Smart Use of Smart Devices in Your Home: A Smart-Home Security and Privacy Workshop for the General Public

Tushar M. Jois
tjois@ccny.cuny.edu
City College of New York
New York, NY, USA

Tina Pavlovich
tina.pavlovich@dartmouth.edu
Dartmouth College
Hanover, NH, USA

Brigid M. McCarron
brigid.m.mccarron.26@dartmouth.edu
Dartmouth College
Hanover, NH, USA

David Kotz
david.f.kotz@dartmouth.edu
Dartmouth College
Hanover, NH, USA

Timothy J. Pierson
timothy.j.pierson@dartmouth.edu
Dartmouth College
Hanover, NH, USA

ABSTRACT

With 'smart' technology becoming more prevalent in homes, computing is increasingly embedded into everyday life. The benefits are well-advertised, but the risks associated with these technologies are not as clearly articulated. We aim to address this gap by educating community members on some of these risks, and providing actionable advice to mitigate risks. To this end, we describe our efforts to design and implement a hands-on workshop for the public on smart-home security and privacy.

Our workshop curriculum centers on the smart-home device lifecycle: obtaining, installing, using, and removing devices in a home. For each phase of the lifecycle, we present possible vulnerabilities along with preventative measures relevant to a general audience. We integrate a hands-on activity for participants to put best-practices into action throughout the presentation.

We ran our workshop at a science museum in June 2023, and we used participant surveys to evaluate the effectiveness of our curriculum. Prior to the workshop, 38.8% of survey responses did not meet learning objectives, 22.4% partially met them, and 38.8% fully met them. After the workshop, only 9.2% of responses did not meet learning objectives, while 29.6% partially met them and 61.2% fully met them. Our experience shows that consumer-focused workshops can aid in bridging information gaps and are a promising form of outreach.

CCS CONCEPTS

• **Applied computing** → **Interactive learning environments**; • **Computer systems organization** → *Sensors and actuators*; • **Security and privacy** → *Social aspects of security and privacy*.

KEYWORDS

public outreach, security and privacy, smart home

SIGCSE 2024, March 20–23, 2024, Portland, OR, USA

ACM ISBN 979-8-4007-0423-9/24/03…$15.00
https://doi.org/10.1145/3626252.3630925

ACM Reference Format:
Tushar M. Jois, Tina Pavlovich, Brigid M. McCarron, David Kotz, and Timothy J. Pierson. 2024. Smart Use of Smart Devices in Your Home: A Smart-Home Security and Privacy Workshop for the General Public. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2024), March 20–23, 2024, Portland, OR, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3626252.3630925

1 INTRODUCTION

The rise of the Internet-of-Things (IoT) has enabled the *smart home*, where everyday activities in the management of a home – from turning on lights to controlling sprinklers – are augmented with computation. Smart-home devices often work in concert, leading to greater functionality and convenience for their users. These devices are relatively inexpensive and designed to be used by anyone, helping bridge the digital divide for populations traditionally under-served by technology [5]. These benefits have led to a massive growth in adoption; in 2022, 14.2% of households worldwide had some sort of smart-home functionality, a number expected to grow to 28.8% (or over 672 million households) by 2027 [20].

Coinciding with this democratization of computing is a raft of new security and privacy risks impacting smart-home devices and data, e.g., [2, 7, 12, 14, 17]. While news articles report on security and privacy issues in corporate settings, it is unclear if the public fully comprehends the security impacts to themselves [8]. Our goal was to make consumers aware of the specific threats *they* could encounter and to provide actionable defenses against them.

To achieve this goal, we designed an active learning workshop that introduces members of the public to these security and privacy issues, and highlights specific steps they can take immediately to improve their security and privacy. Uniquely, we incorporate the *smart-home lifecycle*, i.e., the consumer's phases of interaction with smart-home devices, directly into our workshop. This structure allows us to describe the problem from the consumer perspective and help participants to better connect with the course material.

The workshop is one 90-minute session on the topic of smart-home security and privacy, aimed at the general public. Through this curriculum, we provide specific and actionable knowledge rooted in practical scenarios. We also maintain a generous facilitator to participant ratio (1:3), which enables meaningful, guided, active-learning opportunities. We ran this workshop at a science museum in June 2023, as an event open to the public.

