From Frustration to Function: A Study on Usability Challenges in Smart Home IoT Devices

Vignay Chanda, Luoyao Hao, Henning Schulzrinne

Department of Computer Science, Columbia University, New York, NY, USA
Email: vc2608@columbia.edu, {lyhao, hgs}@cs.columbia.edu

2024 IEEE 21st Consumer Communications & Networking Conference (CCNC) | 979-8-3503-0457-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/CCNC51664.2024.10454634

***Abstract*—IoT devices have significantly altered the methods of interaction, operation, and functionality within home environments. However, individuals, particularly those with limited technical proficiency who stand to gain the most from these advancements, likely encounter challenges stemming from the intricate setup processes, a critical stage with the potential to limit their widespread adoption. Thus, we focus on the user experience during the setup phase of mainstream smart home devices and conduct an empirical study of 15 representative smart home IoT devices. We scrupulously examine their setup processes, as well as accompanying instructions and user manuals, to assess multi-faceted usability concerns. Our findings reveal 19 usability issues, indicating notable barriers, inconsistencies, and a lack of intuitiveness, which may deter consumers from successfully configuring and using these devices.**

I. Introduction

Internet of Things (IoT) heralds a transformation of our daily lives, making home appliances more interoperable and actionable through a wide range of smart home devices, such as security cameras, power strips, and voice assistants. Despite the enhanced lifestyle and the elevated comfort, security, and convenience, promised by smart home devices, there are clear roadblocks in the form of multi-faceted usability challenges, primarily for those lacking technical expertise. The initial setup phase becomes a particularly critical hurdle, with a tangle of complexities and functionalities that might be navigable for tech-savvy users but can pose insurmountable challenges for others, thereby barring them from experiencing advanced post-setup features [1]. For instance, a common procedure of paring devices to Wi-Fi while activating Bluetooth at the same time, may result in concerns among users cautious or inexperienced with devices.

Unfortunately, the importance of usability and user experience during the setup phase is somewhat understated and understudied, despite its pivotal role in shaping a user's first impression of the device, and consequently their further interaction and engagement with it. Zeng and Roesner [2] delve into the intricacies of multi-user scenarios, revealing concerns among smart home IoT users related to the cumbersome nature of security and privacy configurations. Vetrivel et al. [1] examine customer reviews and emphasize that the majority of feedback pertaining to security steps during setup is from non-technical reviews. The study highlights substantial concerns about device setup among non-tech-savvy users, particularly regarding the usability of devices, where twice as many users encounter friction compared to those who do not. Jakobi et al. [3] unveil a disconnection between user desires and system configuration during installation, finding that even when features are technically supported, usability issues prevent users from leveraging them effectively.

While the concerns and enhancement of usability during the initial configurations and interactions with devices have been recurrently mentioned, existing efforts mainly focus on user interviews or product reviews. Explicit experience of first-hand usability concerns during the setup phase remains underrepresented in existing studies. Centered on the initial setup, we rigorously explore and illuminate potential usability concerns intrinsic to smart home devices. In doing so, our work seeks to not only fill the blank area but also offer a nuanced understanding and meticulous details of usability challenges users may encounter during the setup of devices.

Fig. 1. 15 of our home IoT devices are studied in this paper.

In this study, we analyze the setup procedures, associated features, and their instructions for 15 key smart home IoT devices from our collection, as shown in Figure 1. Drawing from classic usability principles, we propose consistency and memorability as augmented usability criteria tailored for IoT. Our examination of the setup procedures reveals 19 distinct usability challenges encompassing facets like device onboarding, privacy, access sharing, consistency, and memorability. Furthermore, we provide an extensive documentation[1], detailing all the configurations and relevant device features, facilitating readers to understand the nuances without the prerequisite of possessing or interacting with the device.

[1]A comprehensive report is available at https://www.cs.columbia.edu/~lyhao/paper/iotusability.pdf.

II. Methodology Overview

This section outlines the methodology employed to evaluate the usability and user interaction aspects of the selected IoT devices. These devices are categorized into five distinct types of commonly used smart home devices, as presented in Table I. Each device is thoroughly documented across five major categories to learn about the potential usability challenges.

Different from major usability studies that typically rely on human subject research methods such as interviews, questionnaires, in-home studies, or online review analysis, we apply a document-centric approach. Our primary goal is to produce a comprehensive device report detailing each step of the configuration process, enabling interested readers to delve into usability specifics without the need to purchase and reconfigure devices or experience functionalities firsthand. Rather than seeking user-centric comments or perspectives, we pursue granular, device-centric details. This decision is underscored by several considerations: (1) Prior research has stated usability challenges via human-based studies, and we do not intend to gather generic opinions in this domain. (2) Our earlier experience suggests that user opinions on IoT applications tend to align, without notable deviations [4]. (3) Given the number of devices and multi-faceted usability aspects under scrutiny, a thorough examination requires roughly a hundred hours. This makes human subject research impractical, particularly when evaluating memorability, which requires users to revisit tasks after a long interval. Thus, rather than gathering a broad understanding of user experiences, we aim to draw on all conceivable usability concerns tied to the setup phase of devices in our possession.

