International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 03, March 2017
www.ijates.com
ijates
ISSN 2348 - 7550

IMPROVED APPROACH FOR INTRANET MAILING IN PRETTY GOOD PRIVACY (PGP)

Sravan Kumar G[1], J Deepthi[2]

[1]Assistant Professor, [2]Associate Professor, CSE Department,
Sphoorthy Engineering College, JNTUH, Hyderabad (India)

ABSTRACT

A cryptosystem must essentially offer security services such as Data Integrity, Authentication, Confidentiality and Non-Repudiation (four basic pillars of the cryptosystem). This paper focuses on improved configuration to achieve Non-Repudiation service while addressing security and cryptographic processing overhead issues involved in providing this service. Non-Repudiation service ensures that repudiation is not being done by either sender or receiver. This service allows the receiver and sender to be provided by proof of origin and proof of delivery respectively in the communication. Non-Repudiation of Origin (NRO) and Non-repudiation Receipt (NRR) services together called Mutual Non-Repudiation (MNR) service and is achieved by the cryptosystem, only if the entities involved in the communication exchange themselves with proof of origin (Non-Repudiation Origin) and proof of delivery (Non-Repudiation Receipt). This paper provides an approach that addresses issues such as inefficient configuration, security breaches involved in the system and finally relieves the server by letting it to do forwarding tasks in a secure fashion without compromising the security.

Keywords: One-time-only session key, Digital Signature, Enhanced Pretty Good Privacy, Mutual Non-Repudiation, Non-Repudiation, Non-Repudiation of Origin, Non-Repudiation of Receipt, Pretty Good Privacy.

I. INTRODUCTION

A cryptosystem must basically provide security services such as Data Integrity, Authentication, Confidentiality and Non-Repudiation. Data Integrity ensures no modifications during the transit of the message over network. Authentication verifies authenticity of the sender and the receiver. Confidentiality preserves the privacy of the sender and receiver by letting information accessible to only authorized users. Non Repudiation ensures that repudiation is not being done by either sender or receiver. This service allows the receiver and sender to be provided by proof of origin and proof of delivery respectively in the communication. Repudiation is one of the contemporary issues in the security aspects, requires high attention to address it with a solution such that entities in the communication can't deny the message sent among them. Many protocols have been developed to boost up the security of the email communication which is one time activity that doesn't require handshaking. There are separate protocols which are used to provide security for email messages such as S/MIME and Pretty Good Privacy (PGP) [3]. PGP by Phil Zimmermann is one of those protocols focused to provide security services such as Data Integrity, Authentication, Confidentiality and Non-Repudiation of Origin. PGP ensures Non-

Repudiation of origin which is incomplete Non-Repudiation service led to an Enhanced Pretty Good Privacy (EPGP). EPGP approach focused on Mutual Non-Repudiation service that ensures Non-Repudiation of Origin at receiver and Non-Repudiation of Receipt at sender.

PGP is package for securing emails and file communications [4]. It is open source package, which is available online for users [4]. PGP is a hybrid cryptosystem; it is combination of some of the best known encryption algorithms in existence [2]. Pretty Good Privacy (PGP) combines best features of both conventional and public key cryptography to strengthen cryptographic security of email communication over network. While PGP has the speediness of symmetric-key encryption algorithm, it maintains the high level of security of a public-key encryption algorithm [2]. PGP employs compression techniques to save transmission time of the message and disk space. Most of the cryptanalysis techniques exploit patterns found in the plaintext to crack cipher. Compression techniques reduce these patterns found in the plain text and thereby greatly enhances resistance to cryptanalysis. PGP creates a session key, which is one-time-only secret key [5]. This key which is random number, generated from the random movements of the mouse and the keystrokes, works with conventional algorithm that is about 1000 times faster than public key encryption.

II. RELATED WORK

PGP officially has been used for email contents and attachments encryption [4]. PGP can provide wide range of services like email and attachment security, digital signature, encrypting of whole hard disk, security of files and folders, encrypted HTTP request/response on the client server architecture [4]. PGP successfully implemented security services such as Data Integrity, Authentication, Confidentiality and part of Non-Repudiation service which is Non-Repudiation of Origin. In PGP, NRO service has been achieved by letting the sender to use its private key that results Digital Signature while composing a message to receiver. Digital Signature that has been prepared at sender ensures proof of origin to the receiver. Thus NRO service has been achieved due to the default configuration of public key and conventional encryption algorithms in PGP. In Email system, it is equally required to implement both services NRO and NRR but PGP ensures only NRO service without NRR service. Therefore EPGP method had focused on the configuration to achieve NRR service that ensures proof of receipt with the help of trusted third party called server. The idea of EPGP is to overcome PGP's drawback of incomplete Non-Repudiation service [1]. EPGP assures NRR by allowing receiver to decrypt message only after sharing its Digital signature to the server. Digital Signature by receiver assures proof of receipt to the sender and ensures NRR along with NRO which is one default features of PGP. NRR service depends on one-time-only session key which is encrypted by server public key, enables the receiver to decrypt the message by the receiver but this one-time-only session key is handed over to the receiver, only when receiver submits its Digital signature on the message to server that in turn forwards to the sender. The Digital Signature that forwarded by receiver to sender via server, assures proof of receipt to sender and ensures NRR service.

