International Journal of Engineering (IJE)
Singaporean Journal of Scientific Research(SJSR)
Vol 6.No.2 2014 Pp. 100-101
available at:www.iaaet.org/sjsr
Paper Received :10-03-2014
Paper Accepted:20-03-2014
Paper Reviewed by: 1Prof.Dr. K. Raj Kannan 2. Chai Cheng Yue
Editor : Dr. Ken Ya Chen

ENHANCED AUTHENTICATED GROUP SECRET KEY FOR SHARED ACCESS PROTOCOL

Sabeena.A.S[1] and Mrs. B. Kalaiselvi[2]
[1]Student, [2]Asst. Professor
Department of CSE,
Mahendra Engineering College For women,
Kumaramangalam- 637 205

ABSTRACT

To achieve secure group communication, an authenticated group key is needed. In this paper we propose an Enhanced Authenticated Group Secret Key. The proposed protocol achieves key confidentiality due to the security of shamirs secret sharing.It provides key authentication by providing a single authentication message to all members. It resists against both insider and outsider attack .In this system the key as well as the message is encrypted for security. Key transfer protocols rely on a mutually trusted key generation centre(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.

Index Terms- Group Key Transfer Potocol,secret sharing,confidentiality,authentication.

1. INTODUCTION

The Project entitled “Email Security” which is a web application mainly focus on encryption and decryption. The users are user and administrator. The aim of the project is to develop an authenticated key that allows user to protect his page from an unauthorised person. Using this only authorized person can enter in to their account.

Message integrity, which guarantees that the contents of the message where not changed when it was in transfer, is also an important security requirement in a distributed system. Message Confidentiality is one of the most important features in secure group communication. Message confidentiality ensures that the sender confidential data which can be read only by an authorized and intended receiver. Hence, the confidential data is secured in efficient way such that it is not tampered by unauthorized users.

A message encrypted with a public key can only be decrypted by the corresponding private key. The opposite is also true: if a message is encrypted by a private key it can only be decrypted by the corresponding public key.

2. THE ENHANCED PROTOCOL

The proposed system provides an improved secure authenticated key transfer protocol based on Shamir’s secret sharing The proposed protocol achieves 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 proposed scheme resists against both inside and outside attacks.

The existing system only encrypted the message but the proposed system enhanced to such a way that both the message and key would be encrypted using Shamir's algorithm and provides an extra layer of security.

We assume that there are members 1, . . . , in a group. In order to achieve secure communication, the group's session keys are needed to be securely distributed among all authorized members prior to exchanging communication messages. Typically, the deputy of KGC is to select fresh session keys and securely distribute them, in a way that only authorized member can derive the session key upon receiving the broadcasted messages. First of all, each member is required to register at KGC. Then, KGC makes records of all registered members, and removes any unsubscribed members.

The improved authenticated group key transfer protocol consists of pre-distributing phase and distributing phase.

Pre-distributing phase.

KGC publishes = where and are cryptographic primes, publishes secure hash functions ℎ1( ) and ℎ2( ). Then, registers at KGC, shares his long term secret (,) with KGC in a secure manner.

Distributing phase.

Step 1. The initiator sends key sharing request to KGC with a list as { 1, 2, . . . , }, KGC broadcasts it.

Step 2. Each member (1 ≤ ≤) broadcasts a random challenge ∈ to KGC as a response.

Step 3. KGC randomly selects a group key , generates ( ) passing through (0,) and (, ⊕ℎ1(, ,)) (1 ≤ ≤), where & denotes + (mod). Then, KGC computes additional points { = (, ( ))} =1, and authentication message Auth = ℎ2(, 1, … , , 1, … , , 1, … ,). Finally,KGC broadcasts Auth and { } =1.

Step 4. Each member computes ( ) with his shared secret (, & ℎ1(, ,)) and the broadcasted messages { } =1, recovers = (0). Next, authenticates with Auth.

Note that, all communications in distributing phase are in an open broadcast channel.

3. CONCLUSION

In this paper, we proposed an enhanced authenticated group key transfer protocol based on secret sharing. We showed that the proposed protocol achieves confidentiality and authentication in a secure and efficient way. Furthermore, we demonstrated that existing system does not resist against insider attacks, while the proposed scheme could resist against both inside and outside attacks. And both message and key would be encrypted.

REFERENCES

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

[2]. .J. Katz and M. Yung, "Scalable protocols for authenticated groupkey exchange," Journal of Cryptology, vol. 20, pp. 85-113, 2007.

[3]. Kerem kaskalogulu,kamer kaya,ali adymn selcuk "Threshold Broadcast Encryption With Reduced complexity"

[4]. R. Velumadhava Rao1, K Selvamani2, R Elakkiya" A secure key transfer protocol for group communication