t, and makes t additional points publicly known. For each authorized group member, including the secret shared with KGC, he/she knows (t + 1) points in total on f(x) Thus, any authorized group member are able to reconstruct the polynomial f(x) and recover the group key k.

C. Key Authentication

It is to provide assurance to authorized group members that the group key is distributed by KGC; but not by an attacker.
Auth is a one-way hash output with the secret group key and all members' random challenges as input. Since the group key is known only to authorized group members and KGC, unauthorized members cannot forge this value. Any insider also cannot forge a group key without being detected since the group key is a function of the secret shared between each group member and KGC.
In our protocol, we only focus on protecting group key information broadcasted from KGC to all group members. Our authenticated group key transfer protocol consists of three processes:

- Initialization of KGC
- User registration
- Group key

D. Initiali Initialization of KGC

The KGC randomly chooses two safe primes p and q (i.e., primes such that p1= p-1/2 and q1=q-1/2 are also primes) and compute n ¼ pq. n is made publicly known.

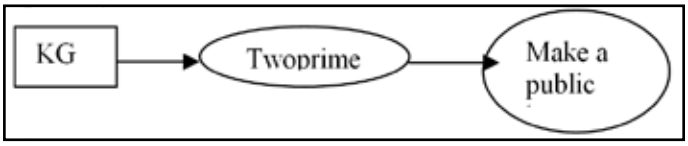

Fig. 1:

E. User Registration

Each user is required to register at KGC for subscribing the key distribution service. The KGC keeps tracking all registered users and removing any unsubscribed users. During registration, KGC shares a secret, (xi, yi), with each user Ui, where xi, yi €Zn.

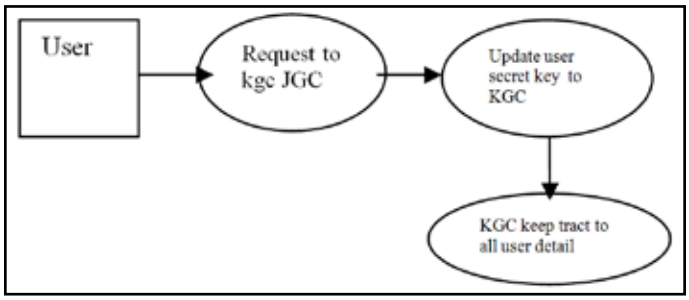

Fig. 2:

F. Group Key Generation and Distribution

Upon receiving a group key generation request from any user, KGC needs to randomly selects a group key and access all shared secrets with group members. KGC needs to distribute this group key to all group members in a secure and authenticated manner. All communication between KGC and group members are in a broadcast channel.
The key generation and distribution process contains five steps.

- The initiator sends a key generation request to KGC with a list of group members as {U1,U2, . . . , Ut}
- KGC broadcasts the list of all participating members,{U1, U2, . . . ; Ut}, as a response
- Each participating group member needs to send a random challenge, Ri €Zn, to KGC.
- KGC randomly selects a group key, k
- For each group member, Ui, knowing the shared secret, (xi,yi) and t additional public points, Pi, for i = 1, . . . , t, on f(x), is able to compute the polynomial f(x) and recover the group key k = f(0). Then, Ui computes h(k; U1, . . . , Ut,R1, . . ., Rt, P1, . . . , Pt) and checks whether this hash value is identical to Auth. If these two values are identical, Ui authenticates the group key is sent from KGC.

IV. Conclusion

Key transfer protocols rely on a mutually trusted Key Generation Center (KGC) to select session keys and transport session keys to all communication entities secretly. Most often, KGC encrypts session keys under another secret key shared with each entity during registration. In this paper, we propose an authenticated key transfer protocol based on secret sharing scheme that KGC can broadcast group key information to all group members at once and only authorized group members can recover the group key; but unauthorized users cannot recover the group key. The confidentiality of this transformation is information theoretically secure. We also provide authentication for transporting this group key.
The receiver has minimal computational requirements for symmetric key recovery. For the generation of each new key, a simple operation (i.e., construction of a polynomial) is performed. The degree of the polynomial is not a critical design factor.

References

[1] Lein Harn, Changlu Lin,"Authenticated Group Key Transfer Protocol Based on Secret Sharing", IEEE transactions on computers, Vol. 59, No. 6, JUNE 2010.
[2] William Stallings,"Cryptography and Network Security", fourth ed. Pearson Education, 2009
[3] E.Bresson, O.Chevassut, D.Pointcheval,"Provably-Secure Authenticated Group Diffie- Hellman Key Exchange", ACM Trans. Information and systems Security, Vol. 10, No.

3, pp. 255- 264, Aug. 2007.
[4] J.Katz, M.Yung,"Scalable Protocols for Authenticated Group Key Exchange", J. Cryptology, Vol. 20, pp. 85-113, 2007.
[5] W.G.Tzeng.,"A Secure Fault-Tolerant Conference Key Agreement Protocol", IEEE Trans.Computer, Vol. 51, No. 4, pp. 373-379, Apr. 2002.
[6] Johannes A.Buchmann,"Introduction to cryptography", second ed, Springer-Verlog NY,LLC, 2005.
[7] K.H.Huang,Y.F.Chung, H.H.Lee, F.Lai, T.S.Chen,"A Conference Key Agreement Protocol with Fault-Tolerant Capability", Computer Standard and Interfaces, Vol. 31, pp. 401-405, Jan 2009.
[8] G.R.Blakley,"Safeguarding Cryptographic Keys", Proc Am. Federation of Information Processing Soc. (AFIPS'79) Nat'l Computer Conf., Vol. 48, pp. 313-317, 1979.
[9] A.Shamir,"How to share a Secret",Comm ACM, Vol. 22, No. 11, pp. 612-613, 1979.
[10] Lein Harn, Changlu Lin,"Authenticated Group Key Transfer Protocol Based on Secret Sharing", IEEETrans.Computers, Vol. 59, No. 6, pp. 842-846, June 2010.

V. Kishore, Assoc. prof in CSE Dept. and HOD of SANA Engineering College. He attained his master from JNTU Hyd and pursuing his doctorate from CMJ University. He is having 11 years of experience in the field of CSE Department.

Sk.Abdul Rasheed, obtained his B.E.from the Madras University. He pursuing his M.Tech Computer Science & Engineering from JNTU HYDERABAD. His Research interest includes Network Security and Information Security based on Secret Key for Group Members.

Sk. Akbar, Asst.prof in CSE Dept of SANA Engineering College. He attained his master from Central University Hyderabad and pursuing his doctorate from Central University Hyderabad. He is having 4 years of experience in the field of CSE Department.