IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Efficiency and Limitation of Secure Protocol in E-Mail Services.

N.Vijayalakshmi[*1], E.Sivajothi[2], Dr.P.Vivekanandan[3]

[*1,2]Research Scholar, CEG Campus, Anna University, Chennai, India

[3]A.C.Tech, Computer centre, Anna University, Chennai, India

Vijinatarajan23@gmail.com

Abstract

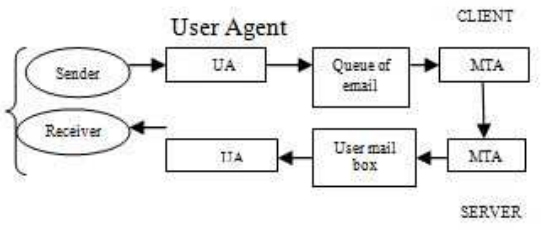
Nowadays email plays an important role in day to day activity. But there is an issue that whether we are sending or receiving the mail in a secure manner. The security is one of the critical areas where we have to analyze all sort of in-convenient and privacy of the user. To establish the email security, we have to analyze several protocols and specify the efficiency and the limitation of the secure protocol. Most of the email system send message from one server to another by using Simple Mail Transfer Protocol (SMTP) [1]. It is an application layered protocol. The message can be retrieved by POP or IMAP. To pursue authentication and confidentiality service, we use PGP. S/MIME is a standardize protocol used to encrypt and digitally sign email correspondence. Further, the study on the knowledge of secure protocol and the confidence in email system is presented.

Keywords— SMTP, PGP, S/MIME, SECURITY ISSUES

Introduction

SMTP is the common mechanism for email among different host within the TCP/IP suite. In this SMTP, client opens the connection to the server SMTP by the means of TCP. Through this connection the mail is sent, here the SMTP servers trace out the TCP connection. The SMTP client initializes the connection on the specified port. After the successful connection, the two processes deliver the request-response dialogue.

The Client process transmits the mail address of the sender and receiver. The server process and accepts the mail address. The Basic model of SMTP is shown below:



This model supports two types of mail delivery methods, they are end- to-end and store and forward. By using this SMTP can transfer the mail to another process on the same network or different network by means of gateway. The two basic components are User Agent (UA) and the Mail Transfer Agent (MTA).

MTA works as a background process, but the UA directly interacts with the user. MTA usually complemented with the email clients and they typically employ a different protocol. The UA uses POP3 and IMAP for retrieving the message.

Security Issue Of SMTP

The vulnerability problem can be grouped into three types .They are high risk, medium to high risk and low to medium risk. The high risk categories as buffer overflow, bounced piping attacks and host-shell-gaining attacks [2].

In the medium to high, it includes denial of service attack and at low to medium risk; it handles with mail relay, mail queue manipulation attack, and crashing anti – virus software attack. Normally e-mail server does not verify the claimed sender identity, it simply passes the mail to the specified address. When the bulk messages are sent, the server gets slow. To avoid this, first the spam mail must be identified. Mismatches between the IP address and the domain name in the header will leave to spam mail. The protection and security process in many of the industry configure their SMTP server and other service in such a way it will automatically reject the blacklist mail server.

The issues in the SMTP are:

- It guarantees the confidentiality which is transmitted over the open medium
- Sender authentication is verified whenever it is claimed by the sender
- It refers certain policy such as stopping the transmission of spam e-mail and mail containing virus
- It has weak security issue such as non repudiation and denial of service
- It does not provide the proof against the sniffers and man-in-middle attack.

A number of vulnerabilities in SMTP that users are not authenticated and it trust in message exchange. The server does not verify the message and everything is done in assumption. The sending server specifies any address and sends the message. The receiving server accepts the message and continues the process, thus it allows fake address and hide the true user identity. E-mail spoofing can be used in malicious purpose such as spreading virus which leads to phishing attacks [3].

One has to guarantees the authentication, here PGP is a remarkable phenomenon which provides a confidentiality and authentication services. The main purpose of using this protocol is specified below:

- It is free worldwide version which can be run in different platform
- This protocol is based on the secure review. This package includes RSA, D-H public key encryption
- It has a standardized scheme for encrypting files and message to individual which is used to communicate secure throughout the network.
- It is not developed or controlled by any standard organization.

