Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography

Matthias Fassl
matthias.fassl@cispa.de
CISPA Helmholtz Center for Information Security
Saarland University

Katharina Krombholz
krombholz@cispa.de
CISPA Helmholtz Center for Information Security

Figure 1: Two people authenticating their secure messaging conversation

ABSTRACT

Authentication ceremonies detect and mitigate Man-in-the-Middle (MitM) attacks on end-to-end encrypted messengers, such as Signal, WhatsApp, or Threema. However, prior work found that adoption remains low as non-expert users have difficulties using them correctly. Anecdotal evidence suggests that security researchers also have trouble authenticating others. Since their issues are probably unrelated to user comprehension or usability, the root causes may lie deeper.

This work explores these root causes using autoethnography. The first author kept a five-month research diary of their experience with authentication ceremonies. The results uncover points of failure while planning and conducting authentication ceremonies. They include cognitive load, forgetfulness, social awkwardness, and explanations required by a communication partner. Additionally, this work identifies and discusses how sociocultural aspects affect authentication ceremonies. Lastly, this work discusses a design approach for cooperative security that employs cultural transcoding to improve sociocultural aspects of security by design.

CCS CONCEPTS

• Security and privacy → Social aspects of security and privacy; **• Social and professional topics → Cultural characteristics**; **• Human-centered computing → Empirical studies in collaborative and social computing**.

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581508

KEYWORDS

End-to-End-Encrypted Messaging, MitM Attacks, Authentication Ceremonies, Social Cybersecurity, Autoethnography

ACM Reference Format:
Matthias Fassl and Katharina Krombholz. 2023. Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3544548.3581508

1 INTRODUCTION

Successful MitM attackers are able to read and also fake messages in end-to-end encrypted instant messaging conversations while their active attack is ongoing. Authentication ceremonies, which require verifying cryptographic keys with conversation partners, detect and mitigate these attacks. However, users have several issues with these ceremonies: They are unaware of them, do not understand their purpose, and have trouble finding and conducting them [13]. But not only end users have trouble with authentication ceremonies. Anecdotal evidence suggests that even security experts, such as we researchers, have problems keeping contacts authenticated – even though this is our area of expertise! Hence, we suspect that authentication ceremonies suffer from deeper problems than merely a lack of UI usability or user comprehension.

Previous work on authentication ceremonies focused on user behavior in lab settings [12, 29–31], some of which simulated MitM attacks [22, 33]. Lab settings are great environments to study usability issues in a controlled way. And studying user behavior during attacks is crucial since users require protection in these exact moments. However, real-world conditions for authentication are more complex. First, users are likely not in proximity when they recognize the need to authenticate or notice key-reset notifications. Second, since key resets usually happen for benign reasons, users will not necessarily be in a hurry to conduct a new authentication

ceremony. Hence, users will most likely plan a future authentication ceremony with their contact. Authentication ceremonies are social cybersecurity [34] mechanisms, which depend on conversation partners to meet up and cooperate to improve their security equally. As such, social and cultural expectations and practices affect their success, as Uzun et al. [27] suggested in their work.

RQ1: What problems do knowledgeable and motivated users encounter when planning and conducting authentication ceremonies?

RQ2: How do social and cultural factors impact authentication ceremonies between conversation partners?

To understand the potential issues around planning authentication ceremonies and navigating social and cultural issues, we conduct an autoethnography based on a five-month research diary documenting the first author's authentication experience. While autoethnographic approaches are uncommon in the field of Usable Privacy and Security (UPS) — Turner et al.'s work [26] being a rare example — researchers of the closely related HCI field regularly use it to gain a deeper understanding of how technology affects users' lives [4, 14–17, 20, 23, 24]. In contrast to other types of diary studies, self-inquiries can easily be long-term, are deeply introspective, and combine the analysis step with data collection – adapting the data collection method according to preliminary analysis results. Autoethnographies focus their analysis on social interactions and the cultural rules that govern them [5]. Since security experts rarely report their own failures to cope with security systematically, this work may provide valuable insights as an autoethnography. While strict generalizability is not a meaningful goal for this kind of qualitative research [3], we improve the transferability of our results by describing the first author's background and all the situations in as much detail as possible.

The first author aims to authenticate as many contacts as possible in naturalistic settings for this study. Prior work identified the issues of lacking user comprehension and lacking usability of the user interfaces [13]. However, since the first author is a security researcher who understands the underlying issues and knows how to conduct authentication ceremonies correctly, these potential barriers should not apply. Autoethnography enables the study of authentication ceremonies in infrequent and naturalistic contexts, which are not easily accessible with other study designs or participants.

This paper contributes: (1) a phase model of planned authentication ceremonies, comprising need recognition, planning, meeting, convincing, and authenticating; (2) the identification of failure points in the planning process, such as forgetting, social awkwardness, and necessary explanations; (3) an account of subjective emotions of guilt and frustration that constituted the first author's authentication experience; and (4) a discussion about sociocultural barriers and facilitators of authentication.

2 BACKGROUND AND RELATED WORK

First, we provide some background on the security benefits and process of authentication ceremonies in end-to-end encrypted messengers. Then, this section presents the theoretical framework of autoethnography, data collection methods, and work from the related HCI field. Afterward, this section briefly introduces the concept of social cybersecurity, explaining why autoethnography is a suitable approach to research this area. Finally, this section elaborates the research on authentication ceremonies, discussing prior work's chosen methods and the identified issues.

2.1 Authentication Ceremonies in End-to-End Encrypted Messengers

To communicate with a conversation partner, end-to-end-encrypted messengers need to know the recipient's public key. In most modern messengers, this public key comes from a central key server and is trusted without further verification. MitM attackers impersonate this key server, either by directly taking control of the key server or with an active attack at the network level. With the powers of the key server, MitM attackers can convince the clients of both conversation partners to use a different encryption key (which is in the attacker's possession) for communicating (see Figure 2). As a consequence, successful MitM attackers can read and manipulate all messages in a conversation as long as the active attack continues. In 2018, the Dutch police appears to have used such an attack to intercept messages sent via IronChat [10]. To detect and mitigate these MitM attacks, end users need to authenticate the key material, i.e., verify that they are using the correct encryption key to communicate with their conversation partner. Most end-to-end encrypted messengers offer a dedicated authentication ceremony for this purpose.

There are many different versions of authentication ceremonies, most are intended for in-person authentication (e.g., in Signal, WhatsApp, or Telegram's secret chats) but some are also designed for remote use. During calls in Viber, conversation partners compare a secret identification key; in Telegram calls, conversation partners compare a set of emojis; and for the Wire messenger, users record a video of themselves announcing the short authentication strings (SAS) that correspond to their key. However, meeting in person is usually preferable because (a) it is a secure out-of-band communication channel and (b) scanning others' QR codes is simpler and less exhausting than remotely reading and comparing safety numbers [30]. Here, we describe the steps to authenticate a conversation in Signal and WhatsApp in person with QR codes. Figure 3 shows the corresponding user interface to each of the steps.

(1) Both conversation partners open up the shared conversation in their messenger.
(2) They open the authentication interface by clicking on their contact's name and selecting "View Safety Number".
(3) The conversation partners take turns showing their QR code and letting the others scan it. Users scan by tapping the QR code or pressing the corresponding button, depending on the operating system and messenger.
(4) If the scan is successful, the conversation can be marked as verified. If the check fails, the conversation is under attack and must not be used for communication.
(5) The verified marker vanishes when either end reinstalls the messenger, one of the conversation partners gets a new phone, or when the conversation is under attack. Repeating the authentication ceremony is required in all cases.

If users are aware of authentication ceremonies, they will need to decide which conversation they want to protect since this will

require expending additional effort to avoid MitM attacks. In general, even unauthenticated conversations are still protected from various passive eavesdropping attacks and are more secure than regular email or SMS conversations.

Fassl et al. [8] found that end users mostly considered authenticating messenger conversations with friends, partners, and family members. However, the perceived overhead of arranging meetings might have impacted participants' responses. Also, other types of contacts, such as tax advisors, lawyers, or business partners, might be sensitive conversation partners outside the immediate circle of friends, partners, and family members.

2.2 Autoethnography

According to Chang [5], autoethnography is a self-reflective form of cultural analysis. The term describes the method and final product alike. It assumes that the self learns and upholds values, norms, and customs to become part of a cultural group. Thus, we can learn about cultural factors by understanding the relationship between the self and others. Self-narrative reports are the basis for autoethnographies. Additional explanations connect these personal experiences to the cultural environment. According to Ellis and Bochner [7], autoethnographies comprise three parts: research process (graphy), culture (ethno), and the self (auto). However, the focus on these parts varies widely among researchers. Some emphasize personal experience, while others give more space to cultural explanations. For researchers, autoethnography is a practical approach for investigating human relations in their cultural context. It improves the cultural understanding of the self and others while invoking self-reflection and self-examination among its readers [5]. According to Chang [5], autoethnographers collect data by chronicling their past, i.e., memories, and recording field data. Usually, they avoid mixing these two. Recorded field data includes routines, rituals, celebrations, or cultural artifacts. The focus lies on experiences, stories, and objects with sociocultural significance. In parallel to data collection, autoethnographers use inventorying to evaluate and organize their data, i.e., they select, prioritize, rank, and categorize collected data.

