International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 5 Issue 3, March-2016

Enhanced E-mail Security Protocol Based on Hybrid Cryptographic Systems

Dr. Mahmood Khalel Ibrahem

Al-Nahrain University, College of Information Engineering, Iraq

ABSTRACT

E-mail becomes an important service in the digital economy and E-mail security has become a hot topic in Information Technology circles as new threats, exploits and vulnerabilities affecting E-mail clients by inusing sophisticated tools. Researchers have developed a number of security protocols and services, but still it needs further work to be done. In this paper we discuss famous existing E-mail security protocols and their drawback, and present a new protocol based on public key cryptography to transfer secret key securely and symmetric cryptosystems to provide authentication, confidentiality, and integrity.

Keywords: E-mail, S/MIME, PGP, Security Services.

1. INTRODUCTION

Electronic mail is considered as a significant business tool and grew vastly during the last decade from simple local area network linking a few users on a single computer to large international networks connecting users on millions of different hosts with addition of using mobile access and wireless networks. This development brings a large number of threats that endanger information communication and commercial activities, which consequently create increasing demands of organization to keep their electronic mail, secure [1].

Electronic mail security requirement is not far from traditional paper mail security requirement. Authentication, integrity and confidentiality services are the main security services that required by both, paper and electronic mail (a signed message is protected inside an envelope). Users want to have confidence about the sender of the mail and originality and secrecy of the contents. Beside Authentication, Electronic mail Encryption and Electronic mail Digital Signature are needed to achieve integrity and confidentiality in Electronic mail messaging [2].

Existing electronic mail security systems that use symmetric and asymmetric cryptographic schemes suffer from key management problems. Identity Based Cryptography (IBC) systems, which have been proposed to address such key management issues, also suffer from the key escrow problem, which violates the non-repudiation feature that should be offered by security systems [3]. In this paper, literature survey of previous work and existing e-mail security systems is presented. A simple prototype of e-mail security protocol is proposed to enhance security services for e-mail clients.

2. LITERATURE SURVEY

A. Suresh Kumar Balakrishnan and V. P. Jagathy Raj (2016) proposed an implementation of a practical, secure email system based on "certifcateless cryptography, which uses Domain Name System (DNS)" as the infrastructure for public key exchange and a secure key token fingerprint authentication system for user authentication. The message payload is encrypted by a per-email symmetric key generated from a secret value, the public and private keys of both the sender and the receiver. They claimed that the proposed mailing system is secure against standard security model [4].

B. Nik Unger etal. (2015) evaluated existing secure electronic mail systems and present an evaluation framework for their "security, usability, and ease-of-adoption properties". They identify "innovative and promising approaches used in the wild" that are not considered by the academic literature. They identified three key challenges: "trust establishment, conversation security, and transport privacy".

They claimed that "Trust establishment approaches offering strong security and privacy features perform poorly from a usability and adoption perspective, whereas some hybrid approaches that have not been well studied in the academic literature might provide better trade-offs in practice". Finally they concluded, "transport privacy appears to be the most difficult problem to solve without paying significant performance penalties" [5].

C. Ladar Levison (2014) presented a comprehensive document of the design of the "Dark Internet Mail Environment (DIME)", also they presented the requirements for successful implementation of "DIME" including the protocols and message format specification. This document provides an analysis of security attack vectors and a discussion covering techniques to mitigate those vectors. The security of DIME is dependent on the strength of the user's password and the strength of an endpoint's defenses. DIME strives to create a secure system that guarantees the secure delivery of email while minimize leakage of information along the delivery path [6].

D. Gurpal Singh Chhabra and Dilpreet Singh Bajwa (2015) reviewed working and architecture of current email systems and the security protocols followed generally to secure email communications and the limitations they contained, further email forensics which is a process to analyze email contents, header information, transit path for email, sender or receiver information and other details to collect evidence against culprit or to secure their proposed system. They also discussed common email forensic investigation technique and tools used in email forensic process [7].

E. Shahin Fatima etal. (2015), explored the differences between X. 509 and PGP Public key Infrastructure methods. They discussed in their paper X.509 certificate, creation of certificate, revocation of certificate, its authentication procedures and PGP certificates. They presented an analysis to highlight the differences between both systems and to provide the reasons for their usage. They concluded that the main drawback of PGP is how to distribute public keys. They considered the X.509 method is more flexible and advanced than the PGP method because in PGP it requires that everybody that participates in it takes responsibility and makes decisions for himself. However they thought that the X.509 is the right approach, because of personal privacy and security reasons [8].

