2019 IEEE European Symposium on Security and Privacy (EuroS&P)

In Encryption We Don't Trust: The Effect of End-To-End Encryption to the Masses on User Perception

Sergej Dechand
University of Bonn
Bonn, Germany
dechand@cs.uni-bonn.de

Alena Naiakshina
University of Bonn
Bonn, Germany
naiakshi@cs.uni-bonn.de

Anastasia Danilova
University of Bonn
Bonn, Germany
danilova@cs.uni-bonn.de

Matthew Smith
University of Bonn, Fraunhofer FKIE
Bonn, Germany
smith@cs.uni-bonn.de

***Abstract*—With WhatsApp's adoption of the Signal Protocol as its default, end-to-end encryption by the masses happened almost overnight. Unlike iMessage, WhatsApp notifies users that encryption is enabled, explicitly informing users about improved privacy. This rare feature gives us an opportunity to study people's understandings and perceptions of secure messaging pre- and post-mass messenger encryption (pre/post-MME). To study changes in perceptions, we compared the results of two mental models studies: one conducted in 2015 pre-MME and one in 2017 post-MME. Our primary finding is that users do not trust encryption as currently offered. When asked about encryption in the study, most stated that they had heard of encryption, but only a few understood the implications, even on a high level. Their consensus view was that no technical solution to stop skilled attackers from getting their data exists. Even with a major development, such as WhatsApp rolling out end-to-end encryption, people still do not feel well protected by their technology. Surprisingly, despite WhatsApp's end-to-end security info messages and the high media attention, the majority of the participants were not even aware of encryption. Most participants had an almost correct threat model, but don't believe that there is a technical solution to stop knowledgeable attackers to read their messages. Using technology made them feel vulnerable.**

I. Introduction

Before 2016, most mobile communication, such as short messaging services (SMS) or messaging apps, did not provide any end-to-end encryption. One popular exception was `iMessage`. However, it still lacked a user interface for key authentication, thus creating a vulnerability to man-in-the-middle attacks. It also did not advertise any of its security features. With `WhatsApp`'s introduction of the `Signal` protocol as its default, authenticated end-to-end message encryption suddenly became available to the masses [43]. `WhatsApp` notifies users that their messages are end-to-end encrypted every time a new conversation is opened and offers an optional authentication process based on quick response codes or key fingerprints [43, 13].

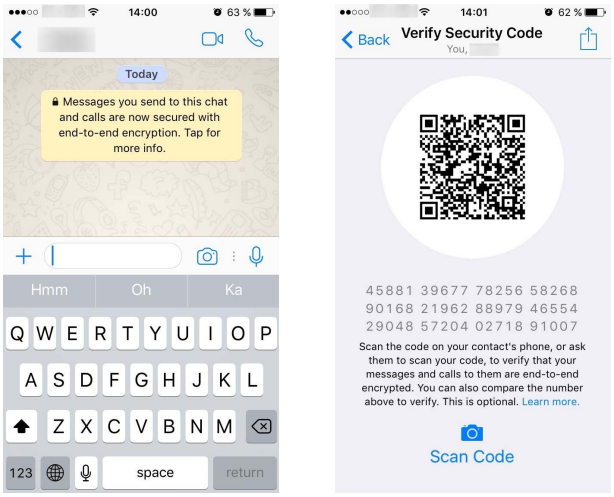
Even though various cryptography protocols as OpenPGP, off-the-record messaging, and Tor, have been available for decades [8, 5, 2], they have all failed to achieve widespread adoption due to usability issues, such as key management and key authentication and sometimes even unreliable message delivery. Previous work has shown that end users struggle with security tools for email encryption [44, 16, 32, 24]. The general perception is still that usability problems are to blame for the woes of encryption solutions. However, we propose that perceptions and mental model issues might remain hindrances even when security mechanisms provide good usability. The introduction of a very usable end-to-end encryption solution provides the ideal opportunity to study this aspect.

To capture users' perception and understanding, we conducted a qualitative user study based on interviews to illustrate average users' mental models *before* and *after* the *mass messenger encryption* event (pre- vs. post-MME). The methodology and the first 11 interviews were conducted in July and August 2015. In January and February 2017, approximately nine months after `WhatsApp`'s introduction of end-to-end encryption, we conducted another set of interviews (post-MME) to be able to compare mental models before and after the introduction of this widespread encryption mechanism. In 2017, we re-invited some participants from the 2015 group and invited 11 new participants to enable a direct comparison. The results of both groups were analyzed individually. We chose this mixed set because taking part in the *pre-MME* study was very likely to have shaped the participants' opinions. Recruiting both old and new participants allowed us to see both a within group and a between group view of this event.

Our study was aimed at identifying aspects helping messenger developers implement usable and secure software, so it was important to understand how people imagine the process of sending and receiving mobile messages. We considered two main methods: classic text messages (SMS) and `WhatsApp`. Rather than technical details, we focused on whether end users understand high-level concepts and more importantly, the implications of encryption. The first part of our study was started before the widespread adoption of end-to-end encryption services, so we considered the transition of users' mental models after the introduction of *mass messenger encryption*. Our key findings are:

1) **Users do not trust encryption**. Most of our participant were well aware of who is theoretically capable of eavesdropping on their communication. However, they *overestimated the capabilities* of potential attackers, e.g.,

DOI 10.1109/EuroSP.2019.00037



(a) WhatsApp Encryption (b) WhatsApp Authentication

Fig. 1: WhatsApp's implementation of end-to-end encryption based on the Signal protocol [35].

skilled neighbours could break the encryption and read their messages. At the same time, they *underestimated cryptographic capabilities*, sharing the consensus that there is no technical solution stopping skilled attackers from breaking encryption. Most stated that they had heard about encryption, but only a few understood the implications, even on a high level.

2) **Users lack awareness**. Despite WhatsApp's introduction of end-to-end encryption in April 2016, most users were still unaware of it nine months later. More surprisingly, when directly asked about the info message (see Figure 1a), many participants reported noticing it but chose to ignore it or failed to understand the implications correctly.
3) **SMS is more secure than WhatsApp.** Almost all the participants believed that SMS is more secure than WhatsApp. The participants justified this belief with two reasons: first, they considered the Internet to be *evil* and second, they held opinion that SMS messages seldom cross country borders.
4) **Users do not feel targeted.** In general, government and special service surveillance was perceived critically, especially if executed by foreign countries. However, most participants believed that they would never be targeted. A few participants saw benign, exceptional cases for the police in fighting crime and terrorism but rejected the idea of mass surveillance. Finally, the majority thought that governments and hackers are able to break any kind of encryption.
5) **Study participation raises awareness and attention.** The participants who took part in our 2015 study were more aware of encryption and security in the second interview. For instance, some used alternative messengers such as Threema, Signal and Telegram. This was mainly because the participants were critical of WhatsApp's acquisition. In contrast, the newly-invited participants never used other apps except for LINE.

The rest of the paper is structured in the following way: in Section II we review related work. Section III describes our methodology and its limitations. In Section IV we present the results of our focus groups. In Sections V and VI we compare the results of the pre- and post-MME single interviews. An extra section (Section VII) is dedicate to the 4 re-invited participants. Finally, in Sections VIII and IX we discuss our results, provide recommendations, and conclude.

II. Related Work

In this section, we discuss the usage of current security solutions in messaging and prior attempts to improve their usability. We also discuss work on gathering user perceptions and obtaining people's mental models in the human-computer interaction and especially the usable security and privacy community.

A. Communication Security

Starting with the commercially available email encryption PGP [8], a large body of security communication tools (e.g., Tor, Off-the-Record Messaging (OTR) and others) followed [14, 37, 5]. However, the famous Johnny user studies and follow-up work confirmed that end users are overwhelmed with most security tools [44, 16, 32, 15, 24]. For instance, some required hard key management [44, 8, 2], and others had session issues with less reliable mobile environments [5, 2, 33, 38, 34].

