Design Considerations for Usable Authentication in Smart Homes

Sarah Prange
sarah.prange@unibw.de
Bundeswehr University Munich
LMU Munich
Germany, Munich

Ceenu George
ceenu.george@ifi.lmu.de
LMU Munich
Germany, Munich

Florian Alt
florian.alt@unibw.de
Bundeswehr University Munich
Germany, Munich

ABSTRACT

Smart home devices are on the rise. To provide their rich variety of features, they collect, store and process a considerable amount of (potentially sensitive) user data. However, authentication mechanisms on such devices a) have limited usability or b) are non-existing. To close this gap, we investigated, on one hand, users' perspectives towards potential privacy and security risks as well as how they imagine usable authentication mechanisms in future smart homes. On the other hand, we considered security experts' perspectives on authentication for smart homes. In particular, we conducted semi-structured interviews (N=20) with potential smart home users using the story completion method and a focus group with security experts (N=10). We found what kind of devices users would choose and why, potential challenges regarding privacy and security, and potential solutions. We discussed and verified these with security experts. We derive and reflect on a set of design implications for usable authentication mechanisms for smart homes and suggest directions for future research. Our work can assist designers and practitioners when implementing appropriate security mechanisms for smart homes.

CCS CONCEPTS

• **Human-centered computing** → *Ubiquitous and mobile devices*;
• **Security and privacy** → Usability in security and privacy.

KEYWORDS

smart homes, smart devices, usable security, privacy, authentication, story completion, thematic analysis

ACM Reference Format:
Sarah Prange, Ceenu George, and Florian Alt. 2021. Design Considerations for Usable Authentication in Smart Homes. In *Mensch und Computer '21, September 05–08, Ingolstadt, Germany*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/1122445.1122456

MuC '21, September 05–08, Ingolstadt, Germany

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The "Internet of Things" (IoT) arrived in our homes. Smart home devices come in different forms and with various features [27], serving purposes such as increasing comfort through home automation, enabling sustainable energy consumption [18], or supporting users in the household (e.g., cleaning robots or smart fridges).

Many of the aforementioned smart devices collect and provide access to sensitive data. Vacuum-cleaning robots may collect a floor-map of the house, smart meters monitoring water and energy consumption can assess when users are at home, smart fridges can place orders at the owner's expense, and smart TVs can access paid streaming accounts. As a result, there is a need to rethink how to design such devices in a secure and privacy-preserving way. In particular, means for authentication provided by such devices are scarce [17] and/or limited in security and/or usability [5]. For example, devices a) only require credentials once upon setup, b) rely on additional devices such as the user's smartphone as a proxy or c) transfer desktop metaphors [10] and require users to employ conventional authentication via unsuitable input modalities (e.g., passwords on a TV's remote control).

To address this, the users' perspective on security and privacy needs to be better understood, with the ultimate goal of supporting the design of usable authentication for smart homes. Obtaining such knowledge is important in smart homes, since this environment contains both, personal devices as well as devices shared by multiple people. As a result, knowledge from devices that are exclusively used by one person, such as smartphones, cannot easily be applied.

To close this gap, we conducted 20 interviews with users and non-users of smart home devices, using the story completion method [6]. We chose this method, since it fosters users to think beyond state of-the-art and imagine how smart devices may be used in the future. The story covered: choice of certain devices, setup process, interaction with the device, authentication, and potential issues that might arise by shared use with various roles (i.e., multiple users in shared households, children, guests). We then applied thematic analysis.

Our approach is complemented by conducting a focus group with security experts (N=10), where findings from the story completion method were discussed and further factors influencing the design of usable authentication for smart homes were identified.

Users and experts would design authentication mechanisms depending on the task for which devices are used, the data they are protecting, and the frequency of using the to-be-protected device. However, while users considered certain devices (e.g., cleaning robots) less critical and would thus not employ authentication, security experts were more sensitive as to which threats are possible and would employ authentication for here as well.

Based on the obtained insights from users and security experts, we discuss implications for the design of usable and secure authentication mechanisms for smart homes as well as directions for further research. In particular, the devices' modalities, access to functionality and data, and users' roles are of high relevance when designing authentication. Our work is useful for researchers as well as practitioners concerned with usable security in smart homes.

2 BACKGROUND & RELATED WORK

2.1 Smart Devices and Shared Use

Smart devices come in various form factors [27] and can serve different purposes in(smart) homes, including, but not limited to, sustainable energy consumption or home automation (cf. [18] for an overview). Hence, smart devices received considerable attention from the HCI community, in particular regarding suitable interaction models (e.g., [15]), usage and adoption. Also privacy concerns were subject to research [45, 47, 49] and some efforts have been made to design appropriate privacy mechanisms [38, 43].

Moreover, shared use of smart home devices has been investigated. Prior work highlighted that guests, children and co-inhabitants can use the device owner's account without them knowing [9]. Multiple users, including children and elderly people, accessing IoT devices may lead to challenges [2]. Prior results are based on a literature survey rather than on a user-centric study, which motivated our work. Garg et al. highlighted challenges of shared use as a results of their diary study, suggesting various levels of agency for users of the same device [8]. Sung et al. also include multiple users in their personalisation study for smart hoovers and propose a stronger focus on multi-user access [37]. Multi-user scenarios require suitable access control mechanisms [10, 46]. Ouaddah et al. provide an overview of access control for the IoT [25].

2.2 Authentication in Smart Homes

While providing valuable new features, IoT devices are prone to novel threats and attacks [48]. In the particular case of smart homes, there are two major classes of attackers [10]: external and internal. The latter have legitimate physical access to the smart home. At the same time, smart home devices often provide limited affordances for authentication and employ mechanisms adapted from smartphones and desktops [10]. Hence, users' experience of such mechanisms is limited [4, 5]. Others provide no security mechanisms at all [17].

Research tried to tackle this challenge. On one hand, prior work highlighted the need for authentication in smart homes and recommended authentication to be seamlessly integrated with devices [12]. Furthermore, as a home is – in contrast to online accounts – naturally shared, roles and relationships within the home should be considered when designing authentication [10, 36]. The general tension between home- vs device-centric authentication mechanisms has been discussed by Prange et al. [27]. On the other hand, few research proposed concrete solutions. An example virtual touch sensing to identify users by how they "pet" IoT devices [16]. Other examples include the use of biometrics (e.g., gait-based authentication [21]), analysing network traffic [24] or device-free authentication using WiFi signals to capture users' daily life activities [31]. Shah et al. provide an overview of novel authentication mechanisms for ubiquitous devices [30] not specific to smart homes.

2.3 Summary

In summary, authentication mechanisms commonly known from personal devices (e.g., smartphones) cannot easily be adapted for smart devices. On one hand, smart devices often do not provide the required input modalities (e.g., a touch screen or fingerprint sensor). On the other hand, authentication mechanisms need to blend with how sensitive the protected data is as well as with the way in which users interact with the device. In particular, for frequent use, time-consuming authentication mechanisms (e.g., taking out the smartphone and launching an associated app) lead to a significant authentication overhead. Knowledge-based mechanisms (i.e. mechanisms such as PINs or passwords that require people to remember a secret) further exacerbate the problem of people having to remember more passwords than they possibly can. Finally, in shared household scenarios, sharing the authentication secret might be desirable in some, but not in other cases. To address the aforementioned challenges, we explore how future authentication mechanisms for smart homes can be designed to be usable as well as secure. In particular, we investigated which mechanisms end-users would imagine *usable* in a smart home (study I, Section 3) and assessed *security* in a subsequent expert focus group (Section 4).

3 STUDY I: STORY COMPLETION

To understand the requirements for future smart device's privacy and security mechanisms, we set out to capture users' opinion and desires with regard to smart home interactions. In particular, we chose to conduct a story completion study [6]. This method provides participants the beginning of a story and then asks them to complete it as to their imagination.

