RESEARCH ARTICLE OPEN ACCESS

Survey Report on Cryptography in E-Mail Security

[1]Nitin Kumar, [2]Satvik Yadav, [3]Mohit Sejwal, [4]Nitasha Soni
Manav Rachna International Institute Of Research And Study, Faridabad, Haryana
Corresponding Author; nitin Kumar

ABSTRACT: Today's e-mail security plays very important role in every fields. For those securities PGP, SMTP and MIME are mostly used protocols for message transfer. But, it lacks securities like privacy, security of E-Mail message. To make E-Mail statement more safe and concealed, servers adopted one or more securities protocols like (PGP, SMTP, MIME, etc).

KEYWORDS: Introduction, E-Mail security protocols, PGP, SMTP, MIME, security problems, overcome the security problems.

Date of Submission: 28-02-2019 Date of acceptance: 25-03-2019

I. INTRODUCTION

E-Mail is one of the oldest and popular network applications as well. It is used transfer the message from sender end to receiver end. During transmission it includes many types of virus and worms.Pretty good privacy and secure/ multipurpose internet mail extension are two example of secure e-mail system used in various platform like window, UNIX and other. E-Mail security is the major topic dealing with the illicit access of electronic mail. This illicit access can happen while an email is in broadcast as well as when it is stored on e-mail servers or on a customer computer.

E-Mail infiltrates many area of the internet full stop [1]. The benefits of the e-mail are for more than desired so it is used for frequently in daily activities. Businesses depends on e-mail to update their databases, plan and manufacture their output Now these days even we can send e-mail via mobile phones and PDA,s too. Main purpose of e-mail security is to e-mail message should be private only sender and the receiver must be able to communicate a secure communication.

II. HOW E-MAIL WORKS

An e-mail from computer to server:
Path 1- firstly the message is transfer to the server.
Path 2- The server again transfer the message to next server. Server uses the message to check the message from every server [2].

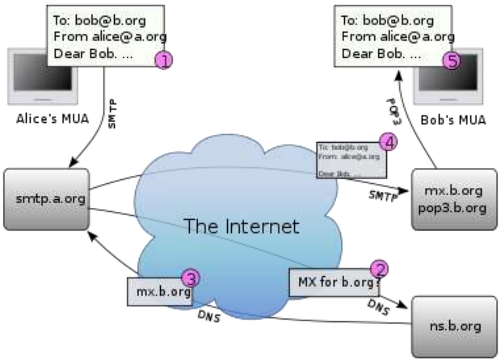

Fig-1 How E-Mail work

III. E-MAIL SECURITY PROTOCOLS

SSL - SSL stand for secure socket layer which is used to encrypt/decrypt personnel data along the insecure network environment. In the HTTP, the type of data encrypted / decrypted includes the URL, the HTTP header, cookies and the data submitted through different forms. A web page is more protected or it can private and then propel E-mail message request layer to transport layer since it control between these two protocols[3]. The SSL protocol can be separated into two parts- i.e. handshake protocol layer and record protocol layer**.**

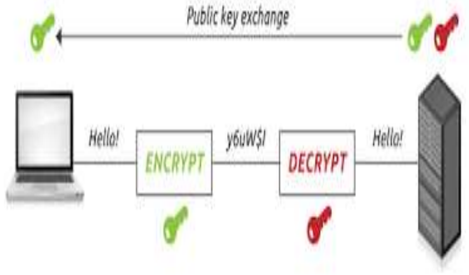

Fig-2 SSL (Secure socket layer)

SSH- SSH stand for secure shell it is a protocol commonly reffered as SSH for secure transfer of message over an insecure channel[5]. SSH is reasonably proficient, when very small bit of message are transferred. it is caused by the fact that SSH was residential to subway manually that happen in remote shell access. SSH keys is usually used technique of SSH verification are stored in different incompatible disc system[4][6]. SSH protocol exist in two versions- SSH1 and SSH2. SSH1 was found vulnerable to several attacks and SSH2 was found in public key and passward authentication.

