Mail Security Gateway Mechanism for Email Security

Linna Fan[1, a], Yufeng Ma[1,b] and Wanli Kou[1,c] ,Dong Kang[1,d] and Tianqi Wang[1,e]
1 Xi'an Communications Institute, China
[a]fanlinnafanlinna@163.com, [b]Mauf@163.com, [c]13389249896@163.com
[d]roller6041@sina.com,[e]734029755@qq.com

Abstract.

In order to solve the problem that email is not safe when transmitted in external link, the paper designed the Mail Security Gateway. It can encrypt and sign the email for its users and change the user as least as possible. The analysis shows that the Mail Security Gateway can provide security enhancement such as confidentiality, integrity, non repudiation and is very convenient to deploy in trans regional company.

Keywords: Email; Security; Gateway

Introduction

With the developments of Internet, email has become one of the most widely used applications. It is the most popular application with most users [1]. With its convenience and instantaneity, email is one ideal tool for people to communicate with others. But upto present most users don't know how to protect their Internet communications, and even don't attachimportance to the security of email [2].

There are two broad privacy vulnerabilities associated with conventional email: the vulnerability of the email's content (which is normally transmitted in plain text), and the metadata that can be derived from the email's header [3].

Many researchers have been focusing on the email security. Reference [4] proposed new protocol to replace SMTP (Simple Mail Transfer Protocol). This can fundamentally resolve the problem. But SMTP is widely used that it cannot be

replaced in a short time. Reference [5] proposed a new designed email server. And someone also turns to secure email service for help. For example, Lavabit and Silent Circle are two secure email services. But the US Government demanded that the company hand over its encryption keys. Lavabit recently shut down its secure email service because its founder, Ladar Levison, was forced to hand over encryption keys to the FBI. Rather than allowing them to snoop on his customers, he closed the company completely [3]. Besides the reason that US Government, Cristian Thiago Moecke and Melanie Volkamer also said in reference [6] that most email uses not use the security enhancement function because they don't understand it. So the security enhancement should be set insecurity provider.

Because of the reason above, paper designed a Mail Security Gateway, which can provide security for its users.

The design of the Mail Security Gateway

We think the external link is unsafe but the local area network is secure. So our Mail Security Gateway is used to protect email from external attacker. What requirement should the Mail Security Gateway meet? Firstly, it should provide confidentiality for email. Then the attacker external cannot understand the email. Secondly, it should have integrity checking function to make sure the email is not changed by others. Thirdly, the signature function is very important to support non repudiation. At last, the mail encryption gateway should verify its users through certificate and change its user as least as possible.

Mail Security Gateway. In order to simplify the user's configuration, we put the works of email encryption and decryption all in a Mail Security Gateway. Then the user almost cannot feel it. Why we designed it as this? That is because almost all companies have their own email servers. If we improve their security, we should change its network architecture as least as possible.

Fig. 1 is the construction of Mail Security Gateway. It can be divided into two parts. One is MTA. Another is ED module. MTA's function is same to other Mail Transfer Agent, which is responsible for local mail delivery and remote mail relay

[7]. The difference between Mail Security Gateway and other email server is its ED module part. It is responsible for encryption and decryption of email. It has five parts, which can provide functions of email encryption, decryption, signature and verify. Besides these, it also contains a key library, which are keys used for encryption, decryption and signature.

