Evaluating ambiguity of privacy indicators in a secure email app

Borce Stojkovski and Gabriele Lenzini[1]

Interdisciplinary Centre for Security, Reliability and Trust (SnT)
University of Luxembourg
name.surname@uni.lu

Abstract

Informing laymen of security situations is a notoriously hard problem. Users are usually not cognoscenti of all the various secure and insecure situations that may arise, and this can be further worsened by certain visual indicators that instead of helping users, fail to convey clear and unambiguous messages. Even in well established and studied applications, like email clients providing end-to-end encryption, the problem seems far from being solved. Motivated to verify this claim, we studied the communication qualities of four privacy icons (in the form of coloured shapes) in conveying specific security messages, relevant for a particular secure emailing system called p≡p. We questioned 42 users in three different sessions, where we showed them 10 privacy ratings, along with their explanations, and asked them to match the rating and explanation with the four privacy icons. We compared the participants' associations to those made by the p≡p developers.

The results, still preliminary, are not encouraging. Except for the two most extreme cases, *Secure and trusted* and *Under attack*, users almost entirely missed to get the indicators' intended messages. In particular, they did not grasp certain concepts such as *Unsecure email* and *Secure email*, which in turn were fundamental for the engineers. Our work has certain limitations and further investigation is required, but already at this stage our research calls for a closer collaboration between app engineers and icon designers. In the context of p≡p, our work has triggered a deeper discussion on the icon design choices and a potential revamp is on the way.

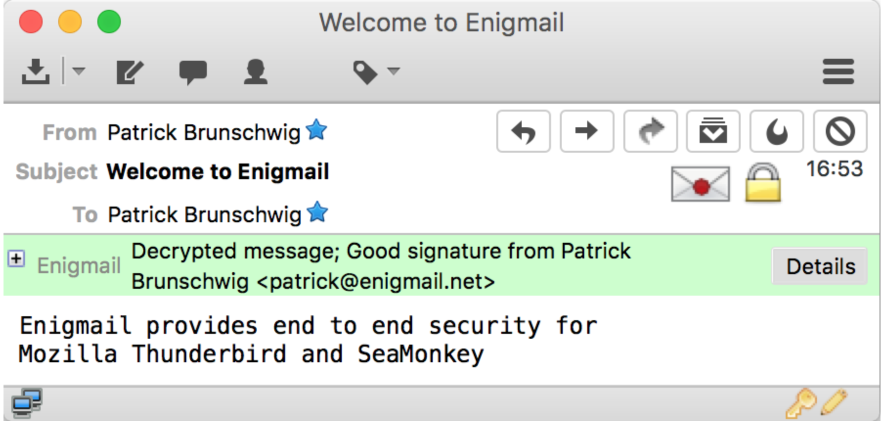
1 Introduction

This work reports on preliminary research where we questioned how users understand *security indicators*—either used independently, or alongside text labels, or with explanations—that are shown in an email application that offers end-to-end encryption[1].

Security indicators are graphical clues or icons that, in secure email apps, are reserved to tell users about two specific concepts: *confidentiality* of a message, meaning that an email is or has been encrypted, and *authenticity and integrity*, meaning that the message is coming from a trusted party, that is, from a party whose public key we hold and trust. Different choices exist to express those concepts either in their positive and in their negative variants (e.g. violation of confidentiality, untruthfulness of a party, and lack of any knowledge on the matter), but there is no uniformity in how different apps should graphically convey those messages.

We investigate the question in the context of "Pretty Easy Privacy"[2](p≡p), a relatively new secure email app that attempts to deploy a traffic-light semantic as a "clear and easily understandable presentation" of the different privacy states that messages and communication peers can have[16]. The design choices regarding the indicators within p≡p diverge from those

[1] We will call such applications "secure email apps", or "secure emails"
[2] https://www.pep.security/



Welcome to Enigmail

From Patrick Brunschwig

Subject **Welcome to Enigmail**

To Patrick Brunschwig

16:53

Enigmail Decrypted message; Good signature from Patrick Brunschwig <patrick@enigmail.net>

Enigmail provides end to end security for Mozilla Thunderbird and SeaMonkey

Figure 1: Enigmail security indicators

of other applications, and how this reflects on users has not been studied before. Furthermore, other secure email apps also differ from one another. Overlooking that Lausch *et al.* [15] discuss that an "envelope" in various conditions (e.g. broken, closed, open) is a better metaphor than a "padlock" in its various forms (e.g. open or closed, and red or green-coloured), applications opt for their own security icons and metaphors—for instance, the popular open-source Enigmail[3] for Thunderbird uses padlocks for confidentiality and sealed envelopes for authentication and integrity (see Figure 1). The reasoning underpinning choices is often not explicitly stated.

