“Where did you first meet the owner?” – Exploring Usable Authentication for Smart Home Visitors

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

Sarah Delgado Rodriguez
University of the Bundeswehr Munich
Munich, Germany
sarah.delgado@unibw.de

Timo Döding
LMU Munich
Munich, Germany
timo.doeding@googlemail.com

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

Figure 1: In this paper, we explore design challenges for usable authentication for visitor scenarios in smart homes. In particular, visitors can have varying relations and visit at varying frequency; the smart home environment may provide various functionalities and comprise the presence of bystanders; and authentication can be designed in various ways with regards to timing and responsibility for authenticating, and the concrete mechanism (authentication factor and modality).

ABSTRACT

Visitors in smart homes might want to use certain device features, as far as permitted by the device owner (e.g., streaming music on a smart speaker). At the same time, protecting access to features from attackers is crucial, motivating a need for authentication. However, it is unclear if and how smart home visitors should authenticate as they usually do not have access to respective interfaces. We explore considerations for the design of authentication for visitors evolving around, e.g., the visitors themselves as well as the environment and concrete mechanisms. Moreover, we suggest a concrete idea: *security questions* to authenticate visitors in smart homes. In an interview study ($N = 24$), we found that owners and visitors appreciated the low effort and would adapt our approach. We conclude with future research directions that we hope will spark further discussions around the design of authentication for smart homes, considering visitors and owners alike.

CCS CONCEPTS

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

CHI '22 Extended Abstracts, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9156-6/22/04…$15.00
https://doi.org/10.1145/3491101.3519777

KEYWORDS

smart homes, smart devices, usable security, authentication, security questions, visitors

ACM Reference Format:
Sarah Prange, Sarah Delgado Rodriguez, Timo Döding, and Florian Alt. 2022. “Where did you first meet the owner?” – Exploring Usable Authentication for Smart Home Visitors. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3491101.3519777

1 INTRODUCTION

Smart homes are on the rise with an increasing number of devices being available on the worldwide market. These devices foster a variety of features with great benefits for users such as, e.g., home automation or sustainable energy consumption (cf. [23] for an overview). At the same time, these devices are vulnerable to novel attacks and threats [39], coming from within or outside the home [13]. To mitigate these, employing authentication on such devices is crucial [2, 14, 28, 39].

However, existing mechanisms on smart home devices oftentimes follow conventional metaphors [13] and, hence, do not suit the device and purpose. Think about, e.g., entering secure passwords that should be long and contain special characters on a smart TV's remote control. The result is low usability and user experience [7, 8], and, as a consequence, mechanisms being rarely used albeit being necessary to protect the home. Moreover, such mechanisms mainly target those who are the main users, i.e. have access to related device interfaces and accounts with associated services.

However, device owners might want to provide access to certain devices and features to other stakeholders such as visitors [1, 22, 24, 37]. For instance, primary users might allow others to employ short-term changes to, e.g., temperature, but keep exclusive rights for automation rules (e.g., regulating temperature over night). Another example are features that require a (paid) user account such as, e.g., streaming music. To allow visitors to use these features, either on the owners' or even their own accounts, they need to authenticate. At the same time, they might not have access to the device's configuration interfaces and should not interfere with the device owners' access rights and configurations.

In this work, we explore challenges for the design of usable authentication for smart home visitors, evolving around the visitors themselves, the smart home environment, and opportunities for authentication (cf. Figure 1). Moreover, we present one concrete idea as an example, that is the use of *security questions* to authenticate smart home visitors. Questions could cover, e.g., the relationship to the owner, and could be employed as voice interface via, e.g., a smart speaker to be accessible for visitors. We assessed the perception of both, smart home owners and visitors, towards this approach in an exploratory interview study. We used a Wizard-of-Oz voice interface to simulate the authentication procedure. We found that participants in both roles appreciated the idea and found the mechanism easy to use. However, they also raised a potential for attacks towards the mechanism and our sample questions. We suggest to mitigate these by employing personalized or dynamic security questions for visitor authentication.

Based on our exploration, we discuss possible directions for future work. We hope our work to stimulate further discussions and research around authentication in smart homes that (also) targets visitor scenarios.

