A Survey on S/MIME E-mail Security

Mrs. Bansari H Kotecha[1], Prof. Tushar J Raval[2], Prof. Karishma A Chaudhary[3]

[1] *Student, Computer Engineering Department, L D college of Engineering, Gujarat, India*
[2] *Associate Professor, Computer Engineering Department, L D college of Engineering, Gujarat, India*
[3] *Assistant Professor, Computer Engineering Department, L D college of Engineering, Gujarat, India*

ABSTRACT

Many organizations, both large and small, face difficult choices when considering secure data transfer between stakeholder groups. Virtual teams made up of internal colleagues, outside partners and even potential clients find need to collaborate effectively and securely, requiring cost effective ways to authenticate the integrity of data they receive but also the need to maintain confidentiality.This is especially true with data transmission systems using the open Internet to relay e-mail and storage being so freely available in the "cloud" to collaborate (Google Docs,Dropbox etc). This paper focuses on the S/MIME protocol which occupies an ever-evolving space in the communications spectrum. Over time it has proven to be robust enough to cope with an array of different environment preferences and requirements.

Keyword : - *E-mail Security , S/MIME, Email Certificates*

1. Introduction

Email has been a very common medium of communication these days. It somewhat replaces the traditional surface mail and many of the traditional ways of communication Today people send and read emails from their personal computers, business workstation, PDAs and even cell phones. As people do more business communication over email, their requirement for email security increases. A huge volume of information travels over internet among people and organizations. The owner of sensitive information and important business correspondence over emails needs to be secured from any possible forgery. Moreover, there is need for privacy, authentication of authorship, and confirmation of email delivery to the destined recipient . In surface mail privacy is maintained, as messages remain sealed in envelopes. Surface mail delivery may be confirmed by taking signature from the recipient upon delivery of the mail. But such mechanisms are not available for email messages. significant efforts have been made to apply cryptographic techniques to achieve email security. Among them, Secure/Multipurpose Internet Mail Extension (S/MIME) probably most widely used.

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME. It is on an IETF standards track and defined in a number of documents, most importantly RFCs. S/MIME was originally developed by RSA Data Security Inc. S/MIME (Secure / Multipurpose Internet Mail Extensions) is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages described in RFC 1521.

The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication. The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key. The session key is inserted in each section's header, and is 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. In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication

can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.

1.1 Function

S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). S/MIME specifies the application/pkcs7-mime (smime-type "enveloped-data") type for data enveloping (encrypting): the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an application/pkcs7-mime MIME entity.S/MIME functionality is built into the vast majority of modern e-mail software and interoperates between them.

1.2 Security Services of S/MIME

S/MIME provides two security services: Digital signatures & Message encryption

1.1.1 Digital Signatures

Digital signatures are the more commonly used service of S/MIME digital signatures provide the following security capabilities: Authentication, Nonrepudiation, Data Integrity.

1.1.2 Message Encryption

Message encryption provides a solution to information disclosure. SMTP-based Internet e-mail does not secure messages. An SMTP Internet e-mail message can be read by anyone who sees it as it travels or views it where it is stored. These problems are addressed by S/MIME through the use of encryption. Encryption is a way to change information so that it cannot be be read or understood until it is changed back into a readable and understandable form. Although message encryption is not as widely used as digital signatures, it does address what many perceive as the most serious weakness in Internet e-mail. Message encryption provides two specific security services: Confidentiality, Data Integrity