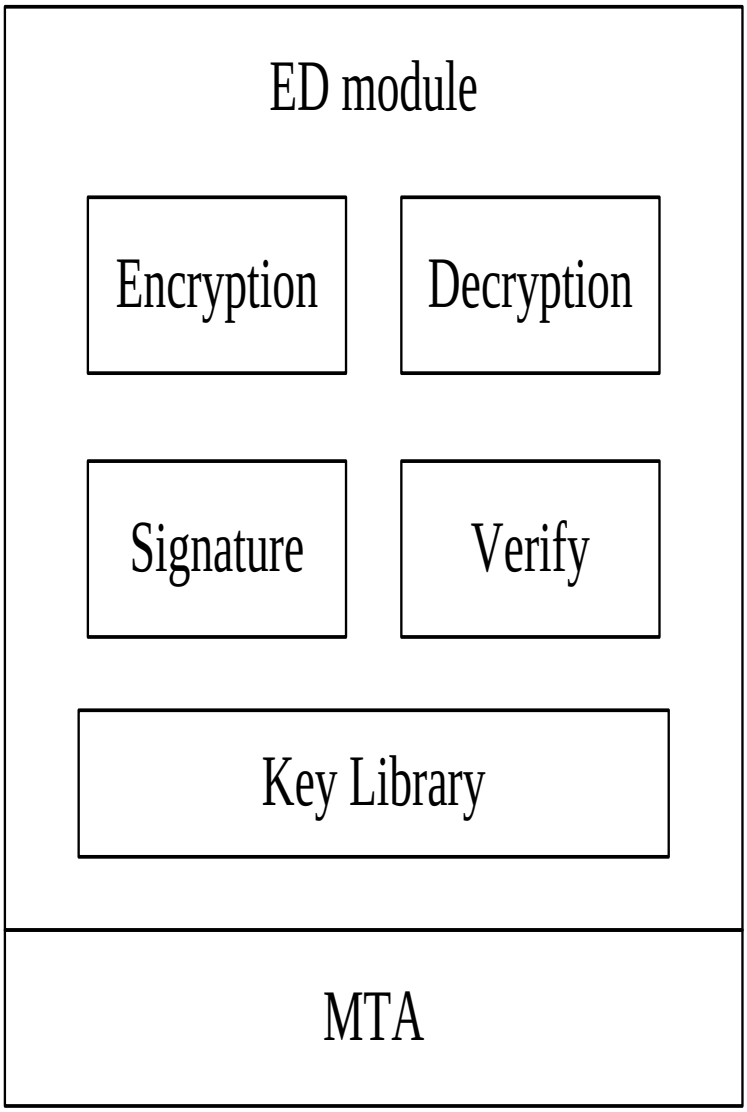

Fig. 1. Construction of Mail Security Gateway

The deployment of the Mail Security Gateway.

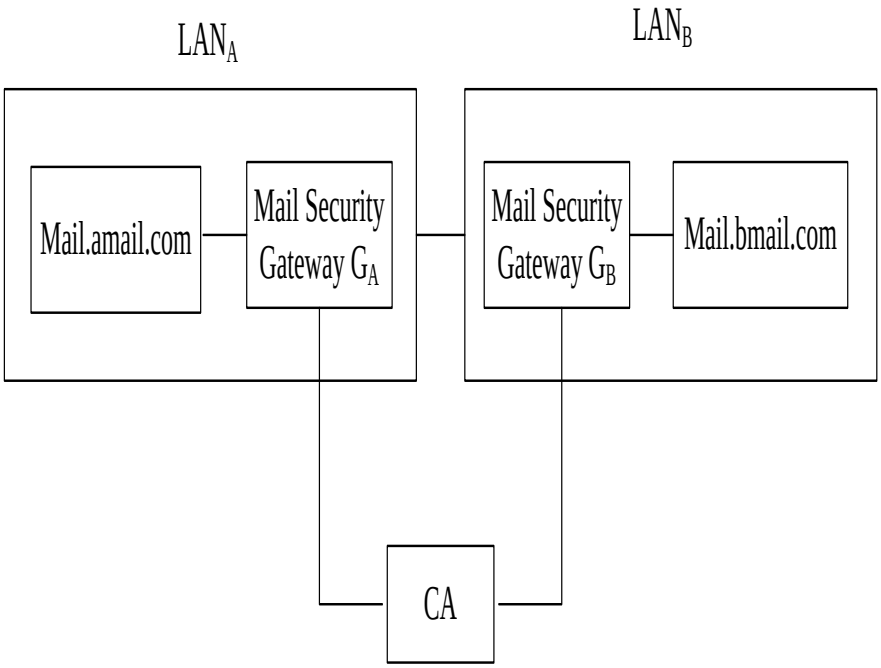

Fig. 2. The deployment of the Mail Security Gateway

The Mail Security Gateway is used to secure the local area network. So it should be put in the local area network. It must be configured as the relay host. Then all emails of users that send to external recipient will pass the Mail Security Gateway.

As shown in Fig. 2, LAN_A is a company's local area network. Mail.amail.com is its email server. Mail security gateway GA is set as its Mail Security Gateway. We think the inner of the local area network is safe. Usually LAN_A is a company's local area network. Email between inner users all use the Mail.amail.com. So email transfers in plain text in LAN_A. However, if the company has other subsidiary, for example LAN_B, there must be a Mail security gateway G_B. LAN_B uses its own email server Mail.bmail.com. Then no matter how many relay hosts passes, the email is always transferred in the ciphertext. When the encrypted email

reaches LAN_B, it first will be decrypted by G_B. After that, the recipient in LANB can read the email normally.

There is another scenario. If the recipient is in another place currently and the place is not a subsidiary of the company, there will not be a Mail Security Gateway to decrypt the email for the recipient. Then our Mail Security Gateway must provide multiple encryption form. It can be password encryption or pdf encryption. Then the password can be transmitted to recipient through other secure channel, such as short message.