Table 1: Learning objectives of our workshop, with associated phase(s) in the smart-home lifecycle.

Learning objective	Lifecycle phase(s)
LO1: Participants can define what a smart-home device is.	Obtaining, Installing, Using, Removing
LO2: Participants understand key security and privacy issues.	Obtaining, Installing, Using, Removing
LO3: Participants are aware of the variety of parties who might have unauthorized use, including accidental use.	Using
LO4: Participants are empowered to protect their data from unauthorized use.	Installing, Using, Removing
LO5: Participants are comfortable with securely setting up and decommissioning a smart-home device.	Installing, Removing
LO6: Participants are aware of where they can find trusted information on smart devices.	Obtaining
LO7: Participants are knowledgeable in the steps needed before taking or giving a secondhand device.	Removing

Prior efforts. Academics study smart-home security and disseminate their results in academic venues. Unfortunately, scientific literature can be too technical for non-experts to follow and implement on their own. Online news articles about new vulnerabilities are written for a more general audience, but can lack actionable information about necessary mitigations [8]. The education community has developed dedicated smart-home cybersecurity coursework (e.g., [11, 21, 24]), with a focus on tertiary education [23]. Cybersecurity, however, is important for *anyone* who interacts with smart-home devices – including adults who may no longer be in the formal education system. When performing our literature search, we were unable to find cybersecurity outreach programs that are focused on smart-home security and privacy for general adult audiences. These types of workshops may exist, but the organizers of these workshops have not necessarily published their design or effectiveness results as a scholarly work.

Contributions. In this experience report, we present our efforts to educate the general public through outreach about new smart-home security and privacy risks. We contribute the following:

(1) *Workshop design.* We describe the design of our smart-home security and privacy workshop, including its organization, curriculum content, and hands-on activity components. Novel to our approach is the application of the *smart-home lifecycle*, the consumer's phases of interaction with their smart-home devices, as an organizing model for learning.
(2) *Workshop effectiveness.* We provide insights into the impacts of this workshop on participants through a series of surveys performed before and after one implementation of the workshop. We also reflect on how we can build on and improve the workshop in future iterations.

2 WORKSHOP DESIGN

We first discuss our workshop's approach and curriculum content.

2.1 Approach

We designed the workshop to be an in-person offering about 90 minutes long geared towards a general adult audience. The event was held at the Montshire Museum of Science in Norwich, Vermont. Public trust in museums as an institution remains high [25], making this an appropriate choice as a venue. We advertised the event via the museum's email list, social media, and local news media.

Organizing model. To achieve our outreach goals, we wanted to present the workshop from a consumer point-of-view. Based on our analysis of the literature [16–18] and our experience, we identified four phases of consumer interaction with a smart-home device:

(1) *Obtaining a device.* Consumers receive a device through purchase or as a gift.
(2) *Installing a device.* Consumers then install the device physically in their home and connect it to their network.
(3) *Using a device.* Once purchased and installed, consumers use their device for its functionality.
(4) *Removing a device.* Finally, when the consumer is finished using a device, they will remove it from their home, and dispose of it or pass it on to somebody else.

Together, we refer to these phases as the *smart-home lifecycle*. We believe that our novel approach of organizing the workshop around this model focuses on topics most relevant to consumers' interactions with smart-home devices. The lifecycle also provides a useful framework for a hands-on activity on selecting, configuring, using, and discarding IoT devices.

Learning objectives. With this lifecycle in mind, we create concrete learning objectives, listed in Table 1, for smart-home security and privacy. We evaluate the effectiveness of our workshop in achieving these learning objectives via surveys (Section 3).

2.2 Content

This section details the content developed for and presented during the workshop, which is consumer-facing in nature, but is informed by the smart-home security and privacy literature (e.g., [2, 7, 12, 14, 17]). We have released our slides, activities, and organization documentation as artifacts for the community.[1]

Preliminaries. The workshop was led by 5 instructors who presented the core content. The room for the event was organized in round tables of 4–6 people, where 1–2 of those were facilitators, and the rest were participants. Each facilitator had knowledge of smart-home security and helped the instructors at the front of the room as needed throughout the workshop.