2. E-mail Certificates

2.1 Personal E-mail Certificates

An E-mail Certificate (EC) is a digital signature certificates that is used for the purpose of signing and encrypting e-mail messages and authenticates an e-mail address. A Personal Email Certificate (PEC) is an E-mail Certificate that authenticates an e-mail address of an individual. This certificate contains an e-mail address in subject field or subject alternate field. The structure and format of these certificates may vary across CAs, however, the key usage included in these certificates is at least “Digital Signature” and “Key Encipherment”. The certificate may be used for signing in case digital signature is indicated by key usage extension and email protection OID is included in extended key usage extension. Signing may be permitted but the certificate may put restriction on encrypting S/MIME messages in case the extended key usage extension is present in it. Interpersonal message S/MIME receiving agents must check *emailProtection* or the *anyExtendedKeyUsage* OID in case the extended key usage extension is present in the certificate. The explicit presence of only extended key usage extension or other OIDs as well may be required for S/MIME uses other than interpersonal messaging. In an e-mail certificate *digitalSignature*, and *keyEncipherment* bits are set and the key usage extension is marked as critical. In case the certificate contains key usage extension but either the *digitalSignature* or the *nonReputudation* bit is not set, S/MIME receiving agents do not accept signature of a message.

2.2 Multiple E-mail Address Crtificates

An e-mail certificate or personal e-mail certificate permits its use with single e-mail address. To make an e-mail certificate useful for signing and encryption from more than one e-mail account of an individual, multiple e-mail address certificates have been proposed . A multiple e-mail address certificate binds more than one e-mail address with an individual. For such a certificate, multiple e-mail addresses are contained either in subject field or subject alternate name files or in both. Inclusion of more than one e-mail address in the e-mail certificate does not disturb the existing X.509 certificate structure, because RFC 5280 does not restrict the number of email addresses that may be included in the subject alternate name field of the certificate to one. Such a certificate is useful to individuals and businesses that possess more than one e-mail addresses to send or receive e-mail messages. It is required that the CA issuing a multiple address e-mail certificates to individuals verifies all mail accounts of the individual to be bind in the certificate. Using a single e-mail address certificate for the purpose of S/MIME will reduce costs incurred on to

purchase multiple certificates. It will also simplify certificate management.

The comparison of S/MIME mail sending and receiving practice-employing use of certificates (both single address and multiple address) across mail clients is shown in chart 1.

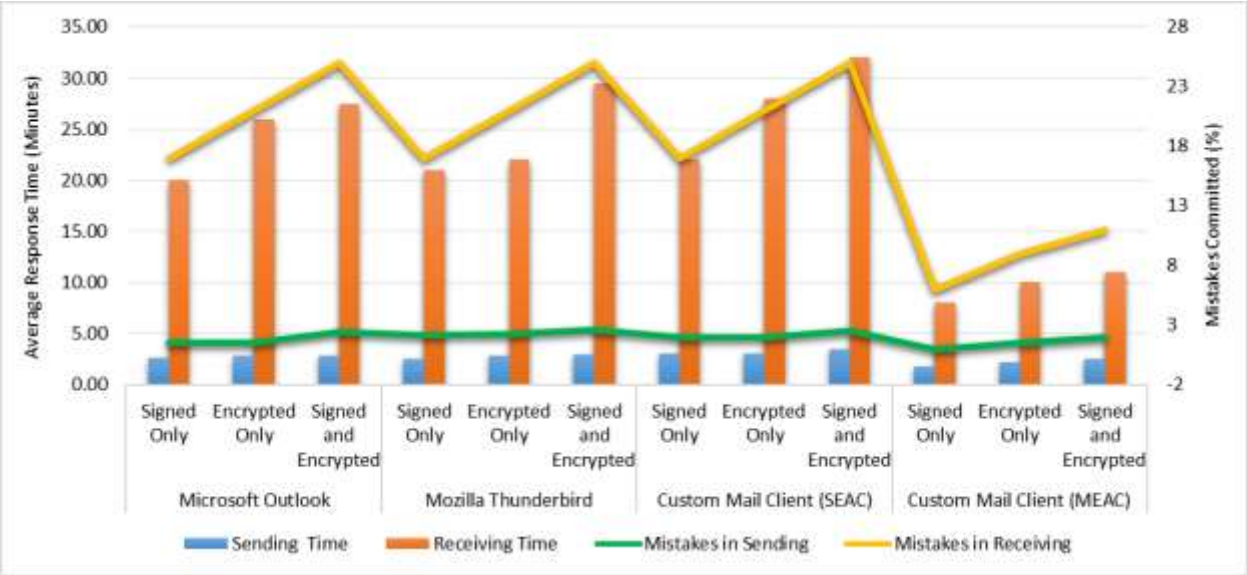

Chart -1: E-mail sending and receiving practice using S/MIME *(with single and multiple e-mail address certificates)*

