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

Juan Ramón Ponce Mauriés[1], *Kat Krol*[2,‡],
Simon Parkin[1], *Ruba Abu-Salma*[1], *and M. Angela Sasse*[1]
[1] *University College London,*
{*juan.mauries.15, s.parkin, ruba.abu-salma.13, a.sasse*}*@ucl.ac.uk*
[2] *University of Cambridge, kat.krol@cl.cam.ac.uk*

Abstract

Background. Since Whitten and Tygar's seminal study of PGP 5.0 in 1999, there have been continuing efforts to produce email encryption tools for adoption by a wider user base, where these efforts vary in how well they consider the usability and utility needs of prospective users.
Aim. We conducted a study aiming to assess the user experience of two open-source encryption software tools – Enigmail and Mailvelope.
Method. We carried out a three-part user study (installation, home use, and debrief) with two groups of users using either Enigmail or Mailvelope. Users had access to help during installation (installation guide and experimenter with domain-specific knowledge), and were set a primary task of organising a mock flash mob using encrypted emails in the course of a week.
Results. Participants struggled to install the tools – they would not have been able to complete installation without help. Even with help, setup time was around 40 minutes. Participants using Mailvelope failed to encrypt their initial emails due to usability problems. Participants said they were unlikely to continue using the tools after the study, indicating that their creators must also consider utility.
Conclusions. Through our mixed study approach, we conclude that Mailvelope and Enigmail had too many software quality and usability issues to be adopted by mainstream users. Methodologically, the study made us rethink the role of the experimenter as that of a helper assisting novice users with setting up a demanding technology.

1 Introduction

Usability issues have been regularly cited as a barrier to the adoption of email encryption [23] since Whitten and Tygar's seminal paper "Why Johnny Can't Encrypt" [24]. The paper received the USENIX Security Test of Time Award in 2015, which might be interpreted to mean that this state of affairs persists. Recent research [17] reports that users are increasingly learning about security threats from various sources, such that they may be more receptive to adopting email encryption tools than ever before. There has been increasing effort to provide end-to-end encryption and eliminate barriers to adoption, such as key distribution [24, 23, 20, 6].

The motivation behind the study described here was to observe and analyse novice users' first encounter with such tools: 18 years after Johnny, how easy is it to configure and use an encrypted email client?

We know that users prefer to use email encryption tools which integrate with email systems they are already using [19]. Thus, we chose to study two current open-source, integrated PGP email encryption tools – Enigmail and Mailvelope. We observed users across three stages of activity, within a group-based study: an installation group session, home use over a week with assigned group communication tasks, and a debrief group session. Ten participants completed the study, divided into two groups of four and six participants using Enigmail and Mailvelope respectively. The approach was validated by findings showing that barriers were encountered across all phases of the study for both tools, in many places requiring the assistance of a knowledgeable experimenter to complete the various stages. This raises questions about the role of a knowledgeable expert in the process of learning to use a complex piece of software and overcoming barriers to effective use, where the experimenter may need to take on this duty.

2 Background

Lack of usability has been demonstrated to hamper both the adoption and actual security of email encryption. Whitten and Tygar [24] explored whether PGP 5.0 could

[‡]The study was conducted while the author was at University College London (UCL).

be used by the general public to effectively secure emails. The authors employed two evaluation methods: (1) a hybrid of a cognitive walk-through and heuristic evaluation, and (2) a lab-based user study. Problems were identified in the user interface design which introduced security risks – most lab participants were incapable of using the PGP software securely. It was concluded that making security usable requires the development of domain-specific user interface design principles and techniques.

Garfinkel and Miller [10] performed a user study of the CoPilot email client and Key Continuity Management (KCM), where KCM automates key generation, key management, and message-signing. The authors concluded that KCM and CoPilot improved usability by managing encryption tasks on behalf of users. In contrast, Ruoti et al. [20] suggested that designers should focus on manual encryption to provide transparency and engender trust in encrypted tools. Subsequent studies (e.g., [11, 9, 21, 23]) have followed the findings of Whitten and Tygar's original work, for instance, through studies of secure communications in two-way radios [7], and opportunistic email encryption [8].