Our choice was motivated by two factors: Firstly, we wanted users to imagine future scenarios without being limited by state-of-the-art smart devices. Secondly, although the smart device market is continuously growing, it has not penetrated all households yet [29], hence allowing us to include both, users and non-users.

We extended the original methodology by Clarke et al. [6] to allow shifting the focus towards potential problems and issues related to privacy and security, and in particular authentication. Similar to the original method, participants were given the start of a story. However, in our design, we guided users' stories in the further course of the interview by suggesting pre-defined story changes. Later parts of the story were based on the device participants chose in the beginning. Changes were introduced in the same order to all participants to form a consistent storyline (see Section 3.2 for details). We wanted to immerse all participants in the scenario, device choice, and functionality before thinking about authentication and potential problems. Note that this study particularly focused on mechanisms that are *usable* as imagined by participants. As for the *security* perspective, we conducted a focus group with security experts (see Section 4).

3.1 Motivation for Stories

The motivation for our stories is two-fold. On one hand, current smart home systems rarely provide security mechanisms (such as, e.g., access control) [17], but are at the same time prone to new threats [48] from within or outside the smart home [10]. If existing, security mechanisms for smart devices are of limited user

experience [4, 5]. Hence, our stories not only cover device choice (part A), but also (imagined) functionality and usability (part B), and authentication mechanisms (part C). On the other hand, challenges arise from shared device scenarios within households (cf. [8, 9]) with a potential for inside attacks [10] (part D). In particular, we cover the following roles: shared use within a relationship [8, 46] (D1), and visitors [1, 19, 44], including children [20, 40, 46] (D2-3).

3.2 Stories

We created a scenario around Lara and Tim, a couple who recently moved together in their house and is interested in buying a smart home device (cf. Appendix A for full interview guide). The interviewees had to complete the story. To focus the story towards challenges of shared use and authentication, we implemented structured changes. We describe those changes below.

A. Choice First, participants needed to decide on a *specific smart device*, motivate their decision as well as describe expectations and potential use cases. We intentionally left this choice to the participants to help them immerse in the story. The following parts are based on this device.

B. Functionality & Usability After they ordered and received their smart device, they needed to describe how they setup the device in their home infrastructure. This included the setup process, functionality, and interaction modalities. We wanted to understand if participants see setting up an authentication process as part of the initial setup (as it is the case, e.g., for mobile devices).

C. Authentication Mechanisms As smart devices may collect and store personal data, they should describe a suitable authentication mechanism for the device, considering how frequently it would be used. This part of the story should encourage participants to brainstorm concrete mechanisms.

D. Shared Use Prior work identified varying types of users that share smart home devices, including spouse, children and friends [8]. Based on their results, we included D1-D3 to provoke stories with specific types of users to understand whether authentication mechanisms differ depending on types of users sharing the device.

D.1. Couple Problems may arise within the household, as Lara and Tim share the smart device. We asked participants to come up with such problems that are a result of sharing, and to also include potential solutions.

D.2. Children As children (Lara's nieces/nephews) visit their home, Tim gets worried as IoT devices pose a privacy risk for children [20, 40] and consequences from children playing with devices are unknown. The story should comprise negative aspects and countermeasures.

D.3. Worried Guest A very privacy concerned friend is visiting Lara and Tim. They want to convince their friend about their smart device and, thus, their home still being secure and privacy-preserving (e.g., from surveillance).

3.3 Recruiting & Procedure

Participants were recruited and interviewed in a public park close to the local university and compensated with one free, non-alcoholic drink. After agreeing to take part in the study, participants were given a short introduction to the topic of the interview and information on our research and data collection. Independent of their prior knowledge, this included a description of the setup and a list of possible smart devices. They were then asked to sign a consent form. Next, they were introduced to the concept of the story completion exercise. For the main part of the study, participants were given the beginning of Lara's and Tim's story and asked to complete it. The rest of the interview was structured according to the story changes described in the previous section. After the story completion exercise, we gave participants the opportunity to give feedback or ask questions. We audio recorded all sessions.

3.4 Participants

We recruited 20 participants. The majority (15) was between 20 and 29 years old (2 below, 3 above this age), 9 identified as female (others as male), mainly students (11) or employees (6). Five had at least one smart home device. Out of those, all had a smart TV, 2 had an Amazon Alexa, 1 a Sonos music system and 1 a smart thermostat. We did not count smartphones, although they were mentioned by two participants. On a 5-point Likert scale (1=do not agree at all; 5=strongly agree), participants perceived their technical affinity as rather high (Mean=4.6, SD=0.6).

3.5 Limitations

The study was completed among students in Germany, with the majority being below 30 years old. Results may thus only apply to a similar target group. However, smart home technology is popular among this age group in Germany [35]. Also, our sample size is limited ($N = 20$). Note, however, that only little new information is gained beyond 20 participants [22].

Participants may have been influenced by experiences with smart devices. However, we believe this to be a minor limitation, as (a) there were only five participants who already owned a smart device, and (b) we did not notice any differences in stories between users and non-users. Changes to the story were based on hypothetical situations users might encounter. We ordered the changes based on how we expected them to naturally occur (e.g., purchasing the device, setting it up, choosing an authentication mechanism, shared use). Generally, shared use could occur before setting up authentication. We acknowledge that we did not consider this case.

Finally, experimenter bias is a known limitation for qualitative studies. As such, there may be alternative themes or names that may be given to certain sections. However, we believe that this would not influence the resulting design considerations.

3.6 Ethical Considerations

With our study, we made sure to follow all guidelines provided by our institution(s) and all national data protection regulations. In particular, we limited the collection of personal data to a minimum. All data was assigned to a pseudonym chosen by the participants.

3.7 Data Analysis

We conducted 20 interviews with an average length of 20 minutes. One participant data was excluded due to technical issues with the audio file. We transcribed all other interviews. Results were analysed through thematic analysis [3] by two experimenters.

Firstly, we independently went through half of the dataset each. Secondly, we merged our codes and iteratively found sub themes. We went through each story part (A-D) and analysed top-level aspects as directly derived from our interviews. This includes which **A** choice participants made (*Appliances*) and why (*Reasons*), **B** how they imagine the device in terms of *Functionality*, *Setup* and *Interaction Modalities*, and which **C** *Authentication Mechanism* they would imagine. We further looked into which *Problems & Concerns* may arise from **D** *Shared Use* depending on type of user, namely, **D.1** couples, **D.2** children, and **D.3** guests, including potential *Solutions*. Sub level themes resulted from our iterative analysis. We found and included *Attacks & Threats* as an additional top level theme, as participants voiced those without our guidance. To provide a descriptive overview of our data, we give counts for device choice and authentication mechanisms. Appendix C shows the full list of codes. Quotes were translated from the original language. We cite participants (P) with their self-chosen ID. We explicitly mark quotes of device owners with, e.g., $P27_{owner}$.

3.8 Results

3.8.1 Appliances & Reasons (A). Participants mentioned various devices. Most popular were *household* devices (21 mentions; including vacuum cleaning robots, fridges washing machines, coffee machines, dish washers, heaters, lights), followed by *entertainment* (7; including smart voice assistants and TV), and *security* (3; front door camera and door lock). Some also included multiple devices. Note that only one of the current smart home users chose the device they already have (smart voice assistant, $P19_{owner}$) for their story.

Participants described reasons for purchasing a particular smart device mainly with increased *comfort*. They mentioned *priority* and *frequency of use*, *societal benefits* and *control* over their home to motivate their device choice. The aim of this part was to immerse participants in the story rather than to explore actual appliances and reasons. Hence, we will not include them in the later discussion. However, they are included in our results. Overall, these confirm prior work that explored reasons for smart home usage [11].

