Improved Approach for Computer Networking In Pretty Smart Privacy (PGP)

E. Sainiharika[1], K. Sandhya[2], M. Ravali[3], B. Sushma[4]
Department of Computer Science & Engineering
Balaji Institute of Technology & Science, Narsampet, Telangana, India.

Abstract:

A cryptosystem should primarily provide security services like knowledge Integrity, Authentication, Confidentiality and Non- Repudiation (four basic pillars of the cryptosystem). This paper focuses on improved configuration to realize Non-Repudiation service whereas addressing security and crypto logic process overhead problems concerned in providing this service. Non-Repudiation service ensures that repudiation isn't being done by either sender or receiver. This service permits the receiver and sender to be provided by proof of origin and proof of delivery severally within the communication. Non- Repudiation of Origin (NRO) and Non- repudiation Receipt (NRR) services along referred to as Mutual Non-Repudiation (MNR) service and is achieved by the cryptosystem, given that the entities concerned within the communication exchange themselves with proof of origin (Non-Repudiation Origin) and proof of delivery (Non-Repudiation Receipt). This paper provides associate degree approach that addresses problems like inefficient configuration, security breaches concerned within the system and at last relieves the server by material possession it to try and do forwarding tasks during a secure fashion while not compromising the safety.

Index Terms: One-time-only session key, Digital Signature, increased pretty smart Privacy, Mutual Non-Repudiation, Non-Repudiation, Non-Repudiation of Origin, Non-Repudiation of Receipt, and Pretty smart Privacy.

1. INTRODUCTION:

A cryptosystem should primarily offer security services like information Integrity, Authentication, Confidentiality and Non-Repudiation. Information Integrity ensures no modifications throughout the transit of the message over network. Authentication verifies genuineness of the sender and also the receiver. Confidentiality preserves the privacy of the sender and receiver by material possession data accessible to solely licensed users. Non Repudiation ensures that repudiation isn't being done by either sender or receiver. This service permits the receiver and sender to be provided by proof of origin and proof of delivery severally within the communication. Repudiation is one in every of the modern problems within the security aspects, needs high attention to deal with it with an answer specified entities within the communication can't deny the message sent among them. Several protocols are developed to spice up the safety of the e-mail communication that is only once activity

That doesn't need handclasp. There are separate protocols that are wont to offer security for email messages like S/MIME and Pretty smart Privacy (PGP) [3]. PGP by Phil Zimmermann is one in every of those protocols centered to supply security services like information Integrity, Authentication, Confidentiality and Non-Repudiation of Origin. PGP ensures Non-Repudiation of origin that is incomplete Non-Repudiation service light- emitting diode to associate increased pretty smart Privacy (EPGP). EPGP approach centered 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 isa 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.

2. RELATED WORK:

PGP formally has been used for email contents and attachments cryptography [4]. PGP will offer wide selection of services like email and attachment security, digital signature, encrypting of whole hard disc, security of files and folders, encrypted hypertext transfer protocol request/response on the shopper server design [4]. PGP with success enforced security services like information Integrity, Authentication, Confidentiality and a part of Non-Repudiation service that is Non- Repudiation of Origin. In PGP, National Reconnaissance Office service has been achieved by lease the sender to use its non- public key that results Digital Signature whereas composing a message to receiver. Digital Signature that has been ready at sender ensures proof of origin to the receiver. so National Reconnaissance Office service has been achieved because of the default configuration of public key and traditional cryptography algorithms in PGP. In Email system, it's equally needed to implement each services National Reconnaissance Office and NRR however PGP ensures solely National Reconnaissance Office service while not NRR service. so EPGP technique had centered on the configuration to attain NRR service that ensures proof of receipt with the assistance of sure third party referred to as server. the concept of EPGP is to beat PGP's disadvantage of incomplete Non-Repudiation service [1]. EPGP assures NRR by permitting receiver to rewrite message solely when sharing its Digital signature to the server. Digital Signature by receiver assures proof of receipt to the sender and ensures NRR together with National Reconnaissance Office that is one default options of PGP. NRR service depends on one-time-only session key that is encrypted by server public key, permits the receiver to rewrite the message by the receiver however this one-time-only session key's handed over to the receiver, only receiver submits its Digital signature on the message to server that successively 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 each NRR and United States intelligence agency services, has sure 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.

