Special Issue Research Article

Verena Zimmermann*, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner

Assessing Users' Privacy and Security Concerns of Smart Home Technologies

https://doi.org/10.1515/icom-2019-0015

Abstract: Smart Home technologies have the potential to increase the quality of life, home security and facilitate elderly care. Therefore, they require access to a plethora of data about the users' homes and private lives. Resulting security and privacy concerns form a relevant barrier to adopting this promising technology. Aiming to support end users' informed decision-making through addressing the concerns we first conducted semi-structured interviews with 42 potential and little-experienced Smart Home users. Their diverse concerns were clustered into four themes that center around attacks on Smart Home data and devices, the perceived loss of control, the trade-off between functionality and security, and user-centric concerns as compared to concerns on a societal level. Second, we discuss measures to address the four themes from an interdisciplinary perspective. The paper concludes with recommendations for addressing user concerns and for supporting developers in designing user-centered Smart Home technologies.

Keywords: Smart Home, Privacy and Security, User Perceptions, Internet of Things

1 Introduction

Smart Home (SH) technologies are promising to facilitate our everyday life and household activities, to increase home security, and to support the autonomous living of elderly people. In a SH everyday objects such as housing technology (e. g., heating, lighting), household devices (e. g., washing machines, fridges) and consumer electronics (e. g., TVs, computers) are connected intelligently by information, communication and sensor technologies. The interconnected technologies can be monitored, accessed and controlled to serve the needs of the SH user [1, 2, 3, 4].

Although SH technologies are increasingly available to end users, the current level of adoption still falls behind [5, 6, 7]. Reasons include high cost, inflexibility, poor usability [7, 8], and a lack of general user involvement [9, 10]. Privacy and security concerns constitute another relevant barrier of adoption [2, 5, 11]. To use their full potential, SH technologies require access to a plethora of information about the user's home and private life. However, this information is vulnerable to misuse by malicious providers or third parties.

Privacy and security concerns of people with no or little SH experience emerged in focus groups on user requirements for SH technologies [8], and also play a major role for elderly citizens' perceptions of SH and health care technologies [12, 13, 14] and their willingness to adopt these [15, 16].

Yet, little research has been conducted on analyzing the security and privacy concerns of people who are interested in owning SH technologies, but have not yet adopted them due to their concerns in more depth [2]. This group, however, is of great relevance as their concerns and perceptions potentially influence the decision to adopt SH technologies and the way these technologies are used.

Contribution: The aim of this research thus is to support informed decision-making by prospective users. To do so, we first needed to understand the users' perceptions of SH technologies and thus provide an in-depth investigation of end-users' security and privacy concerns as our main contribution. From the findings, and by taking into account related work from different disciplines, we derived recommendations for smart home developers and researchers to support better-informed decision-making through addressing the users' concerns and increasing transparency of SH technologies (see research procedure in Figure 1). Our key findings are as follows:

– Conducting semi-structured interviews with 42 potential and little-experienced SH users from Germany, we

***Corresponding author: Verena Zimmermann,** Work and Engineering Psychology, Technische Universität Darmstadt, Darmstadt, Germany, e-mail: verena.zimmermann@tu-darmstadt.de
Paul Gerber, Work and Engineering Psychology, Technische Universität Darmstadt, Darmstadt, Germany, e-mail: paul.gerber@tu-darmstadt.de
Karola Marky, Telecooperation Lab, Technische Universität Darmstadt, Darmstadt, Germany; and Keio University, Yokohama, Japan, e-mail: marky@tk.tu-darmstadt.de
Leon Böck, Telecooperation Lab, Technische Universität Darmstadt, Darmstadt, Germany, e-mail: boeck@tk.tu-darmstadt.de
Florian Kirchbuchner, Fraunhofer Institute for Computer Graphics, Darmstadt, Germany, e-mail: florian.kirchbuchner@igd.fraunhofer.de

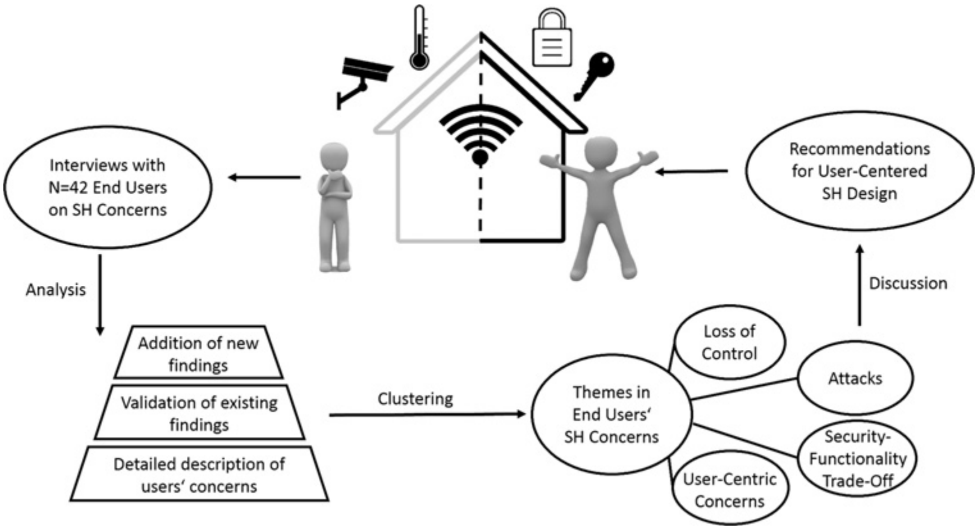

Figure 1: Research Procedure and Contribution.

found several concerns that could be clustered into four themes that center around (1) attacks on SH data and devices, (2) the perceived loss of control, (3) the trade-off between functionality and security, and (4) user-centric concerns as compared to concerns on a societal level.

- We extend previous research with a nuanced categorization of concerns, e. g., in terms of attacks to exert psychological pressure on SH inhabitants.
- An additional comparison of cloud-based and local data processing SH concepts adds an important piece to understanding the users' tension between needs for security and functionality.
- Technical security seems to be a necessary but not sufficient condition for addressing user concerns. Communicating privacy and security features to the users is equally important. We recommend to not only design concrete and actionable threat notifications, but also to reassure users of normal operations. Enhancing the transparency of SH processes and implementing fallback mechanisms for manual handling of SH devices might contribute to a sense of control deemed important by end users.

2 Related Work

With the progressive development of SH technologies and the diversification of use cases, interconnected technologies became increasingly interwoven with the users' private lives. The resulting implications thereof have raised interest among researchers and practitioners during the last years. In particular, studies concerned *user perceptions* and *barriers that hinder adoption* of SH technologies in general, as well as *privacy and security concerns*.

2.1 User Perceptions

Frequently mentioned perceived or anticipated benefits of SHs are the facilitation of everyday life, an increase in comfort [17, 18], cost savings and environmental protection [18, 19, 20, 21, 22, 23, 24, 25] as well as enhanced security and control over the status of one's home [18]. In general, users seem to be more interested in what the system does and less in how this is achieved (e. g., which algorithms are used) [26]. This is in line with studies of end users' mental models in which users expressed a rather simplified understanding of SH processes and technical details, but focused on the functionalities SH technologies provide [27]. They wish access to up-to-date state information [28] that should be more than pure data presentation because users expect visual feedback from the system [19, 29, 30]. Here, the integration of the data from different sources into an overall interface and the use of metaphors seem to support understanding of the system and its functioning [19, 29]. Further, users consider a feeling of personal control over the system to be essential [26, 31].

2.2 Barriers for Adopting SH Technologies

Common SH technologies require end users to have technical skills to gain access to all information and control functions [32]. Even before purchasing, the users have to overcome significant obstacles and are often overwhelmed by the sheer number of available devices making it difficult to translate their wishes into required hardware components [33]. Illustrations of the benefits are often lacking [33], so that the subjective added value of SHs remains unclear [7]. Lacking interoperability between devices from different manufacturers leads to uncertainty, and requires compromises between flexibility and ease of installation [7, 33]. Users are concerned regarding maintaining security during operation, especially due to the frequent lack of easy-to-use security tools [7]. Moreover, the necessity of structural adaptations to the building for the installation of automation technology, the uncertainty regarding the future security of the devices, especially in the context of rapid technological development, and the high acquisition costs proved to be further obstacles [7, 33]. Other obstacles could be a lack of trust in the manufacturer or provider of the system [34] and concerns for a lack of control over autonomously operating systems in one's household [26, 34, 35]. Finally, privacy and security concerns described in the next section form a relevant barrier for adoption.

2.3 Privacy and Security Concerns

A study on elderly people's perceptions of SHs [12] revealed that privacy concerns play an even larger role for the participants than ease of use. Participants in a study by Rodden *et al.* [34] expressed little privacy concerns about the nature of the data itself, but strong concerns about how companies handle the data. Participants were primarily concerned about increased advertising and selling their data for profit. In this context, an investigation in users' knowledge about and mental models of the Internet revealed that users with more articulated technical models perceived more privacy threats [36].

Brush *et al.* [7] analyzed 14 SHs in a field study and found concerns in terms of security-critical devices. Remote access was perceived as a double-edged sword, allowing additional control while increasing security concerns. Study participants also expressed concerns about the individual privacy of different household members when using SH technologies [29, 37]. For example, children might feel uncomfortable about their parents being able to check their whereabouts.

Gerber *et al.* [1] asked the participants of an online survey for perceived privacy consequences of using SH technologies. About one-third of the responses addressed general privacy concerns, the remaining responses, however, addressed concerns not related to privacy.

Emami-Naeini *et al.* [11] presented users with randomized IoT scenarios with different implications on privacy. The results indicated that users were more comfortable with data being collected in public settings and less comfortable with biometrics or data sharing with third parties. They wished to be notified about data collection in scenarios perceived as uncomfortable. Similarly, Apthorpe *et al.* [38] conducted a survey based on the Contextual Integrity privacy framework to analyze privacy norms in SHs.