3.8.2 Functionality, Setup & Interaction (B). To further immerse participants in the story, we asked them to describe (desired) *functionality* and *interaction modalities*. With this part, our aim was to provoke thoughts around the device, its access to data, and a potential need for authentication, including available modalities.

Functionality. Many household devices should take over usual tasks, including, but not limited to, ordering groceries (P33, P80), manage shopping lists (P33), or vacuum cleaning (P42, P71). P36 would have liked if their hoover plays music to drown out the cleaning noise. P71 would have wished for an "allround" hoover, including indoor (vacuum cleaning) and outdoor (lawn mowing) use, playing music, being waterproof and pre-programmable.

Interaction Modalities. For the respective devices, stories included multiple interaction modalities, mainly via *voice* and *touch* input, but also using *companion apps* on smartphones, and others. Note, that some participants did not include a concrete modality, and some also mentioned multiple interaction modalities for one device (e.g., a display at the device as well as a companion app, P80). While voice was most prominent, P5 explicitly mentioned that it might be challenging for food orders. P53 and P80 involved an additional *smart assistant* as proxy for interaction. P26 described a (limited) list of voice commands for their smart device to hang up in a prominent shared place like the kitchen. P42 and P71 mentioned *no interaction*, as the device is acting *autonomously*. P71 further mentioned "indirect" interaction, i.e. *"close the doors of rooms which it [the vacuum cleaner robot] should not enter"*. Interaction modalities being (not) available may have a strong impact on the design of authentication.

Authentication Mechanisms		
Biometrics	fingerprint	11
	face scan	6
	voice (commands, recognition)	6
	other (iris, hand)	2
Token	proximity of smartphone	1
Knowledge	PIN	3
Other		5
Modalities	at the device itself	11
	via an app / the smartphone	7
	at an additional device	4

Table 1: Overview of authentication mechanisms participants mentioned in their stories.

Setup. Necessary steps for the *initial setup*, as described by participants, included the connection of the smart device to both, the Internet and/or other devices within the home. While some participants would simply "plug and play", others would read the manual first. Regarding *authentication*, participants mentioned that it might be necessary to enter credentials (P69, P80), login on the device via a second factor (i.e., downloading a code and entering it on the device, P14) or authenticate the new device automatically, depending on other devices within the home ($P19_{owner}$, P21).

3.8.3 Authentication Mechanisms (C). We asked participants to add an authentication mechanism to protect personal data as collected or being accessed by their chosen device from illegitimate access.

Some participants mentioned multiple authentication mechanisms per device. We considered the final mention (cf. Table 1).

Participants mainly referred to biometric mechanisms. They appreciated that such mechanisms would be easy and convenient to use (e.g., *"you just need to approach the device and it recognises you [via face recognition]", P24*). *Other* mechanisms included two-factor authentication (by sending a code to the smartphone, P21) or encryption of the collected data using a public/private key pair (P42). P42 would also deactivate the Internet connection completely when a device is not in use rather than employing authentication.

Many participants would use the smartphone as a proxy for authentication, or another additional device such as a remote control for smart TVs ($P27_{owner}$) or a voice assistant (P69, cf. Table 1, *Modalities*). At the same time, $P39_{owner}$ states that *"a vacuum cleaning robot may anyways not be that privacy relevant"* and using an app (incl. the phone's unlock mechanism) may be enough protection.

We found differences in *when and how often* participants would authenticate. Examples include *once upon setup*; unlocking *when entering the home* (e.g., *"Maybe it's only when they enter their flat. As soon as they touch the door handle, the whole household is unlocked as it is by then clear that it's the legitimate owner."* , P53) or *per use* (e.g., prevent children / party guest from ordering food via the smart fridge, P1).

Furthermore, some participants raised *challenges* with potential authentication mechanisms without being explicitly asked for it. Examples include technical limitations, such as fingerprints not working (*"It [fingerprint authentication at the smart fridge] is unpractical if the fingers are wet during cooking."*, P1), thus preferring another mechanism (face scan in the case of P1), and unwillingness to share biometric (i.e., fingerprint) data with the device provider (P22). $P39_{owner}$ mentioned face recognition would need to work with multiple faces in a shared household scenario (whereas FaceID on their phone can only store one face, $P39_{owner}$). Furthermore, in family-shared scenarios, voices and faces are similar by default, which may lead to false positives. Another challenge is authentication at doors of smart homes. Memorable passcodes may be too easy to guess for potential attackers (e.g., family member names) and voice recognition too unstable (e.g., when user is hoarse) or too easy to mimic (compared to, e.g., fingerprint, $P27_{owner}$).

3.8.4 Problems & Concerns of Shared Use (D). Although some problems were user type specific, the majority can be applied to all. Hence, we mainly focused our analysis on overarching themes of problems and concerns that directly or indirectly open a need for suitable authentication mechanisms and are thus included in our design implications (e.g., the presence of multiple users and/or bystanders, cf. Section 5.3 or the frequency of usage and related issues, cf. Section 5.2).

Users & Bystanders. Some problems involved only *one user* and the smart device. As an example, $P19_{owner}$ and P5 mentioned possible "response delays" that they might find annoying. The second, more prominent problem group included *bystanders* (e.g., children/visitors). Shared use was problematic, as it involved shared data access (e.g., *'The partner can see when lots of meat is ordered, although they decided to be vegan together."*, P24) and changing settings (*"Users with similar voices might accidentally change settings."*, P69). Similar concerns were voiced by $P19_{owner}$ and P22, who said that not differentiating users over time leads to annoyance.

Several problems with *children* were identified: Firstly, children could "break" (P22) something, "lock access" (P21) or "order too much [online]" (P1). However, the more severe consequence of misuse was possible physical harm (e.g., *"Kids are only a problem when the smart device is something that can hurt someone, e.g. windows that can break, jalousies that fall on someones head, etc."*, P24).

Furthermore, *visitors* might not like (P5) or not agree to the use of smart devices (P5, $P19_{owner}$). $P19_{owner}$ specifically asked whether *"co-located people gave consent?"* when asked about how they would interact with smart devices and P1 asked *"who is responsible for creating trust [towards the device]"*.

Responsibilities & Ownership. As our story protagonists will share the smart device by default, participants mentioned issues regarding *responsibilities* and *ownership*. As an example, participants mentioned that preferences of users may interfere, leading to annoyance of users, but also to unclear settings of the device ($P19_{owner}$, P22, P33, and $P39_{owner}$). Furthermore, in case of the device being able to place orders, double purchases may occur (P80), leading to monetary loss. Especially for such cases, permissions seem to be unclear, e.g. *"Who is allowed to do what? Can Lara use Tim's PayPal account?"* (P42). From a technology perspective, sharing devices oftentimes means to manage multiple user accounts. Some participants mentioned this might be limited, e.g., a smart coffee machine may not be able to store enough profiles (P53).

Frequency. Problems, as illustrated in our stories, may occur at various *frequencies*. While problems from sharing the device with other inhabitants may occur daily, problems with guests and visitors may only emerge occasionally. Another factor might be the *frequency of interaction*. If interaction (e.g., based on voice commands) fails during a frequent task (e.g., cooking), it might be more annoying than on rare tasks.

Frequency also had a subjective component. P71 perceived *"changing of the Roomba bin bag"* to be a frequent problem, as it was *"tedious and fault prone"*. Another comment describing a *maintenance* problem was the *"management and extension of [data] storage/space"* (P14). Participants had different opinions as to how this should be handled. P22 suggested data should *"stay on the local device"* until the owner decides what to store *"on the internet on a monthly basis"*, whereas P14 suggested this needs to be done when *"the storage is full"*. For a smart fridge, $P23_{owner}$ expected to be informed *"every time my girlfriend orders tons of vegan food"*.

3.8.5 Attacks & Threats. Although we focused the story line mainly around usability aspects, we found participants specifically raising concerns regarding potential threats and attacks, coming from within or outside the smart home [10]. As threats are an important aspect to consider for the design of authentication mechanisms, we included this additional theme.