Recent studies of encryption have explored socio-technical factors. Gaw et al. [12] interviewed employees in an organisation, finding alongside usability a range of social factors influence adoption of encrypted email, such as the perceived importance of specific messages and the perceived line between secrecy and paranoia. Renaud et al. [18] explored adoption factors across several dimensions, such as awareness of privacy risks and motivation to protect against violation of emails. User interviews captured mental models of email security, identifying adoption challenges, such as incomplete threat models and lack of understanding of email architecture. Ruoti et al. [19] conducted lab-based studies with pairs of novices cooperating to send an encrypted email with a range of email tools, finding that lack of transparency impacted trust, and that the availability of effective tutorials was critical.

Here, we present a novel approach to studying use of encrypted email tools – a combination of lab-based setup with groups of participants using their own computers, home use of encrypted email to perform a shared task, and debrief in a lab setting to measure perception of the tools. This allows us to explore where barriers can emerge during the process of adopting and acclimatising to encrypted email.

3 Method

Our study aimed to compare characteristics of Enigmail and Mailvelope, to understand the facilitators and obstacles behind adoption of encrypted email solutions. We chose Mailvelope and Enigmail as they are end-to-end encrypted, open-source, and available free of charge. While Enigmail is a stand-alone extension to the Thunderbird email client, Mailvelope is an integrated solution, as either a Chrome extension or Firefox add-on.

3.1 Design

We conducted a three-part study with one group of participants installing and using Enigmail alongside Thunderbird, while the other group using Mailvelope. Participants used their own laptops during the study, as follows:

- **Lab-based setup.** Participants were interviewed about their email-related habits, and asked to install, configure, and begin using their assigned tool.
- **Home use of encrypted email.** Participants were given a task to complete outside of the lab setting, organising a mock flash mob campaign via encrypted email over one week. Participants sent emails to each other to agree on the location and music for the mock event, and to confirm the location with the experimenter. They also sent emails to a new member of the group (another researcher).
- **Lab-based feedback session.** Participants discussed their experience of Enigmail or Mailvelope.

Participants were asked to bring their own laptops to the study, to preserve ecological validity [13, 14]. They were provided with printed copies of the installation guides for either Thunderbird and Enigmail or Mailvelope. Crucially, the experimenter was available to assist participants – rather than presume to lead them – during the setup phase, and was contactable during the home-use phase. Participants were asked to note when they completed specific tasks on another sheet: (1) installing Thunderbird (only for the Enigmail group), (2) installing the Enigmail extension for Thunderbird *or* the Mailvelope extension on Firefox or Chrome, (3) configuring the extension (generating a private and public key pair), (4) sharing public keys with other group members, and (5) sending an encrypted email to the study coordinator.

At the lab-based debrief session, participants completed System Usability Scale (SUS) [5] forms for both Enigmail and Mailvelope. The SUS questionnaire consists of ten statements, where users indicate how strongly they agree with each statement on a five-point Likert scale. At the end of the final session, participants received £30 for their participation.

3.2 Participants

Participants were recruited through a research participant pool at University College London. It is a participant

pool where members of the general public can register and sign up for research studies. Prospective participants completed a pre-screening questionnaire to indicate occupation, age, gender, whether they had previously used an email client, and if they had any experience with email encryption tools.

Overall, 52 individuals completed the pre-screening questionnaire. Two groups were formed, with six participants each, so as to be resilient to unanticipated no-shows. Those with a background in computer science were excluded to favour non-technical users. Two of the invited Enigmail participants did not attend on the day of the lab-based setup session. The final sample was as follows: the Enigmail group had four participants, two females and two males. Their mean age was 32.7 ($SD = 20.2$, range: 23–45). The Mailvelope group consisted of four females and two males, with a mean age of 39.6 ($SD = 9.1$, range: 24–76).

3.3 Procedure

Upon arrival, participants were asked to read the information sheet and sign a consent form. The first group was tasked with installing Mozilla Thunderbird and the encryption extension Enigmail. The second group was assigned the browser extension Mailvelope that works with Firefox or Chrome web browsers. An explanation of the tasks to be completed was given, but users were not briefed on the specific goal of the study until the end of the final session one week later.

3.4 Role of the experimenter

We initially conceived the role of the experimenter to be that of a session facilitator, asking participants about their experiences with the tools, and eliciting their mental models of how encryption works. As Enigmail and Mailvelope are targeted towards mainstream users, we provided participants with official setup guides published by the developers of the tools.