F. Afnan S. Babrahem etal. (2015) presented various methods to enhance the security services of electronic mail systems. They found that the main enhancements are in authentication of user identity, confidentiality and privacy of the e-mail communication. They showed that "those enhancements have improved the performance of the proposed systems and they reached the required level of security". They summarized a "comparison between the proposed systems according to their level of security, and figured out the limitations of each system in order to execute them in a future work" [9].

G. Hongfeng Zhu etal. (2015) proposed a new one-way authenticated key agreement scheme based on multi-server architecture. Compared with related literatures recently, they claimed that "the proposed scheme can not only own high efficiency and unique functions, but is also robust to various attacks and achieves perfect forward secrecy". Finally, they presented "the security proof and the efficiency analysis of the proposed scheme" [10].

H. Sameera Mushtaq etal. (2015) gave a general depiction of different cryptographic methods with parameters. They claimed that each method and calculation is novel in its own particular terms. They conclude that Private Key encryption, quantum cryptography and crypto steganography are the best in light of the fact that these are so fiery and quick that they can't be delicate effectively. Distinctive methodologies have exhibited through the level of security increments [11].

I. Italo Dacosta etal. (2014) presented "EmailCloak, an email alias service with public key encryption capabilities which relaxes email encryption requirements by relying on a privacy-respecting third-party". Emails sent and received by the user are automatically encrypted with his/her public key by EmailCloak before being forwarded to, and stored by his/her email provider. They claimed that "this approach, offers multiple benefits: simplified key management, selective and automatic encryption, advanced deployment options and transparency towards other parties". Moreover, they concluded that their "experimental evaluation shows that the overhead introduced by EmailCloak is adequate for email communications". They made their implementation publicly available [12].

J. Dharmendra Choukse etal. (2012) explained "inherent weakness in email infrastructure and methodologies to improve the security of the email infrastructure". They also point out in their paper advantages and disadvantages in different aspects of electronic mail infrastructure design approaches and the implementation of Email Security in IPS Academy [13].

3. EXISTING E-MAIL SECURITY SYSTEMS

The most common scenario of e-mail exchange is a one-way system, which implies that clients are connected to the e-mail server through a LAN or a WAN. Clients invoke User Agent program (UA) and Message transfer Agent (MTA) to prepare and transmit messages. MTA program is responsible for transfer of messages between sender and receiver servers. Security protocols is implanted within the e-mail architecture to provide security services such as; authentication, integrity and confidentiality. Two famous e-mail security protocols will be discussed below.

A. Secure/Multipurpose Internet Mail Extension (S/MIME)

S/MIME is an electronic mail security protocol which is developed to provide security services for electronic mail and guarantee the confidentiality and non-repudiation of electronic messages. The protocol is an extension of the

"Multipurpose Internet Mail Extension (MIME) protocol". S/MIME support several cryptographic algorithms such as Triple DES (TDES), AES, RC2/40, RSA, Diffie-Hellman, SHA-1, and Digital Signature Standard (DSS). S/MIME uses secured certificate information to produce a public key cryptography standard (PKCS) object and message hash value which will be encrypted using the initiator private key [8].

The S/MIME protocol is based on public-key cryptography; therefore, it encrypt the content of the message but does not encrypt the communication. The components of the message are encoded according to the MIME standard, and encrypted using a session key. The session key is enclosed in each section's header, and encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message. Non-repudiation of recipient achieved by the use of signed receipt. However, this assumes the recipient to be a fair participant in the sense that the recipient returns a signed receipt, if the sender asks for it. Therefore, non-repudiation depends on the recipient's decision [14, 15].

The message's hash is encrypted with the sender's private key, interceptors can read the content of the message's hash, but this will guarantee the sender's identity, since only the sender can encrypt a message with his private key and decrypt with his public key [16].

B. Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a public key cryptography electronic mail security systems and considered as one of the most advanced encryption algorithms on the market existing for over 25 years. It combines best of conventional and public key cryptography. First of all, a pair of Public and Private key has to be generated with a secure passphrase. Then, Public key has to be shared with all intended recipients. Private key should never be shared [14, 15]. Encryption of the message content happens directly on the user device, by using the recipient's Public key. Once it reaches recipient device, the only way to decrypt it, is by use of unique Private Key with the correct passphrase at the moment of decryption.