1.1 The hard quest for good security indicators

The lack of standards is surely not helping secure email designers to converge in choosing the same security indicators. Part of the problem is the considerable amount of different situations that arise when talking about email confidentiality, authenticity, and integrity: distinguishing and representing all of them with icons, or with a combination of icons, does not have any obvious solutions.

Even the choice of what is the right metaphor is unclear and, at least in the end-to-end encryption case, it seems that metaphors do not help users understand the real functionality of an application [3]. Thus, designers find themselves in the difficult position to either simplify the message, at risk of paternalizing users (= not letting them be in control), or deliver a fully fledged description, at risk of confusing them.

Recently the situation may have gotten worse. The General Data Protection Regulation (GDPR) suggests the use of icons in order to give a meaningful overview of the intended processing in an *"easily visible, intelligible and clearly legible manner"* (Art. 12.7) [8]. The GDPR has renewed a general interest in security indicators. While most of them are variants of padlocks and shields, many others are new, and more are expected to be proposed in response to the GDPR call.

Without a common agreement on what security icons to use and in which circumstances, having a large pool of icons to choose from may actually confuse app designers and users alike. For example, research on security indicators in the context of web browsers, which has been an active research area for almost two decades [4, 12], cautions that people don't always

[3] https://www.enigmail.net

understand security indicators. In contrast to the pictograms of bio or chemical hazards, which are standardized internationally by the Globally Harmonized System [17], at the moment there is no equivalent agreement that can characterize what security 'hazards' are and how they can be represented.

And, unlike written texts for which tests of understandability exist, icons do not have an accepted intelligibility test. Thus, secure email engineers have to find their ways without clear guidelines and instruments for the design of security indicators.

Even in the case of security applications that have been available for decades, like secure email apps, there is still room for improvement. Our investigation brings up some data that can revive a discussion about the pros and cons of certain design choices in this application domain. By shedding light on the use of the traffic-light semantic within a new system that aspires to bring "crypto to the masses", our work contributes to the discourse on the usability and effectiveness of security and privacy indicators, which in the secure email context has received relatively little attention.

2 Background and Research Questions

p≡p is an opportunistic peer-to-peer end-to-end encryption software which tries to unburden users from managing their encryption keys. p≡p automatically generates user keys, appends the public key to each outgoing message, and extracts and stores keys from incoming messages. Messages are automatically encrypted and decrypted. Peers can be verified to be authentic by a second-channel out-of-bound communication, e.g. a phone call where the peers verify a human-friendly version of their fingerprint; this version is a sequence of easily readable words, called *trustwords*, taken from a dictionary according to an index that depends on the combination of the two peers' fingerprints.

Depending on several factors, each communication channel to different peers may have a different privacy status. For example, the system can independently and automatically categorise a particular message as *reliable* whenever it can be encrypted or decrypted with sufficient cryptographic parameters. However, the system cannot independently categorise the message as *trusted* unless the user carries out a p≡p handshake and confirms to trust the sender in the p≡p interface.

Internally, p≡p distinguishes among 13 situations which are surjectively mapped into *colour codes*

(chosen according to a traffic light semantics), *privacy rating labels*, as well as corresponding *privacy rating explanations* [16]. Table 1 provides an overview of the different internal ratings, codes and labels. Table 2 provides an overview of how these ratings are currently displayed in the user interface of p≡p for Thunderbird.

For instance, the p≡p rating *"mistrust"* is assigned the colour code *"red"*, the user interface label *"Mistrusted"*, and explanation *"This message has a communication partner that has previously been marked as mistrusted"*.

In addition, p≡p uses *privacy indicators* which are icons from an icon set made up of four coloured shapes (e.g. see Figure 2 and Figure 3) corresponding to the colour code assigned to each situation. *"Under Attack"*, *"Broken"*, and *"Mistrusted"* are the situations represented by a red square, for instance. The rating codes from *0* to *5* are not assigned any colour label, however, in the user interface, these codes are represented by a gray circle. Reliable communication (i.e. rating code *6*) is represented using a yellow shape, and trusted communication (i.e. colour code *7*) is represented with a green shape.