Our study extends the scope of this research from privacy to security. Further, instead of providing scenarios, we qualitatively explore which threats users are aware of and concerned about.

Zeng *et al.* [2] found that while technical security concerns related to SH technologies have received much attention, relatively little research has been conducted on end user security and privacy concerns. Some studies have thus focused on concerns and experiences of SH owners, i. e. people that have already adopted SH technologies. For example, Zeng *et al.* [2] conducted interviews with 15 SH administrators and residents to explore their concerns in the interaction with SHs. The concerns most often mentioned related to physical security and general home privacy. Still, many participants were generally not concerned about potential threats. A recent interview study by Zheng *et al.* [39] focused on the experiences of eleven SH owners and revealed that convenience was a major factor for adopting SH technologies and for disregarding personal privacy concerns. Emami-Naeini *et al.* [40] conducted interviews with 24 participants who had purchased IoT devices to explore how security and privacy aspects influenced the purchase decision in general. Most participants reported not having considered the topic prior to the purchase, but having been concerned about privacy and security afterwards. For those who sought information prior to purchase, it was difficult or impossible to find.

While these studies provide valuable insights in terms of SH owners, Zeng *et al.* [2] suggest that future work should study a population of non-users as people not having adopted SH technologies yet may have other or more pronounced concerns that hinder adoption in the first place.

We fill this gap with our study that considers, but contrasts with other research in the following ways: We analyze the specific concerns of a large interview sample of end users related to the security and privacy of SH technologies. Thereby, the focus is on users with no or little SH experience to include concerns that potentially hinder adoption in the first place. Further, we aim to cover diverse concerns by including different SH concepts in the interview study that constitute different levels of security and privacy. They are presented in the next section.

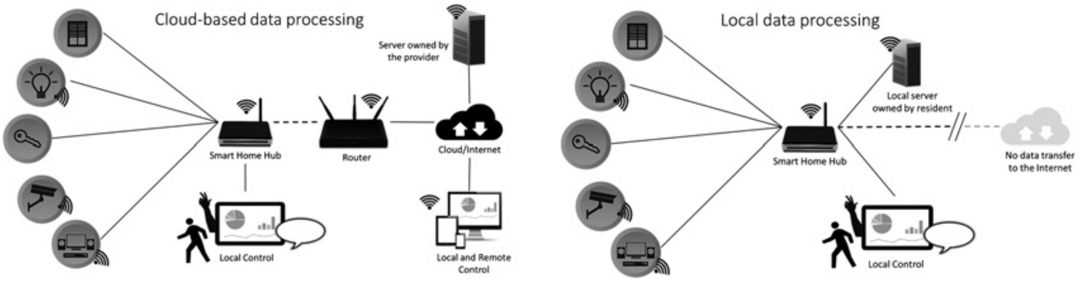

Figure 2: Sketches of cloud-based (left) and local (right) processing of SH data.

3 Smart Home Concepts

A possibility to differentiate the wide range of existing SH concepts in terms of privacy and security is the way SH data is handled and stored:

Regardless of the specific SH architecture, every SH consists of sensors and actors that are deployed within the SH environment. The data collected or processed by these components is manifold, i. e., it encompasses room temperatures, instructions to close a window, information about the contents of a fridge or even videos from a surveillance camera. A common approach to coordinate this privacy and security sensitive data is the use of a so-called Smart Home Hub that serves as a control center and provides an interface between the SH sensors, devices, and users.

The scale of possible solutions how the hub handles the SH data ranges from a completely cloud-based concept over several hybrid approaches to a completely local concept.

To gain insight into the users' privacy and security concerns we not only asked users in terms of their understanding of SHs but also provided the participants of our interview study with sketches of different SH concepts (see Figure 2). We chose to include the two concepts located at the two endpoints of the range of possible SH solutions for two reasons. First, we aimed for an easy understanding of lay users and thus a clear differentiation. Second, by choosing two concepts far apart from one another we aimed to increase the variance in the participants' answers and to avoid a central tendency bias [41].

3.1 Cloud-Based Data Processing

The sketch on the left side depicted in Figure 2 represents a SH concept with cloud-based data processing and storage. This and similar concepts are currently used by large commercial SH providers such as Amazon Alexa,[1] Google Home,[2] Stringify[3] or Yonomi.[4]

For the cloud-based data processing concept, data is sent from the SH to a centralized server or cloud service that processes and stores it. This provides three major benefits:

1. The SH can be accessed from anywhere in the world, given an Internet-enabled device, e. g., a smartphone. This enables functionalities such as turning up the heat before arriving at home or checking security cameras remotely.
2. Online platforms can connect SHs from multiple vendors, enabling additional functionality.
3. Service providers can use their superior computational power to provide services based on artificial intelligence, e. g., voice assistants.

While the Internet-connection of the SH enables the benefits mentioned above and automatic updates, it also exposes the SH to additional privacy and security related risks, e. g., privacy-sensitive information could be leaked by a service provider. Further, the Internet-connectivity allows third parties to attack the SH from the Internet and to exploit detected vulnerabilities on a wide scale.

3.2 Local Data Processing

Similar to the first concept SH data in the local data processing concept is exchanged between the SH technologies and a Smart Home Hub (Figure 2). In contrast to the first sketch, however, the data is not sent from the Smart Home Hub to an external server or cloud but only to a personal

[1] https://developer.amazon.com/alexa/smart-home (accessed 02/26/2019).

[2] https://store.google.com/de/category/connected_home (accessed 02/26/2019).

[3] https://www.stringify.com/ (accessed 02/26/2019).

[4] https://www.yonomi.co (accessed 02/26/2019).

server within the own home. There it is processed and/or stored. However, this comes at the cost of decreased functionality and potentially an increased cost of setting up the SH. As this server is not connected to the Internet, users cannot view or change their SH status and functions remotely. Also, some artificial intelligence based features might not be available. These require large amounts of data and processing power that may not always be available for local SHs. However, as all data is stored and processed within the SH the risk of a malicious service provider misusing the users' data, or attackers stealing privacy-sensitive data from the cloud-servers is mitigated. Furthermore, the lack of an Internet connection also reduces the threat of remote attacks against the SH as these would require the physical proximity of an attacker. However, the lack of an Internet connection also prevents automatic updates. Therefore, fixing known vulnerabilities, or updating functionalities in SH requires more effort for the local approach.

4 Interview Study

To confirm and extend the user perceptions and concerns in terms of the security and privacy of SHs we conducted interviews with 42 participants in Germany. We opted for semi-structured interviews because they allowed for a certain degree of standardization while offering the flexibility to react to the participants' responses.

4.1 Method and Procedure

Before the interview, the participants received an informed consent sheet about the study's aims, procedure, and ethical considerations. In line with the guidelines provided by the university's ethics committee, participation was voluntary and could be aborted any time without fearing negative consequences. The data was handled anonymously and the recordings of the interview, that participants consented to, were deleted after transcribing the data. We kept collecting data until the participants' responses started repeating and no new concerns emerged, thus saturation was reached. For the interview questions and material used in our study, the reader is referred to the paper's Appendix A. The structure of the interview was as follows:

In the first part of the interview, we aimed to explore the users' general perceptions and mental models of SH. Therefore, the participants were asked to describe their concept of a SH, their perceived benefits, and their general as well as security and privacy concerns.

In the second part, we introduced a general definition of SHs to ensure a common understanding and explained the two concepts: the cloud-based and the local concept (see Figure 2). Both sketches were shown at the same time to avoid sequential effects. After answering potential questions, the participants were interviewed about their general perceptions of the two concepts. The final part compared the two concepts in terms of general concerns as well as specific privacy and security concerns.

After the interview the participants were asked to provide demographics and to rate the two SH concepts in terms of privacy, security, and intention to use on a 7-point Likert scale ranging from "1 – I do not agree at all" to "7 – I absolutely agree".

Insights into the users' definitions of the SH concept, its expected functionality and components derived from the first part of the interview have been explored and published separately (see [27]) while this research focuses on the users' specific privacy and security concerns in terms of SHs.

4.2 Participants

Our sample consisted of 42 participants from different locations in Germany, of whom 18 identified as female and 24 as male. Their age ranged from 20 to 57 years ($M = 33.69$, $SD = 13.41$). The participants rated their IT-security expertise with $M = 3.10$ ($SD = 2.09$) on a seven-point scale. Furthermore, six had an IT-background and nine had a technical or engineering background. The remaining participants were students of various disciplines ($N = 12$), clerks ($N = 4$), teachers ($N = 2$) and others ($N = 10$). A total of nine participants had completed an apprenticeship, 23 participants held a graduate degree. Participants were recruited via mailing-lists and snowball sampling and each participant was compensated with an Amazon voucher with a value of 5 Euros. SH experience varied among the participants: 21 had not previously used SH technologies, 18 had little SH experience (i. e., using a minimum of three automated rule-based technologies, such as automated heating, time-controlled shutters or motion sensors). Only three used SH systems with a central Smart Home Hub such as Amazon Echo.

5 Results

The following section describes the results with a focus on the findings in terms of specific privacy and security concerns. It further compares the perceptions of the two SH concepts.

Table 1: Overview over the main concerns described in the interviews (*N* denotes the number of participants).

