ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Taxonomy of E-Mail Security Protocol

Ankur Dumka, Ravi Tomar, J.C.Patni, Abhineet Anand

Assistant Professor, Centre for information Technology, University of Petroleum and Energy Studies,Dehradun, India

ABSTRACT - The Email messaging is one of the most popular uses of the internet & the multiple internet user can exchange messages within short span of time using To (Original recipient), Cc (Carbon copy) and /or Bcc (Blind Carbon Copy) Facilities. Thus Email becomes the most popular application on the internet. It is also by far the most popular application on intra company networks. Securing e-mail is something that must be done by the users themselves, because they are the ones who will actually be sending & receiving the messages. However, security administrators can gives user the tools they need to be fighting the problems. S/MIME, PGP &PEM are very popular methods of encrypting e-mail .Email users need to be educated about security though because the popularity & functionality of e-mail is only going to increase.

KEYWORDS - PGP, PEM, S/MIME, SMTP, Cryptographic function

I. INTRODUCTION

Email is quite arguably the most important application for personal & business communication across the internet. People depend on it for sending text, image & even sound files to destinations .This is a far cry from the postal service & even the pony express for delivering the messages to their destination in days & weeks. Email was designed to be both easy to use & quick for fast end to end message delivery. Consequently, the security of email message has become an extremely important issue.

Securing email is something that must be done by the user themself, because they are the one who will actually be sending & receiving the messages. However security administrators can give users the tools they need to fight the problems. Server based & desktop based virus protection can help against malicious code, & spam filters attempt to block all unsolicited commercial e-mail. E-mail users need to be educated about security, though, because the popularity & functionality of e-mail is only going to increase.

The goal of Email security will be to provide secure method for sending & receiving email over the internet. This will include both service provider technologies, as well as, end user client solutions to encompass E-mail technology as whole.

The security protocol must encapsulate an essential set of cryptographic function .The security protocol support three cryptographic functions.

Encryption: The process of encoding plain text message into cipher text message is called as encryption.

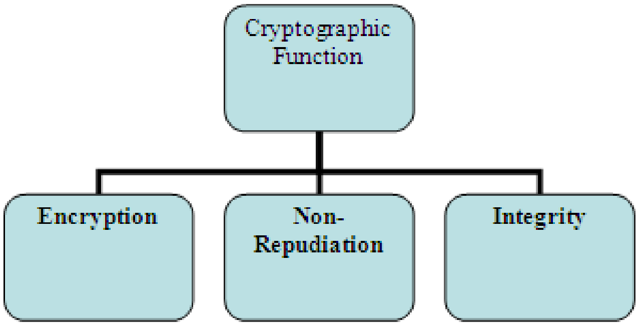
Non-Repudiation: Provide protection against denial by one of the entities included in a communication of having participated in all or part of the communication.,

Non-Repudiation, Origin: Proof that a message was sent by the specified party.

Non-repudiation, Destination: Proof that the message was received by the specified party.

Integrity: The transmitted message is never altered. The assurances that message received are exactly as sent by an authorized entity.

To ensure the e-mail security all these cryptographic function must implement with in a security protocol. There are three e-mail security protocols.



II.PEM

PEM is a set of standards for adding a security overlay to Internet e-mail providing message confidentiality and integrity. This set of standards describes security non-repudiation for electronic commerce applications. Protocol that can be used above the common Simple Mail Transport Protocol (SMTP) or the UNIX-to-UNIX Copy Protocol (UUCP). The PEM security enhancements provide three security services: message integrity, message origin authentication, and message confidentiality. The PEM enhancements can be used as a foundation to provide non-repudiation for electronic commerce application.

The PEM standard defines the use of the RSA public key algorithm to be used for key management and digital signature operations, and the DES algorithm is included for message confidentiality encryption

PEM is an e-mail security standard adopted by the Internet Architecture Board (IAB) to provide secure electronic mail communication over the internet.PEM was initially developed by the Internet Research Task Force (IRTF) & Privacy Security Research Group (PSRG). PEM provide several security services through various phases.