Rating Code	Rating Label	Colour code	Colour Label
-3	under attack	-1	red
-2	broken	-1	red
-1	mistrust	-1	red
0	undefined	0	no colour
1	cannot decrypt	0	no colour
2	have no key	0	no colour
3	unencrypted	0	no colour
4	unencrypted for some	0	no colour
5	unreliable	0	no colour
6	reliable	1	yellow
7	trusted	2	green
8	trusted and anonymized	2	green
9	fully anonymous	2	green

Table 1: Overview of the internal privacy rating codes, colour codes, and labels

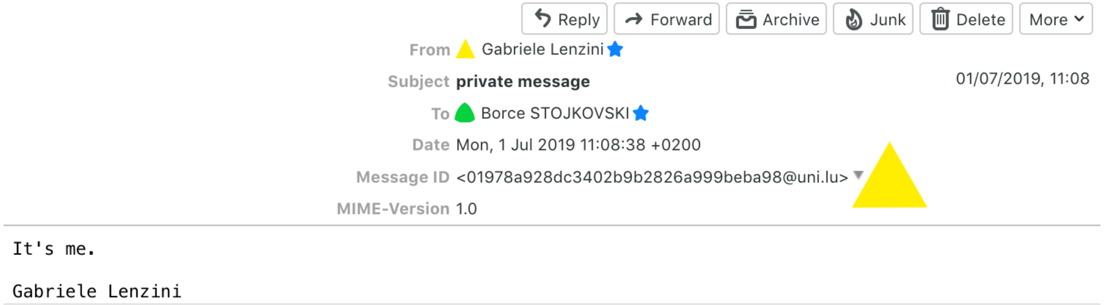
Rating Code	User Interface Label	User Interface Explanation
-3	Under Attack	This message is not secure and has been tampered with.
-2	Broken	This message has broken encryption or formatting.
-1	Mistrusted	This message has a communication partner that has previously been marked as mistrusted.
0	Unknown	This message does not contain enough information to determine if it is secure.
1	Cannot Decrypt	This message cannot be decrypted because the key is not available.
3	Unsecure	This message is unsecure.
4	Unsecure for Some	This message is unsecure for some communication partners.
5	Unreliable Security	This message has unreliable protection.
6	Secure	This message is secure but you still need to verify the identity of your communication partner.
7	Secure & Trusted	This message is secure and trusted.

Table 2: Overview of the privacy ratings as displayed in the UI of p≡p for Thunderbird

The design choice of p≡p's privacy icons is justified by arguments, but not by evidence. While discussing with the p≡p developers, we were told that the shapes are meant to be easily understood by colour-blind persons, and were suggested after consultation with experts. The colour choices are meant to reflect the universally-deployed traffic light semantic.

There are many interesting questions that could be investigated, such as, how to draw user attention to these indicators; where to display those icons in the user interface; what situations do such shapes suggest to users; are shapes better than conventional icons (e.g. envelopes), etc.

Nevertheless, here we conduct an enquiry into the most basic question of "how would



From Gabriele Lenzini

Subject **private message** 01/07/2019, 11:08

To Borce STOJKOVSKI

Date Mon, 1 Jul 2019 11:08:38 +0200

Message ID <01978a928dc3402b9b2826a999beba98@uni.lu>

MIME-Version 1.0

```
It's me.

Gabriele Lenzini
```

Figure 2: p≡p for Thunderbird, privacy indicators

prospective or first-time p≡p users understand the p≡p privacy indicators". Formally stated, we intend to shed light on the following research questions:

