Zero Trust Can Completely Solve the Problem of Email Security

(May 17, 2021)

Zero Trust is a security concept, that is, not trusting anyone or anything. Although this is not a new technology, it is an innovative security concept that points out a clear direction for the development of network security in the era of digital transformation. Especially in the current global epidemic, remote office has become the norm. According to statistics from Microsoft's website, email usage in the business and education industries has increased by 28% year-on-year, and more than 90% of phishing attacks are carried out via email. Office 365 detects and blocks nearly 40 million phishing emails every month. Therefore, every organization must take measures to prevent and stop phishing email security threats, which is very important.

So, how can we eradicate these malicious email attacks? Let's first look at the two main types of email attacks: One is impersonating the email address of the company's president or government agencies to send fraudulent emails to users, requesting payment or providing important personal account information, etc. This is due to the "flaw" in the design of the email, because the sender's email address can be fake easily. If the recipient's mail server has set the SPF, fraudulent emails often use similar domain names to send fraudulent emails, such as admin@micr0soft.com (using 0 instead of o) to fake Microsoft corporate email.

The above picture shows a fake HSBC email. The sender's email address does indeed use HSBC domain name, which is very deceptive. If the user clicks the URL in the email, it will link to a fake HSBC website that look like HSBC official website, and let the user enter the bank account and password, then many users were tricked.

The second type is the unsecured web email service. Web mail is very convenient to log in to the mailbox, user can use any browser to log in to the mailbox to view email, but the password is often very simple, very easy to be enumerated and guessed, and easy to be obtained by malicious keyloggers. After the user logs in, since all emails are in cleartext, all confidential information in the emails can be easily stolen. There are two security issues here: one is that username/password authentication is insecure, and the other is that the email content itself is not encrypted and stored in cleartext in the mail server. Even if the mail server has TLS transmission encryption enabled, it can only guarantee the security of the email during transmission.

So, can Zero Trust solve the problem of email security? The answer is yes! The core idea of Zero Trust is not to trust anyone, not to believe in emails claiming to be the president of the company, because the sender's email address can be forged. If you can stick to this point and don't believe in any emails about payment or submission of any confidential information, then you will not be deceived!

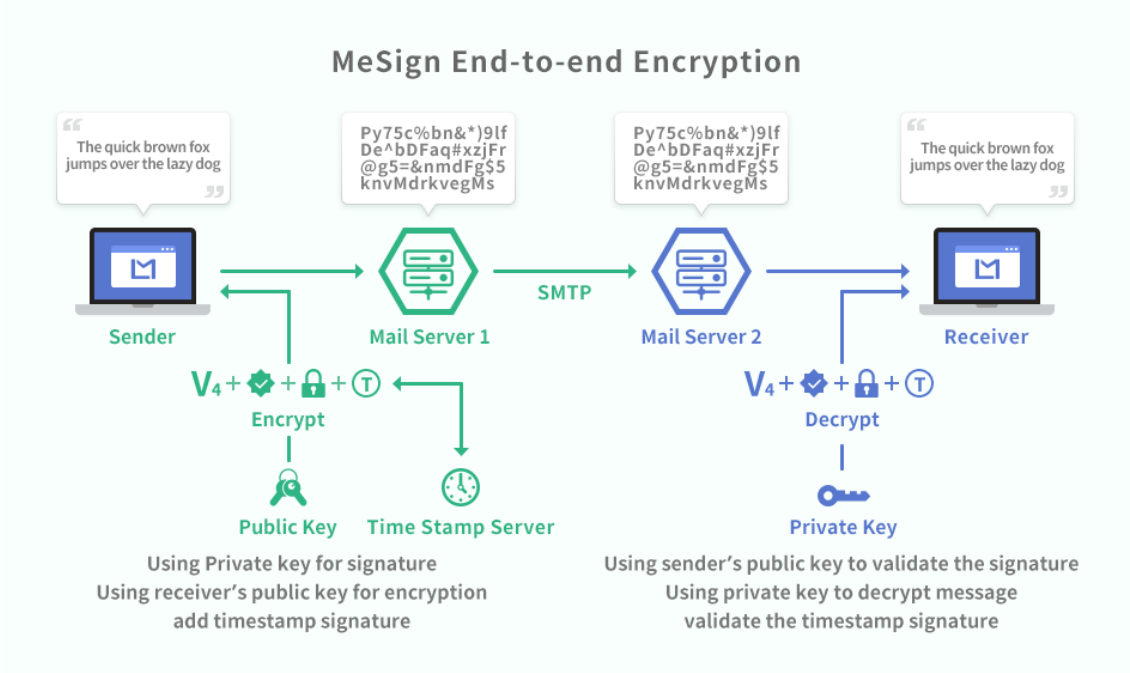
Of course, just doing the above is not enough, and it does not completely solve the problem of email fraud. MeSign email encryption and digital signature solution is a Zero Trust email security solution based on PKI technology. The specific main points are as follows.

