Why Doesn't Jane Protect Her Privacy?

Karen Renaud[1], Melanie Volkamer[2], and Arne Renkema-Padmos[2]

[1] School of Computing Science, University of Glasgow, Glasgow, UK
karen.renaud@glasgow.ac.uk
[2] CASED / TU Darmstadt, Hochschulstraße 10, 64289, Darmstadt, Germany
name.surname@cased.de

Abstract. End-to-end encryption has been heralded by privacy and security researchers as an effective defence against dragnet surveillance, but there is no evidence of widespread end-user uptake. We argue that the non-adoption of end-to-end encryption might not be entirely due to usability issues identified by Whitten and Tygar in their seminal paper "Why Johnny Can't Encrypt". Our investigation revealed a number of fundamental issues such as incomplete threat models, misaligned incentives, and a general absence of understanding of the email architecture. From our data and related research literature we found evidence of a number of potential explanations for the low uptake of end-to-end encryption. This suggests that merely increasing the availability and usability of encryption functionality in email clients will not automatically encourage increased deployment by email users. We shall have to focus, first, on building comprehensive end-user mental models related to email, and email security. We conclude by suggesting directions for future research.

Keywords: email, end-to-end encryption, privacy, security, mental model

1 Introduction

Email was introduced in MIT's CTSS MAIL around 1965 [46]. At this point privacy was not a primary concern. Subsequently, STARTTLS [36, 25] led to the deployment of opportunistic transport layer encryption for email transmission. Recently, more email providers have started applying it by default, effectively protecting email privacy in transit. However, email providers themselves, and those who might be able to hack into the email servers, have full access to our email communication. *End-to-end* (E2E) encryption by end-users would protect emails from access by email providers and hackers too. Facilitating tools are readily available, including PGP/OpenPGP [4, 10, 9], PEM [30–33], MOSS [13], PKCS#7 [26], and S/MIME [39–41] according to Davis [14]. However, they generally have minimal real-world application outside of specific use cases.

The "Summer of Snowden" [23] has put digital security back in the limelight, and there has been a slew of new proposals for facilitating E2E encrypted secure messaging (e.g. DarkMail, LEAP, Pond, Mailpile, Brair), but there is, as yet, little evidence of mass uptake of E2E email encryption. The question that remains is *"Why is the use of end-to-end email security so limited?"* Previously, the poor usability of E2E encryption tools was advanced as the most likely explanation [50, 44]. However, usability has improved

in the interim and this might no longer be the primary obstacle it used to be. Other papers cite interoperability difficulties between different tools and technical problems as contributing factors [34]. The research question we want to answer is: "*which other explanations, besides the previously highlighted problems, could explain the low uptake of E2E encryption?*" If other reasons exist, they will need to be addressed before we can hope to increase the uptake of E2E encryption.

To explore other potential explanations, we need to consider more human related than purely usability aspects because E2E email encryption is undeniably effortful. Hence the user has to be convinced of the need for E2E encryption, and the rewards that will accrue as a result [7]. Consequently, it makes sense to study end-user mental models of email and email security; i.e. do users actually understand the threats to their emails and do they know which particular threats could be ameliorated by means of E2E encryption? Note that if users don't have the correct mental models, or don't have any mental model of email architecture and potential threats at all, they are unlikely to encrypt their emails. If this is so, then in addition to addressing the technical and usability issues of email encryption, we will have to work on developing the correct mental models, so that these can eventually lead to a desire to encrypt and subsequent adoption. Some researchers have reported issues with respect to flawed end-user mental models in other security related contexts: with respect to anonymous credentials [49], wrt. firewalls [38, 15], wrt. warnings [6], and wrt. mobile security [29]. Thus it is very likely, that similar issues wrt. mental models related to email, and email security, exist.

We conducted semi-structured interviews with lay people and a survey (containing the same questions) with a class of computer science students because we chose to focus on these two different groups to explore their respective end-user mental models. We anticipated that their mental models would differ given their very different backgrounds.

In order to answer our research question, we proposed seven possible explanations why people do not generally use E2E email encryption deduced from a natural progression from awareness, to understanding, to acting (Section 2). These seven possible explanations were evaluated based on an analysis of the interviews and survey responses as well as by examining related research literature in the context of usable security and mental models (Sections 3 and 4). We confirmed six of the seven explanations. Obviously, in order to change the situation in the future towards more privacy protection in email communication, all of these need to be addressed. We thus conclude the paper by suggesting that future work focus on finding ways to address these different themes (Section 5). Due to the general nature of our findings and proposals, we expect that amelioration will apply equally to email communication and to other privacy-critical applications.

2 Proposed Explanations

Here we provide a list of possible explanations for non-uptake of E2E encryption. To generate these explanations we formulated a developmental pathway to adoption of E2E email encryption. We identified seven different states starting with general, then usability-related and then states related to interoperability and technology (see Fig. 1):

1. They do not have any *awareness* of privacy as a concern.

2. They are aware of the possibility of privacy violation of their emails but do not take any action for a variety of different reasons, perhaps because it does not *concern* them.
3. They know that the privacy of their emails can be violated but are not aware that this can happen in transit or at the mail server side. They may subsequently attempt to protect themselves against client-based threats, but *do not use E2E encryption*.
4. They know that the privacy of their emails can be violated in transit or at the mail server side but they *do not take any action* because they fail to see the need to act.
5. They know that the privacy of their emails can be violated (transit/server) and they want to prevent this but they *do not know how* to protect their emails against these types of threats, i.e. that they should use E2E encryption. They lack the knowledge, or have only partial knowledge.
6. They are concerned that the privacy of their emails can be violated (transit/server) and they understand that they can use E2E encryption to prevent this, but they *can't* do it.
7. They are concerned that the privacy of their emails can be violated and they understand that they can use E2E encryption to prevent this, and they are able to do it, but still they have reasons not to — *they get side-tracked for some or other reason*.