Consequently, up to the beginning of 2016 the majority of exchanged personal messages including email and messengers remained unsecured. With the growing popularity of the Signal messenger and its protocol providing similar security features as OTR and a better integration in mobile environments [36, 34, 38], WhatsApp integrated it in early 2016 [43]. Similarly to iMessage, end-to-end encryption is activated by default. Additionally, it provides an optional authentication verifying the absence of man-in-the-middle attacks and can be done by using QR codes or comparing numeric hash representation with 60-digit numbers, as shown in Figure 1b [43, 13].

B. Mental Models

To elicit users' understanding and perception in an area, a commonly used method in psychology, and recently in the usable security and privacy area, is based on mental models [9, 28]. More specifically, mental models describe what exactly users think about a specific topic or problem; they disclose that people form diagrams in their minds, which help them to build their understanding of the world and to solve the problems that emerge when they have to interact with complex systems [20, 28].

Various usable security researchers adopted mental models of users' understanding regarding technologies based on the Internet [42, 41, 21, 31, 21, 22, 29]. Having unrealistic mental models regarding communication may induce a risk based on

users' activities. Previous work specifically named some of the misunderstandings [41, 40]. We propose that developers should take users' mental models in consideration when designing messaging protocols rather than assuming that their users understand cryptographic details. This approach could lead to a greater acceptance of secure messaging software as users will not be confused or frustrated by the complexity of public key encryption.

Asgharpour et al. [3] found that security experts and non-experts have different mental models of security risks. They proposed that risk communication should not be designed based on experts' mental models, as it is mostly done, but rather should be designed based on end users' point of view.

Bravo-Lillo et al. [7] designed a mental model in order to understand how users think about computer security warnings. The study compared advanced and novice user's behavior dealing with computer security warnings and was supposed to help developers to improve their warning design.

Wash [41] conducted a study in order to understand the users' mental models of attackers and security technologies, and to explain why users strictly follow some security advice from computer security experts and ignore others.

Furthermore, a multi-method user study was conducted by Vaniea et al. [39] to get a better understanding of how people make decisions about software updates.

C. User Perceptions of Secure Messaging

Adoption criteria of secure messaging tools and services as well as social influence on users decision of security tools and security behavior have been intensively investigated in the past [17, 11, 23, 12]. For example, De Luca et al. [23] conducted an online survey with 1500 participants, making a quantitative analysis of *how much of a role* security played in people's decisions to use a mobile messenger. As often suspected in the usable security field, their results suggest that security plays a minor role, and the available contacts in a messenger clearly dominate their decision making.

Furthermore, Bai et al. [4] investigated whether users are able to understand the difference between a *key-exchange* and a *key-directory* model. Their results show that users are well aware of usability and security trade-off, but favored key directories.

Renauld et al. [31] investigated why the usage of end-to-end encrypted emails is limited. Their study revealed issues such as incomplete threat models, misaligned incentives, and a general absence of understanding of email architecture. In contrast to their work, we did not stop the interview sessions if the term encryption was not mentioned by participants. Rather, we asked our participants about encryption and how they imagine it is supposed to work. This procedure ensures that participants, who have a general idea of encryption, but might not conceive of the term, could still express their knowledge.

Abu-Salma et al. [1] conducted 60 qualitative interviews analyzing the obstacles to the adoption of mobile messaging applications. Their participants were additionally advised to explain encryption. Interestingly, the participants indicated telephony as a service, which is more secure than text messaging. Although the study of Abu-Salma et al. was conducted with another methodology and in the UK, the findings show remarkable similarities to our study. For instance, their participants observed SMS as more secure than instant messaging, an opinion which was also shared by our participants in Germany.

III. Methodology

To capture end users' understanding of mobile communication, we conducted semi-structured interviews with 22 participants from Germany. We conducted our interviews before and after `WhatsApp`'s introduction of end-to-end encryption, so we could observe changes in end users' mental models. The *pre-mass messenger encryption (pre-MME)* interviews were conducted with 11 participants in July and August 2015. The *post-mass messenger encryption (post-MME)* interviews were conducted with 11 new invited and 4 re-invited participants in January and February 2017.

Our study was designed to offer insights into the following aspects of users' perceptions of encrypted messaging:

- **Understanding of the architecture:** how users imagine mobile communication works and whether they distinguish between SMS and instant messaging.
- **Threat model:** who users assume is able to eavesdrop and whether there are ways to prevent it.
- **Understanding of encryption:** how do users imagine encryption and authentication and whether they understand the implications.
- **Impact of end-to-end encryption:** change in users' understanding of mobile communication after `WhatsApp`'s introduction of end-to-end encryption (post-MME).

A. Interview Guideline Design

A major challenge in designing semi-structured interviews to capture users' understandings and mental models is to design an interview guideline covering the necessary topics. Previous work in this area either opted to use more open questions with a large unstructured part, or refined their interviews based on pre-studies [1]. To improve this process, we used *focus groups*, to iteratively develop a guideline for individual interviews [30]. Focus groups are an approved methodology with a long history of use in psychological studies to collect qualitative data [26, 19]. A skilled moderator leads an interactive group discussion with multiple participants by using a guideline of a set of carefully predetermined structured questions. We used the focus group methodology as a more refined and structured way of a pre-study justifying the final interview guideline [30]. We performed 3 focus group iterations, adapted and improved our interview guideline with each iteration. In addition to the moderated discussion, we asked our participants to support their thoughts with drawings, in order to let them visualize their perceptions [31, 21, 22, 29].

B. Focus Groups

We conducted 3 focus group iterations in 2015 [27]. For the recruitment of participants we used the theoretical sampling

approach [30]. The first focus group was recruited at our university. Two student assistants invited participants who were on campus. To get a more diversity for the second and third focus groups, we recruited students of non-technical degrees from other universities and older people with less academic background. Participation was rewarded with snacks and refreshments. A single, skilled researcher led and moderated the focus group discussions by using a carefully predetermined semi-structured guideline. The moderator was accompanied by an assistant researcher, who served as a note-taker for important observations.

The first part of the guideline was used to gain a first glimpse of the participants' mental model of mobile messaging communication. An empty sheet of paper with only two individuals, Alice and Bob on it, was handed out to the focus groups. The participants were asked to describe how Alice and Bob could communicate with each other and to draw stations important for their communication. The second part covered perceptions of encryption and authentication. The participants were asked to think about eavesdroppers and to highlight threatening spots in their drawings. They were also asked how eavesdropping might be prevented. To gain insight into the participants' perceptions of Man-in-the-Middle scenarios, we asked how Alice could be sure that the person she was communicating with was really Bob, in other words, how it can be guaranteed that communication partners are the persons whom they claim to be. All the questions were open-ended to encourage the participants to express their thoughts in detail. The guideline was refined after each focus group, e.g., by adding relevant questions and removing less relevant questions.

The first group's participants were undergraduate computer science students (first and second year), 1 female and 6 male with an average age of 21 years. The second focus group had 6 participants (2 male and 4 female) with an average age of 24 years. The group consisted of students (e.g., medicine, architecture) and employees (e.g., logopedics) in fields less related to computer science. Considering the younger age and the student status of most participants, we invited older participants with less technical backgrounds (cleaner, scholar, housewife, pastor, vendor, geriatric nurse, mechanic and a carpenter) to join the third focus group. This group consisted of 8 people, 3 male and 5 female with an average age of 47.5 years. Each focus group discussion lasted approximately 60 minutes.

Based on the three iterations of focus groups, we created a semi-structured guideline for individual interviews (see Appendix A). For instance, instead of using unfamiliar persons such as Alice and Bob, we decided to ask the participants how they thought communication with their friends worked. Additionally, the focus group participants mentioned SMS and `WhatsApp` as communication applications they used often. So, we concentrated on these applications in our individual interviews. Finally, most participants in the focus groups were confused by the expression *authentication*. We, therefore, neither mentioned the term *authentication* nor used a helping scenario in the individual interviews.

