Secure E-Mail Messaging to Selected Group Members Using PGP Technique

Sachin Tripathi and G.P.Biswas
Department of Computer Science & Engineering
Indian School of Mines University, Dhanbad-826004, Jharkhand, India

ABSTRACT

The E-mail messaging is one of the most popular uses of the Internet and the multiple Internet users can exchange messages within short span of time using To(Original recipient) ,Cc(Carbon Copy) and /or Bcc(Blind Carbon copy) facilities. Although the security of the important E-mail messages is an important issue, no such security is supported by the Internet standards. Recently one well known scheme, called PGP (Pretty Good Privacy) is proposed for personal security of E-mail messages, but it can transmit encrypted message to single recipient only,i.e. ,the same encrypted message can not be transmitted to the multiple recipients if Cc and Bcc options are used. This paper proposes two modifications of the PGP that avoid the limitation of the PGP of not transmitting same encrypted message to multiple receipients.The basic idea is that a group comprising To, Cc and Bcc recipients is initially formed, a group key among them is generated using any group key generation scheme, which is then used (instead of the using the public key of the single recipients as done in PGP) to encrypt the session key. Since the secret group key is known to all recipients, they can extract session key and decrypt the confidential message correctly. This is one of the proposed modifications of PGP technique. The other modification is to remove the use of public key cryptosystem in PGP and this is done simply by generating signature of the E-mail message using group key (instead of using the sender's private key).It not only increases the processing speed of the PGP, but also simplifies it by avoiding to preserve the private key ring and public key ring of the participants.

Keywords: Pretty Good Privacy (PGP), CCEGK Group Key Algorithm , Asymmetric and Symmetric Cryptography

1. INTRODUCTION

In today's scenario, E-mail messaging is very popular application of Internet and frequently used by any Internet user to send the message in less amount of time. During the E-mail message transmission over insecure Internet any one can trace the original E-mail message easily. Some of the cases the secure transmission of E-mail message is required. Hence to provide the secure transmission of E-mail message over open insecure Internet, recently a scheme called Pretty Good Privacy (PGP) has been proposed recently. At present there are mainly three security protocols for Email messages are already in use, which are PGP (Pretty Good Privacy) [2], PEM [1] and S/MIME [3]. PGP is one of the important one out of three as it is simple, supports the conventional cryptographic techniques and completely free and usable by mass people. Since PGP can not transmit the same encrypted message can not be transmitted to the multiple recipients if *Cc* and *Bcc* options are used. Hence this paper proposes two modifications by the use of group key. The proposed modification is based on use of group key, where group key is generated using any group key generation scheme [4] [5] [6] [7] [8].First we proposes the use of group key for encrypting the session key at the message sender side instead of E-mail message receiver's public key. Since all recipients of an E-mail message are sharing same group key, so they can extract session key after decryption using symmetric encryption method like DES with group key and final decrypt the confidential E-mail message correctly. The group key can also be used to remove the use of public key cryptosystem in PGP and this is done simply by generating signature of the E-mail message using group key (instead of using the sender's private key).The use of group key for signature generation simplifies the PGP scheme and increases the processing speed of the PGP and avoid the use of private key ring and public key ring of the participants. Hence both of the modifications reduce the number of keys required for secure E-mail message transmission and corresponding overhead.

The paper is organized as follows. The section-2 provides the detailed description of Pretty Good Privacy (PGP) scheme. Then section-3 discusses the modifications of PGP by the use of group key, and the advantages of proposed modifications in PGP that gives the effectiveness of proposals, followed by conclusion.

2. DESCRIPTION OF PGP

PGP is the application layer protocol in TCP/IP protocol suit. Pretty Good Privacy is designed to create authenticated and confidential E-mails. Pretty Good Privacy (PGP) is a very popular program used by any Internet user for secure E-mail messaging and was developed by Philip R. Zimmermann [2] in 1991. PGP uses available cryptographic techniques like, symmetric/asymmetric encryption/decryption and digital signature to create confidential and authenticated E-mail. Basically the PGP mainly includes RSA, DSS, CAST-128,

IDEA or 3DES, SHA-1 that are considered to be secured. The PGP is open source free available software, thus attracts mass Internet users for secure E-mail messaging.

The notations used in figures throughout the paper are as follows.