Autoethnography, narrative inquiries, and self-studies all privilege the self in the research design. According to Hamilton [11], narrative inquiry shares stories of the researchers' experiences so that others may learn from them. Self-studies are systematic inquires into the researchers' own practices to gain knowledge about them and improve them. In contrast, autoethnography highlights the changing perspectives of the self and puts experiences in their broader cultural context. Commonly, researchers write in the first person when they use these approaches.

Autoethnography is a rarely used method in Usable Privacy and Security (UPS) research, e.g., Turner et al. [26]'s work on smart home cyber security practices in their family. However, researchers in Human-Computer Interaction (HCI) regularly apply autoethnography to study how technology affects users. Spiel [23] used it to demonstrate how technical infrastructures reinforce binary gender ideology by documenting their experience with systems not allowing them to register their gender correctly. Jain et al. [15] used it to highlight tensions and nuances during the travels of a hard-of-hearing individual, focusing on difficult social conversations, navigation problems, and personal assistive technologies. Stephen et al. [24] provide an autoethnographic account of the barriers an independent blind traveler faced during her 28-day cruise, focusing on the use of technology to access visual information and maps. Chamberlain et al. [4] explore autoethnography as a method to self-design personal heritage soundscapes. Lockton et al. [16] designed a series of research probes that enable autoethnographic exploration, investigating students' bedtime routines, sleep patterns, personal time scheduling strategies, and sleep in non-traditional places. Lucero [17] conducted an autoethnography to understand how living without a mobile phone affects their life. O'Kane et al. [20] used autoethnography to evaluate a wrist blood pressure monitor. They argue that it enabled them to empathize with users in contexts that are otherwise hard to investigate using traditional in-situ studies.

Assessing Methodological Fit. We assessed the methodological fit of autoethnography to our research problem along three criteria: The value that the first author's vantage point adds to answering the research question, the required level of introspection and reflection, and the appropriateness of a socio-cultural analysis lens for the research questions.

(1) *Vantage point:* The first author's vantage point is primarily that of a security expert and offers two benefits: They can collect more data on all parts of the authentication process since their background knowledge of authentication ceremonies helps them complete ceremonies even when others can not. Similarly, Turner et al. [26] thought their increased cybersecurity awareness as experts may have generated more data for their autoethnographic work on smart home security practices. Also, with their experience in Usable Privacy and Security, the first author can provide explanations at different levels of complexity to engage and educate people with varying technical know-how.
(2) *Introspection:* Self-studies provide a unique ability to researchers: introspection of the feelings and thought processes behind one's actions and adapting and refining the used research methods based on them. These abilities are useful for studying authentication ceremonies because ceremonies incorporate social interactions that come with social expectations, boundaries, feelings, and context-dependent norms. Direct access to the experience and sufficient time for reflecting on them makes an in-depth analysis easier for researchers. Understanding these aspects with a diary study with multiple participants can be more difficult. Participants know that researchers will read the diary entries, which limits the amount and type of information in them. To get a comparable level of analysis to an autoethnography, researchers would need to question participants repeatedly about each (potentially embarrassing) experience during the ongoing analysis process — resulting in a resource-intensive hybrid between diary and interview study.
(3) *Sociocultural analysis:* Authentication ceremonies require that two communication partners cooperate to increase their security. Thus, they are a sociotechnical system that researchers can analyze through a sociocultural lens. While the sociocultural analysis of ethnographic approaches is not

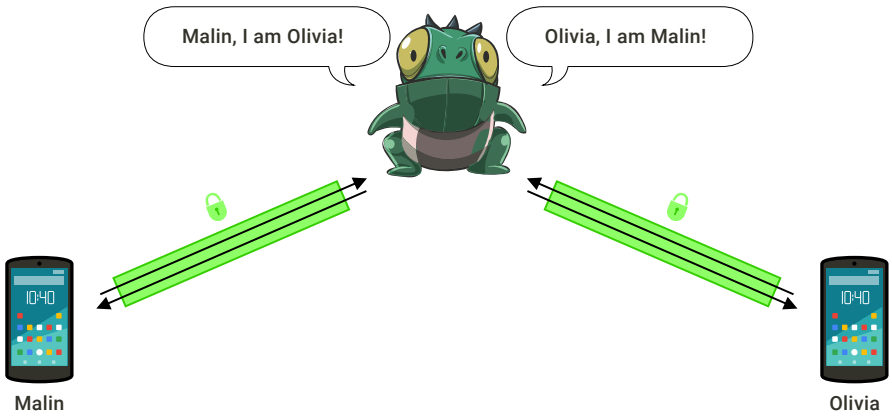


Figure 2: The MitM attacker (the monster) convinces the messenger clients (of Malin and Olivia) that they should use their encryption key instead of their conversation partner's. During an ongoing attack, the monster will have to continuously forward Olivia and Malin's messages.

strictly necessary, it does provide a lens to understand the underlying social and technical issues of using authentication ceremonies more completely.

While we could use a regular diary study or ethnography to learn more about others' difficulties with authentication ceremonies in their daily life, an autoethnography gives us a more in-depth understanding of one person's experience.

2.3 Social Cybersecurity

Social cybersecurity research recognizes that security mechanisms are often social in nature [34]. However, security tools are still built primarily with an individual user in mind, resulting in a social-technical gap [1] between technology's abilities and what it requires socially from users. Exploring this social-technical gap works well with autoethnography because it connects individuals' security-tool experience with its sociocultural context. Also, studying social cybersecurity tool usage is challenging because of the naturalistic settings and infrequent use. And as O'Kane observed in prior work on non-routine use of technology [20], autoethnography is valuable to study usage under these constraints.

Wu et al. [34] structure the research on social cybersecurity into four categories: negotiating access to shared resources, shared and social authentication, managing self-representation, and influencing others' security and privacy behaviors. While not explicitly mentioned, authentication ceremonies in secure messengers are shared and social authentication mechanisms: Two messenger users cooperate to detect and mitigate MitM attacks against their conversation.

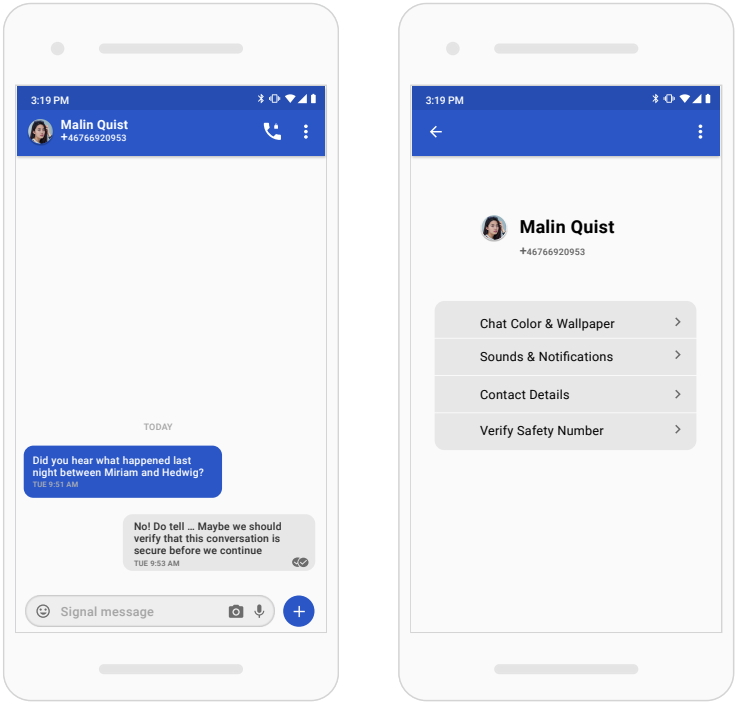
Prior work extensively studied the usability issues of authentication ceremonies in a lab. Herzberg et al. [12] studied the usability of WhatsApp, Viber, Telegram, and Signal. They found that participants were unaware of the need to authenticate and that 56.5% of them could not do so after being asked. Schröder et al. [22] found that the majority of participating CS students failed to detect and mitigate MitM attacks using Signal's authentication ceremony. Vaziripour et al. [30] compared authentication ceremonies of Viber, WhatsApp, and Facebook Messenger. They found that only 14% of their study participants successfully verified the key material without further explanation. When Vaziripour et al. [28] surveyed Iranian Telegram users, they found that only 29.6% had ever used the authentication ceremony in text conversations.

Researchers proposed several usability improvements to authentication ceremonies. Vaziripour et al. [31] streamlined Signal's ceremony by providing easy access and additional guidance. Wu et al. [33] produced new visual indicators, new notification dialogs, and a simplified notification flow. Vaziripour et al. [29] partially removed users from the loop by using Keybase for an authentication method based on social media. Fassl et al. [8] redesigned authentication ceremonies from the ground up and found that user-centered prototypes can increase users' comprehension of the security implications. These design changes that prior work suggested may solve some of the problems associated with authentication ceremonies. However, since their implementations are not (yet) widespread, it is hard to understand their effects on the users' daily life, i.e., in infrequent and naturalistic scenarios.