C. Individual Interview Participants

For the individual interviews, we recruited participants by placing advertisements on *eBay Kleinanzeigen* (a German private marketplace website similar to *Craigslist*). We also asked the participants in the 2015-group whether they would like to participate in our study in 2017 again. Those interested were invited to individual interviews to our university. Participation in the interviews was rewarded with 15 Euro. A table showing the demographics of the participants can be found in the Appendix E.

Pre-MME (2015): 11 participants were invited to talk about messaging architecture and security. The sample consisted of 7 females and 4 males with an average age of 29 years. The average self-reported level of technical knowledge (see Section III-E) was 8 (medium). All participants had diverse professions, like students, office assistants, food service workers, scientific assistant etc. The student participants studied business informatics, computer science, economics and media management.

Post-MME (2017): We established two groups in 2017: (1) 4 re-invited participants from the 2015 study[1] and (2) 11 new participants. 6 female and 5 male, with an average age of 31 years. Four of the new invited participants were students in computer science unrelated programs including economics, medicine, agriculture, and teaching. Three participants were self-employed in the beauty treatment, economics and health care industries. One participant reported to be working as a paramedic and another participant was unemployed. Their average self-reported level of technical knowledge was 6 (medium).

In both studies, the coders discussed after each evaluated interview whether theoretical saturation [6, 10] was reached or whether more participants were needed to be sampled. In case of a disagreement between the coders, further participants were invited. Saturation was reached when both coders agreed that no new codes/themes emerged.

D. Individual Interview Procedure

We conducted 11 individual interviews in 2015 before `WhatsApp`'s introduction of end-to-end encryption in 2017. After this, we conducted further 15 individual interviews to identify the mental model changes. All the interviews were conducted in German and followed the same methodology and guideline. To avoid experimenter bias, the same interviewer conducted them. Each interview lasted from 30 to 40 minutes.

First, the participants had to answer demographic questions and how often they use SMS and `WhatsApp` (see Appendix B). Next, the participants were presented a brief scenario:

> *You would like to communicate with a friend using your mobile phone. You would like to send a text message to your friend via Short Messaging Service*

[1]We invited all participants from the original group in order to examine whether their mental models changed after the introduction of E2E encryption. Only 4 of 11 participants were willing to join the new study. We did not receive any answer from the other 7.

(SMS) or via `WhatsApp`*. Please draw how you think the communication looks like.*

The interview technique was designed to give as little hints as possible. As in the focus groups, the participants were handed a sketch of two individuals. If participants indicated differences in their mental models of SMS and `WhatsApp`, they were requested to make two drawings. Also, in the case of space limitations, we handed out another blank sheet of paper for the second service. The participants were also asked what parties they thought could eavesdrop communication. They indicated stations where these parties could eavesdrop. If participants did not mention encryption, we asked them whether they had heard of it and requested that they explain and draw how they imagined encryption. The participants had to indicate whether they believed that `WhatsApp` or SMS messages are encrypted and if they knew of or used any apps providing encryption. Finally, the participants were asked how a message could be explicitly assigned to a person. The guideline for the individual interviews can be found in the Appendix A.

E. Evaluation

We conducted a qualitative analysis for the single interviews and focus groups. All interviews were transcribed in German. Two researchers independently coded and evaluated every transcription following a three-step procedure: (1) using *open coding* to develop concepts and categories, (2) developing connections among the categories, and (3) drawing conclusions by assigning users' individual statements to the categories [19]. Differences between the two coders were resolved through discussion to avoid interpretation bias. Relevant statements and expressions from the participants' mental models were translated into English by the same researchers.

To report statements by the participants from single interviews, we label them P1-P11 in the pre-MME (2015) group and from N1-N11 for the post-MME (2017) group. The 4 re-invited participants are referred to with their initial labels from 2015: P1, P5, P6, and P9. In relevant cases, we also report how many participants stated specific themes to indicate their frequency and distribution, although we do not aim to generate quantitative results.

To assess participants' technical experience, they rated statements on a 5-point Likert-Scale (see Appendix C). We calculated a ratio indicating the technical background of participants from 0 to 12 (low: 0-3, medium: 4-8, high: 9-12). More details on the calculation can also be found in the Appendix C.

F. Limitations

Despite high individual demographic differences, our sample contains only participants with a German cultural background. The results might not be the same in different cultures. Based on historic background, language nuances but also local media exposure in Germany, the results in this paper might not be applied to other cultures directly.

Furthermore, we used *eBay Kleinanzeigen* (similar to *Craigslist*) to recruit our participants. Thus, we have a self-selection bias and could only sample in the population of people using this service.

A qualitative approach does not claim to provide generalization. Qualitative work such as this is only the first step on the road to generalizable results as it can help exploring reasoning and views of participants.

G. Ethics

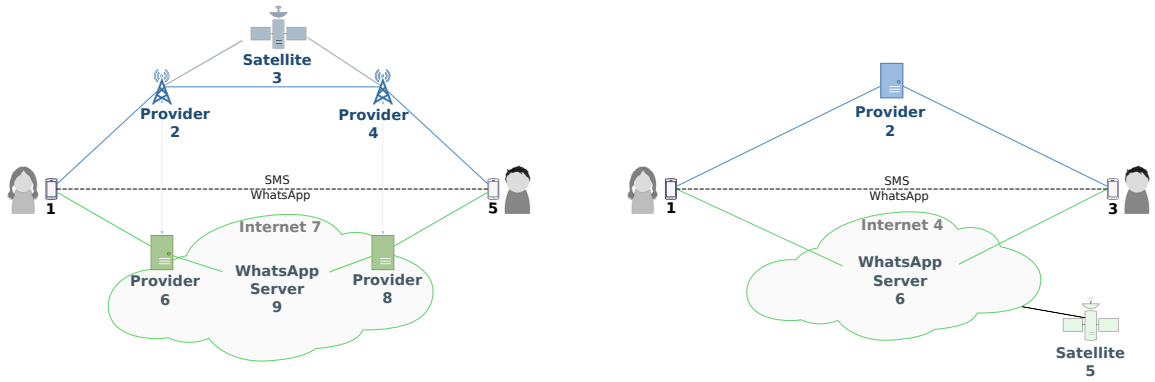
Since our study was conducted in Germany, it was not required to pass an IRB review. However, our study complies with the strict German privacy regulations. At the end of the first study we asked if participants would be willing to be contacted again. The contact data was stored separately. The data was collected anonymously and the participants were informed about withdrawing their data during or after the study.

IV. Focus Group Results

Although the participants in the focus groups were from different age ranges and professions, all the groups mentioned some general points [27]. Most participants appeared skeptical of and expressed insecurity when using mobile messaging communication. They believed that almost anyone could eavesdrop on their messages at every station if someone, whether companies or individuals, was eager enough or had the proficiency to do so. Although all the participants had security concerns they nevertheless still actively used services they mistrusted on their mobile phones. However, a number of participants stated that they did not send any sensitive information by mobile phone. For that, they preferred to meet in person or write emails. Several reasons motivated this behavior: some participants did not understand the system behind SMS and `WhatsApp`, and others did not know how to protect their messages from eavesdropping.

Various participants were concerned about `WhatsApp` and its security, but did not switch to secure messengers because all their contacts still used `WhatsApp`. Nevertheless, the participants stated that if more of their contacts and other people started to use secure messaging apps, they would too. All the groups mentioned encryption in connection to preventing eavesdropping.

Some believed that not even encryption can protect their messages. Most importantly, the second and third groups showed that the majority of users were not familiar with public-key cryptography. The only concepts they could imagine involved passwords and symmetric encryption. The participants suggested that the key exchange should involve a personal meeting or sharing a secret. One interesting aspect mentioned by the second group was that mobile numbers are connected to `WhatsApp`. The second group seemed to trust this kind of control. In contrast the first focus group stated that this is not a method trustworthy at all. The third focus group became aware of the potential threat from the man-in-the-middle attacks by going through a simplified scenario with Alice, Bob and Eve. This indicates that users are capable to understand the threats without effort, but didn't realize the threat on their own.