Concern		Examples	*N*
Attack-unrelated concerns	Loss of control	being helpless, no manual functionality of devices, dependency	27
	Technical problems	outages, problems with internet connection or devices	22
	Safety-related concerns	causing a flooding, starting a fire, being trapped inside the house	6
Attack-related concerns: SH devices	Unwanted control of end devices	manipulation of cameras and smart locks, change of settings	34
	…to induce technical problems	fooling of sensors, causing a short circuit	11
	…to drive users mad	psychological pressure, making fun, “challenge” for hackers	10
	Burglary/Theft	intrusion of one’s home, theft of valuables	31
Attack-related concerns: SH data	Unwanted collection of SH data	espionage, unwanted data collection without a specific purpose	16
	…to plan burglaries	spy out times of absence, identify valuables	21
	…to analyze one’s “life”	analysis of one’s preferences, consumer behavior, personal habits	19
	…to cause financial harm	money transfers from one’s bank accounts, placing orders in one’s name	17
	…to misuse data	blackmailing, unwanted deletion of data	16
	…to create targeted advertisement	buying suggestions, sending salesmen and catalogues	15
	…to identify one’s position	profiles of movement, identification of current position	9

5.1 Interview Results

According to the exploratory nature of the study the interviews were transcribed and analyzed based on an open coding approach after Mayring [42]. The categorization was conducted by two of the paper’s authors in an iterative process: After independently categorizing a small percentage of transcripts they agreed on a joint codebook that was again refined in several meetings and after categorizing about 50 % of the transcripts. As the approach focused on refining and improving the categorization it combined phases of independent coding, and phases of joint comparison and discussion of the codings to solve ambiguities and achieve consensual validation [43]. Overall, three categories and 14 sub categories were formed concerning the participants’ concerns (see Table 1), six categories and 21 sub categories were developed to categorize the perceived attack surfaces (see section 5.1.3), and three categories and 14 sub categories were formed comparing the perceptions of local and cloud-based data processing (see section 5.1.4). The complete codebook can be found in the Supplementary Material. Participants’ statements could be assigned to several categories if they included different aspects. Several notions of one participant belonging to the same category were only counted once. If participants described a scenario they explicitly stated not to be concerned about, it was not coded as a threat or concern, for instance:

> *“I don’t belong to the people who are concerned about that, via the smoke detector that one has in his room, that you are eavesdropped.”* (P3).

Overall, the participants named a variety of concerns in terms of SHs that can be divided into three broad categories: (1) concerns unrelated to attacks and concerns related to attacks that can further be divided into (2) data-related and (3) device-related concerns. Similar to the results of Emami-Naeini *et al.* [40] participants did seldom differentiate between security and privacy, or described attack scenarios falling into both categories, so that the concerns are reported together. Table 1 provides an overview of the concerns most commonly mentioned by the participants. We also analyzed the attack surfaces mentioned by the participants and their evaluation of the local versus cloud-based data processing concepts.

5.1.1 Concerns Unrelated to Attacks

About half of the participants feared technical problems of SH technologies ($N = 22$). Another main concerns was perceived loss of control ($N = 27$) that included two aspects: First, 15 participants anticipated to be unable to use devices manually in case of a technical problem. For example, they feared not to be able to unlock a door secured by a smart lock or to not be able to use a smart washing machine in case of a technical failure, for example:

> *"What I can imagine, what is bloody stupid, if the control fails you can't perhaps open or close some doors [...]"* (P9).

Another participant said:

> *"The whole thing is controlled via the Internet. That means I can't turn on the light anymore, I can't influence the heater, I can't [...] draw water anymore because the pump can't be controlled, and that's all because the Internet has failed"* (P26).

Second, 20 participants expressed concerns that the growing dependency on and trust in SH technologies led to a loss of control and rendered them helpless in case of a technical failure. For example, one participant stated:

> *"My biggest concern would be that I'm completely helpless in case of an outage. Because nothing works anymore"* (P3).

Others feared not being able to act on their own due to not having learned or practiced it, for instance:

> *"I ask myself, what happens if the electricity fails for a whole week, how will the user use all his things if he has never learned it. If the technology has done that for him. That's like a child that has never learned to ride a bike and sits on a bike with 18 years of age for the first time"* (P6).

Other examples illustrate the concern for a loss of control to the technology:

> *"Well, I have concerns, in terms of, that we let ourselves being controlled. That we are being mechanized [...] Accordingly, I see that... that this is like a modern iron chain with which we are becoming slaves"* (P7) and *"Of course it scares me that maybe sometime my house decides what is good for me"* (P42).

5.1.2 Concerns Related to Attacks

In some cases ($N = 11$) technical problems were also related to security concerns, e. g. participants stated that technical problems could be actively created by attackers (e. g. provoking a certain reaction of the SH devices by displaying deceptive video images) or lead to dangerous situations (e. g., a fire due to a short circuit). This is expressed in the following quote:

> *"If, for example, someone controls my stove and likes to cause a disturbance, and just switches on all stoves in the street when they are not switched on normally, and while probably all inhabitants are away for work, then it is possible that something has been left on the hotplate and starts to burn and so on"* (P37).

One of the most common concerns, however, was that of burglars using SH data and devices to plan ($N = 22$) and conduct a burglary ($N = 32$), e. g., to analyze

> *"When someone is at home and when not, which valuables are placed where"* (P18) or to *"turn off my security technology from the outside and my house is being robbed"* (P42).

Another common concern is that of attackers accessing and remotely controlling one's SH devices ($N = 34$). For example, participants feared that

> *"Someone can just remotely open up my house"* (P24) or that *"I [as a third party] can hack into the WiFi, I can control everything, I can unlock the door, I can configure the TV, I could also, for example, download illegal content from the Internet"* (P13).

Some participants believed that attackers might manipulate SH devices just for fun or to drive the inhabitants mad ($N = 10$), e. g.,

> *"Someone just wants to make me angry and turns the heating to 40 °C in the summer"* (P36).

Further concerns centered around a third party collecting SH data for various negative reasons, such as analyzing one's life ($N = 19$), manipulating with a targeted advertisement ($N = 15$) or causing financial harm ($N = 17$). For example:

> *"If you are doing everything via the same network, banking transactions via online banking and similar things, that perhaps some bank data could be stolen"* (P29).

5.1.3 Attack Surfaces

In terms of possible attack surfaces people recognized that attackers could access SH data while being stored on an external server or cloud ($N = 32$), during transmission ($N = 34$) via the Internet, radio signals, Bluetooth or cable, or through stealing or accessing the control device ($N = 18$). They further consider local networks or devices, such as a personal WiFi network, a SH Hub, router or local server ($N = 33$) as vulnerable. However, technical information on *how* attacks take place were rare. Most participants shared an abstract understanding of an attacker somehow "*logging in*", "*hooking into*" or "*intruding*". Some participants mentioned software vulnerabilities ($N = 10$), authentication ($N = 10$) and the interconnectedness of devices as a weak spot ($N = 9$):

> *"When one thing doesn't work anymore, like a chain of lights in earlier times, that nothing works anymore"* (P10).

Only a few participants provided more specific attack scenarios, e. g., conducting Distributed Denial of Service (DDoS) attacks ($N = 4$), Man-in-the-middle attacks

Table 2: Test statistics of the user perceptions of cloud-based and local data processing. (Z = test value, p = significance level, r = effect size).

Item	Cloud-based concept			Local concept			Differences		
	M	SD	$\tilde{x}$	M	SD	$\tilde{x}$	Z	p	r
My privacy is protected in SH based on ...	2.83	1.50	2	5.12	1.45	6	−5.067	< .001	.78
If I had the possibility I'd like to use SH based on ...	3.76	2.12	4	4.76	2.10	5	−2.346	.019	.36
SH based on ... are secure, i. e. protected against attacks.	2.60	1.53	2	4.79	1.62	5	−4.931	< .001	.76

($N = 2$), exploiting the negligence of security standards ($N = 6$) or providing malware-infected hardware or software ($N = 3$). One participant stated:

> *"Who looks into the hardware? It could, of course, be that something is in some dubious hardware, that you perhaps bought second hand somewhere or else, that well influences your privacy"* (P20).

5.1.4 Comparison Local and Cloud-Based Data Processing

Nearly all of the participants ($N = 40$) provided scenarios in which an attacker might gain access to the data or devices in a cloud-based SH concept. Further, 37 participants perceived their security and privacy to be better protected in a local data processing concept. Still, most of these participants ($N = 29$) also thought attacks on a local data processing smart home concept possible and thus perceived neither concept as entirely secure. Only three participants believed a cloud-based SH concept to be more secure than a local one due to the better protection of a server hosted by a large organization.

More participants mentioned that one had to be physically close to attack a SH when referring to the local data-processing concept ($N = 10$) compared to the cloud-based one ($N = 2$), e. g., P9 thought attacks only possible when

> *"Someone is near the house, just within the detection range of the Smart Home Hub".*

Further, more people viewed local networks (16 compared to 7) and the local server (8 compared to 1) as vulnerable in a local SH concept, whereas the external server (32 compared to 2), the "Internet" (18 compared to 4) and the router (14 compared to 3) were most often viewed as the weak spots of the cloud-based SH concept.

In terms of functionality, most participants expected a SH to be controllable and accessible remotely as was expressed in their definitions of a SH and also in the functions they expected ($N = 26$). One participant expected that

> *"I can, when I'm on holiday, with the smartphone or another computer, operate the control so that I can view the cameras whether everything is okay."* (P6) and another that
> *"the system, with the help of the smart phone's position data, calculates when one is home and turns on the heating"* (P8).

Further, six participants specifically rated the local data processing to be of no use due to the missing possibility to access and control the SH remotely. One participant summarized the trade-off as

> *"From a security perspective the local data processing has an advantage but also the functional disadvantage that I simply can't control remotely"* (P30).

5.1.5 Questionnaire Results

A statistical and optical analysis of the participants' ratings revealed deviations from a normal distribution. Non-parametric Wilcoxon-tests were thus used to test differences between the two concepts on a significance level of $p \leq .05$ (see Table 2). The local data processing concept was perceived to significantly better protect the user's privacy and security. Further, the participants' intention to use local data processing was significantly higher than the intention to use cloud-based data-processing. Effect sizes between $r = .3$ and $r = .5$ can be interpreted as medium effects, effect sizes above $r = .5$ can be interpreted as large effects [44].

