IJETAE
EXPLORING RESEARCH AND INNOVATIONS

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013)

Securing Email Applications from Various Cyber Issues

Vineeta Tiwari[1], Neha Chandel[2], Anshul Jain[3]

Student, Information Technology, Swami Vivekananda College of Engineering, Indore, India

***Abstract* - Information Security and integrity are becoming more important as we use email for personal communication and business. As it is excessively used it is highly prone to Cyber Attacks, threats and malwares. The most common of these are masquerading, modification, and Phishing attacks. In order to provide security against these, many tools have been proposed such as Privacy Enhancement Mail (PEM), Pretty Good Privacy (PGP). Although these tools provide security features like Data Integrity, Non-Repudiation, Encryption, But somewhere fails to provide higher level of Authentication and Confidentiality. This paper focus on the security issues that are still to be overcome even after the use of any of these existing email privacy tools, considering the solutions prevailing to avoid security risks and hence make the email communication security proof.**

***Keywords*- Cyberattack, Information security, Data Integrity, Authentication, Masquerading, Confidentiality.**

I. INTRODUCTION

The protection of email from unauthorized access and inspection is known as electronic privacy. In countries with a constitutional guarantee of the secrecy of correspondence, Email is equated with letters and thus legally protected from all forms of eavesdropping. Businesses are increasingly relying on electronic mail to correspond with clients and colleagues. As more sensitive information is transferred online, the need for email privacy becomes more necessary.

An e-mail server accepts, forward, deliver and store messages. Neither the user nor their computers are required to be online simultaneously. Information Security and integrity are becoming more important as we use email for personal communication and business.[1] As we know that email is insecure to both passive and active attacks. However, it may surprise us to learn just how insecure it really is. For example did you know that messages which you thought were deleted years ago may be sitting on server's half way around the world? Or that your messages can be read and modified in transit, even before they reach their destination? Or even that the username and password you use to login to your email servers can be stolen and used by hackers? [2]

Three components of email system are:-

1. Message Envelope
2. Message Header
3. Message Body

The Internet is an expansive network of computers, much of which is unprotected against malicious attacks. From the time it is composed to the time it is read, email travels along this unprotected Internet, perpetually exposed to electronic dangers. The protection of email from unauthorized access and inspection is known as electronic privacy. Email is vulnerable to both passive and active attacks. Passive threats include Release of message contents, and Traffic analysis while active threats include Modification of message contents, Masquerade, Replay, and Denial of Service (DOS). Actually, all the mentioned threats are applicable to the traditional email protocols.

II. PROBLEM DOMAIN

Email is, in general, Completely Insecure! The security issues include:

- Invasion of Privacy
- Eavesdropping
- Identity Theft
- Message Modification
- False Messages
- Message Replay
- Unprotected Backups
- Repudiation (Sender denies that she/he sent it)

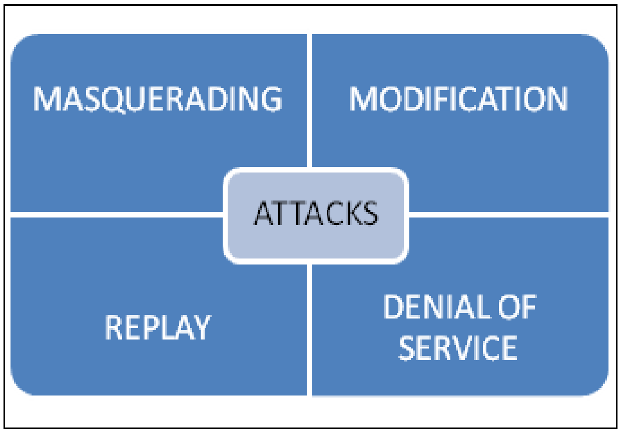

Fig1: Shows various active attacks

Some of the ways for email security are:

SSL: It is simple and easy to use SSL to secure the communications between your computers and your email service provider's computers.