1. Which of the 4 visual icons do users associate with the different p≡p privacy ratings?

2. Which of the 4 visual icons do users associate with the different p≡p privacy rating explanations?

3 Methodology

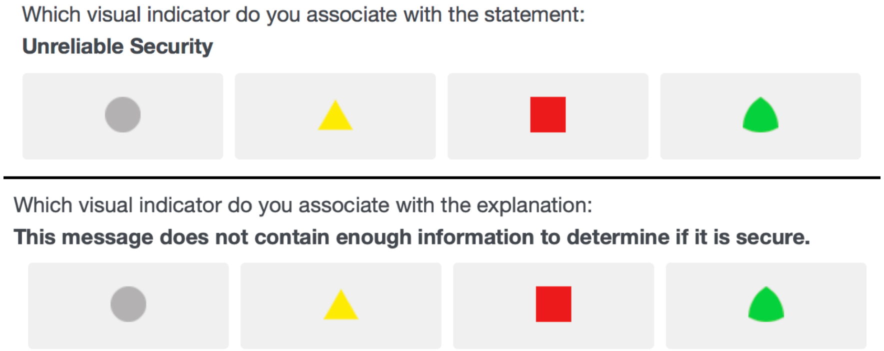
We conducted three online studies to assess how people would interpret the various privacy rating indicators offered by the p≡p email encryption system. Table 3 provides an overview of the user test sessions, the number of participants per session as well as the focus of investigation.

	Privacy Ratings	**Privacy Rating Explanations**	**Number of Participants**
Session 1	×		16
Session 2	×	×	12
Session 3	×	×	14
Total evaluations	42	26	

Table 3: User Test Sessions

3.1 Study structure

The first part of the study contained a block of 10 questions which asked participants to choose an icon which according to them best corresponds to a given privacy statement i.e. rating (see Figure 3 upper part for an example). The second part of the study similarly asked the participants to match an icon to a privacy rating explanation (see Figure 3 lower part). The last part of the study asked about demographics. The 10 privacy rating statements and explanations were drawn from the p≡p for Thunderbird distribution (Enigmail/p≡p version 2.0.12 (20190707-1417). To minimize order bias, the sequence of all questions per block was



Which visual indicator do you associate with the statement:
Unreliable Security

Which visual indicator do you associate with the explanation:
This message does not contain enough information to determine if it is secure.

Figure 3: Sample questions asking participants to choose the icon which according to them best corresponds to a privacy statement i.e. rating (*upper question*), and a privacy rating explanation (*lower question*)

randomized for each test participant. The order of all answer choices (icons) per question was also randomized. The studies were administered via Qualtrics[4].

3.2 Participants

All participants are relatively tech-savvy, with at least a Bachelor's degree. The participants of Session 1 and 2 are based in Luxembourg and were recruited at the University of Luxembourg via an email invitation to participate in a pilot study (Session 1) and during a lecture on Security Engineering (Session 2). No incentive was offered to the participants of Sessions 1 and 2. The participants of Session 3 are based in different European countries and were recruited in Portugal during a workshop on User Experience in security and privacy-critical systems. As a compensation for their participation in the study, all participants of Session 3 were offered a commercial license of p≡p for continued use of their paid apps i.e. the Outlook and Android distributions.

3.3 Analysis

We performed a comparative analysis to understand if our participants associated icons to the various privacy ratings and explanations in the same way as implemented by p≡p. If the icon chosen by the majority of participants is the same as the one chosen by p≡p, the alignment test for that rating or explanation equals *"MATCH"*, and otherwise *"NO MATCH"*.

The *Match strength* refers to how many participants selected the same icon as p≡p. Hence, the higher the match, the narrower the gap between what the developers wanted to communicate via the system and what the users understood. Similarly, the lower the match, the higher the ambiguity of the intended privacy indicator.

[4] https://www.qualtrics.com

4 Results

Figure 4 summarizes the participant responses, detailing the distribution of votes per icon for each rating statement and explanation. The distribution under the most voted icon by the participants is formatted in bold letters. The number of people that have voted for the same icon as currently implemented in p≡p is underlined. Hence, in case of a *match*, the distribution of the icon is formatted as bold and underlined.

These preliminary results highlight profound differences in what p≡p tries to convey to users in terms of the security and privacy rating of messages and how prospective or first-time p≡p users would interpret those ratings. The icon displayed by p≡p matches the association made by the test participants in only 4 out of 10 cases. When it comes to rating explanations, there is a match only in 3 out of 10 cases. There is additionally the internal inconsistency in the case of Items 2, 4 and 9 where either the statement or the corresponding explanation match the icon choice, and not both.