At the design stage of the study, we did not envisage the role of the experimenter to be an instructor telling participants how to set up the tools. However, the pilot session we conducted before the main study sessions made us change this element of the study design. In the pilot study, we used a convenience sample consisting of colleagues who mostly had a computer science background. They were asked to perform the exact same tasks as our participants. The pilot session of the setup lab-session took in excess of 1.5 hours, where despite the sessions being full of discussion about the instructions, the pilot participants struggled with the installation process to such a degree that it was necessary for the experimenter, a domain-knowledge expert, to guide them through the process to successful installation and use. As a result, the experimenter was briefed to not actively lead participants through the setup steps, but to respond to requests for help from participants if they arose during the session(s).

3.5 Research ethics

The study was conducted after having been approved by UCL's Research Ethics Committee (approval number: 9423/001). The research was also registered with the UK Data Protection Act 1998 (Z6364106/2016/07/11). We did not collect any personally identifiable information. We temporarily stored demographics and contact detail information to be able to select participants and invite them to the study. This information and the recordings made during the group sessions were securely disposed of at the end of the study.

4 Results

4.1 Task completion and times

The average task completion times are shown in Figure 1. The average completion time for all tasks was 48.1 minutes for the Enigmail group, and 40.4 minutes for the Mailvelope group. Task times are self-reported, so values may not be precisely accurate, but are indicative of the time it took for each group to complete the tasks assigned to them. The majority of participants in both groups reached and completed the final task. However, it can be seen that even with (minimal) assistance from the knowledgeable experimenter it can take novices in the region of half an hour to set up and test encrypted email. Average task times for Enigmail are shown alongside notable participant quotes in Figure 3, and for Mailvelope in Figure 4 (see Appendix).

All Enigmail participants completed the four mock campaign tasks successfully. In the Mailvelope group, one out of six participants was unable to complete the third and fourth setup task (e.g., importing a new public key from a new participant and sending encrypted email to this person). This participant, P4-M,[1] downloaded the attachment correctly but imported an incomplete block of text as part of the public key. Participant P2-M was unable to complete task four due to a broken laptop.

4.1.1 SUS

A SUS score can range from 0 (poor) to 100 (excellent). The average score for Enigmail was 63.1 (range: 57.5–77.5, $SD = 9.7$), and for Mailvelope was 50.8 (range:

[1] Participants are referred to as P*X*-E for those in the Enigmail group, and P*X*-M in the Mailvelope group.

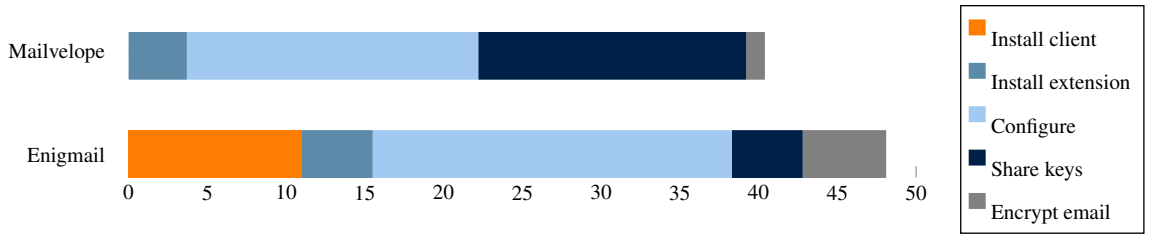

Figure 1: Task times in minutes for Enigmail and Mailvelope.

27.5–70, $SD = 19.4$). This result means that Enigmail achieved "Good Usability", whereas Mailvelope achieved "OK Usability". An unpaired t-test showed that these differences were not statistically significant ($p = 0.28$), possibly due to a small sample size.

4.2 Qualitative results

The audio-recordings of the sessions were transcribed, and the transcripts were analysed using thematic analysis [4]. The analysis identified the following themes.

4.2.1 Sharing sensitive information

Participants generally considered personally identifying information to be sensitive (e.g., when shopping online or entering passport details for flights). They felt that disclosure of this information could expose them to the risk of identity theft or leakage of, for instance, online banking details.

