Advanced Group Key Distribution Protocol with Hardware Token Security

Soni Davi D S, Arun Kumar M

Abstract— Now a day's providing security for messages in group communication is more essential and critical one. So the Key establishment protocol needs to provide security, confidentiality, authentication and integrity for session keys to be sent messages to any system in network. Key distributed protocols fully rely on trusted Key Generation Center (KGC) to compute group key and to distribute the group keys to all communication parties in a secured and secret manner. The secret key is generated using RSA algorithm .In this proposed protocol the secret key is encrypted by using DES algorithm and stored in the database. In this paper also describing a method to overcome the problems created by hackers by providing a secondary security using a hardware token device.

Index Terms— Key Generation Centre,Session key, Group Key transfer protocol, USB authentication, Secret sharing, key distribution protocol,Confidentiality

---

1 INTRODUCTION

Security is concerned with the ability of a system to prevent unauthorized access to information or services. Traditionally, security issues have been associated with large databases. Confidentiality, Integrity and Authenticity are three fundamental objectives of security. Authentication and access control techniques are used to provide confidentiality. Data encryption is often used to provide Integrity. In a group KGC[1] can generates the separate key to particular user in a group.
In most secure communication, the following security functions are commonly considered:

- Message confidentiality: Message confidentiality ensures the sender that the message can be read only by an intended receiver.
- Message authentication: Message authentication: Message authentication ensures the receiver that the message was sent by a specified sender and the message was not altered en route.

Thus, before exchanging communication messages, a key establishment protocol [4] needs to distribute one-time secret session keys to all participating entities. The key establishment protocol also needs to provide confidentiality and authentication for session keys. According to [1][4], there are two types of key establishment protocols: key transfer protocols and key agreement protocols. Key transfer protocols rely on a mutually trusted key generation center (KGC) to select session keys and then transport session keys to all communication entities secretly. The most commonly used key agreement protocol is Diffie-Hellman (DH) key agreement protocol [2]. In DH protocol, the session key is determined by exchanging public keys of two communication entities. Since the public key itself does not provide any authentication, a digital signature [8] can be attached to the public key to provide authentication. However, DH public key distribution algorithm can only provide session key for two entities; not for a group more than two members.
When a secure communication involves more than two entities, a group key is needed for all group members. Most well-known group key management protocols can be classified into two categories: Centralized group key management protocols and Distributed group key management protocols.

The class of centralized group key management protocols is the most widely used group key management protocols.The proposed protocol achieves key freshness and key confidentiality due to the security feature of Shamir's secret sharing and secure hash function, and provides key authentication by broadcasting a single authentication message. The encrypted private key are hided and stored in a database. Furthermore, the proposed scheme resists against both insider and outsider attacks by using a hardware token device such as USB.

2 RELATED WORK

In this section, introduce some fundamental backgrounds.

Based on Conference key agreement from secret sharing[3], proposes new conference key agreement protocols based on secret sharing. Discuss roles of the dealer and recovery algorithms in the trust structure which is the necessary condition for any key establishment protocol to achieve the intended

- *Soni Davi D S is currently pursuing masters degree program in Computer Science engineering in Illahia college of engineering and technology,Mahathma Gandhi University, Kerala,India. E-mail: sonidavi@gmail.com*
- *Arun Kumar M is currently workingas Assistant Professor in Computer Science department ,Illahia college of engineering and technology,Mahathma Gandhi University,Kerala,India. E-mail: arunpvmn@gmail.com*

security goals. This conference key agreement protocol tackles the problem of entity authentication in conference key agreement protocols. The entity authentication is replaced by group authentication. To start a new conference all principals have to be active and broadcast their shares. If the conference goes ahead, all principals are sure that all principals are present and alive. It also explains possible modifications and extensions of the protocol.

[5] Provably authenticated group diffie-hellman key exchange, Dynamic group diffie-hellman protocols for authenticated key exchange (AKE) are designed to work in a scenario in which the group membership is not known in advance but where parties may join and may also leave the multicast group at any given time. While several schemes have been proposed to deal with this scenario no formal treatment for this cryptographic problem has ever been suggested. In this define a security model for this problem and use it to precisely define authenticated key exchange (AKE) with implicit authentication as the fundamental goal, and the entity-authentication goal as well.

Based on provably-secure authenticated group diffie-hellman key exchange [6], it describing the security of two entities. Authenticated key exchange protocols allow two participants A and B, communicating over a public network and each holding an authentication means, to exchange a shared secret value. Methods designed to deal with this cryptographic problem ensure A (resp. B) that no other participants aside from B (resp. A) can learn any information about the agreed value, and often also ensure A and B that their respective partner has actually computed this value. A natural extension to this cryptographic method is to consider a pool of participants exchanging a shared secret value and to provide a formal treatment for it. Starting from the famous 2-party Diffie-Hellman (DH) key exchange protocol,[2] and from its authenticated variants, security experts have extended it to the multi-party setting for over a decade and completed a formal analysis in the framework of modern cryptography in the past few years.