2 BACKGROUND & RELATED WORK

Smart homes are typically multi-device, but also multi-user environments. Devices are naturally shared [38] among owners and other inhabitants, but also *visitors* [13]. Visitors are users who do not live in the smart home (hence, are not the owners of the devices), but might be present in the environment and potentially interact with the devices [1, 9, 22, 24, 37]. Examples include, but are not limited to, remote living family members and friends, but also (foreign) subtenants or maintenance workers. While some features should be made accessible to them [13, 38], they should not have access to sensitive features [9, 19] or be able to change configurations [16]. As such, suitable access control, authentication mechanisms or guest modes are required [13, 38]. However, only few consumer smart home systems allow to actually define different user roles and the manual configuration of guest access is burdensome for users [22].

Smart Home Authentication. As smart home devices are prone to novel attacks and threats [39], from within or outside the smart home [13], employing authentication is indispensable [2, 14, 28, 39]. Authentication for smart homes should consider the various roles and relationships [13, 35] and be seamlessly integrated [15]. For instance, authentication for voice assistants should be natural, unobtrusive, and adapt to the context (e.g., presence of bystanders) [28]. Examples include identifying users based on biometrics (e.g., gait [25] or voice [28]), touch sensing on devices [20], network traffic [27], or WiFi signals [34].

Security Questions. Security questions are a popular means for fallback authentication [3, 5, 10, 18, 32]. Typically, questions are fixed (by the provider), open (freely chosen by users), or a mix of both [17] and often come into play once users loose access to their primary credentials. However, questions are often chosen poorly [32], hence, can easily be forgotten or guessed [33], and many chosen questions have low entropy answers [18]. Moreover, users often provide fake answers to mitigate guessing, which in turn compromises memorability and security as it decreases the distribution of answers [5]. One approach to mitigate this is to base security questions on personal (potentially changing) information. These *dynamic security questions* are easy for users, while being harder to guess for attackers [3, 12]. Questions can, e.g., be based on personal internet activities [3], on personal daily memory captured through users' smartphones [10], or on device usage behavior (e.g., app usage or calls) [12]. However, questions need to address a trade-off between usability and security [12] as the most secure questions come with worst memorability [5]. Questions based on shared knowledge among friends can increase usability while being hard to guess for strangers [36]. Lastly, asking multiple questions can increase security [18] and accuracy [12].

Summary. The design of usable authentication mechanisms poses a challenge in multi-user, multi-device smart home contexts (cf. [29]). While visitors have been recognized as potential attackers [22, 28], it is unclear if and how legitimate visitors should authenticate to access features that device owners permitted to them. In this late-breaking work, we discuss challenges for the design of visitor authentication based on related work, and present one concrete sample idea. In particular, we make use of *security questions*, that usually serve as a fallback mechanism for primary users to reclaim access to their own accounts. In our scenario, we take this approach to a conversation between smart home owner, visitor, and authentication mechanism (employed, e.g., on a voice assistant). By answering a number of questions that cover, e.g., aspects of their relationship, visitors can authenticate to access device features as permitted by the owner.

3 DESIGN CHALLENGES

Based on related work, we derive and discuss challenges for the design of authentication for visitors in smart homes.

3.1 Visitor Types

Visitors in smart home scenarios can be characterized by the following attributes:

3.1.1 Relation to Owner. The relation between visitors and device owners is crucial when it comes to privacy decisions in smart home environments [24, 30]. Similarly, this aspect also comes into play when owners decide which features should be accessible for visitors [13]. The relation might range from *very close* visitors (e.g., family members who live in different households) to *strangers* (e.g.,

subtenants or maintenance workers), and fluently cover any type of relation in between.

3.1.2 Visit Frequency. To assess authentication overhead, the usage frequency of a smart home device needs to be considered [29]. Similarly, the frequency in which a visitor is present in the respective smart home is an interesting aspect. This may range from one time visits to very frequent visits every other day.

3.2 Environment & Setting

Other interesting aspects are the devices' functionalities, as well as the presence of one or both, owner and visitor.