Inside. Potential "attackers" might appear *inside* the smart home in several ways. *Mimicry* attacks [14] might occur in such a way that children could impersonate their parents (i.e., actively try to trick a voice recognition system) ($P27_{owner}$). However, *similarity* might also lead to an unintended threat, as relatives sound similar to each other by nature (i.e., confusing the voice recognition without intention). As a consequence, children might get access to improper content (P5, $P27_{owner}$) or place undesired food orders (P1). Furthermore, users might want to prevent (potentially drunk) party guests from ordering food (P1) or changing settings of smart devices. Finally, a feeling of surveillance (P36) or fear of dependence on technology (*"life not possible without a smart home"*, $P27_{owner}$) are potential threats within smart homes.

Outside. Attacks might also come from *outside* the smart home. While this may occur in the form of physical attacks (i.e., burglary, P71), others may also be purely digital / cyber-based. Types of attacks participants mentioned ranged from hacking (P36, P42), via (undesired) permanent video recording and transfer from unexpected devices (e.g., from a webcam in the smart TV, P36) to complete surveillance ($P27_{owner}$). For these types of attacks, consequences are severe, as somebody with illegitimate access *"could control my whole house"* (P36). P42 further stated that *"bad guys make it public on the Internet that and how it is possible"*, which may foster further outside attacks on smart homes.

Misconceptions. On one hand, we found participants describing security measures on smart devices as unnecessary, as a hoover might not be privacy invasive ($P39_{owner}$). However, we consider

such data indeed protect-worthy as, for example, recent data leakage of such vacuum cleaning robots mapping home's floor plans shows[1]. On the other hand, we found overly sceptical participants who would disconnect devices from the internet completely (P42, P66) or even put them in the freezer to stop tracking (P71).

3.8.6 Solutions. Participant suggested various solutions when facing problems (cf. story part D) or, more precisely, threats (cf. previous section). We grouped them into two categories which we describe below.

Empowerment through the Technology. In some stories, improving technology resolved the threat or gave users more power to avoid it before it happened. P14 suggested that smart devices should automatically log users off if they have not used it for a while. P21 described a "kids sensor" to disable access for children. Participants had great expectations towards the device, considering its "smartness" (e.g., *"device sends alarm [when faced with a threat]"*, P36). An extension of internal storage (P14) or improved voice recognition (P69) could solve some of the problems. Participants were expecting the smart device to automatically detect and deal with a possible threat or problem.

Empowerment through the User. Users also provided solutions such as unplugging the device (P27) and even putting it in the freezer (*"In the freezer it cannot harm anyone [..] I would not be able to get unwanted spam if it is in the freezer"*, P71) to stop privacy invasion. Having rooms that are free of smart devices and, hence, "safe" ($P23_{owner}$) was another alternative. In $P23_{owner}$'s story, the male protagonist was able to "see the girlfriend's orders" and had the "power" to make changes to it. Having access to data and being able to edit and delete it, seemed to be linked to a sense of power over the device (and its users). A recurring theme was *education* – for oneself but also for guests (e.g., *"Getting a live demonstration of how easily something is hacked would help me understand how to be more secure in interacting with a smart device."*, P42 and *"[...] guests should be educated about what data is being stored and captured. Of course this is a difficult conversation but if you explain it carefully and with facts, they will listen to it [...]."*, $P39_{owner}$).

3.9 Summary

Participants mainly chose known devices for known purposes (cf., e.g., [18] for an overview). However, we used this part of the story (A-B) to immerse participants in the scenario and to be able to focus on authentication mechanisms that are specific to smart home devices rather than to ubiquitous devices in general.

Independent of whether participants owned a smart home device or not, they mentioned authentication mechanisms and problems equally. Notably, device owners mentioned aspects not specific to their devices. For instance, $P19_{owner}$ mentioned the device they already have (smart voice assistant), but elaborated the story beyond what is currently common for it (i.e., the users' phone as token for authentication). Other device owners mentioned different devices in their stories, e.g. $P27_{owner}$ owns a smart TV, but mentioned a smart voice assistant and voice based authentication in their story.

[1] https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html, last accessed June 3, 2021

To summarise, all stories of all participants raised aspects that open a need for authentication, e.g. the potential for attacks from within the smart home [10]. Examples from prior work include children who are misusing the smart home for their gain [8] and smart lights that left shared users in the dark when the owner left the house [9]. To respond to issues of shared use, participants mentioned the need to create multiple profiles. This would empower them to give rights to specific groups of users and educate them about their profile. Geeng and Roesner [9] discuss this in the context of "relationships" between the owner and the user, implying that the person who buys and installs it might not necessarily be the user, again opening a need for authentication.

Finally, access control [10, 25, 39] and shared use [8] have been subject to prior work. However, we specifically focused on users' perspective of potential problems and threats that may occur in the smart home and, in consequence, impact the design of suitable authentication mechanisms. In contrast to prior work, we also assessed these findings from a security perspective in a focus group. In particular, our findings from users' stories informed the questions we discussed with the focus group experts (e.g., potential threats in smart homes and authentication mechanisms for particular devices).

4 STUDY II: EXPERT FOCUS GROUP

We conducted a focus group ($N = 10$) to assess our findings from a security experts' perspective. We chose this method to encourage discussions among participants with various competencies in the field of IT/usable security. Experts were recruited among PhD students ($N = 7$), post-docs ($N = 2$), and professors ($N = 1$) from a research institute on cyber security, with which two of the authors are affiliated. Participants were experts in different sub fields of IT security, including network security, software security, as well as usable security. The purpose of the focus group was twofold: (1) we were interested in how the views' of end users and security experts match, to validate our findings; (2) we complemented our initial investigation with further insights that ultimately shaped our design implications presented in the following.

4.1 Procedure

The session took one hour. After explaining the purpose of the focus group, we presented insights from the story completion exercise and discussed these. Discussions were complemented with a brainstorming about solutions to aspects identified in the first study. The focus group evolved around the following topics: threats, threat recognition, awareness of data tracking, sensitivity of data collected by smart devices, and suitable authentication mechanisms for particular devices (cf. Appendix B for details).

4.2 Results

We now summarise the results from our focus group. We cite experts (E) with randomly assigned IDs (range 1-10).

4.2.1 Attacks & Threats. Experts discussed potential attacks and threats emerging from smart devices.

Physical Harm. Analogous attacks may potentially be transferred to or be supported by smart devices, resulting in physical attacks

on the home, or even cause physical harm to the user. Examples included eavesdropping sensitive information (manually or supported by, e.g., a smart speaker), burglary, lock out scenarios, fire (via, e.g., a smart oven), or creating strobe effects by turning lights on and off at high frequency, which might cause seizures.

Network & System Attacks. A single smart device may serve as a "jumping point" for other devices. Hackers may further attack the home via DDoS (distributed denial of service) attacks or read sensitive data from network traffic (e.g., if the user is at home). The experts further questioned how the system might react in case of unforeseen events (e.g., guests present in the home). Devices might get "out of control". Adversarial attacks were mentioned in case access to the device includes machine learning (such as face recognition).

Data Access & Privacy. Further potential attacks on users and their smart homes included privacy breaches and surveillance issues. Interestingly, experts not only saw guests' privacy at risk (as we discussed previously for our stories in study I), but also the owner's privacy in case a visitor comes to the owner's home with tracking technologies.

4.2.2 Automatic Threat Recognition. For some threats, the security experts found solutions that detected threats automatically. Experts suggested that usage pattern may be used to detect a) intrusion or b) harmful behaviour of the smart system. These kind of "survey systems" (E3) need to be independent to the main smart device.