All participants expressed that they had needed to share sensitive information at some point. Diverse means were mentioned; two participants had shared sensitive information via regular email, a further two via the telephone, and three via messaging applications such as WhatsApp or Facebook Messenger. Two participants stressed that they, as users, have to trust the service provider, or otherwise not use the service at all:

> *"I mean... you basically have to put your trust in it, otherwise you just don't use the email or you don't use the messenger service, you know?"* (P5-M)

Participants spoke of unintended recipients who might access their emails. All Mailvelope participants agreed with P4-M's sentiment: *"Well, I think [...] Gmail, it's checked every time we use it and all of our data is known to them."* Participant P3-M argued that their emails would not be a target for malicious parties: *"We are not... important enough for somebody to hack my personal email... we are not Hillary Clinton!"*

4.2.2 Encryption

All participants had previously heard of "encryption", but did not report having used a dedicated email encryption tool. Participant P4-E had, however, previously tried to install Mailvelope a few months prior to the study:

> *"I tried to install Mailvelope, yeah, but only got half-way through 'cause I really couldn't understand how to do the rest of it..."*

Participant P2-E noted having *"seen people use PGP and stuff"* without having used it personally, despite having *"technical friends"* who encrypt their emails. In response, P3-M explained the mechanism behind encryption as follows:

> *"It kind of converts the entire message into some kind of codes and then you send to the recipient in the form of code and then something happens... I don't know what happens..."*

There was a consensus amongst participants that encryption did something to the original message that prevented an unintended person from reading the message.

Participants also commented on recent news, airing concerns about anonymous browsing and government involvement. P1-E commented: *"Recently the government was trying to block... something they were trying, they didn't want the encryption because obviously they want access to your emails..."* They further elaborated that using encryption might draw attention: *"If all our communications are being monitored, wouldn't having encryption make you a suspect of some suspicious activity instead?"*

4.2.3 Installation and configuration

Participants from both groups agreed that the installation of the extensions was straightforward (including Thunderbird for the Enigmail group). For P1-M, installing the Mailvelope extension was perhaps too seamless:

> *"There was no way of knowing if we had done it or not. It would have been good if there'd*

been a bar across the top saying or showing how much of it was installed, or saying it was installed because I wasn't absolutely sure if it was finished…"

All participants agreed that configuration of the extensions was complicated. For Enigmail, the experimenter had to intervene because there was a bug in the setup wizard. When the setup wizard tried to download the GnuPG component required by Enigmail to do the cryptographic work, a progress bar was shown with the progress of this download. However, the download and installation did not actually start, and no error message or warning message was displayed.

The Mailvelope group complained that after installation, the steps required to configure the extension were unclear. They found locating the button to open the options menu was frustrating since they did not know what to look for. Participant P2-M commented: *"It was a bit complex, I had to ask many times, it was complicated…"* Enigmail users similarly complained that the process was convoluted, difficult to follow, and that it was hard to completely understand all available options, and then decide which one to choose. P4-E elaborated:

"… 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."

All participants completed the steps up until key exchange without incident. Those in the Mailvelope group were frustrated at being unable to share public keys. The key-generation setup wizard had an option to automatically upload a public key to Mailvelope's key servers, but this process did not work – even when the option was selected, the keys were not uploaded. Participants instead had to copy and paste the key or download it as a file to manually share it with others.

Experimenter intervention was necessary to explain the manual process needed to effectively exchange keys. P4-M was evidently frustrated: *"It's too complicated, it's too much!"* All participants agreed that this step was the worst, as it was unclear what to do intuitively or from the official guide. P5-M: *"Finding the keys, importing them, that was pretty difficult!"*. Participants' mental models of encryption did not relate the use of two keys:

"I didn't understand the need for keys, this is all new to me… I can use email, but I don't know why we need a key… so I would have given up, I think!" (P1-M)

4.2.4 Thunderbird and Enigmail

The Enigmail group generally did not like the encryption experience. When asked if any changes would make the tool better, the focus was on the setup process. P3-E saw too many steps in the installation and configuration process:

"I was thinking it should be built into Thunderbird, just using one piece of software, so just basically the install is like: "Where [do] you want to install it?" and then: "Do you need to set up keys?" or whatever."

P4-E made comparisons to the use of other applications:

"It needs to be literally as easy as installing some of the other apps, you know, that you can just download and have encryption that way."

When considering the design of the Thunderbird interface, P1-E commented that:

"I didn't really like the interface of Thunderbird, I thought it was a little bit more clunky, umm, it had very old-school interface."

