2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) | 978-1-6654-1658-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/TRUSTCOM53373.2021.00138

How to Increase Smart Home Security and Privacy Risk Perception

Reyhan Duezguen, Peter Mayer, Benjamin Berens, Christopher Beckmann, Lukas Aldag, Mattia Mossano
Melanie Volkamer, Thorsten Strufe
Karlsruhe Institute of Technology, firstname.lastname@kit.edu

***Abstract*—With continuous technological advancements, our homes become smarter by interconnecting more and more devices. Smart homes provide many advantages. However, they also introduce new privacy and security risks. Recent studies show that only a few people are aware of abstract risks, and most people are not aware of specific negative consequences. We developed a privacy and security awareness intervention for people who want to inform themselves about risks in the smart home context. Our intervention is based on research literature on risk perception and feedback from both lay users and security and privacy experts. We evaluated our intervention regarding its influence on participants' perceived threat, privacy attitude, motivation to avoid threats, willingness to pay, and time commitment to configure protective measures. The results of this evaluation show a significant increase for all these aspects. We also compared our intervention to information that users could obtain during an Internet search on the topic. In this comparison, our intervention evokes a significantly higher perceived threat and privacy attitude. It showed no significant difference for the other three scales. We discuss our findings in light of related work.**

***Index Terms*—smart home, risk intervention, security & privacy risk perception**

I. Introduction

The adoption of smart home devices is rapidly growing with expectations to exceed $53 billion in market size globally by 2022 [46]. Smart homes have many advantages for users such as automation, remote control, and physical safety [5], [6]. But these advantages come alongside a variety of security and privacy risks as shown and discussed in prior research [10], [19]. These risks evolve in particular due to various network-level issues (e.g. unencrypted exchange over WiFi) [2], [44] as well as device- and application-level issues (e.g. granted more privileges than needed, weak authentication, credentials stored in plaintext, third-party security breaches) which can for example lead to eavesdropping or "man-in-the-middle" attacks [7], [19]. However, vendors of smart home devices do not take action on educating their users on security and privacy risks [30]. Thus, it does not come as a surprise that smart home users were found to have a limited perception of security and privacy risks. Indeed, research has shown that only few people are aware of abstract risks and almost none are aware of specific negative consequences (e.g. being stalked or not getting a job), for both smart home devices [23], [31], [48], [54] and for other technologies [4], [27], [45].

Yet, an appropriate level of risk perception can be important for users of smart home devices as a prerequisite to them initiating actions to mitigate these risks. If users are not aware of and do not perceive the security and privacy risks they face, they will have little incentive to acquire knowledge on how to protect themselves and their devices (e.g., configure devices to optimize the privacy protection) [55].

This paper aims to provide an intervention that comprises enough information to people interested in this topic to effectively raise their perception of security and privacy risks of smart homes and to motivate them to take protective actions regarding their security and privacy when using smart home devices. The intervention was designed based on literature on risk communication, but considers as part of the development process also feedback from security and privacy experts on the one hand as well as lay smart home users on the other hand. We evaluated the intervention's effectiveness in an online survey with 131 participants. The intervention shows a significant effect on people's risk perception and motivation to use protective measures. Compared to a simulated Internet search, the intervention performs significantly better in raising risk perception and shows no significant difference in motivating to use protective measures.

II. Risk Perception Intervention

In this section, we first provide an overview of the literature our intervention is based on. Then, we describe the structure and the content of our intervention. Last but not least, we report on the feedback we got from experts and lay-users and the improvements we derived from this feedback.

A. Background Literature

1) Misconceptions Regarding Trust in Manufacturer: Studies investigated reasons for smart home user's lack of concern about security and privacy risks. Zeng et al. [54] conducted semi-structured interviews with smart home users. They discovered that *users on the one hand trust smart home manufacturers and third parties, while identifying these companies most frequently as potential adversaries* on the other hand. Even if they acknowledge manufacturers as potential adversarial actors, they feel not personally targeted and believe their mitigation strategies are sufficient. In similar studies [53], [55], this phenomenon is also explained by user's trust in

This work was partially funded by the European Unions Horizon 2020 Research and Innovation Programme through the GHOST project under Grant Agreement No. 740923. The research was furthermore supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS) at Karlsruhe Institute of Technology.

2324-9013/21/$31.00 ©2021 IEEE
DOI 10.1109/TrustCom53373.2021.00138

smart home manufactures, especially their brand familiarity and reputation. Trust in manufacturers was one of the drivers of adopting smart home devices. Users believed that trusted manufacturers already include adequate security and privacy protection in their devices and were confident that no further protective measures are required [55].

2) Mix of Abstract Risks and Specific Consequences: Our research is built on the findings from Gerber et al. [24]. The authors investigate mental models on risk perception of using smart home devices. In a between-subject study, the authors asked lay users to rate four abstract and five specific privacy risk scenarios according their probability and severity – the two aspects of risks. Participants perceived abstract risk scenarios as very likely but of medium severity. Whereas, participants evaluated specific privacy risk scenarios as less likely but of medium and high severity. Especially, risks related to physical safety and financial loss were perceived as the most severe. Thus the authors argue, that – to successfully raise risk perception and motivate individuals to better protect themselves – *any intervention needs to include both abstract risks and specific negative consequences*. Furthermore, the authors of [24] showed that severity and likelihood of several concrete consequences were perceived very differently by people, as not all consequences apply to everyone to the same extent. Thus, to address a broad audience, it is necessary to include concrete consequences from a broad scope of use cases in an intervention.

3) Types of Concrete Negative Consequences: Karwatzki et al. [29] conducted an extensive study to uncover individuals' perceptions of negative consequences from data use. They asked focus groups to name all possible privacy consequences of a well established technology and categorized them into the following *seven types of consequences*: physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related.

