ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0041

Application Layer Protocols to Protect Electronic Mail from Security Threads

Arwa Husien, Ghassan Samara
Department of computer science
Zarqa University
Zarqa, Jordan

***Abstract*—Electronic mail is the most widely used service from internet utilities, as it is experiencing phenomenal growth for personal uses and organizations. E-mail more valuable than phone for business communications, there are many threads for Electronic mail systems security such that phishing Electronic mail, spam, virus, spyware, and malware. Because of the nature of E-mail applications, Electronic mail security is a priority concern for many organizations and security practitioners face a unique set of management issues. Security levels, policies, privacy issues, confidentiality, message integrity. In this paper we discuss how to ensure the safety and security of corporate Electronic mail environment, detailing threats that should be prepared to avoid them, and tools that should be used to mitigate them.**

Keywords— Electronic mail; Security; PGP; S/MIME; e-mail security; Security Protocols.

I. *INTRODUCTION*

Electronic mail is the most widely used and regarded service of network utilities, although it is very old service in the technology world, also Electronic mail still prevails as a significant business tool, E-mail systems have experienced phenomenal growth, from simple systems linking a few users on a single computer to vast international networks connecting correspondents on literally millions of different hosts.

However, there are some changes in using electronic mail systems over time, with more demands for mobile access-using wireless networks- and personal use the need of organizations today to keep their electronic mail systems secure due to the central role electronic mail plays in the modern enterprise.

Nowadays message contents are insecure, may be inspection by unauthorized people during its travelling in the network, there are Many corporate Electronic mail systems come with built-in security tools, but they are not nearly enough, According to experts at Trend Labs, the amount of Electronic mail considered bad jumped within the range of 88–90% of Electronic mail sent during the first three quarters of both 2010 and 2011.[4]

With the huge explosion of growing reliance on electronic mail for every essential and nonessential purpose, a demand for authentication and confidentiality services are grew rapidly. What users need is something more akin to standard mail (contents protected inside an envelope), they need to have confidence about the sender of the mail and its contents, as shown in figure(1) Electronic mail Encryption and Electronic mail Digital Signature are needed to achieve integrity and confidentiality in Electronic mail messaging.[2]

With more targeted threats across Network environment, how can the aspects of today's electronic mail services be protected?

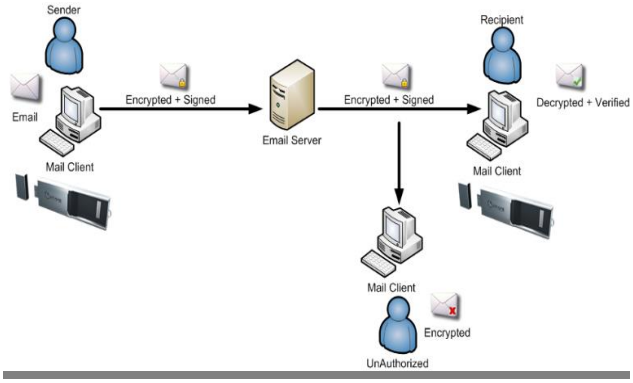

Fig.1.Electronic mail Security [8].

In network world we have a lot of application layer protocols for Electronic mail service such that Multipurpose Internet Mail Extension (MIME) which is an extension to the RFC 5322 protocol that is intended to solve problems and limitations of using Simple Mail Transfer Protocol (SMTP), which defined in RFC 821 which is traditional e-mail format standard, The most recent version of this format specification is RFC 5322, some of SMTP problems that it don't transmit all binary objects such that executable files, cannot transmit text data which includes national language characters, SMTP servers sometimes reject mail message over a certain size.