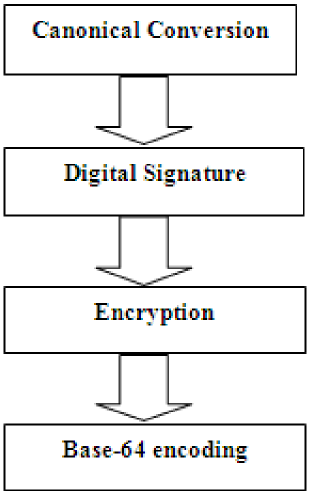


Fig 1. Various Phases in PEM

Canonical Conversion: There is a distinct possibility that the sender & receiver of an e-mail message use computer that have different architecture & operating system. PEM transform each e-mail message into an abstract, canonical representation. This means that regardless of the architecture & the operating system of sending & the receiving computers. The e-mail always travels in a uniform, independent format.

Digital Signature: This is a typical process of digital signature. It starts by creating a message digest of the e-mail message using an algorithm such as MD-2 or MD-5.Thus message digest thus created is then encrypted with the sender's private key to form the sender's digital signature.

Encryption: In the process of encryption the original e-mail & the digital signature are encrypted together with a symmetric key

Base -64 encoding: The base -64 encoding(also called as Radix-64 encoding)process transform arbitrary binary input into printable character output.
PGP:Phil Zimmerman is the father of Pretty good privacy protocol. He is credited with the creation of PGP.Cyber security based on PGP for DNP3 to strengthen computer network security. This PGP based cyber security provides authentication capabilities using public key cryptography with enhanced performance using symmetric key for the most of the encryption.The most significant aspect of PGP are that it supports the basic requirement of cryptography is quite simple to use & is completely free,including it's source code & documentation.

PGP implements e-mail security in a way that the user sends the e-mail,& the mail agent applies encryption as specified in them, the mail program's programming. The content is encrypted with the generated symmetric key,& that key is encrypted with the public key of the recipient of the e-mail or with the private key of the sender. The sender can also choose to sign the mail with their private key, allowing the recipient to authenticate the sender.PGP support Public key infrastructure(PKI)provided by the multiple vendors,including X.509 certificates.LDAP key sources such as Microsoft's Active Directory,& Novell's NDS.

PGP Freeware adds the security feature by offering information
Protection for individual computers. The types of added security include:
Data encryption, including email, stored files, and instant messaging
Virtual private networking, for secure remote communications

Data encryption enables users to protect information that they send out such as emails as well as information that they store on their own computers. Files and messages are encrypted with a user's key, which works in conjunction with scrambling algorithms to produce data that can be decrypted only by its intended recipients
.Data encryption is also an important part of a Virtual Private Network (VPN): information is first encrypted and then sent in this secure form over the Internet—an otherwise very insecure medium—to a remote host. Virtual Private Networks are a feature of PGP net, which is a PGP tool used for setting up VPNs. We should now be familiar with an overall picture of what PGP does.
PGP offers several features and utilities to help us secure our email, files, disk, and network traffic with encryption and authentication.
Here is what we can do with PGP:

- Encrypt/sign and decrypt/verify within any application. With the PGP menus and email plug-ins, we can access PGP functions while in any application.
- Create and manage keys. Use PGP keys to create, view, and maintain our own PGP key pair as well as any public keys of other users that we have added to our public key ring.
- Create self-decrypting archives (SDAs).We can create self-decrypting executable files that anyone can decrypt with the proper password. This feature is especially convenient for sending encrypted files to people who do not have PGP installed.
- Permanently erase files, folders, and free disk space. we can use the PGP Wipe utility to thoroughly delete our sensitive files and folders without leaving fragments of their data behind. We can also use PGP Free Space Wiper to erase the free disk space on your hard drive that contains data
From previously deleted files and programs. Both utilities ensure that our deleted data is unrecoverable.
- Secure network traffic. We can use PGP net, a Virtual Private Network (VPN), to communicate securely and economically with other PGP net users over the internet.

PGP includes:

Digital Signature: This is a typical process of digital signature. It starts by creating a message digest of the e-mail message using an algorithm such as MD-2 or MD-5.Thus message digest thus created is then encrypted with the senders' private key to form the sender's digital signature.

