International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Review towards Email Security by using Message Encryption and Digital Signature

Radhika P. Yawale†* and V. B. Gadicha†

†Computer Science and Engineering, P. R. Patil COET Amravati, Maharashtra, India

Accepted 20 March 2015, Available online 25 March 2015, **Vol.5, No.2 (April 2015)**

Abstract

Now a day's electronic mail is the most widely used application on the internet. Using email, a various internet users can send a messages to other internet users. At the same time security of an email messages is the biggest important issue while sending the sensitive information, like bank transactions, commercial secrets, even countries intelligence information are being deliver through emails. So to achieve email security we need to use such a mechanism which provides the security to these emails. For this we can used the S/MIME (Secure Multipurpose Internet Mail Extension) for secure email communication. So, in this paper I present the review on the security mechanism provided by S/MIME which has been Industry standard for secure email exchange.

Keywords*: Email security, massage encryption, digital signature, S/MIME, SMTP, PGP.*

Introduction

Traditional email systems using the text base SMTP protocol, which means that a person can compose a text message and send it over the internet to the recipient. But in the modern era, only exchanging the text messages is not quite sufficient, people wants to exchange the multimedia messages like audio, video, images etc. So, for this we use the MIME protocol(Multipurpose Internet Mail Extensions) which is defined in RFCs 2045 to 2049. Where five new headers are added in the email system by the MIME specification, these are MIME-version, content-type, content-transfer-encoding, content-id, content-description. To provide the security to the basic MIME system we have to used the S/MIME. S/MIME secures the MIME entity by using mainly two services data encryption and digital signature. MIME entity is nothing but the entire message or it may be sub part of whole message. Digital signature and message encryption achieve the authentication, data integrity, non-repudiation, and data confidentiality respectively.

Objective

- To enhance the data security in email system.
- It provides attractive functions for higher flexibility of email communication.
- To provide a comprehensive solution to the security issues that affect SMTP-based Internet e-mail system along with widespread e-mail connectivity.
- To maintain the data integrity, authentication and non-repudiation of multimedia message over emails using digital signature and encryption.

Review of Literature

For the text email messages RFC 822 defines the format. An email message consist of mainly consist of two portions: body of the message and headers. Very first SMTP was used for the email communications. If we are using the SMTP protocol then electronic mails are transfer within the servers of client and senders. SMTP it's a connection oriented and text based protocol. But there are some drawbacks like it doesn't provide any security services also it uses only 7-bit ASCII representation for characters. 7-bit ASCII cannot represent special characters whose ASCII value is greater than 127. Also SMTP cannot send any binary data.

Extending the RFC 822 mail standard, the new standard Privacy Enhanced Mail(PEM) is developed by the Internet Activities Board's Privacy Task Force (D. Crocker *et al*, 1982). There are various features are offered by the PEM like encryption, non-repudiation, and message integrity. In PEM digital certificates are used for the authentication. But there is some drawback with PEM that the user's public key is certified by their local CAs, and this local CAs must certified by policy CA, which itself needed to be registered to the root CA known as Internet Policy

*Corresponding author **Radhika P. Yawale** is a Student and **V. B. Gadicha** is working as HOD

Registration Authority(IPRA) (D. Chandwick, N. Cicovic, A. Young *et al*, 1997). Because of such infrastructure, mostly PEM based email system are not establish.

Phil Zimmerman creates the Pretty Good Privacy protocol in 1991. He is a father of PGP. In which during secure communication mainly five operations will be perform that is digital signature, compression, encryption, enveloping and finally base 64 encoding (H. C. Van Tilborg *et al*, 2005). It provides the confidentiality, authentication, data integration and non-repudiation security services. In which session key is used for message encryption with symmetric key encryption technique again session key is encrypted by using asymmetric key encryption technique. Unlike PEM, PGP does not needed that user's public key certified by CAs. In which user will decide her level of trust on certain certificate. PGP decides the trust model for itself known as "web of trust" (S. L. Garfinkel, D. Margrave, J. I. Schiller, R. C. Miller, E. Nordlander *et al*, 2005). But PGP having some negative aspects like it does not support non textual data. It mainly deal with the private key and if it is lost then data also losted.
Multimedia Internet Mail Extension (MIME) is allow to send non-ASCII data or we can say that multimedia messages like audios, videos, images etc. (J. R. Blum *et al*, 2002) by adding some additional headers like MIME-Version, Content-Type, Content-Transfer-Encoding, Content-Id, Content-Description. To provide the security to the MIME contents S/MIME(Secure/Multimedia Internet Mail Extension) is used. S/MIME uses the different cryptographic algorithms like Diffie-Hellman, RSA, SHA-1 or DES 3.

Working of S/MIME

The S/MIME standard is based on the principal of public key encryption which is used to authenticate the sender and provides the data confidentiality. In which sender will generates the digital signature by applying a SHA-1 algorithm on the message content which results the message digest, after that message digest is then encrypted by the senders private key and finally we have get the digital signature. Then this digital signature is append to the message and send it to the receiver side. After that receiver will verify the signature and confirms that the message was come from proper person.