Introduction. We began the workshop with instructor introductions, some relevant definitions, and then a vignette motivating the problem of misuse of a smart home. In this vignette, a parent leaves their child at home with a babysitter. The parents in our example are comfortable with the sitter having a snack, but would be uncomfortable with the sitter rummaging through cabinets. Similarly, in the smart-home setting, which we illustrate in Figure 1, we highlighted that the parents may not mind the sitter using a smart TV or adjusting a smart thermostat but would not approve of a sitter interfacing with the home's smart speaker to purchase a doll house [10]. We believe that this example is widely applicable: even if a participant cannot directly relate to the situation, it is

[1] Available at https://splice-project.org/workshop-materials/

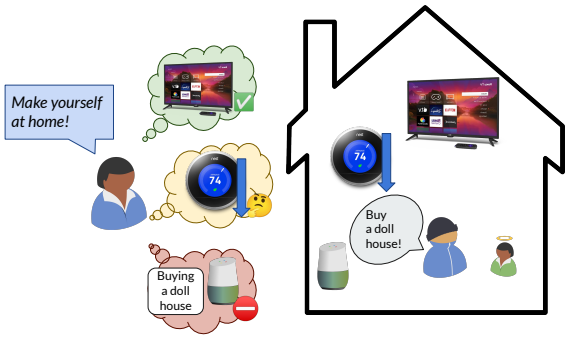

Figure 1: Our example vignette, in which a parent has different levels of comfort with a visiting babysitter using their different smart-home devices.

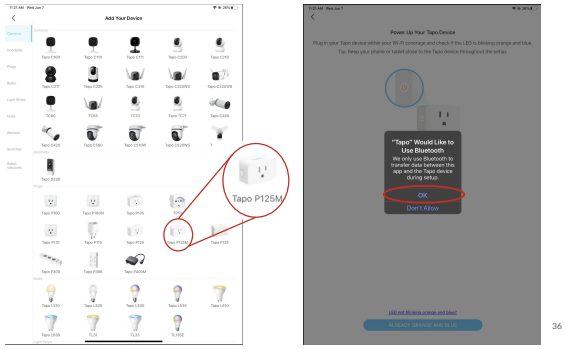

Figure 2: An example slide from our activity showing how to connect to the smart plug.

relatively easy to imagine. The comparison to a non-smart-home setting helps participants get into the adversarial mindset necessary to discuss security and privacy [4].

We used this opportunity to introduce formal terminology, like *unauthorized local use of devices*, and shared news articles that show that such unauthorized use is a real-world threat (e.g., [10]). We also defined and shared examples of unauthorized *remote* access by adversaries who compromise devices over the network (e.g., [22]).

Opening discussion. Once we presented our perspective on the problem, we asked participants to discuss among themselves what they believe are the biggest threats to smart homes. Our facilitators at each table helped guide conversations and answer participant questions. After a few minutes of discussion, participants shared conversation topics with the larger group. We saw a range of worries, ranging from threats to specific smart-home devices, to a general fear of 'hackers'. This instant feedback helped us gauge how our audience viewed the problem of smart-home security and calibrate the rest of the workshop to address the concerns raised. It also helped to set the tone of the workshop as one of active learning.

Obtaining a device. We then entered the main content of the workshop, via the smart-home lifecycle. In presenting the first stage, of *obtaining* a device, our focus was on encouraging participants to engage in effective pre-purchase research. We motivated this topic by showing that a simple search for a "doorbell camera" results in a number of cameras from several manufacturers and sellers. We suggested looking for reputable manufacturers with a track record of prioritizing the security of their devices, while avoiding devices that are from brands with no track record. We also pointed out sources that provide trustworthy device reviews (e.g., [6, 15, 26]).

Performing this kind of pre-purchase research can help consumers avoid vendors that may not be prepared to handle attacks that impact the complex IoT supply chain [17]. A more reputable manufacturer likely provides information on its security practices and has a documented history of its responses to attacks and breaches. We cautioned the audience that picking reputable manufacturers will not eliminate all attacks against their devices; rather, we present it as a mitigation of the risks inherent to smart homes. This theme of mitigation – rather than elimination – recurs frequently in our workshop.