4) Communicating Risks: Garg & Camp [22] investigated how users perceive security and privacy risks in online environments. They asked 93 participants in a survey to rate different aspects of security and privacy risks to identify dimensions of online risks. They found that the factor of time has the biggest influence in shaping risk perception. *Older risks and risks closer to the physical world are better understood and considered more hazardous*. They explained their findings with previous results from [35] and [49]. Van Schaik et al. [50] conducted an online study with 436 UK and US students to investigate cyber-security hazards. They found that identity theft is among the risks that evoked the highest risk perception, which is in line with results from Garg & Camp [22]. Furthermore, in [11], Camp suggests to *link security risks to crimes*. This approach lets people experience themselves better as potential victims and call for action. Additionally, interventions should explain complex security aspects in an understandable fashion, e.g., using simple language. Without some understanding of the issues, an adequate response is unlikely [8], [51].

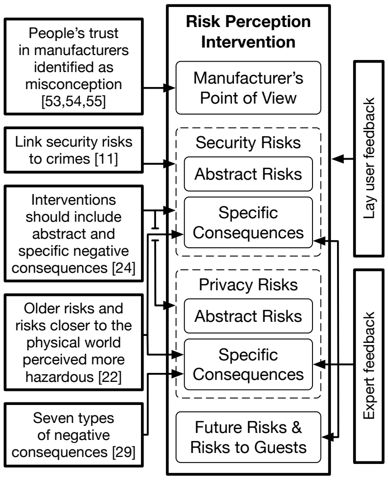

People's trust in manufacturers identified as misconception [53,54,55]
Link security risks to crimes [11]
Interventions should include abstract and specific negative consequences [24]
Older risks and risks closer to the physical world perceived more hazardous [22]
Seven types of negative consequences [29]
Risk Perception Intervention
Manufacturer's Point of View
Security Risks
Abstract Risks
Specific Consequences
Privacy Risks
Abstract Risks
Specific Consequences
Future Risks & Risks to Guests
Lay user feedback
Expert feedback

Fig. 1: The intervention and the input used for its development.

B. Structure and Content

The intervention's first section presents the point of view of smart home manufacturers on security and privacy issues to explain their motivation on potential data leaks and shortcuts manufacturers might take in the protection of their users. The goal in this is to address the findings described in Section II-A1, i.e., allowing individuals to understand the misconception surrounding all manufacturers' trustworthiness.

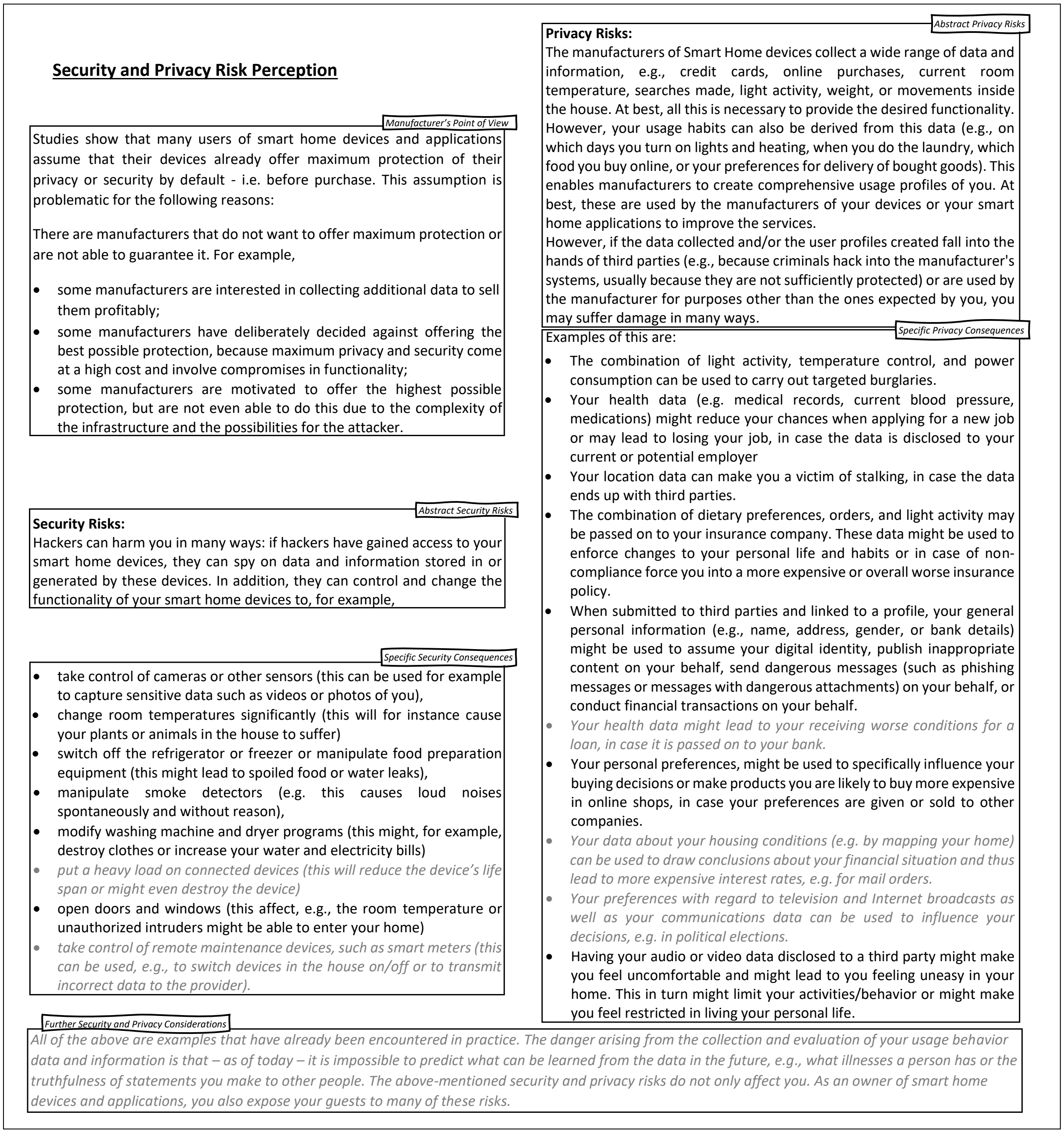
Then, the intervention includes a section on security and thereafter one on privacy. Following the findings from Section II-A2, we first provide in each of these two sections abstract risks followed by a number of specific consequences. The text on abstract privacy risks is based on the one used in [24]. The text on abstract security risks has a similar style.