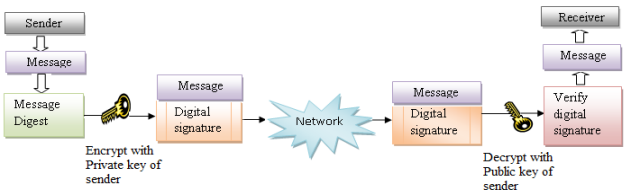

Fig 1: Creation and verification of digital signature

In addition, message is encrypted by using session key which provides the data confidentiality. The session key is then encrypted by using public key of receiver. So, that only the recipient is able to open the message body by using receiver's private key which maintains the confidentiality. Here Diffie-Hellman algorithm is used for exchanging a key.

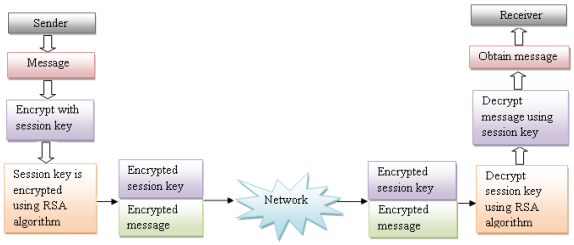

Fig 2: Encryption in S/MIME

Security services of S/MIME

S/MIME mainly provides the two security services which are known as digital signature and message encryption.

- **Digital signature**

Digital signature is one of the important service provided by the S/MIME, also it provides the following services:

1. **Authentication:** In authentication both sender and receiver should be authenticated. It means both the sender and receiver should be able to confirm the identity of the other party involved in communication. In face to face human communication it is very easy to solve this problem by human reorganization. But over any medium when two communicating entities never see each other then authentication is very difficult. So, by using digital signature this problem will solve.
2. **Non-repudiation:** The uniqueness of signature prevents the possibility of denying something after having done it by the sender. Which means the non-repudiation does not allow the sender of a message to disprove the claim of not sending that message.
3. **Data Integrity:** If sender will send any message and it will not reach to the receiver side as it is then we can say that the integrity of message is not maintain. Digital signature will provide the data integrity service. When receiver verifies the signature then he assured that the message that was obtained is the same message that was signed and send by the sender, no alteration has been done during transmission.

- **Message encryption**

Message encryption is the another important security service provided by S/MIME. Actually encryption it's a way of changing a message in unreadable form because of which no one can understood until it is not change

back to the readable form. It will again provide following services:

1. **Confidentiality:** Data confidentiality means no one is able to understand the contents of message only receiver is able to read that message only after decrypt that message by using some specific key. For encryption of message different encryption algorithms are used like RSA which is a asymmetric algorithm.
2. **Integrity:** With digital signature, message encryption is also maintains the data integrity.

Security issues with S/MIME

- If any sender wants to send any private message to the multiple users then sender needs to generate multiple envelopes for the different recipients. Then all the envelopes are collect in the stack and then send it to each of the user (K. Chen, W. Wei, X. Ding *et al*, 2005). This approach of S/MIME maximizes the computational cost at the sender's side.
- S/MIME does not provide the protection to the headers. In RFC 2633 clearly given that S/MIME version 3 does not provide any type of protection to the header, it will only protect the contents of message (B. Ramsdell *et al*, 1999).
- S/MIME permit email clients to store emails as they receive in the form of encrypted format with the recipient's public key, which can be decrypted by corresponding private key of receiver. But if the private key get lost or expired and he revokes new key then stored emails are not accessible (S. L. Garfinkel *et al*, 2003).

Conclusion

Technically S/MIME offers the better security services in email communications like authentication, data integrity, non-repudiation, confidentiality, which makes the email communication more powerful in a secure manner.

Unlike other security protocols like PEM and PGP, S/MIME provides the security to the multimedia messages like audio, video, images etc. S/MIME provides the better way for the regular users of online communication. It doesn't required any additional software to be install. And it is well adapted to any possible future technology.

References

D. Crocker (1982), RFC 822: Standard for the format of ARPA internet text message.

D. Chadwick, N. Cicovic and A. Young.(1997), Merging and extending the PEM and PGP trust models-the ICE-TEL trust model. *Network, IEEE,* 11(3).

H. C. van Tilborg (2005), Encyclopedia of Cryptography and Security. *Springer-Verlag New York, Inc., Secaucus, NJ, USA*.

S. L. Garfinkel, D. Margrave, J. I. Schiller, R. C. Miller and E. Nordlander (2005), How to make secure email easier to use. In CHI '05: *Proceedings of the SIGCHI conference on Human factors in computing systems, pages 701-710, New York, NY, USA, ACM.*

R. Blum.(2002), Open Source Email Security. *Sams Publishing*, USA.

K. Chen, W. Wei and X. Ding.(2005), Multiplex encryption: A practical approach to encrypting multi-recipient emails. In *ICICS,* pages 269-279.

B. Ramsdell (1999) RFC 2633: S/MIME version 3 message specification

S. L. Garfinkel.(2003), Enabling email confidentiality through the use of opportunistic encryption. In dg.: *Proceedings of the annual national conference on Digital government research, pages 1-4. Digital Government Society of North America*

Minhaz Fahim Zibran. (2011), Cryptographic Security for Emails: A Focus on S/*MIME, The University of Saskatchewan Department of Computer Scienc*

K.Suganya(2013), A Novel Approach for S/MIME, *International Journal of Advance Research in Computer Science and Management Studies.*