(a) Before End-To-End Security

(b) After End-To-End Security

Fig. 2: Aggregated Mental Models of Individual Interviews.
The upper parts of the illustration (blue) refer to messaging via SMS whereas the lower illustration (green) refers to messaging via `WhatsApp`. Stations mentioned by our participants were indicated with individual numbers (see Appendix D).

Importantly, all the focus groups mentioned the NSA and governments as potential adversaries. Obviously, most the participants had noticed the NSA spying scandal and realized that their messages could easily be captured by different parties, particularly the U.S. government. This finding shows that news and stories influence mental models.

V. Individuals' Architecture Understanding

Most importantly, our analysis shows that even though end-to-end security did not gain high attention among our users, all the participants were aware of the interception risks of both systems (`WhatsApp` and SMS). We present the results in subsections focusing on different areas of mobile communication. In each subsection, we describe the results from our first iteration *before the introduction of end-to-end security to the masses (2015)*. If the users' mental models changed in the follow-up iteration *after the introduction of end-to-end security to the masses (2017)*, we also discuss the differences in a separate paragraph. For the comparison of 2015 and 2017, we consider the results of the 11 participants in 2015 and the 11 new participants in 2017.

A. Messaging Architecture

Our main goal was to illustrate the users' understandings of messaging infrastructure. Therefore, we asked participants of how they imagined messaging communication between two persons. The mental model drawings of the individual participants can be found online.[2] Ignoring minor details discussed in the following, all participants' mental models had great similarities. We, therefore, summed the individual mental models into a single aggregated model of messaging architecture by including stations mentioned by our participants, and summarizing terms, such as, server, provider, and radio mast referred to as providers' base stations by the participants (see Appendix D). Figure 2a shows the summarized mental model of all the 2015 participants and Figure 2b for 2017. Almost all the participants distinguished between communication via SMS and `WhatsApp`.

1) Pre-MME (2015): In 2015, the participants mentioned different intermediate stations. First, all the participants mentioned a mobile provider base station (specifically referred as a radio mast by P4, P7, P8, P10, and P11) as a point, through which an SMS message passed on its way to the other communicating peer. P1, P2, P5, P6, P7, P10, and P11 included one or more mobile providers or ISPs (Internet Service Providers) in their visualizations for SMS. Moreover, P1, P3, P5, P6, P8, P9, and P11 mentioned servers as an intermediate stop in the architecture. P3 and P6 distinguished between servers in foreign countries and Germany. Some participants (P2, P8, and P10) believed that satellites were involved in mobile communication.

Asked to extend their drawing of SMS or make another diagram for messaging via `WhatsApp`, almost all the participants identified the Internet as the basic difference between the two (Figure 2a, lower illustration):

> "Yes, in my opinion, it looks different because [the text messages] are sent through the Internet, which is an external service. Thus, it definitely works in a different way." (P1)

P1, P8, and P9 differentiated between mobile servers for SMS and Internet servers for `WhatsApp`. P8 stated that the Internet works via satellites. Additionally, the `WhatsApp` provider often referred to as a server by the participants, was specified as the core difference from SMS.

[2]The original mental model drawings of the individual participants were handwritten and in German. In order to ensure participants' anonymity we transcribed all drawings. Additionally, they were translated in English: https://net.cs.uni-bonn.de/fileadmin/user_upload/smith/EuroSP19_MentalModel_Drawings.pdf

Adversary	Stations Pre-MME	#P	Stations Post-MME	#N
Mobile Provider	2, 2 ↔ 4, 3, 6	4	1 ↔ 2, 2, 2 ↔ 3	4
German Government	2, 3, 4, *	5	2	3
German Law Enforcement	1, 1 ↔ 2, 2	3	1 ↔ 2, 2 , 2 ↔ 3	2
US Law Enforcement	2	2	3	1
German Intelligence Agencies	2 ↔ 4, 2	4	1 ↔ 2, 2↔ 3	2
Foreign Intelligence Agencies	2	2	2 ↔ 3	3
Hackers	1, 2, 2 ↔ 4, 3, 7	7	1 ↔ 2 , 2 , 2 ↔ 3, 3	8

TABLE I: SMS adversaries mentioned by our participants before and after the introduction of MME. *Stations Pre-MME* (related to Figure 2a) and *Stations Post-MME* (related to Figure 2b) show the stations where participants (#P of 11/#N of 11) expect adversaries to eavesdrop on their messages. Attackers indicated between two stations were marked by arrows; * indicates "everywhere".

Adversary	Stations Pre-MME	#P	Stations Post-MME	#N
WhatsApp	7, 9	9	1 ↔ 3 , 4 , 5 , 6	9
Mobile Provider	6	2	1 ↔ 4	2
German Government	1, 2, 9, *	3	2 ↔ 3	3
Foreign Governments	6 ↔ 9, 9, *	6	1 ↔ 3, 6	4
German Law Enforcement	1 ↔ 9, 2, 9	3	1 ↔ 3, 3	1
Foreign Law Enforcement	9	3	1, 3	1
German Intelligence Agencies	2	5	6	3
Foreign Intelligence Agencies	6 ↔ 9, 7,	2	4, 6	5
Hackers	1, 2, 9	6	1, 3, 3 ↔ 6, 4, 6	9
Commercial Companies	7 ↔ 9, 9	5	3 ↔ 6, 6	2
Facebook/Zuckerberg	7 ↔ 9	4	1, 3 ↔ 5, 3 ↔ 6, 6	4
Spying Apps (e.g., Viruses)	1	4		0

TABLE II: `WhatsApp` adversaries mentioned by our participants before and after the introduction of MME. Same table structure as in Table I.

2) Post-MME (2017): We found only minor differences between the mental models of the participants in 2015 and 2017 (new participants). The 2015 participants often called several provider base stations radio masts or towers. This changed slightly in 2017, when most of the participants specified only one provider base station for SMS (N1, N3, N4, N6, N7, N9, and N11). N2, N5, and N8, however, still identified more than one provider base station. For example, N2's mobile communication was represented by only three single radio masts connected to each other. Finally, in 2015 *satellites* were associated with mobile communication for text messages, while in 2017 the participants N2-N4 believed satellites were also required for the Internet.

B. Threat Model

Table I and Table II summarize the threat model for SMS and `WhatsApp` shared by the participants. To give an impression of how often adversaries were mentioned, we also provide the number of participants (#P/#N of 11) who mentioned them.

1) Pre-MME (2015): When investigating the participants' threat models, they all agreed that eavesdropping was possible at various stations involved in communication channels. This position captured the generally skeptical sentiments all the participants have shown when speaking of security of mobile communication.

The most significant result of our study was that messages sent via the SMS were felt to be more secure than `WhatsApp` messages. Various reasons were mentioned. First, because `WhatsApp` messages are sent via the Internet, participants often stated that `WhatsApp` is more prone to eavesdropping. Second, banks and post offices also use SMS in order to send important data (P7). Third, P7, P8, P9 and P10 believed that SMS is more difficult to be hacked. Almost all participants mentioned `WhatsApp` and hackers as potential adversaries.

However, P6 and P10 believed that ordinary people are not likely to be targeted for surveillance. They stated that either rich, famous people, politicians or criminals are targeted: "I do not think that everybody is being monitored. I'm an unimportant person and don't write dangerous or bad stuff" (P6).

In the following, we discuss the adversaries mentioned by the participants in more detail.

Mobile Providers and ISPs: P2 assumed that mobile providers were not allowed to access the messages. In contrast, P7 explained that mobile providers maintained relations with governments and spies, and P7 argued that governments did not necessarily need to cooperate with mobile providers to access the messages. Also, P8 added that hackers and governments could access radio providers.

Government and Law Enforcement: Half of the participants mentioned German and foreign governments (e.g., U.S. and Russia) as potential adversaries. Most participants stated that the German government could read their messages when they use SMS for mobile communication. P2 speculated that the German government could only read SMS messages at satellites

and that it is impossible to protect SMSes from governments because it is unfeasible to control the satellites. Furthermore, P8 noted that German government could install malware, such as key loggers and trojans, on mobile devices.

