ISSN: 2321-7782 (Online)
Volume 2, Issue 6, June 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Group Communication Using-A Dynamic Key Generation Protocol

B. T. Geetha[1]
Research Scholar
Sathyabama University
Chennai – India

Dr. M. V. Srinath[2]
Head – Content Development
Efuture Soft
Chennai – India

V. Perumal[3]
Associate Professor
Saveetha Engineering College
Chennai – India

Abstract: ***The objective of this paper is to generate a dynamic key protocol to achieve the group communication using the Key Generation Centre and prevent possible attacks in communication. 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 secure. We also provide authentication for transporting this group key.

Keywords: KGC, Dynamic Key, Group key.

I. INTRODUCTION

The most important issue in communication is security, in most secure communication, the following two security functions are commonly considered **Message confidentiality** ensures the sender that the message can be read only by an intended receiver. **Message authentication** ensures the receiver that the message was sent by a specified sender and the message was not altered en route.

To implement these two functions, one-time session keys need to be shared among communication entities to encrypt and authenticate messages. Thus, before exchanging communication messages, a key establishment protocol 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 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. Most often, KGC encrypts session keys under another secret key shared with each entity during registration.

In key agreement protocols, all communication entities are involved to determine session keys. The most commonly used key agreement protocol is Diffie-Hellman (DH) key agreement protocol.

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 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.

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.

II. System Analysis

A. *Existing system*

The most commonly used key agreement protocol is Diffie-Hellman key agreement protocol. 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 can be attached to the public key to provide authentication. DH public key distribution algorithm can only provide session key for two entities not for a group more than two members. The main disadvantage of this approach is to require every user to store a large size of secrets.

B. *Proposed system*

Each user needs to register at KGC to subscribe the group key transfer service and to establish a secret with KGC. Thus, a secure channel is needed initially to share this secret with each user. Later, KGC can transport the group key and interact with all group members in a broadcast channel. The confidentiality of group key distribution is information theoretically secure. That is, the security of this transfer of group key to each group member does not depend on any computational assumption. The authentication of the group key is achieved by broadcasting a single authentication message to all group members.

III. Networking

A. TCP/IP STACK

The TCP/IP stack is shorter than the OSI one. TCP is a connection-oriented protocol, UDP (User Datagram Protocol) is a connectionless protocol.

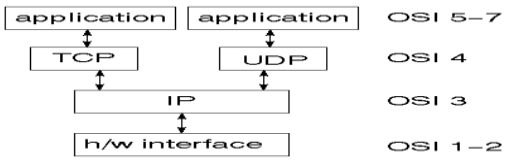


Fig 1 – TCP/IP STACK

B. IP Datagrams

The IP layer provides a connectionless and unreliable delivery system. It considers each datagram independently of the others. Any association between datagram must be supplied by the higher layers. The IP layer supplies a checksum that includes its own header. The header includes the source and destination addresses. The IP layer handles routing through an Internet. It is also responsible for breaking up large datagram into smaller ones for transmission and reassembling them at the other end.

C. TCP

TCP supplies logic to give a reliable connection-oriented protocol above IP. It provides a virtual circuit that two processes can use to communicate.

D Internet Addresses

In order to use a service, you must be able to find it. The Internet uses an address scheme for machines so that they can be located. The address is a 32 bit integer which gives the IP address. This encodes a network ID and more addressing. The network ID falls into various classes according to the size of the network address.

E. Network Address

Class A uses 8 bits for the network address with 24 bits left over for other addressing. Class B uses 16 bit network addressing. Class C uses 24 bit network addressing and class D uses all 32.

F. Subnet Address

Internally, the UNIX network is divided into sub networks. Building 11 is currently on one sub network and uses 10-bit addressing, allowing 1024 different hosts.

G. Host Address

Class A uses 8 bits are finally used for host addresses within our subnet. This places a limit of 256 machines that can be on the subnet.

H. Total Address

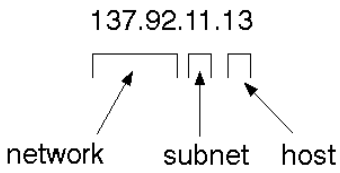


Fig.2 IP Addressing

The 32 bit address is usually written as 4 integers separated by dots.

I. Port Address

A service exists on a host, and is identified by its port. This is a 16 bit number. To send a message to a server, you send it to the port for that service of the host that it is running on. This is not location transparency! Certain of these ports are "well known".

J. Sockets

A socket is a data structure maintained by the system to handle network connections. A socket is created using the call socket. It returns an integer that is like a file descriptor. In fact, under Windows, this handle can be used with Read File and Write File functions.

```
#include <sys/types.h>

#include <sys/socket.h>

int socket (int family, int type, int protocol);
```

Here "family" will be AF_INET for IP communications, protocol will be zero, and type will depend on whether TCP or UDP is used. Two processes wishing to communicate over a network create a socket each. These are similar to two ends of a pipe - but the actual pipe does not yet exist.