Response time to correctly send and view received S/MIME mail either encrypted or signed or both encrypted and signed was greatly reduced by the use of multiple address email certificates. Users took less time to select certificate for encryption/signing and decryption/signature verification. The average response time remained 1.8 to 2.5 minutes, which is far less in comparison to time taken when single e-mail address certificates were used.

3. Proxy as a Security Solution

Security functions are shifted from the user to the proxy server. As users are the most critical component of the entire system when it comes to security, an approach was to separate security functionalities from users and delegate them to the dedicated proxy server. Nonetheless, the user is the one that is still responsible for security, i.e. the proxy is not in the position to read any emails or security credentials of the user, without the input of the user's credentials.

By using the concept of a web proxy extra security functionalities are provided to the user. This design and proposal can be used for other research areas, such as Internet of Things or secure m-commerce systems. Although these two areas are conceptually different, we use the same concept for both. In this design the proxy server is responsible for establishing a secure link with the user and delegating as many interactions as possible from the user's workstation or mobile device. Our secure e-mail proxy implementation represents our first–level solution towards the use of this approach and technology and will also be used later as a paradigm for more concrete and complicated system designs. PKCS #7 and S/MIME packaging are general mechanisms to secure e-mail systems. They can be used generally for all e-mail communications and are recommended to guarantee confidentiality and authenticity.

When using a mobile device, the use of the security proxies becomes even more important. Mobile devices have limited capabilities and so a user can delegate to the trusted party the secure operations he/she would like to execute and be reassured that the contents he/she receives meet the desired security and data protection requirements.

Moreover, since the proxy server functions act as a delegate for the more "heavy" computations in terms of processor and network speed, potential bottleneck on the mobile side will be avoided, especially when being in lack of network coverage (limited Internet speed) or low battery (avoid using heavy processor-related tasks).

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work

4. IMPLEMENTATION

The architecture comprises two servers: the proxy server, which handles all the communication with the appropriate parties (users, CAs, e-mail servers) and the associated CA server. Users login to the proxy server using their e-mail address and password of the native e-mail account. The proxy server identifies the native e-mail server from the e-mail address and performs the authentication of the user with the native e-mail server. The protocols used are different, depending on the native e-mail server. The list of protocols and mail servers currently supported are given in Table 1.

	Protocol	Incoming Server	Incoming Port	Outgoing Server	Outgoing Port
Gmail	imap	imap.gmail.com	993	smtp.gmail.com	465
Hotmail	pop3	pop3.live.com	995	smtp.live.com	587
Yahoo Mail	pop3	plus.pop.mail.yahoo.com	995	plus.smtp.mail.yahoo.com	465
KTH Mail	imap	webmail.kth.se	993	smtp.kth.se	465
JRC scientific Mail	imap	email.jrc.it	993	email.jrc.it	465

Table 1:- Mail servers available with secure e-mail system

Once the authentication is successful, the proxy fetches the list of e-mails from the native e-mail server and displays them to the user, exactly the same way as they would be displayed when using a normal web–based client. The user from this menu can have access to all normal mail functionalities, exactly as if he would use a desktop mailclient. A screenshot of the secure email's inbox can be seen in Fig. 2.

Finally, the connection between the proxy and the user is always secure. For this reason, the use of a standard SSL connection between the two parties is implemented. The architecture and the interactions between the parties in a normal workflow are shown in Fig. 1.