In their paper "Secure Messaging Authentication Ceremonies are Broken", Herzberg et al. [13] summarize the current state of research: Users do not understand encryption, cryptographic keys, and the concept of MitM attacks. When facing a MitM attack in a lab environment, they have significant issues finding and completing ceremonies successfully. In contrast, this work applies autoethnography to identify how sociocultural factors unrelated to either comprehension or usability affect the use of authentication ceremonies.

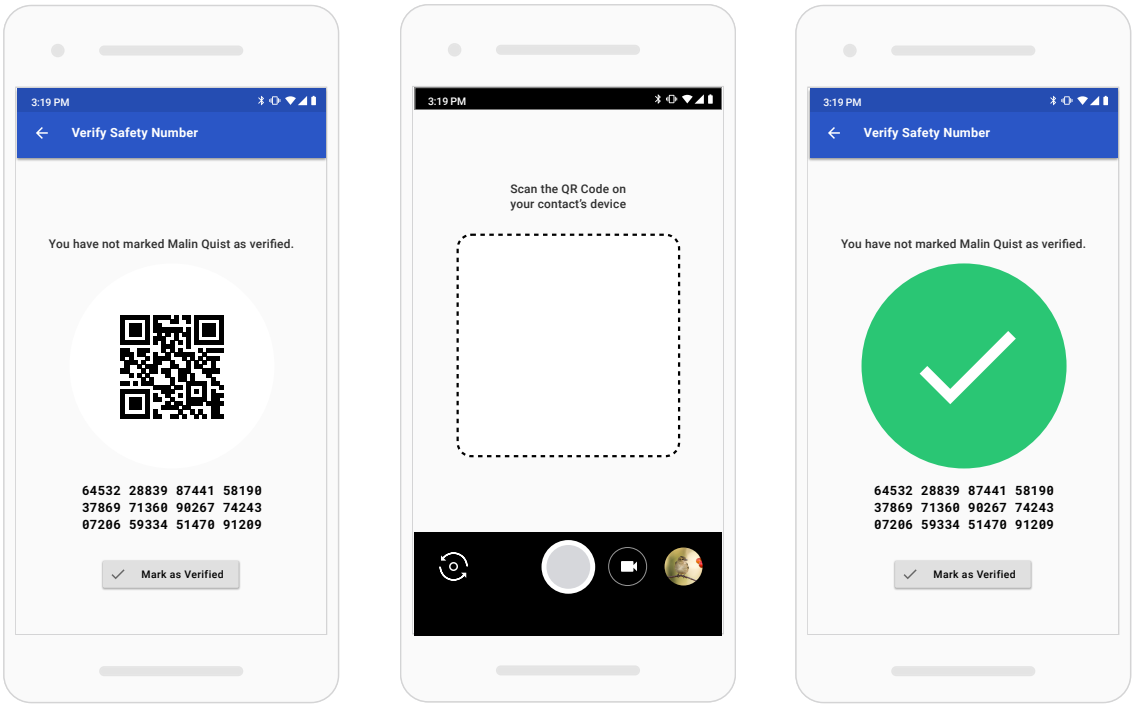
3 METHODOLOGY

Authentication ceremonies are social cybersecurity [34] mechanisms, which depend on conversation partners to meet up and improve their security equally. In this work, we try to understand how a user who fulfills all prerequisites, i.e., knowledgeable about security of messengers, experienced with the messenger interface, and sufficiently motivated, copes with authentication ceremonies



(a) Open the messenger conversation.

(b) Select "Verify Safety Number" in the conversation menu.



(c) Show QR code to conversation partner.

(d) Scan conversation partner's QR code.

(e) If check is successful, mark conversation as verified.

Figure 3: The step-by-step procedure to authenticate conversations in Signal and WhatsApp. The procedure is similar in other messengers that offer an authentication ceremony.

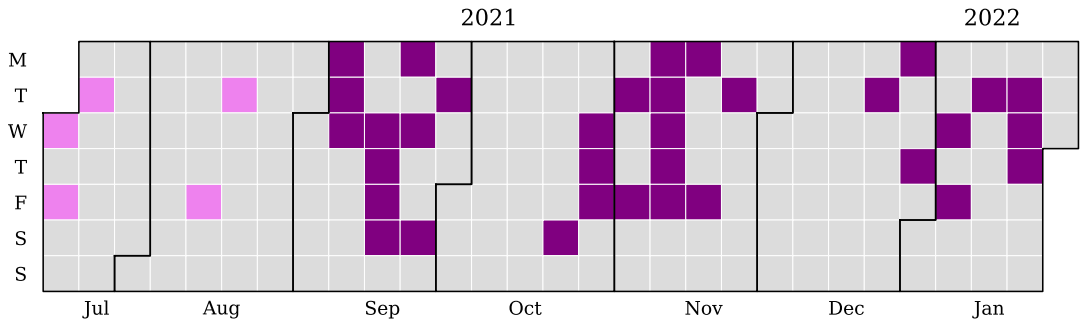


Figure 4: Calendar overview of diary entries. Dark purple days mark regular diary entries, while light pink days mark memories added at a later time.

in their daily life and how social and cultural factors impact these interactions.

Autoethnography, a self-reflective form of cultural analysis [5], is a powerful tool for understanding these ceremonies in-depth. We decided to use an autoethnographic approach based on three criteria: the usefulness of the first author's vantage point, the required level of introspection, and the necessity of sociocultural analysis. Section 2.2 contains the complete deliberation. In summary, we found that: (1) The *vantage point* as a usable security expert adds value to the analysis by collecting more data points and empathizing with people at different levels of skill and interest — instrumental to answering RQ1. In Turner et al.'s autoethnography [26], their cybersecurity expertise helped to reflect on their family's problems with security mechanisms in the smart home. (2) The *introspection* and reflection on the experienced authentication ceremonies help understand the scope of problems with authentication ceremonies and the depth of sociocultural issues. Achieving the same level of analysis with regular diary studies may be difficult. (3) The *sociocultural analysis* is necessary to answer RQ2.

Compared to lab studies, which use artificial scenarios and interactions, autoethnographies offer insights into more naturalistic experiences in the field. Long-term diaries are the appropriate basis for understanding these infrequently occurring authentication ceremonies. However, as discussed in Section 3.2, autoethnographies can not offer insights into entirely uninhibited natural interactions since the research question always influences the behavior to some extent when the researcher is also the participant.

In our systematic autoethnography approach, the first author's subjective experiences influence data collection, analysis, and results. The upcoming sections use the first person to communicate this influence honestly.

3.1 Procedure and Analysis

The autoethnography's data source is a research diary covering the five-month study period. For these five months, my goal was to authenticate as many secure messaging conversations as possible with any secure messenger installed on my phone (Signal, WhatsApp, and Telegram). While I would probably not try to authenticate every messenger conversation outside of this study — because not every conversation is that important — I did not want to limit myself to a specific subset of contacts for this study. This way, I could understand how different types of contacts and their social-context impact the corresponding authentication ceremony. In the spirit of Glaser and Strauss [9], I did not want to limit my data collection with preconceived theories. Hence, I tried to document all my unfiltered thoughts on authentication ceremonies. These thoughts can come up at any time, so the study required the possibility of creating diary entries on any nearby personal device. Day One, a personal journaling app, fulfills this requirement. Initially, I followed a trigger-based approach to collect data, creating diary entries whenever thinking about authentication ceremonies and describing as many details as possible. Over time, I developed more specific documentation patterns, closing in on reoccurring phenomena. In general, diary entries focused on either planning an authentication, the authentication ceremonies themselves, memories of past events concerning authentication, and introspection or analysis. Additionally, entries described immediate surroundings and what triggered thoughts about authentication. Later, I decided to add a periodic diary reminder, forcing me to reflect on overlooked authentication opportunities. Section A contains the guidelines I used for these diary entries. The length of all diary entries ranged from 30 to 400 words. However, most entries were between 50 and 90 words long. Sometimes I started shorter diary entries on the smartphone, only noting keywords, and expanded them later on my desktop computer.

Due to the nature of autoethnographic approaches, i.e., researching one's own experiences, data collection and analysis are parallel processes. I made this transparent by documenting ongoing analytic thoughts in the research diary. While these introspective moments provided some initial insights during the data collection phase, I also applied a structured approach to analyzing diary entries. To gather an overview of the concepts in the diary, I started with an open coding procedure on all entries with the help of qualitative data analysis software (ATLAS.ti 9). Based on this initial overview, I focused further analysis on planning phases, subjective emotional experience, and social and cultural aspects. For each diary entry, I consulted a Feeling Wheel [32] to help articulate corresponding emotions accurately. Autoethnography analyzes researchers' personal experiences in addition to the literal diary entries. Hence,

calculating inter-rater reliability or discussing agreement among several researchers is methodologically not appropriate [19], since other researchers may read the diary but can hardly reflect on the experience. However, I shared the diary in confidence with co-authors to identify overlooked aspects. That they did not find any that may be explained by our similar cultural background and opinions on the research topic.

