Dead on Arrival: Recovering from Fatal Flaws in Email Encryption Tools

Juan Ramón Ponce Mauriés, Kat Krol*, Simon Parkin,
Ruba Abu-Salma, and M. Angela Sasse

University College London

*University of Cambridge

LASER 2017, Arlington, VA **19/10/2017**

Introduction

- Lack of usability hinders both the adoption and actual security of email encryption.
- "Why Johnny Can't Encrypt" (Test of Time Award, 2015).

Research Question

- 18 years after the Johnny paper, how easy is it to configure and use an encrypted email client?
- Enigmail is a stand-alone extension to the Thunderbird email client.
- Mailvelope is an integrated solution, as either a Chrome extension or a Firefox add-on.

Method

We conducted a three-stage study:

- Stage 1: Lab-based setup
- Stage 2: Home use of encrypted email
- Stage 3: Lab-based feedback session

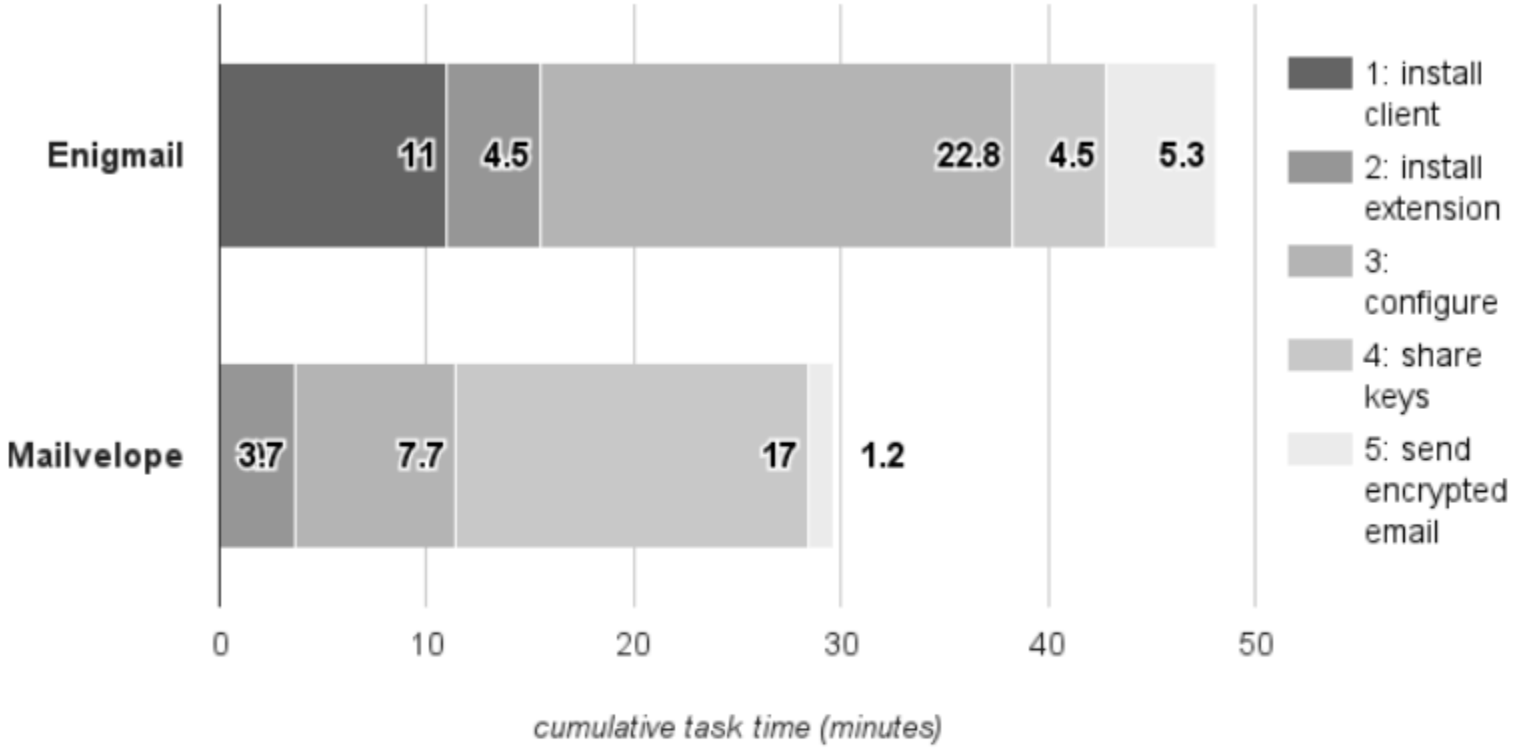
The experimenter had to act as 'technical support'.