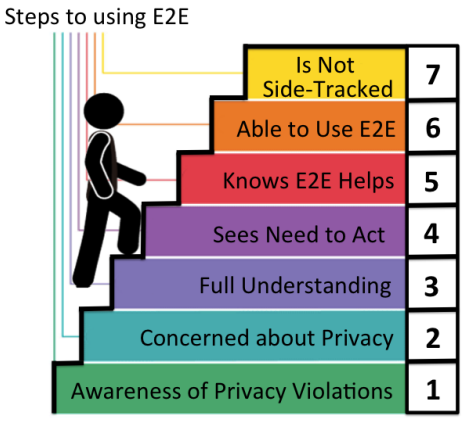

Fig. 1. Progression Towards E2E Encryption Deployment

For each of these explanations we will examine the relevant research literature and statements made by the participants in our study to see whether each is supported or challenged.

3 The Study

We performed an exploratory study consisting of semi-structured interviews, and subsequent qualitative analysis in order to identify users' mental models of email security

and thereby to answer the question *"Which of the Proposed Explanations for the Non-Uptake of E2E Encryption Can be Validated?"*. The research philosophy of this study is interpretivistic [51]. This is typical for research carried out where explanations are sought for activities in natural settings where we hope to make cautious generalisations based on a study of a limited number of participants. The research approach is inductive, seeking to construct theories by means of identification of patterns in the data [5].

From 2 to 6 December 2013[3], we performed 21 interviews in Glasgow, of whom 18 participants consented to having their interview recorded and transcribed. The participants were a convenience sample of students and staff at The University of Glasgow, and were recruited through personal and social networks.

The questions in the study were based on several discussion sessions among the authors. As there is no 'one' widely-accepted method for identifying mental models, we decided to use both drawings with think-aloud and semi-structured interviews in order to gather both types of data.

Both parts were tested in a pre-study. For the test run, the survey was given to six people to fill in on paper, and the drawing tasks were also tried in-person with two individuals, as well as generally asking around to get an impression of people's frame of mind. From the pre-study we became aware of unclear question framing. For the study design we removed stickers with concrete threats (e.g. NSA, anonymous, viruses), created a custom diagram to be used in the debrief, added think-aloud, updated the way that questions were asked (e.g. specifically asking about security problems), and reworked the stickers based on icons from Microsoft Outlook 2013.

For the interviews, first the participant received a warm-up exercise for think-aloud, was handed the questionnaire, and then the questions were asked while the responses were recorded over audio. They were debriefed afterwards. These question categories were included in the study:

Free-hand drawing Participants were asked to draw the transmission infrastructure and process that allows an email from a friend to arrive in their inbox. They were asked if they would change the drawing if they were sending the email, or if the email was sent by a bank.

Template drawing In the second stage, a sheet of stickers was given to the participants, and they were asked to make another drawing of the transmission infrastructure. They were told they did not have to use all stickers and that they could draw additional items.

Security problems Participants were asked what security problems they were aware of regarding email, who causes these problems, and where they are caused. They were asked to mark the location where the problem takes place on the diagram made from the stickers.

Security concerns They were also asked about their general level of concern around the security problems of email that they mentioned, which problems they were most and least concerned about (as well as the reason), and what coping mechanisms they put in place to deal with the concerns they had.

[3] We obtained ethical approval from the College of Science and Engineering at Glasgow University (#CSE01327).

Demographics Participants were asked whether they used webmail and/or a desktop client, which email client they use, their occupation, sex, and age group.

Debriefing and Closing Remarks At the end of the study the interviewed participants were debriefed about the true goal of the study.

Permission was requested for a transcript of the recording to be made and used in a publication. They were also asked whether they were willing to take part in future studies, and whether they would like to receive a copy of the paper resulting from this research.

Participants were informed about the topic of the study (transmission of email), but were not briefed about the precise goal of the study (determining understanding of email security). Note that we did not mention the concept of end-to-end encryption to the participants, nor did we suggest that they ought to encrypt their emails. They were told that they could stop at any time, and that they would not be penalised in any way for doing so when participating in any courses taught by the researchers.

The interview group consisted of 9 females and 12 males, with 7 individuals in age group 18-24 and 14 individuals in age group 25-34. Of the participants, 8 used webmail, 11 used webmail and desktop email clients, and 2 weren't sure.

In addition to the data collected from lay persons, we also wanted to collect data from computer science students as they ought to have a better understanding of the email infrastructure and the potential threats. However, due to resource limitations, it was not possible to conduct and transcribe another twenty interviews, so we administered a survey containing the same questions to a classroom context. We acknowledge that this stoppes us from collecting individual think-aloud transcripts or speaking to the students personally but we did gain valuable insights despite these limitations.

Both the survey and interview groups stepped through the same survey: the same materials were used for both. The interviewer walked through all questions with the interview participants. The classroom group completed the survey individually without assistance.

The survey group consisted of 8 females and 16 males (1 blank answer), with 12 individuals in age group 18-24, 11 individuals in age group 25-34, and 1 individual in age group 35-44 (1 blank answer). Of the participants, 13 used webmail, 8 used webmail and desktop email clients, 3 used desktop clients, and one was not sure.

4 Results & Reflection

We performed a qualitative analysis of the results, based on an inductive approach, to determine which of the explanations could be supported. We independently analysed our participants' responses, then conferred in order to agree.

Since this was a qualitative study we, like Wash [48], do not report how many users alluded to each of the explanations in their statements. We do attempt to give a flavour of our findings, in order to allow the reader to understand the different mental models that are revealed by our study.

In the following subsections we report on whether any statements made by the participants support or challenge the explanations we advanced in Section 2. We also discuss the results in relation to existing findings from the literature. As described in the

study section, we performed the study with two groups: lay people and experts. We did not detect any differences between the two groups, however, so the rest of this section is an analysis of both the interviews and the surveys.

4.1 Explanation 1: No Privacy Awareness

A possible reason why E2E encryption is not widely used might be that people do not have any *awareness* of privacy as a concern.