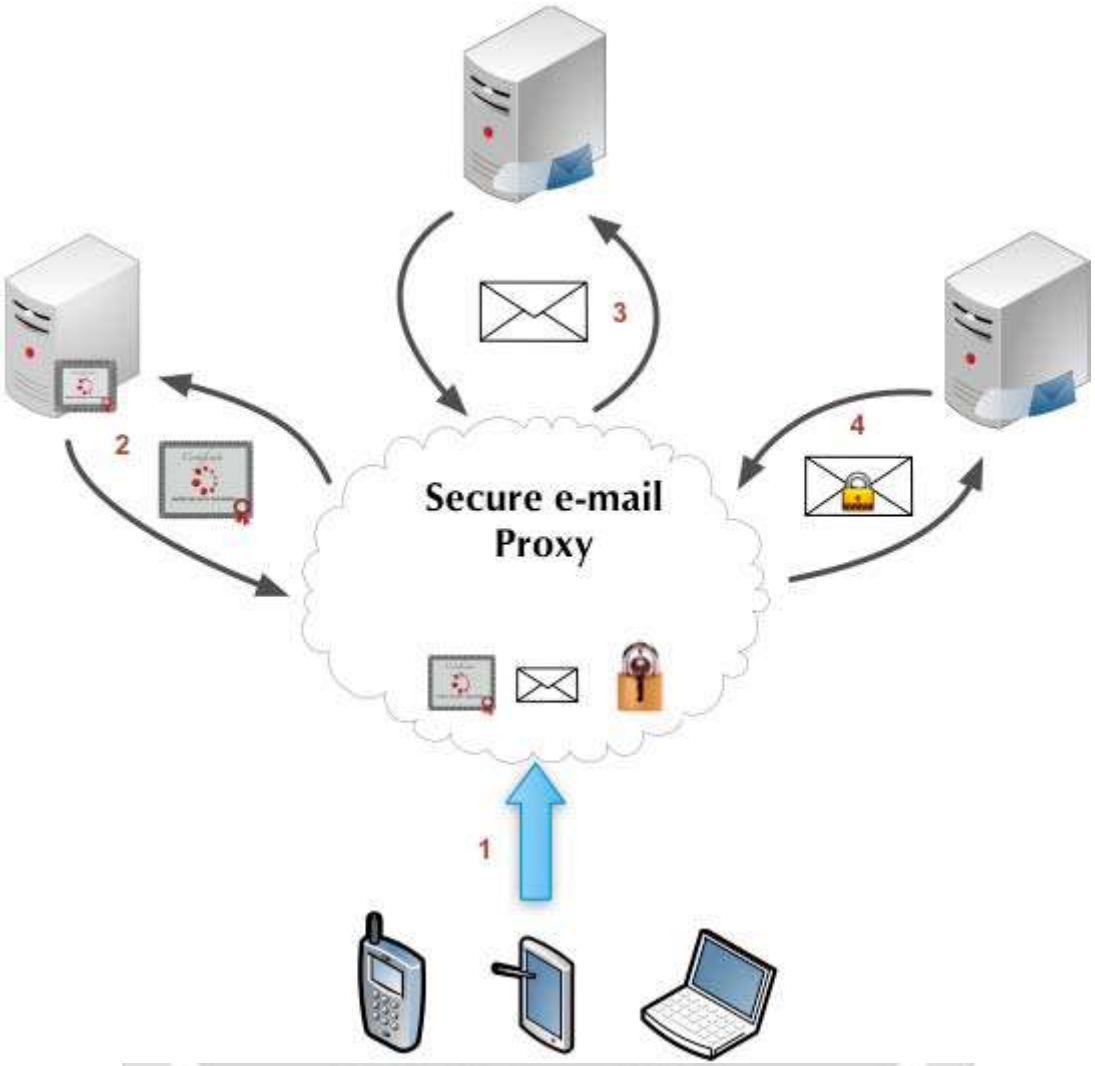

Figure 1:- Secure e-mail proxy interactions

Figure 2:- A screenshot of the secure email's inbox

4.1 Security Features

When the user logs in for the first time, a RSA key-pair is automatically generated and a certificate is requested from the CA for his/her account. As the process is automated, the Common Name of the Distinguished Name (DN) is set

to the user's e-mail address. They are both stored on the proxy and they are encrypted with the user's login credentials. As the standard secure e-mail approachrequires, the private key is used to sign outgoing e-mails and certificates are used by recipients to verify the sender's signature.

