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 recipients. 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 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.

Reference

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


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


Index Terms

Computer Science

Security

Key words

Pretty Good Privacy (PGP)

CCEGK Group

Key Algorithm

Asymmetric and Symmetric Cryptography