Participant P4-E said that even though she liked the idea of encryption, the whole process of getting it to work was too complicated. She attributed it to her age, after hearing about encryption, she had genuine privacy concerns:

"Because it's there I would use it, but It's too complicated, maybe because I'm 45 and maybe it's the younger generation of people who put their whole lives on the Internet, you know, and privacy, the idea of privacy is changing… and I… even though I haven't got any sensitive information really, it's just about protecting my own privacy. It's just like getting letters in the post, you wouldn't necessarily just leave your letters laying around for people to read…"

P4-E explained usability was necessary for adoption by all users:

"If I say to some of my friends or even my elderly parents: "Hey! That's encrypted e-mail!", it's just not going to happen and it's not like I really understand it. It needs to be literally as easy as installing some of the other apps, you know, that you can just download and have encryption that way. For me, it has to get to that point really for general consumption…"

Participants commented that once the applications had been configured, the interface in fact simplified the use of encrypted email as well as public key sharing. They all noticed the warning messages when an email was going to be sent unencrypted. They also said that sharing their public key was easy and convenient because they only had to click one button.

All those in the Enigmail group did, however, say that they would likely remove it from their laptops after the study. P3-E explained:

> *"I'll reinstall it if I have specific reasons like someone sends me an encoded message or I need to send someone something, but it's taking a lot of space."*

4.2.5 Mailvelope

Once through the process of exchanging keys, Mailvelope users felt that the rest was easy to do. P3-M and P2-M commented, respectively, that *"I think it was fairly simple to use after that and yeah!... I can see myself using this with people that I email often..."* and that *"it was kind of cool to learn that it was that easy, to be able to encrypt an email... I didn't realise that you could just add something to your Gmail... you know, an add-on and do it that easily..."*

All participants felt confident using the system after a few days completing tasks, and wanted to share their comments. P1-M: *"I didn't know that just adding an extension you could do all that... encrypting and decrypting..."* P6-M struggled to complete tasks for the first few days of home use, having forgotten the passphrase for their private key. They were upset about missing the tasks:

> *"So I tried all the password permutations, so I was so confused... I still wonder why it is... I used something easy to remember... After several days, I said "Oh my goodness!" I had to tell you I had forgotten..."*

Once asked to repeat the process of generating new keys, they were excited to exchange the new public key, where *"that was one thing that I managed to do and I feel quite proud about that!"*

There were some comments as to how to improve Mailvelope's interface and the process of encrypting emails. Three participants reported that the button to activate encryption was not obvious, leaving them prone to sending unencrypted email (see Figure 2 for a screenshot depicting the encryption button). P3-M explained:

> *"Perhaps something more prominent than just that tiny button, because I did it a couple of times, I was writing the text until I realised."*

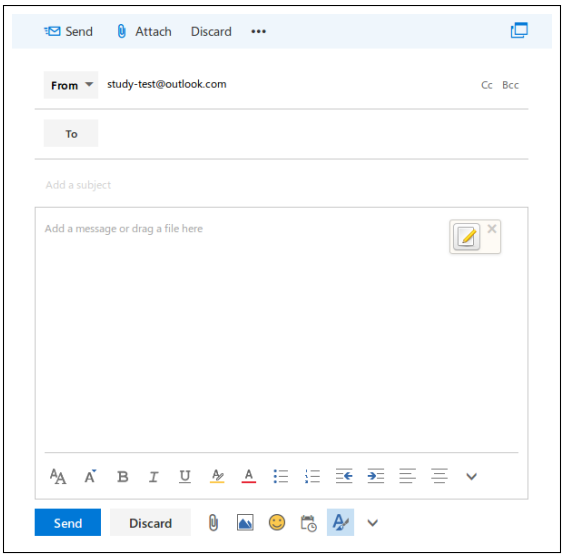

Figure 2: A screenshot of the user interface for Mailvelope displaying the encryption button on the right.

P6-M expressed a concern that the tool did not warn them when they tried to send their public key, and instead attached the private key:

> *"It's just not safe, I mean, they should definitely send a warning message saying "Do you really want to send your private key...?" or something. Yeah... I sent my private key, it should at least warn once. There are so many times when you do something and it's like "Are you sure?" and for the private key it just sends..."*

All those in the group agreed that despite interface issues, Mailvelope was easy to use once they were familiar with the process. Some members of the group mentioned that they would try to use the tool with friends and family. P4-M explained:

> *"I'll keep it but to be honest, I doubt I'll use it... I just don't email sensitive information with people... that often..."*

4.2.6 Interoperability: network effects

In the final session, in both groups when discussing their possible future use of the tools, participants raised concerns that their contacts would need to install these tools as well. While it is true that their contacts would need to install a PGP-based client, the participants in both groups thought it would need to be the exact same one that they had. They were surprised when we explained to them that any PGP-client would be able to exchange encrypted

messages with another PGP-client. It was an interesting mental model that could have been influenced by messaging applications for smartphones that generally do not offer interoperability. Research has shown that the adoption of such messaging apps may be influenced by network effects [1].