Where are the public keys and private keys used for encryption and decryption come from? It is just the function of CA. CA is responsible for key generation. The generated keys will be sent to corresponding Mail Security Gateway. The Mail Security Gateway will maintain its users' keys. All encryption and decryption are done by Mail Security Gateway.

The working process of the Mail Security Gateway.

The process of a sender in LAN_A sending email to a recipient in LAN_B is as follows:

(1) Sender S in LAN_A sends an email e using his mailbox M_S

e: $S \rightarrow M_S$

If the recipient is an internal user, the email e will distributed to the recipient R's mailbox M_R and the process end. Else it will be processed by step (2) and follow steps.

(2) The email is obtained by the Mail Security Gateway G_A

e: $M_S \rightarrow G_A$

(3) G_A processes the email e

G_A:$En_{pbR}(e)||Sig_{prS}(Hash(e))$

$En_{pbR}(e)$ is to encrypt email e using recipient R's public key pbR. Hash(e) is the hash value of e. Then G_A signs the Hash(e) using R's private key prR. That is

$Sig_{prS}(Hash(e))$. Then GA concatenates $En_{pbR}(e)$ and $Sig_{prS}(Hash(e))$ to form $En_{pbR}(e)||Sig_{prS}(Hash(e))$.

(4) The processed email goes to the G_B of LAN_B

$En_{pbR}(e)||Sig_{prS}(Hash(e))$: $G_A \rightarrow G_B$

(5) G_B processes the encrypted email e

G_B:$De_{prR}(En_{pbR}(e))$, $De_{pbS}(Sig_{prS}(Hash(e)))$

Then G_B get e and verify $Sig_{prS}(Hash(e))$ whether it is S's signature or not and get Hash(e). After that, GB compute the hash value of e Hash(e)' and compares it with Hash(e). If they are equal to each other, the email e is not falsified by others. If not, G_B will throw e away.

(6) The email is sent to recipient R's mailbox M_B

If the email e is correct through verification, the email will be sent to recipient R's mailbox M_R.

e:$G_B \rightarrow M_R$

Then the recipient can obtain his email through software client or browser.

Analysis of the Mail Security Gateway.

The Mail Security Gateway should meet the requirements of mail security mentioned in section "The design of the Mail Security Gateway". Next we will analyze its security.

Confidentiality. In external link, the Mail Security Gateway can provide confidentiality for email. Because in external link $En_{pbR}(e)||Sig_{prS}(Hash(e))$ is transferred. Even attacker intercepts this data, he cannot understand it because he hasn't the recipient's private key prR to decrypt $En_{pbR}(e)$.

Integrity. The mechanism can also satisfy mail integrity. If the attacker changes the transmitted data from $En_{pbR}(e)$ to D, when the recipient receives $D||Sig_{prS}(Hash(e))$, he decrypts D and computes its hash value. Compared with Hash(e), they are not same to each other. So the recipient will not believe the email.

Non Repudiation. Non Repudiation is that the sender cannot deny the email come from him. When the recipient received$En_{pbR}(e)||Sig_{prS}(Hash(e))$, because $Sig_{prS}(Hash(e))$ is signed by sender S. So S cannot repudiate that the email sender is him. Then the mechanism can provide non repudiation.

Conclusions

Paper designed the Mail Security Gateway for trans regional company. The design and working process of the Mail Security Gateway was given. Through the analysis the Mail Security Gateway can provided security enhancement such as confidentiality, integrity and non repudiation. Besides this, it is convenient to deploy in a local area network.

References

[1] Tao Qu. The email road for enterprise-enterprise email market analysis through internet in China. China Information Technology (2007), p.43-45.

[2] Lina Zhang, Menghai Jiang. The security email based on smart card. 2012 International Conference on Medical Physics and Biomedical Engineering (2012), p.1634-1639.

[3] Danny Bradbury, Can we make email secure? Network Security (2014), p.13-16.

[4] http://www.sciencedirect.com/science/article/pii/S1361372313700988. New secure email protocol promised. Computer Fraud &Security (2013), p.3.

[5] Guizhong Li. Research on the small and medium-sized enterprises secure email system and its realization in chinese. University of Electronic Science and Technology of China (2011).

[6] Cristian Thiago Moecke and Melanie Volkamer. Usable secure emailcommunications: criteria andevaluation of existing approaches. Information Management &Computer Security (2013), p.41-51.

[7] Xiaoling Bao. The research and realization of secure email system for a special purpose in Chinese. Beijing Jiaotong University, 2010.06.