We made sure to include at least one specific consequence per category from Section II-A3. We also made sure that specific consequences speaking to different groups of individuals were included, thereby following the recommendations in [24]. Furthermore, in the formulation of the specific consequences, the findings from Section II-A4 were considered. For example, we linked specific consequences to well-known crimes from the physical world, e.g., targeted burglaries by creating user profiles to determine absence from home or by taking control of smart doors and windows. Note, the specific privacy related consequences which we included in the intervention were inspired by the messages tested in [24].

The input used during the development of the intervention is depicted in Fig. 1 and the final content of the intervention in Fig. 2. Note that this final version of the content already includes modifications based on feedback from experts and lay users as outlined in the next section (Section II-C).

C. Collecting and Integrating Feedback

In two rounds of feedback, the intervention was first checked by several security and privacy experts regarding its completeness and then feedback was collected from lay users regarding its understandability.



Security and Privacy Risk Perception

Manufacturer's Point of View

Studies show that many users of smart home devices and applications assume that their devices already offer maximum protection of their privacy or security by default - i.e. before purchase. This assumption is problematic for the following reasons:

There are manufacturers that do not want to offer maximum protection or are not able to guarantee it. For example,

- some manufacturers are interested in collecting additional data to sell them profitably;
- some manufacturers have deliberately decided against offering the best possible protection, because maximum privacy and security come at a high cost and involve compromises in functionality;
- some manufacturers are motivated to offer the highest possible protection, but are not even able to do this due to the complexity of the infrastructure and the possibilities for the attacker.

Security Risks:
Hackers can harm you in many ways: if hackers have gained access to your smart home devices, they can spy on data and information stored in or generated by these devices. In addition, they can control and change the functionality of your smart home devices to, for example,

- take control of cameras or other sensors (this can be used for example to capture sensitive data such as videos or photos of you),
- change room temperatures significantly (this will for instance cause your plants or animals in the house to suffer)
- switch off the refrigerator or freezer or manipulate food preparation equipment (this might lead to spoiled food or water leaks),
- manipulate smoke detectors (e.g. this causes loud noises spontaneously and without reason),
- modify washing machine and dryer programs (this might, for example, destroy clothes or increase your water and electricity bills)
- *put a heavy load on connected devices (this will reduce the device's life span or might even destroy the device)*
- open doors and windows (this affect, e.g., the room temperature or unauthorized intruders might be able to enter your home)
- *take control of remote maintenance devices, such as smart meters (this can be used, e.g., to switch devices in the house on/off or to transmit incorrect data to the provider).*

Privacy Risks:
The manufacturers of Smart Home devices collect a wide range of data and information, e.g., credit cards, online purchases, current room temperature, searches made, light activity, weight, or movements inside the house. At best, all this is necessary to provide the desired functionality. However, your usage habits can also be derived from this data (e.g., on which days you turn on lights and heating, when you do the laundry, which food you buy online, or your preferences for delivery of bought goods). This enables manufacturers to create comprehensive usage profiles of you. At best, these are used by the manufacturers of your devices or your smart home applications to improve the services.
However, if the data collected and/or the user profiles created fall into the hands of third parties (e.g., because criminals hack into the manufacturer's systems, usually because they are not sufficiently protected) or are used by the manufacturer for purposes other than the ones expected by you, you may suffer damage in many ways.

Examples of this are:

- The combination of light activity, temperature control, and power consumption can be used to carry out targeted burglaries.
- Your health data (e.g. medical records, current blood pressure, medications) might reduce your chances when applying for a new job or may lead to losing your job, in case the data is disclosed to your current or potential employer
- Your location data can make you a victim of stalking, in case the data ends up with third parties.
- The combination of dietary preferences, orders, and light activity may be passed on to your insurance company. These data might be used to enforce changes to your personal life and habits or in case of non-compliance force you into a more expensive or overall worse insurance policy.
- When submitted to third parties and linked to a profile, your general personal information (e.g., name, address, gender, or bank details) might be used to assume your digital identity, publish inappropriate content on your behalf, send dangerous messages (such as phishing messages or messages with dangerous attachments) on your behalf, or conduct financial transactions on your behalf.
- *Your health data might lead to your receiving worse conditions for a loan, in case it is passed on to your bank.*
- Your personal preferences, might be used to specifically influence your buying decisions or make products you are likely to buy more expensive in online shops, in case your preferences are given or sold to other companies.
- *Your data about your housing conditions (e.g. by mapping your home) can be used to draw conclusions about your financial situation and thus lead to more expensive interest rates, e.g. for mail orders.*
- *Your preferences with regard to television and Internet broadcasts as well as your communications data can be used to influence your decisions, e.g. in political elections.*
- Having your audio or video data disclosed to a third party might make you feel uncomfortable and might lead to you feeling uneasy in your home. This in turn might limit your activities/behavior or might make you feel restricted in living your personal life.