Installing a device. For our next phase, *installing* the device, we focus on the configuration necessary after physical placement in the home. Our advice in this section is designed to avoid the access control attacks that can occur due to weak or default passwords (e.g., [2, 7]). We first highlighted password attacks, such as social engineering, brute force, or re-use. We used this understanding of weak passwords to describe how to create strong passwords. We recommended the use of *passphrases* [19] – long, random combinations of words and numbers – and to store these passphrases into password managers (e.g., [1, 3]). We also discussed two-factor authentication and how enabling it leads to higher security.

Activity, part 1. We wanted to give the participants an opportunity to try out these concepts, hands-on, with a live activity on a real IoT device. We chose the TP-Link Tapo P125M smart plug as the example device, based on its availability in large quantities, modern iPad app, and automatic updates [9]. Each table received one such smart plug and an iPad to configure and control it.

For the first part of the activity, we guided participants through the initial configuration of the plug: creating an account, setting up the device, and connecting the device to Wi-Fi. We made an effort to connect our activity back to the concepts presented earlier, such as using a strong passphrase when creating an account. Figure 2 shows a screen capture from our activity.

This part was relatively lengthy (~20 minutes), due to the numerous steps involved in configuring a device for the first time. To make this length more manageable, we provided each table with printed hand-outs of the activity's steps. We observed a range of technology skills in our participants. On one end, some participants breezed through the entire activity, even skipping ahead past our presentation. Other participants struggled to type in special characters on the iPad keyboard. Our facilitators at each table assisted less technology-adept participants and engaged the more advanced participants by exploring additional features of the smart plug.

Using a device. Although this stage of the lifecycle is arguably the longest stage in terms of consumer-device interaction, we focused our presentation on two topics: (1) preventing unauthorized local access to devices and (2) preventing unauthorized remote access to devices. For (1), we recalled the initial vignette of the babysitter coming to the family home to watch a child, and focused on mitigations such as guest mode, parental controls, disabling features,

and providing temporary access. For (2), we explained the cycle of device manufacturers identifying vulnerabilities in various ways, issuing software updates to improve the device's performance, features, or enhance security, and finally having users update their device software. We mentioned the benefit of turning on automatic updates if available, and participants asked questions about how to verify that a software update originates from the manufacturer.

Activity, part 2. Because of the simple functionality of a smart plug, our chosen device did not have a local guest mode like discussed in the previous section. It did, however, have two-factor authentication and automatic updates available, so we used this part of the activity to briefly highlight these security features.

Removing a device. The final phase of the lifecycle is *removing* a device from the smart home. To emphasize the importance of this step, we showed the types of data that can accumulate on the device and in-cloud over the course of the lifecycle. We then instructed the participants to look for account deletion and factory reset before getting rid of a device. This part is often overlooked, as forensic data recovery attacks are possible against devices (e.g., [12, 14]).

Activity, part 3. The final part of our activity works through the safe removal of the smart plug, removing it from the network and resetting it to factory settings. Thus, our activity – like our workshop curriculum more broadly – is end-to-end.

Conclusion. We ended our tour of the smart-home lifecycle by summarizing the workshop to this point, which focused primarily on the technical solutions to the problems that arise in smart-home settings. To supplement this technical content, we also discuss the *social* aspect of security in smart homes [13], which may not be immediately obvious to our audience.

We returned to the babysitting example, but this time posited that the unauthorized use originally presented in our opening vignette could have been prevented by simply setting expectations with the visitor: in other words, making ground rules for the smart home. The technical defenses discussed would help in protecting against both local and remote misuse of the smart home, but being explicit about what is and is not allowed helps avoid accidental local misuse from honest-but-curious guests like our babysitter.

Closing discussion. After presenting this alternative solution, we proposed another discussion question, asking our participants to think about how they could set expectations with their guests and visitors, and how they would feel about doing so. We hoped that this discussion would reinforce that security and privacy is not just technical. Our participants appeared engaged with this, envisioning scenarios where they would or would not decide to apply social controls on top of any technical ones.

3 WORKSHOP EFFECTIVENESS

We now present our workshop survey results to quantify efficacy.