3.2.1 Access to Functionality. Smart devices' functionalities can be grouped in different categories [16], which can serve as a basis to define access permissions [13, 38]. Moreover, visitors should generally have limited access to devices and only be able to access functionalities while they are physically present in the home [13, 22, 38]. We suggest that, depending on owners' preferences and specific capabilities, visitors should (not) be able to authenticate for using the respective feature:

- **basic:** For basic features, *authentication is not necessary*. This particularly holds true for functionalities that can be acquired through physical switches [13, 16, 38] and by anybody in physical vicinity of the respective controls such as, e.g., turning on lights or opening jalousies.
- **restricted:** For other features, owners might want to make them available for visitors, but *authentication is necessary*. For instance, visitors might be allowed to play music on the owners' smart speaker, but would need to authenticate (potentially with their own streaming account) first.
- **forbidden:** Lastly, some functionality might not be accessible for visitors and, hence, *authentication is not possible* for visitors. Examples include, but are not limited to, changing automation rules or security settings in the home [13, 16].

3.2.2 Presence. The scenarios might differ in terms of who is currently present in the smart home. First and foremost, *both*, owner and visitor, could be present when it comes to using the owners' device features (e.g., visiting a friend and watching a movie on the smart TV). However, it might also be that *owners only* are present, in case they provide remote access to certain visitors (e.g., friends who can access files on a shared file system in the home network). Moreover, it could be the case that *visitors only* are present (e.g., tourists in a rental apartment who aim to use smart devices in place), which potentially means to (temporarily) restrict owners' access to protect visitors' privacy [22]. Lastly, the presence of bystanders, e.g. visitors who are not the one currently authenticating, is an interesting aspect [28]. For instance, they might observe or eavesdrop the authentication procedure which puts a risk on both, owner and visitor.

3.3 Authentication Mode

The authentication mechanism itself could be implemented in various ways. We discuss some considerations below.

3.3.1 Timing. Prior work suggests that smart home authentication could be employed before, during, or after a main task or device use [29]. In line with this suggestion, visitors could authenticate *before* they actually use any feature within the smart home (e.g., directly upon arrival), *during* their visit (e.g., upon first use of any device or at a specified time), or *after* their visit (e.g., in case visitors placed an order or changed crucial settings, to verify if these should persist and on which account).

3.3.2 Responsibility. Another interesting question is who is responsible to trigger the actual authentication procedure. For instance, the *visitor* could *actively request* a specific device functionality or feature and, hence, authentication would be initiated. Another option would be that the *owner asks visitors* to authenticate. Lastly, the *smart home* could initiate the authentication procedure *automatically*, e.g. at specific times (based on, e.g., a calendar entry indicating guests in the home) or when recognizing non-inhabitants being present (based on, e.g., new personal devices such as smartphones being in range of the smart home network).

3.3.3 Factor. Authentication can be based on one (or a combination) of three main factors: knowledge, token, or biometrics [26]. A *biometric* mechanism, while being convenient and effortless, would require visitors to share biometric data with the device owner and/or potentially unknown devices and providers, which might be undesirable [29]. Looking at *token* based authentication, the question arises as to who would be responsible to provide and carry these tokens (i.e., owners or visitors themselves), and when these would be handed out (e.g., upon first visit). *Knowledge-based* mechanisms, as being highly familiar to users and still widely applied, could be easily implemented for visitors as well. For instance, they could set a personal password or PIN for their visit.

3.3.4 Modality. Lastly, it should be considered that visitors might not have access to devices' configuration and/or authentication interfaces, especially if these are available in companion applications only. As a result, visitors who need to authenticate in a foreign smart home should be able to do so via, e.g., *the device itself* or *their personal devices*.

4 IDEA: SECURITY QUESTIONS FOR VISITOR AUTHENTICATION

In the following, we present and discuss one concrete idea to authenticate (also) visitors in smart homes: using *security questions*. Such a mechanism would put a number of questions to both, owner and visitor. In our setting, owners would then accept or deny the visitor's answer rather than the system verifying answers automatically. Questions should be designed in such a way that they are easy to remember for users, but hard to guess for attackers [12]. For instance, questions could cover aspects of the relationship between owner and visitor (e.g., *"Where did you first meet?"*). To make the mechanism accessible for visitors, it could be employed as voice interface (e.g., on a smart speaker [31]) and, hence, be included in a conversation between the two.

4.1 Exploration Study

To assess users' general opinion towards this idea in a smart home context, we conducted interviews with pairs of owners and visitors using a Wizard-of-Oz voice interface for the questions.

Table 1: Sample Smart Home Functionalities: We chose a set of functionalities with basic, restricted (using their own accounts), and forbidden visitor access.