IV. System Design

A. Design Process

Design involves identification of classes, their relationships as well as their collaboration. In objectory, classes are divided into entity classes, interface classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that are helpful only after the construction of the class diagram. In the Fusion method, some object-oriented approaches like Object Modeling Technique (OMT), Classes, Responsibilities, Collaborators (CRC), etc., are used. Objectory used the term "agents" to represent some of the hardware and software systems .In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software project is worked out by both the analyst and the designer. The analyst creates the use case diagram. The designer creates the class diagram. But the designer can do this only after the analyst creates the use case diagram...

B. System Architecture

The process of the design implemented with the system architecture view comprises of the parts of the project work that encapsulates all modules ranging from module to module communication, setting initializations and system.

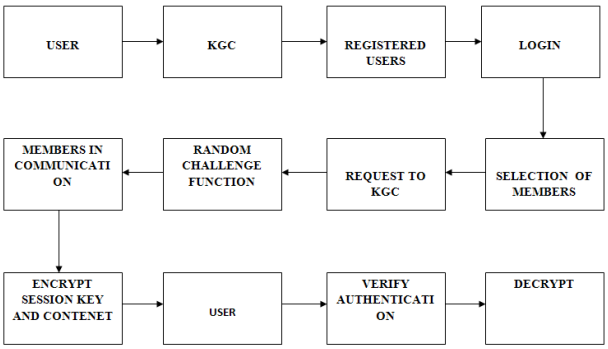


Fig 3. System Architecture Diagram

V. Key Generation Center (KGC)

A. Initialization Of Key Generation Center

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 = pq. N is made publicly known.

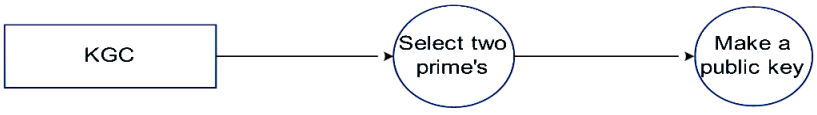


Fig.4 Initialization Of Key Generation Center

B. 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 E z.

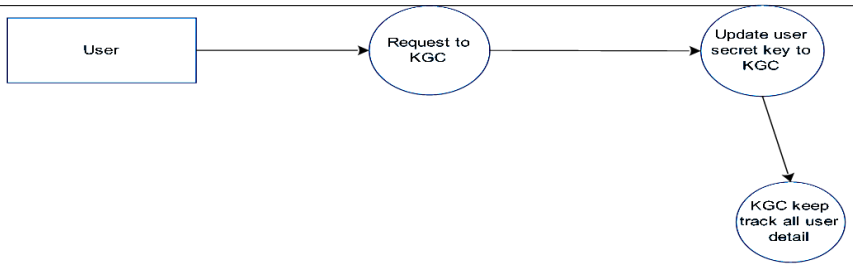


Fig 5. User Registration

C. 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…ut} and shared secrets are (xi yi) for I =1; . . . ; 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; . . . ; Ut).

Step 2. KGC broadcasts the list of all participating members, (U1; U2; . . . ; Ut), as a response.

Step 3. Each participating group member needs to send a random challenge, R1 E Z_to KGC.

Step 4. KGC randomly selects a group key, k, and generates an interpolated polynomial.

Step 5. For each group member, Ui, knowing the shared secret $(x_i, y_i \oplus R_i)$ 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, U2….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.

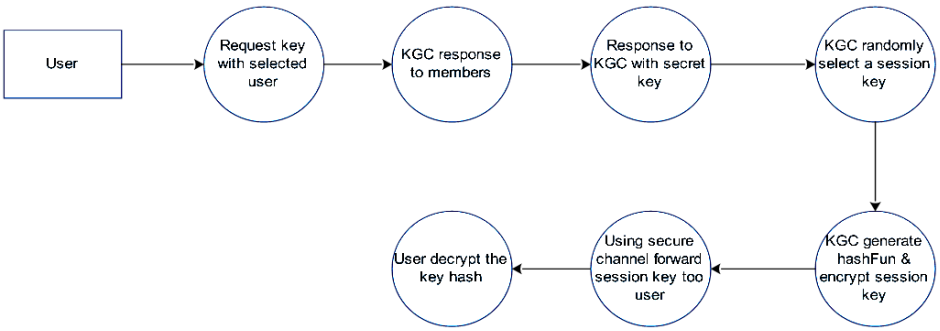
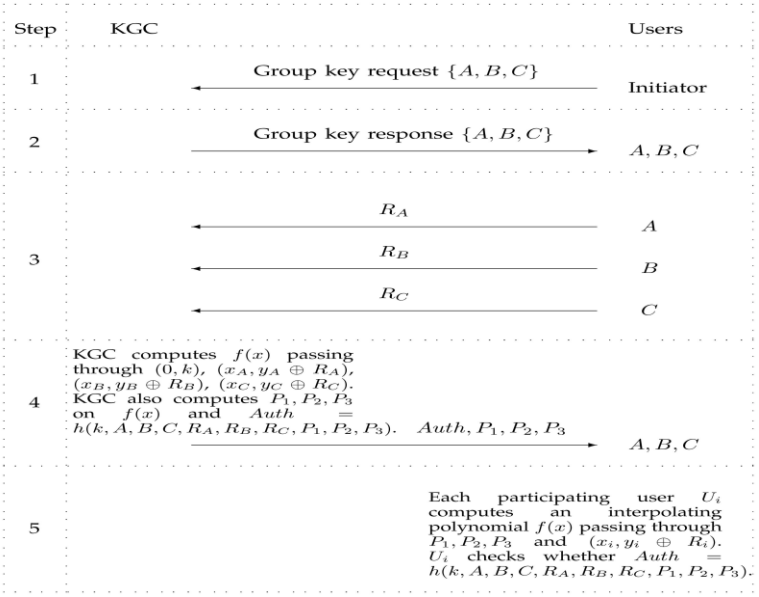