All of the above are examples that have already been encountered in practice. The danger arising from the collection and evaluation of your usage behavior data and information is that – as of today – it is impossible to predict what can be learned from the data in the future, e.g., what illnesses a person has or the truthfulness of statements you make to other people. The above-mentioned security and privacy risks do not only affect you. As an owner of smart home devices and applications, you also expose your guests to many of these risks.

Fig. 2: Smart home security and privacy risk perception intervention. Highlighted sections are additions from experts.

a) Expert Feedback: We had the chance to gather feedback from consortium partners of our EU project on smart homes. These partners were experts in the domain of smart home security and privacy from academia and industry. They were asked to check for completeness, i.e., are any important or frequently occurring specific security and privacy consequences missing. They listed a number of further specific consequences. As there were too many to be included, we discussed with them how to proceed. We agreed on adding three further privacy consequences, i.e., one psychological and two resource-oriented. The experts also mentioned, that the key advantage of increased functionality when smart home devices are connected to a network and interconnect with other smart home devices or access online resources, can cause security threats when their network access is not well protected. Thus, we added two security related consequences to emphasize the importance of network protection. Moreover, based on the experts' feedback and a discussion of this feedback, we decided to add a paragraph on 'Further Security and Privacy Considerations' to the intervention. The added risks are displayed highlighted in Fig. 2.

b) Lay User Feedback: Thanks to the same EU project, almost 50 lay smart home users could be asked to read and feedback the intervention as well. Those lay users agreed for the EU project as a whole to participate in trials, i.e., having smart home technology installed in their homes together with a security/privacy gateway. We asked the participants to read the text and let us know what is unclear, what they like, and what they do not like. The feedback was collected by the partners in the respective countries and languages. Afterwards, the feedback was discussed with the partners and changes to the intervention were derived. This included a number of small changes. Some lay users remarked that the intervention is relatively long. However, the length of the text was necessary to include the findings from Section II-A. We argue that the intervention's use for educational purposes warrants the inclusion of all the information. Thus, we decided to leave the high density of information in the intervention unchanged.

III. Evaluation of the Intervention

This section outlines our research questions and hypotheses. Then, our user study, recruiting process and ethical considerations, as well as the analysis methodology are presented.

A. Research Questions and Hypotheses

Our intervention aims to raise the perception of security and privacy risks in the smart home context. The two research questions presented in the remainder of this section serve to assess the effectiveness of this intervention.

1) RQ-1 — Raising Risk Perception: The first aspect we aim to investigate is raising the risk perception of our participants. The research question guiding this investigation is:

RQ-1: ***What is the effect of our intervention on people's perception of privacy and security risks of smart home?***

Based on the literature presented in Section II-A we assume the presence of an effect on our participants' perception of security and privacy risks. Therefore, we formulated two hypotheses to assess the participants' threat perception (H_{PT-1} and H_{PT-2}) and two hypotheses to assess their privacy attitude (H_{PA-1} and H_{PA-2}). In the following, we present each of the four hypotheses and describe the scales used in our questionnaires for the respective assessments.

a) Perceived Threat: The two hypotheses pertaining to the effect of our participants' threat perception are:

H_{PT-1}: *Our awareness intervention significantly increases people's security and privacy threat perception in the context of smart home.*

H_{PT-2}: *Our awareness intervention increases people's security and privacy threat perception in the context of smart home significantly higher than interventions available on the Internet.*

We investigated the effect on *perceived threat* using the scales from the Technology Threat Avoidance Theory (TTAT) by Liang & Xue [34]. Their items for perceived threat were developed based on the substantial meaning [42]. We adapted the items from Liang & Xue used in [34]. The adaptation was necessary to reflect the different context, i.e. from spyware to smart home security and privacy risks and refer to threats to user's security and privacy. Instead of the Likert scale we decided to use the Visual Analogue Scale (VAS). VAS is a continuous line displaying the labels ”strongly disagree” and ”strongly agree” at either end. The participants can select any value between the two ends of the line continuously on a range of one to 101. By using VAS we avoid the disadvantages of Likert scale, such as bias through response style or ordinal measurement data [47].

b) Privacy Attitude: The two hypotheses pertaining to the effect on our participants' privacy attitude are:

H_{PA-1}: *The awareness intervention has a significant effect on people's privacy attitude with respect to smart homes in terms of higher privacy concerns.*

H_{PA-2}: *The awareness intervention has a significantly higher effect on people's privacy attitude with respect to smart homes in terms of higher privacy concerns than interventions available on the Internet.*

Our items to measure participants' *privacy attitude* are based on those proposed by Dienlin & Trepte [16] who used them to investigate online privacy behaviour in the context of social networks. They developed the items based on the guidelines of the Theory of Planned Behaviour (TPB) [20]. They use six different semantic differentials which are either bi-dimensional (e.g. bad vs. good) or uni-dimensional (e.g. worrying vs. not worrying). The statement preceding the differentials were adapted to the context of our study. Analogously to perceived threat, VAS were used here, too (i.e., from ”very bad”=1 to ”very good”=101).

2) RQ-2 — Motivation to Use Protective Measures: The second aspect we aim to investigate in our study is the participants' motivation to use protective measures. The research question guiding this investigation is:

RQ-2: ***Does our intervention have an effect on individuals' motivation to use protective measures to reduce privacy and security risks in the smart home context?***

To our knowledge the available research does not allow formulating directed hypotheses with respect to RQ-2. Thus, its investigation is explorative in nature. To answer RQ-2, we measured our participants avoidance motivation, willingness to pay for protective measures, and time commitment for configuring protective measures. We investigate the effect on *avoidance motivation* using the scale from the TTAT suggested by Liang & Xue [34] which was also adapted to the context of our study. Their items were derived from behavioural intention measures by Davis et al. [13], [14]. To measure *willingness to pay for protective measures*, we simply asked participants to state the maximum amount of money they would spend on protective measures. Participants could specify the amount of money in Euros by typing it in a given text box. Similar questions were stated in [9], [21] to measure willingness to pay. We assessed user's *time commitment for configuring the protective measure* by asking the maximum amount of time they would take for configuration. Participants got a text box to specify the amount of time.