Visitor Access	Sample Functionalities
basic (no authentication necessary)	turning smart lights on/off opening/closing smart jalousies setting a temperature on the smart heating
restricted (visitor authentication necessary)	streaming music on the smart speaker streaming a movie on the smart TV personalized coffee (smart coffee machine)
forbidden (visitor authentication not possible)	obtaining admin rights accessing the history of voice commands setting routines (e.g., shutters up when sun rises)

Table 2: Sample Security Questions: We chose a set of easy, medium, and hard questions. Note that questions address the visitor while referring to the owner of the smart home.

Question Category	Sample Security Questions
easy	When did the both of you first meet? In which city did the both of you meet the first time? Which hobby do you have in common?
medium	What binds you two together? How many smart home devices do you own together? What was your first activity together?
hard	Where did you meet last time? Which restaurant have you visited most together? What was the furthest place you have been to together?

4.1.1 *Apparatus.*

Wizard-of-Oz Interface. To support our interviews, we built an interface with basic text-to-speech features, to simulate interaction with a voice interface for participants. Using the Web Speech API[1], the experimenter could generate voice output for the security questions and responses by manually reacting to participants' answers. Participants only heard the audio output while not seeing or directly interacting with the actual (click) interface.

Functionalities & Questions. We chose various sample functionalities to cover *basic* (e.g., lights on), *restricted* (e.g., play music via own streaming account), and *forbidden* (e.g., configuring routines) visitor access (cf. Section 3.2.1 and Table 1). Moreover, we choose a set of 9 security questions in three different categories (3 each, see Table 2 for sample questions): easy (covering basic facts about the relationship), medium (more in depth questions with rarely changing answers), and hard (about ongoing activities with answers potentially changing frequently).

4.1.2 *Study Design.*

We conducted a within-subjects study with two independent variables, FUNCTIONALITY (cf. Table 1) and QUESTION (cf. Table 2). We recruited pairs of visitor and owner. All participant pairs went through all sample FUNCTIONALITIES. We counterbalanced the order of visitors access (basic, restricted, and forbidden) and conducted three rounds per pair to cover all functionalities. For each functionality requiring authentication (restricted), participants had to go through three security QUESTIONS: one easy, medium, and hard in counterbalanced order. As such, every participant pair answered and assessed every security QUESTION.

4.1.3 *Procedure.*

After participants agreed to take part in the study, they were sent a consent form, information on the general procedure, instructions on the authentication mechanism, and a link for the Zoom meeting.

We started the actual session with assigning participant pairs to one owner and one visitor role. We then guided them through three rounds (to cover all functionalities and questions in counterbalanced order). After every round, participants filled in Likert scales on the perceived security and usability of the current security questions (see Table 3 for the items). We complemented the session with separate interviews with both participants (using Zoom's "Breakout Rooms"[2]) and questionnaires (including demographics, affinity for technology, and general privacy concerns) filled in separately. We gave both participants the option for questions and further feedback.

4.1.4 *Recruitment & Participants.*

We recruited a total of 24 participants (12 pairs) through university mailing lists and social media. Pairs of participants were required to know each other well while not living in the same household, as this is a common relation in smart home contexts [9]. At least one of the pair should own at least one smart home device (to take the role of the owner in our study). A session took around 60 minutes and they received online shopping vouchers at 10€ or study credits per person.

Participants were 18 to 35 years old ($Mean = 23$, $SD = 4.01$). 12 of them identified as female, others as male. Most of them were students ($N = 21$), 2 were full-time employees, and 1 was an apprentice. Participants were generally aware of privacy concerns as assessed through the 10-item IUIPC questionnaire [21]: they rated their wish for *Control* ($Mean = 6.01$, $SD = 1.24$), *Awareness* of data practices ($Mean = 6.56$, $SD = 0.90$), and *Collection* of personal data vs benefits ($Mean = 5.51$, $SD = 1.51$). Moreover, their affinity for technology was rather high following the ATI scale [11] (ranging from 1 to 6, overall: $Mean = 4.37$, $SD = 1.27$; owners: $Mean = 4.62$, $SD = 1.11$; visitors: $Mean = 4.13$, $SD = 1.36$). Most participants owned smart devices, mainly smart TVs (7 visitors, 9 owners), smart speakers (2 visitors, 6 owners) and smart lights (2 visitors, 4 owners). They also had experience with sharing their device with co-inhabitants ($N = 6$) and visitors ($N = 4$). However they did not employ authentication for visitors and/or shared their own accounts.