Fig 6. Key Generation And Distribution



D. Encryption and Decryption

In this module we are encrypting the messages using the session key. After encrypt the message it will be forwarded to selected neighbors. The neighbors get the encrypted message using the session key it will be decrypt the messages.

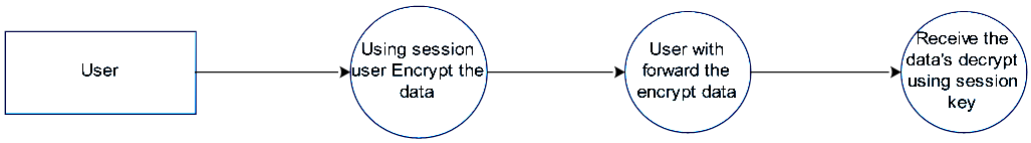


Fig 8.Encryption And Decryption

VI. CONCLUSION

We have proposed an efficient group key transfer protocol based on secret sharing. Every user needs to register at a trusted KGC initially and preshare a secret with KGC. KGC broadcasts group key information to all group members at once. The confidentiality of our group key distribution is information theoretically secure. We provide group key authentication. Security analysis for possible attacks is included.

References

1. Gartner, "Market Insight: The Outlook on Mobile Payment," Market Analysis and Statistics, May 2010.
2. Juniper Research, "NFC Mobile Payments & Retail Marketing – Business Models & Forecasts 2012-2017," May 2012.
3. ISO/IEC 15946-1:2008, "Information technology – Security methods – Cryptographic methods based on elliptic curves – Part 1: General," Apr. 2008.
4. ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security service and protocol," ISO/IEC, May 2010.
5. ISO/IEC 13157-2:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.
6. H. Eun, H. Lee, J. Son, S. Kim, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," IEEE International Conference on Consumer Electronics (ICCE), pp. 380-381, Jan. 2012.
7. ISO/IEC 18092:2004, "Information technology – Telecommunications and information exchange between systems – Near field Communication – Interface and Protocol (NFCIP-1)," ISO/IEC, Apr. 2004.
8. J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 574-582, May 2011.
9. E. Haselsteiner and K. Breitfuß, "Security in Near field Communication (NFC) – Strengths and Weaknesses –," RFIDSec 2006, Jul. 2006.
10. IEEE Std. 1363-2000, IEEE Standard Specifications for Public-Key Cryptography, Jan. 2000.
11. G. Calandriello, P. Papadimitratos, J.P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in VANET," Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (VANET 2007), pp. 19-28, 2007.

12. D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," Proceedings of the 2010 IEEE Vehicular Networking Conference (VNC 2010), pp. 174-181, Dec. 2010.

13. J.-H. Lee, J. Chen, and T. Ernst, "Securing mobile network prefix provisioning for NEMO based vehicular networks," Mathematical and Computer Modelling, vol. 55, No. 1, pp. 170-187, Jan. 2012.

14. Yamini Indla,, M. Sampath Kumar," Extended Group Key Transfer Protocol for Authentication Using DES based on Secret Sharing in Cloud ", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012).

AUTHOR(S) PROFILE

Mrs.B.T.Geetha received her M.E in Applied Electronics from MKU, Madurai in 2000 and B.E in EEE from MSU, Tirunelveli in 1998.She is presently with Maamallan Institute of Technology, Chennai as an Associate professor in the Department of Electronics and Communication Engineering.

Dr.M.V.Srinath is Leading the Instructional Design team at current position in developing resources which includes CBT, e-Learning and Instructional materials for clients and in house. He has published more than 35 Journals in National and International level and he also presented more than 60 papers in the National and International conferences. He has delivered more than 50 key note addresses and invited talks to different Universities and Colleges. He is a member of different Professional bodies like ISTE, CSI, Member, Member World Council for Curriculum and Instruction, Member Indian Society for Training and Development and etc..