P3 and P8 mentioned the Pentagon as an eavesdropping party in the U.S. government. P8 and P9 both mentioned Asian and Chinese governments. P9 also assumed that the Russian government could eavesdrop. Additionally, the participants mentioned the U.S. law enforcement agencies: FBI, CSI, CIA.

Some participants (P8, P10, and P11) distinguished between permitted data access and illegitimate data access: when someone collects data but does nothing with it vs. access data without your knowledge and deliberately spies on the data. For example, German and U.S. law enforcement and the German government were mentioned as eavesdroppers in context of terrorism and crime prevention (P3, P5, P6, and P9-P11). P10 believed that key words such as *bomb* and *terrorist* are logged and counted. If a log shows an unusual large amount of such key words, the sender is monitored and controlled.

Intelligence Agencies: P3 remembered that the NSA eavesdropped on German Chancellor Angela Merkel. The German media reported on mass surveillance. More than half of the participants (P1, P7-P11) mentioned the NSA as a potential eavesdropper in `WhatsApp` communication. The German Federal Intelligence Service (BND) was also explicitly mentioned by P8 and P10.

Hackers: Almost all participants (P3, P4, P6-P11) identified hackers as a party, which can eavesdrop text messages. In particular, P4 mentioned Russian hackers. Further, P6 differentiated between "good hackers" (searching for exploits and vulnerabilities) and "bad hackers" (stalker and criminals in general). P7, on the other side, referred to hackers as "teenager without friends" or "[someone] connected to the mafia." P9 explained that some hackers sell the data, which they obtain. Hackers who are collecting data for marketing were also mentioned by P10. A larger part of our participants believed hackers are able to access the messages on all stations.

Commercial Companies: P5 believed that text messages are scanned. Further, some participants assumed that commercial companies like Amazon (P2), newspaper (P2) or advertisement agencies (P5, P9, P10) buy data from the `WhatsApp` company in order to advertise. However, they are only capable to access the data through contacting the `WhatsApp` company.

Smartphones, Malware and the Internet: P10 named updates as a security threat because users are not aware of what they are downloading and do not know whether mobile devices send information to app providers. P6 and P11 mentioned malware, such as trojans. While P6 reported that malware could come from the governments, P11 believed the malware is downloaded when surfing on web pages with smartphones. Furthermore, P6 assumed that smartphones were easier to break into than into older mobile devices. Additionally, P6 stated that SMS is more secure than `WhatsApp` because it does not use the Internet. Similarly, P4 opined that "the Internet is evil. Everyone can listen to and read everything."

Fusion of Facebook and WhatsApp: P2 and P5 commented critically on the fusion of `WhatsApp` and Facebook in 2014:

> "I think it is defined in general terms and conditions that `WhatsApp` can use pictures etc. that are sent. Therefore, I believe that companies, which could profit from eavesdropping, [can read the messages]." (P2)

These participants assumed that Facebook is capable of accessing all messages from `WhatsApp`: For instance, P2 equated Facebook with Mark Elliot Zuckerberg: "The founder Zuckerberg [can read messages]. He also started up a company for that" (P2).

WhatsApp: For `WhatsApp` communication almost all of the participants mentioned the `WhatsApp` provider, hackers, the U.S. government, and the Secret Service as potential eavesdroppers. The participants had great doubts about the Internet technology as well as about `WhatsApp` as a company:

> "In principle, I assume that `WhatsApp` is able to decrypt messages. `WhatsApp` can read the messages [within their server]." (P1)

In addition to that, P5 believed that `WhatsApp` scans the messages for important information. P5 also remarked that `WhatsApp` reveals details about the communicating party, e.g., the online status or profile pictures.

2) Post-MME (2017): When comparing the adversaries, the new participants mentioned the same adversaries as the old participants. More interestingly, even though six participants (N3, N4, N7, N9-N11) noticed that `WhatsApp` introduced end-to-end encryption, they still considered `WhatsApp` to be capable of reading and accessing the messages.

Additionally, all participants except N7 reported that they did not change their behavior after they saw the notification for the end-to-end encryption. Furthermore, our participants stated that they did not understand the message. Even though six participants noticed the encryption of `WhatsApp` only three participants (N1, N5, N9) thought `WhatsApp` to be more secure than SMS. Our participants lack trust in encryption as well as lack knowledge of end-to-end encryption technology.

Finally, comparing pre-MME and post-MME it is notable that post-MME no participants thought that spying apps are included in the threat model for `WhatsApp`.

VI. Individuals' Cryptography Understanding

A. Pre-MME (2015)

The participants were asked whether they believed that SMS or `WhatsApp` messages were encrypted. Almost all participants (P1-P10) assumed that SMS messages are encrypted but again indicated that the mobile provider and the German government could decrypt their messages. Regarding

WhatsApp, participants had mixed feelings. P1, P3, P6, P9 and P10 stated that WhatsApp messages are encrypted, the rest stated that they are not encrypted. P1, P3, P6 and P9 assumed that WhatsApp has access to their messages independently of whether the messages are encrypted or not.

Four participants were able to name alternative secure messaging apps to WhatsApp, mentioning Threema (P7-P9, P11) and Telegram (P8). P1 stated that Tor could be used for secure email communication. However, eight participants (P1-P7, P10) stated that they have never used secure messaging apps. Although P4 used the app MyEnigma, which advertises end-to-end encryption, she did not state to use an encryption app. P9 and P11 tested Threema, but only P11 used the app for a longer time. Finally, most of the participants stated that they would be interested in a secure messaging app. However, they do not trust the app provider offering such services.

Encryption: Three participants (P3, P5, P10) needed an encryption tip, but could explain the idea of encryption after that very well. Participants defined encryption in the following way:

- A kind of a secret code (P5-P8, P10).
- Every message gets an encryption code, key or password.
- A change of data, so it is only possible to read the message with special information.
- A secret language in which all the letters are exchanged by numbers or symbols.
- Encryption is a "blockade" or "barrier", which is difficult to break like an anti-virus software or a firewall.
- Analogy with a ZIP-file: "Both parties need to have the protection app. [The text message] is passing through the Internet, but not to an extra company. Directly after sending the message, it has to be packed. Imagine it like ZIP-files. For the text messages you would also need a program, which is able to unpack" (P2).

Only one participant (P11) mentioned "end-to-end encryption" as well as illustrated asymmetrical encryption with private and public keys (student of business informatics).

Some participants believed that even if encryption is used it can be decrypted: "Actually nothing is secure, because software exist, which can decrypt everything" (P6). Therefore, the majority of the participants believed that the provider of a secure app handles the encryption and thus has access to the code. Consequently, the app provider is able to read all of their messages. To prevent eavesdropping by the secure app provider, P4 mentioned an idea of separate services for encryption and messaging. P6 expressed another idea: when developing an encryption application, the developer team splits the code in several parts. Then every member would be responsible for one part of the encryption. If the team combines the individual parts of the program they can break the code. Also P10 assumed that if the user wants to be secure, he needs to handle the encryption manually. It seems that users expect to put a certain amount of work in order to be/feel secure.

Authentication: In the next part, the participants were requested to think about authentication, specifically, how a message can be assigned to a unique person. Eight participants (P1-P5, and P7-P9) mentioned mobile phone numbers, but assumed that mobile providers could also imitate mobile phone numbers. Alternatively, a key and a password were mentioned by three participants (P1, P2, and P11). Two participants (P1, P10) commented that the only alternative was a personal meeting for comparing a password or exchanging a key:

> "There are classical methods in which each side owns a key. It would only be completely safe, if you meet physically and exchanged the keys. [...] Meeting physically means that you exchange the keys without using an electronic device. You can never be sure whether the post office or anybody else reads along. [...] I believe exchanging a key privately is the only solution providing full security" (P1).