4.2 Results

We conducted 12 sessions with a total of 108 security questions (9 per session). The vast majority ($N = 101$) of questions was answered correctly, according to owners' approval. Also, both, visitors and owners, were generally positive towards our idea. The usability of our concept was assessed as good according to the system usability scale [4, 6] (overall: $Mean = 77.40$, $SD = 12.92$; owners: $Mean = 73.54$, $SD = 9.65$; visitors: $Mean = 81.25$, $SD = 14.52$).

4.2.1 *Perception of Mechanism and Questions.*

We assessed participants' opinion of our chosen security questions on 5-point Likert scales (5: strongly agree, see Table 3 and Figure 2 for an overview). In particular, it was acceptable for participants to say the answers loud (overall $Median = 5$ for all question categories) and that the system would collect the necessary data and process the answers

[1] https://developer.mozilla.org/en-US/docs/Web/API/Web_Speech_API/Using_the_Web_Speech_API, last accessed January 4, 2022

[2] https://support.zoom.us/hc/en-us/articles/206476093, last accessed January 4, 2022

Table 3: Study Results: Assessment of easy, medium and hard security questions on 5-point Likert items (5=strongly agree). In particular, we report the median (Md) and standard deviation (SD) for participants in the visitor (V) and owner (O) group.

	easy				medium				hard			
	Md (V)	SD (V)	Md (O)	SD (O)	Md (V)	SD (V)	Md (O)	SD (O)	Md (V)	SD (V)	Md (O)	SD (O)
It was acceptable for me to say the answer out loud.	5	1.43	5	0.35	5	1.26	5	0.62	4	1.31	5	0.53
It was acceptable for me that the system knows and collects my answer.	3	1.47	5	1.48	4	1.49	4	1.38	3	1.47	4	1.57
It was easy for me to answer the question.	5	1.13	5	1.48	4	1.46	5	1.49	3	1.49	5	1.29
Someone who knows *the visitor* can answer the question correctly.	2	1.39	4	1.26	2	1.55	3	1.47	2	1.38	3	1.37
Someone who knows *the owner* can answer the question correctly.	2	1.35	4	1.26	2	1.55	3	1.51	2	1.39	3	1.36
Someone who knows *both* can answer the question correctly.	4	0.87	5	0.85	4	1.14	4	1.16	3	1.06	4	1.07
A stranger can answer the question correctly.	1	0.86	1	0.92	1	0.76	1	0.93	1	0.68	1	0.66

(overall $Median = 4$ for easy and medium, $Median = 3$ for hard). Furthermore, it was perceived easy to answer the questions (overall $Median = 5$ for easy, $Median = 4$ for medium and hard). Regarding the authentication procedure, participants found it efficient and perceived low effort (5 visitors, 6 owners): *"I really like it, because it prevents strangers from accessing personal data"* (P1, visitor). Four owners particularly highlighted the categorization of functionalities as useful: *"I found it very thoughtful: (...) as soon as data is involved, authentication is required (...)"* (P8, owner).

4.2.2 Privacy & Security Concerns. In terms of potential attacks, participants agreed that known individuals (either to the owner, the visitor, or both) could answer the questions correctly (see Figure 2). However, they rather disagreed that strangers could provide correct answers ($Median = 1$ for all question categories). Nevertheless, participants mentioned a potential for attacks (3 visitors, 2 owners) by, e.g. overhearing the answer or finding it on social media. Few participants found the questions too personal and felt uncomfortable sharing the answers (3 visitors, 4 owners): *"I do not like the system to know where I was"* (P6, visitor). One owner mentioned that an attacker could simply confirm every answer and provide access to illegitimate visitors.

4.2.3 Adoption & Improvement. Many participants would adapt the mechanism in the future (6 visitors, 5 owners). Six participants in the visitor role stated they would also use it if they were the owner of the smart home, and nine owners would use it as visitor. Some participants raised suggestions for improvement. For instance, some suggested that the security questions should be customizable (2 visitors, 7 owners) or more relationship specific (1 visitor, 3 owners) to be more resistant against attackers. Two visitors suggested not requiring owner's approval, but instead verifying answers with stored data or using a preset PIN instead of questions. Two owners suggested adapting to context by, e.g., not reading the questions out loud in case of bystanders being present.