When the user wants to send an encrypted or signed (or both) e-mail, the private key is decrypted on the fly (and kept in memory) and S/MIME formatting is per-formed with the original text of the e-mail. The user is not aware of any of these cryptographic processing details, as everything is performed transparently and by the proxy server. The user just selects, prior to sending an e-mail, the option to sign or/and encrypt the letter. The certificate of the recipient is fetched automatically by the proxy from the local database of cryptographic keys. At that moment, the recipient(s) of the encrypted e-mail(s) must be registered in the same instance of our secure e-mail proxy, so that their certificate is available to the proxy. The e-mail address of the recipient is used as the unique identifier. As a result the recipient's certificate is found in the local database and the S/MIME packaging is performed according to the corresponding Internet standards.

When the recipient receives an encrypted e-mail, he/she will not be able to read it when fetching it and opening it directly from the native e-mail server. Instead when accessing the native e–mail server directly, he/she will just see an S/MIME attachment as a file with the standard .p7m extension and an empty body of the e-mail. However, when he/she uses the secure e-mail proxy after his/her login, the proxy will automatically understand that the e-mail is encrypted and will automatically perform decryption when the user clicks on the selected e-mail in order to read it. At the same time, he/she will see a notification that the letter is encrypted. The exact same procedure is performed with signed e-mails with the only difference being the attachment extension, which in this case is .p7s. A comparison of how an encrypted e-mail is viewed when using our secure email system and how it is viewed when accessing it directly from the native e-mail server (Gmail in this example) can be seen in Fig 3 and Fig. 4.