5.2 Results Summary

Nearly all participants described specific privacy and security concerns in terms of SHs. Whereas related work often summarized the participants' concerns as privacy or (physical) security concerns on an abstract level, we derived a more nuanced categorization of concerns (see Table 1). These could be further clustered into the following four themes:

(1) Concerns Unrelated to Attacks: Threats unrelated to attacks that mainly comprise concerns connected to a perceived dependency from and loss of control to the technology.

(2) Concerns Related to Attacks: Concerns about the SH data (e. g., advertisements) or devices (e. g., manipulation of sensors), and concerns about attacks on the SH itself (e. g., burglaries). The responses of the participants thereby focused on the consequences (i. e. the *what*) instead of the process (i. e. the *how*).

(3) Security-Functionality Trade-Off: Comparing cloud-based and local data processing concepts the participants perceived the local concept to be more secure, but the cloud-based concept to be beneficial in terms of remote control. This was often expressed in a perceived trade-off between security/privacy and functionality.

(4) User-centric vs. Societal Perspective: The vast majority of participants only described scenarios that would affect themselves from a user-centric perspective, i. e. scenarios and consequences that would affect their security, personal data or valuables. Concerns for other inhabitants, bystanders, guests or society at large were merely mentioned at all.

6 Discussion and Recommendations

In the following, we describe the four themes of user concerns stated in Section 5.2 in greater detail and discuss how to address them from a technical and psychological perspective. To do so, we turn to grounded findings from related research and derive recommendations for researchers and developers of SH technologies. Recommendations that potentially help with more than one theme of concern will be repeated in the appropriate section under the same name and number.

6.1 Theme 1: Concerns Unrelated to Attacks

As described in section 5.1.1 many participants mentioned concerns unrelated to attacks. Among those, $N = 27$ from the 42 participants expressed concerns related to a perceived loss of control and dependency from technology when using SH technologies. One particular concern was that the malfunction of one component renders the functionality of all other components useless or affects the regular functioning of the SH (e. g., an electrical short circuit in the smart lock leads to the inability to operate the door). Participants also feared a dependency on SHs due to not being able to handle devices manually. Concerns regarding a loss of control to SH technologies have also be found by other researchers, e. g. [45, 46]. Providing SH users with control has thus been a recommendation in several papers [26, 47, 48]. Yet, the issue seems to be more complicated in light of the quite nuanced concerns expressed by the participants in this study.

6.1.1 Technical and Psychological Measures

From a psychological perspective the sense of being in control plays an important role for humans [49] and is therefore crucial to be maintained in SHs.

Many of the participants' concerns were related to potential malfunctions of SH technologies, therefore technical fallback mechanisms to enable the operation of a device in the event of a malfunction should be implemented **(R1)**. Also in a co-design study, some users' designs included the option to disconnect devices from the Internet and to work in an offline manner [50]. Still, it is essential to communicate these features to the user. Thereby, it should be considered that users quickly switch back to known behaviors and solutions if unexpected system reactions (e. g., a crash) occur [17]. Further, control was perceived highest in known forms of interaction and lowest in less familiar ones [51]. Therefore, SH developers should rely on known interaction forms as fallback mechanisms **(R2)**. This can involve a wide variety of approaches, from mechanical actuators, such as levers or locks, to allow opening of a window or operating the heating despite a malfunction, to browser interfaces for enabling reconfiguration of the SH via a PC even if the smartphone has been stolen. This technological redundancy, i. e. the mix of new and old technology, is a frequently observed property of highly reliable systems [52]. Nevertheless, for certain devices implementing a fallback mechanism can be challenging or even impossible, especially if the smart component is essential for the device's functionality (e. g., smart electronic assistants). Not only, but also in these cases, psychological aspects come into play. A second possibility might thus comprise measures to increase the perceived sense of control, i. e., understanding, certainty, and predictability.

The connection of different components, the data flow between them and other background actions are typically not visible for the SH users [53, 54]. Measures to increase the transparency of SH states, settings, and actions in a usable way might thus be promising **(R3)**. Considering user needs, the focus should thereby be on *what* the system is doing compared to *how* this is achieved [26]. For instance, a calendar metaphor used in studies for visualizing interactions with multiple users and to support elderly people in daily activities can increase understanding [29, 55]. By using a well-known metaphor for time sequences for the recognition of usage patterns (e. g. household routines) the user can identify new automation possibilities on this basis and configure the SH accordingly. The metaphor integrates the data of different devices into a unified user interface and enables users to directly recognize the status of all devices and household members, and to adjust their planning or the SH configuration accordingly. Further, Castelli *et al.* [54] found that visualization can be leveraged to facilitate monitoring, and thereby might contribute to a sense of certainty.

Wharton *et al.* [56] propose questions such as "Will the user know that the action constitutes progress in terms of the users' task?" for testing system usability. This would, for example, be given if the label of a button relates well with the action it triggers. Asking these or similar usability-related questions while designing and evaluating SH interfaces might well facilitate for the user to exercise control by contributing to the understanding, certainty and predictability **(R4)**. In [57] the disappearance of computers was already envisioned. However, not in the sense of extinction, but rather in the sense that users no longer perceive the device themselves, but only use it to achieve their goals. Weiser describes how the more a person learns or interacts with something, the more commonplace devices such as smartphones are, the less the action itself is perceived, i. e. the *how*, but the user can concentrate entirely on the goal, i. e. the *what*. It is not relevant for the user how, on a technological level, the SH fulfils its purpose, but it is important to know *what* decisions are made, so that the user retains control. Finally, SH technologies should not only *allow* users to exercise control, but also *enable* user control in all phases of SH use **(R5)**. It should thereby be considered that users' needs in terms of privacy and system accountability change over time from the need for in-depth awareness information towards management by exception [58]. At the beginning, the focus is on getting to know the new system in order to build trust in its reliability. Users check whether the SH functions as planned, and whether their configuration has been carried out correctly. The SH should therefore provide a clear overview of the current status as well as a searchable history of past events so that the user can review decisions made by the SH and make corrections if necessary [59]. When the user trusts that the SH will usually function as intended, the desired type of information changes. Users then aim to be informed when something does not work, requires their direct attention or needs to be maintained (e. g. battery replacement). To also address the concerns of users not yet using or starting to use SH technologies they should be allowed to see and test SH interfaces designed for user control before purchase. SH configurators, as suggested by [60], offer one possibility for this. They can provide an individual selection of application scenarios and inform about required components, data collection and handling, as well as suggestions for providers.

6.1.2 Recommendations

(R1) Fallback: Implement fallback mechanisms for technical malfunctions wherever possible and communicate these to the user.

(R2) Error Management: Design for error management, i. e. providing instructions for the next actions the user can take to achieve his goal. Also, rely on known forms of interaction wherever possible.

(R3) Transparency: Not only notify users of threats but also convey normal operation to reassure the user. Make system states transparent by using visualizations, tangible interaction or suitable metaphors.

(R4) Usability: Ensure usability and understandability of interfaces with established usability guidelines to enable users to exercise control.

(R5) Control: Allow for the user to exercise control in all phases of SH use (before purchase, during configuration and normal operation, and in case of malfunction or threats).

6.2 Theme 2: Concerns Related to Attacks

As depicted in Table 1 the participants mainly feared attacks on their SH devices (e. g., manipulation of the devices) and their SH data (e. g., espionage of preferences). A concern shared by three-quarters of the participants was the fear of burglaries ($N = 31$) facilitated by the misuse of SH data and devices. This is especially interesting since a popular use case for SHs mentioned by the participants is to increase home security. Still, some of our findings seem to mirror those by Zeng *et al.* [2] where physical security was the most prevalent concern among actual SH administrators. However, comparing the findings in depth differences become apparent: Whereas the administrators' threat models were sparse, the scenarios described by our mainly non-experienced participants were often very detailed. Further, the administrators named a couple of attack scenarios but often stated not to be concerned about these while the scenarios in our study were mostly formulated as concerns. The few cases in which participants stated not to be concerned about a scenario were consequently not coded as a threat or concern in our study. Multi-user problems found by others [2, 29, 37] were not mentioned by our sample indicating that participants might only become aware of these when actually experiencing them.

Still, whereas the participants described potential threats in detail, they only seemed to have an abstract construction of how the attacks would take place. A fuzzy understanding of a third party hacking in or hooking into SH devices, or somehow intercepting data transmission was prevalent among the participants. Reasons for the users' fuzzy concept of attacks may include a limited technical understanding of lay users [12, 36] and a lack of interest in the details of *how* the system achieves something compared to *what* the system does [26, 61]. Another problem might be that, in contrast to physical attacks, digital attacks do seldom leave visible traces that directly allow the user to understand that something has happened, and how it was conducted. In line with that, other research identifies problems arising from the non-transparency of SH technologies [53, 54].

6.2.1 Technical and Psychological Measures

Some of the users' concerns can be related to real-world examples of potential or actual attacks: For example, in 2018 Newman [62] described how a vulnerability (that has then been fixed) in Amazon Echo's API could be used to turn an Echo into a covert spying device. Even though concrete numbers of people experiencing different types of attacks or the likelihood thereof are currently lacking, the users' concerns need to be addressed to support informed decision making and the user-centered development of SH technologies.

First, to address the concerns, implementing technical security measures is a prerequisite, especially as research attests that current devices are often weakly protected and thus provide attack surfaces for third parties [63, 64, 65]. Attacks need to be prevented **(R6)** or at least detected by technical solutions such as the ones proposed by Hossain *et al.* [66] or Antonakakis *et al.* [63]: security hardening, automatic updates, notifications, device identification, defragmentation and end-of-life consideration. Detailed recommendations are also published by the European Union Agency for Network and Information Security (ENISA) [67]. Furthermore, reactive security mechanisms, for example, an Intrusion Detection System (IDS), can monitor the entire network without changes to the individual components. Furthermore, they can automatically intervene upon the detection of a threat, e. g., by disconnecting an affected device from the Internet. An approach for detecting privacy leaks in mobile applications as suggested by [68] might also be applicable for detecting privacy threats in SHs. This approach checks whether data access or transfer is necessary for the functionality of the respective application using a combination of static and dynamic code analysis. If the request is not justified, it is handled as a privacy leak, which should be communicated to the user.