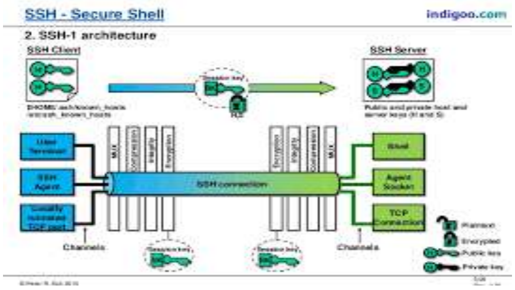

Fig-3 SSH (Secure shell)

SFTP- SFTP stands for secure shell file transfer protocol it is used to file transfer in a specialized subsystem for isolated file and folder manipulation. It ia type of SSH2 layer family member; however some message support it even with SSH1. SFTP, it contain less command . However, it support basic operation for file supervision. SFTP doesn't have a modify control address list and file names must be relative to users home folder or base folder of the message. The standard recommended avioding path for e-mail security purpose[3][4].

internet
ciphertext
ciphertext
encryption
decryption
plaintext
plaintext

Fig-4 SFTP (Secure shell file transfer protocol)

TLS- TLS stands for transmission layer security protocol which provides a common security platform at the transport layer for all the applictions. TLS consist of four component protocol i.e. handshake layer, change cipher spec layer, alert layer and record layer. These layer are used to negotiating cryptography algorithm, establishment of shared secret keys and securing the application data[6].

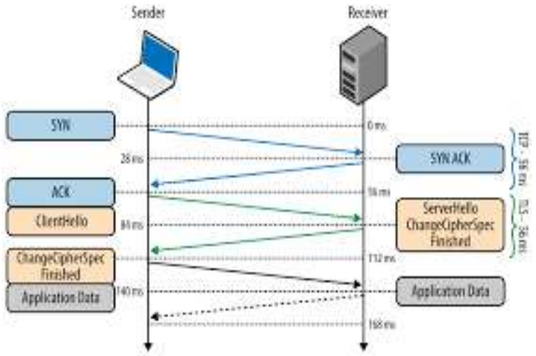

Fig-5 TLS (Transport layer protocol)

PGP

PGP stands for pretty good privacy which was developed for securing E-Mail messages and storing files securely for future retrieval. PGP is a accepted program which is used to check E-Mail over the network such as internet[5]. It can too be used to transfer the encrypted digital signature to lets the receiver checks the senders identity and knows that the message was not changed on the transmission royte. Available together as freeware and the short cost commercial versions, PGP is used by large amount privacy-ensuring programs by persons and is too used by many corporations. PGP means standard for E-Mail security. PGP can also be used to encrypted files being saved so that they are illegible by other users[7].

Operations of PGP are:- (a) authentication- message authentication can be carried out using digital signature. Alise as the sender computer digest of the message using SHA-1 and signs the digest using her private key.

(b) compression-compressionbefore encryption and after signature is the preffered option. By default, PGP follows this order.

(c) confidentiality- PGP encrypt message using symmetric-key encryption. Since mail is one way and one time operation, a new symmetric key is to be generated for each message and sent with the encrypted message.

(d) segmentation- there is usually limitation of maximum size of a message in E-Mail system. PGP automatically subdivides the E-mail message is too large into smaller segments.

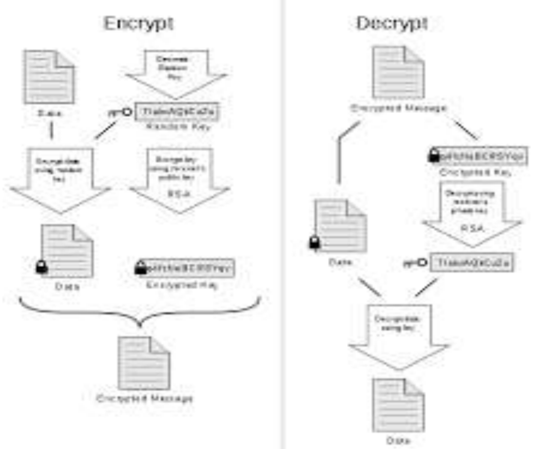

Fig-6 PGP(Pretty good service)

SMTP

SMTP stands for simple mail transfer protocol which is based on client-server model. It uses TCP as well known as port TCP port number 25 for the server[7]. All the commands, response and messages SMTP are in ASCII (american standard code for information interchange) format from 33 to 126 and the control symbol (CR,LF).