The function and the services of PGP is specified below:

Function	Algorithm used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. The message digest is encrypted by either of the specified algorithm, the sender private key along with the message
Message encryption	CAST or TRIPLE DES or RSA	The given message is encrypted using CAST. The session key is encrypted using RSA
Compression	ZIP	Using ZIP, one can compress the message for storing and transmitting
Email compatibility	Radix 64 conversion	It provides the transparency for email

In this key generation, it should follow certain requirements:

- Generating unpredictable session, key is required
- It should allow multiple key with the multiple user
- Its entity maintain its own public and private key

The above tabular column explains the service of PGP. The authentication is done by using the hash function for encryption, it uses RSA or DSS. Here the messages are compressed using ZIP algorithm. Due to the SHA-1, it will assure that no one generates the new message. The next service is confidentiality which encrypts the message and then store in the file.

The steps followed in this process are specified below:

- The sender generates a message and a random number is generated in the session
- The message is encrypted using CAST or 3DES along with the session key
- The session key is encrypted by RSA using the recipient's public Key and the message is sent.
- The receiver use RSA along the private key to decrypt and recover the session key
- The obtained session key is used to decrypt the message.

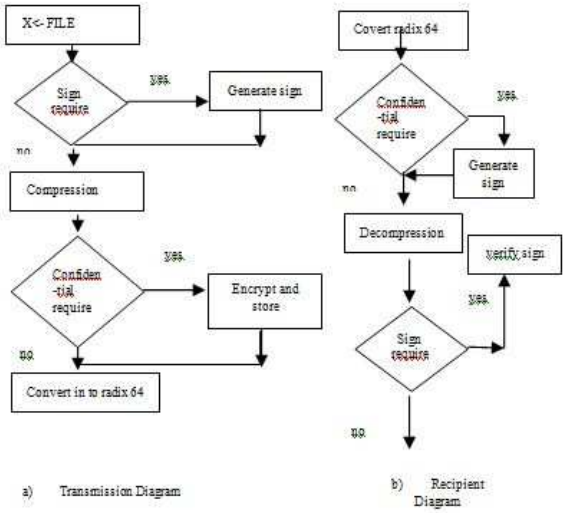
The next service is compression; by using this, we can save the space for email transmission and file storage. In the algorithm, the compression is specified as Z and for decompression, it is indicated as Z-1. In compression, it has to follow specified steps:

1. The main reason for compressing the message before digital signature is given below:

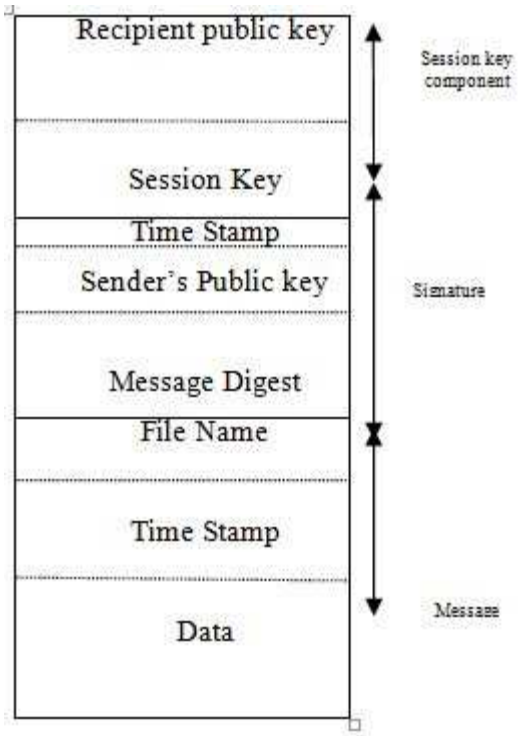
- we sign before uncompression of message, there is no need for evaluating with the compression algorithm

- Since PGP has in different version, one has to implement the algorithm common to all version

2. To strengthen the cryptographic security one has to compress the message before encryption. The structure of transmission of message using PGP is shown below diagram (a), (b)



The key structure plays a vital role for providing authentication and it is specified below:



Public key encryption is central to PGP. It is used for two purposes: sender uses his/her private key for placing his/her digital signature on the outgoing message, and the sender uses the receiver's public key for encrypting the secret session key [3].

One can expect people to have multiple public and private keys. This will happen in several reasons. For example, if an individual wish to retire an old public key, but, it allows for a smooth transition, may decide to make available both the old and the new public key for a while.

