Email encryption still has a long way to go with a heavy load

The author first used email in 1995. At that time, the author used the Eudora, dialed into Hong Kong Telecom to access the Internet, and used the mailbox provided by HKT NetVigator to send emails. Later, the author registered Hotmail, Yahoo and MSN email accounts. From then to now, the author has been using email for work for 30 years, so the author have a special liking for email communication. Although instant messaging and social media are very popular now, various formal communications around the world are still mainly based on email, and its dominant position has never been shaken. Email is equivalent to paper letters and can be permanently saved in the mailbox for later reference. It is a very precious asset. Unlike chats that it disappears after the chat, and unlike public information posted on social media, email is your private message.

The author learned how to use email certificates to encrypt emails when reselling GeoTrust email certificates in 2004, and have been addicted to S/MIME email encryption ever since. After years of experience using encrypted emails, I have come to realize how inconvenient email encryption is, and it is precisely because of this inconvenience that email encryption has not yet become popular.

However, now almost all email services have been migrated to the cloud, and emails are transmitted and stored in plain text. It is obvious that plain text emails can no longer be used with confidence by users. However, the largest Internet traffic, HTTP traffic, has implemented mandatory HTTPS encryption and is close to universal HTTPs encryption, which effectively guarantees the zero trust security of HTTP traffic. As for the security of email traffic, although the "Federal Zero Trust Strategy" released by the US government emphasizes the importance of email encryption while emphasizing HTTPS encryption, there is currently no email encryption solution with good user experience on the market, so no specific solution that can be implemented can be given.

There are various email encryption solutions on the market. This article summarizes the various solutions so that everyone can have a more comprehensive understanding of email encryption.

1. Email Client Encryption

When email was invented, it was in plain text, including email transmission, and the plain text of email was stored in the email server. With the popularization of email, the S/MIME encrypted email standard appeared, and CAs issued email certificates, and email clients supported the use of email certificates to encrypt emails. Commonly used email clients such as Outlook, Thunderbird, and Apple Mail all support the S/MIME standard to implement email encryption.

There are other solutions on the market that support PGP email encryption and IBC email encryption. These two solutions only focus on encryption, and do not focus on sender identity validation. The author believes that emails not only need to be encrypted, but also need to prove the sender's trusted identity. Only a trusted identity validated by a trusted third-party CA can prevent email identity fraud. Both are very important, and only the S/MIME solution can do this. S /MIME is not only what the author loves, but also the technical route adopted by most email encryption solutions in the industry, and it is also a solution adopted by commonly used email clients. The International Standards Organization - CA/Browser Forum has also specially established an S/MIME Certificate Working Group and formulated the S/MIME certificate baseline requirements, requiring the global trusted CA to follow this standard from September 1, 2023. This is the greatest recognition of S/MIME encryption technology in the global industry, allowing CAs to issue S/MIME email certificates in a regulated manner for the first time. Therefore, ZoTrus Technology email encryption solution is a solution that adopts the S/MIME standard. This article only talks about S/MIME encryption and digital signature solutions.

There are three main obstacles to the widespread adoption of S/MIME technology for email encryption in email clients:

(1) **You must apply for an email certificate from a CA**

The certificate application process is very cumbersome, and after obtaining the certificate, you still need to configure the certificate in email clients, renew the certificate every year, manage the certificate private key yourself, etc.

(2) **You must first exchange public keys with the recipient**

The sender must send a digitally signed email to the recipient, and the recipient must reply with a digitally signed email to complete the public key exchange before they can start sending encrypted emails. In other words, the other party must also have an email certificate and configure it on the client software before it can be used.

(3) **You must manage your own private keys**

This is very important, including managing expired certificate private keys. Many of the author's early encrypted emails can no longer be decrypted because the certificate private key used for encryption is lost or the protection password is forgotten. This is a pain for users who use email encryption. Sometimes important emails that are urgently needed are found but cannot be decrypted.

It is these three application barriers that hinder the popularization of S/MIME encryption technology. As a result, this advanced technology, which had already formulated the RFC 2311 international standard in 1998, has not been widely used today, 26 years later. People still have to endure the insecurity of plaintext emails because they are too difficult to use, and non-professionals cannot handle such complex encryption technology.