4.2.3 Increase Awareness of Data Tracking. To increase the awareness of data being tracked, experts suggested visualisations [26] (e.g., AR based), and notifications (e.g., on the user's smartphone or smart watch). A further suggestion for awareness of Alexa currently tracking was to explicitly ask her "Do you still hear me?". All experts agreed that it is the law makers' responsibility to enforce means to increase tracking awareness, such as, e.g., physical signs (cf. signs in areas under video surveillance according to national data protection regulations). For smart devices, this may also mean to propose regulations to limit the reach of tracking. For example, E2 said *"if users knew that microphones on smart devices were limited to track within 2 metres, they may not need visualisations or notifications every time they face a new smart device"*. Another suggestion was to let users *"see or hear what the system tracks"* (E4). E3 highlighted that it might be of interest to distinguish devices being on vs recording. Finally, the consensus was that the system should adapt to the user's perception of privacy rather than the other way round. Thus, the system should recognise users' (dis)comfort regarding data tracking and sharing rather than the user hiding from certain devices or taking extreme measures such as putting it in the freezer to have a private moment.

4.2.4 Authentication Mechanisms. Finally, to investigate the need for varying authentication mechanisms and to brainstorm their conceptualisation, we discussed concrete device types, namely smart hoovers, fridges, lights and voice assistants, which are among the most mentioned from study I. Most ($N = 5$) experts considered voice assistants most critical (i.e., highly protect-worthy), followed by lights and the fridge. Two experts emphasised that it depends on the specific device's capabilities rather than general device types.

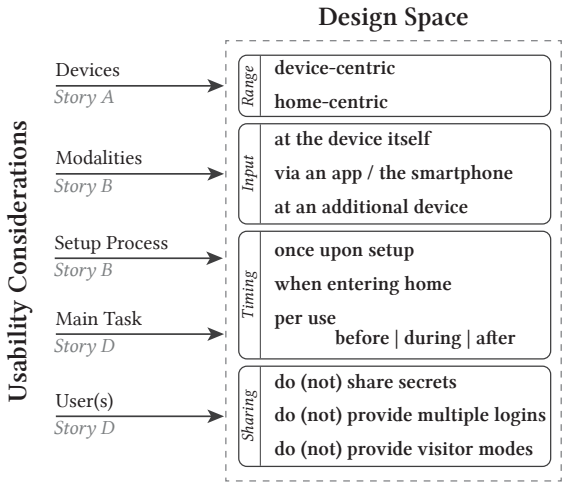

Figure 1: Usability considerations as derived from our story completion interviews (story parts A, B, and D) informing the design of authentication mechanisms for smart homes.

Experts further suggested concrete mechanisms for smart fridges, coffee machines and voice assistants, considering that the authentication secret might (not) be shared with other (adult) members of the household, children, or guests. Examples included biometric (E5) or continuous (E10) authentication, further mechanisms such as rights or access management (e.g., main owner ultimately approves orders via the smart fridge), and multi-factor authentication.

5 DESIGN IMPLICATIONS

Based on the findings from our two studies, i.e. the users' and security experts' perspective, we now discuss and summarise the implications for the design of usable authentication for smart homes. Note that, while participants' stories and experts' suggestions evolved around concrete mechanisms for concrete devices, we base the following implications on overarching themes that emerged from our analysis. We hope these to be useful for researchers and practitioners when it comes to a) implementing novel authentication mechanisms for smart homes and b) evaluating the suitability of existing mechanisms for smart homes.

From a usability perspective, we suggest to consider the (potentially multiple) *device(s)* and respective modalities, the user's current *main task*, as well as the involved *user(s)* (Figure 1 provides an overview). Moreover, users' *preferences* and *technical capabilities* should be considered. Further security factors are the (potentially sensitive) *data* as well as potential attackers and threats (cf. Figure 2 for an overview).

5.1 Range & Input

Participants described various smart devices in their stories. Those come with various built-in interaction modalities. While this opens opportunities for novel authentication techniques (based on, e.g., voice), it is also limiting the feasibility of conventional authentication on novel smart home devices. As an example, P42 described that they would like to have the possibility to enter passwords on their hoover, hence added a keyboard to the imaginary device

within their story. P26 described an additional touch pad, which allows for biometric authentication and adjustment of the hoover's settings. This opens two main directions for the design of authentication mechanisms for smart devices. On one hand, the feasibility of relying on *the device*'s modalities for the user to employ (explicit or implicit) authentication could be further explored. On the other hand, it might be even better to involve *a second (third, fourth, ...) device* for authentication as many participants mentioned the smartphone as additional device or proxy for the authentication. Another approach could be to not employ device-centric, but home-centric authentication as described in prior work [27].

5.2 Timing

Participants' stories indicated that they would authenticate at different times. Some participants indicated that they would authenticate *once upon setting up* the device. Another opportunity was to authenticate *when entering home* – i.e., if the legitimate user arrives, the smart home would be unlocked.

We also found several *tasks* during which participants would use (and hence, potentially need to authenticate with) smart devices. A common, "problematic" scenario was cooking as hands may be occupied or dirty, hence limiting interaction possibilities (e.g., P1). Authentication always is a secondary task. Especially in home scenarios, users want to benefit from the comfort and features of smart devices and focus on their main task rather than on security.

This opens several directions for the design of authentication mechanisms. Authentication could, e.g., be employed *before* an actual task. P53 suggests authentication when entering home (i.e., at the door handle). Other possibilities could include authentication when entering certain rooms (e.g., the kitchen) or explicitly before starting a task (e.g., cooking). Such approaches align with the way in which authentication is currently implemented for smartphones or desktop computers, i.e. users authenticate once and then get full access to all features and data.

For authentication *during* a task, limited interaction and cognitive resources of users need to be considered. Continuous authentication mechanisms (E10) open a chance to authenticate users unobtrusively and effortless, e.g, based on users' physiological and/or behavioural features (e.g., voice, gait) while interacting with their smart devices. Finally, it might also be necessary to authenticate only *after* a task. As an example, authentication could be employed at the end of the actual food ordering process at a smart fridge to prevent children or party guests from ordering.

Furthermore, the *frequency* of using a device and related concerns appeared in participants' stories. Especially if a device is being used frequently, authentication overhead should be reduced by, e.g., employing implicit mechanisms that only occasionally require explicit approval by users.

5.3 Sharing

Smart home devices are likely to be shared between household inhabitants. As discussed within our stories, problems may arise from sharing the device. This, on one hand, opens a need for managing authentication by multiple legitimate users, who may have varying permissions. As an example, users might want to actively share the authentication secret to, e.g., let guests control the music or subtenants to control the heating. However, these types of users should have limited permissions (e.g., only short-term changes of settings). On the other hand, certain user groups could be restricted from access to, e.g., let children not use the smart oven without supervision. Regarding the device's setup, some participants would login to the smart device as a first step. At the same time, they were struggling with the complexity of the overall setup process (P22) and wished for it be as intuitive as possible (P53). Thus, authentication could be made a mandatory part of the initial setup process. However, contrary to smartphones, this process also needs to consider multiple users by default while balancing the complexity of the overall setup.

5.4 Authentication Factors

There is three main authentication factors: knowledge, token, or biometric [23]. Users in our stories mainly wished for biometric mechanisms, as they found it intuitive and easy to use. Among those, fingerprint scans were especially popular, as well-known from current smartphones. However, not every device carries the capability to scan and process fingerprints or other biometric data itself. In such cases, the smartphone could serve as a workaround and handle biometric authentication – this however requires users to switch to an additional device. Another option is to leverage device capabilities for a suitable authentication mechanism (e.g., using a smart devices' input modalities to enter a secret). Apart from biometric authentication, experts suggested continuous (i.e., implicit) mechanisms as another option. These are effortless for users as they can run in the background and do not require users to remember a secret at all. Illegitimate users such as visitors can be locked out once detected.