EPGP that ensures both NRR and NRO services, has certain limitations

- Sender entities has been made to rely on server security strength i.e., sender entity uses server public key to encrypt one time session key and thus results to compromising of sender and receiver confidentiality, if server gets compromised.
- To hand over one-time-only session key to receiver, server made to decrypt one time session key using its private key and encrypt again using receiver's public key. This leads to cryptographic processing

(encryption and decryption) overhead for n number of senders and receivers for which server acts as third party.

III. PROPOSED METHOD

The proposed method provides improved configuration for the secure and less cryptographic processing overhead email communication by assuring Mutual Non-Repudiation service (combination of both NRR and NRO). Security services such as Data Integrity, Authentication, confidentiality and Non-Repudiation provided with NRO and NRR called MNR have been assured in this proposed method by addressing limitations that are highlighted in EPGP method. In this method, configuration has been proposed to address the limitations of EPGP such as server security aspect and cryptographic processing overhead. First limitation of EPGP i.e., server security aspect is handled by letting one time session key is being encrypted by using receiver's public key and there by maintaining security at their respective ends (at sender and receiver) rather than relying on server which on compromising let the entire senders and receivers compromise. Second limitation of EPGP are handled by allowing the server to forward message to receiver and Digital Signature of the message to the sender in secure fashion without involving much cryptographic processing.

In this method, one-time-only session key is allowed to be encrypted by using receiver's public key and server let to forward only hash of the message rather than the message. Hash of the message consists of less and fixed bits based on hash algorithms and there by reduces transmission bandwidth along with cryptographic processing. Server after receiving message from sender calculates hash of the message and forwards it to receiver by requesting it to send Digital Signature that assures proof of receipt to the sender. Once Digital Signature is being obtained from receiver, server forwards Digital Signature to sender and message to receiver that decrypts one-time-session key by using its private key. Once one-time-only session key is known, receiver can obtain the plain text that is sent by sender.

The proposed method includes three phases

I. Transmission phase
II. Secure NNR phase
III. Reception phase

Let A and B be the sending and receiving entities respectively.

D be the server entity and M be the plain text.

H	– Hash Algorithm
DSS_{KU}	- Digital Signature Standard Encryption and Decryption
Z	- Zip Algorithm for compression
E_{KS}	- Symmetric Encryption using one-time-only session key
E_{KU}, E_{KR}	- Encryption using public and private key
D_{KU}, D_{KR}	- Decryption using public and private key
R64	- Conversion to Radix 64 ASCII format
||	-Concatenation

I. *Transmission phase:* Transmission phase of this method is similar to PGP transmission phase but varies with transmission phase of EPGP. In PGP transmission phase, one-time-only session key is encrypted by using receiver's public key whereas in EPGP transmission, one-time-only session key is encrypted by using server public key.

Transmission Phase: Cryptographic Processing at Sender (A)

A: M1 = H[M]

A: $M1^1 = DSS_{KRA}[M1]$

A: $M2 = [M1^1]||[M]$

A: M3 = Z[M2]

A: $M3^1 = E_{KS}[M3]$

A: $M4 = M3^1||E_{KUB}[KS]$

A: M5 = R64 [M4]

II. *Secure NRR phase:* Message obtained from transmission phase is not forwarded to receiver by server. As email system is asynchronous communication system that employs connectionless type of communication, server stores obtained message from transmission until receiver come online. Once receiver comes online, server forwards hash of the obtained message but not message. Receiver calculates Digital Signature on the hashed message and sends to server. This Digital signature sent by receiver assures proof of receipt and is forwarded to sender by the server. Once server sends Digital Signature to the sender, message obtained from sender is forwarded to receiver by the server.

Proposed Method: Cryptographic Processing at Server (D)

A ⟶ D: M5 ---------- (1)

D ⟶ B: M6 = H[M5] ---------- (2)

B ⟶ D: $E_{KUD}[E_{KRB}[M6]]$ ---------- (3)

D ⟶ A: $E_{KUA}[E_{KRB}[M6]]$ ---------- (4)

D ⟶ B: M5 ---------- (5)

$E_{KRB}[M6]$ is Digital Signature calculated by Receiver B and sent to Sender A via Server D.

