



Kaspersky says CoinVault and Bitcryptor done



U.S. Air Force adds extra pay for cyberspace specialists



Sponsored Editorial Content

Identifying
data
security
vulnerabilities

November 2015 Issue

Editorial

[Pushing past shock and yawn](#)

Threat of the month

[Threat of the Month, November 2015](#)[Subscribe](#)

Next Article in News

[Archive](#)

Tom Reeve



November 02, 2015

Cyber products don't belong on munitions list, State Dept. DTAG says

Modern PGP is unusable according to academic study

Share this article:

- facebook
- twitter
- linkedin
- google
- Comments
- Email
- Print

Modern PGP clients such as Mailvelope – designed to support encrypted email communications – are so difficult to use that few individuals are able to configure and use them.

In a laboratory study of 20 individuals, grouped into 10 pairs, the researchers from Brigham Young University in the US found that only one pair of users were able to set up Mailvelope to communicate securely with each other.

The [study](#), entitled, “Why Johnny still can't Encrypt: Evaluating the usability of a modern PGP client” was produced by Scott Ruoti, Jeff Andersen, Daniel Zappala and Kent Seamons.

The issue was studied 15 years ago and then again nine years ago and in both cases it was found to be anything but user-friendly.

Even the creator of [PGP](#) doesn't use PGP because it [doesn't work with his MacBook](#).

The researchers chose to use Mailvelope because it was the only secure email system promoted by the Electronic Frontier Foundation's secure message score card that integrates with webmail providers, which the researchers felt was an important feature for many users. They also noted that it received 4.6 out of five stars from 242 users on the Chrome Web Store and that in their own user testing it was about as usable as alternatives such as GPG Tools, Enigmail and Google's End-to-End Encryption.

All of the participants were chosen partly on the basis of having a Gmail account.

Study participants were required to sit in separate rooms and communicate with their partner only via email. They were given an hour to complete a series of tasks which included installing the software, generating GPG keys and sending a secret message to each other.



Modern PGP clients such as Mailvelope – designed to support encrypted email communications – are so difficult to use that few individuals are able to configure and use them.

Of the ten pairs, only one was successful – but as the researchers noted, the successful pair was unique in having a participant who had previously studied public key cryptography.

The researchers recommended that Mailvelope should have some integrated tutorials to help new users through the setup process and it should include an "approachable description" of public key cryptography to help users manage their own keys.

A weakness of mail encryption programs is the issue of communicating with new users who have not installed encrypted email software. The researchers recommended that PGP tools issue automatically generated emails to unknown recipients to prompt them to install the software and generate a public key to share with the sender. And they said that non-PGP users need help when receiving encrypted emails.


Mistakes made by participants included encrypting message's using the sender's public key, adding their secret message to the PGP block itself in the PGP compose window and generating a key pair with their friend's information and then using that public key to encrypt their message.

In one case, the researchers noted wryly, a participant sent his private key and keyring password to his friend in a desperate attempt to help him decrypt the message.

This article originally appeared on SC Magazine UK.

0

Share this article:

- [facebook](#)
- [twitter](#)
- [linkedin](#)
- [google](#)
-  [Comments](#)
- [Email](#)
- [Print](#)

You must be a registered member of SC Magazine to post a comment.

[Click here to login](#) | [Click here to register](#)

Sponsored Links

[SANS Cyber Defense Initiative \(CDI\) 2015 – DC - December 12 – 19: 30+ Information Security Courses taught by leading Practitioners – Save \\$4200 thru Nov 11th.](#)