MEG: The Email Mobile Encryption Gateway

Gregory Rehm, Michael Thompson, Brad Busenius, and Jennifer Fowler

University of California, Davis, {Argonne National Laboratory grehm@ucdavis.edu
{thompsonm,bbusenius,jfowler}@anl.gov

May 18, 2016

1 Abstract

Email cryptography has long been considered a problem that was too hard to practically solve. MEG, or the Mobile Encryption Gateway aims to solve many of the problems associated with email encryption by making it both practical, easy, and flexible to perform. MEG will perform automatic decryption and encryption of all emails using PGP allowing users to not worry about the internal workings of how encryption works. MEG is meant to be email client agnostic enabling users to use any mail service they desire to send messages. Most importantly MEG is end-to-end encrypted ensuring that the users information stays private only to them. As a result we hope that MEG will finally provide users with the solution they need to encrypt their emails as easily as they send unencrypted mail.

2 Introduction

Email cryptography has long been considered a problem that was too hard to practically solve. The reigning standard of email encryption is S/MIME and has the ability to perform end to end encryption for email. However S/MIME has the downside of also being difficult to set up by an average user. One must also contact a Certificate Authority (CA) for an S/MIME certificate which requires some delay in time and a payment. Other paid email services offer to simplify this process but often their code is unauditable and is commonly riddled with security vulnerabilities.

If we want to remove the centralized CA from the encryption process then our only other alternative is to use PGP. PGP is decentralized and operates over web of trust. Assuming that a user has properly performed their web of trust PGP is just as secure as S/MIME and is able to validate the identity of the participants in a communication. Despite advantages of being decentralized, PGP is notoriously difficult to use. In a famous study name "Why Johnny Can't Encrypt" researchers found that most study participants couldn't even encrypt their emails using GUI tools for simplifying PGP actions. The few that were able to encrypt their communications were prone to displaying their private key in plaintext, defeating the entire purpose of encryption. Followup studies with improved PGP GUI tools have had no more success with study partipantsthan the original trial. Once again there exist paid services to automate PGP but they too suffer from lack of end to end encryption and have unauditable code. There exist other free, open source methods of email encryption but they require a user to use a special email client and disallow use of clients that the user has grown accustomed to.

MEG aims to address all of the issues with email encryption mentioned above. We use PGP in MEG to avoid the centralized nature and cost associated with S/MIME certificates. To avoid the usability problems

associated with PGP MEG aims to handle everything for the user automatically. Key creation, encryption, decryption, the signing of messages and keys are all handled by the MEG app. MEG is completely end to end encrypted and even MEG systems will have no ability to read user communications so user data stays private exclusively to the user. MEG is email client agnostic. We can link with any other email provider such as GMail or Yahoo Mail. This way the user does not have to choose completely different mail clients just to get encrypted mail. MEG is also free and completely open source as we believe having our code open to audit only makes the service more secure and private.