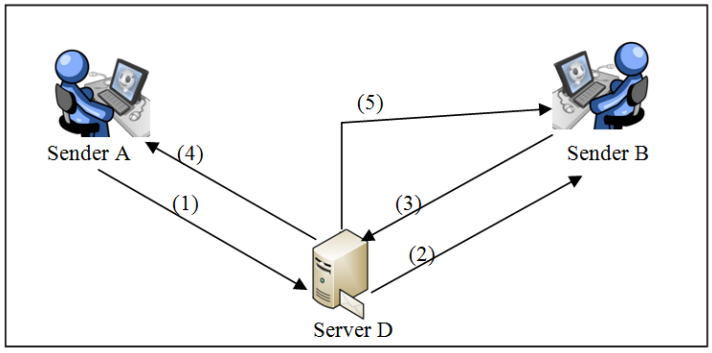

Fig. 1 Architecture specifying Secure NRR Phase (Proposed Method)

III. Reception Phase: Receiver obtains the message from the server, only after forwarding its digital signature to the server. In this phase, receiver performs exactly reverse to the transmission phase to extract the plaintext created by sender.

Cryptographic Processing at Receiver (B)

B: $M4 = R64^{-1}[M5]$

B: $M3 = D_{KRB}[KS] || D_{KS}[M3^1]$

B: $M2 = Z^{-1}[M3]$

B: $M1 = DSS_{KUA}[M1^1]$

M1 message is the obtained hash of the message. M2 message contains plain text and the Digital Signature which upon decryption by using public key of sender obtains hash of the plain text. This obtained hashed message is verified against the calculated hash obtained by hashing on extracted plain text. Data Integrity is ensured when obtained hash and calculated hash are same.

IV. PERFORMANCE COMPARISON

The performance comparison of Enhanced Pretty Good Privacy (EPGP) and the proposed approach which can be termed as Improved EPGP are compared in the following table.

EPGP	***Improved EPGP***
In this approach, one-time-only session key is encrypted by public key of server and thereby led server to involve in the cryptographic processing in sharing one-time-only session key to the receiver during session established between server and receiver.	In this approach, one-time-only session key is encrypted by public key of receiver, resulting server relieved from cryptographic processing overhead for each session established between server and receiver.
EPGP may compromise its security when server is compromised by the attempts of attacker and thus results insecure communication. In this approach server has been involved in security aspect and forwarding role.	Improved EPGP is robust to attacks because of the design that maintains security at the respective ends (sender and receiver) rather than at server i.e., attacks on server cannot result insecure communication because server is only involved in forwarding role.
In this, receiver has been allowed to prepare its Digital signature on the message sent by sender via server.	Improved approach let the receiver to prepare Digital Signature on the hash of the message sent by sender via server and thereby minimizes transmission bandwidth.

Table 1. Comparisons between EPGP and Improved EPGP

V. CONCLUSION AND FUTURE DIRECTIONS

A cryptosystem that provides email communication to the entities requires the effective implementation attaining the four basic pillars of security services such as Data Integrity, Authentication, Confidentiality and Non-Repudiation. PGP method ensured Data Integrity, Authentication, Confidentiality and a part of Non-Repudiation service with best features of conventional, public key encryption algorithms and hash algorithms. PGP with unfair Non-repudiation has been addressed in EPGP method by assuring NRR service along with NRO service resulting MNR service. The configuration to achieve NRR service in EPGP led to limitations which are server security compromising aspect, session key overhead and cryptographic processing overhead at server. This paper addresses the limitations in EPGP method with the proposed method that saves transmission time, storage; more importantly relieved the server from cryptographic processing overhead and session key overhead by letting the senders to use receivers public key to encrypt session key. The proposed method focused on minimal network bandwidth utilization can be employed in the encryption of HTTP request/response traffic over internet. This method achieves MNR service while maintaining security at the respective ends (sender and receiver), encourages its configuration in intranet mailing communication. Server that has been relived from cryptographic processing overheads makes the intranet mailing system scalable. E-commerce applications, banking and financial applications that require MNR with enhanced security and minimal cryptographic processing overhead can also employ this improved approach.

REFERENCES

[1] A.S.N Chakravarthy, A.S.S.D Toyaza, “A Novel Approach for Intranet Mailing for Providing User Authentication”, International Journal of Computer Science and Information Security, Vol. 9, No. 6, pp. 158-162, June 2011.

[2] Vikas Gupta, Harprabhdeep Singh, “Enhance the Data Security Using PGP & DES in MANET”, International Journal of Computer Science and Technology, Vol. 4, Issue 6, pp. 208-213, June 2014.

[3] Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy and A.Z Ghalwash, “Chaotic Encryption Based PGP Protocol”, International Journal of Computer Science and Telecommunications, Vol. 4, Issue 2, pp. 1-8, February 2013.

[4] Babak Nouri-Moghaddam, Mohammad Ismaeil Shahabian, Hamid Reza Naji, “Multi-Agent Based PGP Architecture, International Journal of Research”, Vol. 4, Issue 3, pp 38-47, March 2014.

[5] Suni Ashwathi, Praveen Tripathi, Akhilesh Kosta, “Stegano PGP with Enhance Security”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 12, pp. 1258-1262, December 2013.