H: SHA-1, Hash Function
E, D: Asymmetric Encryption/Decryption
e, d: Symmetric encryption/decryption
Z, Z^{-1}: Compression/Decompression using ZIP Algorithm
PR, PU: Private and Public Key
A, B: E-Mail Message sender/receiver
+ : Concatenation

The basic steps used in PGP at sender and receiver side, to create confidential and authenticated E-mail message are as follows.

a.E-mail Message Sender Side

1. Sender of E-mail Message creates original E-mail message and generates a 160 bits message digest of the original E-mail message using SHA-1 hash function. Message digest is encrypted using RSA algorithm with sender's private key (PR_A) called digital signature and prepended to the message.

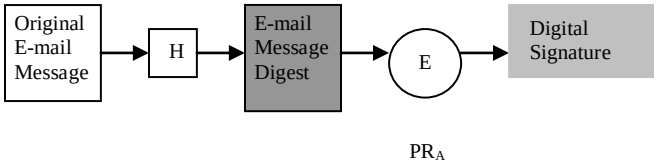


Figure 2.1: Digital Signature Generation

2. PGP uses ZIP compression algorithm and compress E-mail message after prepended digital signature to the message.

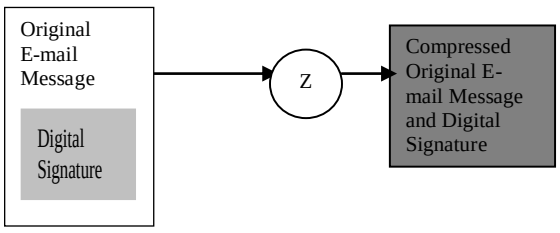


Figure 2.2: Message Compression Using ZIP Technique

3. Compressed original E-mail message and digital signature are encrypted using symmetric encryption algorithm (CAST-128 or IDEA or 3-DES) using randomly generated session key. The session key (K_S) is encrypted using RSA algorithm with receiver's public key (PU_B) and prepended to the encrypted compressed original E-mail message and digital signature.

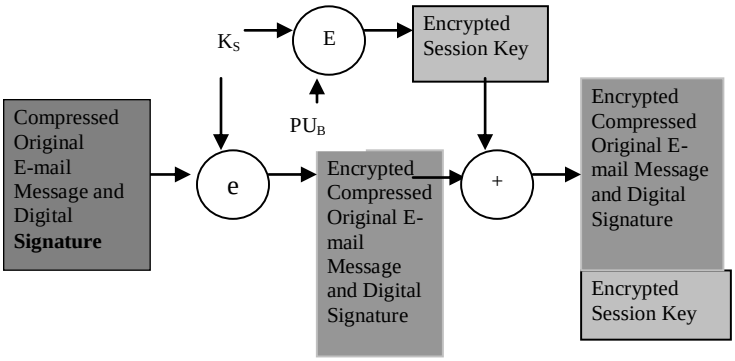


Figure 2.3: Encryption of Compressed Original E-mail Message and Session Key

4. Finally sender sends the message obtained in step (3) to receiver.

b.E-mail message Receiver Side

The receiver performs the following steps when receives the message sent by E-mail message sender.

1. The receiver decrypt the session key (K_S) using receiver's private key (PR_B) and then after decryption using session key (K_S) obtains the compressed original E-mail message and digital signature.

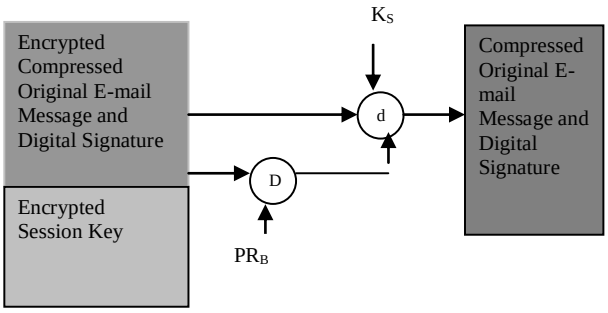


Figure 2.4: Decryption of Compressed Original E-Mail Message and Session Key

2. After decompression the receiver obtains the original E- mail message and digital signature.

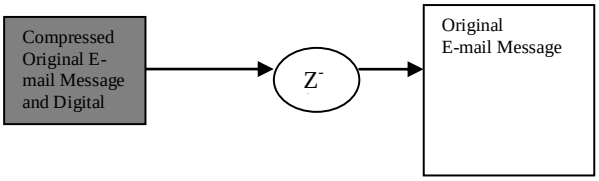


Figure 2.5: Message Decompression Using ZIP Technique

3. The receiver generates a *160 bits* message digest of the received original E-mail message using SHA-1 hash function .Then decrypts the digital signature using sender's public key(PU_A) and obtains the message digest , matches these two message digest if match occurs then conclude, no changes are made during transmission.