In November 2021, two months after beginning the study, I conducted a preliminary structured analysis. In the collected data, I identified groups of entries that repeatedly centered around different parts of the process for planning and conducting authentication ceremonies. Based on this observation, I modeled the phases of planned authentication ceremonies (see Figure 5). Using this model, I placed all diary events in their appropriate context. Additionally, I used an explicitly abductive approach to identify areas of interest that were up to this point missing from the collected data. For example, during the study, I often forgot about planned authentication ceremonies. Forgetfulness impacted my trigger-based data collection strategy because it relied on me thinking about authentication. Hence, I added a periodic reminder to my diary software to identify and document missed authentication opportunities. At the end of January 2021, I conducted my final structured analysis. Based on the preliminary analysis of the data entries, I focused on three areas of interest: (1) potential barriers to planned authentication ceremonies and their location in the phase model, (2) subjective emotions and insecurities during the process of planning and conducting authentication ceremonies, and (3) the social and cultural aspects that impact authentication ceremonies. Section B of the Appendix includes the entire translated codebook.

3.2 Limitations

As with any methodological choice, autoethnographies come with limitations. The primary one is a lack of generality. Since all results stem from one person's experience, it is difficult to claim that they generalize. However, as Braun and Clarke [3] explain, strict generalizability is usually not a meaningful goal in qualitative research. Instead, they advocate for a more flexible 'transferability' approach that leaves it to the readers to identify how the results apply to similar kinds of situations and people. To improve the transferability of this work, we provided a detailed description of the first author's background in Section 3.4 and the circumstances and context of each interaction in as much detail as possible without compromising others' identities. Depending on the context, identified issues transfer to non-experts, albeit in a more severe manner. Put simply, when security mechanisms pose a problem to security experts we can not expect laypeople to do much better, regardless of user education and motivation. The lack of generality seems acceptable in order to surface issues that may affect users who are attentive to the need for authentication.

The second limitation is how the research affects the described behavior and experience. In an autoethnography, the researcher and participant are the same, making it hard to delineate naturally-occurring behavior from research-influenced behavior. However, to some extent, this is a common issue with many research approaches, e.g., the artifical scenarios in lab studies affect participant behavior and certain interview questions or environments will influence responses to some degree. To mitigate the effects of this issue, this work transparently communicates the ways in which the research approach may have influenced the reported results.

3.3 Overview of Collected Diary Data

From Sept. 3rd 2021 until Jan. 26nd 2022, I collected 69 entries in the research diary. In total, the diary contains 17 successful authentication attempts. While it is challenging to define clearly when an authentication attempt failed, I identified seven missed opportunities for authentication. I authenticated conversation partners in Austria, Germany, and Japan – almost all of them in person. I authenticated two contacts during a video call, one currently living in Japan and a work colleague I rarely see in person. In neither case, the video quality was good enough to scan the QR codes. Instead, we compared the safety number verbally. Figure 4 shows the distribution of created diary entries during the study period, whereby some days have multiple entries. Entries before Sept. 3rd represent memories I added after the start of the study.

3.4 My Cultural, Educational, and Security Background

Researchers' positionality affects all their research. Autoethnography, which focuses on their experiences, amplifies that effect. This section provides context about my environment and prior experience so that readers may judge the results in the appropriate context.

I am a white European man who grew up in the suburbs of a large metropolitan area in central Europe. I attended a high school specializing in applied Information and Communication Technologies (ICT). During that time, I was fascinated by the local hackspace and its security and privacy-minded members, which later led to my first part-time job at an NGO focused on data protection and privacy.

My first exposure to authentication ceremonies was PGP key signing. At that time, my circle of friends haphazardly authenticated PGP keys even though we never encrypted any emails. Using PGP and authenticating PGP keys seemed like a way of signaling that we belonged to the security and privacy-aware community.

During my master's in computer engineering, I became more interested in the then up-and-coming secure mobile messengers. I explained their purpose and corresponding threat models to countless users while demonstrating how to conduct them. During my Ph.D., I designed alternative ceremonies in the hope of improving usability and user comprehension through improved design. During this research, I was intrigued because even security researchers in my surroundings rarely authenticated any of their messenger contacts.

Since authentication ceremonies are social in nature, it also makes sense to tell you about my usual social demeanor. While I am critical of the introversion-extroversion dichotomy, I consider myself more an Introvert. I carefully balance my need for time alone with my need for social interaction. Disliking large parties, I prefer meeting one or two people at a time for in-depth conversations about personal problems, wishes, and dreams. Meeting new people or people I do not know well can be a draining experience, mostly

because I try to learn others' potential boundaries that I do not want to overstep so early after meeting.

3.5 Ethical Considerations

As this study collects subjective experiences with authentication ceremonies, it is not subject to our institution's ethical review process. However, studying experiences with authentication ceremonies necessarily involves other people – who can not meaningfully consent to their involvement in the study. I tackle this ethical issue by carefully considering which details of the encounters to describe. While contacts may identify themselves in the descriptions, I avoid disclosing more information than necessary.

4 RESULTS

I analyzed the resulting diary entries along three dimensions: (1) What process of planning and conducting authentication ceremonies looks like and what may go wrong; (2) Subjective emotions when planning and conducting authentication ceremonies, i.e., the authentication experience; and (3) The impact of the sociocultural environment on cooperative security mechanisms such as these.

4.1 Barriers during the Stages of Authentication Ceremonies

To give an overview of what the authentication process entails and also to embed my autobiographical reports in the correct context, I summarized the different phases of my experiences based on my collected diary entries in Figure 5. The following parts describe each of these phases in detail.

Recognizing Need. During the study, I depended on two different approaches to identify who to authenticate. The first and more intuitive approach is an ad-hoc in-the-moment authentication. When meeting and chatting with contacts, I sometimes remembered my wish to authenticate them. However, I could not depend on this method because often, I did not remember that wish in time. More than once, I remembered too late after the person was no longer within reach, e.g., when I sent them a follow-up message or when I wrote a diary entry thinking about missed authentication opportunities. However, as the study progressed, I habituated myself to think about authentication ceremonies when meeting people – making this approach more practicable. Although it only happened once during the study, I found it easier to authenticate others during the initial exchange of contact details. After we both had each other's phone numbers, I merely had to ask if they used a messenger and if I could authenticate them.

When I recognized the need to authenticate and the contact was not within reach, I had to plan a meeting for the authentication ceremony. For previously authenticated contacts, some secure messengers (e.g., Signal) alert users about encryption key changes before sending a potentially compromised message. In the one instance this happened to me, I wrote my conversation partner that we should authenticate again without making any specific plans. It turns out they had recently gotten a new phone, which is a common reason for changed keys. The alert worked insofar that it reminded me to make specific plans with that contact a week later. Since I did not want to depend on these alerts for this study, I also used a more structured approach. I scoured my list of conversations and checked if I needed to authenticate them (again). Usually, I sorted these lists by the location of the contacts and how easy it would be to meet them in person.

It is difficult to define what constitutes a failure this early in authentication ceremonies. Hence, it is hard to count the number of failed authentication attempts. However, I found it challenging to identify the need for ad-hoc in-the-moment authentication in time. And while I identified the need for planned authentication pretty well, I had a difficult time keeping track of them – at no point was I sure about someone's authentication status without double-checking in the messenger application.

Planning Meetings. Recognizing the need to authenticate while concerned contacts are within reach simplifies the authentication process. When they are not around during this realization, the process becomes more difficult. Then, planning a meeting is necessary.

At first, I planned these meetings around who I needed to authenticate. I tried to remember who to authenticate, checked the authentication status of recent messenger conversations, and sometimes reread the diary. Of course, further factors influenced my decision to set up a meeting, e.g., how much I enjoy spending time with them or the required logistics. Planning meetings was a considerable effort. Often, I documented in the diary that I would like a meeting – without planning one. In other cases, I managed to organize meetings (at least tentatively) and postponed them due to the pandemic. Once, a contact organized a meeting after I vaguely suggested one. This experience encouraged me to try to delegate some of the mental load of authentication ceremonies. So I asked conversation partners to remember to authenticate the next time we meet – with no success.

Later during the study, I stopped planning meetings based on the need to authenticate. Instead, I met who I wanted to meet and waited for suitable authentication opportunities. Hence, I shifted my focus from planning opportunities to identifying them. The Christmas season's social events provided ample authentication opportunities. They relieved me from having to plan separate meetings. Also, they made it possible to authenticate conversation partners when setting up an in-person meeting might have been socially inappropriate.