Analysis from interviews/survey. We did not find any general evidence for this explanation from the interviews and surveys — the participants were indeed aware of the fact that their privacy could be violated when using email. Quotes that support the case that people are aware of privacy are:

> ".. it kind of gets more into the privacy of people's life, somehow"
> "it's just like a virtual ... loss ... of privacy"
> "it's about privacy concern and he is collecting data, and based on that data maybe he is profiling"
> "mitigate by not sending emails containing sensitive information.

In particular, general privacy-related violations were mentioned far more frequently than specific concerns such as the integrity, authenticity and availability of email. There is also some evidence that the NSA's activities have had some influence as shown by quotes like

> "... NSA, a group of intelligence; they are just monitoring normal people"

Findings from literature. In the literature there are similar findings that people are more aware of privacy violations than of any other type of violations [47]. Few people mentioned specific aspects such as integrity and availability in a study into online security understanding [19]. In a study on connection security, people only considered confidentiality and encryption in their definitions [18]. For smartphones the issue of theft and loss made availability salient in a study on smartphone security [35].

Summary. While the majority appeared aware of privacy concerns related to email, there was at least one who did not mention privacy, sensitive data, private data or anything related to this.

4.2 Explanation 2: Privacy Aware, but Not Concerned

Another explanation that can be advanced is that they are not concerned about the problems even though they are aware of the potential privacy violations that can occur.

Analysis from interviews/survey. From the interviews and surveys, different reasons have been identified that may help to explain why people may not see the need to protect their privacy in the email context even though they are aware of potential privacy issues. Relevant statements and corresponding quotes from the study are:

Theme 1: Nothing to hide: "And I don't feel that I have something to [laughs] to hide, though I don't like people, uh, getting in my stuff"; "[I'm least concerned about] [s]nooping. I think that unless I have something to hide it doesn't bother me."; "But in general, I don't know if that is that, uh, important or is it that interesting. I don't know. It, it's not very sensitive, so the risk is not that high,"; "Given for me as a private person because I don't have, you know, so private data which I'm concerned about that no one ever should read that and I—like 99% of my emails are just formal stuff ".

Theme 2: No harm "But they are not affected directly."; "Not to do any harm to me, rather he is actually collecting data."; "I think, umm, that would always happen, the monitoring thing. So, I would say that yeah ... the, the hacking thing is more, more of a concern."

Theme 3: They don't feel important enough "Emails of some high officials, high-position officials in government so ... they may ... cause problems."; "I think it just, um, depends on your personality if you have someone famous."

Theme 4: Private emails are not critical "I would be more concerned if it was my official Inbox, of my company, but this I'm, I'm since I am a student and I am right now only talking about my personal email box"; "I'm talking about personal emails there."; "So I think there are possibly two main cyber threats for me as a private person, and then if you're an institution or a business company, then there might be more"

Theme 5: Someone else's responsibility "There has to be the clients, or the, the, the person providing the client services is responsible for making sure that it's secure. So if you have a decent email service provider they should be able to ensure that you can only see emails that are on your account and you only see emails after you've logged on, and things like that"; "You-the whole thing about not just email security but the whole cyber security in general, you have to ... we're most of the time at the mercy of the people providing the service."

Theme 6: Assuming that security is already taken care of "I'm not, I'm not aware of any, sort of, like, when I'm sending just a general email, umm, I assume [laughs] that it's quite safe and it hasn't been commandeered by an external source, or anything like that."; "That's why it's personal computer and personal email. That's-I think that's the, the, the worst case scenario if every time I send an email or had a conversation online, someone else can see it. It's not good."; "It works, but I suppose that the securities during the, during that path we draw before, it should be really h-hard to break, first of all."

Findings from literature. Other researchers studying privacy issues in other contexts such as social networks also concluded that there was often a mismatch between being aware of privacy issues and taking action. Acquisti and Grossklags found that "even if individuals have access to complete information about their privacy risks and modes

of protection, they might not be able to process vast amounts of data to formulate a rational privacy-sensitive decision" [2]. Users might also be driven by immediate gratification over rational decision-making [1]. Gross and Rosson [24] confirm the attitude of generally feeling that security was the IT department's job, not that of their study's participants.

Summary. There is plenty of evidence, both from our study and from the literature, that if people are generally aware of privacy issues with email communication this does not mean that they will expend the effort to protect their privacy. Thus, we can conclude that this second explanation is indeed a feasible reason why E2E encryption is not widely used.

4.3 Explanation 3: Privacy Concerned with Misconceptions

A third possible explanation is that users know that the privacy of their emails can be violated but do not know that this can happen both in transit and at the mail server. They may subsequently attempt to protect themselves against other types of threats and might not use E2E encryption.

Analysis from interviews/survey. Analysing the interviews and the surveys reveals that neither threats at the email server side in terms of either hacking the server or internals having access, nor threats on the network, are those that are most often mentioned. The threats that are most often mentioned are related to password security and malicious attachments.

Theme 1: Password Issues: Quotes which clearly provide evidence that most people have password problems in mind when thinking about how to secure email communication are: "I think this is the main thing, related... basically, if your password is secure with you, then I think your mailbox is secure."; "If your password is... you know, falls into the wrong hands... most concerned obviously is someone getting access into my mailbox, obviously, by logging in";

The responses to the question on countermeasures show that people mentioning password-related threats also mention corresponding countermeasures such as: "Trying to use as many different passwords as possible without keeping, uh, keep forgetting them."; "Good password, change password regulary."; "Set a very good password, including numericals and alphabets, lowercase, uppercase, special characters.";

Theme 2: Malicious Attachment: Quotes indicating that people have malicious attachments in mind when thinking about email related threat are: "files you don't really want to . you might receive viruses"; "if you open an attachment which includes viruses or something like that"; "you can receive any virus".