To guarantee that the message contents have not been altered during transmission, a message can be digitally signed. Message signing happens at the moment of sending and is signed by a unique Private Key of a sender. Verification happens on the recipient's device with a sender Public key and no passphrase is required for signature verification [16]. However, PGP suffer some drawback such as key ring management because in PGP it requires that everybody that participates in it takes responsibility and makes decisions for himself. Generally, key management is one of the challenges in PGP and PKI-based systems. In order to initiate a secure communication in PGP, sender requires to obtain the receiver's public key in advance. There are many public key servers from where we can retrieve other keys of other people and we can store our keys also. Moreover, servers also do not check to ensure that the person who is storing the key is actually the same person indicated by the key identifier. Secure channel is required to protect it from man-in-the-middle attacks [7].

PGP users' needs to store private key ring backup in a safe place in order to be able to decrypt old encrypted messages. Moreover, If private key is compromised, then old or new messages can be decrypted, therefore, PGP needs to create a certificate revocation list (CRL) to store compromised keys which must be shared with all users [8].

4. PROPOSED E-MAIL SECURITY PROTOCOL

Sending an e-mail is a one-way activity and no session process, hence there is no handshaking to negotiate on cryptographic algorithms. In e-mail security, the sender of the message needs to include the name or identifier of the algorithms used in security services. Consequently, secret key needs to be sent in secret with each message using public key of the receiver as an attachment with the message.

The proposed protocol is a prototype protocol which uses public key cryptography to encrypt secret key ($_{Ks}$) of the sender and send it securely to the recipient, and uses generated secrete key to sign and encrypt the message to guarantee integrity and confidentiality. Authentication and non-repudiation is maintained by sending random number (Nonce) to both; the server and the recipient. The protocol consists of two stages;

The first stage comprises of clients registration and delivering their identification and public keys to the e-mail server and this can be done one time. The second stage starts when a registered client wish to send a message to any other registered client. The second stage includes requesting public key of the recipient and perform required security services (Integrity, confidentiality), and secret key encryption. The second stage ends with receiving recipient's receipt of reception from the recipient to the sender.

The proposed protocol is listed below. Figure-1 illustrates the architecture of protocol, figure-2 illustrates message transmission and reception flowchart, figure-3 shows message transmission block diagram, and figure-4 shows message reception block diagram.

Notation

||	Concatenation
A, B, … N	Clients
CM	ciphered Message
D	Decryption process
E	Encryption process
ID_i	Identifier of client i
K_s	Secret Key
M	message
N_{ij}	Random Number (Nonce) created by client i and sent to client j
PR_i	Private key of client i
PU_i	Public key of client i
PW_i	Password of client i
S	E-Mail Server
SG	sign a message
SM	signed message

Registration Stage (All Clients Create E-Mail Account)

1. Create Account (All Clients create Accounts)

A: generate ID_a, PW_a A → S: ID_a, PW_a
B: generate ID_b, PW_b B → S: ID_b, PW_b
…….
N: generate ID_n, PW_n N → S: ID_n, PW_n

2. Initialization (All Clients Generate Public Key Pair)

A: generate PU_a, PR_a A → S: $E(PW_a, PU_a)$
B: generate PU_b, PR_b B → S: $E(PW_b, PU_b)$
……
N: generate PU_n, PR_n, PW_i N → S: $E(PW_i, PU_n)$

Communication Stage

1. A:S (A Request PUb from Server)

A → S: $E(PW_a, ID_a || ID_b || N_{as})$
S → A: $E(PW_a, PU_b || N_{as})$
A: $D(PW_a, PU_b || N_{as})$ → get PU_b, verify N_{as}?

2. A: B (A Send Message to B)

A: compose M, generate Ks, N_{ab}
Integrity?: $MS = SG(K_s, M)$
Confidentiality?: $MC = E(K_s, M)$
A→ B: $E(PU_b, K_s) || E(K_s, N_{ab}) || E(K_s, M)$

3. (B Receive Message)

B: $D(PR_b, K_s)$ → get K_s
$D(K_s, N_{ab})$ →get N_{ab}
$D(K_s, M)$ → get M
$SG(K_s, M)$? → Compare MS' = MS?
B → A: $E(PU_a, N_{ab})$
A: $D(PR_a, N_{ab})$ → verify N_{ab}?