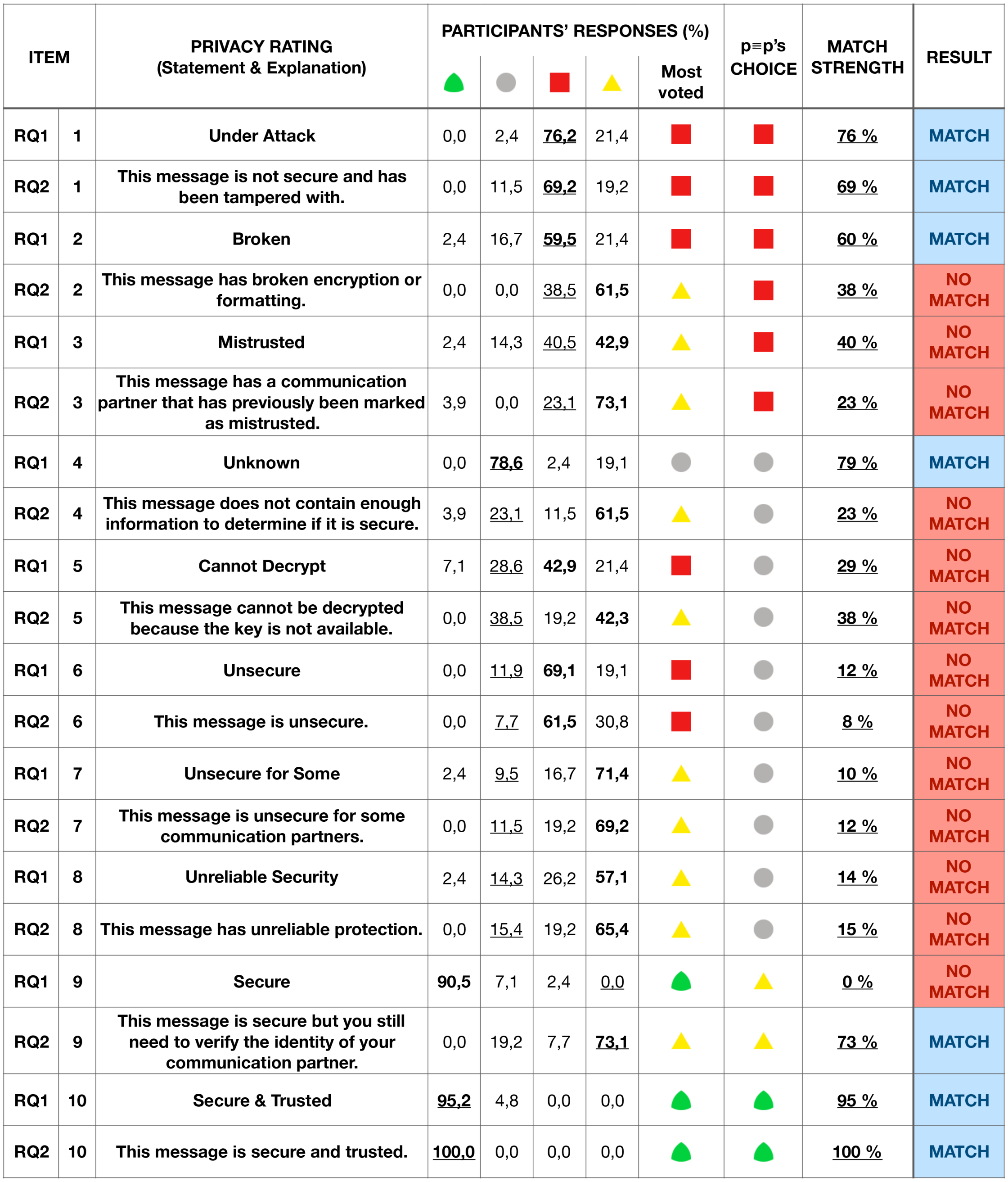
While we notice a strong alignment between the p≡p and participants' choice in the case of a fully secure rating (Item 10), the alignment is less strong on the other end of the spectrum (Items 1 and 2). In all other cases (except for Item 4) the associations people make are different from the intentions of the designer. This is even more worrying given the fact such indicators will very likely be shown before the ones on the extremes of the rating spectrum (e.g. existing email messages or those received/sent unencrypted after installing p≡p have the privacy rating "Unsecure").

The match strength is the lowest (=0%) in the case of RQ1-Item 9. The results suggest that if p≡p displayed a yellow triangle as a visual indicator of a privacy rating for a message, no prospective or first-time user would associate it with a "Secure" status, which is contrary to what p≡p tries to communicate. This is probably not too surprising given our constant pattern recognition efforts [10] in combination with the ubiquity of the triangle in hazard alerting or warning symbols [21]. Unfortunately, without a deeper understanding of how secure email works or additional context, such as an explanation (RQ2-Item 9), it is hard to foresee why p≡p is trying to denote that the message is "Secure", yet cautiously.