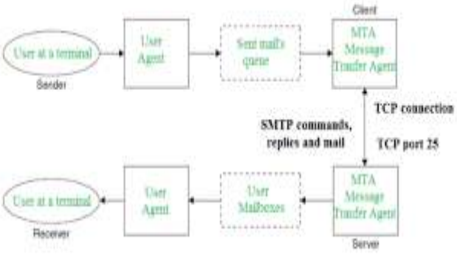

Fig-7 SMTP(Simple mail transfer protocol)

MIME

MIME stands for multipurpose internet mail extension it is a supplementary protocol that addresses these issues by transforming non-ASCII data into 7-bit ASCII at the sender end. The message is retransformed at the receiving end back to its original data type. Executable files, binary objects, text data of other language. There is a size limitation. SMTP servers may rejects mails having size greatest than the prescribed size[6][8]. In MIME, there are seven major content-type –text, image, audio, video, multipart, applications, messages. Security to the E-Mail services is provided by the way of additional MIME content type ie S/MIME i.e.secure multipurpose internet mail extension.

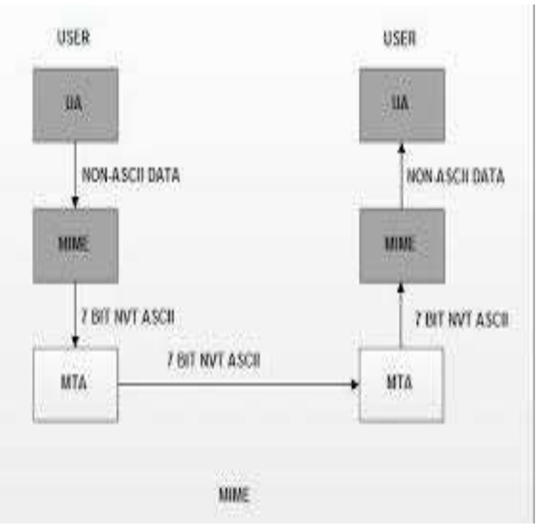

Fig-8 MIME (Multipurpose internet mail extension)

IV. CONCLUSION

E-Mail play very important role in every field like education, business, officies,industries etc-etc. E-mail is a important part of our daily work and along with that we deals with e-mail in our day to day work. As more and more users connect to the network.

Billion of dollar of transaction proceed every hour along the network, main advantage while using E-mail is low cost. Security can be built at a common platform for all applications, e.g. at the transport layer or at the network layer.

REFERENCES

[1]. Apukapadia, (2007)”a case study for secure e-mailcommunication”,IEEEsecurity&privacy,pp.80-84.

[2]. p.hoffman, (2002)“SMTP services extension for secure SMTP over transport layer security”, IETF RFC 3207.

[3]. C.morris and s.smith, (2007)“toward usefull secure e-mail”, IEEE technology and society magazine, pp.25-34.

[4]. J.lyon and m.wong, (2006)”sender id: authentication E-mail”, internet engineering taskforce (IETF), RF C4406.

[5]. Tony bradley (2000), CISSP-ISSAP,E-mail virus protection handbook.

[6]. John wiley & sons, ISBN: 047105318x, (1995), E-mail security, how to keep your electronic message private.

[7]. prakash c.gupta, (2015)”cryptography and network security”, pp 254-274.

[8]. Eagle, (2012)”network security”, pp 26-27.

Nitin Kumar" Survey Report on Cryptography in E-Mail Security" International Journal of Engineering Research and Applications (IJERA), Vol. 09, No.03, 2019, pp. 20-22