5 DIRECTIONS FOR FUTURE RESEARCH

5.1 Visitor Relations & Access

In our study, we recruited pairs of visitors and owners who knew each other well and, hence, it is likely that access to device features will be provided among each other. However, visitor scenarios in the context of smart homes are more complex in daily life, ranging from various types of visitors to related permissions [9, 13, 22, 37, 38]. Designing access control for smart homes is challenging due to this complex role system [13]. For instance, owners might distinguish between close family members and new acquaintances, and, consequently, (not) provide access to device features. Hence, authentication for certain features should be made available for some, but not all users [29]. Also, our security questions targeted common experiences of owner and visitor, which might not exist (yet) for first time visits or rental apartment scenarios. Moreover, short visits, in which devices are not being used, do not require authentication, while authentication might be required more frequently during longer visit. An interesting question for future research is how to handle *visitors of various types* with *various access permissions*? How could an authentication mechanism adapt to the fluent transition between a foreign and known visitor?

5.2 Authentication (Not) Necessary

In our study, we covered a range of device functionalities including such that require authentication and some that do not require authentication. An interesting question is how to classify device features (automatically) in these categories [29]. Visitor access adds another dimension to this, as owners might have individual preferences with regards to which features visitors should need to authenticate for, and which are not accessible to them. Moreover, requiring authentication from (trusted) visitors might lead to conflicts and mistrust. While a possible solution is to provide full access to owners' devices and accounts to visitors without legitimization, this is not ideal from a security perspective. As such, it is necessary to employ and use authentication for visitors to protect the visited home from attackers. However, it is unclear how this can be enforced. It remains to be investigated: *how can conflicts be mitigated among owners and visitors? How can authentication be seamlessly integrated in the visit?*

5.3 (Dynamic) Security Questions in the Smart Home Context

For the concrete mechanism we investigated in our study, we chose a set of fixed questions that we believed to cover easy, medium and hard questions. Prior work suggested the use of *dynamic security questions* based on (changing) personal data (e.g. "Who did you call last week?") [12]. Some of our security questions also have the potential to change over time (e.g., "Where did you meet last time?"), making it harder for attackers. Participants assessed these "hard" questions as easy to answer as static/simpler questions, making them promising candidates for such an authentication mechanism. At the same time, privacy needs to be considered when designing such questions. As such, the question content should not reveal too much personal information [12]. Authenticating visitors should not invade their, the owners', or bystanders' privacy. Moreover,

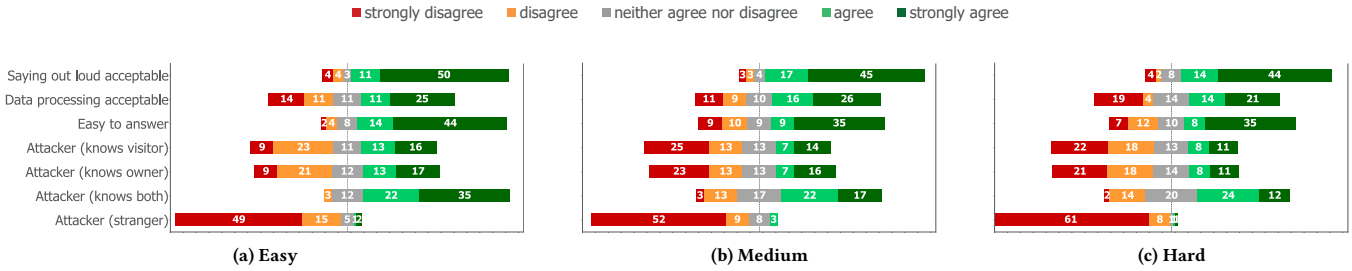

Figure 2: Study Results: Summary of participants' assessment of the security questions per category (5-point Likert scales, 5=strongly agree). Note that every participant ($N = 24$) assessed three security questions per category, hence the total number of responses is 72. Plots for single questions can be found in the supplementary material of this paper.

retrieving personal information is becoming increasingly easy (e.g., through social media), potentially supporting attackers in gaining answers to security questions [32]. The main challenge that remains is to design questions that are easy to answer, hard for attackers, and keep the privacy of both, owner and visitor [12]. Future work should look into how security questions can be designed to be *relatively easy for both, visitor and owner, while keeping their privacy towards each other and be resistant against attacks.*

6 CONCLUSION

In this paper, we explore design considerations for usable authentication for visitors in smart homes, including various types of visitors, device functionalities, and authentication modes. We present and discuss one concrete sample idea, that is the use of security questions to authenticate visitors. Questions covering the relationship to the owner were well accepted by participants in our exploratory study. We would like to motivate further research around the complexity of foreign and known visitors, the design of (dynamic) questions, and (not) enforcing authentication for certain smart home features. With our late-breaking work, we hope to spark discussions around this and further opportunities for visitor authentication in the smart home context.