S/MIME is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA which is Algorithm by Rivest, Shamir & Adleman for data security, also Pretty Good Privacy (PGP) is secure Electronic mail program, although both PGP and S/MIME are on an Internet Engineering Task Force (IETF) standards track, it appears that S/MIME used as industry standard for commercial and organizational use, while PGP used for personal e-mail .[2 , 3]

This paper discusses how users can ensuring the safety and security of corporate Electronic mail environment, detailing threats that should we prepare to avoid them, and tools may be used to mitigate them.

doi:10.15849/icit.2015.0041

Electronic mail messages are the most cost-effective way to transmit information, as significant importance of electronic mail messaging and huge number of Electronic mail threads, such as spam, viruses and malwares, users need proper security measures to obtain the electronic mail security goals of confidentiality, message integrity, authentication, and non-repudiation from original.

Abbreviations and Acronyms

- PGP: Pretty Good Privacy.
- S/MIME: Security/ Multipurpose Internet Mail Extension.
- E-mail: Electronic mail.
- RSA: Rivest, Shamir & Adleman.

II. PREVIOUS STUDIES:

A. threats of email security

1) *viruses*: One of the most publicized and high risk of all the issues is viruses. Viruses are so dangerous ; they often deliver *highly* fatal load, destroying data, and dropping down entire mail systems.
Most of the viruses that were responsible for actual disasters during that time were either Internet worms or mass mailer viruses. To make matters worse, both of these virus types staying around longer than other types, even after anti-virus products have included protection against them. [11]

2) *SPAM:* Another major threat to email security today is SPAM (junk Email), often cited by organizations as being their number one concern, SPAM is considered a security threat because it can carry viruses, malicious code, and fraudulent solicitations for private information [11] . "junk email could cost a company with 500 employees nearly $750,000 each year" [12] .

3) *Phishing:* Phishing (identity theft), is a newer threat to email security. Phishing is the process where identity thieves target customers of financial institutions, using common spamming techniques to generate huge numbers of emails with the intent of luring customers to spoofed web sites and Trapping them into giving personal information such as passwords. [11]

Phishing the most common methods of attack. Some of the threat and defenses are as follows masquerading: an attacker pretends to be someone else. In such situation, a criminal can set up a storefront and collect thousands or billions of credit card numbers from unsuspecting consumers. [10]

4) *The man in the middle:*The man in the middle attack and session hijacking attack occurs when an attacker inserts Itself between two parties and pretends to be one of the parties.

5) *Eavesdropping:* Eavesdropping happen when attacker listens to a private communication. The attacker views information as it is sent over the network. [10].

6) *Data diddling*: Data diddling attack happened when an attacker changes the data while it routing between communication parties.

7) *Dictionary attacks:* a dictionary attack happen when an attacker uses large set likely combinations to guess a secret. aka, an attacker may choose one widely used password and try them all until the password is discovered.

8) *Denial of service attack:* denial of service attack occurs when an attacker floods the Email with hundred or even million of messages. Though the attacker does not benefit, service is denied to legitimate users. This is one of the most difficult attacks to thwart.

B. The defense for each Email security threat

1) The defense for Phishing attack is authentication. By using an authentication agent or digital certificates, you force the user to prove his or her identity. Through authentication you ensure that only trusted users can engage in sessions. [10]

2) The defense for the man in the middle and session hijacking attack is digital certificates or digital signatures. Both Parties of communication should proved to each other; that they know a secret that is known only to them. This Is usually done by digitally signing a message and sending it to the other party, also asking the other party to send a digitally signed message. [10]

3) The defense for eavesdropping attack is encryption using where only the authorized recipient will be able to decrypt.

4) The defense for dictionary attack is strong passwords. Passwords that are not common name,(like fist name, last name, or birthrate), words or references are harder to crack with a brute force attack such as a dictionary attack.

5) The defense for denial of service attack is authentication service filtering. By authenticating users on authenticated parties can send message.

6) The defense for Data diddling attack is a decrypted message digest. An encrypted mess digest records random segment of the original message so receiver recalculate the message digest, then compare it with the received message digest. If the message altered then encrypted again in its road, an encrypted message digest provides a method of authenticating the integrity of the data.

