PGP and S/MIME

For PGP I used Gmail with the Chrome extension “mymail-crypt.” The extension made it easy for me to create a 2048 bit PGP key using OpenPGP.js. It also allowed me to compose my message in Gmail, then easily encrypt and/or sign the message with the click of a button. For S/MIME I acquired an X.509 certificate from Comodo then imported that certificate into Outlook. Outlook gave me an option to automatically sign all of my emails sent through Outlook and automatically encrypt when sending to a trusted recipient (a recipient whose certificate I have and trust).

The biggest difference between PGP and S/MIME is that PGP relies on a “Web of Trust” and users exchanging their public keys with those they want to communicate with, whereas S/MIME relies on hierarchical certificate validation system through a trusted third party. Because you basically self-sign your own PGP keys, there is no way to know whether a particular key is valid or not. You could make up a key pair for any email address, and no central authority can validate it.

I have never sent secure email before, mostly because I am not paranoid about my email privacy or security. Email serves as a convenient way for me to send information, but I realize that it is not secure, so I am careful about what information I send in emails. I didn’t find the process of sending secure email very difficult, but it was certainly a hassle. When using PGP, I was annoyed that once I sent an encrypted message, there was no way for me to decrypt it (and read it) because it was encrypted with the recipient’s public key. S/MIME wasn’t much better because I had to use a mail client (Outlook) instead of my usual Gmail. I don’t plan on continuing to use secure email because it is not convenient and I have no need for extra security with my emails.

I worked with Ryan Stringham. Once I got my certificate and PGP key, I tested sending emails with each to myself. (I actually got two certificates and two PGP keys, one for each of my email accounts.) After I had successfully sent encrypted emails to myself and decrypted them, I sent emails back and forth with Ryan. The initial setup and testing was not too difficult. I had to look up a lot of things online, but I ran into very few problems.

**Grading:** (50 points max)

20/20 pts - Well written report within the length guidelines

20/20 pts – Successfully exchanged both PGP and S/MIME messages

* Exchange both signed and encrypted/signed messages

10/10 pts – Successfully exchange email with a fellow student

* Exchanged with Ryan Stringham

**50/50 Total**