3 OBJECTIVES

3.1 Model

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[7] with each user. For group communication, a broadcast message is sent to all group members at once. The confidentiality of group key is theoretically secure. For providing a secondary security for the registered users , using an hardware token security. This is one of the strongest security.

In this Paper suggest a hardware token security. Which is one of the strongest security to overcome the problem created by hackers. There are lots of hardware token devices such as RFID, FingerPrint, CD/DVD,USB etc. From this pick USB as hardware token because of its simplicity and it is easy to carry.

To detect the PNP Device ID from the USB two methods are used. This ID is submitted along with secret key while submitting the registration form. All Plug and Play devices must contain a Plug and Play device ID in order to allow the operating system to uniquely recognize the device so that it can load the appropriate driver software.

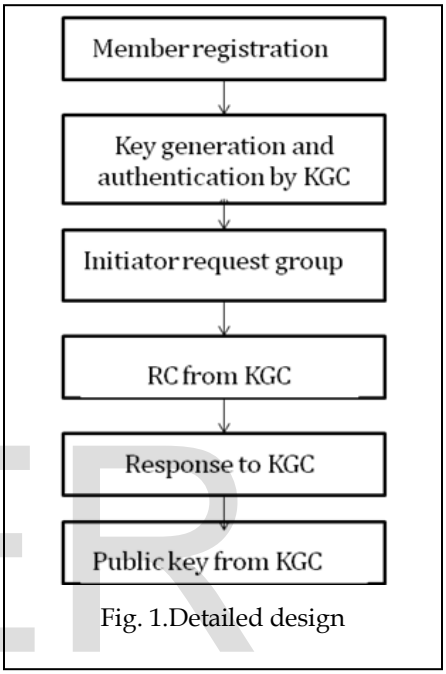


Fig. 1.Detailed design

Fig.1 shows the detailed design of our proposed protocol.
Each user needs to register at KGC so that a private key is generated using RSA algorithm for each user and forwarded to them. Along with this key the PNP device id of USB is also stored in to the database. Login can be done with the username, password and generated private key hence the message is authenticated. The initiator sends key sharing request for communication to KGC. The KGC broadcasts a random challenge in the form of questioner to each member. The members willing for communication response the random challenge and KGC provides the public key to each member.KGC encrypts the randomly selected group key under the secret Shared with each user during registration and sends the key to each group member separately. But make sure that, before registration and login plug the usb to resist against attackers. The PNP device ID is used for authentication

3.2 Goals

The main security goals for our proposed protocol are: 1) Key Freshness 2) Key Confidentiality 3) Key Authentication 4) USB Authentication

Key freshness 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. Key confidentiality is to protect the group key such that it can only be recovered by authorized group members; but not by any unauthorized user. Key authentication is to provide assurance to authorized group members that the group key is distributed by KGC; but not by an attacker. USB authentication is to protect the entire protocol from attackers.

In our protocol, we focus on protecting the entire group communication information broadcasted from KGC to all group members. The service request and challenge messages from users to KGC are not authenticated. Thus, an attacker can impersonate a user to request for a group key service. In addition, attacker can also modify information transmitted from users to KGC without being detected. We need to analyze security threats caused by these attacks. In our security analysis, we will conclude that none of these attacks can successfully attack to authorized group members since attackers can neither obtain the group key nor share a group key with authorized group members. User/message authentication and key confirmation can be easily incorporated into our protocol since each user has shared a secret key with KGC during registration. However, these security features are beyond the scope of our fundamental protocol.

4 OUR PROPOSED PROTOCOL

The Proposed Protocol consists of five processes:

- Initialization of KGC
- User registration
- Key generation and distribution
- USB authentication

Initialization of KGC: The KGC randomly chooses two safe primes p and q (i.e., primes such that p' = (P-1)/2 and q' = (Q-1)/2 are also primes) and compute n = pq. n is made publicly known.

User Registration: Each user is required to register at KGC for subscribing the key distribution service. Before registration plug the USB in the port. The KGC keeps tracking all registered users and removing any unsubscribed users. During registration, KGC shares a secret, (xi yi) with each user Ut, where xi, yi €Zn. This secret key is encrypted (fig.2)using DES algorithm and stored into the database along with this secret key the serial id of USB is also stored into the database.

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.

For example we assume that a group consists of t members {U1, U2,..., Utg} and shared secrets are (xi,yi), for i = i,... ,t. The key generation and distribution process contains five steps

• Step 1. The initiator sends a key generation request to KGC with a list of group members as {U1,U2,..., Utg}.