5.5 Data

We found various (personal) data as being accessed by smart devices. Additionally, we found misconceptions in participants' stories with regards to what data devices have access to and how privacy sensitive this data is. Sensitive data is also collected where unexpected (e.g., floor plans mapped by vacuum cleaner robots). Consequences of illegitimate access and data leakages can be severe (e.g., "control my whole house", P36 and attackers potentially changing access credentials to lockout the main user, E10). For the design of authentication mechanisms, we propose to consider the sensitivity of the involved data. This may have an impact on the acceptable effort for authentication, but also on the choice of authentication with regards to security. As an example, the desired security level for devices capable of placing orders might be higher as for devices that control lights.

5.6 Attacks & Threats

Independent of the type of threat, users want the smart device to recognise a threat and deal with it (e.g., *"It [the smart device] logs all users and recognises them, so it should know when there is a threat [guest, child, unwanted user]."*, P5). We assume that this expectation is grounded in two factors: Firstly, there is more space available to add additional hardware (e.g. sensors). Compared to a smartphone that is limited by its affordance to be handheld, a smart home device may be larger. Secondly, participants are aware

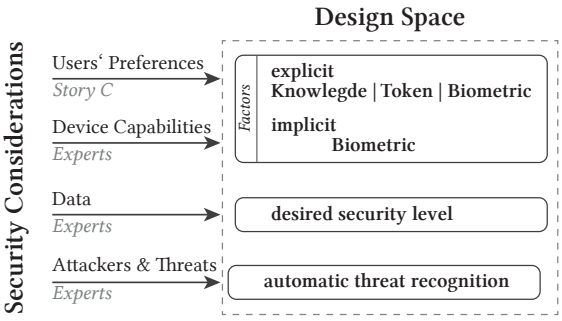

Figure 2: Security considerations as derived from our story completion interviews (part C) and expert focus group informing the design of smart homes authentication mechanisms.

that the device tracks a lot of different kinds of data. Although they did not voice this explicitly, they mentioned various types of data that was captured and expected it to be used to personalise and automate household activities.

An alternative approach could let an additional system track usage patterns to *double check* whether a particular smart device is being externally manipulated or whether the user's behavioural patterns match the ones of legitimate owners, as previous work shows that such patterns can identify users [42].

6 DISCUSSION & FUTURE RESEARCH DIRECTIONS

6.1 Reflections on Methodology

Using the story completion method, we assessed users' choice of authentication mechanisms that they consider *usable*. We argue that this is in line with authentication setup procedures on, e.g. smartphones, where the assessment of security is not in users' hands: users can chose from a number of *secure* mechanisms as suggested by the provider.

After all, our aim was not to create a comprehensive list of design considerations, but rather explore themes that are valuable from a user's and a security expert's perspective. These could be validated and further extended by iteratively developing specific prototypes that were designed based on our considerations, and testing those in-the-wild, i.e. in users' homes. Note that design options still need to be carefully chosen per case and that the same considerations may lead to the design of various mechanisms. Future work could investigate their design, potential implementations, usability and security, including authentication for specific devices as well as for smart homes as whole. Lastly, another focus group with experts from not only academia, but also professionals might lead to further valuable insights.

6.2 Authentication in Smart Homes

Apart from the actual design and implementation, authentication in the home raises further interesting questions. Firstly, when and where within our (smart) homes do we authenticate? It starts when entering home by unlocking the door, as suggested by P53. It could also be at a particular room which is considered sensitive (e.g., the bedroom), or at a particular device or device setup, such as the TV or home movie kit. Secondly, against whom do we actually authenticate? While this is clear for a single platform (e.g., a video streaming platform), it is rather unclear in the complex ecosystem of smart homes. As an example, a smart TV might have access to various video streaming providers, each of which requires users to provide credentials to access paid content. A smart fridge might be able to place orders at various grocery stores. A smart hub does not only have access to devices within the home, but also to the manufacturers' service(s). Future work should investigate how this labyrinth of data and services can be protected, but at the same time made accessible to users without generating an authentication overload.

Lastly, a more extreme approach is to not provide any conventional authentication at all, but rather assume that users with physical access to smart devices have access to basic functionality such as, e.g., turning on lights [46]. This approach however reaches its limits as soon as an illegitimate individual gets physical access to the home, be it, e.g., an attacker or an initially legitimate user (e.g., a room mate who moved out). An interesting question for future work is how a decision about "basic" (accessible without any authentication) and "advanced" functionality can be made, and how this can be implemented. Also, how can users be supported in setting this up and maintaining this? Furthermore, in line with our experts, how should such a system react if an intrusion is detected?

6.3 Devices' Roles in Private Households

Our data suggests that users' perception of privacy and security varies depending on the type of device. Participants presumed devices that do mundane tasks (e.g., an automated hoover) to be less of a threat – with regards to amount of tracked data and possible harm that can be done with it – than an intelligent fridge, which is capable of ordering groceries and knows the food plan. In American households, mundane chores are often times outsourced to a cleaning help [41]. It can be presumed that these type of bystanders have a key to homes and access to varying degrees of private data. Similarly, someone who organises the fridge in a private household is a family member, who also has access to private data. We argue that these preconceptions about which smart device is more or less of a threat is based on who (guests vs. parents vs. kids) users associate with that task and the perception they have of what private data that person knows – rather than the actual data that the smart device tracks. There is an opportunity to benefit from such a misconception by assigning *roles* to smart devices. Future work may explore, whether such a system supports users in understanding how much data is being saved and how it affects their privacy.

6.4 Further Security & Privacy Mechanisms

While we focused our stories around authentication, other mechanisms might further help to preserve users' privacy, increase security and manage responsibilities in shared scenarios in future smart homes. As an example, it oftentimes seems to be unclear who is the main owner of the smart device in shared households and, thus, who is responsible for final (e.g., purchase) decisions and settings. We describe possible mechanisms below.

6.4.1 Manage Access. Users want to be able to access their data, decide what to share and understand how their decisions affect the interaction with their smart device. There is a need for transparency on data handling, as suggested by prior work [7]. Making this more transparent also supports users' need to educate guests and minors who did not agree to be tracked. We question whether it is indeed the device owner's responsibility to get agreement from guests. For public surveillance systems, it is the device owners' responsibility to indicate how and where passers by are being tracked. However, public spaces have a different notion of trust and privacy compared to private households. The latter suggests a more trustworthy atmosphere and thus also more privacy [13, 33], which makes consent for being tracked a necessity in order to avoid being "creeped out" [32]. Moreover, prior work shows that privacy concerns generally exist in smart homes [45, 47, 49] and willingness to share sensitive data is limited [28]. Smart home usage can reveal personal health data (e.g. content of the fridge, time spent in front of the smart TV vs. on a smart training device), which might fit the quantified self movement, but not suit users' desires for privacy. To our knowledge, prior work has not investigated where users see the break even (if it exists) between amount of data being shared vs. their advantage with regards to societal goals and comfort. Moreover, the dynamic nature of roles within households [10, 46] poses a challenge for authorisation and access control in smart homes. For instance, our experts suggested that only the primary owner of a smart fridge could approve food orders. This in turn would allow, e.g., visitors to place orders in the shopping basket, but not execute a payment. Users' stories also questioned responsibility in the context of the couple scenario, and who of them would be allowed to do what with the smart device. Prior work suggested to focus on functionality rather than devices [10]. This raises interesting questions for future work, including the permissions associated with roles in smart homes, and the employment of these when it comes to access to data and functionality.

6.4.2 Increase Awareness. Furthermore, users need to be educated about the reach of the tracking. In the context of smart devices, there is ambiguity about how far the tracking reaches. Non-experts are not able to differentiate between devices, sensors and their ability, but rather draw a relationship between the smart device and the room it is in (e.g., kitchen) or the smart device and the task it upholds (e.g., hoovering). Visitors consider their familiarity to the device owner and environment rather than the device itself when it comes to privacy decisions [19]. We found both, end-users and security experts, wishing for indications of devices being active and/or tracking data, which would ultimately support them in informed privacy decisions.