3.1 Assessment Strategy

We designed 3 surveys for our study. First, we included a physical pre-workshop survey (**S1**) with space for free-form responses to assess participants' knowledge of the learning objectives shown in Table 1. We also gathered demographic information. After the workshop, participants were provided with a physical post-workshop survey (**S2**). S2 included the same questions as S1 with an additional section with Likert response types to understand the participants' impressions of the workshop itself. We also asked attendees for their email address, so we could send them materials from the workshop and an online survey via Qualtrics 2.5 weeks later (**S3**). S3 was only two questions and the goal was to assess the relevance and permanence of the topics and lessons shared in the workshop.

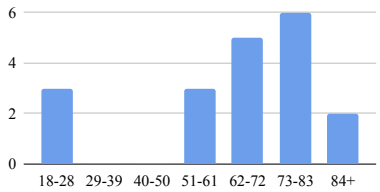

Figure 3: Distribution of participant ages.

Ethical concerns. Before we conducted our research, our project plan received institutional review board (IRB) review and approval. We included a consent form with S1, stating that participation in our surveys was entirely voluntary and that participants could choose to not answer any questions. We provided additional context to explain why were asking for demographic and contact information. We also informed the participants that their data would be kept confidential amongst the project team members. To this end, we secured access to the physical surveys and scanned copies. We present only anonymized insights from the surveys in this work.

3.2 Participant Demographics (S1)

We had 19 total participants, 9 of whom were women (47.4%), and 10 men (52.6%); 18 were white or Caucasian, and 1 was Hispanic. Participant age distributions are shown in Figure 3; note the bimodal distribution of a few younger adults and many older adults.

3.3 Participant Learning (S1, S2)

Responses to S1 and S2 were transcribed after the event, and each participant was assigned a participant ID number. Each survey response was categorized based on whether it met our learning objectives. If a response showed no knowledge of the topic, the response was categorized as not met (NM). If a response showed partial knowledge of the topic or had correct components but was not fully correct, the response was categorized as partially met (PM). If a response was both correct and specific, it was categorized as fully met (FM).

Table 2 includes analysis of S1 and S2 responses from the 14 participants who filled out both surveys, whom we refer to collectively as the "survey group." Overall, 38.8% of these responses to S1 did not meet learning objectives, 22.4% partially met them, and 38.8% fully met them. Only 9.2% of responses to S2 did not meet learning objectives, while 29.6% partially met them and 61.2% fully met them. The number of participant responses which did not meet learning objectives decreased from S1 to S2 for all except LO2, on which participants already had generally strong knowledge prior to the workshop. The following paragraphs describe insights gleaned

Table 2: Survey questions with associated learning objectives (LO). We note the number of participants who filled out both S1 and S2 (14) whose survey responses did not meet (NM), partially met (PM), or fully met (FM) learning objectives.

Survey question	LO	S1			S2		
		NM	PM	FM	NM	PM	FM
How would you describe a "smart-home device"?	LO1	5	2	7	0	4	10
What security and privacy risks could you encounter when engaging with your smart-home devices?	LO2	2	2	10	2	2	10
Who could access your friend or family member's smart-home devices aside from them?	LO3	5	1	8	2	2	10
How knowledgeable do you feel in being able to protect your data from unauthorized use?	LO4	5	6	3	1	10	3
What are some ways you can improve the security of your smart-home devices?	LO5	8	3	3	2	2	10
Do you know of any resources to find trusted information on smart-home devices? If yes, please list them.	LO6	9	3	2	2	2	10
What are some steps somebody should take when giving or receiving a second-hand smart-home device?	LO7	4	5	5	0	7	7

from our analysis of the survey group's responses per learning objective, and the common themes we saw across responses.

LO1. Workshop participants had a fair original understanding of what constitutes a smart-home device. The most common theme for LO1 in S1 was that devices had some form of Internet connectivity. In S2, the most common theme was inter-connectivity, with Internet connectivity now being the second most common theme. Although our workshop content did not specifically cover device inter-connectivity, we saw this as a positive knowledge gain amongst participants. We also asked about the number of devices each participant had. The survey group had an average of 6.1 devices in S1, although that rose to 6.9 by S2. This change could be attributed to the participants in the survey group either changing their definitions of a smart home device after our workshop or recalling additional devices in their home.

