IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 34-36

Security Enhancements in Electronic Mail Systems

D.Ananthi
Assistant Professor in Computer Science, Annai Women's College, Karur

Abstract: *Email Security has become the forefront of network management and implementation. In distributed environments, electronic mail is the most used network based application. Users able to send e-mail to others, who are connected directly or indirectly to the internet using communications suite, Electronic mail networks have grown in both size and importance in a very short period of time. Electronic mail security describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. Now a day's variety of security mechanisms is implemented. Email security is the collective action used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts. This paper delivers two approaches that are used to protect email from unauthenticated access.*

Keywords: *Authentication, Confidentiality, E-mail Security Enhancements, Cryptographic Algorithms (SHA, DSS...)*

I. Introduction

There are number of security mechanisms are used in email, two of them are described here. One is Pretty Good Privacy approach another one is S/MIME .Any person can understand and be aware of illegal access on Email attacks. Even though there are defensive techniques to prevent email security threats, one cannot guarantee a secured email network. When developing a secure network, the following enhancements need to be considered.

Confidentiality: Protection from disclosure of email.

Authentication: Ensure the users of the network must prove their access rights and identity.

Message integrity: Protection from modification.

Non-repudiation of origin: Protection from denial by sender. Ensure a message transmission between parties via digital signature and/or encryption.

II. Pretty Good Privacy

It can be used to create a secure e-mail message or to store a file securely for future retrieval. It was developed by Phil Zimmermann. It provides confidentiality and authentication services that can be used for electronic mail and file storage application. Phil Zimmermann has done the following;

1. Selected best available crypto algorithms.
2. Integrated these algorithms into a general purpose application that is independent of operating systems and processor such as UNIX, PC, Macintosh and other systems.

The PGP has grown and it is widely used for a number of reasons;

1. It is available free that run on variety of platforms.
2. This package includes RSA, DSS and Diffie-Hellman for public key encryption; CAST-128, IDEA for symmetric encryption; and SHa-1 for hash coding.
3. It was not developed by, nor is it controlled by governmental or standard organization.

PGP Operations

Operation of PGP consists four services; Authentication, Confidentiality, Commpression, E-mail Compatibility.

Authentication

1. Sender creates message.
2. SHA-1 is used to generate a 160 bit hash code of the message.
3. Attached RSA signed hash to message with RSA.
4. Receiver decrypts & recovers hash code.
5. Receiver verifies received message, if it is matched with senders message, the message is accepted as authentic.

Confidentiality

1. Sender forms 128-bit random session key.
2. Message is encrypted using CAST-128 with session key.
3. Session key is encrypted with RSA using the recipient's public key.
4. Receiver decrypts & recovers session key.
5. Session key is used to decrypt message.

Compression

By default PGP compresses message after applying the signature but before encryption. The benefit of compression is saving space both for email transmission and filr storage. ZIP compression algorithmis used for compression and $Z^{-1}$for decompressuion.

E-Mail Compatibility

PGP segments messages is too big. It produces binary (encrypted) data appends a CRC. Email was designed only for text that is need to encode binary into printable ASCII character. Uses radix-64 or base-64 algorithm Maps 3 bytes to 4 printable characters.

III. S/MIME

Secure /Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the standard MIME email format based on asymmetric cryptography to protect our mails from unwanted access This technology was developed by RSA Data Security.

S/MIME Operation

RFC 822 defines a format for text messages that are sent using email. The format adds text messages an envolope of metadata called as header. It is seprated from body of the mail by a blank line. Each line in the header consists of a keyword such as From, To, Subject & Date.

MIME Headers

MIME indroduces a five new headers, such as;

- **(i) MIME Version:** This field must have the parameter vale 1.0. It indicates that the message conforms to RFC 2045 and 2046.
- **(ii) Content Type:** Describes the Data contined in the body with sufficient detail so that the receiver can pick the appropriate mechnism to represent the data to the user. There are seven different major type of content and a total of fifteen subtypes. The content type and subtype can be seperated by a slash and it also includes parameters.
- **(iii) Contet Transfer Encoding:** It indicates the type of transformation that has been used to represent body of the message that is acceptable for mail transport.
- **(iv) Content ID:** It is used to identify MIME entities in multiple contexts.
- **(v) Content Description:** A text description of the object within the body. Eg:audio data

S/MIME Functionality

S/MIME provides the following functions;

(i) Enveloped Data: This Consists of encrypted content of any type and encryption keys foe one or more recipients.

(ii) Signed Data: A digital signature is formed by taking the message digest of the content to be signed and encrypting with the private key of the signer.

(iii) Clear Signed Data: As with signed data , a digital signature of the content is formed. In this case, the digital signature is only encoded using base 64.

(iv) Signed and Enveloped Data: Signed only and encrypted only entities can be nested, so that encrypted data may be signed and signed data or clear signed data may be encrypted.

IV. Conclusion

In this paper introduced two different types of electronic mail security approaches that are used to enhance the security of electronic mail. The enhancements are founded in two directions, which are the authentication and confidentiality of the e-mail transforming.

References

Journal Papers:

[1]. Ms.Supriya and Mrs.Manju Khari, “MANET security breaches: Threat to a Secure communication platform”, International Journal on AdHoc Networking Systems

[2]. (IJANS) Vol. 2, No. 2, April 2012

[3]. Satyam Shrivastava, Sonali Jain “A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network “International Journal of Computer Science & Engineering Technology (IJCSET) Vol.4. No.3. 2013 ISSN : 2229-334

Books:

[4]. William Stallings, *Cryptography and Network Security* (Principles and Practice, Pearson, Fifth Edition).