Thomas Hart
CS 465
Project 10 – S/MIME and PGP

I did my secure email with Ben Grant (the TA). It took a couple tries for me to figure out. I didn't put together that we had to send unencrypted messages to exchange keys (PGP) or certificates (S/MIME) instead of the system doing a quick handshake type of operation independent from the user. Once I figured that out, I was able to send my key for PGP and imported Ben's. Then we were able to send encrypted emails. Same for S/MIME.

PGP

PGP stands for "Pretty Good Privacy" and is an older version of encrypted email using asymmetric encryption. It usually needs a plugin to work. I downloaded Mozilla Thunderbird, originally to figure out S/MIME, but there was an option to generate a PGP key right in the app. I generated a 4096 RSA key and used that to email with.

SUS: **(Bold numbers are my ratings)**

1. I think that I would like to use this system frequently. **2** – 1 = 1
2. I found the system unnecessarily complex. 5 – **1** = 4
3. I thought the system was easy to use. **4** – 1 = 3
4. I think that I would need the support of a technical person to be able to use this system. 5 – **1** = 4
5. I found the various functions in this system were well integrated. **4** – 1 = 3
6. I thought there was too much inconsistency in this system. 5 – **2** = 3
7. I would imagine that most people would learn to use this system very quickly. **4** – 1 = 3
8. I found the system very cumbersome to use. 5 – **1** = 4
9. I felt very confident using the system. **5** – 1 = 4
10. I needed to learn a lot of things before I could get going with this system. 5 – **2** = 3

1+4+3+4+3+3+3+4+4+3 = 33 32 * 2.5 = 80
Score out of 100: 80 **This one got about an 'A'**

S/MIME

S/MIME is a newer version of encrypted email that means "Secure/Multipurpose Internet Mail Extension". I used Actalis.com to get a free certificate for S/MIME. I had to verify my email, after which I was sent a private RSA key and an email with the PKCS12 credentials. Using Mozilla Thunderbird, I was able to set up the S/MIME certificate for digital signing and encryption using the private key and PKCS12 given to me. The private key is now able to decrypt messages and sign emails.

SUS: **(Bold numbers are my ratings)**

1. I think that I would like to use this system frequently. **2** – 1 = 1
2. I found the system unnecessarily complex. 5 – **2** = 3
3. I thought the system was easy to use. **5** – 2 = 3
4. I think that I would need the support of a technical person to be able to use this system. 5 – **1** = 4
5. I found the various functions in this system were well integrated. **4** – 1 = 3
6. I thought there was too much inconsistency in this system. 5 – **2** = 3

7. I would imagine that most people would learn to use this system very quickly. **3** – 1 = 2
8. I found the system very cumbersome to use. 5 – **1** = 4
9. I felt very confident using the system. **5** – 1 = 4
10. I needed to learn a lot of things before I could get going with this system. 5 – **3** = 2

1+3+3+4+3+3+2+4+4+2 = 29 29 * 2.5 = 72.5

Score out of 100: 72.5 **This one got a little over a 'C'**

Difficulties

Mozilla Thunderbird made the process easy, so I didn't have many hang ups with the app. When writing a message, there is a drop-down arrow that allows you to switch between PGP and S/MIME, so long as you have the keys set up correctly. This dropdown also lets you toggle encryption on or off so you can send unsecured emails or send keys/certificates. Mozilla Thunderbird had clear areas to import the PKCS12 and set up S/MIME once I had the necessary items from a third-party website.

The most difficult part was working with Actalis.com. I tried sending my main email address, but it didn't send a verification like it said it would. It finally worked after multiple tries. I then used the verification code to get my private key and PKCS12 credentials, but it seemed like the browser froze. I never saw the page that showed me the private key, but it still sent me the PKCS12 credentials. Without the private key, I had a useless setup with that email. I went through the same process with another email, having to send it multiple times to get a verification message. The browser seemed to freeze again, but after waiting a while, I fortunately got the private key. My guess is that it takes time to generate the keys, but the website should at least have a prompt indicating the user to wait. Otherwise, most people will think the browser has frozen and close out, having no way to get the private key again. Figuring out that website was my most time-consuming issue.

The next most time-consuming issue was getting confused when sending the emails as mentioned in the first paragraph of the report. I had to send an unencrypted email to exchange keys before sending the encrypted emails.

Another possible issue I noticed was user error. If a user forgets to check the "require encryption" option on Mozilla Thunderbird, the emails could be sent without security. They could also send using the wrong encryption technology. I don't believe there was a prompt when to notify the user of these things before sending out emails.

Will I Use Secure Email in the Future?

I don't think I would use this type of email frequently. It's not super difficult to use, especially after its all been set up, but I don't know who would go to the trouble of setting things up on their end. I'm not sending or receiving things that are confidential enough to worry about this either. I assume all my banking information on my banking sites are secure, and I don't use my email for things like that. If I started making a crazy amount of money that drew attention from strangers, I might use this to protect against email attacks. If I became famous, the same might be true. I don't think either of those situations will be true anytime soon, so this email is a bit extra in my opinion.