Experts' proposal to tackle this problem was twofold: Firstly, in alignment with prior work [33] that drew the attention to law makers' responsibility, experts agreed that there is a need to create regulations on how far certain sensors are allowed to track. This would avoid ambiguity regarding sensors and their technical ability, which non-experts are not equipped to know. Secondly, they suggested visualisation systems to inform users about the reach of tracking [26] and/or sending notifications to users (e.g., as soon as tracking becomes active or providing information on-demand). Also, various modalities were mentioned such as smartphones, smart watches, the devices themselves or additional lights as suggested in prior work [34]. However, no sensitive information should be provided by this indication (e.g., a burglar should not recognise that surveillance is active) nor should users be overloaded with information.

7 CONCLUSION

With this work, we explore design considerations for usable authentication mechanisms for future smart homes. Interviews with non-expert end users ($N = 20$) using the story completion method provided insights in choice for devices and motivational factors, potential authentication mechanisms as well as problems with various stakeholders. We complement our findings by a focus group with security experts ($N = 10$). Ultimately, we derived implications for the design of authentication mechanisms and discuss directions for future research, which we hope to be useful for researchers and practitioners. In particular, the available modalities of devices, their access to data and functionality, as well as multiple users and their roles essentially impact the design of smart home authentication that is usable as well as secure.

ACKNOWLEDGMENTS

We would like to thank Vanessa Sarakiotis and Bastian Wagner for their help with conducting the interviews. The presented work was funded by the German Research Foundation (DFG) under project no. 425869382 and by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom].

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (Oct. 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini. 2018. Ethical Design in the Internet of Things. *Science and Engineering Ethics* 24, 3 (01 Jun 2018), 905–925. https://doi.org/10.1007/s11948-016-9754-5

[3] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. *APA handbook of research methods in psychology. Research designs: Quantitative, qualitative, neuropsychological, and biological* 2 (2012), 57–71.

[4] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 185–204. https://www.usenix.org/conference/soups2020/presentation/chalhoub

[5] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3334480.3382850

[6] Victoria Clarke, Nikki Hayfield, Naomi Moller, and Irmgard Tischner. 2017. Once Upon A Time…: Story Completion Methods. *Collecting Qualitative Data: A Practical Guide to Textual, Media and Virtual Techniques* 1 (2017), 45–70.

[7] Malin Eiband, Daniel Buschek, and Heinrich Hussmann. 2020. How to Support Users in Understanding Intelligent Systems? Structuring the Discussion. arXiv:2001.08301 [cs.HC]

[8] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 2, Article 44 (June 2019), 21 pages. https://doi.org/10.1145/3328915

[9] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 268, 13 pages. https://doi.org/10.1145/3290605.3300498

[10] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[11] Martin J Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In *Proceedings of the Halfway to the Future Symposium 2019* (Nottingham, United Kingdom) *(HTTF 2019)*. Association for Computing Machinery, New York, NY, USA, Article 5, 8 pages. https://doi.org/10.1145/3363384.3363389

[12] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling Multi-User Controls in Smart Home Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (Dallas, Texas, USA) *(IoTS&P '17)*. Association for Computing Machinery, New York, NY, USA, 49–54. https://doi.org/10.1145/3139937.3139941

[13] Adam N. Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield. 2010. Privacy, Trust, and Self-Disclosure Online. *Human–Computer Interaction* 25, 1 (2010), 1–24. https://doi.org/10.1080/07370020903586662 arXiv:https://www.tandfonline.com/doi/pdf/10.1080/07370020903586662

[14] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Augmented Reality-Based Mimicry Attacks on Behaviour-Based Smartphone Authentication. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services* (Munich, Germany) *(MobiSys '18)*. Association for Computing Machinery, New York, NY, USA, 41–53. https://doi.org/10.1145/3210240.3210317

[15] Christine Kühnel, Tilo Westermann, Fabian Hemmert, Sven Kratz, Alexander Müller, and Sebastian Möller. 2011. I'm home: Defining and evaluating a gesture set for smart-home control. *International Journal of Human-Computer Studies* 69, 11 (2011), 693 – 704. https://doi.org/10.1016/j.ijhcs.2011.04.005

[16] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. In *The 25th Annual International Conference on Mobile Computing and Networking*. Association for Computing Machinery, New York, NY, USA, Article 33, 17 pages. https://doi.org/10.1145/3300061.3345434

[17] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. Association for Computing Machinery, New York, NY, USA, 117–122. https://doi.org/10.1145/3301293.3302371

[18] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139 – 154. https://doi.org/10.1016/j.techfore.2018.08.015

[19] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[20] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[21] Lukas Mecke, Ken Pfeuffer, Sarah Prange, and Florian Alt. 2018. Open Sesame! User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 153–159. https://doi.org/10.1145/3282894.3282923

[22] M Granger Morgan, Baruch Fischhoff, Ann Bostrom, Cynthia J Atman, et al. 2002. *Risk communication: A mental models approach*. Cambridge University Press, Cambridge, United Kingdom.

[23] L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (Dec 2003), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611

[24] Talha Ongun, Alina Oprea, Cristina Nita-Rotaru, Mihai Christodorescu, and Negin Salajegheh. 2018. The House That Knows You: User Authentication Based on IoT Data. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 2255–2257. https://doi.org/10.1145/3243734.3278523

[25] Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, and Abdellah Ait Ouahman. 2017. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks* 112 (2017), 237 – 262. https://doi.org/10.1016/j.comnet.2016.11.007

[26] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 69, 18 pages. https://doi.org/10.1145/3411764.3445067

[27] Sarah Prange, Emanuel von Zezschwitz, and Florian Alt. 2019. Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (Stockholm, Sweden). IEEE, New York, NY, USA, 154–158. https://doi.org/10.1109/EuroSPW.2019.00024

[28] Aare Puussaar, Adrian K. Clear, and Peter Wright. 2017. Enhancing Personal Informatics Through Social Sensemaking. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 6936–6942. https://doi.org/10.1145/3025453.3025804

[29] B. Qolomany, A. Al-Fuqaha, A. Gupta, D. Benhaddou, S. Alwajidi, J. Qadir, and A. C. Fong. 2019. Leveraging Machine Learning and Big Data for Smart Buildings: A Comprehensive Survey. *IEEE Access* 7 (2019), 90316–90356. https://doi.org/10.1109/ACCESS.2019.2926642

[30] S. W. Shah and S. S. Kanhere. 2019. Recent Trends in User Authentication – A Survey. *IEEE Access* 7 (2019), 112505–112519. https://doi.org/10.1109/ACCESS.2019.2932400

[31] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. 2017. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-Enabled IoT. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (Chennai, India) *(Mobihoc '17)*. Association for Computing Machinery, New York, NY, USA, Article 5, 10 pages. https://doi.org/10.1145/3084041.3084061

[32] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421

[33] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76 (2015), 146 – 164. https://doi.org/10.1016/j.comnet.2014.11.008

[34] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[35] Statista. 2020. Smart Home Report 2020. https://de.statista.com/statistik/studie/id/41155/dokument/smart-home-report/ last accessed April 15, 2021.

[36] Elizabeth Stobert and Robert Biddle. 2013. Authentication in the Home. In *Workshop on Home Usable Privacy and Security (HUPS)*, Vol. 29. HUPS 2013, Newcastle, UK, 209–218. https://cups.cs.cmu.edu/soups/2013/HUPS/HUPS13-ElizabethStobert.pdf

[37] JaYoung Sung, Rebecca E. Grinter, and Henrik I. Christensen. 2009. "Pimp My Roomba": Designing for Personalization. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. Association for Computing Machinery, New York, NY, USA, 193–196. https://doi.org/10.1145/1518701.1518732

[38] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? arXiv:1911.07701 [cs.HC]

[39] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*, Vol. 29. HUPS 2013, Newcastle, UK, 209–218.