Similarly, responses to the question on countermeasures show again that people mentioning malicious attachments also mention anti-virus software (e.g."From the sending side, well, you might actually, ahh, send something you're not aware to send somehow, ahh, or you might actually end up sending emails even though you don't know it") or advocating careful usage as a corresponding countermeasure. Examples for careful

usage are: “Don’t open any emails from an unknown.”; “I do my own mental virus scan in my limited abilities, in my head.”.

Theme 3: Further Mentioned Threats: Other mentioned threats not related to the server or transit threats are:

- ***Concerned about security of end-point devices***
  “I’m not an expert at all but, ahh, got a virus, and for that reason it kept on sending automatic emails from his ... his email address”, “But for some reason these random emails pop up and ... on my Hotmail before. I had to cancel it because all these people were getting emails from me that I had ... um, when I was in the military. And they were all getting emails, and I hadn’t sent any emails.”.
- ***Concerned about someone having physical access to their device***
  “[A]t the university, sometimes I open my mailbox and I just forget to, ahh, sign out.”;
  “I work with my laptop, and sometimes I leave my laptop alone.”

Findings from literature. People in our study were most likely to mention password security and virus as malicious attachments which is related to Wash’s [48] findings on “names for viruses models about viruses, spyware, adware, and other forms of malware [were] which referred to [by everyone] under the umbrella term virus’” [48]. Also related to Wash’s and others’ findings is that one of the issues with security is that people’s s are incomplete i.e. they try to apply countermeasures against those threats they are aware of and they think these will address all threats.

Finally with respect to encryption in particular, Garfinkel suggests that the trust model of PGP (Web of Trust) is too hard for many users to grasp [21]. Keller *et al.* [27] report that the detailed properties of the cryptographic primitives that are used in public-key cryptography can be hard to grasp. Additionally the public-key infrastructures, on which many E2E encrypted email programmes are built, might be difficult to comprehend: “[T]he usability problems uncovered in the Johnny user study were not driven by the PGP 5.0 program itself, nor by the lack of training offered within the program, but by the underlying key certification model used by PGP.” [21].

Summary. While this shows that when people are aware of a concrete threat, in this case passwords being hacked and malicious attachments, they take or try to take remedial actions. However, our analysis also provides evidence that some people are not aware of any other threats and in particular are not aware of threats related to the server and the transit. Correspondingly there is evidence for explanation 3, that many participants have various (mis)understandings that direct them towards specific countermeasures that are not relevant for adoption of E2E encryption.

4.4 Explanation 4: Privacy Concerned, with Sound Understanding, but Does Not See Need to Act

The fourth possible explanation is that users know that the privacy of their emails can be violated, and have a sound understanding that this can happen during transit or at the

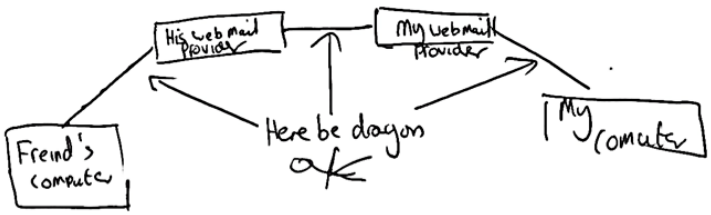

Fig. 2. Understanding of the email architecture of participant B-24: "here be dragons"

mail server side, and also know that they can use E2E encryption. However, they do not take any action for different reasons.

First, we validated whether there were actually people who were aware of threats related to the server and transmission. There is strong evidence that at least some people are aware of these threats as the following quotes show (as well as Figure 2): "I don't like my personal emails to be accessible by the email provider", "it's always that they have control on everything"; "It's a bit strange that Google can read what I am, uh, sending or, uh, receiving from-from friends, or-or-or partners or businessmen.; "The data transmission in general, from server to Internet, should... could be, could be a problem."; "I would imagine it would be somewhere from leaving her computer to being out here, and then before coming then in my computer."

Analysis from interviews/survey. In order to validate this explanation from the interviews and surveys, we checked whether people who mentioned threats related to the server or the transit necessarily saw the need to protect against these threats. We identified reasons why it might be worthwhile for people to take action themselves to protect against hackers gaining access to the mail servers, against email service providers having access, or even against anyone listening on the network. For each of the three themes we provide quotes:

Theme 1: No need to protect against hackers gaining access "... or to the server, but I don't know how, ... how easy it is to ... have access in the whole server for a company"; "With the cyber security in place, I think Gmail would not allow someone to get into its stuff like that. So probably, I might be a little less concerned about that."; "I'm the least concerned about hackers. Okay. That's mainly because I use two-step verifica- verification on my email, and I will see if it works."; "I think the server is most sensitive one, but for me it's less concern because, um, I care about the money I have to pay and if I want it very secure I have to invest money."

Theme 2: No need to protect against email providers having access in general... "You can say that for security reason it might be useful" [having access to the e-mails]; "But sometimes it looks at patterns and words in the email. Most of them, they will actually read the email. Maybe then scan through the message and they see things that sound fishy, they, they can highlight to you that the message looks like it's not very genuine"

- ***... as they only scan to enable targeted advertisements ...*** "Who can scan your email and know the content. And then based an advertising"; "They you need to be able to parse it, right, for targeted ads"; "Possibly least concerned is if something, uh, if my email provider is reading or like scripting my emails and therefore showing me possible or targeted ads. ... Because to be honest, if I don't want them I'll just switch the email provider."
- ***... as they only access because security agencies require access:*** "[NSA] they requested Facebook or Google to pass certain information so the problem can appear here as well when they request them to release certain data or maybe my, ahh, email service provider, they can also actually access my email and see what's going on"

Theme 3: No Need to Protect against network related attacks "And there's always the chance that it could be intercepted and read, and maybe even duplicated and stuff like that. [..] So I really don't see that as a big problem."