Second, in case of threat detection or reactive security measures, it would be important to inform the user about the threat, the action undertaken and the reason for the intervention. In general, system states, including critical states but also normal operation, need to be conveyed to the user in an understandable way **(R7 and R3)**. To achieve this Jakobi *et al.* [33] suggest using suitable visualizations. When designing such visualizations, it can help to imagine answering typical SH users security and privacy-related questions such as "Is everything o. k.?" and "Does my SH work as expected?". This also might provide users with a feeling of security and certainty [54].

Third, security or privacy notifications should make digital threats more graspable for the user to allow the development of meaningful threat models. Similar to visible, physical security threats, notifications should support the users to understand what has happened and which components or data of the SH are affected. The user should be informed which measures have been undertaken (e. g., the user is informed that a security camera video can't be uploaded due to an ongoing jamming attack) and suggest actionable ways to cope with the threat (e. g., turning off device, setting a new password) to avoid a feeling of helplessness **(R8)**. To address the concerns of users that have not yet adopted SH technologies again an interactive configurator to support an understanding of the interplay between technologies and to visualize resulting privacy and security threats, especially with remote access or the use of external servers, might be a suitable approach [60]. Another promising idea is the introduction of privacy and security labels to support the consideration of these factors in the actual purchase decision as suggested by Emami-Naeini *et al* [40]. This proposal summarizes key information on individual products such as a surveillance camera and includes the kind of data used, the respective purpose, information on updates or encryption, and an overall evaluation. A similar approach is followed by [69], which examines a selection of smart devices with regard to various security and privacy criteria and makes the results available to potential buyers in a summarized form.

Finally, it is important to mention, that especially R7 and R8 only apply to detected threats. In the rapidly evolving smart home context there might be new, not yet detected security vulnerabilities or attacks. Considering current security best practices and releasing regular security updates in line with R6 is therefore essential. However, it is possible that an attack remains undetected by the system. In that case, there are two possibilities. If the attack has visible effects, users might spot anomalies in the system's state or behaviour which can be enhanced by designing for transparency in line with **R3**. Users may then report the anomalies and thereby contribute to finding a solution to the attack. If no effects are visible to the user, then an attack might go undetected and the system as well as the user perceive the system as working normally. The only precaution in this case might be to notify the user of the system's state in a suitable way, e. g. instead of claiming "100 % security" the system might convey that absolute security can't be achieved with statements like "no threat detected".

6.2.2 Recommendations

(R3) Transparency: Not only notify users of threats but also convey normal operation to reassure users. Make system states transparent by using visualizations, tangible interaction or suitable metaphors.

(R6) Technical Security: Consider standards and best practices for secure system design to prevent attacks.

(R7) Threat Detection: Notify users of threats in a salient way to allow for immediate action. Users should be notified of threats that concern themselves but also about threats that may impact the security and privacy of others.

(R8) Design of Threat Notifications: Design threat notifications to make digital threats graspable and help users to understand what has happened and who/what is affected. Provide users with actionable suggestions to cope with and recover from threats.

6.3 Theme 3: Security-Functionality Trade-off

As expressed in the interview and questionnaire responses (see results sections 5.1.4 and 5.1.5) users perceived the local data processing as more secure and privacy-friendly than the cloud-based data processing. Thus, the participants seem to value privacy and security but half of them ($N = 26$) also expected remote control of SHs devices which was expressed in their definitions and described the functionality of SHs. Similar tensions have been discovered in other studies [2, 13, 39, 70]. Thus, the participants' perceptions mirror the trade-off between security and functionality that we described from a technical perspective in section 3.

6.3.1 Technical and Psychological Measures

This trade-off can be addressed by concepts that constitute a compromise between the local and the cloud-based data processing. In line with our suggestions above, security best practices **(R6)** should be considered when implementing SH components. However, connecting the SH to the Internet will inevitably increase the potential attack surface of the SH. A possible compromise from a psychological point of view could be to analyze and focus on the scenarios in which users require remote control **(R9)**. For instance, users might wish to monitor and control SH devices remotely while being on holiday but do not deem that necessary in everyday life. Another scenario might be that users would like to be notified about a potential threat (e. g., oven left turned on with nobody at home) but not about uncritical states. In case of a detected threat, the Internet connection could be activated to allow immediate remote control and deactivated as soon as the user has chosen an option (e. g., turn off oven). Further, multiple-user scenarios and context should be considered in this regard, e. g., consider a remote user logging into a security camera while the primary user is located at home which creates a potential for spying on the primary user. Depending on the outcome of studies analyzing the users' need for remote control in-depth, SH developers could choose from or combine the following strategies to address their needs: Limit remote access to certain devices or usage scenarios, allow remote observation but not control, or design an interface for the users to manage remote access by themselves.

6.3.2 Recommendations

(R6) Technical Security: Consider standards and best practices for secure system design to prevent attacks.

(R9) Functionality: Consider user needs for functionality such as remote control while maintaining maximum security by limiting Internet access to required devices or scenarios. Provide users with options to monitor and change Internet access.

6.4 Theme 4: User-Centric vs. Societal Perspective

The perceptions and concerns of the participants concentrated on aspects that directly affected themselves and their home (e. g., burglaries, manipulation of own SH devices, and misuse of personal data). Potential attacks that would affect others inside or outside the home, or society at large, did not seem to play an important role for the participants. As mentioned in results section 5.1.3 only four participants described DDoS attacks as a potential threat scenario.

This finding is reasonable from the users' point of view and might also be influenced by the way the questions in the interview were phrased (see the interview questions in Appendix A.1). In the interview, participants were not prompted to think about societal impacts and the sketches of different SH concepts only depicted a single SH.

Still, the threat posed by attackers misusing SH devices and data for a greater purpose is not to be underestimated. DDoS attacks on critical infrastructures can negatively impact whole populations and finally single SH users as well. For example, maliciously operated high wattage devices, e. g., air conditioners or heaters, could be used to cause large scale blackouts in the power grid [71]. Furthermore, misusing SH data for manipulating or spying on society at large, e. g., to influence voting results or purchase decisions, may finally lead to negative outcomes for others and the SH users themselves. Here, the matter of (legal) responsibility poses another challenge and remains unsolved yet. This includes, e. g., the responsibility for adequately ensuring the protection of one's own devices or for ensuring the privacy of audio data collected from guests or bystanders [72].

6.4.1 Technical and Psychological Measures

Neither our sample nor others in the literature that we are aware of, seemed to be aware of or especially concerned about the societal impacts of SH technologies. Still, due to its relevance, we suggest taking a closer look. To avoid putting even more strain and responsibility on the end users, we refrain from suggesting education and awareness measures. Instead, we propose: First, SH developers should follow standards and best practices in securing SH technologies **(R6)**. Promising solutions for threat detection are network-based IDSs as they facilitate the implementation of countermeasures in case of a detected attack (see Section 6.2.1). Further, developers should consider implementing usable security mechanisms from related areas, e. g., support users in choosing strong passwords with the help of password meters [73] instead of using a default password.

Second, whenever an attack or the users' configuration might negatively impact others, the users should be notified **(R7)** to help the user understand the potential impact on others or society even though the user him or herself might not be negatively affected directly. In line with related work, the notifications could, for example, take the form of symbols or visualizations that help the users to develop meaningful mental models. They should further suggest suitable actions to cope with the threat to not leave the user concerned or helpless **(R8)**.

6.4.2 Recommendations

(R6) Technical Security: Consider standards and best practices for secure system design to prevent attacks.

(R7) Threat Detection: Notify users of threats in a salient way to allow for immediate action. Users should be notified of threats that concern themselves but also about threats that may impact the security and privacy of others.

(R8) Design of Threat Notifications: Design threat notifications to make digital threats graspable and help users to understand what has happened and who/what is affected. Provide users with actionable suggestions to cope with and recover from threats.

7 Limitations and Future Work

Like every study, this research is subject to some limitations. First, the study took place in Germany where the participants might be slightly more privacy-sensitive than in other cultures. The results might thus not be generalizable to different cultures and further work is needed to compare intercultural differences.

Second, due to the exploratory nature of the study, a quantification of the users' level of concern in terms of the reported scenarios was not possible. Still, future research might benefit from combining qualitative research with quantifying measures similar to the ones used by [1] or [11] to support researchers in focusing on the most pressing user concerns.

Third, after having explored the participants' concepts of SHs we provided them with a general definition and two sketches of a local and cloud-based data processing concept in the second part of the interview. We provided the sketches to explain SH processes, ensure a common understanding and increase the diversity of responses by broadening the participants' perspective. Still, it is possible that the definition, as well as the provided sketches, might have influenced the participants' responses.

Fourth, the recommendations derived here are grounded in our findings and interdisciplinary literature. Still, further research is needed to evaluate and extend them, perhaps towards a list of principles with a selection of practical ideas for each recommendation. Further, we hope to stimulate the development and evaluation of actionable solutions for user-centered SH design resulting from the recommendations. Future research should also explore measures to especially address concerns in potential users that do not yet use SH technologies. For example, co-design studies as suggested by [50] that include potential users or the development of an interactive and freely accessible SH configurator might help to address concerns and reduce uncertainties.