2. Email TLS encryption

The email sending protocol SMTP and the receiving protocol POP3/IMAP are both designed to be transmitted in plain text, so the industry's first action is to implement TLS encryption for the SMTP and IMAP protocol, learn from HTTPS encryption, and use SSL certificates to implement transmission encryption for sending and receiving emails. In other words, both SMTP mail servers and IMAP mail servers must deploy SSL certificates to implement email transmission encryption to ensure that an encrypted channel is used when users send emails from email clients to mail servers, and that encrypted channels are used to transmit emails from the sender's mail server to the recipient's mail server. The recipient also uses an encrypted channel to retrieve emails from the mail server to ensure that plain text emails will not be illegally stolen or tampered with during transmission.

However, this TLS transmission encryption requires that both the sending and receiving mail servers support TLS transmission encryption, which means that emails are still transmitted in plain text on the party that does not deploy SSL certificates, and it is still impossible to guarantee the full encryption of emails during the entire transmission process. Therefore, there is an international standard RFC 8461 (MTA-STS, SMTP Strict Transport Security), which is a standard for enforcing full TLS transmission encryption. SMTP servers can refuse to send emails to mail servers that do not deploy trusted SSL certificates to ensure the full encryption of email transmission.

This technology is invisible to email users, but please note that this technology only solves the security of plain text emails in transmission, and it does not achieve end-to-end encryption like email clients do with email certificate encryption. If the email is sent in ciphertext, the SMTP transmission process can also ensure the security of email transmission without using TLS transmission encryption. Even if the email is transmitted to the email server through TLS encryption, it is still stored in plain text in the cloud email server, which still cannot reassure users, because the email service provider can read the user's email content manually or by machine. Some email service providers make profits by machine-reading email content and displaying advertisements next to the email content.

3. Webmail Encryption

The leader of this type of solution is ProtonMail from Switzerland, which supports email encryption through email client and Web, and seems to have received good market share from users. The author must point out that the core problem of this email encryption service is a conflict of interest between different roles. ProtonMail provides both email content hosting services and email encryption services, and it manages the encryption keys for users. You should be able to find the problem with this so-called email encryption service that absolutely protects user privacy. In other words, ProtonMail has both the encrypted email content of the user and the key to decrypt it. Can users still rest assured that the encrypted email is really safe?

4. Email Gateway Encryption

This is a solution that does not require any modification to the existing email client, and it is invisible to email users. There are many such solutions on the market. The author has tried a solution from a well-known email security company, which supports S/MIME email encryption, but it requires users to apply for an email certificate from the CA and upload the email certificate (private key) to the gateway. The gateway then calls the email certificate to implement email encryption and decryption.

This is a solution similar to that of an email client. There are still three application barriers that exist in email clients in implementing email encryption, and the author do not repeat these problems.

5. The road to email encryption with ZoTrus is difficult but the mission must be accomplished

The author has been practicing email encryption since 2004, and it has been 20 years now. The author has deeply realized the difficulty of email encryption. The author still remembers the original intention and continues to explore the optimal solution for email encryption after re-starting a business. The upcoming ZoTrus Email Security Service will be the latest answer given by the author, so stay tuned.

The author's 20 years of email encryption practice can be divided into three stages:

Phase I: Selling email certificates and instructing users to use email clients to implement email encryption.

At this stage, the author's main work was on selling email certificates and providing users with completely free one-year email certificates. A detailed guide to using email certificates was provided to users, including how to configure email certificates in commonly used email client software, how to send digitally signed emails and encrypted emails, how senders and receivers exchange public keys, etc. This stage was very tiring, and the only reward was a deep understanding of how difficult email encryption is to use, because CA only sells email certificates, and email client developers only guarantee that users can use email certificates to achieve encryption after they have configured them correctly, and there is no connection between the two industries and no seamless user experience connected.

Phase II: Developed an email client to automate email encryption, but it was not completed.

It is precisely because the author knows how difficult it is to implement email encryption using email clients and email certificates, so the author decided to develop an email client software (MeSign APP). This email client is not a normal email client, but a client software that can automatically configure email certificates for users for free. It can realize automatic encryption of emails invisibly. Users only need to change to an email client software. This is the world's first email encryption automation solution similar to the HTTPS encryption automation solution (ACME). It realizes the seamless connection between CAs and email client developers, combining the two into one to realize automatic email encryption. But unfortunately, after MeSign was acquired, the author had to leave, and this self-developed email client project has been stranded before it was fully completed.