Findings from literature. There is an interesting aspect regarding paying for security and how much people are willing to pay. Will they accept insecure or less secure services as long as these are free? This has also been studied and presented in the literature. "[I]ndividuals are willing to trade privacy for convenience or bargain the release of personal information in exchange fore relatively small rewards." [2], and "Many perverse aspects of information security that had been long known to practitioners but just dismissed as 'bad weather' turn out to be quite explicable in terms of the incentives facing individuals and organisations, and in terms of different kinds of market failure." [3]. Finally, the "nothing to hide" fallacy [45] comes across strongly. Conti and Sobiesk [12] found that many of the respondents in their study also exhibited this perception.

Summary Our data provides evidence that this fourth explanation (that is, that users know that the privacy of their emails can be violated, and have a sound understanding that this can happen during transit or at the mail server side, but do not take any action) is a viable explanation for the poor uptake of E2E encryption.

4.5 Explanation 5: Privacy Concerned, with Sound Understanding, but Does Not Know How to Act

Another possible explanation is that while people are aware that their privacy can be violated, are concerned about privacy problems, and see the need to prevent these, they may not be aware of the efficacy of E2E encryption to protect their communications. They may believe that other measures are efficacious. Because they do not know, or are only partially aware, that they can use E2E encryption as a precaution, they do not use/consider it but may consider other options.

Findings from interviews/surveys. The analysis of the surveys, in particular, revealed a number of themes why people do not use E2E encryption although they see a need to protect themselves (against server side privacy violations ans against network attacks).

The identified themes are 'think there is nothing they can do', 'unclear about countermeasures', and 'wrong understanding of encryption'. In the following we explain these themes and provide quotes for each of the themes:

Theme 1: Think there is nothing they can do: Due to the lack of knowledge about encryption and, in particular, about E2E encryption, some people believe that they cannot prevent email providers from gaining access to their emails. Quotes providing evidence for this theme are: "Is never gonna change."; "There's no solution for that."; "It's always that they have control on everything."

Theme 2: Other types of (more or less effective) countermeasures: "So whenever, uh, I have to send some very, like, uh, highly, uh, you know, secret information, I do not prefer mail. I prefer talking on phone; "Like to split up into different things, and I would say that send some of them by Facebook, but some of them by emails; "I am definitely not sending my credit card information or stuff like that or very-very personal data within, um, an email. I try to do that personally or within different steps."

Theme 3: Wrong understanding of encryption: Overall, only very few participants mentioned the term 'encryption' at all. Most of those who mentioned it seem to have a wrong understanding of encryption and in particular E2E encryption as the following quotes show: "Definitely encrypt the email, make sure I knew it wasn't a fake."; "[I'm aware of problems related to] firewall and cryptography, public and private passwords" Of particular interest is this statement from one of the participants using https: "The only thing that I use is I actually enable https for my Facebook, Gmail, etcetera. So I use secured connection to login, so that like I use SSL and there... it's a secure.". This is only a first step however, and only secures the connection between the device and the mail provider but does not mitigate against the amail provider or any connection afterwards as https might not be enabled.

Findings from literature. Wash [48] postulates that people had some idea of some kinds of threats and tried to use countermeasures that they believed would address the threats they were aware of. If their threat models are incorrect these countermeasures will probably not help, but the invisibility of breaches will keep them blissfully unaware of this. Gross and Rosson [24] reported that the participants in their study had an incorrect and dated understanding of the actual threats they were subject to. They seemed to conflate security with functionality in many cases.

Summary. Based on the findings from the interviews and surveys, and the findings in the literature, we can confirm the explanation that some people do not use E2E encrypted email because they are not aware, or do not understand, the protection techniques that are available.

4.6 Explanation 6: Privacy Concerned, Wants to Act, but Cannot

In this subsection we analyse whether the theoretical explanation of "They know that the privacy of their emails can be violated (transit/server) and they understand that they can use E2E encryption to prevent this, but they are not able to use it".

Findings from interviews/surveys. The analysis of the interviews and the surveys does not provide much evidence that this is actually a reason, i.e. not being *able* to encrypt was not something our participants complained about. The only related quote is:

> "[Encrypting email is] less effective because not everyone knows to to user this / decrypt / etc.)"

The fact that participants did not mention more related issues might be because we did not use the term "E2E encryption" in our questions and, in particular, we did not ask our participants whether they ever tried to use E2E encryption or to relate their experiences with using it. This omission was deliberate: we wanted to gauge *their* mental models, not prompt them by mentioning E2E encryption.

Findings from literature. One of the mantras of the field of usable security is that security systems are not used because they are too complicated, because people *cannot* use them. Whitten & Tygar published their seminal "Johnny" paper in 1999 [50]. They suggest that security software is intrinsically harder to use than "normal" software [50].

Many of the papers published about email encryption and the difficulties users experience with it make a basic assumption that the problem is that they *can't* encrypt [50, 11, 44, 20, 52, 34, 43]. This suggests that the user wants to do something but is prevented from doing so by the complexity of the system and the poor design of the interface. Some researchers have worked on creating better interfaces to address this problem [17].

Summary. While the Whitten and Tygar paper states that poor usability is discouraging adoption, many people do not even reach this stage, and are stuck in different mindsets. Thus, while users with good understanding and motivation may be foiled by poor user interface design or a lack of technological support, many have different reasons for non-adoption that will need to be resolved before contributions to the usability challenge become meaningful.

4.7 Explanation 7: Privacy Concerned, Knows how to Act, Can Act but Does Not

In this subsection we analyse whether the theoretical explanation of "They know that the privacy of their emails can be violated (transit/server), and they understand that they can use E2E encryption to prevent this, and they are able to use the tools, but they get side-tracked for some reason.' was mentioned by our participants or by other researchers.

Findings from interviews/surveys. From the data we collected there is no evidence to confirm this explanation.