5 Discussion and conclusions

Participants in both groups were familiar with using email clients, both in the browser and as standalone applications. They were also aware of encryption, and had a basic understanding of what it did to messages, where learning about security technologies from popular news is not uncommon [17]. Participants simply reported that they would not use email to share sensitive information, having found other ways to share such information that were felt as being more secure, and voicing a lack of trust in the medium (in line with studies of pairs of novices using encryption tools [19]). Both products integrate with existing solutions. However, Mailvelope integrated with a browser, permitting users to continue to use existing email clients that they were familiar with. Where explicit/visible encryption is seen as necessary, the effort may lie in paving a way for these features to be integrated into existing popular platforms, and to emphasise interoperability between tools [2].

Participants used the tools on their own laptops. Integration with existing applications was highlighted as an advantage of Mailvelope, although encryption tools were compared to email clients that participants were familiar with, such as Gmail. If an encryption tool appears alien, it compounds the challenge of learning how to operate it effectively.

Both tools had bugs; downloading the GnuPG component required by Enigmail and automatically uploading a public key to Mailvelope's key servers did not work. Participants had to do both manually after being instructed by the experimenter. Mailvelope's option to encrypt was not immediately obvious as previously shown by Schochlow et al. [22], where prevention of errors is a fundamental precursor to providing usable interfaces [15]. Effective user interaction with encryption tools still lies in following basic interface design principles, and there were specific hurdles with each tool.

Ideally, the experimenter has an observatory role in a study like this, but because of the shortcomings of the technologies, they had to step out of this role and take on a more active approach of responding to participants' questions. Without an informed expert present, many participants reported that they would not have continued trying to use the tool(s) in reality. One flaw can be enough to dissuade potential users. However, with guidance, the setup was completed for all participants in both groups. Results suggest that guided habituation of encryption tools can overcome hurdles in the comprehension of encryption. This may be a useful approach for practical use of encrypted email. However, for security user studies, employing researchers who act strictly as experimenters and without domain knowledge has its own advantages [14]. Having a knowledgeable expert close by can be a natural way of learning how to use a new technology [16], where this study has also been an opportunity to observe how having a *helper* available to provide assistance can overcome obstacles which have a known – albeit complicated and demanding – solution.

Adoption barriers appeared across all three stages of our study and for both tools. Practitioners and researchers may continue to study emerging encrypted email solutions to progressively identify isolated barriers to adoption. However, security software developers continue to rely on an intuitive sense of what constitutes usability [3]. If we want any chance of promoting adoption, basic software quality and usability need to be delivered first and foremost. Furthermore, developers also need to draw on usability and design expertise: if the tools are seen as "retro", and do not meet user expectations, we can hardly expect them to be adopted.

Acknowledgements

We would like to thank all LASER attendees and anonymous reviewers for their feedback. Kat Krol's work was supported by a Secure Usability Fellowship from the Open Technology Fund and Simply Secure. Ruba Abu-Salma's work was supported by a SUDS (Supporting Usability and Design in Security) Fellowship from the Open Technology Fund and Simply Secure. We would like to thank Ania Piotrowska, Ingolf Becker and Seb Aebischer for their help in editing this paper.

References

[1] ABU-SALMA, R., KROL, K., PARKIN, S., KOH, V., KWAN, K., MAHBOOB, J., TRABOULSI, Z., AND SASSE, M. A. The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. In *European Workshop on Usable Security (EuroUSEC)* (2017).

[2] ABU-SALMA, R., SASSE, M. A., BONNEAU, J., DANILOVA, A., NAIAKSHINA, A., AND SMITH, M. Obstacles to the Adoption of Secure Communication Tools. In *IEEE Symposium on Security and Privacy (S&P)* (2017).

