Matthew Austin

Server Security

Tian Guanyu

11 December 2018

Simple and Easy-to-Use Secure Email

In the article “Private Webmail 2.0: Simple and Easy-to-Use Secure Email” by the author’s Scott Ruoti, Jeff Andersen, Travis Hendershot, Daniel Zappala, Kent Seamons go over several easy was to make email secure. The authors introduce Private Webmail 2.0 (Pwm 2.0) as an improvement upon the run of the mill email’s usability and security. With Pwm 2.0, users are able to send secure encrypted emails with a usability, make few mistakes, and have a great understanding of email message protection.

Regular emails is becoming more secure with the enabling of encryption and authentication. The weakness that those things have is incorrect configuration, which makes them open to attacks. Email in transit has proven to be able to be secure but email at rest is still insecure. Therefore, service providers are able to scan and read email messages. End-to-end encryption is much stronger as the service provider will not be able to read the messages only the intended recipient. The only problem with that mechanism is that its usability is extremely low for an average email user. With Pwm 2.0 the user can have the best of both worlds by having a email that is secure and have a easily usable interface. In their article, through studies and observations of users using Pwm 2.0 they were able to assess whether or not Pwm 2.0 system is a definite improvement that finally fills the gap between security and usability.

For the study they made modifications the interface to make it more usable to the average user. The Pwm 2.0 scored a 80.0 on the System Usability Scale. The End-to-end auto encryption a state of the art mechanism that has a miniscule flaws, they only weakness to it is human error. Therefore the threat model of the Pwm 2.0 is mostly user based. The threat model goes as follows: User, Webmail Provider, IBE Key server, and Adversary.

To decrease human error the authors improved the interface and information on Pwm 2.0. They delayed encryption, but showing a visible representation of the email being encrypted to give the user peace of mind that the email is actually being encrypted. Composite Interface that gives users prompts or makes buttons more noticeable, so that mistakes are mitigated. Tutorials that are within Pwm 2.0 as well as other videos and information on how to use it. Gave the user the option for automatic and manual encryption. After the study, majority of the users said that Pwm 2.0 system was usable and was able to complete tasks within an efficient time. Out of the 306 tested participants only two percent of the users made mistakes. Ninety-two percent of the users stated that the tutorials were helpful and that they were able to easy instruct new users. The users preferred delayed encryption of manual because they thought that the time between hitting the send button and the message actually being sent was to quick and therefore untrustworthy. Overall throughout their studies and assessments they conclude that their modifications to the Pwm 2.0 extremely improved user usability and trust.