5 Discussion

Understanding why there is a dichotomy between what the developers wanted to convey with the different privacy indicators in p≡p and how prospective users would interpret them, or which privacy indicators could be better in narrowing this chasm, is not in the scope of this investigation. Nevertheless, we hypothesize that the following elements potentially play a role:

- the shapes of the indicators
- the colours of the indicators
- the traffic light metaphor used for the indicators
- the choice of words in the statements and explanations
- the perception of risk associated with the shapes, colours, metaphor and wordings of the indicators
- the clustering of risks
- the understandability of the indicators
- the awareness and concern about different scenarios and privacy ratings



ITEM		PRIVACY RATING (Statement & Explanation)	PARTICIPANTS' RESPONSES (%)					p≡p's CHOICE	MATCH STRENGTH	RESULT
			🟢	●	🟥	▲	Most voted			
RQ1	1	Under Attack	0,0	2,4	**76,2**	21,4	🟥	🟥	**76 %**	MATCH
RQ2	1	This message is not secure and has been tampered with.	0,0	11,5	**69,2**	19,2	🟥	🟥	**69 %**	MATCH
RQ1	2	Broken	2,4	16,7	**59,5**	21,4	🟥	🟥	**60 %**	MATCH
RQ2	2	This message has broken encryption or formatting.	0,0	0,0	38,5	**61,5**	▲	🟥	**38 %**	NO MATCH
RQ1	3	Mistrusted	2,4	14,3	40,5	**42,9**	▲	🟥	**40 %**	NO MATCH
RQ2	3	This message has a communication partner that has previously been marked as mistrusted.	3,9	0,0	23,1	**73,1**	▲	🟥	**23 %**	NO MATCH
RQ1	4	Unknown	0,0	**78,6**	2,4	19,1	●	●	**79 %**	MATCH
RQ2	4	This message does not contain enough information to determine if it is secure.	3,9	23,1	11,5	**61,5**	▲	●	**23 %**	NO MATCH
RQ1	5	Cannot Decrypt	7,1	28,6	**42,9**	21,4	🟥	●	**29 %**	NO MATCH
RQ2	5	This message cannot be decrypted because the key is not available.	0,0	38,5	19,2	**42,3**	▲	●	**38 %**	NO MATCH
RQ1	6	Unsecure	0,0	11,9	**69,1**	19,1	🟥	●	**12 %**	NO MATCH
RQ2	6	This message is unsecure.	0,0	7,7	**61,5**	30,8	🟥	●	**8 %**	NO MATCH
RQ1	7	Unsecure for Some	2,4	9,5	16,7	**71,4**	▲	●	**10 %**	NO MATCH
RQ2	7	This message is unsecure for some communication partners.	0,0	11,5	19,2	**69,2**	▲	●	**12 %**	NO MATCH
RQ1	8	Unreliable Security	2,4	14,3	26,2	**57,1**	▲	●	**14 %**	NO MATCH
RQ2	8	This message has unreliable protection.	0,0	15,4	19,2	**65,4**	▲	●	**15 %**	NO MATCH
RQ1	9	Secure	**90,5**	7,1	2,4	0,0	🟢	▲	**0 %**	NO MATCH
RQ2	9	This message is secure but you still need to verify the identity of your communication partner.	0,0	19,2	7,7	**73,1**	▲	▲	**73 %**	MATCH
RQ1	10	Secure & Trusted	**95,2**	4,8	0,0	0,0	🟢	🟢	**95 %**	MATCH
RQ2	10	This message is secure and trusted.	**100,0**	0,0	0,0	0,0	🟢	🟢	**100 %**	MATCH

Figure 4: Results of the preliminary investigation of alignment between participants' associations of p≡p privacy ratings, explanations and visual icons against the actual associations as implemented in several applications of p≡p.

(For each item, the match strength refers to the percentage of participants that associated an icon to a statement or explanation in the same fashion as it is currently implemented by p≡p.)