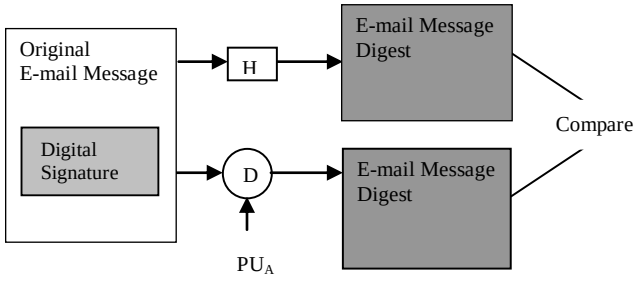


Figure 2.6: Digital Signature Verification

3. PROPOSED MODIFICATIONS IN PGP

This section proposes the use of single group key instead of public/private key for encryption/decryption. The proposed modification is based on idea that a group among the E-mail message sender and multiple E-mail message receivers has already been formed and group key has already been calculated using CCEGK [4] group key generation technique.

This section proposes the use of group key in two ways.

i) The group key is used to encrypt the session key instead of receiver's public key. Hence same encrypted message can be transmitted to multiple recipients.

ii) The group key is used to encrypt the session key as well as for digital signature .Hence avoid the use of public key cryptosystem in PGP.

3.1 Session Key Encryption

First we describe the PGP scheme, when group key is used to only encrypt the session key .The steps are as follows at E-mail message sender and receiver side.

a.E-mail Message Sender Side

1. Sender of the E-mail message follows the same step sequence as discussed in previous section to create digital signature and for compression.

2.Sender of E-mail message generates a random session key(K_S) and encrypts the compressed original E-mail message and digital signature using session key by any symmetric encryption algorithm (CAST-128 or IDEA or 3-DES).

3. Session key K_S is encrypted using symmetric encryption algorithm (CAST-128 or IDEA or 3-DES) with group key G_{KEY} and prepended to the compressed encrypted original E-mail message and signature.

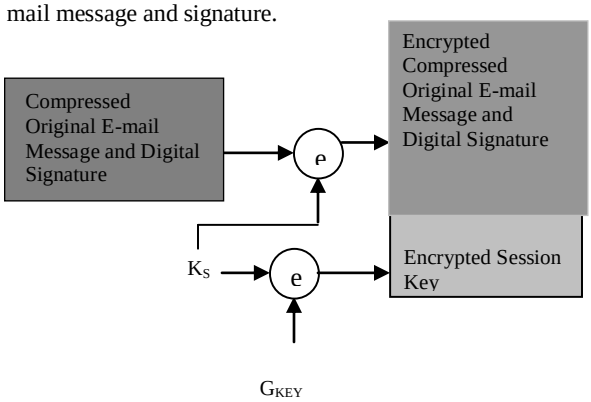


Figure 3.1: Proposed Encryption of Session Key Using Group Key

b.E-mail Message Receiver Side

1. The E-mail message receiver, obtain session key after decryption using DES with group key.

2. Session key is used to decrypt the original compressed original E-mail message and digital signature.

3. Receiver follows the same step sequence as described in previous section for digital signature verification and to obtain original E-mail message.

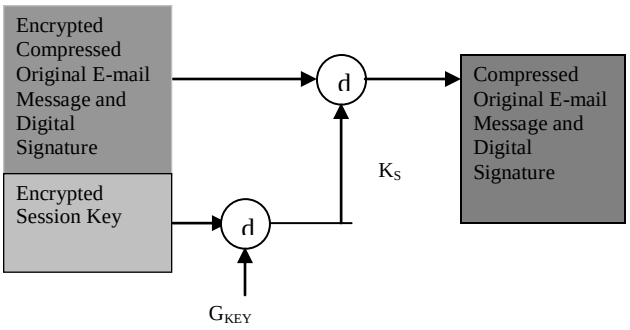


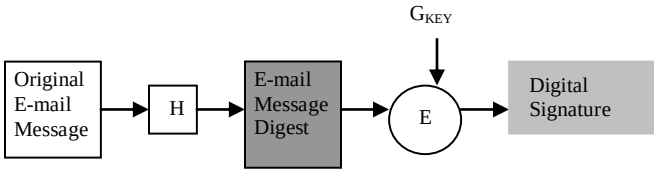
Figure 3.2: Proposed Decryption of Session Key Using Group Key

3.2 Digital Signature Generation

Now we describe the second use of group key, where group key is used to encrypt the session key as well as for digital signature. The steps are as follows at E-mail message sender and receiver side.

a.E-mail Message Sender Side

1. Sender of E-mail message creates original E-mail message and generates a 160 bits message digest of the original E-mail message using SHA-1, hash function. The message digest is encrypted using any symmetric encryption algorithm (CAST-128 or IDEA or 3-DES) with group key called digital signature and prepended to the message.