B. Study Design

We used a within-subject study design to measure the effect of our intervention as well as a between-subject study design to compare our intervention with the baseline group. An online survey was conducted. The survey was implemented in SoSci Survey and conducted in Germany. The interventions as well as the questions were provided in German. In particular, the scales from the literature were translated to German using the back-translation technique. The procedure of the study is described in the following paragraphs.

Phase 1: Participants were first shown some information about the study and asked to consent to participate in the study and the processing of their data (see Section III-D for more details). Then, they were asked about their experience with smart home devices and their motivation to use them.

Phase 2: Participants were asked to answer a number of questions on perceived threat, privacy attitudes, avoidance motivation, willingness to pay and time commitment for configuration of protective measures. These are the items introduced in the previous subsection.

Phase 3: Participants were assigned to either the study group or the baseline group at random. The baseline group had access to a simulated Google search result (see Section III-C for more details). Since the search results presented to the baseline group also contained descriptions of the term smart home and mentioned advantages of smart homes, we added to our intervention a short description about smart homes and their advantages for the study group participants as well. Both groups were instructed to inform themselves about advantages and disadvantages regarding smart homes. Note, we used this more neutral wording in an attempt to minimize the bias towards only disadvantages and not prime the participants unnecessarily. Both participant groups were able to read the provided information as long as they wanted; but had to do so for a minimum for four minutes before they could advance to the next phase of the study. This was implemented to increase the likelihood that they take their time. The four minutes were based on a pre-study in which we asked people to read the text very carefully and the minimum time taken in this pre-study was four minutes. We implemented one more check: Participants of the baseline group had to click on at least one of the search results before being allowed to proceed. Such a restriction was not necessary for the study group, as there was only one intervention.

Phase 4: The participants had to answer the same questions as during phase two again. This phase also contained two attention check questions to filter out participants who did not read the instructions carefully.

Phase 5: The survey concluded with questions on participants' demographics. Last but not least, we thanked participants for their participation.

C. Baseline Group

Participants in the baseline group were shown the top ten Google search results based on the search term "smart home / IoT security and privacy risks". We decided to provide the top ten results, as research on browsing behaviour shows that attention and click rates sharply drop after the tenth result, which is the number of results Google presents on the first page [25], [28]. Participants saw a simulated search overview in the survey, recreating the look and feel of a real Google search. They were able to choose and read the individual search results by clicking on them in the search overview. After reading the content of the website they could return to the search overview at any time and choose another one of the search results. To decrease the ordering bias, the order of the search results in the overview was randomised for each participant.

D. Recruiting and Ethics

Participants were recruited from the Clickworker panel which is a crowdsourcing platform similar to Amazon Mechanical Turk, geared towards German speaking individuals [15]. Based on our pre-studies, we determined the duration of answering the survey to be 16 minutes. The minimum wage in Germany at the time of the study was 9.50 Euros per hour. Thus, participant's received 2.60 Euros for finishing the survey.

All ethical requirements defined by our university's ethics committee for research with human participants were met. In particular, on the first page of the survey, participants received a informed consent by revealing the study's purpose and data processing. For any doubts or questions regarding the study, contact information of the researchers were given in the survey. Participants had the option to withdraw from the study at any point without providing any reason by closing the tab of their browser with the survey. They were also instructed that by cancelling the survey, all data collected so far would be deleted. Participants were assured that their responses are stored in an anonymised form and would only be used for study purposes. In the beginning, participants were also explicitly advised that the survey contains attention questions.

E. Analysis of the Results

To assess the effect of the intervention, the aforementioned scales were measured twice, i.e. before and after the intervention. Therefore, we conducted a repeated measures ANOVA for each scale. Furthermore, the effect sizes proposed by Morris and DeShon [38], [39] were calculated for each of the scales in the repeated ANOVA. Cohen [12] suggested to categorize an effect as medium for $d \geq 0.5$ and as large for $d \geq 0.8$. To compare our intervention with the intervention in the baseline group we looked at statistical differences of these measurements. We used a mixed design ANOVA adding the type of the intervention as the between-subject factor.

IV. Results

Overall, 159 participants completed the survey and passed the attention questions. 28 of them were excluded due to giving answers which were identified as outliers deviating more than 1.5-times the interquartile range from the mean. An overview of the demographics of the remaining 131 participants can be found in Tab. I. The remainder of this section presents the results of our study along our two research questions.

TABLE I: Participant demographics.

		All		**Baseline Group**		**Study Group**	
Age		N	%	N	%	N	%
	<20	2	1.5	2	3.0	0	0.0
	20-25	27	20.6	17	25.8	12	17.4
	26-35	50	38.2	20	30.3	30	43.5
	36-45	27	20.6	16	24.2	11	15.9
	46-55	14	10.7	5	7.6	9	13.0
	56-65	10	7.6	6	9.1	4	5.8
	>65	1	0.8	0	0.0	1	1.4
Gender		N	%	N	%	N	%
	m	78	59.5	39	59.1	39	56.5
	w	62	39.7	25	37.9	27	39.1
	n/a	1	0.8	0	0.0	1	1.4
Smart home device owner		N	%	N	%	N	%
	yes	78	59.5	36	56.3	42	62.7
	no	53	40.5	28	43.7	25	37.3
IT expertise	Average	1.641		1.554		1.724	
	SD	3.985		3.308		4.537	

A. *RQ-1 – Raising Risk Perception*

In order to determine the effect of our awareness intervention on people's risk perception, we measured the participants' perceived threat (to evaluate H_{PT-1} and H_{PT-2}) and privacy attitude (to evaluate H_{PA-1} and H_{PA-2}).