Other participants (P3, P6, P10) mentioned that they would agree on a word and would append it to the message or simply ask the other person something, which only the person could know. P8 noticed that encryption is a contrast to authentication. In summary, most of the participants did not understand why authentication was needed:

> "But I have not sent [the message to a third party], but to my friend. I assume that my friend and I have accounts, Alex27 and Kati07, for example. Then I send a message to them. Why should Pia23 read along? The Internet does not know my password, only me and my friend do." (P2)

B. Post-MME (2017)

By comparing mental models of encryption between pre- and post-MME, we recognized that they did not change. Participants described encryption in a similar way, using symmetrical passwords or codes. The majority of participants said that WhatsApp is able to access the messages even if they deploy end-to-end encryption. Participants had troubles with understanding the term end-to-end encryption and feel like it is impossible that the WhatsApp company is not able to access the messages because they provide the encryption in the first place.

N10 mentioned that she uses WhatsApp but did not encrypt because it requires to scan the QR code of the other party. Obviously, even though she noticed the notification WhatsApp gives at the beginning of a conversation, she believed that the message is not automatically encrypted and that she needs to put an effort to encrypt her messages.

Our participants in 2017 still fail to understand how authentication can be achieved. Some participants believe they would notice if a certain message does not come from the sender (different style of writing or language). Further, all participants except one (N10) did not know about the security code verification. Even worse, the only participant who successfully scanned the code (N10) thought afterwards that WhatsApp does not offer encryption as default. As mentioned above, she

thought that only after scanning the code the messages are encrypted.

VII. Re-invited Participants Post-MME (2017)

Four participants (P1, P5, P6, P9) agreed to repeat our study giving us the chance to compare their mental models of 2015 and 2017. The re-joint participants all reported that they use WhatsApp regularly, compared to 2015 where some reported to use it rather often.

Messaging Architecture: In terms of mobile messaging architecture the participants stuck to their remaining mental models. P1 and P6 established a more detailed view on the architecture. P1 mentioned satellites and P6 added a new drawing for WhatsApp with a WhatsApp server as an intermediate station.

Threat Model: The threat model and the possible adversaries remained as strong as in 2015. While in 2015 P1 thought everybody could read WhatsApp messages, in 2017 he was sure that no one except the WhatsApp company can read WhatsApp messages any longer. He also did not mention the German or American government as eavesdroppers any more. In 2017 P5 additionally named the NSA as eavesdropper for every station (SMS and WhatsApp), but no longer the German government.

Although all participants recognized that WhatsApp introduced encryption, P1, P5 and P9 were sure that WhatsApp could access the keys. Further, P9 believed that "everyone who is a bit clever can decrypt". P6 was the only one from our re-invited participants, who believed that WhatsApp's encryption protects users' messages from eavesdroppers. She indicated that WhatsApp is probably using extra software for encryption preventing also the company from reading the messages. However, it should be considered that P6 is a Computer Science student and thus, we expect her to be more knowledgeable than lay people.

Encryption: In 2015 all four participants thought SMS were encrypted, while in 2017 only P9 still believed that SMS are encrypted (but using an universal encryption key). P5 was the only one in 2017 still thinking SMS is more secure than WhatsApp.

All participants were aware that WhatsApp introduced encryption. We assume that our study increased the awareness of the participants. Still, the introduction of end-to-end encryption in WhatsApp did not change the behavior of our four participants:

> "I still would not send a PIN over WhatsApp because it is personal information. If I *had* to, I would not feel differently before and after WhatsApp did it." (P9)

Authentication: Regarding two-party authentication in 2017 there are still misconceptions of WhatsApp's QR code: "I only used the QR code for WhatsApp web" (P6). P9 did not know about the QR code in WhatsApp because she has not found it in the app. However, she was aware that Threema uses the QR code for authentication.

VIII. Discussion and Implications

In previous work on mental models and security perception, researchers examined the current state at a given point in time. To the best of our knowledge, this is the first work studying behavior and understanding changes of users between two points in time separated by an important event: the introduction of end-to-end message encryption to the masses.

In this section we elaborate on the implications of our results for the security community. In addition to our takeaways based on our findings, we make concrete recommendations what messenger and protocol developers could do in the future.

One of the key differences between the encryption introduced by WhatsApp (and iMessage) is that they are extremely usable - to a point that it is almost impossible to make a mistake. This stands in strong contrast to *classical* approaches such as PGP, S/MIME and others, which suffer from many usability problems. Studies have shown that the majority of users made catastrophic mistakes in those cases.

However, our study results show that the introduction and usage of a highly usable security mechanism did not lead to higher perception or valuation of the security technology. In our view, this means that it was not just poor usability, which hindered the adoption of past end-to-end encryption schemes but also the unsurprising fact that users are overwhelmed by technology in general and consider themselves to be helpless and vulnerable against skilled attackers.

The fact that encryption was turned on without any user interaction and further, that the use does not require any additional interaction is what made this role-out a success. However, this success comes at a price. Unlike with PGP the WhatsApp and iMessage solutions rely on trusted first-parties, namely the message providers. The providers can change keys and mount attacks with little risk of being exposed since there is still limited awareness of the underlying end-to-end security mechanism.

A. Takeaways and Recommendations

Our most important takeaway is that end users do not trust encryption, and this has not been changed by the widespread adoption of usable encryption mechanisms. Even though the participants had an almost correct threat model, they felt vulnerable when using technology and were skeptical to any technical solutions to prevent the attacks. When asked about encryption, most stated they had heard of encryption but only few understood the implications even on a high level. Their consensus was that there is no technical solution stopping skilled attackers from eavesdropping. The fact that encryption increases the effort required to do so was not raised in any significant manner. More surprisingly, despite WhatsApp's end-to-end encryption information messages that pop up with every new communication partner and the high media attention surrounding iMessage and WhatsApp encryption, the majority of our participants were still not aware of it.

The success of WhatsApp's and iMessage's security solutions is based on the fact that end users do not have to understand what is happening. This seems like a very sensible

way forward: "Users should not have to care about security - it should just be there for them." The failure of the introduction and usage of end-to-end encryption to raise awareness or increase the desire for protection shows that continuing down the route of trying to educate users is likely to fail as it has in the past.

This leaves some big challenges for the community to tackle. One of the main reason why `WhatsApp` and `iMessage` have succeeded where previous solutions have failed is the fact that the products are under control of a single entity acting as a trusted entity. This makes the creation of a usable solution significantly easier. However, it also introduces the challenge of preventing the key manager from tampering with the keys. This confirms the demand for user-interaction-free solutions, such as key transparency and CONIKS [18, 25]. On the other hand, email encryption has to battle with the fact that dozens of email clients and hundred of providers are in use and without any concept for key management.

The results of our study suggest that attempts to provide security against key-change attacks by informing the user of changed keys might not succeed. For the time being we recommend that the community accepts the fact that there is a vendor lock-in since the effort to create a usable version of PGP has shown that the engineering effort to create a multi-client, multi-provider solution is a Herculean engineering task and in our view focusing on the less challenging problem. Thus, based on the results of our study, we propose that the open challenge is to fulfill the following criteria in a closed-ecosystem to start with:

- *Work on users' trust.* Our study suggests that end users underestimate the power of cryptography. As stated by P5, "Even Mrs. Merkel was hacked and all messages decrypted. So decrypting messages of an end user, the little customer, is probably not a big deal. [...] In the end, everything can be decrypted, interpreted or read."
- *Speak users language.* Despite this being a well known recommendation and part of Nielsen's usability principles this is still an issue in modern apps. Improving the notification in `WhatsApp` by using a more user-friendly language, e.g., understandable wording of end-to-end encryption. In our study, the participants stated that they ignored this message due to unfamiliar terms. For instance, N3 stated when asked about `WhatsApp`'s end-to-end encryption: "Oh that was what this annoying notification was about?"
- *Keep it simple for users.* As already adopted in various mobile messengers, users should not need to do anything for security. This was confirmed by our participants questioning the need to authenticate contacts manually: "It would be too inconvenient to scan QR codes of all contacts" (N10).
- *Fewer notification, which the user does not understand.* The party managing the keys should not be able to mount a man-in-the-middle attack by pushing new keys to a client. Only in this event a user should be notified. User struggle to understand the notification shown by `WhatsApp`.