Meeting. When finally meeting contacts, I had difficulties identifying an appropriate time and place to bring up authentication. Usually, meetings begin with a ritual of greetings and inquiries about well-being. I certainly did not want to disrupt my friends when they recount their struggles with "Yeah, that's very interesting, but can we scan these QR codes now?". That would be disrespectful. It is unlikely that anyone would not want to treat friends like that. For me, this led to a repeating cycle of remembering that I wanted to talk about authentication and then deciding that the current situation was not the most appropriate one. For example, I postponed the topic of authentication during a lunch meal because I thought too many people were sitting at the table, a situation in which it could be impolite and awkward to attract everyone's attention to an authentication ceremony. On a different occasion, I postponed the topic because my conversation partner and I were strolling in a park when I remembered it. It seemed inappropriate to stop walking, stand in a circle, maybe block someone else's path to conduct a ceremony. However, postponing the topic can also backfire. During

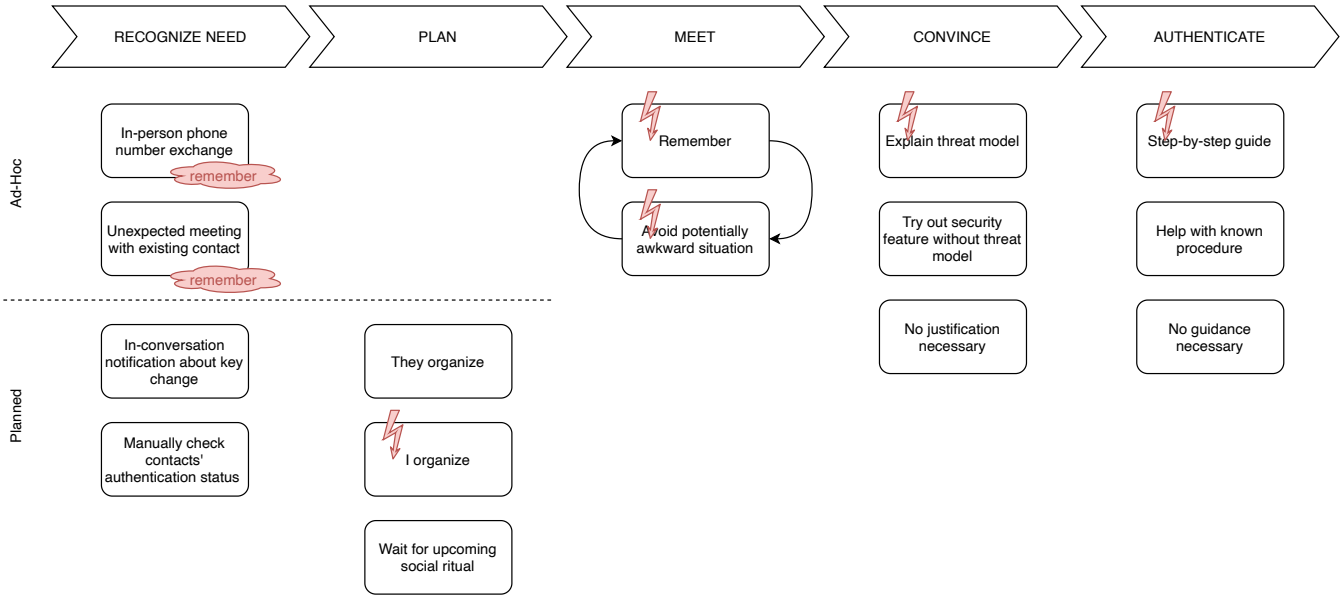


Figure 5: Planning authentication ceremonies: a process overview. Red lightning marks potential barriers.

a night out at the bar with a friend, I completely forgot about the authentication after I decided to postpone it. I forgot so thoroughly that I only remembered a month later, during an analysis session, that authentication was my original intent for that meeting! I had fun regardless.

This cycle of postponing is one of the reasons which made it easier to authenticate people I meet regularly. These more informal meetings include more calm moments in which it is not as rude to take out a smartphone or introduce an entirely new topic. However, since I usually talk in person to contacts I meet regularly, authenticating their secure messaging conversation is less important to my overall security.

Convincing. As a security researcher studying authentication ceremonies, I benefited from my perceived authority on the subject when asking others to authenticate. Had it been someone else, I am unsure if people would have followed along as readily.

If someone had not heard of authentication ceremonies before, I explained my research topic to them, inviting them to follow along with their messenger. This approach of interlocking the explanation of my field of research with their participation felt a bit manipulative. There is practically no way for them to deny my wish without coming across as rude. However, I did not feel too bad – it resulted in education about end-to-end encryption with no perceivable downsides.

For me, the most demanding authentication partner was a fellow security researcher. In pursuit of knowledge, they questioned everything and asked for detailed explanations of the encryption, the threat model, and the feasibility of practical attacks. This scrutiny came from a fellow peer after I described this as my area of research. An uncomfortable situation – it felt like they were questioning the validity of my research, even though they probably were honestly interested in the subject. In the end, they went along with the authentication ceremony, but it was a tough sell.

However, in many cases, requests for authentication ceremonies required no justification. Most of these cases were contacts I had authenticated at least once prior.

Authentication. For the most part, I did not encounter any issues with the authentication ceremony interface and procedure. I have extensive experience conducting authentication ceremonies. When contacts offered me their phone, I declined and instead instructed them in a step-by-step manner. Interestingly, I found that almost everybody (including the people I authenticated previously) had problems initiating the verification procedure. Afterward, they often asked what authentication ceremonies achieve. Usually, I tried to explain the effect in simple terms, e.g., "It makes sure that my phone encrypts the messages so that only your phone can read them. If the codes do not match, someone could be listening in and messing with our messages." At the beginning of this study, I thought my experience prevented me from experiencing usability issues. I was wrong. While I know the ins and outs of my preferred end-to-end encrypted messenger, I encountered a problem re-authenticating a secure chat on Telegram. Usually, I initiated a ceremony by sending a message to the contact, making it easier to find the correct conversation. However, I could not find this secure chat in my list, so I asked my contact to send a message to me – which I did not get. I was confused but did not want to dwell on it, so I gave up. Later I found out that secure chats on Telegram are only available on the devices that created them. Hence, my contact and I would have needed to create a new secure chat in any case.

Summary of My Barriers to Authentication.

(1) Planing meetings takes effort. Waiting for good authentication opportunities is easier.

(2) Forgetfulness. Remembering authentication plans and others' current authentication status is hard.
(3) The cycle of postponing. Remembering authentication in unsuitable situations leads to postponing.
(4) Convincing others to authenticate can be stressful.
(5) Some authentication procedures are still unintuitive.

4.2 Emotions during Planning and Conducting Authentication Ceremonies

Bella and Viganò suggested that security mechanisms should provide an enjoyable and beautiful experience, i.e., beautiful security [2]. In my experience during the study, authentication ceremonies did not fulfill the beautiful security criteria. This section describes my subjective emotional experiences while planning and conducting authentication ceremonies.

Overwhelmed by the mental load of planning authentication ceremonies. During most of the study, I felt overwhelmed by the information I needed to keep in mind. Even though I regularly checked the authentication status of my conversations, I felt stressed because I was never really sure about the authentication status of the people I met. Regularly thinking about authentication and potential opportunities became a significant part of my mental load. Often, I forgot to take advantage of good authentication opportunities. In these cases, I became frustrated and annoyed at myself. In contrast, I was usually even more proud of myself when I identified and remembered an authentication opportunity. I am glad that this study is over. I hope that I can forget about the need to authenticate and other people's authentication status now.

Worried about embarrassment or rejection in meetings. During meetings, I worried about the right time to ask for an authentication ceremony – postponing the request until an appropriate situation came up. Asking in an inappropriate situation could inconvenience my contact, hindering them from more entertaining, interesting, or relevant activities than authentication. In turn, I would be embarrassed for inconveniencing my contact. When the response to my request for authentication was not as enthusiastic as I had hoped, I felt rejected, inadequate, or even threatened. These feelings were at least partially related to the fact that authentication ceremonies are part of my research focus. Hence, skepticism and critique felt like an attack on my identity as a security researcher. In contrast, when my contacts eagerly went along with the authentication ceremony and asked relevant questions that I could answer, I felt respected, confident in my abilities, and proud to teach them something they found interesting and valuable.

Mostly content with the results. It felt good to complete authentication ceremonies and see the resulting "Verified" checkmark. It created a sense of achievement and progress. I was even happier when an entire group received the checkmark, i.e., I had authenticated all of its participants. Collecting is a powerful drive for many people. So, a group checkmark may have a similar effect to badge systems in gamification approaches [35]. However, not all authentication attempts ended on a positive note. Some secure messengers confounded me when they did not behave as expected. For example, one messenger claimed that I had marked someone as unverified while I did not remember doing so – making me doubt reality. In another instance, I wanted to reauthenticate a contact who had gotten a new phone. However, that conversation had remained verified. To this day, I still do not know why.

Carefully treading around conversation partner's emotions. Near the end of the study, I noticed that some contacts felt called out when asked for authentication. They got very defensive and felt the need to justify why they usually did not take certain security precautions. While this did not happen too often, it took some effort to convince them that I did not want to shame their behavior with my request. Usually, I explained that it is appropriate not to take security precautions they do not deem necessary, as long as this is their conscious choice. Thus, secure messenger users may need to consider their conversation partner's emotions about security in their request for authentication.

4.3 Sociocultural Aspects of Authentication Ceremonies

Previous result sections focused mainly on describing my experiences while planning and conducting authentication ceremonies. In the spirit of autoethnography, this section places these experiences into their broader sociocultural context. Thereby examining how sociocultural factors may hinder or facilitate authentication ceremonies.