So, PGP must allow for the possibility that the receiver of a message may have stored multiple keys for a given sender.

This raises the following procedural questions:

1. How does the recipient know which public key it is?
2. How does the recipient know which of the corresponding public keys to use?

This leads to wastage of space because RSA public key is represented as hundreds of decimal digit. By using PGP, One can solve the above mentioned problem by using Key Identifier (KI) [7]. Another unique feature of PGP is Certificate Authority (CA). By using this, one can establish trust for authentication.

Limitation of PGP

- ✓ In this, PGP mainly deals with the private key if it is lost all the data is lost
- ✓ The biggest threat is tampering and imitation of public key.
- ✓ Depending upon the algorithm the standards get changed.

Therefore, PGP leads to loss of privacy, hence, one requires to design and formulate a better protocol. One prefers Secure/Multipurpose Internet Mail Extension (S/MIME).

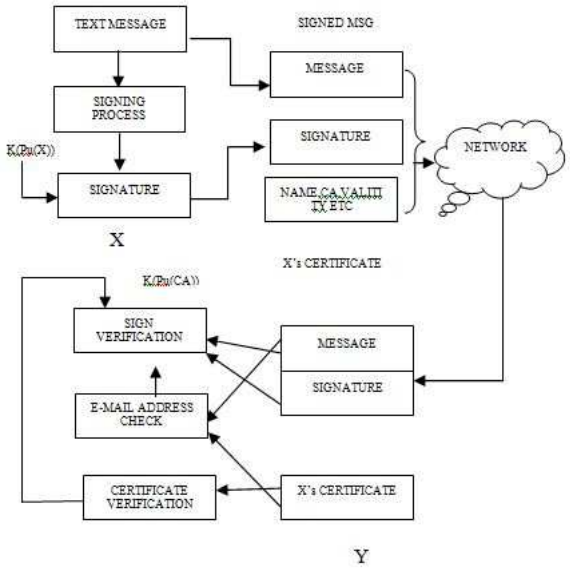
S/MIME is an asymmetric cryptography technique which is used to authenticate sender and provide strong signature semantics [9]. S/MIME is not a product, but a standard feature that is support by e-mail client programs, like MS outlook, Mozilla, Netscape messenger.

A signature block is generated by applying cryptographic signature generation function over the message. For this process, one can use sender private key. The recipient verifies the signature using the public key of the sender. Here, the receiver has to make sure that the public key is belonging to the particular sender. To avoid this, it uses digital certificates. It provides approved binding between the identity of the certificate holder and their public key. Certificates are issued by trusted certification

authorities (CA'S) with their digital signature over the certificate content. In this, before verifying the signature over the mail, the recipient checks the sender certificate to find the public key.

Working of S/MIME In Digital Signature

The sender generates his/her digital signature over the content and then append to the message. The recipient processes the certificate and the signed message separately. The life cycle of signed message between X and Y is shown below,



In the above all verification and control at the recipient (Y) is right, then it indicates the successful signed and verified message. The following are the stages to authenticate e-mail using S/MIME digital signature:

1. Authority in the trusted public certificates, which publishes digital signature for each e-mail addresses.
2. Each sent e-mail will be inserted a digital signature with private key. By using this, it provides a way to prove the authentication of "FROM" address.
3. The recipient will be equipped with S/MIME protocol whose function has to be verified the digital signature.

Cryptographic Algorithms

Hash functions: S/MIME-compatible e-mail software must support SHA-1 (Secure Hash Standard) and should support MD5 [3] (Message Digest Algorithm) in order to provide backward-compatibility with MD5-digested S/MIME v2 messages.

Encrypted e-mail	
encrypted message	encrypted with the session key
encrypted session key	encrypted with the recipient's public key—can only be decrypted using the recipient's private key
algorithm identifier	to tell the receiver's software which decryption algorithm to use
sender's public key	to enable the recipient to encrypt his response

Digital signatures to encrypt the message digest: the S/MIME client must support DSS (Digital Signature Standard) and should support RSA (Rivest, Shamir, and Adleman).

Content encryption to encrypt the message content (symmetrically, using a random session key), tripleDES [6] must be supported and RC2[7] (40-bit, considered insecure2)should also be supported for compatibility reasons. Earlier S/MIME versions only required support for 40-bit RC2 encryption in order to be compatible with US export regulations.