5. PROPOSED PROTOCOL SECURITY SERVICES

A. Authentication

The proposed system is an identity based authentication system, in which the sender login to the server using his password then uses his password (PW_a) to encrypt his request to the server with the addition of using a nonce random number (N_{as}) to authenticate the server by verifying this number from the server reply. This procedure implies mutual authentication between the server and the sender. The following protocol fragment illustrates the procedure.

A → S:	$E(PW_a, ID_a \| \| ID_b \| \| N_{as})$	
S → A:	$E(PW_a, PU_b \| \| N_{as})$	
A:	$D(PW_a, PU_b \| \| N_{as})$	→ Get PU_b, verify N_{as}?

B. Secret Key Exchange

The protocol uses public key encryption to transmit the secret key (Ks), while using symmetric encryption to sign and encrypt the message. The secret key is encrypted with the public key of the receiver (PU_b) and concatenated with the encrypted message. With the addition, the protocol perform mutual between sender (A) and receiver (B) by encrypting a random nonce number (N_{ab}) and verifying the returned number from the receiver reply.

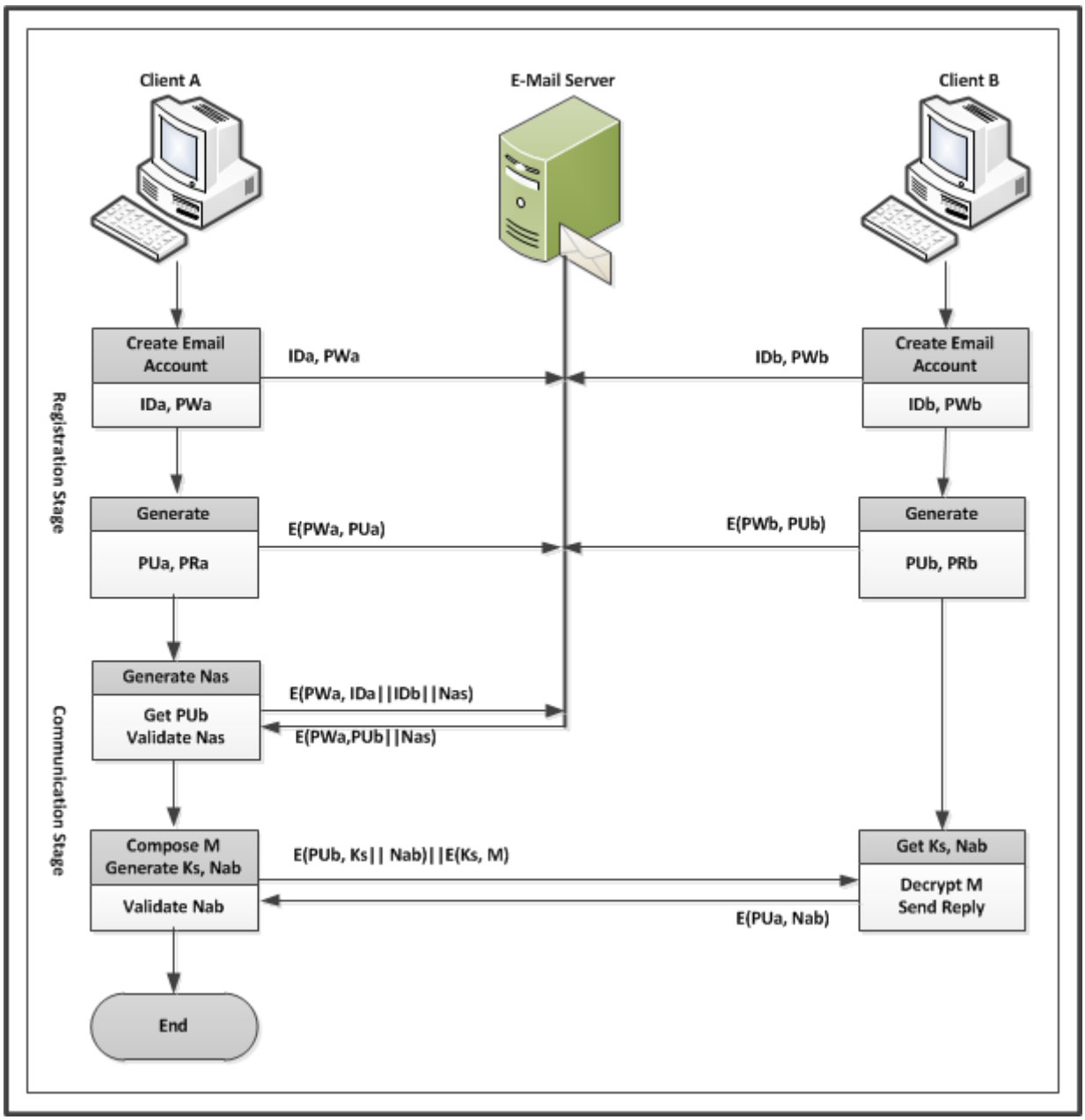

Figure 1 proposed Secure E-Mail Protocol

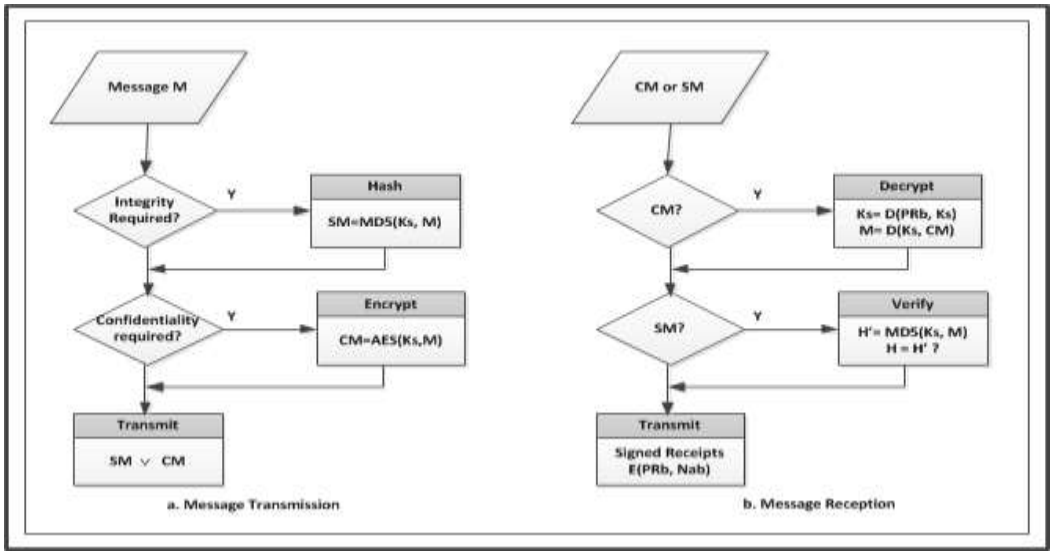

Figure 2 a. Message Transmission flowchart, b. Message Reception Flowchart

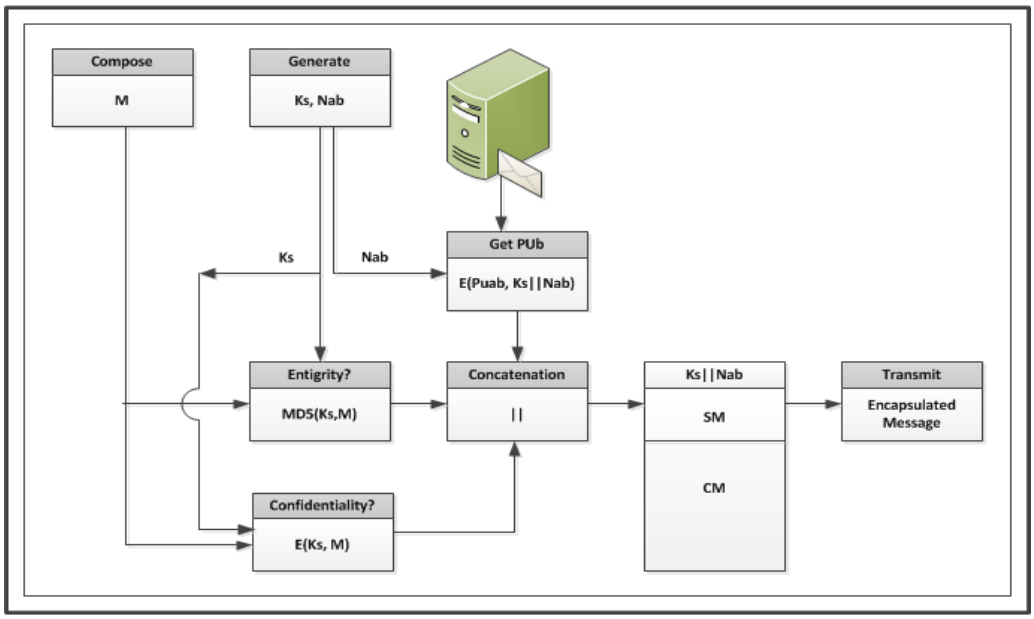

Figure 3 Message Transmission Block Diagram

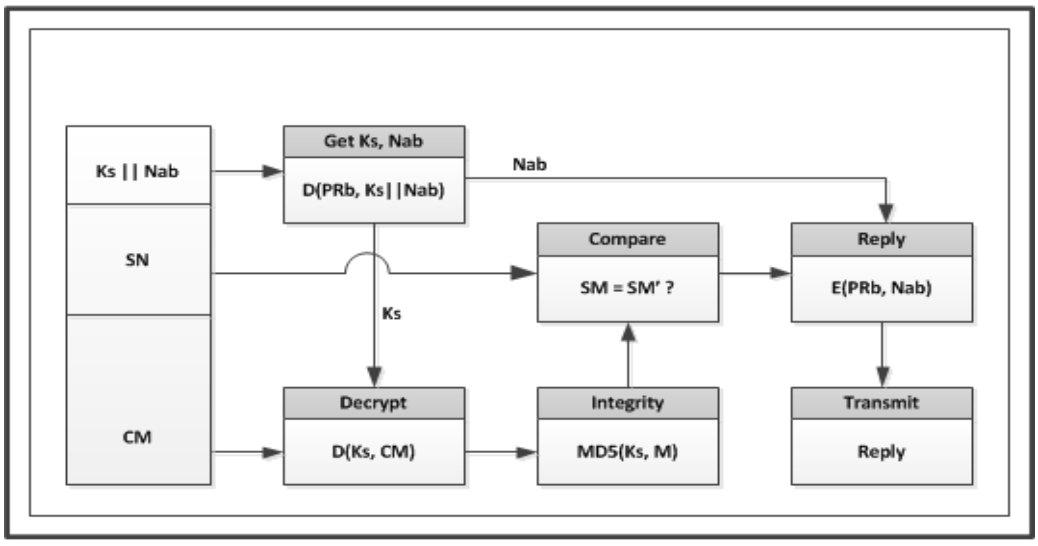

Figure 4 Message Reception Block Diagram

C. Integrity and confidentiality

The protocol perform integrity and confidentiality as an optional services according to the user requirements; if the sender choose to sign the message then the protocol will sign the message (using MD5 for example) with the generated secret key (K_s) to produce message signature (MS). The same thing is done with message encryption to produce ciphered message (MC). The whole message is encapsulated and transmitted to the receiver. The following protocol fragment illustrates those functions. Figure-5 illustrates the transmitted message format.

A: compose M, generate Ks, N_{ab}	
Integrity?:	$MS = SG(K_s, M)$
Confidentiality?:	$MC = E(K_s, M)$
A→ B:	$E(PU_b, K_s) \| E(K_s, N_{ab}) \| E(K_s, M)$

The receiver decompose the received message into three parts; decrypt the first part (secret key $K_{s)}$ using his private number (PR_b), then he uses this key to verify the message signature (MS) and decrypt the ciphered message (MC). Finally the receiver encrypts nonce number (N_{ab}) with sender public key (PU_a) and resend it to the sender to complete mutual authentication. The final step can be considered as receipt acknowledgment. The following protocol fragment illustrates those functions.

$D(PR_b, K_s)$ → get K_s		
	$D(K_s, N_{ab})$	→get N_{ab}
	$D(K_s, M)$	→ get M
	$SG(K_s, M)$?	→ compare MS' = MS ?
B → A:	$E(PU_a, N_{ab})$	
A:	$D(PR_a, N_{ab})$	→ verify N_{ab}?

