

Stop the Email Content "Streaking"

(April 01, 2021)

If someone tells you-"I saw someone streaking on the street today!" Please don't believe it, because today is April Fool's Day! However, the author tells you today - "The email we use every day has been "streaking" for 50 years!" This is true.

As early as January 23, 2006, the author published a technical article "**Stop email content "streaking"**" in the well-known professional computer newspaper "[China ComputerWorld](#)", see below figure in Chinese. 15 years have passed, at present, the security of email content is still not optimistic. Of course, there has been progress. At that time, no email service system in China deployed SSL certificates, but now, most email service systems deployed SSL certificates, which can effectively protect the username and password security when logging in the Web, and also protect the user's IMAP/SMTP communication security. In other words, there is already a part of the email content no longer "streaking".

However, because there are still many mail servers that do not deploy SSL certificates. So, even if the sender's mail server deploys an SSL certificate, but the recipient's mail server does not deploy an SSL certificate, then the email is sent from the sender's mail server to the recipient's mail server is still transmitted in cleartext, and the recipient receive the email from its mail server is also transmitted in cleartext. In other words: simply deploying an SSL certificate on your own mail server does not guarantee the entire encrypted transmission of email, and it is still insecure.

Therefore, if you want to achieve reliable email encryption throughout the entire process, regardless of whether the recipient's mail server deployed a SSL certificate, the email content itself must be encrypted with an email certificate. This end-to-end encryption solution has not yet been popularized today (15 years later), not only in China, but also in the world. This is

because S/MIME email encryption is indeed very cumbersome and requires users to spend money to buy and apply for an email certificate, and then laboriously configures it in the email client. It also needs to exchange the public key with the recipient to realize the email encryption. Even IT personnel may not be able to handle this, the difficulty can be imagined.

Fifteen years have passed in a flash. Fortunately, cloud computing and cloud services are now very mature. MeSign Technology has established a cloud cryptographic infrastructure, and has developed MeSign App (encrypted email client), which integrates "cloud" and "client" working with each other, using S/MIME technology, realize the fully automatic email encryption and digital signature with timestamping at first in the world, making sending encrypted email as simple as sending ordinary cleartext email, users do not need to care about what is an email certificate, and there is no need to apply for email certificate from the CA, and no need to exchange public keys with recipients in advance. It is easy to send encrypted emails with one click, ensuring that email content is no longer "streaking". This innovative email encryption solution has been loved and praised by users in 171 countries/regions around the world now.

In other words, with the fully automatic email encryption solution provided by MeSign Technology, it is expected that the author's dream of "Stop email content "streaking"" in 2006 can be realized. "Remembering the very beginning mind, always have the good end." The author firmly believes that through the continued hard work of MeSigner and together with all Internet users around the world, the great dream of "Email Encryption Only" and "No email content "streaking"" will be realized soon in the future and make the encrypted email truly benefit all mankind.

Attached: "China Computer World" 2016, Issue 4 (January 23, 2006) C24 page of the author's article English translation.

Just attaching importance to the security of email servers cannot prevent email contents from "streaking" on the Internet.

Stop the Email Content "Streaking"

Email has become one of the most important and indispensable communication tools for modern people's personal life and work, which makes the problem of email security more and more prominent. Among them, the most serious problem is people's insufficient understanding of email security. A Google search for "email security" generally talks about how to prevent spam, virus and phishing emails and so on. In fact, the most important aspects of email security include two aspects: First, the security of email servers, including network security, and how to prevent and eliminate spam, virus emails, and phishing emails from the server side. This is the basic requirements of the email service; and another problem is how to ensure the email content will not be illegally stolen, illegally tampered with, and how to prevent illegal users from logging in to legitimate users' email accounts. In these two aspects, the author believes that the latter is more important, and it has not yet attracted people's attention.

It is precisely because there are very important personal confidential information and confidential business information in the email content that some people use illegal means to steal the email content, tamper with the email content, and forge the legal identity to send the fraud email. And since emails are transmitted in cleartext like other Internet applications, it is very easy to steal email content and tamper with email content. The commonly used email web login also uses simple username/password authentication, which makes it very easy to be authenticated, illegally log in to the email account to view and send emails. The above serious problems have not received sufficient attention and corresponding technical measures by email service providers. In fact, the existing mature PKI technology (digital certificate) can solve the above problems, that is, the deployment of SSL certificates for email servers. Use an email certificate to encrypt every email, and use an email certificate to sign every email, so that the recipient can be sure that the email is indeed from the claimed sender.



Among the current email service providers, only MSN (Hotmail) and Google Gmail have

deployed SSL certificates for Web logins, while almost none of the other major email service providers in China have deployed SSL certificates, let alone email certificates are supported, which means that the email messages sent by hundreds of millions of email accounts in China are all "streaking" (transmitted in cleartext) on the Internet, and they are all "postcards" sent by mail, rather than the enveloped letter in the real world, this situation is really very worrying. This irresponsible practice to email users (whether free users or paid users) is worthy of every email consumer taking legal action to protect the legality of consumers. At the same time, we also hope that major email service providers can deploy SSL certificates as soon as possible to ensure email security, so as to gain new competitive advantages in the fierce email service market.



----- END -----



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.