• Step 2. KGC broadcasts the random challenge to all participating members {U1, U2,..., U tg} as response.

• Step 3. Each participating group member needs to send a response for random challenge Ri , to KGC.

• Step 4. KGC randomly selects a group key, k and forwarded to each member in the group upon receiving their response. Different group keys are generated for different group.

• Step 5. For each group member, Ui, knowing the group key can share their secret messages to each members in the group .

USB authentication: USB token is first introduced in Registration where we plug our USB, to detect the PNP Device ID . This ID is submitted along with secret key while submitting the registration form. All Plug and Play devices must contain a Plug and Play device ID in order to allow the operating system to uniquely recognize the device so that it can load the appropriate driver software.

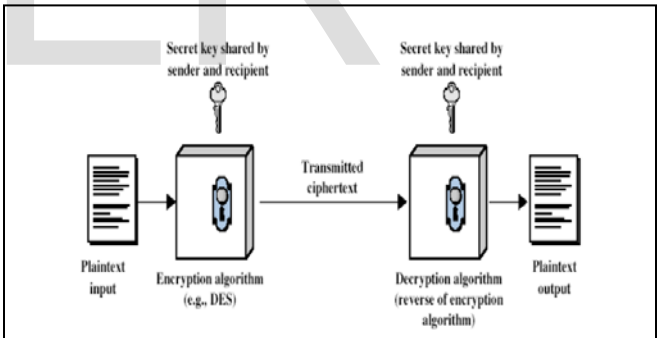


Fig. 2.Encryption/decryption

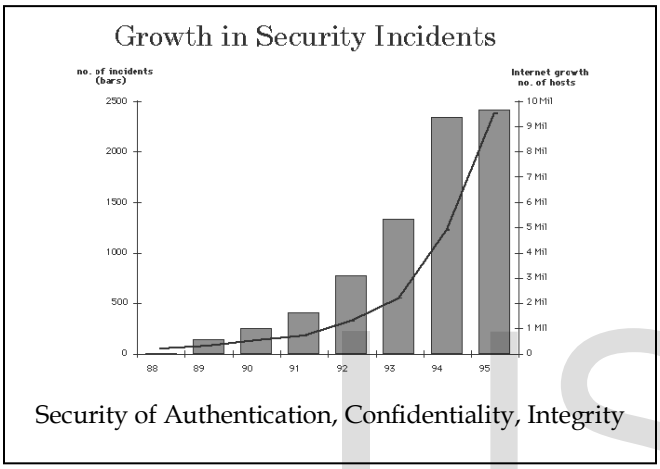
5 SECURITY ANALYSIS

In this section, we first consider two types of adversaries in our proposed protocol, insider and outsider.

Adversaries can be categorized into two types. The first types of adversaries are outsiders of a particular group. The outside attacker can try to recover the secret group key belonging to a group. This attack is related to the confidentiality of group key. In our proposed protocol, only authorized members can

send a request to KGC for requesting a group key service and also providing secondary security to resist against outsider attacker in the form of USB authentication. In security analysis, we will show that the outside attacker gains nothing from this attack .

since the attacker cannot recover the group key. The second type of adversaries are insiders of a group who are authorized to know the secret group key; but inside attacker attempts to recover other member's secret shared with KGC. Since any insider of a group is able to recover the same group key, we need to prevent inside attacker knowing other member's secret shared with KGC.



Security of Authentication, Confidentiality, Integrity

6 CONCLUSION

We have proposed an advanced group key distribution protocol with hardware token security. Every user needs to register at a trusted KGC initially an initiator send group request to KGC.KGC broadcasts group key information to all group members at once after performing some random challenge in the form of questionnaire. The confidentiality of our group key distribution is secure. We also provide group key authentication. Hardware token security to resist against outsider and insider attacks.

REFERENCES

[1] L. Harn and C. Lin, "Authenticated group key transfer protocol based on secret sharing," IEEE Transactions on Computers, vol. 59, no. 6, pp. 842-846, June, 2010.

[2] 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), pp. 255-264, 2001.

[3] C.H. Li and J. Pieprzyk, "Conference Key Agreement from Secret Sharing," Proc. Fourth Australasian Conf. Information Security and Privacy (ACISP '99), pp. 64-76, 1999.

[4] "An improved authenticated group key transfer Protocol based on secret sharing ",Yining liu, chi cheng, jianyu cao and tao jiang, IEEE transactions on computers, vol. X, no. Y, month 2013.

[5] 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), pp. 31-37, 1996.

[6] 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, pp. 255-264, Aug. 2007.

[7] S. Berkovits, "How to Broadcast a Secret," Proc. Eurocrypt '91 Workshop Advances in Cryptology, pp. 536-541, 1991.

[8] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, pp. 120- 126, 1978.