Findings from literature. Users appear to have an over-optimistic bias in their risk perceptions, especially with respect to information security. This self-serving bias is also related to a perception of controllability with respect to information security threats,

i.e. what we control we consider less risky than that which we do not control [42, 37]. Furthermore, interoperability and availability of keys on different devices are issues mentioned by [34]. Another possibility is that users are simply mimimising effort, and encryption, being effortful, seems too much trouble.

Dingledine and Mathewson [16] studied the tendency of users to not use security features. In general, in case of high effort and only a nebulous nature of the consequences, it was not used. Unfortunately, it is difficult to compute the cost of security, or even the lack thereof [28]. Furthermore, Gaw *et al.* [22] offers another potential reason. In the analysed organisation where employees did have the knowledge and ability, email was not universally encrypted. As reasons they identified that employees considered it paranoid to encrypt all emails, suggesting a social element to their decision making.

Summary. While there is not much evidence from our interviews and surveys to support this explanation there is some evidence from the literature supporting this explanation. It is possible that we would also have identified similar themes from interviews if we had included people who either do use, or have discontinued using, E2E encryption.

4.8 Summary & Discussion

Table 1 summarises our findings, in terms of whether our explanations were confirmed by our studies and literature review, or not.

Proposed Explanation	Literature	Participant Statements
1. No Awareness		(✓)
2. No Concern	✓	✓
3. Misconceptions of How to Protect	✓	✓
4. No Perceived Need to Take Action	✓	✓
5. Needs to Take Action But Does Not Know How to Act	✓	✓
6. Inability to use E2E Encryption	✓	
7. Becoming Side-Tracked	✓	

Table 1. Support for the Seven Explanations

We were not able to find strong evidence for a non-awareness of privacy as an explanation for non-adoption of E2E encryption. However, the gap between theoretical and practical privacy awareness pointed out by Burghardt *et al.* [8] could be confirmed in the context of email from our studies as increased awareness does not have converted into widespread adoption of E2E email encryption. Their lack of understanding, misconceptions and incomplete mental models of email security (refering to explanation 2-5) meant they did not even think about using E2E encryption. Correspondingly, it is not too surprising that from the qualitative studies was that not being able or willing to encrypt (poor usability - explanation number 6 and becoming side-tracked - explanation number 7) was rarely mentioned by the participants. These misconceptions also explain why people taking action to protect themselves mainly deploy (traditional) mechanisms such as secure passwords, anti-virus software, and careful usage. From our data, we

identified three cross-cutting factors that could contribute towards the explanations we cited in Section 2. *The first contributory factor could be their lack of understanding, misconceptions and incomplete mental models of email security* might be that there was, in general, very little understanding of how email was transmitted and stored and how the email architecture works. We could observe this from their drawings - e.g. in Figure 3 (computers directly connecting and email floating across to the recipient) and Figure 4 (here the lock and key may indicate that users think that more technologies are in place than HTTPS, and possibly have an expectation of end-to-end encryption) - as well as from their statements:

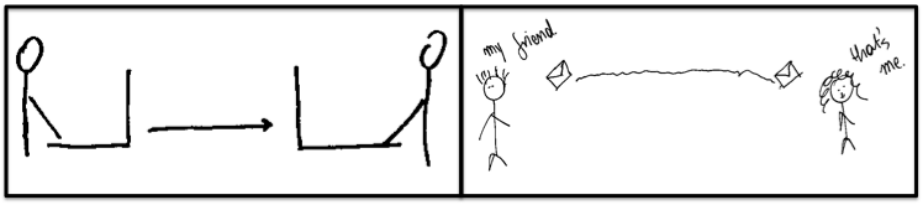

Fig. 3. Examples from first set of drawings

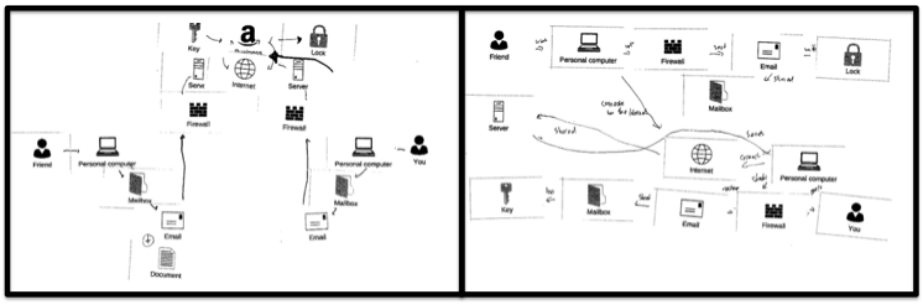

Fig. 4. Examples from second set of drawings

> "[I]t'll go into the sky somewhere, and then it will [go] down to my computer"
> "[I]t's all an invisible process to me. The way that I understand is that you literally just click send' then a second later it appears in their inbox [laughs]."
> "Umm, well, yeah, this type of thing is actually, ahh, quite a ... a mysterious thing for me."

A *second contributory factor* might be that they lack understanding of the possible consequences of not protecting themselves. For instance, most of those who *were*

aware of email providers having full access to their emails rationalised this instead of being concerned. They advanced several reasons for why this was acceptable, e.g. that it facilitated scanning of emails which they considered needed to occur for security purposes or to allow targeted advertisements (the price they pay for a free email service). Others, with more understanding and a greater level of concern, often did not act to protect their privacy because they considered it futile in the face of surveillance actions by powerful governments. Interestingly, there did not seem to be significant differences between mental models held by lay persons and computer science students taking part in our study.

A *third contributory factor* that emerged from our data was that problems might be attributable to the information sources that inform people generally. Our study provided evidence for the fact that people gain knowledge primarily via stories told by others or based on personal experience:

> "I have friends that, uh, their per-their personal accounts w-was hacked."
> "And also I think I've heard from my friend that they could catch everything from here [laughs] somehow."
> "[A friend] got a virus, and for that reason it kept on sending automatic emails from his ... his email address."

This would explain why many people seem to have an awareness of "good password practice", but not about privacy protection using E2E encryption, which has enjoyed much less attention in the media.

