Isai Mercado Oliveros

misaie

October 22, 2015

Encrypted Email

For this project, I used thunderbird on Linux Mint. For PGP encryption, Install the thunderbird extension Enigmail, and for SMIME encryption I used the thunderbird's built in SMIME functionality. In my experience PGP is easier to use if you want an easy and fast solution to send encrypted emails. It is easy to make your own keys, and it is easy to find a way to interchange keys with the other party. Once you have interchanged keys, thunderbird stores them and links them to the email address of the owner. Thus, when you send an email to that person, the email is automatically encrypted, and sent. It is easy and fast because there are no regulations. It works without asking for permission to no entity.

On the other hand, SMIME is more designed for big organizations. One of my biggest problems and frustrations with SMIME was the chain of trusted certificates. I got my free personal certificate from comodo.com. It was a little pain trying to figure out how certificates work and get stored, but once I found out how to export the certificate from the browser to my computer, and then from my computer's folder to thunderbird, I got a problem when trying to send the email. The problem was that the same certificate could not be used for signing and encryption. After I figure that the certificate was only good for one or the other, I sign the email and sent it, so that the public key would be sent with the signature. When the recipient received the email he could not store the public key of my certificate because her thunderbird did not trust my certificate. Finally we figure out that one certificate from the chain was missing, and after

some hours of surfing the internet I found the missing link. Once the certificate was installed, the whole process worked and it was as easy as PGP.

In conclusion, PGP is better if emails are being sent between parties that do not need any kind of organizational structure, because signing and encrypting is very easy. SMIME on the other hand needs more knowledge about certificates, and trust chains, but it is designed for big companies.