Poster: Mental Models – User understanding of messaging and encryption

Alena Naiakshina[1], Anastasia Danilova[1], Sergej Dechand[1], Kat Krol[2], M. Angela Sasse[2] and Matthew Smith[1]
[1] University of Bonn, Germany, {naiakshi, danilova, dechand, smith}@cs.uni-bonn.de
[2] University College London, UK, {k.krol, a.sasse}@cs.ucl.ac.uk

***Abstract*—The surveillance revelations of 2013 have led to an increased interest in secure messaging. While widely adopted apps such as WhatsApp claim to have added certain security features, only limited detailed information is publicly available. On the other hand, open-source messaging apps such as Signal are more transparent and provide extended security and privacy features. However, relatively small user bases of open-source messaging apps might indicate that these solutions are less attractive to users. Our research explores users' mental models of the security of mobile messaging tools, focusing on SMS and WhatsApp in particular. We study users' threat models and their general understanding of security and privacy features. Our results suggest that users have an exaggerated threat model and assume attackers have high capabilities. Most of our participants were aware of encryption. However, while students of computer science were able to explain public-key encryption, laypeople were at most able to imagine symmetric encryption. Furthermore, most participants struggled with the concept of authenticity, for example, by assuming that encryption already provides authenticity and integrity.**

Keywords*—*Mental Model, Focus Groups, Secure Messaging.

I. Introduction

The 2013 revelations on mass surveillance have led the general public to be more concerned about government surveillance [1], [2]. However, email and the most widely adopted messaging apps such as WhatsApp or iMessage do not offer fully transparent end-to-end security. Even though various protocols such as OpenPGP and secure messaging extensions such as OTR have been available for decades, they have not been universally adopted. Previous work under the "Why Johnny can't encrypt" theme has also shown that users struggle with available email encryption software [3]–[5]. In general, secure solutions have been shown to provide poor user experience [6]. Even studies with target groups like journalists indicate that secure messaging protocols are rarely used [7].

In existing research, there is a paucity of studies that would explore how exactly users understand encryption and mobile messaging in general. In order to address this gap, our study is investigating users' understanding and perceptions of mobile messaging architecture and its security.

Renaud et al. [6] investigated the low uptake of end-to-end encryption for email security. Besides the usability issues illustrated elsewhere [3]–[5], the authors proposed further plausible explanations. In order to evaluate their hypotheses, Renaud et al. extracted laypeople and expert mental models of email architecture and email security. In contrast to this previous work, we let our participants explain their perceptions and choices by themselves rather than explaining prevalent facts. Additionally, instead of conducting structured interviews based on assumptions by experts, our pilot study comprised of multiple iterations by using focus groups in order to design appropriate questions for follow-on interviews [8]. By contrast, the findings of our research suggest that users are aware of encryption and their mental models suggest that they often have a high-level understanding of the mobile messaging architecture *and* security features. We also observed that participants with different levels of computer literacy had different mental models. Those with high computer literacy were holding reasonably accurate and comprehensive mental models of security, whereas those with low computer literacy were at most able to imagine symmetric encryption. Instead of improving the usability of public key encryption or hiding it altogether, we suggest developers could consider average users' mental models. Further, participants had little confidence that providers' were offering secure services. Therefore, systems could be built to tap into users' existing perceptions to create trust. For example, one could simulate symmetric encryption using *passwords or codes* provided by the user.

II. Methodology

Mental models are abstractions of users' representations of a complex system, encompassing perceptions and related explanations [9]. In order to gain insight into user perceptions of mobile messaging and its security, we used a combination of two methods: drawings with a think-aloud exercise and semi-structured focus groups. *Focus groups* are a long-standing methodology for collecting qualitative data [10]. In a study session using focus group methodology, a skilled moderator leads an interactive group discussion with several participants using a carefully predetermined guideline [8]. Focus groups are a popular and valued methodology in the field of human-computer interaction and usability testing [11], [12].

In our study, we constructed a guideline for conducting focus groups in a way to first build an understanding of users' mental models behind communication using mobile devices and then addressing the security of communication, defined as confidentiality and authenticity. The questions were open-ended to encourage participants to explain their understanding using their own words. Additionally, a sketch with two individuals with white space in-between was handed out to the groups. Participants were asked to draw the stations their messages go through, explain where they thought their communication might be eavesdropped on and how security fits into the process. We asked participants to compare SMS with WhatsApp which was chosen as an example of a messaging app due to its popularity in Germany. The participants in the first focus group were in the beginning of their undergraduate studies in computer science with an average age of 21. Our second focus group comprised of students of non-technical degrees (e.g., architecture, English) with an average age of 24. For the third group, we recruited participants with no academic background (i.e., no university degree) with the higher average age of 47.