5 Conclusion & Future Work

The Snowden revelations have highlighted the importance of end-to-end encryption as a privacy preserving tool. We posed the question *"Why is the use of end-to-end email security so limited?"*. In order to answer this question, we set out by proposing a developmental pathway, a progression to E2E encryption, comprising of seven explanatory states.

We carried out a qualitative study (both semi-structured interviews and a survey) in order to identify mental models from both lay persons and computer science students. We considered that this study would serve to confirm or challenge our proposed explanations. We also carried out a literature review to determine whether the explanations could be verified from the established research literature. We did confirm four of the seven explanations from our study, and an extra two from the research literature.

As future work it would be beneficial to come up with ways of ameliorating the situation, finding ways of advancing users along the pathway to awareness, concern, knowledge, understanding, usage, and eventual adoption. Since we identified flawed or incomplete mental models in states two to five, specific questions that can be investigated in future to address these mental model related issues could include:

- How can we help users to understand the threats to their emails?
- How can we elicit a sense of concern in end-users with respect to privacy violations such that they make an attempt to explore privacy preservation tools?

– How can we communicate countermeasures and desirable precautionary behaviours effectively?
– How can we dispel the “nothing to hide” myth, so that end users do indeed see the need to act to preserve their privacy once they know how, i.w. better understand the consequences at least in the long run?
– In general, how can we nurture and foster comprehensive and complete mental models of E2E to ensure that users want to encrypt, know how to encrypt and, most importantly, do encrypt.

Acknowledgement

This paper has been developed within the project usable secure email communication’ - which is funded by the CASED (Center for Advanced Security Research Darmstadt) and the Horst Görtz Foundation and the EC SPRIDE project - funded by the German Federal Ministry of Education and Research.

References

1. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce. pp. 21–29. EC ’04, ACM, New York, NY, USA (2004)
2. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security & Privacy 2, 24–30 (2005)
3. Anderson, R., Moore, T.: The economics of information security. Science 314(5799), 610–613 (2006)
4. Atkins, D., Stallings, W., Zimmermann, P.: PGP Message Exchange Formats. RFC 1991 (Informational) (Aug 1996), http://www.ietf.org/rfc/rfc1991.txt, obsoleted by RFC 4880
5. Bhattacherjee, A.: Social science research: principles, methods, and practices (2012)
6. Bravo-Lillo, C., Cranor, L.F., Downs, J.S., Komanduri, S.: Bridging the gap in computer security warnings: A mental model approach. Security & Privacy 9(2), 18–26 (2011)
7. Bright, P., Goodin, D.: Encrypted e-mail: How much annoyance will you tolerate to keep the NSA away? (June 2013), aRS Technica. http://arstechnica.com/security/2013/06/encrypted-e-mail-how-much-annoyance-will-you-tolerate-to-keep-the-nsa-away/
8. Burghardt, T., Buchmann, E., Böhm, K.: Why do privacy-enhancement mechanisms fail, after all? a survey of both, the user and the provider perspective. In: Workshop W2Trust, in conjunction with IFIPTM. vol. 8 (2008)
9. Callas, J., Donnerhacke, L., Finney, H., Shaw, D., Thayer, R.: OpenPGP Message Format. RFC 4880 (Proposed Standard) (Nov 2007), http://www.ietf.org/rfc/rfc4880.txt, updated by RFC 5581
10. Callas, J., Donnerhacke, L., Finney, H., Thayer, R.: OpenPGP Message Format. RFC 2440 (Proposed Standard) (Nov 1998), http://www.ietf.org/rfc/rfc2440.txt, obsoleted by RFC 4880
11. Clark, S., Goodspeed, T., Metzger, P., Wasserman, Z., Xu, K., Blaze, M.: Why (special agent) Johnny (still) can’t encrypt: a security analysis of the APCO project 25 two-way radio system. In: Proceedings of the 20th USENIX conference on Security. pp. 4–4. USENIX Association (2011)

12. Conti, G., Sobiesk, E.: An honest man has nothing to fear: User perceptions on web-based information disclosure. In: Proceedings of the 3rd Symposium on Usable Privacy and Security. pp. 112–121. SOUPS '07, ACM, New York, NY, USA (2007), http://doi.acm.org/10.1145/1280680.1280695
13. Crocker, S., Freed, N., Galvin, J., Murphy, S.: MIME Object Security Services. RFC 1848 (Historic) (Oct 1995), http://www.ietf.org/rfc/rfc1848.txt
14. Davis, D.: Defective sign & encrypt in S/MIME, PKCS# 7, MOSS, PEM, PGP, and XML. In: USENIX Annual Technical Conference, General Track. pp. 65–78 (2001)
15. Diesner, J., Kumaraguru, P., Carley, K.M.: Mental models of data privacy and security extracted from interviews with Indians. 55th Annual Conference of the International Communication Association (ICA), New York (May 26-30, 2005)
16. Dingledine, R., Mathewson, N.: Anonymity Loves Company: Usability and the Network Effect. In: The Fifth Workshop on the Economics of Information Security (WEIS 2006). (26-28 June 2006)
17. Fahl, S., Harbach, M., Muders, T., Smith, M., Sander, U.: Helping Johnny 2.0 to Encrypt His Facebook Conversations. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. pp. 11:1–11:17. SOUPS '12 (2012)
18. Friedman, B., Hurley, D., Howe, D.C., Felten, E., Nissenbaum, H.: Users' conceptions of web security: A comparative study. In: CHI'02 extended abstracts on Human factors in computing systems. pp. 746–747. ACM (2002)
19. Furman, S.M., Theofanos, M.F., Choong, Y.Y., Stanton, B.: Basing cybersecurity training on user perceptions. Security & Privacy, IEEE 10(2), 40–49 (2012)
20. Furnell, S.: Why users cannot use security. Computers & Security 24(4), 274–279 (2005)
21. Garfinkel, S.L., Miller, R.C.: Johnny 2: A user test of key continuity management with s/mime and outlook express. In: Proceedings of the 2005 symposium on Usable privacy and security. pp. 13–24. ACM (2005)
22. Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In: Proceedings of the SIGCHI conference on Human Factors in computing systems. pp. 591–600. ACM (2006)
23. Greenwald, G., MacAskill, E., Poitras, L.: Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian 9 (2013)
24. Gross, J.B., Rosson, M.B.: Looking for trouble: understanding end-user security management. In: Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology. p. 10. ACM (2007)
25. Hoffman, P.: SMTP Service Extension for Secure SMTP over Transport Layer Security. RFC 3207 (Proposed Standard) (Feb 2002), http://www.ietf.org/rfc/rfc3207.txt
26. Kaliski, B.: PKCS #7: Cryptographic Message Syntax Version 1.5. RFC 2315 (Informational) (Mar 1998), http://www.ietf.org/rfc/rfc2315.txt
27. Keller, L., Komm, D., Serafini, G., Sprock, A., Steffen, B.: Teaching public-key cryptography in school. In: Teaching Fundamentals Concepts of Informatics, pp. 112–123. Springer (2010)
28. Lampson, B.: Privacy and security: Usable security: How to get it. Commun. ACM 52(11), 25–27 (Nov 2009)
29. Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J., Zhang, J.: Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. pp. 501–510. UbiComp '12, ACM, New York, NY, USA (2012)
30. Linn, J.: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures. RFC 989 (Feb 1987), http://www.ietf.org/rfc/rfc989.txt, obsoleted by RFCs 1040, 1113