With respect to H_{PT-1} and H_{PA-1}, both scales exhibit better scores after reading the intervention, i.e., increase for perceived threat and decrease for privacy attitude. Perceived threat being initially at 45.2 on the range of 1 to 101 increased by 61% to 72.9. Privacy attitude was initially at 52.7 on the same range and decreased by 31% to 36.5. ANOVA tests showed that reading our intervention led to a significant effect on both, perceived threat ($F(1) = 78.2$, $p = .001$) and privacy attitude ($F(1) = 57.5$, $p = .001$). The effect sizes pertaining to the scales were d = 1.103 (large) and d = -0.948 (large) respectively. Privacy attitude shows a negative effect size as the rating score decreases when the privacy concerns increase. Thus, we accept H_{PT-1} and H_{PA-1}.

Furthermore, we looked at the differences in our participants' perceived threat and privacy attitude between the group reading our intervention and the baseline group. Overall, the effect of the simulated Internet search in the baseline group was less than the effect evoked by our intervention. ANOVA tests showed that the differences were significant for both scales: perceived threat ($F(1) = 4.7$, $p = .033$) and privacy attitude ($F(1) = 9.7$, $p = .002$). Thus, the improvement in perceived threat and privacy attitude is significantly higher for our intervention and we accept H_{PT-2} and H_{PA-2}.

B. *RQ-2 – Motivation to Use Protective Measures*

To investigate the effect on people's motivation to use protective measures, we measured our participants' avoidance motivation, willingness to pay, and time commitment for configuration before and after the intervention. All three scales exhibit better scores after reading the intervention. Avoidance motivation started at 53.4 on a range of 1 to 101 and increased by 24% to 66.2. Willingness to pay for protective measures was at 70,2 Euros and increased by 41% to 99 Euros. Time commitment for configuring protective measures being at 56 minutes increased by 33% to 74.4 minutes. Reading our intervention lead to a significant effect on avoidance motivation ($F(1) = 27.7$, $p = .001$), user's willingness to pay ($F(1) = 21.8$, $p = .001$), and time commitment for configuring protective measures ($F(1) = 21.7, p = .001$). The effect sizes pertaining to the scales were d = 0.648 (medium), d = 0.666 (medium), and d = 0.628 (medium) respectively.

The effect on avoidance motivation, willingness to pay and time commitment for configuration was not significantly different between our intervention and the baseline group. Similar to our intervention, the effect sizes in the baseline group were medium, too.

V. Discussion

In this section we discuss our study's results, limitations and future work as well as related work.

A. *Effectiveness of the Intervention*

Two research questions guided our evaluation of the interventions effectiveness. In the following, we discuss the results and implications pertaining to each of them.

1) RQ-1 — Raising Risk Perception: To investigate the effectiveness of our intervention with respect to raising people's risk perception, we investigated the intervention's effect on the participants' *perceived threat* and their *privacy attitude*. Our intervention seemed to evoke a significant increase in perceived threat with a large effect size of $d = 1.103$. According to the TTAT by Liang & Xue [33], perceived threat is determined by the perceived severity and probability of risks. Thus, we can confirm that following the guidelines in Section II-A2 for increasing both of these factors was effective and our results support these earlier findings. Furthermore, the increase in threat perception was significantly higher for our intervention than in the baseline group, implying an advantage in terms of evoking threat perception for systematically created interventions over freely available information on the Internet.

Our intervention also changed people's privacy attitudes towards higher privacy concerns significantly. The increase was significantly higher compared to the baseline group, which will be also reflected by the effect sizes with d = -0.948 for our intervention and d = -0.466 for the baseline intervention. Furthermore, according to Dienlin & Trepte, with an increase in privacy attitude we can expect to have a positive effect on people's privacy behaviour.

2) RQ-2 — Motivation to Use Protective Measures: The TTAT explains that when people perceive threat they subsequently adopt coping behaviour to avoid the threat. Thus, with an increase in perceived threat avoidance motivation should increase as well. We can confirm this relationship with our measurements for the smart home context. Avoidance motivation shows a significant increase after the intervention. Also willingness to pay for protective measures and the time commitment for configuring protective measures increased significantly after the intervention. Hence, we argue that with interventions based on the findings in the literature as well as feedback from experts and lay users, it is possible to foster security and privacy protective behaviour.

Yet, the effect sizes are not as high as for the perceived threat. The effect size of avoidance motivation is just slightly higher for our intervention than for the baseline group. Also, while the the group which read through our intervention shows a higher increase in threat perception than the baseline group, there is no significant difference in avoidance motivation between the two. One possible explanation might be the convex relationship between threat perception and avoidance motivation reported in [33]. After an initial stark increase, any additional increase in threat perception causes a lower growth rate in avoidance motivation. It is possible that the threat level of the baseline group reached a point where a significant increase in threat perception with a large effect does not cause a significant increase in avoidance motivation anymore.

Additionally, TTAT describes that aside from threat perception, threat avoidability has a positive influence on avoidance motivation (which is in turn moderated by perceived threat) [32], [33]. However, since our study did not include avoidability as a construct, we cannot draw definite conclusions and further studies to investigate this aspect are needed.