8 Conclusion

Aiming to support informed decision making of end users interested in owning SH technologies but not having adopted the technologies yet, we first conducted semi-structured interviews with 42 participants in terms of SH-related security and privacy concerns. The results extend previous work, e. g. in the expressed concern that SH technologies could be manipulations to apply psychological pressure on inhabitants, and led us to an in-depth analysis and nuanced categorization of a variety of attack-related and attack-unrelated concerns. We were also able to show that some concerns overlap with findings from previous studies involving different methods, such as online studies [1, 11], and different samples, such as SH administrators [2]. This highlights their importance for future SH research and shows that the concerns have not been overcome yet.

The findings of our study were then clustered into four themes that center around concerns unrelated to attacks focusing on the perceived loss of control to technology, concerns related attacks on SH data and devices, the trade-off between functionality and security, and user-centric concerns as compared to concerns on a societal level.

We reviewed and discussed previous, interdisciplinary findings that offer potential solutions for the four themes of concern from a technological and psychological perspective. From these, we derived recommendations for smart home developers and researchers to support better-informed decision-making by addressing the users' concerns and increasing transparency of SH technologies.

Following technical security standards and best practices seems to be a necessary but insufficient condition for addressing users' concerns in terms of privacy and security. Even though a reasonable recommendation, researchers find that technical security measures are not yet consistently implemented [63, 64, 65]. Equally important, however, is the communication of privacy and security features to the end user: Potential SH users aim to be informed about the current state of their SH. They should be reassured of normal operation but also notified in case of threats immediately. Threat notifications should include the localization and type of threat, concrete consequences for privacy and security, and actionable recommendations for handling the threat.

Apart from that, it seems that despite the benefits of ubiquitous technologies end users aim to feel in control of what happens in their SH. Developers should thus transparently visualize SH processes to foster the users' understanding, design easy-to-use configuration interfaces, and implement fallback mechanisms that enable users to take control of SH devices, e. g. in case of technical failures.

For each recommendation we point out existing design solutions or examples that take up that recommendation, such as the privacy and security labels developed and tested by Emami-Naeini *et al.* [40] to allow informed decision making of prospective users before purchase and might also be useful for increasing transparency (R3) of SH security and privacy. With this research we hope to support both, end users' in making informed decisions rather than decisions guided by concerns, and SH developers and researchers in designing user-centered SH technologies.

Acknowledgment: The authors would further like to thank Merve Bennighof, Miriam Edel, Bettina Göbes, Oliver Hofmann, Judith Jung, Tasja Lutz, and Melina von Wick who supported the data acquisition for the study presented in this paper.

Funding: This research work has been funded by the German Federal Ministry of Education and Research (BMBF) and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity (16KIS0756K). This work was further supported by the German Federal Ministry of Education and Research (BMBF) within the SWC 2.0 "PrivacyGate" 01|S17050.

Appendix A

A.1 Interview Questions

The first question of each topic served as a starting point. All participants were asked these questions in the same order to allow for a certain degree of standardization and to make sure that all participants provided information on each topic. The questions below following the bullet points served as suggestions for the further conversation and as an orientation for the interviewer. They were used depending on the course of the interview and the answers provided by the participants.

A.1.1 Part 1 – Introduction and General Questions

With this interview we aim to explore your perceptions of SHs. The data collection takes place within a project in which [anonymized] are involved. Your data will be exclusively used for research purposes within this project and not for commercial purposes. Please answer all questions honestly and as detailed as possible. We are interested in your personal opinion, thus there are nor correct or false answers.

1. What is your understanding of the term SH?
   - Can you generalize the definition?
   - What exactly do you mean with that?
   - Can you provide an example?
2. Which terms do you associate with SHs? Provision of a sheet of paper and pencil to collect associations with the term SH.
3. Do you currently use or are you experienced with SH technologies? If yes, which technologies do you use?
4. What benefits would you personally expect using SH technologies?
   - What would be the (dis-)advantages of SH technologies for you personally?
   - What would you use a SH for?/ What do you use your SH for?
5. Please explain to me/sketch how a SHs functions according to your understanding in as much detail as possible.
   - Which components do SHs consist of?
   - How do they interact?
6. Please think about your explanation: Do you have any concerns related to SHs?
   - Do you see risks/ security issues?
   - Do you see privacy protected in a SH?
   - Where could attacks be possible?
   - What kind of attacks are possible?
   - What kind of data could attackers be interested in?

A.1.2 Part 2 – User Perceptions

Now, I'd like to provide you with a definition of SHs that we use in our project:

Definition: Household, in which sensor technology is used to intelligently connect household appliances and devices. These can be monitored and controlled from within the home or remotely to satisfy user needs. Examples:

1. Increase of comfort and quality of life, e. g. household-wide storing and access to audio and video files
2. Efficient use of energy, e. g. reduction of cost for heating through automated adaption of heating to times of absences
3. Home Security, e. g. detection of burglaries via sensors and cameras
4. Health monitoring and support, e. g. monitoring of medical data of senior in nursery homes

The definition was followed by a standardized explanation of the two SH concepts with the help of sketches (see Figure 2). Clarification of questions in terms of understanding.

1. Did your view on SHs change in light of the two concepts just presented? If yes, how?
2. Please look at the two sketches: Do you have new or other concerns? Please first answer the question for one sketch and then for the other.
   - Do you see your privacy protected? If yes, how?
   - Do you think attacks are possible?
   - Where in the sketches could attacks be possible?
   - What kind of attacks are possible?
   - What kind of data could attackers be interested in?
3. What is your general evaluation of SHs/ the two SH concepts?
4. Would you consider to use SH technologies? If yes, which technologies/which concept?

A.2 Part 3 – Rating of SH Concepts

Please indicate to what level you agree with the following statements. To do so, please tick a checkbox on the right-hand side that best aligns with your opinion. The scale ranges from "1- I do not agree at all" to "7 – I absolutely agree". By ticking one the checkboxes in between you can indicate your level of agreement.

- My privacy is protected in SHs based on cloud-based data processing.
- If I had the possibility I'd like to use SHs based on cloud-based data processing.
- SHs based on cloud-based data processing are secure, i. e. protected against attacks.
- My privacy is protected in SHs based on local data processing.
- If I had the possibility I'd like to use SHs based on local data processing.
- SHs based on local data processing are secure, i. e. protected against attacks.

A.3 Part 4 – Demographic Information

Please provide the following demographic information.

- Age: in years
- Gender: male, female, other
- Level of Education: no degree, secondary school degree, high-school diploma, completed vocational training, university degree, other
- Occupation: Open answer

References

[1] Nina Gerber, Benjamin Reinheimer and Melanie Volkamer, Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats, in: *Proceedings of the 2018 Workshop on the Human aspects of Smarthome Security and Privacy*, WSSP'18, USENIX Association, Berkeley, CA, USA, 2018.

[2] Eric Zeng, Shrirang Mare and Franziska Roesner, End User Security & Privacy Concerns with Smart Homes, in: *Proceedings of the 2017 Symposium on Usable Privacy and Security*, SOUPS'17, pp. 65–80, USENIX Association, Berkeley, CA, USA, 2017. ISBN 978-1-931971-39-3.

[3] Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket and Lorraine Whitmarsh, Social Barriers to the Adoption of Smart Homes, *Energy Policy* 63 (2013), 363–374. 10.1016/j.enpol.2013.08.043.

[4] George Demiris and Brian K. Hensel, Technologies for an Aging Society: a Systematic Review of "Smart Home" Applications, *Yearbook of medical informatics* 17 (2008), 33–40. 10.1055/s-0038-1638580.

[5] Kevin Taylor, *GfK – Smart Home. A Global Perspective*, 2016, 23 March, https://de.slideshare.net/jacklaber/180209-smart-home-a-global-perspective (Accessed February 2019).

[6] Stefan Schulze-Sturm, Blickwinkel Smart Home, *Wissenschaft Trifft Praxis* 4 (2016), 5–11.

[7] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu and Colin Dixon, Home Automation in the Wild: Challenges and Opportunities, in: *Proceedings of the 2011 CHI Conference on Human Factors in Computing Systems*, CHI'11, pp. 2115–2124, ACM, New York, NY, USA, 2011. ISBN 978-1-4503-0228-9. 10.1145/1978942.1979249.

[8] William Green, Diane Gyi, Roy Kalawsky and David Atkins, Capturing User Requirements for an Integrated Home Environment, in: *Proceedings of the 2004 Nordic conference on Human-computer Interaction*, NordiCHI'04, pp. 255–258, ACM, New York, NY, USA, 2004. 10.1145/1028014.1028053.

[9] Svetlana Yarosh and Pamela Zave, Locked or Not?: Mental Models of IoT Feature Interaction, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, pp. 2993–2997, ACM, New York, NY, USA, 2017. 10.1145/3025453.3025617.

[10] Corinna Ogonowski, Dirk Förmer, Svenja Gussmann, Philippe Hennes, Kai Hackbarth, Timo Jakobi, Konstantin Kersten, Jens Läkamp, Anil Mengi, Fabian Pursche, Stefan Schulz-Sturm, Gunnar Stevens and Volker Wulf, Living Lab as a Service: Individuelle Dienstleistungen zur nutzerzentrierten Innovationsentwicklung im Smart Home, *Wissenschaft trifft Praxis* 4 (2016), 27–37.

[11] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor and Norman Sadeh, Privacy Expectations and Preferences in an IoT World, in: *Proceedings of the 2017 Symposium on Usable Privacy and Security*, SOUPS'17, pp. 399–412, USENIX Association, Berkeley, CA, USA, 2017. ISBN 978-1-931971-39-3.

[12] Florian Kirchbuchner, Tobias Grosse-Puppendahl, Matthias R. Hastall, Martin Distler and Arjan Kuijper, Ambient intelligence from senior citizens' perspectives: Understanding privacy concerns, technology acceptance, and expectations, in: *Ambient Intelligence*, Lecture Notes in Computer Science 9425, pp. 48–59, Springer International Publishing, Cham, Switzerland, 2015. 10.1007/978-3-319-26005-1_4.