Compression: This is an additional step in PGP. Here the input message as well as the digital signature are compressed together to reduce the size of the final message that will be transmitted. For this the famous zip program is used.ZIP is based on the Lempel-Ziv algorithm.

Digital Enveloping: In this phase ,the symmetric key used for encryption in previous phase of encryption is now encrypted with the receiver's public key. The output of the step 3 & step 4 together form a digital envelope.

Base-64 encoding: The output of the step 4 i.e. digital enveloping is encoded.

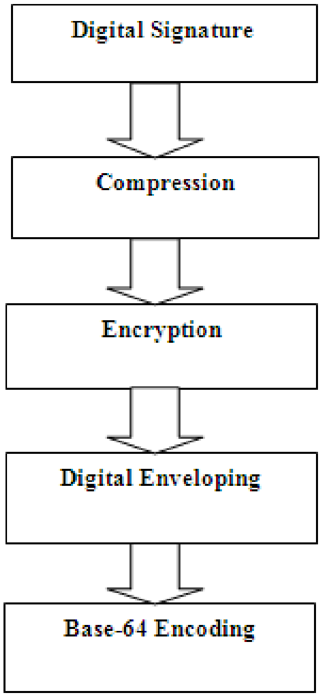


Fig 2. Various phases in PGP

III.S/MIME

MIME is an Internet Engineering Task Force (IETF) solution that allows users to attach non-text objects to Internet messages. MIME-capable e-mail clients can be configured to automatically retrieve and execute data files that are attached to an email message. The MIME standard provides a standard method of providing attachments to e-mail messages. Some of the MIME e-mail programs allow the user to configure what Type of attachments are accepted and how they are interpreted, other programs are not configurable. Users are cautioned to disable the automatic execution and interpretation of mail attachments. The attachments can be examined and processed after the user responds to prompt. In this configuration the user is warned that an attachment is going to be processed and the user has the option of cancelling that processing if they are unsure of the consequences. There is a system in development called atomic mail. Atomic mail is described as a language for interactive and computational e-mail. This language is being developed to provide portability between computer systems for the advanced e-mail attachments as well as to address security concerns. The atomic mail language is being designed with the constraints that processing does no harm and that access to the operating system, CPU, files and other resources is tightly controlled.

S/MIME is a well known standard for secure E-mail exchange. S/MIME build its identity management on E-mail addresses,rather than real names. This fact may sometimes cause sending a signed e-mail with a bogus name on it.

S/MIME, Secure/Multipurpose Internet Mail Extensions, is a standard designed to provide authentication and encryption services to MIME formatted email messages . It isbased on the X.509 certificate standard and the ASN.1 syntax. In the standard,Key transport and Digital signature both depend on public key cryptography. Encryption in S/MIME is work as a two-stage process referred to as creating a digital envelope. First, asymmetric cipher using the content encryption key (CEK) is applied to the message. After that CEK is using the
the CEK is encrypted using the recipient's public key. Both the message and encrypted key are sent.

IV.CONCLUSION

Here we had studied multiple protocols and techniques used for securing the email and thus find out how these protocols and implemented at which part of email that is an essential part of human life. Thus different security protocols like canonical conversion, digital signature, encryption, base4 encoding apart from these protocols we further emphasized on more security features provided to us like digital signature, compression, encryption, digital enveloping. Thus after these we can implement following security within our email and thus secure it from strangers.

REFERENCES

1.) Yang Xiao, Chaitanya Bandela, Xiaojiang (James) Du, Yi Pan, Edilbert Kamal Dass, "Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs", Int. J. Wireless and Mobile Computing, Vol. 1, Nos. 3/4, 2006.

2.) Thomas S.Messerges,Ezzat A. Dabbish,Robert H.Sloan, "Examing smart card security under threatof power analysis attack", IEEE transactions on computers,vol. 51,no.4, aprail 2002.

3.) B.Sridevi,M.Brindha,R.Umamaheswari,Dr.S.Rajaram," implementation of secure & cost effective authentication process in IEEE 802.16e WiMAX, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012

4.) M. Tariq Banday,"Effectiveness and limitation of email security protocol", International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.3, May 2011

5.) Charles J. Kolodgy, Meeting Email Security Head On: Dell's Secure Exchange Services, white paper sponsored by Dell in 2007.

.