At hand over one-time-only session key to receiver, server created to decode just one occasion session key victimization its non- public key and inscribe once more victimization receiver's public key. This results in crypto logical process (encryption and decryption) overhead for n range of senders and receivers that server acts as third party.

3. PROPOSED METHOD:

The planned technique provides improved configuration for the secure and fewer cryptanalytic process overhead email communication by reassuring Mutual Non- Repudiation service (combination of each NRR and NRO). Security services like knowledge Integrity, Authentication, confidentiality and Non-Repudiation supplied with NRO and NRR known as MNR areassured during this planned technique by addressing limitations that are highlighted in EPGP technique. During this technique, configuration has been planned to handle the constraints of EPGP like server security side and cryptanalytic process overhead. initial limitation of EPGP i.e., server security side is handled by property just the once session secret is being encrypted by exploitation receiver's public key and there by maintaining security at their individual ends (at sender and receiver) instead of looking forward to server that on compromising let the complete senders and receivers compromise. Second limitation of EPGP are handled by permitting the server to forward message to receiver and Digital Signature of the message to the sender in secure fashion while not involving a lot of cryptanalytic process.

In this methodology, one-time-only session key's allowed to be encrypted by victimization receiver's public key and server let to forward solely hash of the message instead of the message. Hash of the message consists of less and glued bits supported hash algorithms and there by reduces transmission information measure together with science process. Server when 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 victimization its personal key. Once one-time-only session key's identified, receiver will acquire the plain text that's sent by sender.

The proposed method includes three phases

1. Transmission phase
2. Secure NNR phase
3. Reception phase

Let A and B be the sending and receiving entities respectively.
D is the server entity and M is 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_K - Encryption using public and private key
D_{KU}, D_K- Decryption using public and private key
R64- Conversion to Radix 64 ASCII format-Concatenation

1. Transmission phase:

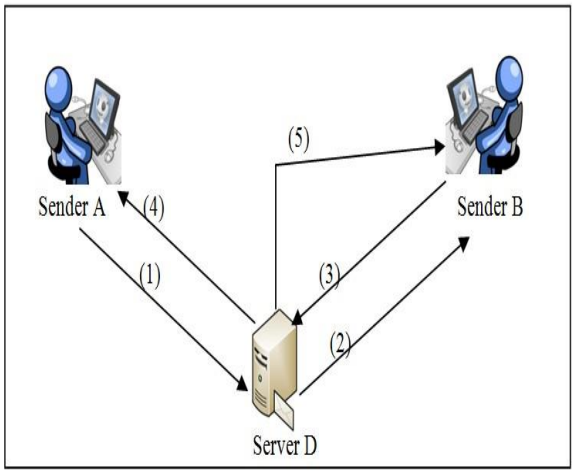
Transmission phase of this method is similar to PGP transmission phase but varies with transmission phase of EPGP. In PGP transmission phase, one-time- only session key is encrypted by using receiver's public key whereas in EPGP transmission, one-time-only session key is encrypted by using server public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

2. 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 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.

3. 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.

4. 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.

Table 1. Comparisons between EPGP and Improved EPGP

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.	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. 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.

5. 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.

6. References:

[1] Ahamed, B. B., & Yuvaraj, D. (2018, October). Framework for Faction of Data in Social Network Using Link Based Mining Process. In International Conference on Intelligent Computing & Optimization (pp. 300-309). Springer, Cham..

[2] Yuvaraj,D., & Dharunyaa, N.R.(2018).Enhanced Data Security Through Data Integrity On Cloud Computing. International Journal of Pure and Applied Mathematics, V118,No.22,P 1079-1083.

[3] Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy and A.Z Ghalwash, "Chaotic Encryption Based PGP Protocol", International Journal of Computer Science andTelecommunications, 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] M, Sivaram, et al. "Securing the Sensor Networks Along With Secured Routing Protocols for Data Transfer in Wireless Sensor Networks." Journal of Emerging Technologies and Innovative Research, vol. 5, no. 10, Oct. 2018, pp. 316–321., doi:http://doi.one/10.1729/Journal.18612.