Key encryption to encrypt the session key, DH[8] (Diffie-Hellmann) must be supported, RSA[5] should also be implemented.

Message Format

S/MIME specifies additional MIME content types to be used for encryption and digital Signatures [9]. A MIME entity (which can be the complete message or subparts of the message) is being wrapped into an encrypted or signed CMS (Cryptographic Message Syntax) object. The CMS object is usually base64 encoded and with content-type application/pkcs7-mime. The additional parameter "S/MIME-type" specifies whether the message has been encrypted or signed. If the message contains a clear-text part (i.e. a clear-signed message), the clear-text part and the CMS object are combined within a multipart/signed content and the CMS object is of content-type application/pkcs7-signature.

Principle of S/MIME

S/MIME consistently use real name as primary identity element in e-mail signature verification. It includes the following:

- Impossibility of having a globally unique name, thus possible naming ambiguities (for example , there might be two john rude in the same country, same organization, same unit)
- It is very hard to obtain a standard name out of complex certificate fields
- Unbreakable attraction of globally unique and application specify e-mail address

This principle leads to the following problem:

- The name information in the certificate and the name in the e-mail become independent to each other, so the certificate looses the importance in e-mail signature verification.
- Recipients are enforced to identify people using their e-mail addresses. But it leads to loss the identity of the user.

Limitation of S/MIME

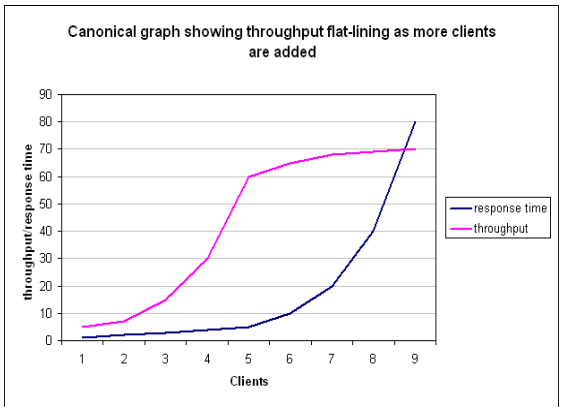
- ✓ Recipients still have to inspect the "From:" address for misleading domains
- ✓ Not all email clients supports S/MIME
- ✓ Recipients may not check certificate revocation status

Sender and recipient gateways must both understand S/MIME digital signatures if using
Gateway server to verify signatures[8].

Performance Of SMTP

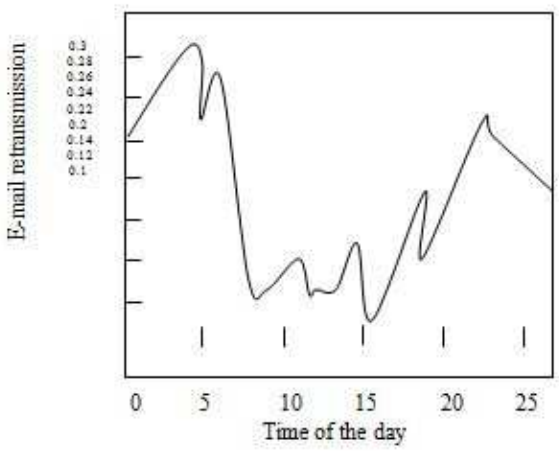
The performance is evaluated by using the number of clients or server has involved in the specified transaction. If one increases the number, there is a chance for the negative impact.

The results are plotted for a series of test runs. Two parameters are measured for each test run; response time (average transaction time) and throughput (average transactions per second). The first test run uses just one client thread; client threads are progressively added in each subsequent run, finishing with nine client threads in the last test run. When the data is graphed, the data points in each set are joined by a line to highlight the differences between test runs. The scale for response times and throughput are both on the left.

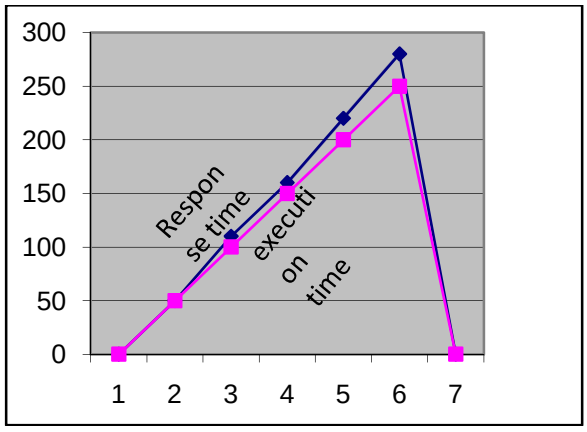


The number of clients increases from 1 to 5, throughput (transactions per second) increases steadily, and response time (transaction time) is barely affected. As the number of client threads increases beyond six, response time gets longer and longer, and the number of transactions processed per second barely increases. The system is saturated.