31. Linn, J.: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures. RFC 1040 (Jan 1988), http://www.ietf.org/rfc/rfc1040.txt, obsoleted by RFC 1113
32. Linn, J.: Privacy enhancement for Internet electronic mail: Part I - message encipherment and authentication procedures. RFC 1113 (Historic) (Aug 1989), http://www.ietf.org/rfc/rfc1113.txt, obsoleted by RFC 1421
33. Linn, J.: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. RFC 1421 (Historic) (Feb 1993), http://www.ietf.org/rfc/rfc1421.txt
34. Moecke, C.T., Volkamer, M.: Usable secure email communications: criteria and evaluation of existing approaches. Information Management & Computer Security 21(1), 41–52 (2013)
35. Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K.: Understanding users' requirements for data protection in smartphones. In: Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on. pp. 228–235. IEEE (2012)
36. Newman, C.: Using TLS with IMAP, POP3 and ACAP. RFC 2595 (Proposed Standard) (Jun 1999), http://www.ietf.org/rfc/rfc2595.txt, updated by RFC 4616
37. Nordgren, L.F., Van Der Pligt, J., Van Harreveld, F.: Unpacking perceived control in risk perception: The mediating role of anticipated regret. Journal of Behavioral Decision Making 20(5), 533–544 (2007)
38. Raja, F., Hawkey, K., Hsu, S., Wang, K.L., Beznosov, K.: Promoting a physical security mental model for personal firewall warnings. In: CHI '11 Extended Abstracts on Human Factors in Computing Systems. pp. 1585–1590. CHI EA '11, ACM, New York, NY, USA (2011)
39. Ramsdell, B.: S/MIME Version 3 Message Specification. RFC 2633 (Proposed Standard) (Jun 1999), http://www.ietf.org/rfc/rfc2633.txt, obsoleted by RFC 3851
40. Ramsdell, B.: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. RFC 3851 (Proposed Standard) (Jul 2004), http://www.ietf.org/rfc/rfc3851.txt, obsoleted by RFC 5751
41. Ramsdell, B., Turner, S.: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. RFC 5751 (Proposed Standard) (Jan 2010), http://www.ietf.org/rfc/rfc5751.txt
42. Rhee, H.S., Ryu, Y.U., Kim, C.T.: I am fine but you are not: Optimistic bias and illusion of control on information security. In: Avison, D.E., Galletta, D.F. (eds.) ICIS. Association for Information Systems (2005), http://dblp.uni-trier.de/db/conf/icis/icis2005.html#RheeRK05
43. Ruoti, S., Kim, N., Burgon, B., van der Horst, T., Seamons, K.: Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. In: Proceedings of the Ninth Symposium on Usable Privacy and Security. pp. 5:1–5:12. SOUPS '13, ACM, New York, NY, USA (2013)
44. Sheng, S., Broderick, L., Koranda, C.A., Hyland, J.J.: Why Johnny still can't encrypt: Evaluating the usability of email encryption software. In: Symposium On Usable Privacy and Security (2006)
45. Solove, D.J.: I've got nothing to hide and other misunderstandings of privacy. San Diego L. Rev. 44, 745 (2007)
46. Van Vleck, T.: Electronic mail and text messaging in CTSS, 1965-1973. Annals of the History of Computing, IEEE 34(1), 4–6 (2012)
47. Volkamer, M., Renaud, K.: Mental models - general introduction and review of their application to human-centred security. Lecture Notes in Computer Science. Papers in Honor of Johannes Buchmann on the Occasion of his 60th Birthday (8260), 255–280 (2013)
48. Wash, R.: Folk Models of Home Computer Security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security. pp. 11:1–11:16. SOUPS '10, ACM, New York, NY, USA (2010)

49. Wästlund, E., Angulo, J., Fischer-Hbner, S.: Evoking comprehensive mental models of anonymous credentials. In: Camenisch, J., Kesdogan, D. (eds.) iNetSeC. Lecture Notes in Computer Science, vol. 7039, pp. 1–14. Springer (2011)
50. Whitten, A., Tygar, J.D.: Why Johnny cant encrypt: A usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium. vol. 99. McGraw-Hill (1999)
51. Williams, M.: Interpretivism and generalisation. Sociology 34(2), 209–224 (2000)
52. Woo, W.K.: How to Exchange Email Securely with Johnny who Still Can't Encrypt. Master's thesis, University of British Columbia (2006)