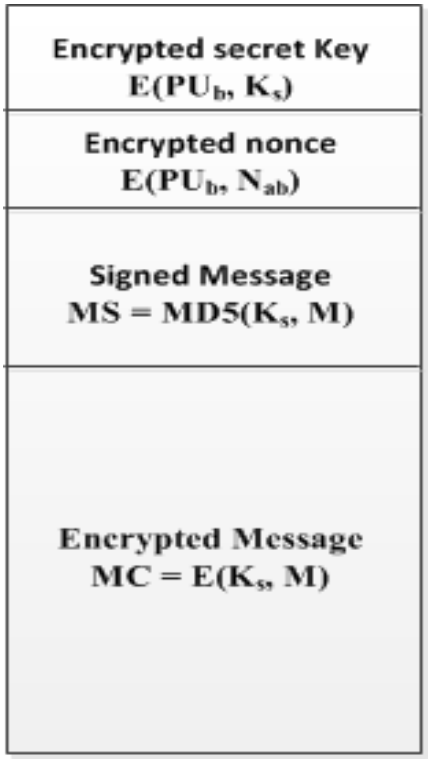

Figure 5 Transmitted Message Format

CONCLUSIONS

a. The proposed protocol released the user from the problem of key ring management appeared in PGP system and resolved it by E-mail server key management system.

b. Key management in the proposed protocol is transparent to the user; the only secret information to be kept by the user is his password.

c. Further elaboration of the proposed protocol is needed for implementation purposes.

REFERENCES

[1]. Arwa Husien, and Ghassan Samara, **"Application Layer Protocols to Protect Electronic Mail from Security Threads",** International Conference on Information Technology, ICIT 2015.
[2]. Tejaswini Herath, Rui Chen, Jeff Wilbur, Jingguo Wang, Ketan Banjara & H. Raghav Rao "**Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service**", Info Systems J, 2012.
[3]. Salah Alabady**, "Design and Implementation of a Network Security Model for Cooperative Network",** International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009.
[4]. Suresh Kumar Balakrishnan and V. P. Jagathy Raj, **"Practical Implementation of a Secure Email System Using Certi_cateless Cryptography and Domain Name System**", International Journal of Network Security, Vol.18, No.1, PP.99-107, Jan. 2016.
[5]. Nik Unger, Joseph Bonneau, Sergej Dechand, Sascha Fahl, Ian Goldberg, Henning Perl and Matthew Smith, "**SoK: Secure Messaging**", Symposium on Security and Privacy, IEEE 2015.
[6]. Ladar Levison, "**Dark Internet Environment: Architecture and Specifications**", National Security Agency, December 2014.
[7]. Gurpal Singh Chhabra, Dilpreet Singh Bajwa, **"Review of E-mail System, Security Protocols and Email Forensics",** International Journal of Computer Science & Communication Networks,Vol 5(3), 201-211, 2015.
[8]. Shahin Fatima, Shish Ahmad, Shadab Siddiqui, "**X. 509 and PGP Public Key Infrastructure methods: A critical review**", IJCSNS International Journal of Computer Science and Network Security, Vol.15 No.5, May 2015.
[9]. Afnan S. Babrahem, Eman T. Alharbi, Aisha M. Alshiky, Saja S. Alqurashi and Jayaprakash Kar, "**Study of the Security Enhancements in Various E-Mail Systems**", Journal of Information Security, Vol. 6, 1-11, 2015.
[10]. Hongfeng Zhu, Yifeng Zhang, and Yan Zhang, "**A One-Way Authentication Key Agreement Scheme with User Anonymity Based on Chaotic maps towards Multi-Server Architecture**", Journal of Information Hiding and Multimedia Signal Processing, Vol. 6, No. 2, March 2015.
[11]. Sameera Mushtaq, Iqra Rafiq and Mehreen Sirshar, **"Quality Analysis of Network Security Using Cryptographic Techniques",** International Journal of Computer and Communication System Engineering (IJCCSE), Vol. 2 (2), 246-254, 2015.
[12]. Italo Dacosta, Andreas Put and Bart De Decker, "**Email Cloak: A Practical and Flexible Approach to Improve Email Privacy**", 9th International Conference on Availability, Reliability and Security, 2014.
[13]. Dharmendra Choukse, Umesh Kumar Singh, Lokesh Laddhani and Rekha Shahapurkar, "**Designing Secure Email Infrastructure",** IEEE, 2012.
[14]. William Stallings, "**Cryptography and Network Security; Principals and Practice**", 5th Ed. 2009.
[15]. Behrouz A. Forouzan, "**Cryptography and Network Security**", McGraw-Hill Int. Ed. 2008.
[16]. Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy and A. Z. Ghalwash, "**Chaotic Encryption Based PGP Protoco**l", International Journal of Computer Science and Telecommunications, Vol. 4, Issue 2, February 2013.