The set of factors which influence privacy protective behaviour is very diverse and complex. Acquisti et al. [3] demonstrate that both psychological and economic factors influence people's desire and ability to protect their privacy. While the details of these factors are beyond the scope of this paper, it is important to note that through providing the intervention, we are addressing some of the psychological factors, e.g. information asymmetries, intangibility of the risks, or illusory control. However, other psychological factors, e.g., herding, adaptation, or bounded rationality remain unaddressed.

B. Limitations and Future Work

The study has some limitations which should be considered when interpreting the results. The intervention was evaluated with participants from Germany. People with different cultural backgrounds show differences in the level of security and privacy awareness in the smart home context [31]. Therefore, it would be helpful to investigate the cultural differences' impact on the intervention's effectiveness and adapt it, if necessary.

Participants of the study were recruited from the Clickworker panel. Considering previous studies on crowdwork [17], [26], our sample might be biased with respect to participants' age, educational background, and technical experience.

For the selection of the top ten results participants were given in the baseline group, we used a clean browser to avoid bias. However, it must be acknowledged that variations in search engines, search terms, and search results can affect the results of our study. However, we argue that using the search results obtained in a clean browser on Google – the search engine with the biggest market share – represents the best approximation of what an average person might find.

We consider our participants' intention regarding their willingness to pay and their time commitment. It was too challenging to run a field experiment to measure actual behaviour, in particular during the current pandemic. Therefore, the online survey design was the only viable option to us.

The next challenge in future work is to reach people with the intervention. Potential means to distribute the intervention could be media entities, agencies, organisations, and schools. Also the manufacturers of smart home devices can use the intervention to explain how they reduce these risks. Text-based materials are helpful for providing details in a structured way and allow distribution either in digital or print form. However, when informing end-users, adaptation of the content into other formats such as a video or as interactive media might render it more fun and easier accessible [1].

In our study we measured the effect of the intervention directly after reading it. We do not know the long-term effects of the intervention. Thus, it might prove worthwhile to investigate the intervention's effectiveness after some months.

C. Related Work

A wide variety of research aims at making people aware of privacy risks pertaining to the smart home devices they have in place by analysing, visualising, or interpreting information flows, e.g., [36], [40], [43]. But they do not provide educational material which explains risks and consequences of privacy exposure. Another line of research proposes to introduce security and privacy labels for IoT products [18], [37]. This information might be more helpful during the buying decision, but does not outline potential consequences.

Williams et al. [52] investigated a game for smart watches to encourage privacy-protective behaviour of smart watch users. The authors suggested to provide more information, as not all participants adjusted their behaviour and complained about being insufficiently informed. Plachkinova & Menard [41] examined smart home security awareness videos. Our study is focused on a text-based awareness intervention maintaining a high information density for in depth learning.

VI. Conclusion

We systematically developed a novel security and privacy awareness intervention to raise people's risk perception for security and privacy risks in the smart home context. Two pillars support the intervention: firstly, the existing research literature, and secondly, feedback from lay users and experts. We evaluated the effectiveness of our intervention in an online study. Reading through the intervention significantly increased participant's risk perception and willingness to use protective measures. In comparison to a simulated Internet search on the topic, the effect of the intervention on risk perception was significantly higher. Based on previous research, e.g., by Dienlin & Trepte [16], it is reasonable to assume that this effect positively impacts actual privacy behavior. Furthermore, we can confirm the TTAT [33] in the smart home context, since our study shows that an increase in perceived threat also causes an increase in avoidance motivation. Based on these findings, our intervention contributes to making the complexity of smart homes and the associated risks tangible even for lay people.

REFERENCES

[1] J. Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, 2014.

[2] M. Abomhara and G.M. Køien. Security and privacy in the internet of things: Current status and open issues. In *PRISMS*, pages 1–8, 2014.

[3] A. Acquisti, L. Brandimarte, and G. Loewenstein. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758, 2020.

[4] A. Aktypi, J.R.C. Nurse, and M. Goldsmith. Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the MPS 2017*, pages 1–11. ACM, 2017.

[5] M.R. Alam, M.B.I. Reaz, and M.A.M. Ali. A review of smart homes—past, present, and future. *IEEE transactions on systems, man, and cybernetics, part C*, 42(6):1190–1203, 2012.

[6] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[7] D. Bastos, M. Shackleton, and F. El-Moussa. Internet of things: A survey of technologies and security risks in smart home and city environments. In *Living in the Internet of Things: Cybersecurity of the IoT-2018*, pages 1–7. IET, 2018.

[8] V.M. Bier. On the state of the art: risk communication to the public. *Reliability engineering & system safety*, 71(2):139–150, 2001.

[9] J.M. Blythe, S.D. Johnson, and M. Manning. What is security worth to consumers? investigating willingness to pay for secure internet of things devices. *Crime Science*, 9(1):1, 2020.

[10] N. Buescher, S. Boukoros, S. Bauregger, and S. Katzenbeisser. Two is not enough: Privacy assessment of aggregation schemes in smart metering. *PoPETs*, 2017(4):198–214, 2017.

[11] L.J. Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3):37–46, 2009.

[12] J. Cohen. *Statistical power analysis for the behavioral sciences*. Academic press, 2013.

[13] F.D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[14] F.D. Davis, R.P. Bagozzi, and P.R. Warshaw. User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8):982–1003, 1989.

[15] X.N. Deng, R. D. Galliers, and K.D. Joshi. Crowdworking-a new digital divide? is design and research implications. In *ECIS*, 2016.

[16] T. Dienlin and S. Trepte. Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 45(3):285–297, 2015.

[17] X. Duan, C. Ho, and M. Yin. Does exposure to diverse perspectives mitigate biases in crowdwork? an explorative study. In *HCOMP 2020*, volume 8, pages 155–158, 2020.

[18] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L.F. Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI*, pages 1–12, 2019.

