Scott Christensen
12/05/16
C.S. 465

Project #11: PGP and S/MIME

Explain the technical details of the keys and certificates you generated.

To be blunt, I didn't run into any technical problems when generating the keys or certificates the certificates. The ides I used and the guides I followed were pretty straight forward.

What email platforms and tools did you use?

In order to generate a PGP signed and encrypted emails, I used Mailvelope. It's a Google Chrome extension the allows one to send secure email between people on Gmail, provided that the two know each other's public keys. Upon downloading this tool, Tyler Holbrook and I send each other out public keys. We then sent one another a signed PGP email to one another and confirmed them. To do this, we had to enter our passwords for an additional layer of security and checked the sign button. Then, we sent one another a PGP email that was both signed and encrypted. The process was the same as the first, but we also had to checked the encrypt option.

Text version of the PGP encrypted and signed message.

-----BEGIN PGP MESSAGE-----

Version: Mailvelope v1.6.0
Comment: https://www.mailvelope.com

wcFMA2SElWYEgE7qARAArcXOcDSvpr14U9yXuMpf8ILuxR7jgLdgvpu7WN5y
/ZlE2iGAzZ+rIHxNT5CNOLhL7ceeDpmwdLkqYz8poPmp/F1cmhUT79URa1IX
Q/Y5tyevqxrgUc44wiv8zzpQrvprOofCW2LP0//u4vMxX26v+JhhBwDOMWtA
ZRkcpShMdf4DE+spoQ5CSxP+rdvi0JNYheBlDGhVN4+abaSjYj7i//wbGbAs
AVleKLCSfkD3KNb0qZy5l0WqCM05K0+18qx7ZUW/RwXrSTQl3sfjqyfBC2T3
RzjwpE2XB8eoUQOhfP9KSFFu08tICy646JcXOa64nj8JMXw1Eu4uvSZu2fKR
qceEEHLyWDGk2W4YUpScJfvTB0dFUDTWY/eZaKf/eMGnsQvawnhTJ6nvtzUd
VEZGb1+Nll+ygzd5AkgLsT65DTtJKdgJ9UJN3BLPEfJavPzI05lQGIFhIujY
2sM+CaVqaqXKUjzItvwrdLJ/h+NbkkNIgJi1W4egX0mvPz0hrp6ss55dKl62

```
WpGADSbzz1UC6SGgn47MaReiHcpH164JII3O2uNnJK++SPM7dcuexV5k5EEj
HOLrj05gnG5+F44YhEXwgCllBsqJLQ5LtPT/SJRGKdrWa/XKKHAaOWrbX9el
PLXpfCaouwyIltjrvaPwYE/KQLfCeSQzRcYpujgGkKDBwEwD//nogUwUOEUB
B/49DMpCqL99H46yFrrqGNAcBRO/QCrrOcWEylurkffWthj/tR/nT30ggO/P
8fzZg3TfLQc0HlWqpRzBdP5A356NT0F8dNts6V+gYy9Gr5jQjig2R9HCoCwL
Jw89z+oTajSb054dAjXuLPu5VoB9lH5hfZ4nOg0Ymif48ApIDLF02Ck1W5ib
5vEzoNxpghf8oYE36Sxd4I8QVhRtZMxL0PAzTEzvNqeNJ85oNi4SJKhku8QP
dvCMkCC1ImwaqyfD03Oxr9uQQpjRJdjaeveiumoJAAbhlJ01f1sh+kA0WcqC
u7hAJC6HXu3i1biZGERY6cE5DMXKfUOxEX61hQOu6gbl0sDKAdDwgdd/Y2Vk
2hyJMypEakMQ/B55De2x37L6bA583X5x8TJEKVWkQzyWGRR3cuiNXugzCbbG
C0C4S0DtcG8h2u+6jxCUtXEQEHwQskRSlp30pq2v76Ruv80ltScnH23Woz0z
pqUDp6bqDsV/Vcg6m+CUaBHO6Ms+e8mI4QaZODUyUjPRbf2M3zE27p01bCLm
7mp/Xw2uvNeQcqY4AElyPCiySNFPDRI6vKEx7OHJRsPI9kQT3yrwA3j+Llyp
ry1fHgDACSnvG9QQnke0ftW0o0iPnChO8Fug9QbOrYEGiz6+TC8OTjvMqAEm
0VEUueFkbFfKKKbz97SEShVj8sSLbT2FCNurNhPVvgyn/74Xyp1oax65PE/I
jmdqKQgKuZQu7o3/IoXp7q9SFftUMvcnAEwr4nKwpRKJvgdzELDPRSRCGA4d
5POE6RdV+e7SirHQbSWch62+RqUlgCviwBvRkY9QcCEoiM/jerPCahpFUg+T
XFSp05Y7E+XdfAoFRZxb1JpKTRbuz9b3UQ==
=qmoz
-----END PGP MESSAGE-----
```

Encrypted message: You are good for nothing, you loser.

In order to generate a S/MIME signed and encrypted emails, I used Fossa Guard. It to is a Google Chrome extension the allows one to send secure email between people on Gmail. we did not, however, have to send each other our public keys. Fossa also had me verify a shared secret key in a confirmation email for an additional layer of security. This I can assume is to be included into the certificate chain. With Tyler Holbrook, we sent one another a signed S/MIME email to one another and confirmed them. To do this, we had to enter our passwords for an additional layer of security and checked the sign button. Then, we sent one another a S/MIME email that was both signed and encrypted. The process was the same as the first, but we instead checked the encrypt option, as signing was covered by Fossa's certificate chain.

What is the difference between PGP and S/MIME?

S/Mime uses certificate chains for verification. PGP, however, does not.

Have you ever sent secure email in the past? Why or why not?

Up until now I have never used any such for of secure email service. The reason why is I simple never felt I had to as I have been under the assumption that Gmail, Facebook Messager, and the other services I use were secure enough. Also, I've never had an work or school transaction that was deemed so confidential that a secure email service was deemed necessary.

Now that you know about secure email technology, will you continue using it in the future? Why or why not?

To be honest, I don't see myself using FOSSA GUARD or any type of S/MIME any time soon, if ever. There was just a large number of steps needed to implement it and it would require a lot of work to get other people I have regular correspondence with to use it as well. I could, however, potentially see myself using Mailvelope or another form of PGP secure email in the future. The set up for it was relatively simple and all that me and others would need to send to one another is our public keys, which isn't detrimental the be sharing across the wire since it's our public key we're talking about.

Self-Grading:

20 pts - Well written report within the length guidelines

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

•10 pts – Successfully exchange secure email (either PGP or S/MIME) with a fellow student

Score: 50/50