First, **DO NOT** trust emails that do not have a digital signature. Every email must have a digital signature. With digital signature, it is impossible for fraudulent email to use bank domain email address to send fraud email, because the signing certificate used for digital signature needs to validate the email account control, and fake bank email sender does not have a real bank email address, so the fake email cannot get the signing certificate bound to the bank email address for digitally signing email. If the fraud email uses a real email address like the

other domain name, it cannot use the fraud domain name email like admin@micr0soft.com to impersonate Microsoft's email, because the fraud email cannot obtain the signing certificate with the Microsoft organization name, because the fraud domain cannot pass the strict third-party CA validation of identity. That is to say: do not trust any email without digital signature to ensure that you will not be deceived! The commonly used email client software such as Outlook and MeSign App will validate whether the digital signature is valid and trusted, MeSign App will display all unsigned email as "The message is not encrypted".

Second, **DO NOT** use unsecure username/password authentication method. Each user must have a digital certificate, the email system can disable Web login or modify the login authentication method of username/password to use digital certificate for strong authentication. Only in this way can the security of the web login of the mailbox be guaranteed.

Third, **DO NOT** believe in the cleartext email is secure, any email service or email security solution, if the email content is still cleartext in the mail server, it is unsecure, and we cannot trust that it is secure. How to do? Use MeSign App to automatically encrypt every email, this can not only ensure the security of emails during transmission, but also ensure that emails are stored in cipher text on the mail server, so that even If the email account password is compromised, it is impossible to obtain the confidential information of the email, thus ensuring the security of the confidential information of the email.



Currently, the reason why the email security problem is still very serious is that the traditional security vendor's solution is only to protect the mail server from being attacked, which is not enough; and the use of VPN to log in to the mail server on the intranet cannot solve all email security problem. The Zero Trust email security solution based on PKI technology does not care whether the mail server is on the intranet or on the cloud. In addition to deploying SSL certificate on the mail server to protect the security of the email transmission, a signing certificate must be used for strong authentication, instead of insecure username and password authentication. As for the email data itself, an encrypting certificate must be used to encrypt every email. The use of MeSign App as the email client software to send and receive emails can ensure that the email data stored on the mail server are all ciphertexts, even if they are obtained illegally, the emails obtained is a pile of wastepaper because they cannot be decrypted, making all email attacks lose their value, then email is secure.

Commonly used email clients such as Outlook and Thunderbird also support S/MIME email encryption and digital signature. Why don't people use digital signature and encryption to protect email security? This is because S/MIME encryption is too complicated. The three hurdles of applying for a certificate, exchanging public keys, and managing keys prevent users from the door of S/MIME.

Only MeSign email encryption and digital signature solutions use PKI technology and Zero Trust security concept completely solve the problem of email security. Do not trust cleartext emails, digitally sign and encrypt every email! MeSign Zero Trust email security solution can truly solve the problem of email security! Welcome to download and use MeSign App for free!

---------- END ----------

Richard Wang
Digitally signed by Richard Wang
ceo@mesign.com

Want to contact me to discuss this topic? Please use MeSign App (-) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.