

Secure Email

Conner Brinkley

11.13.2020

Applied Cryptography
The University of Tennessee

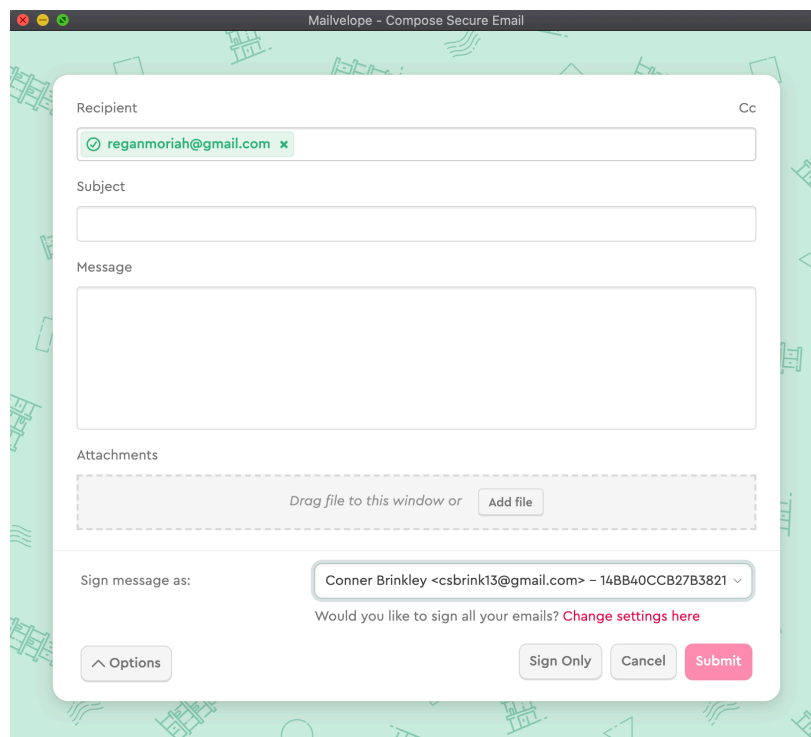
INTRODUCTION

The purpose of this experiment is to explore the usability of modern end-to-end email encryption by installing software for both the S/MIME and PGP protocols and exchanging secure emails with another student, similar to the popular “Why Johnny Can’t Encrypt” experiment. Although secure email software has improved since that paper was written, the answer to the question of whether or not it is worth the trouble for the average person might not be a surprise.

PROCESS

Starting off, I installed a Chrome browser extension called Mailvelope, which supports PGP communication with many webmail providers. It seemed like one of the easier options for the PGP protocol. After installing, I was required to manually generate a key using Mailvelope’s website, so I chose a 4096-bit key using the RSA algorithm. After my key was generated, I switched over to Gmail and noticed that there was a new button next to the “Compose +” option to write a secure email using Mailvelope.

For this experiment, I exchanged emails with Regan Moreno, who also used Mailvelope on their Windows machine. After clicking the button to compose a new secure email, a new window popped up in my browser to compose the message as shown in Figure 1 below.



Mailvelope - Compose Secure Email

Recipient: reganmoriah@gmail.com

Subject:

Message:

Attachments: Drag file to this window or Add file

Sign message as: Conner Brinkley <csbrink13@gmail.com> - 14BB40CCB27B3821

Would you like to sign all your emails? [Change settings here](#)

Options Sign Only Cancel Submit

Figure 1. Secure email in Gmail using Mailvelope.

I assumed that Mailvelope would just use the Gmail interface and do its magic behind the scenes after an email was sent, so when this new window appeared, I was not a huge fan. It was also confusing trying to add Regan's key to my account so that I could successfully encrypt a message. If I had not already known that I needed to obtain whoever's key I am exchanging messages with before encrypting, it would have taken much longer, and I may have given up. Mailvelope should automatically add other user keys when you receive a signed PGP email, but it took a few exchanges between Regan and I before it successfully added their key to my account, which was annoying. However, after several exchanges, we were successfully able to sign and encrypt messages between each other using PGP with Mailvelope.

After successfully exchanging secure emails with PGP, we moved on to S/MIME. I use Apple Mail on my MacBook as my preferred email client, and it actually has built in support for the S/MIME protocol, which made this much smoother from the start than Mailvelope. All that was needed to get started was a certificate that I acquired for free from Actalis in about ten minutes.

Once the certificate was downloaded to my computer, I simply clicked on it, and that prompted the built in Keychain Access app to open. It asked for an admin login to add the certificate to the system, and after access was granted, it automatically generated a 2048-bit key with RSA behind the scenes without ever asking or telling me what it did. I only found the key details because I was specifically looking for it, but the average user would probably never know, which I particularly think is a good thing.