It is often the case that visual input tends to dominate other modalities when it comes to our perceptual and memorial judgements [18]. Colour is one of the characteristics of human visual perception that can carry important meaning and can have an important impact on people's affect, cognition, and behaviour [6]. According to Elliot & Maier's colour-in-context theory [5], some colour meanings and effects are biologically-based, while others are posited to stem from the repeated pairing of colour and particular concepts, messages, and experiences. They state that observing colour-meaning associations over time and cultures can contribute to reinforcing and extending the applicability of those links to objects in the broader environment, such as signs and signals. We did not have the opportunity to perform this investigation with existing p≡p users. We would be interested in comparing such results with the current findings and looking at the role of experience with the system on the interpretation of the privacy ratings and indicators.

Disregarding some regional variations, traffic signs and traffic lights are now found all over the world, and their meaning is internationally recognizable. The corresponding traffic light rating system (*red, amber, green*) is something we have repurposed in many different domains, from nutrition labels for pre-packed products [22] to energy consumption labeling [9] and project management status reporting [7], to name a few. In that respect, the provision of the traffic light colour codes can serve to communicate more accurate, relevant, and comparable information to users, as well as to transmit certain levels of risk or allow for a quick recognition of potential hazards.

Nevertheless, while signs and pictograms have been standardized in specific areas, in many different contexts harmonized communication or a shared understanding of the risk communicated by signs, symbols, or colours cannot be taken for granted [21]. The reasons can range from cross-cultural differences [14] to varying levels of technical expertise within a specific domain. Research on human aspects in the context of end-to-end email encryption suggests that non-expert users have incomplete threat models and a general absence of understanding of the email architecture [19]. As expressed in Section 1, the number of different situations that arise in secure email is not so small. Deciding which ones and how many to represent graphically, as well as, which metaphor to use, is not an easy choice. There is probably not a straightforward answer and there is definitely not a unique one. There are differing views about how transparent should systems for end-to-end email encryption be [1], [20]. In the case of Item 9, it is evident that p≡p attempts to find the balance between these two approaches: on the one hand they would like to instill a sense of security provided by the automatic end-to-end encryption akin to other secure messaging and emailing systems, but on the other hand, they would still like to warn the user of potential threats such as a man-in-the-middle attack that they could be susceptible to if they do not verify the corresponding party via a second secure channel (e.g. by comparing the trustwords in person or over the phone).

While over time, we are likely going to recognize more consistency in the symbols used by security and privacy-critical systems, widely-available UI kits or even standardized icon sets, in the immediate term, developers of such systems should devote an equal amount of attention and resources to understanding their (target) users and the different dimensions and requirements of their socio-technical proposition. As a starting point, developers, and especially teams without user research/UX profiles, should inform themselves of the general paradigms and design principles that align security and usability [23, 13], followed by more recent lessons learnt in this highly-challenging domain that brings together the usable security, HCI and UX disciplines. Fine-grained inspiration could perhaps be drawn from the vast body of work on browser security indicators and warnings (e.g. [11]), in particular, the incremental user-centred approach where proposed designs and changes were validated with thousands of users. Caplin's book [2] could potentially be a useful reference to some developers in the specific context of icons in computer interface design, however, as pointed out by Felt et al. ”Millions of Internet users have recently come online via smartphones without learning ’standard’ iconography from desktop browsers” [11], thus it is important to acknowledge that the expectations of users in terms of interfaces are not necessarily associated with desktop computing and, in many cases, obsolete metaphors.

6 Conclusion and Future Work

We reported on a 42-participant study of users’ perceptions of email privacy ratings in the context of pretty Easy privacy. Although our preliminary study has an evident limitation mainly due to the limited sample size, the outcome suggests that prospective or first-time p≡p users would have a difficulty understanding the privacy information communicated by p≡p.

The findings call for a broader and deeper investigation that would seek to assert which design choices in terms of the privacy rating statement, explanation and visual icon (shape, colour, metaphor etc.) would need to be reconsidered if p≡p would like to accurately communicate the degree of protection that it offers to its users as they send and receive email through its system bearing in mind their experience, awareness and concerns. Our work has triggered a deeper discussion at p≡p on the existing icon design choices and a potential overhaul of the privacy indicators is being deliberated.

From a broader perspective we believe that further and more holistic analyses of the different secure communication systems would be needed in order to identify the different types and degrees of security information communicated by those systems, the effectiveness of the deployed security and privacy indicators as well as their suitability for target audiences with different characteristics and levels of expertise.

We are of the opinion that despite looking trivial, this interaction experience should not be in the way of users adopting systems for end-to-end email encryption, let alone a source of confusion or frustration that could result in unsecure behavior or unwanted leakage of confidential information. This is particularly relevant within an organizational setting, where policy and culture may also contribute towards the way users go about employing end-to-end email encryption.