IX. Conclusion and Future Work

The main goal of this paper was to capture and compare end-user mental models of message encryption. For this, we conducted an in-depth qualitative study consisting of two parts, each with 11 participants: pre- and post-MME. Although `WhatsApp` introduced end-to-end encryption more than nine months before our post-MME study, many participants still were not aware of it and there had been only minor changes in their mental models. Our results suggest that even though users were able to describe the threat model almost correctly, they do not believe that there is any technical possible to stop the attackers. More importantly, misconceptions about cryptography have lead to a lack of trust in encryption in general. The participants reported feeling vulnerable and simply assumed that they cannot protect themselves from attackers. Based on our findings, we make recommendations for how the community can address these challenges.

Our future work consists of studying cultural differences in detail and conducting a quantitative experiment testing users' understanding of different high-level encryption concepts.

X. Acknowledgment

We would like to thank Johanna Deuter for transcribing the original mental model drawings of the individual participants.

References

[1] Ruba Abu-Salma et al. "Obstacles to the Adoption of Secure Communication Tools". In: *Security and Privacy (SP), 2017 IEEE Symposium on (SP'17). IEEE Computer Society*. San Jose, CA: IEEE, 2017.

[2] Chris Alexander and Ian Goldberg. "Improved User Authentication in Off-The-Record Messaging". In: *Workshop on Privacy in the Electronic Society*. ACM, 2007, pp. 41–47.

[3] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. "Mental models of security risks". In: *Financial Cryptography and Data Security*. Springer, 2007, pp. 367–377.

[4] Wei Bai et al. "An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems". In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, 2016, pp. 113–130. ISBN: 978-1-931971-31-7. URL: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/bai.

[5] Nikita Borisov, Ian Goldberg, and Eric Brewer. "Off-the-Record Communication, or, Why Not To Use PGP". In: *Workshop on Privacy in the Electronic Society*. ACM. 2004, pp. 77–84.

[6] Glenn A Bowen. "Naturalistic inquiry and the saturation concept: a research note". In: *Qualitative research* 8.1 (2008), pp. 137–152.

[7] Cristian Bravo-Lillo et al. "Bridging the gap in computer security warnings: A mental model approach". In: *IEEE Security & Privacy* 9.2 (2011), pp. 18–26.

[8] Jon Callas et al. *OpenPGP message format*. Tech. rep. IETF Working Group, 2007.

[9] L Jean Camp. "Mental models of privacy and security". In: *Available at SSRN 922735* (2006).

[10] Kathy Charmaz. *Constructing grounded theory: A practical guide through qualitative analysis*. Sage, 2006.

[11] Sauvik Das et al. "Increasing security sensitivity with social proof: A large-scale experimental confirmation". In: *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. ACM. 2014, pp. 739–749.

[12] Sauvik Das et al. "The effect of social influence on security sensitivity". In: *Proc. SOUPS*. Vol. 14. 2014.

[13] Sergej Dechand et al. "An Empirical Study of Textual Key-Fingerprint Representations". In: *USENIX Security Symposium*. USENIX, 2016.

[14] Roger Dingledine, Nick Mathewson, and Paul Syverson. *Tor: The Second-Generation Onion Router*. Tech. rep. DTIC, 2004.

[15] Facebook. *Facebook Help Center*. 2014. URL: https://www.facebook.com/help/ (visited on 11/03/2014).

[16] Simson L Garfinkel and Robert C Miller. "Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express". In: *Symposium on Usable Privacy and Security*. ACM. 2005, pp. 13–24.

[17] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. "Secrecy, flagging, and paranoia: adoption criteria in encrypted email". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM. 2006, pp. 591–600.

[18] Google. *Safe email - Transparency Report. Email encryption in transit*. Google, June 4, 2014. URL: https://www.google.com/transparencyreport/saferemail (visited on 11/02/2014).

[19] Bryan Jenner et al. *A companion to qualitative research*. Sage, 2004.

[20] Natalie Jones et al. "Mental models: an interdisciplinary synthesis of theory and methods". In: *Ecology and Society* 16.1 (2011).

[21] Ruogu Kang et al. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security". In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, 2015, pp. 39–52. ISBN: 978-1-931971-249. URL: https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[22] Predrag Klasnja et al. "When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2009, pp. 1993–2002.

[23] Alexander De Luca et al. "Expert and Non-Expert Attitudes towards (Secure) Instant Messaging". In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, 2016, pp. 147–157. ISBN: 978-1-931971-31-7. URL: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/deluca.

[24] Susan E McGregor et al. "Investigating the Computer Security Practices and Needs of Journalists." In: *USENIX Security*. USENIX, 2015, pp. 399–414.

[25] Marcela S. Melara et al. *CONIKS: A Privacy-Preserving Consistent Key Service for Secure End-to-End Communication*. Cryptology ePrint Archive Report 2014/1004. 2014. URL: https://eprint.iacr.org/2014/1004.

[26] David L Morgan. "Focus groups". In: *Annual review of sociology* (1996), pp. 129–152.

[27] Alena Naiakshina et al. "Poster: Mental Models-User understanding of messaging and encryption". In: *Proceedings of European Symposium on Security and Privacy. http://www. ieee-security. org/TC/EuroSP2016/posters/number18. pdf*. 2016.

[28] Jakob Nielsen. *Mental Models*. http://www.nngroup.com/articles/mental-models. 3.3.2015. Oct. 2010.

[29] Erika Shehan Poole et al. "More than meets the eye: transforming the user experience of home network management". In: *Proceedings of the 7th ACM conference on Designing interactive systems*. ACM. 2008, pp. 455–464.

[30] Richard A Powell and Helen M Single. "Focus groups". In: *International journal for quality in health care* 8.5 (1996), pp. 499–504.

[31] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. "Why Doesn't Jane Protect Her Privacy?" In: *Privacy Enhancing Technologies*. Springer. 2014, pp. 244–262.

[32] Steve Sheng et al. "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software". In: *Symposium On Usable Privacy and Security*. ACM. 2006.

[33] Ryan Stedman, Kayo Yoshida, and Ian Goldberg. "A User Study of Off-the-Record Messaging". In: *Symposium on Usable Privacy and Security*. ACM. 2008, pp. 95–104.

[34] Open Whisper Systems. *Advanced cryptographic ratcheting*. Nov. 2014. URL: https://whispersystems.org/blog/advanced-ratcheting/ (visited on 11/02/2014).

[35] Open Whisper Systems. *Open Whisper Systems partners with WhatsApp to provide end-to-end encryption*. Nov. 2014. URL: https://whispersystems.org/blog/whatsapp/ (visited on 12/23/2017).

[36] Open Whisper Systems. *Simplifying OTR deniability*. Nov. 2014. URL: https://whispersystems.org/blog/simplifying-otr-deniability (visited on 11/02/2014).

[37] Threema GmbH. *Threema.Seriously secure messaging*. https://threema.ch/de/. 01.04.2015. Apr. 2015.

[38] Nik Unger et al. "SoK: Secure Messaging". In: *Security and Privacy (SP), 2017 IEEE Symposium on (SP'17). IEEE Computer Society*. IEEE. San Jose, CA, 2015.

[39] Kami Vaniea, Emilee Rader, and Rick Wash. "Mental models of software updates". In: *International Communication Association, Seattle, WA, USA, in May* (2014).

[40] Matthias Wachs, Martin Schanzenbach, and Christian Grothoff. “A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System”. In: *Cryptology and Network Security*. Springer, 2014, pp. 127–142.

[41] Rick Wash. “Folk models of home computer security”. In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM. 2010, p. 11.

[42] Rick Wash and Emilee Rader. “Influencing mental models of security: a research agenda”. In: *Proceedings of the 2011 workshop on New security paradigms workshop*. ACM. 2011, pp. 57–66.