ACKNOWLEDGMENTS

We would like to thank all participants for their time and valuable feedback on our idea. This research was funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom].

REFERENCES

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

[2] Bako Ali and Ali Ismail Awad. 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* 18, 3 (2018). https://doi.org/10.3390/s18030817

[3] Anitra Babic, Huijun Xiong, Danfeng Yao, and Liviu Iftode. 2009. Building Robust Authentication Systems with Activity-Based Personal Questions. In *Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration* (Chicago, Illinois, USA) *(SafeConfig '09)*. Association for Computing Machinery, New York, NY, USA, 19–24. https://doi.org/10.1145/1655062.1655067

[4] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies* 4, 3 (2009), 114–123.

[5] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. 2015. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In *Proceedings of the 24th International Conference on World Wide Web* (Florence, Italy) *(WWW '15)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 141–150. https://doi.org/10.1145/2736277.2741691

[6] John Brooke. 1996. SUS: a "quick and dirty" usability scale. *Usability evaluation in industry* 1 (1996), 189.

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

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

[9] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies* 4 (2021), 54–75.

[10] Sauvik Das, Eiji Hayashi, and Jason I. Hong. 2013. Exploring Capturable Everyday Memory for Autobiographical Authentication. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Zurich, Switzerland) *(UbiComp '13)*. Association for Computing Machinery, New York, NY, USA, 211–220. https://doi.org/10.1145/2493432.2493453

[11] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[12] Alina Hang, Alexander De Luca, and Heinrich Hussmann. 2015. I Know What You Did Last Week! Do You? Dynamic Security Questions for Fallback Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1383–1392. https://doi.org/10.1145/2702123.2702131

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

[14] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78 (2018), 398–428. https://doi.org/10.1016/j.cose.2018.07.011

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

[16] Matthew Johnson and Frank Stajano. 2009. Usability of Security Management:Defining the Permissions of Guests. In *Security Protocols*, Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 276–283.

[17] Mike Just. 2005. Designing authentication systems with challenge questions. *Security and usability: Designing secure systems that people can use* (2005), 143–155.

[18] Mike Just and David Aspinall. 2009. Personal Choice and Challenge Questions: A Security and Usability Assessment. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 8, 11 pages. https://doi.org/10.1145/1572532.1572543

[19] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598

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

[21] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032

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

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

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

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

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

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

[28] Alexander Ponticello, Matthias Fassl, and Katharina Krombholz. 2021. Exploring Authentication for Security-Sensitive Tasks on Smart Home Voice Assistants, In Seventeenth Symposium on Usable Privacy and Security. *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. https://publications.cispa.saarland/3433/

[29] Sarah Prange, Ceenu George, and Florian Alt. 2021. Design Considerations for Usable Authentication in Smart Homes. In *Mensch Und Computer 2021* (Ingolstadt, Germany) *(MuC '21)*. Association for Computing Machinery, New York, NY, USA, 311–324. https://doi.org/10.1145/3473856.3473878

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

[31] S. Prange, E. von Zezschwitz, and F. Alt. 2019. Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 154–158. https://doi.org/10.1109/EuroSPW.2019.00024

[32] Ariel Rabkin. 2008. Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook. In *Proceedings of the 4th Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '08)*. Association for Computing Machinery, New York, NY, USA, 13–23. https://doi.org/10.1145/1408664.1408667

[33] Stuart Schechter, A.J. Bernheim Brush, and Serge Egelman. 2009. It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions. In *2009 30th IEEE Symposium on Security and Privacy*. 375–390. https://doi.org/10.1109/SP.2009.11

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

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

[36] Michael Toomim, Xianhang Zhang, James Fogarty, and James A. Landay. 2008. Access Control by Testing for Shared Knowledge. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 193–196. https://doi.org/10.1145/1357054.1357086

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

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

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