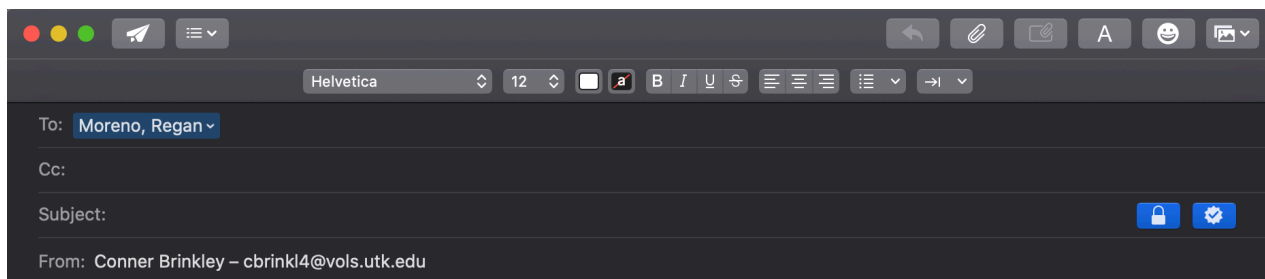


Figure 2. Secure email in Apple Mail.

Now that the certificate was added to the system keychain, two new buttons appeared in Apple Mail when sending an email from the account with the certificate. The two new buttons can be seen above in Figure 2. Clicking the left button digitally signs the message, and the right button encrypts it. However, you are unable to encrypt anything until you receive a signed message from another person.

Regan had some trouble getting S/MIME working on Outlook, which took a day or two, but once they got it set up, the process (at least on my end using Apple Mail) was much easier and integrated than Mailvelope. Regan sent me a signed email with their key that Apple

automatically added to the Keychain Access app, and then we were able to send signed and encrypted messages back and forth. Aside from having to acquire a certificate and entering in an admin password a couple times, the Apple Mail client handled secure emails with S/MIME seamlessly.

RESULTS

After successfully exchanging signed and encrypted emails with Regan using both PGP and S/MIME, I rated each experience using the System Usability Scale (SUS). SUS consists of ten usability questions that are each meant to be given a score between 1 and 5, with a score of 1 meaning “strongly disagree” and 5 meaning “strongly agree.” Table 1 below shows the SUS results with PGP using Mailvelope.

SUS Questionnaire for Mailvelope (PGP)	
I think that I would like to use this system frequently.	1
I found the system unnecessarily complex.	2
I thought the system was easy to use.	3
I think that I would need the support of a technical person to be able to use the system.	1
I found the various functions in this system were well integrated.	3
I thought there was too much inconsistency in this system.	2
I would imagine that most people would learn to use this system very quickly.	1
I found the system very cumbersome to use.	3
I felt very confident using the system.	1
I needed to learn a lot of things before I could get going with this system.	3
FINAL SCORE	45

Table 1. SUS analysis of the PGP protocol using Mailvelope.

The final score at the bottom is supposed to represent a total score out of 100. 45 out of 100 is not the greatest, and this is because of a couple of reasons. Installation was very easy, since it was just a browser extension, but I ran into some problems trying to obtain Regan’s key and sending encrypted emails, as mentioned before. On top of that, manually having to generate a

key is something that I do not think average people would understand the point of, and it is not very well explained in the software. Mailvelope had a decent FAQ on their website, but someone who has not studied computer science would likely give up at that point. For those reasons, in addition to my dislike of webmail, I would probably never use Mailvelope again.

Using S/MIME with Apple Mail was much better, which can be seen in Table 2 below.

SUS Questionnaire for Apple Mail (S/MIME)	
I think that I would like to use this system frequently.	2
I found the system unnecessarily complex.	2
I thought the system was easy to use.	3
I think that I would need the support of a technical person to be able to use the system.	1
I found the various functions in this system were well integrated.	4
I thought there was too much inconsistency in this system.	2
I would imagine that most people would learn to use this system very quickly.	1
I found the system very cumbersome to use.	3
I felt very confident using the system.	3
I needed to learn a lot of things before I could get going with this system.	1
FINAL SCORE	60

Table 2. SUS analysis of the S/MIME protocol using Apple Mail.

60 out of 100 is much better than PGP, but it still does not seem like enough to convince the average Mac owner to start using secure email. I particularly enjoyed how smooth the process was compared to Mailvelope, especially how Apple automatically handled key generation and exchanging behind the scenes.

I would consider using S/MIME with Apple Mail again if I needed to send something confidentially and I absolutely had to use email. It was easy enough to get a free certificate. However, if I had the option, there are so many other simpler ways to send messages securely, so it would probably not be my first choice.

CONCLUSION

In conclusion, secure email software has improved since the famous “Why Johnny Can’t Encrypt” experiment. But has it improved enough to convince average email users to start encrypting their emails? I do not believe so. Although it was not terribly difficult or frustrating, secure alternatives to email like the Signal app are more widely used. Maybe in the future, email clients will come pre-packaged with easier security tools, but until that happens, I do not see any advantage of going out of the way to set up secure email with 3rd party tools over using apps that have security baked in like Signal or WhatsApp.