Christopher LaJon Morgan
CS465: Kent Seamsons
Project #6 Report

Summery of Experiment

Well this was painful. You think that this would be so much easier. This process totally fails the "teach it to your mom" principle. S/MIME is a secure multipurpose internet mail extension. It is a standard for public key encryption and signing of digital mail. This standard can leverage the existing PKI. I set up a certificate with both COMODO and Startcom. Ideally my certificate would be signed by these companies and then these CA's would be trusted in my receiving clients mail clients or computers. This would allow anyone receiving signed mail from me to instantly know it came from me without further commotion. Otherwise, those who receive mail from me would need to trust my certificate the first time and hope it was authentic the first time.

PGP and S/MIME Sort of Explained

PGP works a little bit differently. It is more of a smaller private standard/encryption algorithm. PGP works on an individual trust level. While there are modes for CA's and looking up key information, PGP was originally intended for more one-to-one interactions. In other words, two people either initially trust one another certificates or exchange keys, and then they are good to go.

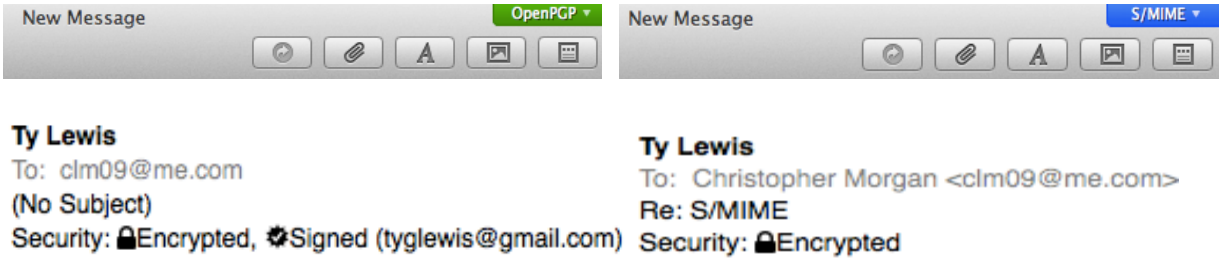
S/MIME was convoluted and frustrating on my mac. It was dealing with the whole CA, ensuring the certificate made it into my keychain and then knowing I needed to restart my mail.app. Once that was all complete, there was still a red cross on my certificate indicating that it was signed by an unknown authority, even though I went through COMODO and Startcom, not sure what this means or how to fix it. PGP on the other hand was seamless for my mac. It was a simple installation (GPG KeyChainAccess), simple key gen, and simple send. It was much nicer than S/MIME.

Process Difficulties / Hard to Use

The most interesting revelation to me was my simple desire as a user. Even being a computer science major, I just wanted to click a sign button and have it work, I just wanted to click a encrypt button and have it work. My biggest disconnect was what was required to sign a document and what was required to send one. Even following RSA and knowing the steps I still got thrown, while on my mac. I just thought it should be easier and more automatic. However, I learned that I need a certificate (RSA key pair) in order to sign a document. My mail client needs access to this (keychain) and anyone wishing to validate my signature (CA). Then to encrypt a document, it is a separate encryption to each recipient (ugly). To do this I need their certificate (RSA public key). I receive this by just having them sign a document and having them send it to me. (Three options here, look up directly from the CA, or validate what they send, or just trust it the first time.)

This just shows me why I have never sent secure email in the past. I really had to know what was going on, need additional software, and it required a third party. This was way too much to expect from the "mom" principle.

Proof Of Work



~I initialed each of these conversations with encrypted PGP and S/MIME messages, and received the following back. The proof is in mail.app's lock symbol. This shows the messages were successfully encrypted.

Who I Worked With

I worked with Ty Lewis for this project. It was initially difficult to figure out exactly how to connect the two certificates. However, once I found a nifty tutorial everything became clear and we were able to get it going. However, we ended up just trusting each other's certificates the first time and not having them validated via a CA. This was a little disappointing.

Questions

My biggest question is WHY? Why haven't we come up with a better, easier, more automated way of securing communication? Is it just the email world that is behind, where browser communication is more up to date? I wonder why this is the case, if it is the case? Is there a business market here?

Grading: 50/50

- 20/20 pts - Well written report within the length guidelines
- 20/20 pts – Successfully exchanged both PGP and S/MIME messages
- 10/10 pts – Successfully exchange email with a fellow student
- 25/25 pts – If you are unable to send secure email after **2 hours of effort**, you may describe in detail your experience and what problems you encountered