LO2. Participants' understanding of security and privacy risks related to smart-home devices was relatively advanced prior to the workshop. In S1, they cited information or data leakage, poor passwords, and unnecessary cloud connections as risks, to name a few. In S2, a new theme emerged in respondents' answers: unauthorized access, which we spent much of the workshop discussing.

LO3. The survey question addressing LO3 was abstracted to "friend or family member's smart-home devices" to encourage participants to get into an adversarial mindset [4]. Participants either had correct answers for this question – themed under anyone with home access/proximity, anybody with access to the Wi-Fi network, or somebody over the Internet – or had no idea prior to the workshop. After the workshop, more participants were able to articulate who could potentially access these devices, and "anybody savvy enough" became a new theme.

LO4. The survey group's self-assessed feelings of knowledge on being able to protect their data from unauthorized use increased from an S1 average of 1.9 to an S2 average of 2.1, for knowledge levels of 1 = not at all, 2 = somewhat, 3 = very.

LO5. Participants generally struggled to identify ways to improve the security of their smart-home devices in S1, although correct answers largely fell under the theme of "using passwords." In S2, the most mentioned theme was tied between "unique/better passwords or passphrases" and "update device software." The responses show not only gains in knowledge of different methods to improve security, but also refinements of pre-existing knowledge.

LO6. In S1, most participants simply mentioned internet searches in their response. Although "Google" remained a popular response in S2, participants supplemented that with mentions of more specific and reputable information sources. "Consumer Reports," "Wirecutter," and "PCMAG" were amongst other answers and were three sources explicitly noted in our presentation. These responses indicate that participants were highly receptive to our advice.

LO7. Prior to the workshop, participants generally knew that it is important to factory reset a secondhand device before giving and after receiving it. After the workshop, answers were more developed, and more participants knew to also delete the device information off the device and log out of any accounts.

3.4 Participant Impressions (S2, S3)

S2 and S3 gauged the participants' opinions on the workshop itself.

Post-workshop (S2). As Figure 4 shows, most of the survey group felt the workshop topics were presented at an appropriate level of detail for them, and they learned something applicable in their own home. When asked whether the promotional material accurately described the workshop, all who responded did so positively.

2.5 weeks later (S3). Five participants responded to S3, as seen in Figure 5. Although the workshop was not as relevant for some, all respondents agreed to some extent that they believe they have the knowledge to apply a concept from this workshop.

3.5 Reflection

We now use the survey responses and our anecdotal evidence to reflect on what went well, what did not, and what to study next.

Successes. As the survey results in Table 2 show, our 90-minute workshop was generally effective in helping surveyed participants attain our learning objectives, either partially or fully. A majority of responses fully met LO1, LO2, LO3, LO5, and LO6 in S2. Also, as depicted in Figure 4, participants broadly agreed that they learned something relevant and that the workshop met their expectations based on its marketing. We believe these successes can be attributed to the inclusion of a motivating vignette and to the lifecycle-based framing of user interactions with smart-home devices.

Anecdotally, we noted that the activity and discussion parts of the workshop were well-received by our participants. The facilitators were critical to the success of the active learning components. They helped customize engagement levels by providing additional exploratory opportunities for participants moving ahead of the demonstration and assisting others who required more guidance. There was a noticeable uptick in interest when facilitators actively

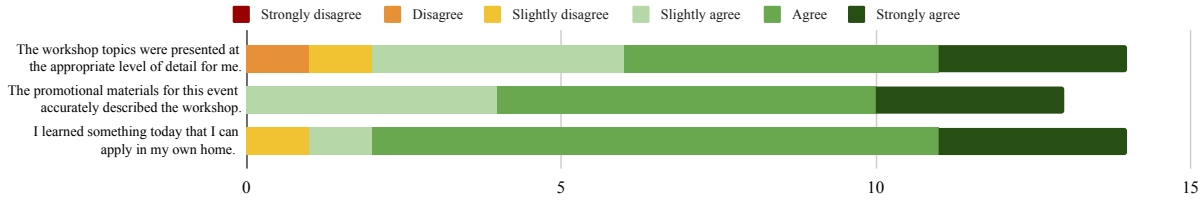

Figure 4: Survey results of participant impressions immediately after the workshop (S2).