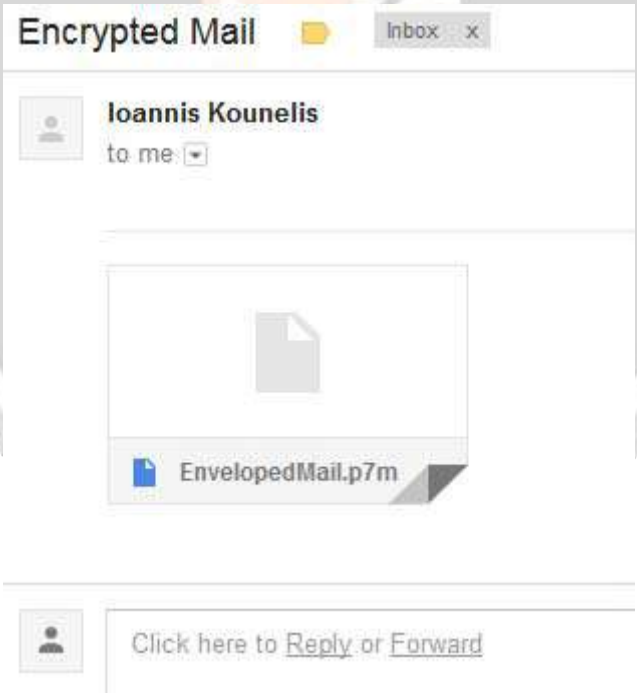

Figure 3:- Encrypted e-mail when opened from the native mail server (Gmail**)**

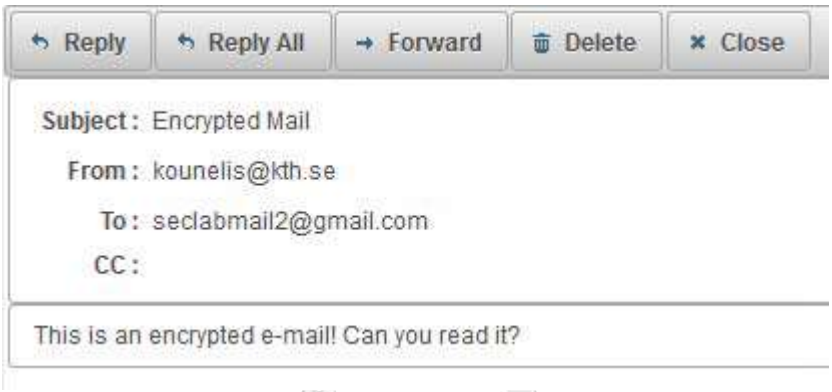

Figure 4:- Encrypted e-mail as seen by using SecureEmail

Decryption is performed by recovering the encryption key packaged in the S/MIME format, using the private key sof the recipient. The RSA private key of the user is already stored at the proxy encrypted with his/her password. When the user has already logged in, fetching and decryption of the private key is performed in order to be used for decrypting encryption keys contained in the incoming emails. A similar process is used to verify the signature of an e-mail, using the public key of the sender extracted from his/her certificate. The user should be made fully aware of the fact that the e-mail password is used as well for the encryption of the keys and as such he should be encouraged to apply a strong policy on his/her password management.

5. CONCLUSIONS & FUTURE WORK

In this paper we have described a secure and privacy enhanced way to handle e-mails based on the concept of secure proxy server. Solution does not introduce any overhead to the user neither does it require any extra software or hardware. More importantly, all the operations are transparent to the end users, so they do not need to be concerned with any configuration or understanding of the underlying technology.

Future research will focus on improving even more user experience when using our secure e-mail proxy. We can aim to create a new login layer to our platform that will allow the user with one account to handle all his/her e-mail accounts. The user will then be able to use the same certificates with all e-mail accounts that he/she chooses, instead of as today having a different certificate for each e-mail account. Moreover, we can plan to extend the system so that it provides federation of multiple proxies by distributing certificates between two or more instances of the Secure email System. This means that for the next version we can introduce scalable federated architecture and utilization of the full PKI hierarchy. For example, if one proxy is deployed in Italy and the other in Sweden, a user that has already created a certificate for his/her account at the Italian proxy should not need to re-generate one if he/she uses the Swedish proxy. The two proxies should communicate and manage secure transfer of certificates in such a case. The current system, being based on unreliable user emails, does not provide any assurance. One of the future extensions is to introduce versions with higher level of assurance in user identities and credentials. This will be achieved by linking the system to trusted and reliable identity and security providers and by using higher assurance authentication protocols, based on strong authentication, use of certificates, two–factor authentication and PIV smart cards.

Finally, future research also focus on the use of secure e-mails and secure e-mail proxy in the area of ecommerce,as already described in the previous sections and on the hardening of the proxy itself, in terms of security. We aim to use the proxy technology and other security features for our future research and demo activities, by enhancing its functionality and capabilities.

5. REFERENCES

[1]. Ben Lightowler, Security Analyst GMO GlobalSign Ltd," S/MIME Compatibility" ,Assessing the compatibility and best practices of using S/MIME encryption
[2]. Minhaz Fahim Zibran," Cryptographic Security for Emails: A Focus on S/MIME" 2011

[3]. K.Suganya ,"A Noval Approach for S/MIME", 2013 International Journal of Advance Research in Computer Science and Management Studies
[4]. Mohamed S.Nabi, M.L Mat Kiah, A.A Zaidan, , B.B Zaidan ,"Suitability of Adopting S/MIME and OpenPGP Email Messages Protocol to Secure Electronic Medical Records", 2013 IEEE
[5]. Ioannis Kounelis, SeadMuftic, Jan Loschner." Secure and Privacy-enhanced E-Mail System based on the Concept of Proxies ",2014 MIPRO
[6]. M. Tariq Banday, Shafiya Afzal Sheikh." S/MIME with Multiple E-mail Address Certificates: A Usability Study", 2014 !EEE