Phase III: Automating email encryption based on ZT Browser; this is a solid step forward.

The author started a new business in June 2021, and he still remembered a German user's love for email encryption automation. After using the APP developed in the second phase, this user called it is a Life Saver, which completely solved the tedious certificate application, email client configuration, public key exchange and key management problems, and completely liberated him from them. Therefore, the author did not forget his original intention and continued to study and explore email encryption automation solutions.

One of the biggest problems encountered in the second phase of developing the email client software was that it is very hard to convince users to change their email client software, because users were already very familiar with using the commonly used email client software, especially large organizations that have been using specific email clients for many years, and email encryption is just a small function. It is impossible to require all employees to change their familiar email client to an unfamiliar email client just because this function is not easy to use. Users are not only very familiar with the use of commonly used email clients, but also have everyone's address book, schedule management, historical emails, etc., which users cannot give up their email client for email encryption.

However, the exploration in the second phase deserves high recognition for achieving automated email encryption, which is the main reason why it is most popular with users. Therefore, the technical route that the author still insists on in the third phase is automatic email encryption, automating the configuration of email certificates for users for free, automating the exchange of public keys, automating email encryption and automating email certificate management. In order to solve the problem that users cannot abandon their commonly used email clients, the new solution must give up the idea of asking users to change email clients and find new solutions.

Fortunately, when the author was developing the HTTPS encryption automation solution, we developed and released ZT Browser. The original starting point was to make the browser support the SM2 algorithm and the SM2 SSL certificate, and it uses the SM2 algorithm to implement HTTPs encryption. Since ZT Browser is the only completely free SM2 supported browser on the market that supports the SM2 algorithm and SM2 certificate transparency, it is very popular now in China. ZT Browser is not only an original general purpose browser based on open source Chromium like Google Chrome, but also a browser that supports the three cryptographic algorithms of RSA/ECC/SM2 to implement adaptive algorithm HTTPS encryption. It is also the world's first build-in PDF reader that validates the digital signature of PDF documents in real time and displays the trusted identity of the digital signer. In other words, whether users care about the SM2 algorithm or the PDF reader that supports digital signatures, users have fallen in love with ZT Browser, which has made the market share of ZT Browser in the global market rise steadily. In just two years, it has covered users in more than 130 countries and regions around the world.

According to third-party statistics, the proportion of users who use browsers to log into Web mail is twice that of users who use email clients. In other words, most users like to log into Web mail directly with browsers to view emails. This points out the general direction of email encryption solutions for us - to build it on ZT Browser, so that users can automatically decrypt encrypted emails when viewing emails with ZT Browser, and automatically encrypt emails when sending emails. The implementation of this function solves the email encryption automation needs of more than 50 % of users. For users who use email clients, the email service also supports browser Web login, because 100% of all email service providers provide the Web login mailbox function. In other words, using a browser to log into the email is an experience and usage experience that all users have, and it can fully cover all email users. All users need to do is to install another browser. Users have actually developed the habit of installing and using multiple browsers.

ZoTrus Technology does not change the user's habit of using familiar email clients, but only requires the installation of an additional browser with excellent functions. It is an acceptable solution for users to automate email encryption. In addition, ZoTrus solution enables the Windows version of Outlook to automatically decrypt emails encrypted with ZT Browser, achieving compatibility with Outlook's S/MIME encryption and decryption functions to the greatest extent.

The upcoming upgraded version of ZT Browser(V2501) supports automatic email encryption and decryption. Users only need to use ZT Browser to log into their mailbox to automatically activate ZoTrus Email Security Service for free. It can also automatically configure dual-algorithm email certificates for users - RSA email certificates and SM2 email certificates for free. Dual-certificate dual-algorithm adaptive encryption allows users to choose which cryptographic algorithm to use by default to implement email encryption. Please look forward to experiencing the different ZoTrus email encryption automation service for free, thanks.

Richard Wang

October 22, 2024
In Shenzhen, China

2024.10.22
00:28:09
+08'00'

Follow ZT Browser at X (Twitter) for more info.
The author has published 74 articles in English (more than 94K words)
and 185 articles in Chinese (more than 531K characters in total).