This works no matter who your recipients are SSL improves security in these ways:

- It establishes that you are contacting your service provider's computers and not someone else's.
- It encrypts the username and password that you use to login to these servers. This mitigates identity theft and other issues.
- It protects your message from eavesdroppers between your computer and your SMTP server. [3]

- *Anonymity:* If you have access to an Anonymous SMTP server, you have an easy way to increase your Internet privacy. Anonymous SMTP provides:
  - IP address privacy so that message recipients cannot determine your computer's Internet address (and thus your location).
  - Email client privacy so that the recipients of your email messages cannot determine what type of email client you are using.
  - A means to strip out any other non-standard "email header" data that may be persisting in your outbound messages. [4]

  PGP and S/MIME: PGP and S/MIME keys use asymmetric key encryption to protect the contents of your messages throughout their complete journeys. They provide:

- Protection against eavesdropping and unwanted backups
- Message Digests to detect whether messages have been altered in transit
- Signatures to prove sender authenticity

Encryption avoids the obstruction of PGP and S/MIME encryption while providing complete security, anonymity, and other features. Unlike computer break-ins and other security problems, problems with email security are very hard to detect. We cannot tell if someone is reading our email or modifying messages subtly until it is too late. We cannot quantify the cost of email and information security problems until it is too late. [5]

III. Related Work

Electronic mail (e-mail) is one of the most important and widely used network applications. It has been used in communications between individuals, business organizations and governmental agencies around the world.

Daily Email Traffic	*2012*	*2013*	*2014*	*2015*	*2016*
Total Worldwide Emails Per Day(B) % Change	144.8	154.6	165.8	178.3	192.2
Business Emails Per Day(B) % change	89.0	101.0 13%	114.3 13%	128.6 13%	143.8 12%
Consumer Emails Per Day(B) % Change	55.8	53.6 -4%	51.5 -4%	49.7 -3%	48.4 -3%

TABLE 1: Statistics on estimation of email usage[6]

The vulnerability of underlying network demands secure e-mail solutions. In a secure e-mail application, the following two security services must be considered:

• *Message confidentiality:* Message confidentiality assures the sender that the message can be read only by the intended receiver.

• *Message authenticity*: Message authenticity assures the receiver that the message was sent by a specified sender and the message was not altered on route.

Currently, there are two widely used secure e-mail solutions, Pretty Good Privacy (PGP)[1] and S/MIME[2]. Both solutions utilize a combination of conventional symmetric key techniques and modern asymmetric-key (i.e. public-key) techniques to provide message confidentiality and message authentication. The recent research on securing emails has been largely focused on the design of new cryptographic protocols to enhance confidentiality.[3]–[6] Although the objective of message authentication can be achieved by using Digital signatures, it also creates a potential privacy threat. The receiver can pass the message and the corresponding digital signature to a third party without the permission of the sender. The digital signature can be verified by any third party. This design inherently provides non-repudiation evidence to the message sender which is not required and even not desired in most e-mail applications.

A. Review of PGP and S/MIME Solutions

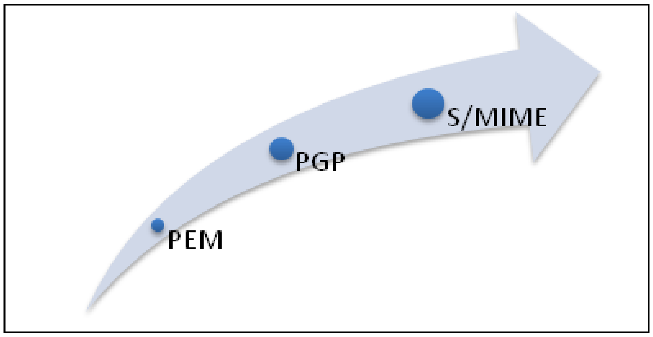

Fig2: Existing Email Privacy Tools

In PGP and S/MIME applications, each user is assumed to have two pairs of public and private keys selected for long term use. One pair of keys is used for message encryption and the other pair is used for digital signature. It is assumed that the public keys of all communication partners have already been securely stored in each user's public-key ring.