III. Results & Discussion

Our preliminary findings show that although the participants of all focus groups were of different backgrounds, they shared some basic mental models. Most of our participants appeared to be sceptical about the security of mobile messaging. They believed that almost anyone is able to eavesdrop on their messages at any station if someone (organisations or individuals) are determined enough or have the capabilities to do so. Although all participants stated having security concerns, they used untrusted services on their mobile phones. To mitigate this, a number of participants reported avoiding sending sensitive content using mobile phones. Instead, they would rather meet in person or switch to email contradicting their own statements about Internet protocols being less secure in comparison to "traditional" communication systems. They reported several reasons for this behaviour: some participants did not know the technologies behind SMS and WhatsApp at all while others did not know how to protect their messages from being eavesdropped on. Most participants reported being concerned about WhatsApp and its security and privacy, but had not switched to secure messaging apps. Nevertheless, they stated they would be willing to adopt a secure messaging app if more of their contacts were using them.

All participants mentioned encryption when asked how eavesdropping can be prevented although some participants believed that even encryption can be broken by various adversaries such as intelligence services. More importantly, the majority of participants in the second and third focus group (with students of non-technical subjects and those without an academic background respectively) were not familiar with public-key cryptography. The only concept they were able to explain involved using passwords and symmetric encryption. In general, authenticity and integrity seemed to be difficult concepts for less computer literate participants. The participants from the second focus group were not aware of additional security properties besides confidentiality. They assumed that an exchanged password, key or "code" is uniquely assigned to a person when encryption is used: "otherwise, the sender would not be able to encrypt the messages correctly". However, participants understood the threat that might arise from a man-in-the-middle attack when it was explained to them in a simple scenario in the third focus group. We believe that providing participants with a simple scenario might help inform and improve their mental models.

An interesting idea mentioned by the participants from the second group was the usage of mobile phone numbers in the registration process of WhatsApp. Only users with the corresponding SIM card are able to use the WhatsApp account of a registered mobile number. Participants perceived this as having control. In contrast, participants in the focus group with computer scientists stated that phone numbers can easily be controlled by professional attackers. All participants mentioned intelligence services, especially the NSA, but also governments in general as potential adversaries.

Our focus groups provided first insights into users' mental models of mobile messaging security. Due to our choice of focus groups as methodology, our results could be biased due to dominant individuals influencing the views of other participants. Although we tried to minimise this bias by recruiting participants of similar backgrounds for each group, we could not prevent some participants influencing the views of others. Therefore, we are currently in the process of conducting single interviews where each participant has the chance to come up with their own ideas and explain their mental models in more detail. The results of the focus groups have provided us with a good basis to refine the questions we ask.

As future work, we are planning to explore the mental models users hold in different countries. To this end, we plan to conduct single interviews with participants recruited from the US and the UK in addition to the interviews already in progress in Germany. The expectation is that mental models could differ because of people's different attitudes towards and perceptions of security and privacy, their government and companies.

References

[1] M. Schulze, "Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal," *Surveillance & Society*, vol. 13, no. 2, p. 197, 2015.

[2] M. Madden. (2014) Public Perceptions of Privacy and Security in the Post-Snowden Era. [Online]. Available: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

[3] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *USENIX Security*, 1999.

[4] S. L. Garfinkel and R. C. Miller, "Johnny 2: A user test of key continuity management with S/MIME and Outlook Express," in *Symposium on Usable Privacy and Security (SOUPS)*, 2005, pp. 13–24.

[5] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why Johnny still can't encrypt: Evaluating the usability of email encryption software," in *Symposium On Usable Privacy and Security*, 2006.

[6] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why Doesn't Jane Protect Her Privacy?" in *Privacy Enhancing Technologies*. Springer, 2014, pp. 244–262.

[7] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists," in *USENIX Security*, 2015, pp. 399–414.

[8] D. L. Morgan, "Focus groups," *Annual review of sociology*, pp. 129–152, 1996.

[9] D. Jonassen and Y. H. Cho, "Externalizing mental models with mindtools," in *Understanding models for learning and instruction*. Springer, 2008, pp. 145–159.

[10] D. L. Morgan, *Focus groups as qualitative research*. Sage publications, 1996, vol. 16.

[11] S. Kurniawan, M. Mahmud, and Y. Nugroho, "A study of the use of mobile phones by older persons," in *CHI'06 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2006, pp. 989–994.

[12] G. Eysenbach and C. Köhler, "How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews," *BMJ*, vol. 324, no. 7337, pp. 573–577, 2002.