C. Email security protocols:

In order for making previous defenses for the main Email attacks ; to achieve the electronic mail security goals of confidentiality, message integrity, authentication, and non-repudiation from original, Mainly we have two protocols (PGP/MIME and S/MIME).

1) PGP

PGP is protocol provides a confidentiality and authentication service that can be used for electronic mail and file storage applications it had developed by the effort of a single person, Phil Zimmermann.

a) PGP functions:

Authentication:

In sender side, sender creates a message, then generate hash code of the message, which encrypted using the sender private key (the signature), and the result is concatenated with the message and compressed using ZIP.

In receiver side, receiver decompressed the massage, sender's public key to decrypt and recover the hash code, Then receiver generates a new hash code, and compares it

doi:10.15849/icit.2015.0041

with the decrypted hash code. If the two match, the message is accepted as authentic.

Confidentiality:

In sender side, sender generates a message and a random 128-bit number to be used as a session key for this message, then message is encrypted with the session key, the session key is encrypted with RSA using the recipient's public key and is pretended to the message.

In receiver side, receiver uses RSA with his private key to decrypt and recover the session key. Moreover, use the session key to decrypt the message.

message created using SHA-1(message digest), which encrypted using DSS or RSA with the sender's private key and included with the message.	
Confidentiality: Message encryption using CAST-128, IDEA, or 3DES, with a one-time session key generated by the sender. the session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA

A. PGP message format as shown in figure (2).

TABLE I. CRYPTOGRAPHIC ALGORITHMS USED IN PGP.

Function	Requirement
Authentication: a hash code of a	DSS/SHA or RSA/SHA

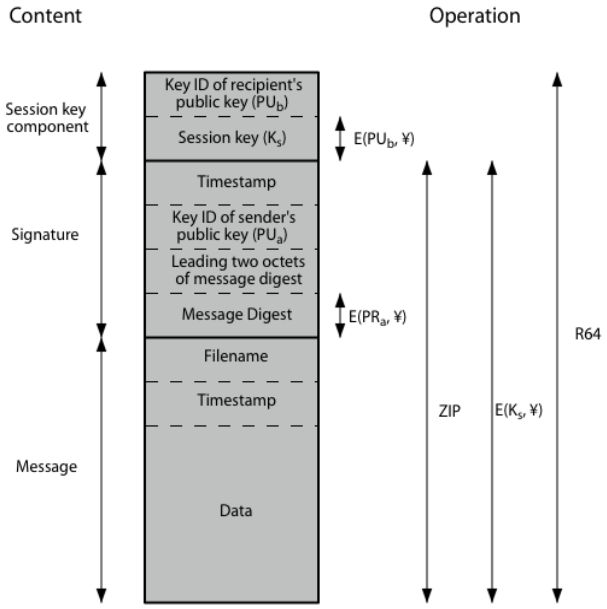

Fig.2 . General Format PGP Message.

b) PGP problems

PGP has several problems. "Key management is considered as a big challenge in PGP and PKI-based solutions in general. Public key cryptography requires the sender to obtain the receiver's public key beforehand, to be able to start any PGP encrypted communication (also it should be done in a secure way to prevent man-in-the-middle attacks). Moreover, there is still no practical secure approach to private key management; users should create a backup of their private key, store it in a safe place and be careful not to lose it, otherwise old encrypted emails cannot be decrypted anymore. Additionally, in case the private key is compromised, the attacker can trivially decrypt all the (old or new) encrypted emails. Therefore, a certificate revocation list (CRL) is required to facilitate the revocation of all compromised keys which also must be shared with all users". [14]

2) S/MIME

S/MIME is a protocol for adding cryptographic security utilities to e-mails. S/MIME requires no change in the sending and receiving MTAs process because this service can be added to the client software installed at sending and receiving clients. Basically its provide sender authentication, non-repudiation of sender, message integrity and message security using encryption and digital signatures.

a) MIME (review).