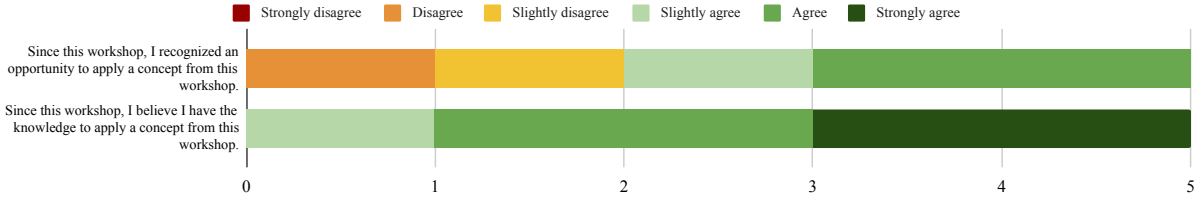

Figure 5: Survey results of participant impressions 2.5 weeks after the workshop (S3).

participated in the session, and, in post-workshop conversations, participants praised their facilitators.

Challenges and potential changes. There are some areas for improvement for the workshop. We noticed that some participants did not meet LO2–LO6 after the workshop. Also, the workshop was not fully relevant to every participant, as seen in Figures 4 and 5. Addressing these issues will likely require tweaks to the curriculum to better emphasize these learning objectives and adding a few more grounding examples for broader relevance.

One of the biggest challenges when attempting a workshop of this type is estimating the pre-existing knowledge of the participants. We planned for a wide range of audience experience, and our use of facilitators helped with this. To ensure material is even better calibrated, however, responses to pre-workshop surveys could be immediately analyzed and used to select workshop topics, so that the presentation is tailored to participant interests and knowledge.

On a related note, we would like to improve our data collection. LO4 only had 3 options: not at all, somewhat, and very knowledgeable. It is possible that the absence of a "reasonably knowledgable" option led to some participants to hedge, leading to an over-representation of "somewhat." Additionally, some participants disagreed that the workshop was at an "appropriate" level of detail, but our phrasing does not provide insight as to if they believed it was too detailed or not enough.

Certain participants encountered accessibility challenges, which we had anticipated for the activity, and addressed by enhancing text readability for those with impaired vision and ensuring thorough explanations of tablet-related steps. Extending accommodations to the slide presentation would enhance overall accessibility. We could proactively gather accommodation requests during the sign-up process and make necessary adjustments prior to the workshop. These steps play a crucial role in ensuring the inclusion of all interested participants, regardless of their individual needs.

Future directions. Our experience opens several opportunities for future work. The most obvious is re-running the workshop in a different location. Our event demographics were dominated by older white men and women with reasonably good knowledge of topics presented, and we cannot claim generality without a larger, more diverse sample. The changes described above would also help with adapting to and engaging with diverse audiences, both in terms of identity and knowledge.

Another future direction involves a modification of the hardware and software used in the activity. Instead of using an off-the-shelf device and app, we propose the creation of a custom smart-home app that would integrate with the presentation. The app would guide participants through the steps of the activity, akin to a tutorial or walk-through. Not using a specific off-the-shelf device would also minimize risk that participants infer the presentation team is recommending that device. This change would require some engineering effort, but would improve the participant experience.

4 CONCLUSION

In this work, we present our workshop on smart-home security and privacy geared towards the general public, and our findings as to its efficacy. Our experience shows that holding consumer-focused community events on the topic of smart-home device security and privacy can aid in bridging information gaps in community members' understandings of devices, their shortcomings, and risk mitigations and are a promising form of outreach. It is our hope that this experience report, along with our presentation materials, spurs the scholarly development and implementation of more events aimed at improving the smart-device security literacy of the general public.

ACKNOWLEDGMENTS

We thank the Montshire Museum of Science for hosting the workshop, Geisel School of Medicine for lending iPads, and Weija He, Benjamin Kallus, Ravindra Mangar, Shreya Suresh, and Chixiang Wang for being facilitators. This work is supported by NSF awards 1955805 and 1955172. The views contained herein are those of the authors and should not be considered those of the NSF.