[19] E. Fernandes, J. Jung, and A. Prakash. Security analysis of emerging smart home applications. In *IEEE SP 2016*, pages 636–654. IEEE, 2016.

[20] M. Fishbein and I. Ajzen. *Predicting and changing behavior: The reasoned action approach.* Psychology Press, 2010.

[21] C.S. Fuller. Is the market for digital privacy a failure? *Public Choice*, 180(3):353–381, 2019.

[22] V. Garg and J. Camp. End user perception of online risk under uncertainty. In *HICSS 2012*, pages 3278–3287. IEEE, 2012.

[23] N. Gerber, B. Reinheimer, and M. Volkamer. Home sweet home? investigating users' awareness of smart home privacy threats. In *WSSP*, 2018.

[24] N. Gerber, B. Reinheimer, and M. Volkamer. Investigating people's privacy risk perception. *PoPETs*, 2019(3):267–288, 2019.

[25] L.A. Granka, T. Joachims, and G. Gay. Eye-tracking analysis of user behavior in www search. In *ACM SIGIR*, pages 478–479, 2004.

[26] T. Görzen. Can experience be trusted? investigating the effect of experience on decision biases in crowdworking platforms. In *HICSS*, pages 4385–4394, 2019.

[27] M. Harbach, S. Fahl, and M. Smith. Who's afraid of which bad wolf? a survey of it security risk awareness. In *CSF*, pages 97–110, 2014.

[28] J. Jiang, D. He, and J. Allan. Searching, browsing, and clicking in a search session: Changes in user behavior by task and over time. In *ACM SIGIR*, pages 607–616, 2014.

[29] S. Karwatzki, M. Trenz, V.K. Tuunainen, and D. Veit. Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, 26(6):688–715, 2017.

[30] J.E. Klobas, T. McGill, and X. Wang. How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security*, 87:101571, 2019.

[31] O. Kulyk, B. Reinheimer, L. Aldag, P. Mayer, N. Gerber, and M. Volkamer. Security and privacy awareness in smart environments–a cross-country investigation. In *FC20*, pages 84–101. Springer, 2020.

[32] R.S. Lazarus and S. Folkman. Stress, coping and adaptation, 1984.

[33] H. Liang and Y. Xue. Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, pages 71–90, 2009.

[34] H. Liang, Y.L. Xue, et al. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, 11(7):1, 2010.

[35] N. Liberman, Y. Trope, and C. Wakslak. Construal level theory and consumer behavior. *JSP*, 17(2):113–117, 2007.

[36] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, and S. Tarkoma. Iot sentinel: Automated device-type identification for security enforcement in iot. In *IEEE ICDCS*, pages 2177–2184, 2017.

[37] P. Morgner, C. Mai, N. Koschate-Fischer, F. Freiling, and Z. Benenson. Security update labels: Establishing economic incentives for security patching of iot consumer products. In *SP'20*, pages 429–446, 2020.

[38] S.B. Morris. Estimating effect sizes from pretest-posttest-control group designs. *Organizational research methods*, 11(2):364–386, 2008.

[39] S.B. Morris and R.P. DeShon. Combining effect size estimates in meta-analysis with repeated measures and independent-groups designs. *Psychological methods*, 7(1):105, 2002.

[40] T.J. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi. Homesnitch: behavior transparency and control for smart home iot devices. In *12th Conference on WISEC*, pages 128–138, 2019.

[41] M. Plachkinova and P. Menard. An examination of gain-and loss-framed messaging on smart home security training programs. *Information Systems Frontiers*, pages 1–22, 2019.

[42] I.M. Rosenstock. The health belief model and preventive health behavior. *Health education monographs*, 2(4):354–386, 1974.

[43] W. Seymour, M.J. Kraemer, R. Binns, and M. Van Kleek. Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the 2020 CHI*, pages 1–14, 2020.

[44] V. Sivaraman, H.H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. Network-level security and privacy control for smart-home iot devices. In *11th WiMob*, pages 163–167. IEEE, 2015.

[45] J. Staddon, D. Huffaker, L. Brown, and A. Sedley. Are privacy concerns a turn-off? engagement and privacy in social networks. In *SOUPS*, pages 1–13, 2012.

[46] Statista. Forecast market size of the global smart home market from 2016 to 2022 (in billion u.s. dollars), 2020. from https://www.statista.com/statistics/682204/global-smart-home-market-size/, Accessed: 2021-04-14.

[47] Y.-T. Sung and J.-S. Wu. The visual analogue scale for rating, ranking and paired-comparison (vas-rrp): a new technique for psychological measurement. *Behavior research methods*, 50(4):1694–1715, 2018.

[48] M. Tabassum, T. Kosinski, and H.R. Lipford. " i don't own the data": End user perceptions of smart home device data practices and risks. In *SOUPS*, 2019.

[49] Y. Trope and N. Liberman. Temporal construal. *Psychological review*, 110(3):403, 2003.

[50] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev. Risk perceptions of cyber-security and precautionary behaviour. *CHB*, 75:547–559, 2017.

[51] P. Wiedemann, H. Schutz, and M. Clauberg. Lessons learned: Avoiding pitfalls in risk communication. In *International Conference and COST 281 Workshop on Emerging EMF Technologies, Potential Sensitive Groups and Health*, 2006.

[52] M. Williams, J.R.C. Nurse, and S. Creese. (smart) watch out! encouraging privacy-protective behavior through interactive games. *International Journal of Human-Computer Studies*, 132:121–137, 2019.

[53] P. Worthy, B. Matthews, and S. Viller. Trust me: doubts and concerns living with the internet of things. In *ACM DIS*, pages 427–434, 2016.

[54] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *SOUPS*, pages 65–80, 2017.

[55] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home iot privacy. *HCI CSCW*, 2(CSCW):1–20, 2018.