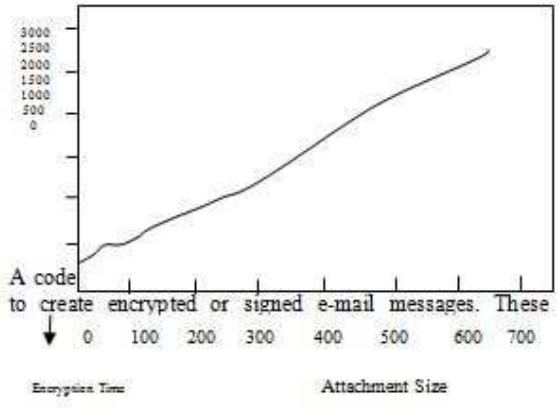
The e-mail retransmission overhead of the proposed scheme is shown below. The proposed spam rejection scheme increases the amount of e-mails received by an MTA. The retransmission overhead is higher during the night time than during daytime. During night time, e-mail traffic consists mainly of spam. Thus, the retransmission overhead due to zombie-relayed spam compared to overall traffic is higher up to 29% of e-mail retransmission overhead. During day time, the non-spam e-mails dominate the total e-mail traffic. Retransmission overhead of zombie-relayed spam e-mails are lower than 16% compared to the overall e-mail traffic. Thus, it clearly specifies how the random changes had been occurring while retransmitting the e-mail.



During monitoring the process, it improves its efficiency and accuracy and detects all system protocol error and failure. In any abnormal case the server gets delay. The representation is shown below:



It is observed that some time delay between the time execution and the respond time.



timing results are shown for encrypted messages. It is obvious that encrypting messages require a higher time.

Conclusion

Email is vulnerable to both passive and active attacks. To provide a reasonable level of privacy, all routers in the email pathway, and all connections between them, must be secured. This is done through data encryption which translates the email's contents into incomprehensible text and can be decrypted only by the recipient. An industry-wide push toward regular encryption of email correspondence is slow in the making. However, there are certain standards that are already in place which some services have begun to employ. It is nature that every user would want to use the rich feature of S/MIME, privacy service of PGP and simple concept of SMTP. Unfortunately, these three protocols have taken separate evolution path. S/MIME itself does not provide privacy enhancement services whereas non-textual objects cannot be enhanced with PGP. The message transferring in SMTP is not authenticated, which leads to message loss. We have to identify the drawbacks in these protocols and try to integrate and form the powerful protocol.

References

[1] M.Tariq Banday, "Effectiveness and Limitations of E-Mail Security Protocols" International Journal of Distributed and Parallel Systems" Vol.2, No.3, May2011.

[2] Sunny gill, "Email security protocol" International Journal of computer trends and technology" March to April issue 2011.

[3] Dhanalakshmi, "Enhanced E-mail authentication against spoofing attacks to migration phishing".

[4] P. Tzerefos, C. Smythe, I. Stergiou, and S. Cvetkovic, "A Comparative Study of Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and X.400 Electronic Mail Protocols", Proceedings of the IEEE 1997 *22nd Conference on Local Computer Networks - LCN, pp 545-554,199.*

[5] R.Sureswaran, "Active e-mail system protocols monitoring algorithm" IEEE Proceeding.

[6] M.Tariq Banday, "Algorithm for detection and prevention of E-mal date spoofing" International journal of computer application" May 2011.

[7] Dai kuobin, "PGP e-mail protocol security analysis and improvement program" 2011 international conference on intelligence science and information engineering.

[8] Halsall, F. (2005). Computer Networking and the Internet (Fifth ed.): Addison-Wesley.

[9] Dusse, S., Hoffman, P., Rams dell, B., Lund blade, L. And Repka, L. (1998). S/MIME Version 2 Message Specification. *Internet Engineering Task Force (IETF)*, RFC 2311.