Authentication ceremonies are embedded in social rituals. Meeting someone exclusively for an authentication ceremony, i.e., meeting without small talk, authenticating, and leaving, seems almost unthinkable – such a meeting sounds ludicrous. In meetings, I generally feel socially obligated to inquire at the very least about the other's well-being. Instead, I embedded my authentication ceremonies without a second thought in social rituals: I went for a walk with my contacts, went cycling with my cycling friends, met contacts for lunch or dinner, or talked with them during the afternoon coffee break at work. After all, I meet friends because I like them and want to catch up with them, not solely for authentication. However, while I do not consider myself shy, I had difficulties arranging meetings with some contacts. In particular, this concerned contacts that I do not know well and with whom I struggled to come up with a good reason for a meeting. Inviting others to a meeting usually implies an interest in a more personal relationship, which does not apply to all my messenger contacts. Hence, authenticating these contacts without arranging a potentially awkward meeting would only be possible if an appropriate situation came up by itself. As a result, some contacts are difficult or even impossible to authenticate if users miss a socially appropriate occasion. Not every authentication ceremony requires a social ritual. For example, I would not feel awkward calling my best friends just for authentication. However, this exception only applies to a few people.

Rules that govern social rituals apply to embedded authentication ceremonies. I authenticated my contacts in physical in-person meetings and remotely over video calls for this study. I decided the mode of meeting according to what felt right to me at the moment. I attempted to stick to familiar settings for authentication ceremonies. When I usually conversed with someone via video call, I arranged a video call. If I usually met someone over dinner, I invited them to

dinner. The idea of deviating from this procedure for an authentication ceremony felt off to me. I did not want to appear rude during the meetings and followed familiar conversational conventions. I avoided hijacking conversations centered around entirely different topics. Instead, I waited for an appropriate topic of conversation, where it seemed like phone use, messaging, or security would fit in. In particular, I avoided bringing up authentication ceremonies when others told me about their recent experiences and worries – I wanted to show that I care and would have felt ashamed of interrupting them in these personal moments. I found that not only can a conversation topic remind me of asking for an authentication ceremony, an authentication ceremony usually also influences the conversation topic for several minutes. Conversation partners may have considered it rude not to follow up on a topic that interested me. Usually, this resulted in a short educational episode about security on smartphones, regardless of whether I had intended it like that or not. Lastly, I found that using phones was not always socially appropriate. Seeing my smartphone reminded me of authentication ceremonies, so remembering them became harder in such scenarios. In any case, remembering an authentication ceremony was less challenging when the social situation allowed taking out phones. Striking up a conversation about messaging and its security was also less challenging when the conversation partner's phone was in view.

Established social practices can make it easier to authenticate others. Asking for an authentication ceremony immediately after exchanging contact details in person did not feel awkward during the study. Hence, this may be a viable approach to authentication when arranging a separate meeting for an authentication ceremony is socially inappropriate. Predictable sociocultural gatherings, such as Christmas, new years celebrations, or birthdays, were a perfect opportunity to conduct authentication ceremonies. Taking part in these gatherings does not require as much planning. Therefore, minimizing planning failures and potential social awkwardness. Also, these gatherings are usually informal so talking about authentication felt less like imposing a topic of conversation on others. Lastly, during some meetings, my planned authentication ceremony influenced others to try authentication ceremonies. This effect is in line with Das et al.'s [6] suggestion that social influence might drive the adoption of a visible security feature. Hence, conducting authentication ceremonies at social gatherings may create social network effects.

5 DISCUSSION

Based on the collected diary entries, two main reasons make it hard to authenticate even for motivated and knowledgeable users. First, planning meetings for authentication ceremonies and identifying good authentication opportunities creates a huge cognitive load. The first author had to think about authentication all the time and remember who they wanted to authenticate. They were bound to forget at least some of the time. Caring about authentication after forgetting once or twice requires a considerable amount of security motivation. Second, sociocultural aspects hinder widespread adoption. It is comparatively easy to authenticate people you meet often and know well. For other types of contacts, the experience was different. Sometimes, it might even be socially inappropriate to arrange meetings for authentication.

Simple measures, such as adding consentful and context-sensitive notifications, may alleviate the cognitive load of authentication. In comparison, overcoming sociocultural barriers to authentication ceremonies requires a dedicated design approach.

5.1 Designing Cooperative Security

Authentication ceremonies are a prime example of cooperative security mechanisms; two contacts need to cooperate to mitigate MitM attacks against either of them. Hence, well-known design principles for individual human-security interactions cannot solve this design challenge.

Other examples of cooperation from the Usable Security literature come to mind: users wait for other users' reviews of software updates before installing them [25], and users depend on their friends, who have their contact data, to keep their contact data private [21]. Enabling and supporting such cooperative behavior requires designing our security explicitly for it.

In the following, we discuss *cultural transcoding* as a core design issue for cooperative security. According to Manovich [18], cultural transcoding is one of the five principles of new media. They assert that new media consists of a *cultural* and a *computer* layer. Both of these layers influence how the other works. The effort of converting one aspect from one layer to the other is what Manovich describes as transcoding. Cooperative security mechanisms have two similar layers: the computer layer, consisting of cryptographic protocols and security requirements, and the cultural layer, i.e., the social rules that govern our interactions. During the study, the first author had to do the entire transcoding effort unsupported. It was their responsibility to integrate authentication ceremonies into their social life in a socially appropriate manner. It remains to be discussed who is responsible for this cultural transcoding work. At the moment, this task has to be performed by users of secure messaging applications. Integrating transcoding work in the design process for cooperative security mechanisms will move a part of this responsibility from the users to the designers.

For authentication ceremonies, an integration could work as follows. (1) Understanding what kinds of situations are appropriate for authentication ceremonies depending on the context of the relationship and other cultural factors; (2) Support users in identifying these situations; and (3) Support users in initiating these ceremonies in a socially appropriate way, e.g., by integrating them into a well-known ritual.

5.2 Self-Inquiry and Autoethnography in Usable Privacy and Security

Qualitative studies in Usable Privacy and Security use diverse methods to study security tools and their users, ranging from field studies to lab studies, using surveys and interviews. All of them are valuable to have in our method catalog. However, self-inquiry studies among security researchers are rare. When we, as researchers, deliberately get involved in studies, we do so in expert roles, e.g., for contextual walkthroughs, designing security features, or analyzing qualitative data. By comparison, we seem to disregard our own user experience with security features. We are users too and hence, our

self-reflections and experiences provide indispensable insights into the usability of security and thus form a valuable baseline for user research. If we have issues using security mechanisms, we should treat this as an early warning sign. This does not mean everything is fine if security researchers have no issues. Neither does it mean we should design security features just for ourselves.

Self-Inquiry is a systematic method to investigate our own experience with security features and tools. Over an extended period, it allows deep introspection of tool use. Whenever security and privacy mechanisms intertwine with social or cultural aspects, autoethnography is a viable research approach. In the case of this study, we chose this approach to systematically collect evidence based on experience instead of relying on anecdotal evidence alone. Since authentication ceremonies are highly contextual and depend on social and cultural factors, autoethnography is especially suitable to investigate them.

From our experience in this work, we found two aspects that future researchers who want to use this method may find useful. First, especially for reoccurring behavior, routinization during the course of the investigation may become an issue. Hence, the diary study itself may influence the behavior under investigation. We coped with this issue using reflection, transparency, and open discussion about its effects. Second, while the experiences and their interpretation are always the first author's, it is helpful to get feedback on how readers with a different background may interpret the situations as reported in the results. Based on that feedback, the authors can add more context to situations when it is necessary to sufficiently understand them.

Personal experiences influence and shape our research ideas. Since we cannot avoid it, we must communicate this influence transparently. We can even embrace this effect by seeking security-relevant experiences to investigate potential research ideas. Documenting these experiences in a diary helps trace the resulting research questions back to them. We plan to explore more kinds of new security technology in this way, documenting experiences, and finding potential research questions based on them.

5.3 Implications for Authentication Ceremony Research

The findings of this work suggest a change of direction for future research on secure messaging authentication ceremonies.

First, the results encourage the use of field studies for future work on the adoption of authentication ceremonies. While evaluating interface usability and user comprehension works well in lab settings, researching sociocultural factors is harder. Field studies of people's regular messenger use enable investigation of users' real-world behavior and the sociocultural factors that influence them. Field studies with proposed authentication ceremonies will likely require cooperation with messenger providers to arrive at results with a high ecologically validity.

Second, future research should include sociocultural factors in data collection and design. As this work demonstrates, current authentication ceremonies do not consider sociocultural factors in their design. However, designing ceremonies for these factors requires understanding their contexts of use. Hence, we need to collect data on how users want to authenticate their secure conversations. Given the security context of authentication ceremonies, focusing on the sociocultural context of users who are targeted by surveillance (e.g., members of protest movements) is likely a good first step.