7 Acknowledgments

Authors are supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared, and the project pEp Security SA / SnT “Protocols for Privacy Security Analysis”. We would like to thank the p≡p team for their collaboration, input and feedback in this project, as well as, the participants of the Human-centered cybersecurity workshop at CHItaly 2019 for the fruitful discussions. Last but not least, we would like to thank the anonymous reviewers at ITASEC 2020 for their comments and suggestions for improvement.

References

[1] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. Leading Johnny to Water: Designing for Usability and Trust. pages 69–88. USENIX Association, 2015.

[2] Steve Caplin. *ICON Design: Graphic Icons in Computer Interface Design.* Watson-Guptill Publications, Inc., USA, 2001.

[3] Albese Demjaha, Jonathan Spring, Ingolf Becker, Simon Parkin, and M Angela Sasse. Metaphors considered harmful ? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. (February):1–12, 2018.

[4] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 581–590, New York, NY, USA, 2006. ACM.

[5] Andrew J Elliot and Markus A Maier. Chapter two - Color-in-Context Theory. volume 45 of *Advances in Experimental Social Psychology*, pages 61–125. Academic Press, 2012.

[6] Andrew J Elliot and Markus A Maier. Color Psychology: Effects of Perceiving Color on Psychological Functioning in Humans. *Annual Review of Psychology*, 65(1):95–120, jan 2014.

[7] C. N. Enoch and L. Labuschagne. Project portfolio management: using fuzzy logic to determine the contribution of portfolio components to organizational objectives. Paper presented at PMI® Research and Education Conference, Limerick, Munster, Ireland. Project Management Institute, Newtown Square, PA, 2012.

[8] EU. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*, L119:1–88, 2016.

[9] EU. Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (Text with EEA relevance.). *Official Journal of the European Union*, L198:1–23, 2017.

[10] Michael W Eysenck. Cognitive psychology : a student's handbook, 2015.

[11] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, Sunny Consolvo, and U C Berkeley. Rethinking Connection Security Indicators. *the Symposium On Usable Privacy and Security (SOUPS)*, (Soups):1–14, 2016.

[12] Batya Friedman, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. Users' conceptions of web security: A comparative study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '02, pages 746–747, New York, NY, USA, 2002. ACM.

[13] Simson L. Garfinkel. *Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable*. PhD thesis, Massachusetts Institute of Technology, 2005.

[14] Ralph B Hupka, Zbigniew Zaleski, Jurgen Otto, Lucy Reidl, and Nadia V Tarabrina. The Colors of Anger, Envy, Fear, and Jealousy: A Cross-Cultural Study. *Journal of Cross-Cultural Psychology*, 28(2):156–171, 1997.

[15] Joscha Lausch, Oliver Wiese, and Volker Roth. What is a Secure Email? *EuroUSEC 2017*, 2017.

[16] Hernâni Marques and Bernie Hoeneisen. pretty Easy privacy (pEp): Mapping of Privacy Rating, 2019. IETF Internet-Draft, https://tools.ietf.org/html/draft-marques-pep-rating-01, Accessed: 30 June 2019.

[17] United Nations. *Globally harmonized system of classification and labelling of chemicals (GHS) - sixth revised edition*. 2015. Accessed: 30 June 2019.

[18] Michael I. Posner, Mary J. Nissen, and Raymond M. Klein. Visual dominance: An information-processing account of its origins and significance. *Psychological Review*, 83(2):157–171, 1976.

[19] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why Doesn't Jane Protect Her Privacy? In Emiliano De Cristofaro and Steven J Murdoch, editors, *Privacy Enhancing Technologies*, pages 244–262, Cham, 2014. Springer International Publishing.

[20] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. "We'Re on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. CHI '16, pages 4298–4308. ACM, 2016.

[21] Tonya L Smith-Jackson and Michael S Wogalter. Users' hazard perceptions of warning components: An examination of colors and symbols. *Proceedings of the Human Factors and Ergonomics Society*

Annual Meeting, 44(32):6–55–6–58, 2000.

[22] UK Department of Health and Social Care. Guide to creating a front of pack (FoP) nutrition label for pre-packed products sold through retail outlets, 2013.

[23] Ka-Ping Yee. Aligning security and usability. *IEEE Security & Privacy*, 2(5):48–55, 2004.