[13] Anandhi Vivek Dhukaram, Chris Baber, Lamia Elloumi, Bert-Jan van Beijnum and Paolo De Stefanis, End-User Perception Towards Pervasive Cardiac Healthcare Services: Benefits, Acceptance, Adoption, Risks, Security, Privacy and Trust, in: *Proceedings of the 2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*, pp. 478–484, IEEE, Piscataway, NJ, USA, 2011. 10.4108/icst.pervasivehealth.2011.246116.

[14] Daphne Townsend, Frank Knoefel and Rafik Goubran, Privacy versus autonomy: a tradeoff model for smart home monitoring technologies, in: *2011 Annual International Conference on the IEEE Engineering in Medicine and Biology Society*, pp. 4749–4752, IEEE, Piscataway, NJ, USA, 2011. 10.1109/IEMBS.2011.6091176.

[15] Christina Jaschinski, Ambient assisted living: towards a model of technology adoption and use among elderly users, in: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, UbiComp'14 Adjunct, pp. 319–324, ACM, New York, NY, USA, 2014. 10.1145/2638728.2638838.

[16] Karen L. Courtney, George Demeris, Marilyn Rantz and Marjorie Skubic, Needing smart home technologies: the perspectives of older adults in continuing care retirement communities, *Informatics in Primary Care* 16 (2008), 195–201. 10.14236/jhi.v16i3.694.

[17] Corinna Ogonowski, Benedikt Ley, Jan Hess, Lin Wan and Volker Wulf, Designing for the Living Room: Long-term User Involvement in a Living Lab, in: *Proceedings of the 2013 CHI Conference on Human Factors in Computing Systems*, CHI'13, pp. 1539–1548, ACM, New York, NY, USA, 2013. 10.1145/2470654.2466205.

[18] Rikke Hagensby Jensen, Yolande Strengers, Jesper Kjeldskov, Larissa Nicholls and Mikael B. Skov, Designing the Desirable Smart Home: A Study of Household Experiences and Energy Consumption Impacts, in: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI'18, pp. 4:1–4:14, ACM, New York, NY, USA, 2018. 10.1145/3173574.3173578.

[19] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens and Volker Wulf, What Happened in My Home?: An End-User Development Approach for Smart Home Data Visualization, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, pp. 853–866, ACM, New York, NY, USA, 2017. 10.1145/3025453.3025485.

[20] Christoffer Björkskog, Giulio Jacucci, Topi Mikkola, Massimo Bertoncini, Luciano Gamberini, Carin Torstensson, Tatu Nieminen, Luigi Briguglio, Pasquale Andriani and G. Firoentino, BeAware: A Framework for Residential Services on Energy Awareness, in: *Proceedings of the 4th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, UbiComm'10, pp. 294–300, IARIA XPS Press, 2010. http://www.thinkmind.org/index.php?view=instance&instance=UBICOMM+2010.

[21] Nico Castelli, Gunnar Stevens, Timo Jakobi and Niko Schönau, *Beyond Eco-feedback: Using Room as a Context to Design New Eco-support Features at Home*, Advances and New Trends in Environmental and Energy Informatics: Selected and Extended Contributions from the 28th International Conference on Informatics for Environmental Protection, Progress in IS, Springer International Publishing, Cham, Switzerland, 2016, pp. 177–195. 10.1007/978-3-319-23455-7_10.

[22] Sarah Darby, The Effectiveness of Feedback on Energy Consumption, *A Review for DEFRA of the Literature on Metering, Billing and Direct Displays* 486 (2006), 26.

[23] Jon Froehlich, Leah Findlater and James Landay, The Design of Eco-feedback Technology, in: *Proceedings of the 2010 CHI Conference on Human Factors in Computing Systems*, CHI'10, pp. 1999–2008, ACM, New York, NY, USA, 2010. 10.1145/1753326.1753629.

[24] Tobias Schwartz, Gunnar Stevens, Timo Jakobi, Sebastian Denef, Leonardo Ramirez, Volker Wulf and Dave Randall, What people do with consumption feedback: a long-term living lab study of a home energy management system, *Interacting with Computers* 27 (2015), 551–576. 10.1093/iwc/iwu009.

[25] Tobias Schwartz, Sebastian Denef, Gunnar Stevens, Leonardo Ramirez and Volker Wulf, Cultivating energy literacy: results from a longitudinal living lab study of a home energy management system, in: *Proceedings of the 2013 CHI Conference on Human Factors in Computing Systems*, CHI'13, pp. 1193–1202, ACM, New York, NY, USA, 2013. 10.1145/2470654.2466154.

[26] Alper T. Alan, Mike Shann, Enrico Costanza, Sarvapali D. Ramchurn and Sven Seuken, It is Too Hot: An In-Situ Study of Three Designs for Heating, in: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI'16, pp. 5262–5273, ACM, New York, NY, USA, 2016. 10.1145/2858036.2858222.

[27] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung and Melina von Wick, 'Home, Smart Home'–Exploring End Users' Mental Models of Smart Homes, *Mensch und Computer 2018 – Workshopband* (2018). 10.18420/muc2018-ws08-0539.

[28] Stephen Snow, Frederik Auffenberg and Monica M. C. Schraefel, Log It While It's Hot: Designing Human Interaction with Smart Thermostats for Shared Work Environments, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, pp. 1595–1606, ACM, New York, NY, USA, 2017. 10.1145/3025453.3025578.

[29] Sarah Mennicken, David Kim and Elaine May Huang, Integrating the Smart Home into the Digital Calendar, in: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI'16, pp. 5958–5969, ACM, New York, NY, USA, 2016. 10.1145/2858036.2858168.

[30] Yaliang Chuang, Lin-Lin Chen and Yoga Liu, Design Vocabulary for Human–IoT Systems Communication, in: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI'18, pp. 274:1–274:11, ACM, New York, NY, USA, 2018. 10.1145/3173574.3173848.

[31] Haiyan Jia, Mu Wu, Eunhwa Jung, Alice Shapiro and S. Shyam Sundar, Balancing human agency and object agency: an end-user interview study of the internet of things, in: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp'12, pp. 1185–1188, ACM, New York, NY, USA, 2012. 10.1145/2370216.2370470.

[32] Sarah Mennicken and Elaine M. Huang, Hacking the natural habitat: an in-the-wild study of smart homes, their development, and the people who live in them, in: *Proceedings of the 2012 international conference on Pervasive Computing*, Pervasive'12, pp. 143–160, Springer, Cham, Switzerland, 2012. 10.1007/978-3-642-31205-2_10.

[33] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens and Volker Wulf, The catch (es) with smart home: Experiences of a living lab field study, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 1620–1633, ACM, New York, NY, USA, 2017. 10.1145/3025453.3025799.

[34] Tom A. Rodden, Joel E. Fischer, Nadia Pantidi, Khaled Bachour and Stuart Moran, At Home with Agents: Exploring Attitudes Towards Future Smart Energy Infrastructures, in: *Proceedings of the 2013 CHI Conference on Human Factors in Computing Systems*, CHI'13, pp. 1173–1182, ACM, New York, NY, USA, 2013. 10.1145/2470654.2466152.

[35] Alex S. Taylor, Richard Harper, Laurel Swan, Shahram Izadi, Abigail Sellen and Mark Perry, Homes that make us smart, *Personal and Ubiquitous Computing* 11 (2007), 383–393. 10.1007/s00779-006-0076-5.

[36] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter and Sara Kiesler, "My data just goes everywhere:" User mental models of the internet and implications for privacy and security, in: *Proceedings of the 2015 Symposium on Usable Privacy and Security*, SOUPS'15, pp. 39–52, USENIX Association, Berkeley, CA, USA, 2015. ISBN 978-1-931971-249.

[37] Blase Ur, Jaeyeon Jung and Stuart Schechter, 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, UbiComp'14, pp. 129–139, ACM, New York, NY, USA, 2014. 10.1145/2632048.2632107.

[38] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman and Nick Feamster, Discovering smart home internet of things privacy norms using contextual integrity, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2 (2018). 10.1145/3214262.

[39] Serena Zheng, Noah Apthorpe, Marshini Chetty and Nick Feamster, User perceptions of smart home IoT privacy, *Proceedings of the ACM on Human-Computer Interaction* 2 (2018). 10.1145/3274469.

[40] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal and Lorrie Faith Cranor, Exploring How Privacy and Security Factor into IoT Device Purchase Behavior, in: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI'19, pp. 534:1–534:12, ACM, New York, NY, USA, 2019. 10.1145/3290605.3300764.

[41] David Shum, John O'Gorman, Brett Myors and Peter Creed, *Psychological testing and assessment*, Oxford University Press Melbourne, 2006.

[42] Philipp Mayring, *Qualitative Inhaltsanalyse*, Handbuch qualitative Forschung in der Psychologie, Springer, Cham, Switzerland, 2010, pp. 601–613. 10.1007/978-3-531-92052-8_42.

[43] Michaela Gläser-Zikuda, *Qualitative Auswertungsverfahren*, Empirische Bildungsforschung (H. Reinders, ed.), VS Verlag für Sozialwissenschaften, Springer, 2011, pp. 109–119.

[44] Andy Field, *Discovering Statistics Using IBM SPSS Statistics. 5th Edition*, 2018.

[45] Joseph F. Coughlin, Lisa A. D'Ambrosio, Bryan Reimer and Michelle R. Pratt, Older adult perceptions of smart home technologies: implications for research, policy & market innovations in healthcare, in: *2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 1810–1815, IEEE, Piscataway, NJ, USA, 2007. 10.1109/IEMBS.2007.4352665.

[46] Nancy V. Wünderlich, Florian von Wangenheim and Mary Jo Bitner, High tech and high touch: a framework for understanding user attitudes and behaviors related to smart interactive services, *Journal of Service Research* 16 (2013), 3–20. 10.1177/1094670512448413.