[43] WhatsApp. *Encryption Overview*. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf. Apr. 2016.

[44] Alma Whitten and J Doug Tygar. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0”. In: *USENIX Security Symposium*. USENIX, 1999.

APPENDIX A
FINAL GUIDELINE

1) **Scenario (5 minutes)**:
   You would like to communicate with a friend via your mobile phone. Therefore, you would like to send a text message via Short Messaging Service (SMS) or via WhatsApp to your friend. Please draw how you think a communication via SMS looks like. Which intermediate stations does the message pass through until it reaches your friend?
   - Does the communication for WhatsApp look similar or different?
     - If YES: Please prepare a second drawing or complete the first one.
2) Can other parties eavesdrop the message?
   - If YES: At which stations in the communication can other parties eavesdrop the message? Please draw it in your sketch. Which parties?
     Lately, there have been reports of "Eavesdropping of messages" in the media. Is there something that comes to your mind concerning this topic?
     - If NO: Have you heard about "Snowden" or the "NSA surveillance scandal?" If NO: proceed with (3, Tip)
3) You assumed that other parties might eavesdrop your message. Are there any countermeasures to prevent that? (1 minute) Tip: Have you heard of encryption?
4) How can somebody encrypt? Could you please explain how you think encryption works? Please draw it in your sketch. (5 minutes)
5) How can you assign a message uniquely to one person? (3 minutes)
   - If answer = "Personal password": Then you would have to agree with your communication partner on an individual password. This could be quite difficult. Can you imagine an alternative?
   - If answer= "Phone number": Would this be sufficient? (Tip: Or could the provider imitate the telephone number?)
6) Do you think SMS messages are encrypted? (1 minute)
   - If YES: Who could eavesdrop the messages? There was no password exchange.
7) Do you think WhatsApp messages are encrypted? (1 minute)
   - If YES: Who could eavesdrop the messages? There was no password exchange.
8) Have you heard of apps offering encryption? (1 minute)
   - If YES: Which can you name?
9) Have you used apps offering encryption? (1 minute)
   - If YES: Which ones?
   - If NO: Would you use apps offering encryption?
10) Are you currently using apps offering encryption? (2 minutes)
    - If YES: Which ones?
    - If NO but already used: Why are you not using the app(s) any longer?

APPENDIX B
DEMOGRAPHIC SURVEY QUESTIONS

1) Gender: *Female / Male*, Age: ... Years
2) How often do you send text messages via `SMS`/ `WhatsApp`? *Regularly - Often - Rarely - Never*
3) What is your highest completed level of education?
4) Recent professional status: Student, subject:...; Employed, profession:...; Unemployed

APPENDIX C
TECHNICAL SCORE

We calculated the technical skill score (0-12) of our participants as follows: (T1 + reverse(T2) + T3) - 3. A value of 0-3 was considered as a **low** technical score, 4-8 was considered a **medium** technical score, and 9-12 was considered a **high** technical score.

- **T1:** I have a good understanding of Computers and the Internet: *1: I disagree - 5: I agree*
- **T2:** I often ask other people for help when I am having problems with my computer. *1: I disagree - 5: I agree*
- **T3:** I am often asked for help when other people have problems with their computer. *1: I disagree - 5: I agree*

APPENDIX D
AGGREGATED MENTAL MODELS OF INDIVIDUAL INTERVIEWS

Stations mentioned by participants before end-to-end security from Figure 2a:

1) **Mobile Phone:** P3, P4, P5, P6, P8, P9, P10
2) **Provider:** P1, P2, P4, P5, P6, P7, P8, P10, P11
3) **Satellite:** P2, P8, P10
4) **Provider:** P1, P2, P7, P8, P10, P11
5) **Mobile Phone:** P3, P4, P5, P6, P8, P9, P10
6) **Provider:** P1, P8, P10, P11
7) **Internet:** P1, P2, P3, P4, P5, P6, P8, P10, P11
8) **Provider:** P1, P8, P11
9) **WhatsApp Server:** P1, P3, P5, P6, P7, P8, P9, P11

Stations mentioned by participants after end-to-end security from Figure 2b:

1) **Mobile Phone:** N2, N3, N4, N5, N6, N7, N10
2) **Provider:** N1, N2, N3, N4, N5, N6, N7, N8, N9, N11
3) **Mobile Phone:** N2, N3, N4, N5, N6, N10
4) **Internet:** N3, N4, N5, N6, N11
5) **Satellite:** N2, N3, N4
6) **WhatsApp Server:** N3, N4, N5, N6, N7, N8, N9, N11

APPENDIX E
DEMOGRAPHICS

The demographics of our participants can be found in Table III.

Participant	Sex	Age	Highest completed level of education	Current employment	Technical Score	How often do you send text messages via SMS	How often do you send text messages via WhatsApp	Used encryption apps	Encryption-tip
P1	Male	33	Master of Applied Biotechnology	Office Assistant	high	Regularly	Rarely	N	N
P2	Female	24	A-Levels	Biotechnical Assistent	medium	Rarely	Regularly	N	N
P3	Female	27	Trained Hairdresser	Caterer / Waitres	low	Rarely	Regularly	N	Y
P4	Female	47	Computer Science	Self-employed	high	Regularly	Rarely	Y	N
P5	Male	26	Advanced technical college entrance qualification	Student Business Administration	high	Rarely	Regularly	N	Y
P6	Female	26	Advanced technical college entrance qualification	Student Computer Science	medium	Rarely	Often	N	N
P7	Female	19	A-Levels	Student Media Informatics	medium	Rarely	Regularly	N	N
P8	Male	26	Diploma Financial Consultant	Public servant Fincancial Administation	high	Often	Regularly	Y	N
P9	Female	46	State examination	Research Assistant Medicin	medium	Regularly	Regularly	Y	N
P10	Female	25	Advanced qualification to enroll for a technical college+ Trained Educator	Unemployed	medium	Regularly	Never	N	Y
P11	Male	23	A-Levels	Student Business Informatics	high	Rarely	Regularly	Y	N
NP1	Male	48	Certificate of Secondary Education + Trained cook	Unemployed	high	Rarely	Regularly	N	N
NP2	Male	22	Advanced qualification to enroll for a technical college	Self-employed Salesperson Health Sector	low	Regularly	Regularly	N	N
NP3	Male	21	A-Levels	Student Aggricultural Studies	high	Regularly	Regularly	N	Y
NP4	Female	27	A-Levels	Student Medicin	medium	Regularly	Regularly	Y (WhatsApp)	N
NP5	Male	53	Trained forwarding merchant	Self-employed Trader	medium	Regularly	Regularly	N	N
NP6	Female	24	Bachelor Education	Student Master of Education	low	Rarely	Regularly	N	
NP7	Male	35	Master Logistics and E-Business	Part-time employed Business Admin.	medium	Regularly	Often	Y (WhatsApp)	Y
NP8	Female	53	Advanced qualification to enroll for a technical college	Self-Employed (Wellness Consulter)	medium	Rarely	Regularly	N	Y
NP9	Female	21	A-Levels	Paramedic	low	Regularly	Often	Y (WhatsApp)	Y
NP10	Female	21	A-Levels	Pharmaceutic, technical Assistant	high	Regularly	Regularly	Y (Line, WhatsApp)	N
NP11	Female	20	A-Levels	Employed in Business Administration	medium	Regularly	Regularly	Y (WhatsApp)	N
2017:P1 from 2015	Male	34	same as in 2015	Assistant of the CEO	high	Regularly	Regularly	Y (WhatsApp)	N
2017:P5 from 2015	Male	28	same as in 2015	same as in 2015	medium	Often	Regularly	N	N
2017:P6 from 2015	Female	27	same as in 2015	same as in 2015	medium	Often	Regularly	Y (Signal)	N
2017:P9 from 2015	Female	47	same as in 2015	same as in 2015	medium	Often	Regularly	Y	N

TABLE III: Demographics of 22 participants