[3] BECKER, I., PARKIN, S., AND SASSE, M. A. Combining Qualitative Coding and Sentiment

Analysis: Deconstructing Perceptions of Usable Security in Organisations. In *Learning from Authoritative Security Experiment Results (LASER) Workshop* (2016).

[4] BRAUN, V., AND CLARKE, V. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology 3*, 2 (2006), 77–101.

[5] BROOKE, J., ET AL. SUS – A Quick and Dirty Usability Scale. *Usability Evaluation in Industry 189*, 194 (1996), 4–7.

[6] CHOE, Y. R., RUOTI, S., ANDERSEN, J., HENDERSHOT, T., ZAPPALA, D., AND SEAMONS, K. There's Hope for Johnny: Automatic vs. Manual Encryption. Tech. rep., Sandia National Laboratories (SNL-CA), Livermore, CA, USA, 2015.

[7] CLARK, S., GOODSPEED, T., METZGER, P., WASSERMAN, Z., XU, K., AND BLAZE, M. Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System. In *USENIX Security Symposium* (2011), pp. 8–12.

[8] GARFINKEL, S. L. Enabling E-mail Confidentiality through the Use of Opportunistic Encryption. In *Annual National Conference on Digital Government Research* (2003), Digital Government Society of North America, pp. 1–4.

[9] GARFINKEL, S. L., MARGRAVE, D., SCHILLER, J. I., NORDLANDER, E., AND MILLER, R. C. How to Make Secure Email Easier to Use. In *Conference on Human Factors in Computing Systems (CHI)* (2005), pp. 701–710.

[10] GARFINKEL, S. L., AND MILLER, R. C. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *ACM Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2005), pp. 13–24.

[11] GARFINKEL, S. L., SCHILLER, J. I., NORDLANDER, E., MARGRAVE, D., AND MILLER, R. C. Views, Reactions and Impact of Digitally-Signed Mail in E-commerce. In *Financial Cryptography and Data Security*. Springer, 2005, pp. 188–202.

[12] GAW, S., FELTEN, E. W., AND FERNANDEZ-KELLY, P. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-mail. In *Conference on Human Factors in Computing Systems (CHI)* (2006), pp. 591–600.

[13] KROL, K., MOROZ, M., AND SASSE, M. A. Don't Work. Can't Work? Why It's Time to Rethink Security Warnings. In *International Conference on Risk and Security of Internet and Systems (CRiSIS)* (2012), IEEE, pp. 1–8.

[14] KROL, K., SPRING, J. M., PARKIN, S., AND SASSE, M. A. Towards Robust Experimental Design for User Studies in Security and Privacy. In *Learning from Authoritative Security Experiment Results (LASER) Workshop* (2016).

[15] MOLICH, R., AND NIELSEN, J. Improving a Human-Computer Dialogue. *Communications of the ACM 33*, 3 (1990), 338–348.

[16] POOLE, E. S., CHETTY, M., MORGAN, T., GRINTER, R. E., AND EDWARDS, W. K. Computer Help at Home: Methods and Motivations for Informal Technical Support. In *ACM Conference on Human Factors in Computing Systems (CHI)* (2009), pp. 739–748.

[17] RADER, E., AND WASH, R. Identifying Patterns in Informal Sources of Security Information. *Journal of Cybersecurity 1*, 1 (2015), 121–144.

[18] RENAUD, K., VOLKAMER, M., AND RENKEMA-PADMOS, A. Why Doesn't Jane Protect Her Privacy? In *Privacy Enhancing Technologies* (2014), Springer, pp. 244–262.

[19] RUOTI, S., ANDERSEN, J., HEIDBRINK, S., O'NEILL, M., VAZIRIPOUR, E., WU, J., ZAPPALA, D., AND SEAMONS, K. "We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. In *ACM Conference on Human Factors and Computing Systems (CHI)* (2016), pp. 4298–4308.

[20] RUOTI, S., KIM, N., BURGON, B., VAN DER HORST, T., AND SEAMONS, K. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. In *ACM Symposium on Usable Privacy and Security (SOUPS)* (2013).

[21] RYAN, J. F., AND REID, B. L. Usable Encryption Enabled by AJAX. In *IEEE International Conference on Networking and Services (ICNS)* (2006), pp. 116–116.