[47] Deógenes Pereira da Silva Junior, Patricia Cristiane de Souza and Cristiano Maciel, Establishing guidelines for user quality of experience in ubiquitous systems, in: *Distributed, Ambient and Pervasive Interactions*, Lecture Notes in Computer Science 9749, pp. 46–57, Springer International Publishing, Cham, Switzerland, 2016. 10.1007/978-3-319-39862-4_5.

[48] Carsten Röcker, Maddy D. Janse, Nathalie Portolan and Norbert Streitz, User requirements for intelligent home environments: a scenario-driven approach and empirical cross-cultural study, in: *Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*, sOc-EUSAI'05, pp. 111–116, ACM, New York, NY, USA, 2005. 10.1145/1107548.1107581.

[49] Ellen A. Skinner, A guide to constructs of control, *Journal of personality and social psychology* 71 (1996), 549–570. 10.1037/0022-3514.71.3.549.

[50] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik and Yang Wang, 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*, CHI'19, ACM, New York, NY, USA, 2019. 10.1145/3290605.3300428.

[51] Michal Luria, Guy Hoffman and Oren Zuckerman, Comparing Social Robot, Screen and Voice Interfaces for Smart-Home Control, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, pp. 580–628, ACM, New York, NY, USA, 2017. 10.1145/3025453.3025786.

[52] Sidney Dekker, *Foundations of Safety Science: A Century of Understanding Accidents and Disasters*, CRC Press, 2019. ISBN 9781351059787.

[53] Ryan Brotman, Winslow Burleson, Jodi Forlizzi, William Heywood and Jisoo Lee, Building change: Constructive design of smart domestic environments for goal achievement, in: *Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems*, CHI'15, pp. 3083–3092, ACM, New York, NY, USA, 2015. 10.1145/2702123.2702602.

[54] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens and Volker Wulf, What happened in my home?: An end-user development approach for smart home data visualization, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, pp. 853–866, ACM, New York, NY, USA, 2017. 10.1145/3025453.3025485.

[55] Alexandra Voit, Elizabeth Stowell, Dominik Weber, Christoph Witte, Daniel Kärcher and Niels Henze, Envisioning an ambient smart calendar to support aging in place, in: *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, UbiComp'16 Adjunct, pp. 1596–1601, ACM, New York, NY, USA, 2016. 10.1145/2968219.2968555.

[56] Cathleen Wharton, The cognitive walkthrough method: A practitioner's guide, *Usability inspection methods* (1994).

[57] Mark Weiser, The Computer for the 21 st Century, *Scientific American* 265 (1991), 94–105. http://www.jstor.org/stable/24938718.

[58] Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie and Volker Wulf, Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2 (2018), 171. 10.1145/3287049.

[59] Brian Y. Lim, Anind K. Dey and Daniel Avrahami, Why and why not explanations improve the intelligibility of context-aware intelligent systems, in: *Proceedings of the 2009 CHI Conference on Human Factors in Computing Systems*, CHI'09, pp. 2119–2128, ACM, New York, NY, USA, 2009. 10.1145/1518701.1519023.

[60] Verena Zimmermann, Ernestine Dickhaut, Paul Gerber and Joachim Vogt, Vision: Shining Light on Smart Homes – Supporting Informed Decision-Making of End Users, *Proceedings of 2019 IEEE European Symposium on Security and Privacy Workshops* (2019), 149–153. 10.1109/EuroSPW.2019.00023.

[61] Rayoung Yang and Mark W. Newman, Learning from a learning thermostat: lessons for intelligent systems for

the home, in: *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp'13, pp. 93–102, ACM, New York, NY, USA, 2013. 10.1177/1094670512448413.

[62] Lily Hay Newman, *Turning an Echo Into a Spy Device Only Took Some Clever Coding*, 2018, 25 April, https://www.wired.com/story/amazon-echo-alexa-skill-spying/ (Accessed July 2019).

[63] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas and Yi Zhou, Understanding the mirai botnet, in: *Proceedings of the 26th USENIX Security Symposium*, USENIX Security'17, pp. 1092–1110, USENIX Association, Berkeley, CA, USA, 2017. ISBN 978-1-931971-40-9.

[64] Lily Hay Newman, The botnet that broke the Internet isn't going away, *Wired* (2016, 12 September), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/?mbid=synd_digg (Accessed October 2019).

[65] HP Inc, *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*, 2014, 29 July, https://www8.hp.com/de/de/hp-news/press-release.html?id=1744676 (Accessed February 2019).

[66] Md Mahmud Hossain, Maziar Fotouhi and Ragib Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: *2015 IEEE World Congress on Services*, pp. 21–28, IEEE, 2015.

[67] ENISA, *Recommendations for IoT – ENISA*, 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot November (Accessed September 2018).

[68] Xiaolei Wang, Andrea Continella, Yuexiang Yang, Yongzhong He and Sencun Zhu, LeakDoctor: Toward Automatically Diagnosing Privacy Leaks in Mobile Applications, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3 (2019), 28. 10.1145/3314415.

[69] Rebecca Ricks and Janice Tsai, *How We Evaluated the Products in Mozilla's *privacy not included Buyer's Guide (2019)*, 2018, 13th November, https://medium.com/@harraton/how-we-evaluated-the-products-in-mozillas-privacy-not-included-buyer-s-guide-2018-6b122f885de0 (Accessed October 2019).

[70] Erika Chin, Adrienne Porter Felt, Vyas Sekar and David Wagner, Measuring user confidence in smartphone security and privacy, in: *Proceedings of the 2012 Symposium on Usable Privacy and Security*, SOUPS'12, pp. 1:1–1:16, ACM, New York, NY, USA, 2012. 10.1145/2335356.2335358.

[71] Saleh Soltan, Prateek Mittal and H. Vincent Poor, BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, in: *Proceedings of the 27th USENIX Security Symposium*, USENIX Security'18, USENIX Association, Berkeley, CA, USA, 2018. ISBN 978-1-939133-04-5.

[72] Katrin Wolf, Karola Marky and Markus Funk, We should start thinking about Privacy Implications of Sonic Input in Everyday Augmented Reality!, in: *Mensch und Computer 2018 – Workshopband*, pp. 353–359, Gesellschaft für Informatik e.V., Bonn, 2018. 10.18420/muc2018-ws07-0466.

[73] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib andet al., Design and evaluation of a data-driven password meter, in: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, pp. 3775–3786, ACM, New York, NY, USA, 2017. 10.1145/3025453.3026050.

Supplemental Material: The online version of this article offers supplementary material (https://doi.org/10.1515/icom-2019-0015).

Bionotes

Verena Zimmermann
Work and Engineering Psychology,
Technische Universität Darmstadt,
Darmstadt, Germany
verena.zimmermann@tu-darmstadt.de

Verena Zimmermann is a doctoral researcher in the working group "Work and Engineering Psychology" at the Department of Psychology since 2016. She studied psychology and graduated with a Master of Science degree in 2015. Working in different research projects within the National Research Center for Applied Cybersecurity (CRISP) Verena Zimmermann is concerned with Human Factors in Security and Safety. Her research interests include usable authentication and communication, nudging in security and privacy, and user-centered Smart Home design.

Paul Gerber
Work and Engineering Psychology,
Technische Universität Darmstadt,
Darmstadt, Germany
paul.gerber@tu-darmstadt.de

Dr. Paul Gerber is a post-doctoral researcher in the working group "Work and Engineering Psychology" at the Department of Psychology since 2012. He works on two research projects within the National Research Center for Applied Cybersecurity (CRISP). His doctoral thesis was concerned with supporting users' privacy-relevant behaviors through suitable information. In the last years he was involved in projects concerning the certified security of mobile applications (ZertApps) and the psychological modelling of behavioral factors in the context of the privacy paradox (MoPPa). Dr. Gerber's further research interests include (mobile) digital privacy and product evaluation.

Karola Marky
Telecooperation Lab, Technische Universität Darmstadt, Darmstadt, Germany
Keio University, Yokohama, Japan
marky@tk.tu-darmstadt.de

Karola Marky is a doctoral Human-Computer Interaction researcher at the Telecooperation Lab at Technische Universität Darmstadt in Germany. She studied Computer Science focusing on IT-security and psychology and graduated with a master's degree in 2017. Her research focuses on human factors in IT-security. This includes the usability and user experience of end-to-end verifiable Internet voting schemes, enhancing the privacy of mobile device users, as well as privacy and security aspects of smart home technologies.

Leon Böck
Telecooperation Lab, Technische Universität Darmstadt, Darmstadt, Germany
boeck@tk.tu-darmstadt.de

Leon Böck is a doctoral researcher at the Telecooperation Lab at Technische Universität Darmstadt. He obtained his Master's degree at Technische Universität Darmstadt in 2017. His research is concerned with the cybersecurity of the Internet of Things, especially with botnet attacks, intrusion detection and defense mechanisms.

Florian Kirchbuchner
Fraunhofer Institute for Computer Graphics, Darmstadt, Germany
florian.kirchbuchner@igd.fraunhofer.de

Florian Kirchbuchner is head of the department for Smart Living & Biometric Technologies at the Fraunhofer Institute for Computer Graphics Research IGD. He is trained as an information and telecommunication systems technician and served as IT expert for the German Army from 2001 to 2009. Afterwards he studied computer science at Technische Universität Darmstadt and graduated with a Master of Science degree in 2014. He has been working at Fraunhofer IGD since 2014. He is also Principal Investigator at the National Research Center for Applied Cybersecurity (CRISP). Mr. Kirchbuchner participated at Software Campus, a management program of the Federal Ministry of Education and Research (BMBF) and is currently doing his PhD at Technische Universität Darmstadt on the topic ”Electric Field Sensing for Smart Support Systems: Applications and Implications”.