REFERENCES

[1] 1Password. 2023. 1Password. https://1password.com/.

[2] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*. 1093–1110.

[3] Bitwarden. 2023. Bitwarden Open Source Password Manager. https://bitwarden.com/.

[4] Sergey Bratus. 2007. What hackers learn that the rest of us don't: Notes on hacker curriculum. *IEEE Security & Privacy* 5, 4 (2007), 72–75.

[5] Jyoti Choudrie, Efpraxia Zamani, and Chike Obuekwe. 2022. Bridging the digital divide in ethnic minority older adults: an organisational qualitative study. *Information Systems Frontiers* 24, 4 (2022), 1355–1375.

[6] Consumer Reports. 2023. Guide to Smart Home Devices & Tech. https://www.consumerreports.org/home-garden/smart-home/guide-to-smart-home-devices-tech-a1007276600/.

[7] Ang Cui and Salvatore J Stolfo. 2010. A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan. In *Proceedings of the 26th Annual Computer Security Applications Conference*. 97–106.

[8] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[9] John R. Delaney. 2023. TP-Link Tapo Mini Smart Wi-Fi Plug (P125M) Review. https://www.pcmag.com/reviews/tp-link-tapo-mini-smart-wi-fi-plug-p125m.

[10] Jennifer Earl. 2017. 6-year-old orders $160 dollhouse, 4 pounds of cookies with Amazon's Echo Dot. *CBS News* (05 01 2017).

[11] Mounib Khanafer and Tushar M Jois. 2023. Towards Application-Driven IoT Education. In *2023 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 1–7.

[12] Soram Kim, Myungseo Park, Sehoon Lee, and Jongsung Kim. 2020. Smart home forensics—data analysis of IoT devices. *Electronics* 9, 8 (2020), 1215.

[13] Martin J Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further exploring communal technology use in smart homes: social expectations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–7.

[14] Shancang Li, Kim-Kwang Raymond Choo, Qindong Sun, William J Buchanan, and Jiuxin Cao. 2019. IoT forensics: Amazon echo as a use case. *IEEE Internet of Things Journal* 6, 4 (2019), 6487–6497.

[15] Angela Moscaritolo. 2023. The Best Smart Home Devices for 2023. https://www.pcmag.com/picks/the-best-smart-home-devices.

[16] Antonio L Maia Neto, Artur LF Souza, Italo Cunha, Michele Nogueira, Ivan Oliveira Nunes, Leonardo Cotta, Nicolas Gentille, Antonio AF Loureiro, Diego F Aranha, Harsh Kupwade Patil, et al. 2016. Aot: Authentication and access control for the entire iot device life-cycle. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. 1–15.

[17] Tope Omitola and Gary Wills. 2018. Towards mapping the security challenges of the Internet of Things (IoT) supply chain. *Procedia Computer Science* 126 (2018), 441–450.

[18] Leila Fatmasari Rahman, Tanir Ozcelebi, and Johan Lukkien. 2018. Understanding IoT systems: a life cycle approach. *Procedia computer science* 130 (2018), 1057–1062.

[19] Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *Proceedings of the eighth symposium on usable privacy and security*. 1–20.

[20] Statista. [n. d.]. Digital Markets: Smart Home – Worldwide. https://www.statista.com/outlook/dmo/smart-home/worldwide.

[21] Zouheir Trabelsi. 2021. Iot based smart home security education using a hands-on approach. In *2021 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 294–301.

[22] Elizabeth Tyree. 2019. 'Look behind you'; Va. family says hackers used Ring cameras to taunt their children. *WSET* (19 12 2019).

[23] Valdemar Švábenský, Jan Vykopal, and Pavel Čeleda. 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Portland, OR, USA) *(SIGCSE '20)*. Association for Computing Machinery, New York, NY, USA, 2–8. https://doi.org/10.1145/3328778.3366816

[24] Feng Wang, Kuai Xu, and Guoliang Xue. 2022. A Holistic Curriculum Towards Teaching Smart Home Security. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2*. 1284–1284.

[25] Wilkening Consulting and AAM. 2021. Museums and Trust Spring 2021.

[26] Wirecutter. 2023. Smart-Home Devices. https://www.nytimes.com/wirecutter/home-garden/smart-home/.