[22] SCHOCHLOW, V., NEUMANN, S., BRAUN, K., AND VOLKAMER, M. Bewertung der GMX/Mailvelope-Ende-zu-Ende-Verschlüsselung. *Datenschutz und Datensicherheit – DuD 40*, 5 (2016), 295–299.

[23] SHENG, S., BRODERICK, L., KORANDA, C. A., AND HYLAND, J. J. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *ACM Symposium on Usable Privacy and Security (SOUPS)* (2006), pp. 3–4.

[24] WHITTEN, A., AND TYGAR, J. D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium* (1999).

Appendix

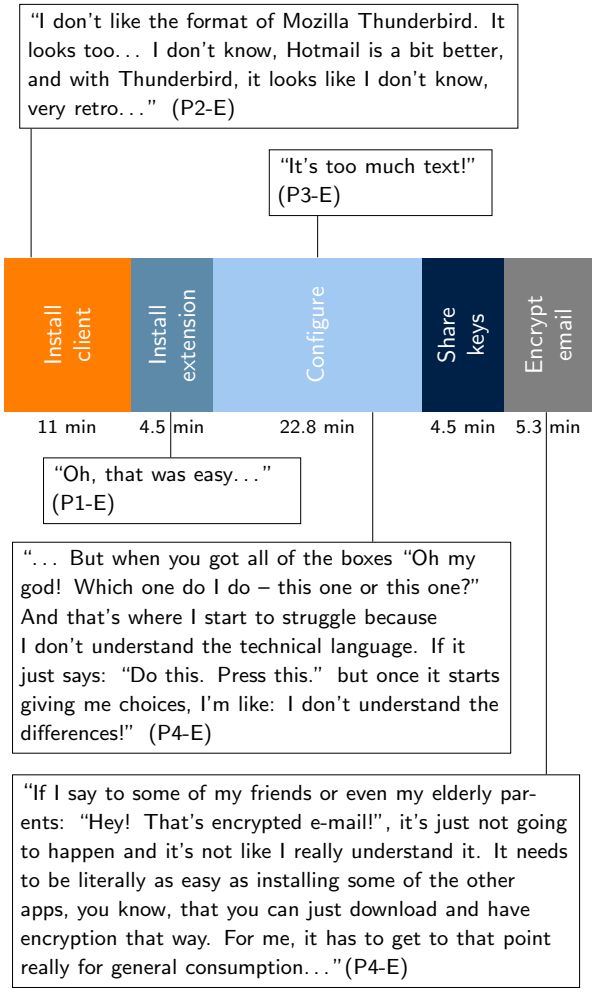

Figure 3: The user journey of setting up Enigmail. The graph shows timings for each step of the setup process with notable participant quotes.

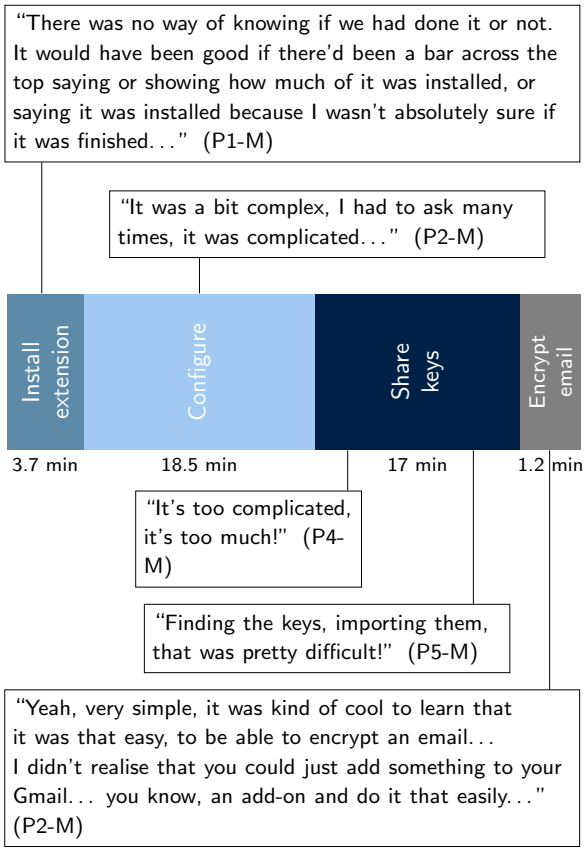

Figure 4: The user journey of setting up Mailvelope. The graph shows timings for each step of the setup process with notable participant quotes.