Group Key Agreement with Local Connectivity

1PROF. HARISH BARAPATRE, 2MANSI NAIK, 3BHAGYASHRI KURLE,
4PRATIBHA GHADAGE

1234Yadavrao Tasgaonkar Institute Of Engineering And Technology
1234Dept. Of Computer Engineering

Abstract - In computer networks security and secrecy in communication is must. For data transformation, transactions and other various operations need to be carried out securely. Group key agreement is an agreement which provides the security in communication of two persons. In social networking it is not possible always to communicate directly with the unknown person. It includes the any third one to communicate through. Group key agreement provides the mechanism in which two users can communicate with each other without interruption or without including any third person. In group key agreement mechanism a special key that is called session key is generated. This key is used for the communication.

1. INTRODUCTION

Group Key agreement is a process of assigning a unique key for communication. In this paper, we studied that on social networks mostly it is not possible to communicate with unknown person directly. Group key agreement provides the mechanism where any two unknown person can communicate directly.

For example on social sites there are groups of people communicate together. But it is not necessary that each and every person in a group well knows each other. Assume their are persons A, B and C. Person A and B are good friends. Person C is a friend of A but B wants to communicate C. So to get the authority to communicate with C, B must have to go through A. Then the communication between them can possible.

But in Group Key Agreement mechanism the directly communication between B and C can possible.

To make this possible we are using the theory of Diffie Hellman algorithm. Diffie Hellman algorithm provides the key exchange mechanism for communication.

Group key agreement is surely more effective for the social networks. We are using passively secure protocol to construct an actively secure protocol. Which is round efficient.

1.1 EXISTING SYSTEM

In social networking there are many applications which provide the data connectivity, communication, file transfer, sharing, uploading and many other operations. But sometimes there are problems in communication between two unknown authorities. Most of the systems does not support to the direct connectivity of unknown authorities’ for communication or data transfer. However the one person is neighbor of another person who cannot get access with their neighbors directly. So sometimes it makes problem connectivity. So this can be helped with the group key agreement to make it possible.

2. PROPOSED SYSTEM

A key-agreement protocol is a protocol where one user is only aware of his neighbors. Two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Sender generates key and sends it to receiver. The connection made between is actively secure protocol using passively secure protocol. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon. Public-key agreement protocol that meets the above criteria was the Diffie–Hellman key exchange, in which two parties jointly exponentiation a generator with random numbers, in such a way that an eavesdropper cannot feasibly determine what the resultant value used to produce a shared key is. Exponential key exchange in and of itself does not specify any prior agreement or subsequent authentication between the participants. It has thus been described as an anonymous key agreement protocol.
2.1 METHODOLOGY

SYSTEM ARCHITECTURE

3. IMPLEMENTATION

3.1 MODULES:

1. Repository Creation:

In this module are used to create an user details for who’s going to login the local connectivity. So previously they need to create repository.

2. Initiator & User Login

Initiator module used to create a repository as well as create a login id. User login are needed a username and password if its correct then enter into the initiator home else create a repository.

3. Key Generation

Key generation is the process of create a public and private key. After store (save) that keys in the database. If its stored then got a success message or failed or retry to enter the key values.

4. Diffie Hellman

Diffie Hellman algorithm are used in this project. This algorithm are used securely exchange the key from public channel. This algorithm are used to secure the internet services.

5. User Interaction

User interaction module are used to know the current status of the encrypted public key.

6. Security

Security is one of the module in this project. Its is used to ensure the security to unauthorized user’s. Public key encryption to private key encryption and private key encryption to public key encryption.

7. Lower Bound

An estimate of a number of operations needed to solve a given problem. Lower bound module is used to display all the details of estimate of problem solving for given problem.

8. Evaluation

Once public and private keys are generated after that encrypt the any one of the key either public or private. After verify the signature of encrypted message. Partial group key are fetched from server then verify it.
4. SOFTWARE DESCRIPTION

The front end of software is developed using Microsoft Visual studio 2008 with .Net and C#. And back end is managed with SQL-Server 2005. Operating system required is from family of Microsoft that means any Microsoft version.

RESULT

![Figure 1. Group Key Agreement with Local Connectivity](image1)

![Figure 2. Communication between users](image2)

![Figure 3. Validating user](image3)

![Figure 4. Performance](image4)

5. CONCLUSIONS

Here we studied the process of key generation for the security of communication. We generated the actively secured protocols by using the passively secured protocols Key generation is a easy way of communicating secretly on social networks.

REFERENCES