Third, focus research and design on motivated and knowledgeable users with specific threat models. Effective security education is a challenge. Therefore, instead of investing research effort in everyone's security education, it might be wiser to identify specific groups of motivated users and work on removing their barriers to authentication ceremonies. The social influence could then lead to broader adoption of authentication ceremonies [6].

Lastly, our proposed phase model informs future research on authentication ceremonies. While prior work focused on the usability and user comprehension of authentication ceremonies, our results imply that other aspects, such as recognizing the need for authentication, planning, and remembering are crucial and should be better supported by technology. With the different challenges that we identified throughout the process, we argue that individual challenges, such as timing, need to be studied thoroughly and with more depth than in previous studies. For example, future design work may help users to identify conversations that are especially important to authenticate — corresponding to the "recognize need" phase. Other types of design work may make planning for authentication ceremonies easier or help identify convenient situations for conducting these ceremonies — corresponding to the "plan" or "meet" phase, respectively.

5.4 Alternative Approaches to Studying Authentication Ceremonies in the Field

While we preferred an autoethnographic approach for our research questions, other approaches – with different benefits and drawbacks – also work well for studying authentication ceremonies in the field. To support future research endeavors, we briefly discuss alternative approaches.

Diary study. Similar to this work, researchers may use a diary study approach to document participants' experience with existing authentication ceremonies. However, a diary study by itself will likely not get many naturally occurring authentication attempts; limiting the available data. One way to mitigate this issue is prompting participants to try to authenticate or ask participants why they did not conduct authentication ceremonies. The responses might tell us if participants felt it was important to authenticate the messaging conversation in question or how awkward or straightforward they found it to bring up the topic. These prompts likely impact users' natural authentication behavior, thereby reducing ecological validity.

Intervention study. An intervention study could be used to understand the factors that influence participants' authentication plans and behaviors. The interventions could explain threat models, demonstrate the necessary user interaction, or use role-playing to get participants used to authentication ceremonies. Afterward, surveys or interviews may help understand which of the interventions have a promising effect.

Prototype field test with pairwise recruiting. Testing a prototype of an authentication ceremony is difficult in the field since not only the participant but also their conversation partner need to use the prototype. Participants cannot use their regular messenger for this type of field test because prototype versions of authentication ceremonies are usually not interoperable with existing messengers. Since participants can only authenticate a limited set of conversations (with other study participants), this study approach lacks natural interaction. Recruiting participants pairwise ensures that each participant can at least authenticate one other person. However, this approach also makes recruiting more difficult.

Prototype field test in cooperation with a messaging company. Cooperation with an operator of a widespread secure messenger enables study designs with more ecological validity. Prototypes can be rolled out in regular A/B tests. Study participants can authenticate any conversation they like because their conversation partners' user interface adopts accordingly. The benefits of this approach are easy recruiting and natural user interactions. However, some form of a prompt might still be necessary to make users aware of the authentication ceremony and tackling qualitative research questions might be more difficult when cooperating with a messaging company. Also, establishing these kinds of cooperation with industry partners may prove difficult.

6 CONCLUSION

In this work, we used autoethnography to investigate why even motivated and knowledgeable users may have difficulties using authentication ceremonies.

Based on the collected data, we found that planning and conducting authentication ceremonies results in a huge cognitive load. The first author needed to keep authentication status in mind, plan meetings, and identify opportunities in time. Often, they forgot about the ceremonies, which resulted in a frustrating experience. Additionally, they had to constantly navigate social rituals to integrate authentication ceremonies in socially acceptable ways. Primarily, this navigation was necessary for formal relationships with acquaintances from work or the members of the extended circle of friends. In contrast, authenticating close friends was less complicated.

Consentful and contextual reminders may alleviate the cognitive load in many cases. However, addressing the social aspects of cooperative security mechanisms, such as authentication ceremonies, is more challenging. Integrating cultural transcoding into the design of cooperative security may improve the situation. Using this approach, designers would consider how culture influences security technology and how the security technology may affect cultural practice. Methods of self-inquiry, such as this work, are applicable in Usable Security and Privacy Research. They indicate design flaws early – if we have trouble using a security mechanism, others may have as well. Ultimately, we need to keep in mind that security researchers are users too. For future research on authentication ceremonies, we recommend using field studies to understand real-world use and the sociocultural factors that influence it.

ACKNOWLEDGMENTS

We thank our colleagues, Alexander Ponticello and Simon Anell, for their help in creating the teaser image. Also, we thank the anonymous reviewers for their helpful feedback and openness to unconventional methodological approaches.

REFERENCES

[1] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human–Computer Interaction* 15, 2-3 (Sept. 2000), 179–203. https://doi.org/10.1207/S15327051HCI1523_5

[2] Giampaolo Bella and Luca Viganò. 2015. Security Is Beautiful. In *Security Protocols XXIII*, Bruce Christianson, Petr Švenda, Vashek Matyáš, James Malcolm, Frank Stajano, and Jonathan Anderson (Eds.). Vol. 9379. Springer International Publishing, Cham, 247–250. https://doi.org/10.1007/978-3-319-26096-9_25

[3] Virginia Braun and Victoria Clarke. 2013. *Successful Qualitative Research: A Practical Guide for Beginners.* SAGE, Los Angeles.

[4] Alan Chamberlain, Mads Bødker, and Konstantinos Papangelis. 2017. Mapping Media and Meaning: Autoethnography as an Approach to Designing Personal Heritage Soundscapes. In *Proceedings of the 12th International Audio Mostly Conference on Augmented and Participatory Sound and Music Experiences (AM '17).* ACM, London, UK, 1–4. https://doi.org/10.1145/3123514.3123536

[5] Heewon Chang. 2008. *Autoethnography as Method.* Number v. 1 in Developing Qualitative Inquiry. Left Coast Press, Walnut Creek, CA, USA.

[6] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15).* ACM, Vancouver, BC, Canada, 1416–1426. https://doi.org/10.1145/2675133.2675225

[7] Carolyn Ellis and Art Bochner. 2000. Autoethnography, Personal Narrative, Reflexivity: Researcher as Subject. In *Handbook of Qualitative Research* (second ed.), Norman K. Denzin and Yvonna S. Lincoln (Eds.). Sage Publications, Thousand Oaks, CA, USA, 733–768. https://dx.doi.org/10.4135/9781446286463

[8] Matthias Fassl, Lea Theresa Gröber, and Katharina Krombholz. 2021. Exploring User-Centered Security Design for Usable Authentication Ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).* ACM, Yokohama, Japan, 1–15. https://doi.org/10.1145/3411764.3445164

[9] Barney G. Glaser and Anselm L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Developmental Psychobiology, Vol. 1. Aldine de Gruyter, New York. https://doi.org/10.2307/2575405

[10] Dan Goodin. 2018. Police Decrypt 258,000 Messages after Breaking Pricey IronChat Crypto App. https://arstechnica.com/?p=1408441

[11] Mary Lynn Hamilton, Laura Smith, and Kristen Worthington. 2008. Fitting the Methodology with the Research: An Exploration of Narrative, Self-Study and Auto-Ethnography. *Studying Teacher Education* 4, 1 (May 2008), 17–28. https://doi.org/10.1080/17425960801976321

[12] Amir Herzberg and Hemi Leibowitz. 2016. Can Johnny Finally Encrypt?: Evaluating E2E-encryption in Popular IM Applications. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust (STAST '16).* ACM, Los Angeles, CA, USA, 17–28. https://doi.org/10.1145/3046055.3046059

[13] Amir Herzberg, Hemi Leibowitz, Kent Seamons, Elham Vaziripour, Justin Wu, and Daniel Zappala. 2021. Secure Messaging Authentication Ceremonies Are Broken. *IEEE Security & Privacy* 19, 2 (March 2021), 29–37. https://doi.org/10.1109/MSEC.2020.3039727

[14] Kristina Höök. 2010. Transferring Qualities from Horseback Riding to Design. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction Extending Boundaries (NordiCHI '10).* ACM, Reykjavik, Iceland, 226–235. https://doi.org/10.1145/1868914.1868943

[15] Dhruv Jain, Audrey Desjardins, Leah Findlater, and Jon E. Froehlich. 2019. Autoethnography of a Hard of Hearing Traveler. In *The 21st International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '19).* ACM, Pittsburgh, PA, USA, 236–248. https://doi.org/10.1145/3308561.3353800

[16] Dan Lockton, Tammar Zea-Wolfson, Jackie Chou, Yuhan (Antonio) Song, Erin Ryan, and Cj Walsh. 2020. Sleep Ecologies: Tools for Snoozy Autoethnography. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference (DIS '20).* ACM, Eindhoven, Netherlands, 1579–1591. https://doi.org/10.1145/3357236.3395482

[17] Andrés Lucero. 2018. Living Without a Mobile Phone: An Autoethnography. In *Proceedings of the 2018 Designing Interactive Systems Conference (DIS '18).* ACM, Hong Kong, China, 765–776. https://doi.org/10.1145/3196709.3196731

[18] Lev Manovich. 2002. *The Language of New Media.* The MIT Press, Cambridge, MA, USA.