Participants

- We recruited participants through a research participant pool at University College London (UCL).
- Final sample:
  - Enigmail group: x4: 2 male and 2 female participants; mean age: 32.7.
  - Mailvelope group: x6: 2 male and 4 female participants; mean age: 39.6.

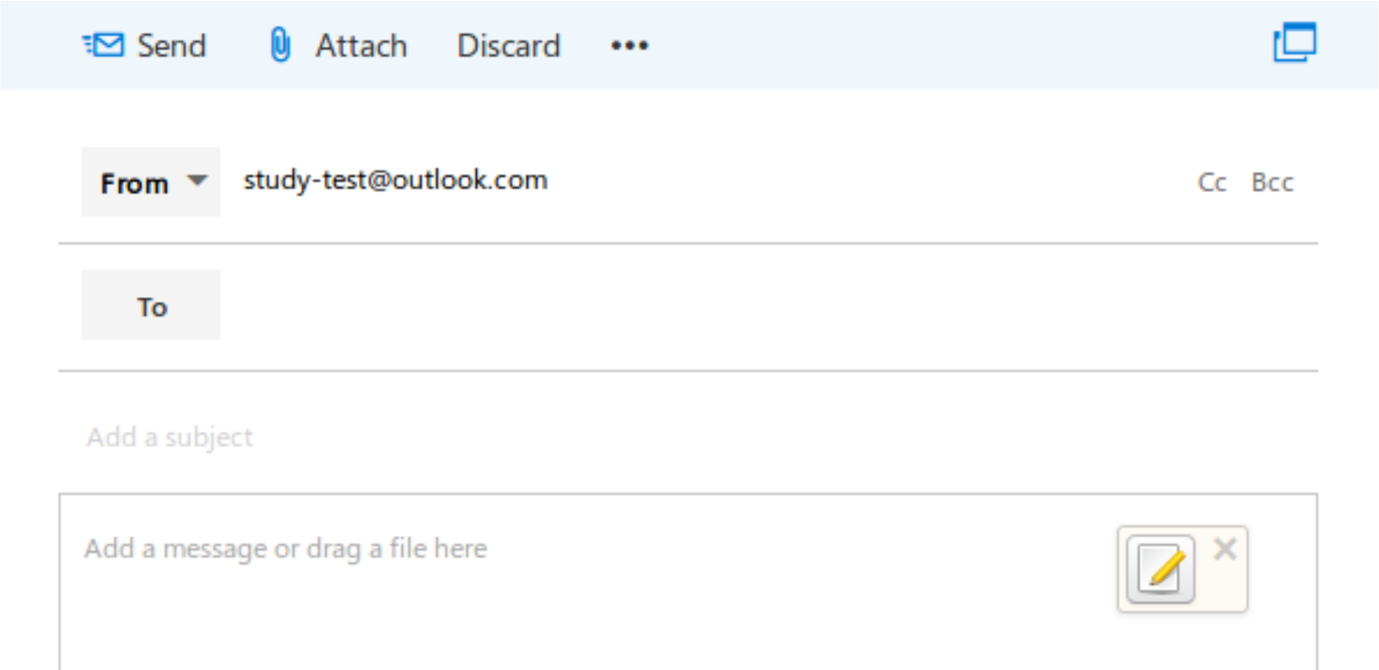
Results: Task Completion Time (1)

- Installation and setup were time consuming



Results: Installation and Configuration (2)

- The option to encrypt was not obvious.



From study-test@outlook.com

Results: Installation and Configuration (3)

- The tools did not speak the language of the users: "*When you get all of the boxes I'm like "Oh my god! Which one do I do, this one or this one?" And that's where I start to struggle because I don't understand the technical language.*" (P4-E)

Results: Key Exchange (4)

- Participants in both groups were unable to share public keys.

Results: Lack of Utility Is a Major Obstacle (5)

- Participants were reluctant to adopt the tools for every day emails:
  - Lack of utility
  - Small user base (network effects)

Discussion

Methodological implications:

- Leveraging technical expertise of the researcher to explore design obstacles.
- How many people can naturally learn a new technology by consulting a known 'IT person'?
- Are lab-based studies artificially pushing participants towards task completion?

Recommendations

- Both tools had bugs: Effective user interaction with encryption tools still lies in following basic interface design principles to fix usability issues.
- Guided habituation of encryption tools can overcome hurdles in the comprehension of encryption.