[40] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[41] Ashley V. Whillans, Elizabeth W. Dunn, Paul Smeets, Rene Bekkers, and Michael I. Norton. 2017. Buying time promotes happiness. *Proceedings of the National Academy of Sciences* 114, 32 (2017), 8523–8527. https://doi.org/10.1073/pnas.1706541114 arXiv:https://www.pnas.org/content/114/32/8523.full.pdf

[42] Roman V. Yampolskiy and Venu Govindaraju. 2008. Behavioural Biometrics: A Survey and Classification. *Int. J. Biometrics* 1, 1 (June 2008), 81–113. https://doi.org/10.1504/IJBM.2008.018665

[43] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 198, 12 pages. https://doi.org/10.1145/3290605.3300428

[44] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (Nov. 2019), 24 pages. https://doi.org/10.1145/3359161

[45] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the 2017 SOUPS Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 65–80.

[46] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[47] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 200. https://doi.org/10.1145/3274469

[48] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu. 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal* 6, 2 (2019), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733

[49] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197–216.

A USER INTERVIEWS: STORY COMPLETION GUIDE

Tim and Lara are a couple, recently having moved together in a common house. Lately, they saw many advertisements on, e.g., Amazon Alexa, electronic door locks, smart cameras, Internet-connected fridges, app-controlled washing machines, smart lights, Internet-connected audio systems, smart TVs, Internet-connected alarm clocks, sensor-equipped microwaves, hoover robots, and many more. Tim and Lara know, that any device exists with many interaction modalities and features.

Please imagine a future scenario in which any imaginable device exists.

A. Appliances and Reasons After both did some research on smart devices, Tim and Lara are now interested in getting one for their new home. However, they are not quite sure which type of device(s) to choose, as many – e.g., security or entertainment devices – promise benefits for daily life. They decide to no longer delay the purchase. What happens next? Please describe the scenario. Include Tim's and Lara's reasons for their choice, and what they expect from the device. Consider that they will probably use the device regularly.

Note: following parts of the story were based on the *<smart device>* that was chosen.

B. Functionality, Setup & Interaction A few days later, the *<smart device>* arrives and Tim and Lara want to try out all functionality. What happens next? How is the device's setup process and what functionality does *<smart device>* provide? How can both interact with the *<smart device>*?

C. Authentication Mechanisms Tim and Lara are aware that smart devices collect and store personal information. Thus, they want to make sure that illegitimate users to not have access to their account. The *<smart device>* can meet this requirement. How could an authentication mechanism look like, that is more than a one-time login, but does not require user input on each and every device use?

D. Problems & Concerns of Shared Use

D.1. Couple After a few weeks, Tim and Lara realise that shared use of a smart device can lead to problems. Which problems could that be and how could future solutions look like?

D.2. Children Lara's sister is visiting every month, together with her children (3 and 5 years old). As they see the *<smart device>*, they want to play around with it. While Lara is busy talking with her sister, Tim is concerned as he is not sure about consequences of using the *<smart device>* for the children.
Please describe (potentially harmful) consequences in this scenario and include potential countermeasures.

D.3. Worried Guest Tim and Lara have a worried guest. This guest is convinced, that any Internet-connected device is used for surveillance by, e.g., secret service or marketing companies.
How can Tim and Lara convince their guest to feel more safe, i.e., that their home is still a safe place? What requirements would the *<smart device>* need to fulfil (e.g., an option to turn off the microphone)?

B EXPERT FOCUS GROUP: PROTOCOL

1. **Threats in Smart Homes**
   - **a)** Think about 5 threats and rank them in order of priority.
   - **b)** How can this threat be automatically recognised?
2. **Data Tracking, Transparency and Management**
   - **a)** From a scale from 1-7 (1=not at all) how much do you agree with this phrase?
     "It is not tracked when I put the smart device in the freezer." [provided on a paper sheet]
   - **b)** How can we increase awareness of what is tracked when and how (e.g., by means of a visualisation)?
     Think about 3 solutions.
   - **c)** From a scale from 1-7 (1=not at all) how much do you agree with this phrase?
     "When guests enter my smart home, they loose the right to their data." [provided on a paper sheet]
   - **d)** How can we share data that is tracked from guests with them?
3. **Privacy and Societal Goals**
   - **a)** Which of the following smart devices are more *privacy intrusive*? Think about, e.g., which data these devices can access. Rank them on a scale from 1 - 4, 1=least intrusive.
     - smart hoover
     - smart fridge
     - smart light
     - smart voice assistant

     I do not think it is possible to rank them. Why?
   - **b)** Which *factors* would you consider when designing an authentication mechanism for smart devices? Think about 5 factors.
     e.g., one central authentication system vs. individual ones for each smart device? e.g., consider context?
4. **Authentication Mechanisms**
   There are three user groups (owner, adult household members, children, guests) and three smart devices (smart fridge, smart voice assistant, smart coffee machine). Lets think about one authentication method for each smart device that can be shared with each group.

C CODES FOR QUALITATIVE ANALYSIS

A Appliances and Reasons.

- Appliances
  - Household
    - vacuum cleaner robot (7)
    - fridge (5)
    - washing machine (4)
    - light (2)
    - heater (1)
    - coffee machine (1)
    - dish washer (1)
  - Entertainment
    - Alexa (6)
    - TV (1)
  - Control
    - smart hub (3)
  - Security
    - camera (1)
    - door lock (1)
- Factors of Influence
  - comfort
  - chores
  - internet access
  - central control
  - automation
  - showing off
  - easy installation
  - safe energy

B Functionality, Setup & Interaction.

- Features
  - Device Features
    - It is always on
    - photo album
    - self programming what it can do
    - efficient
    - scanner checks content
  - Use Cases
    - mange shopping / orders / delievery
    - automation
    - (vacuum) clean
    - change lights
    - lawnmower
    - play music
    - waaterproof
    - indoor and outdoor use
    - create and change profiles
    - personal settings / individual programming
    - play music
    - <not mentioned>
- Setup
  - Establish connection
    - connect with other devices
    - connect to WIFI
    - connect
    - enter Wifi Password

    - internet connection
    - connect with all accounts
  - Authentication
    - automatic authentication depending on other devices
    - two-factor authentication
    - enter login data
  - start the device / first steps
    - plug in
    - unpack
    - turn on
    - download companion app
    - device training time
    - employ light bulb
  - try out / learn device
    - try it out
    - read manual
    - learning by doing
    - watch a video
    - plug and play
  - others
    - sensors
- Interaction Modalities
  - app / smartphone
  - voice commands
  - touch
  - via voice assistant / Alexa
  - 3rd person/friend
  - remote control
  - high importance/dependence
  - via a display
  - none (completely automated)
  - indirect
  - directly with the coffee machine
  - fingerprint
  - face recognition

C Authentication Mechanisms.

- fingerprint (11)
- face recognition/scan (6)
- voice commands / recognition (6)
- login via smartphone / companion app (3)
- PIN (3)
- two-factor authentication over mobile phone (1)
- camera (1)
- connection to WiFi (1)
- door handle (1)
- password (1)
- location dependent authentication with mobile phone (1)
- locks device from being accessed (fridge) for a few min (1)
- only authenticate once upon installation (1)
- token / proximity based (1)

D Problems & Concerns of Shared Use.

- Shared Devices
  - (varying) preferences
  - interferring commands
  - voice recognition failures within family
  - Responsibility
  - Children
    - children may get hurt
    - device may be damaged
    - other/miscellaneous problems
  - Visitors
    - dislike
    - disagree
- other/miscellaneous problems
- Data
  - data leakage to co-living partners
  - knowing when the device is on/off or saving data
- Technology / Device related