MIME is an extension to the RFC 5322 framework that is intended to address some of the problems and limitations of the use of Simple Mail Transfer Protocol (SMTP), MIME provided support for varying content types and multi-part messages.

MIME specification includes the following elements.

doi:10.15849/icit.2015.0041

1. Five new message header fields are defined, which may be included in an RFC 5322 header as shown in figure (3).
2. A number of content formats are defined.
3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

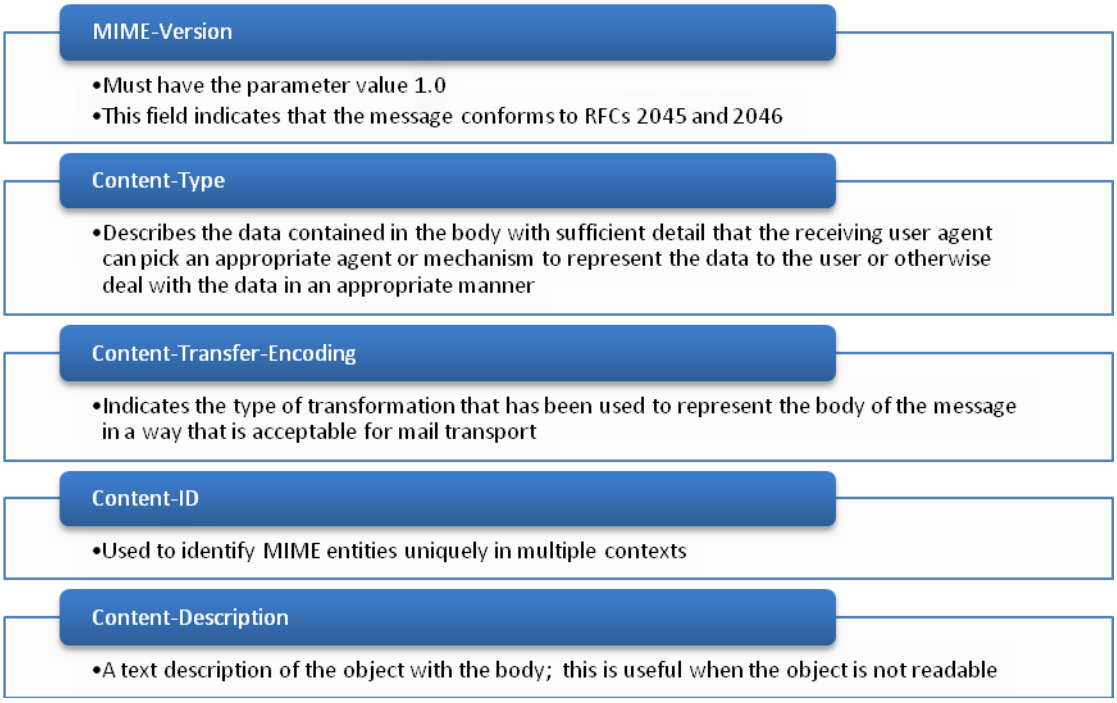

Fig.3 . MIME Headers

Example of MIME Message Structure:

```
From:Nathaniel                Borenstein
<nsb@bellcore.com>
To: Nead Freed <ned@innosoft.com>
Subject: Sample message
MIME-Version: 1.0
Content-type:multipart/mixed;
boundary="simple boundary"

Hello. This section begins the actual
message body,
```

b) S/MIME main functions.

1) Authentication and Confidentiality (Enveloped data)**:** In sender side, sender prepare an envelopedData MIME entity by generate a pseudorandom session key, which encrypted with the receiver public RSA key, Encrypt the message content with the session key. This envelopedData is then encoded into base64. In receiver side, to recover the encrypted message, the receiver first strips off the base64 encoding, then the receiver's private key is used to recover the session key, Finally, the message content is decrypted with the session key.
2) Authentication (Signed data)**:** In sender side, sender compute the message digest (hash function) of the content to be signed, Encrypt the message digest with the signer's private key, Prepare a block known as Signer Info that contains (signer's public key certificate, an identifier of the message digest algorithm, an identifier of the algorithm used to encrypt the message digest, and the encrypted message digest), then message and digest is encoded using base64. The Signer Info followed by the message constitute the signedData.