3.3: Proposed Digital Signature Generation Using Group Key

2. The sender follows the same step sequence as discussed in sub section 3.1, to compress and encrypt the original E-mail message and session key using group key.

b.E-mail Message Receiver Side

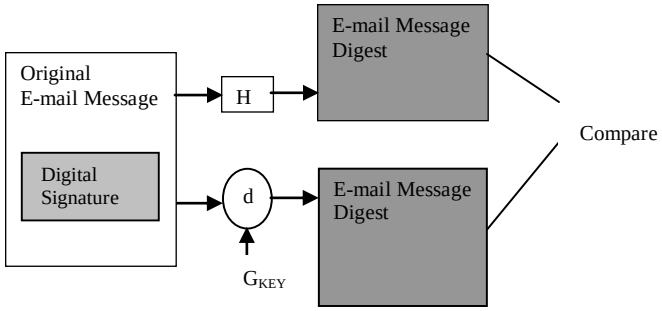
1. The receiver decrypts the session key using group key and obtains the session key. The session key is used to decrypt the compressed original E-mail message and digital signature as discussed in subsection 3.1.

2. Decompress the message obtained in step (3) using ZIP technique and obtain the original E-mail message and digital signature.

3. Decrypt the digital signature using group key and obtain the message digest.

4. Create the fixed size message digest of original E-mail message obtained in step (2) using SHA-1 hash function.

5. Match the message digest obtained in step (4) and step (5), if matches then conclude that no changes are made during transmission.



3.4: Proposed Digital Signature Verification Using Group Key

3.3 Advantages of Proposed Modifications

The proposed modifications provides the following advantages in PGP scheme.

1. Reduce the number of keys required for secure E-mail message transmission and corresponding overhead. Hence Increases the processing speed of PGP at E-mail message sender and receiver side.

2. Same encrypted message can be transmitted to multiple recipients using group key.

3. Avoid the use of public key cryptosystem in PGP.Provides authentication of all group members instead of only sender. Since for digital signature generation also PGP uses group key instead of public/private key pair.

4. CONCLUSION

E-mail messaging is very popular application of Internet and some cases the security of E-mail message is an important issue .Although there are three security protocols PGP,PEM and S/MIME are available for E-mail message security but PGP is

simple, supports the conventional cryptographic techniques and completely free. Hence this paper proposes two modification of PGP using group key, where group key is generated using any group key agreement protocol. The first modification proposes the use of group key to encrypt the session key that avoid the limitation of PGP to transmit the same encrypted message to multiple receipients.The second modification proposes the use of group key instead of sender's private key for digital signature generation that avoids the use of public key cryptosystem in PGP.Hence both modification increases the processing speed of PGP.

References

[1] John Linn,'privacy Enhancement for Internet Electronic Mail, Part I :Message Encryption and Authentication procedures,"RFC 1421, February 1993

[2] Philip Zimmermann ,"The official PGP User's Guide,",MIT Press,1995

[3]Black Ramsdell,"S/MIME Version 3 Message Specification,"RFC2633,June 1999

[4] Shanyu Zheng, David Manz, JIM Alves-Foss: A Communication –Computation efficient group key algorithm for large and dynamic groups. Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 51, Issue 1, January 2007 ,pp: 69 - 93 , 2007.

[5] Y.Kim A.Perrig, G.Tsudik, Tree based group key agreement, ACM Transactions on Information and System Security, 7(1) ,pp:60-96,2004.

[6] Y.Kim, A.Perrig, G.Tsudik, Communication efficient group key agreement .In proceeding 16th International conference on information security: Trusted Information: New decade challenge, June 11-13, 2001, Paris,France

[7] Group Key agreement efficient in communication, IEEE transaction on computers, Vol. 53 n.7 pp.095-921, July 2004

[8]Sachin Tripathi and G.P.Biswas "Design of Efficient Ternary-Tree Based Group Key Agreement Protocol for Dynamic Groups " in proceeding of IAMCOM 2009 held in conjunction with IEEE COMSNETS, January 2009, Bnagalore,India

[9]Data Communications and Networking, Behrouz A Forouzan, TMH Publication

[10] William Stalling 'Cryptography and Network Security ,PHI