[19] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–23. https://doi.org/10.1145/3359174

[20] Aisling Ann O'Kane, Yvonne Rogers, and Ann E. Blandford. 2014. Gaining Empathy for Non-Routine Mobile Device Use through Autoethnography. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14).* ACM, Toronto, ON, Canada, 987–990. https://doi.org/10.1145/2556288.

2557179
[21] Yu Pu and Jens Grossklags. 2017. Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter?. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, USA, 339–355. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/pu
[22] Svenja Schröder, Markus Huber, David Wind, and Christoph Rottermanner. 2016. When SIGNAL Hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging. In *European Workshop on Usable Security (EuroUSEC 2016)*. IEEE, Darmstadt, Germany, 1–7. https://doi.org/10.14722/eurousec.2016.23012
[23] Katta Spiel. 2021. "Why Are They All Obsessed with Gender?" — (Non)Binary Navigations through Technological Infrastructures. In *Designing Interactive Systems Conference 2021 (DIS '21)*. ACM, Virtual Event, USA, 478–494. https://doi.org/10.1145/3461778.3462033
[24] Kate Stephens, Matthew Butler, Leona M Holloway, Cagatay Goncu, and Kim Marriott. 2020. Smooth Sailing? Autoethnography of Recreational Travel by a Blind Person. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20)*. ACM, Virtual Event, Greece, 1–12. https://doi.org/10.1145/3373625.3417011
[25] Yuan Tian, Bin Liu, Weisi Dai, Blase Ur, Patrick Tague, and Lorrie Faith Cranor. 2015. Supporting Privacy-Conscious App Update Decisions with User Reviews. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '15)*. ACM, Denver, CO, USA, 51—61. https://doi.org/10.1145/2808117.2808124
[26] Sarah Turner, Jason R.C. Nurse, and Shujun Li. 2022. "It Was Hard to Find the Words": Using an Autoethnographic Diary Study to Understand the Difficulties of Smart Home Cyber Security Practices. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22 Extended Abstracts)*. ACM, New Orleans, LA, USA, 1–8. https://doi.org/10.1145/3491101.3503577
[27] Ersin Uzun, Nitesh Saxena, and Arun Kumar. 2011. Pairing Devices for Social Interactions: A Comparative Usability Evaluation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, Vancouver, BC, Canada, 2315—2324. https://doi.org/10.1145/1978942.1979282
[28] Elham Vaziripour, Reza Farahbakhsh, Mark O'Neill, Justin Wu, Kent Seamons, and Daniel Zappala. 2018. A Survey Of the Privacy Preferences and Practices of Iranian Users of Telegram. In *Workshop on Usable Security (USEC 2018)*. Internet Society, San Diego, CA, USA, 1–20. https://doi.org/10.14722/usec.2018.23033
[29] Elham Vaziripour, Devon Howard, Jake Tyler, Mark O'Neill, Justin Wu, Kent Seamons, and Daniel Zappala. 2019. I Don't Even Have to Bother Them!: Using Social Media to Automate the Authentication Ceremony in Secure Messaging. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, Glasgow, Scotland, UK, 1—12. https://doi.org/10.1145/3290605.3300323
[30] Elham Vaziripour, Justin Wu, Mark O'Neill, Ray Clinton, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. 2017. Is That You, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, USA, 29—47. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/vaziripour
[31] Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jornad Whitehead, Nick Bonner, Kent Seamons, and Daniel Zappala. 2018. Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, USA, 47—62. https://www.usenix.org/conference/soups2018/presentation/vaziripour
[32] Gloria Willcox. 1982. The Feeling Wheel: A Tool for Expanding Awareness of Emotions and Increasing Spontaneity and Intimacy. *Transactional Analysis Journal* 12, 4 (Oct. 1982), 274–276. https://doi.org/10.1177/036215378201200411
[33] Justin Wu, Cyrus Gattrell, Devon Howard, Jake Tyler, Elham Vaziripour, Kent Seamons, and Daniel Zappala. 2019. "Something Isn't Secure, but I'm Not Sure How That Translates into a Problem": Promoting Autonomy by Designing for Understanding in Signal. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, USA, 137–154. https://www.usenix.org/conference/soups2019/presentation/wu
[34] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1863–1879. https://doi.org/10.1109/SP46214.2022.9833757
[35] Gabe Zichermann and Christopher Cunningham. 2011. *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps* (1st ed.). O'Reilly Media, Sebastopol, CA, USA.

A GUIDELINE FOR RESEARCH DIARY ENTRIES

Based on external triggers:

- Is it a memory?
  - *Try to remember as much details as possible. Use smartphone images and chat conversation history for memory clues.*
- Is it a plan to authenticate?
  - *Is it an abstract or a very concrete plan to authenticate?*
  - *How did I get the idea for this plan?*
- Is it an ad-hoc authentication?
  - *How did I get the idea to authenticate in that moment?*
- Details about the authentication ceremony itself
  - *What was the social context*
  - *Describe conversation topics before authentication ceremony*
  - *How did I remember the authentication ceremony*
  - *How did I ask to authenticate*
  - *Were instructions necessary*
- Is it a memory of a missed authentication opportunity?
  - *Try to think about the possible reasons for missing the opportunity.*

Based on periodic reminders:

- With whom did I meet?
- Did I have an (abstract or concrete) plan to meet these people?
- Did I miss an ad-hoc opportunity to authenticate?
- Do I know if these people I met have a secure messenger?
- Do I chat with them using a secure messenger?

Reflection entries (every two weeks):

- Unstructured thoughts about the social aspects of different meetings, e.g., the personal relationships and the context of these situations.

B CODEBOOK

- Planing and Conducting Authentication Ceremonies
  - AC with in-person exchange of contact details
  - Ad-hoc authentication
  - Ad-hoc check of authentication status
  - Almost forgot plan to authenticate
  - Asking for AC can be awkward in large groups
  - Bad timing of keyreset notification
  - Check contact list for authentication status
  - Cognitive load of planning authentication
  - Concrete plan to authenticate
  - Confused about messenger's UI response
  - Did not want to seem intrusive
  - Explanation of messenger's UI necessary
  - Fear of missing authentication opportunities
  - First time authentication
  - Forgot planned authentication
  - Negotiation about purpose and effects of AC
  - Negotiation: introduce AC as a personal research topic
  - No negotiation necessary (for re-authentication)
  - No planning necessary for people who you meet often
  - Not in the same city (makes planning meetings difficult)
  - Notification about required authentication
  - Other person organized meeting
  - Pre-warned conversation partner about authentication
  - Re-Authentication
  - Recognize need for authentication
  - Recognize need for authentication shortly after meeting

  - Recognize need for AC while planning meeting with a messenger
  - Remembered after meeting during messenger use
  - Remembered because of Phone use during meeting
  - Remembered because of rare or difficult meeting
  - Talk about my research reminded me of AC
  - Tread carefully as not to disturb other kinds of social rituals
  - Unclear how ohter person's authentication status came to be
  - Unexpected change of authentication status
  - Unspecific plan to authenticate in the future
  - Used different messenger for planning and follow-up conversation
  - Wait for upcoming social ritual
- Emotional Experience
  - Angry - Frustrated - Annoyed
  - Anger about my own forgetfulness
  - Bad - Stressed - Overwhelmed
  - Demonstration of competence
  - Desire to explore
  - Disgusted - Disappointed
  - Disgusted - Disapproving - Embarrassing
  - Fearful - Anxious - Worried
  - Fearful - Insecure - Inadequate
  - Fearful - Rejected
  - Fearful - Threatened - Exposed
  - Happy - Accepted - Respected
  - Happy - Content - Free
  - Happy - Interested - Curious
  - Happy - Proud - Confident
  - Happy - Proud - Successful
  - Peaceful - Thoughtful - Pensive
  - Sad - Guilty - Ashamed
  - Sad - Vulnerable - Fragile
  - Satisfaction of success / Amending a mistake
  - Surprised - Amazed - Astonished
  - Surprised - Confused - Perplexed
  - Surprised - Excited - Eager
  - Surprised - Excited - Energetic
  - Surprised - Startled - Shocked
  - Unsure about current authentication status
  - Unsure about future possibilities to meet
- Sociocultural Aspects
  - ACs and Security becomes topic of conversation
  - AC awkward in specific situation
  - AC harmonizes well with established social practice of contact detail exchange
  - AC not (yet) embedded in other social ritual
  - AC without social ritual
  - Authentication in front of others may lead to replication
  - Cooperative planing of Security
  - Demonstration and Explanation of ACs
  - Do not want to burden others with a meeting or an AC
  - Educate others about Security
  - Habituating myself to treat any meeting as a potential AC
  - Meetings not only about authentication, requires socially acceptable framework
  - Meetings with far-away friends is a social ritual
  - Meetings with Friends that I meet often are less ritualistic
  - Postpone AC until contact is geographically closer
  - Smartphone is a visual reminder (with questionable social acceptance)
  - Social Anxiety / Fear of Judgement impacts demand for AC
  - Socially inappropriate to plan a meeting
  - Social aspects more important than threat model
  - Social ritual
  - Topic of conversation triggers AC
  - Unsure if meeting will take place
  - Videocall with contact because it is the usual way of meeting