   In receiver side, to recover the signed message and verify the signature, receiver strips off the base64 encoding, and then the signer's public key is used to decrypt the message digest. Receiver independently computes the message digest and compares it to the decrypted message digest to verify the signature
3) Signed and enveloped data: encrypted data may be signed and signed data or clear-signed data may be encrypted.

doi:10.15849/icit.2015.0041

TABLE II. CRYPTOGRAPHIC ALGORITHMS USED IN S/MIME. [2]

Function	Requirement
Create a message digest to be used informing a digital signature	MUST support SHA-1
Encrypt message digest to form a digital signature.	Receiver SHOULD support MD5 for backward compatibility.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code.	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.

A. S/MIME message format

"The MIME entity is prepared according to the normal rules for MIME message preparation. Then the MIME entity plus some security-related data, such as algorithm identifiers and certificates, are processed by S/MIME to produce what is known as a PKCS object. A PKCS object is then treated as message content and wrapped in MIME". [2]

Example of S/ MIME Message Structure:

```
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Nead Freed <ned@innosoft.com>
Subject: Sample message
MIME-Version: 1.0
Content-Type: application/pkcs7-mime;
smime-type=signeddata;
name=smime.p7m
Content-Transfer-Encoding: base64
567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJh
jH776tbB9HG4VQbnj7
```

B. S/MIME problems.

Complexity of public key cryptography concept, and some user interface related usability problems of email clients supporting S/MIME (discussed are still barriers to S/MIME's adoption. Since S/MIME is not broadly used due to the above mentioned problems, we do not discuss further S/MIME related proposals. [14]

III. CONCLUSION

To summarize the state of secure e-mail software, we can say that software exists now to establish trust between two individuals Such software has actually been available for some time, but the quality and ease of use of available implementations has recently begun to improve. Software is available to secure MIME-based e-mail in a similar manner, although it is old as widespread and is mostly available commercially.

REFERENCES:

[1] J Kurose. and K . Ross, "Computer Networking: A Top-Down Approach", 6th Edition, Addison-Wesley Longman, 2012.

[2] Pfleeger and S. Lawrence Pfleeger. 2006. "Security in Computing" (4th Edition). Prentice Hall PTR, Upper Saddle River, NJ, USA.

[3] W. Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition 2006.

[4] Trend Micro Trend Labs Primer, "Trouble in your inbox. 5 Facts every small business should know about Electronic mail-based threats", Internet Security Threat Report, Volume 19, Oct 2012.

[5] IDC, "Worldwide Messaging Security 2013 – 2017 Forecast and 2012 Vendor Shares", International Data Corporation Aug 2013.

[6] McGuffin, "87-01-96 Security and Control of Electronic Mail by".

[7] http://www.sans.org/?utm_source=web&utm_medium=textad&utm_content=generic_rr_pdf_interst1&utm_campaign=Reading_Room&ref=36923 , last visit 27/4/2014

[8] http://www.softlock.net/eSign-Electronic mail-Security last visit 27/4/2014

[9] IDC, "Worldwide Security Software as a Service 2012 – 2016 Forecast: Delivering Security Through the Cloud" , International Data Corporation Dec 2012.

[10] S. Setapa "Securing E-mail", SANS Institute Reading Room site, 2001.

[11] P. Cocca, "Email Security Threats", SANS Institute Reading Room site, sep 2004.

[12] http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html

[13] M. Tariq Banday, "EFFECTIVENESS and LIMITATIONS OF E-MAIL SECURITY PROTOCOLS", IJDPS, Vol.2, No.3, May 2011.

[14] Pirouz, "SECURING EMAIL THROUGH ONLINE SOCIAL NETWORKS", August 2013