Message confidentiality using digital envelope: A *digital envelope* is a technique used by the sender to transmit the message in such a way that only the intended receiver can read the content of the message.[9] The sender first randomly selects a secret session key and uses this secret key to encrypt message. Then, the sender encrypts this secret session key with the receiver's public key using any public-key encryption algorithm. After receiving the encrypted message, the receiver first uses its private key corresponding to the public key to uncover this secret session key. Then, the receiver uses the secret session key to decrypt the cipher text.

Message authentication using digital signature: PGP and S/MIME both use digital signature to provide message authentication. The message sender uses its private signing key to generate a digital signature on the message digest. The digital signature is attached along with the message and is sent to the receiver. [11] The receiver uses the sender's public key to verify the digital signature. One potential security problem in using digital signature to provide message authentication is that, without consent from the message sender, the receiver can pass the message and its digital signature to a third party. Since the digital signature can provide non-repudiation evidence that can be verified by anyone, this poses a *security threat* to the sender's privacy.

Message confidentiality and message authentication: PGP and S/MIME provide this service by using both, digital signature and digital envelope for the message.

IV. Proposed Algorithm

Our algorithm will offer four different services:

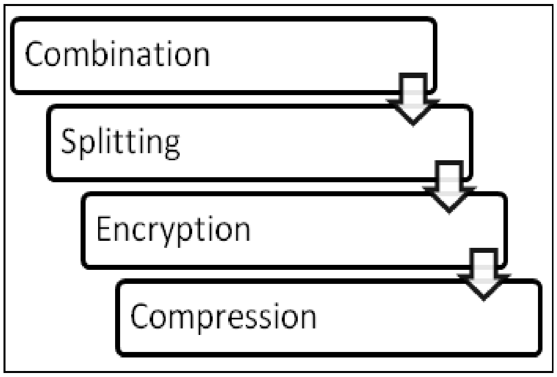

Fig3: Steps of Algorithm

The algorithm proposed by us comprises of mainly four steps which are combination of packets, then splitting them into further small fragments so that they could be comprised into the given size and then those splitted packets are encrypted. These packets are finally compressed using compression algorithm to reduce the size during there transfer. One of the new feature of our algorithm is that instead of digitally signing a message digest as suggested in all existing digital signature algorithms, we propose that the digital signature is applied to the message directly.

V. Conclusion

In this paper, we propose a new algorithm for securing emails using cryptographic functions supported by PGP and S/MIME. This algorithm enables only a specified message receiver to authenticate the message. It also allows the message sender to be able to deny generation of the message. This feature can protect the personal privacy. Thus, this algorithm performs various steps in order to provide a secure mail service.

REFERENCES

[1] S. Garfinkel, PGP: Pretty Good Privacy. OReilly, 1994.

[2] B. Ramsdell, "Secure/multipurpose Internet mail extensions (S/MIME) version 3.1 message specification, RFC 3851," 2004.

[3] B. H. Kim, J. H. Koo, and D. H. Lee, "Robust e-mail protocols with perfect forward secrecy," IEEE Commun. Lett., vol. 10, 2006.

[4] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of robust e-mail protocols with perfect forward secrecy," IEEE Commun. Lett., vol. 11, 2007.

[5] H. Sun, B. Hsieh, and H. Hwang, "Secure e-mail protocols providing perfect forward secrecy," IEEE Commun. Lett., vol. 9, 2005.

[6] A. W. Dent, "Flaws in an e-mail protocol of Sun, Hsieh, and Hwang," IEEE Commun. Lett., vol. 9, 2005.

[7] D. R. L. Brown, "Deniable authentication with RSA and multicasting," Cryptology ePrint Archive, http://eprint.iacr.org/2005/056.pdf, Feb 2005.

[8] C. Kaufman, R. Perlman, and M. Speciner, Network Security. Prentice Hall PTR, 2002.

[9] W. Diffle and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, 1976.

[10] D. Chaum, "Private signature and proof systems," U.S. patent 5,493,614, 1996.

[11] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated verifier signatures," in Proc. Asiacrypt03, vol. LNCS 2894, 2003.

[12] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, 1978.

[13] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, vol. 31, 1985.