TABLE I
A list of types of devices used in the study and their descriptions obtained

Device Type	Description
Smart Plug	A smart plug or a power strip fits between power cords and sockets, functioning as a remote-controlled power switch.
Smart Camera	A smart camera (also called security camera) tracks the happenings in your home and transmit the video to your smartphone or cloud storage for the archive.
Voice Assistant	A plug-in smart speaker allows users to control other smart devices at home by voice control.
Fitness Tracker	A wearable device monitors fitness-related metrics such as walking distance, calorie consumption, and heartbeat.
Smart Bulb	An Internet-capable LED light bulb that can be customized, scheduled, and controlled remotely.

A. Device Initialization and Configuration

In order to accurately and comprehensively evaluate the setup process, we factory-reset each device and approach the initialization and configuration as a new user. Following the guidelines laid out in the user manual, we meticulously document every step encompassing any necessary assembly or physical installation, information from the device's accompanying application, and other key configuration or alternative steps. Our documentation also highlights any challenges faced during the setup, including any troubleshooting measures employed. Any instances where we deviate from the provided instructions, or seek additional information from other sources, are noted and included in the analysis. Through this rigorous process, our aim is to shed light on the user experience, by providing details and highlighting potential pain points.

B. Device Onboarding

We detail the process of connecting each device to the network, with a particular focus on the Wi-Fi network. As the first-time registration of a device into the home network, the device onboarding process is crucial for assessing the device's usability. Nonetheless, the complexity and usability concerns inherent in device onboarding have gathered criticism, and consequently, new approaches are emerging to supersede conventional methodologies [5]. We experience the different onboarding methods, look into the user-friendliness of the options, and identify any potential challenges users might face when connecting the device to their network.

C. Privacy Concern

Understanding the privacy implications of an IoT device is vital in light of escalating worries about data privacy and security in today's digital landscape [6]. We scrutinize the privacy practices, particularly focusing on the specific permissions sought by the device or its paired application, the manner in which these permissions are requested and utilized, as well as the related user interfaces. Through this approach, we identify potential privacy-related usability issues arising from the type of data gathered and the permissions required by the device or its associated application.

D. Grant Device Access

The ability to share control of IoT devices with others is an important feature, as it enables multiple users in a household to manage the devices. We examine the process of granting access to other users and assess its usability and flexibility. Specifically, we document the steps required to share control of each device, including the process of sending and accepting invitations. We also evaluate whether it is possible to share control of devices as a group and whether the sharing permissions can be tailored to individual users, allowing the primary user to control which features and functionalities can be accessed by the granted users.

E. Consistency

Consistency ensures users should not have to wonder if varying words, situations, or actions imply identical meanings [7]. It primarily refers to uniform action sequences, terminology, units, layouts, colors, and typography within a software application [8]. In the context of IoT usability, we propose it as:

Consistency involves maintaining a coherent design, user interface, and functionality across varying models or versions of an IoT device and its associated application. This also extends to different devices within the same product family. It means that users should not encounter ambiguity or confusion regarding whether different terms, tasks, or actions

TABLE II
PERMISSIONS REQUESTED BY SMART PLUGS AND SMART CAMERAS

Permission	Gosund	SmartThings	Etekcity	Kasa	DSP-W320	BN-LINK	Blurams	Kasa Spot	Mi Home	TECKIN
Bluetooth	✓	✓	✓			✓		✓	✓	✓
Location	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Camera	✓	✓				✓			✓	
Local Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Microphone		✓					✓	✓	✓	
Precise Location			✓						✓	

within an application or system are similar or distinct from one another. Consistency in the user experience is essential in human-computer interaction of IoT for several reasons:

- *Reduced learning curve:* When IoT devices maintain consistent design elements and interactions, users can transfer their understanding from one functionality to another, simplifying the setup and integration of new devices within their IoT ecosystem.
- *Enhanced user satisfaction:* Consistency leads to a more predictable and comfortable user experience, which in turn fosters users' trust and confidence in the device and its ecosystem.
- *Increased efficiency:* A consistent interface across the device and its associated platform allows users to complete tasks more efficiently, as they can leverage their familiarity to navigate and operate through the interfaces.

F. Memorability

Memorability entails that a system should be easy to remember, so that casual users are able to return to the system after some period of not having used it, without having to relearn the functionalities [7]. In the context of IoT usability, we propose it as:

Memorability refers to how intuitively users can remember and apply both basic and advanced features of an IoT device or its related application, after not using it for a period of time. Memorability, in essence, emphasizes the ease of "recognition rather than recall". Generally, if users cannot recall how an IoT device functions or the steps to operate it after a period of time, they might find it bothersome to re-consult the manual, if retained, and relearn the procedures. Such hurdles may push them to revert to using the product like a conventional device, without its IoT capabilities. Memorability in human-computer interaction is critical of IoT for several key considerations:

- *Reduced reliance on user manual and external resources:* If users can intuitively recall how to operate an IoT device, they become less reliant on user manuals, online tutorials, or helplines.
- *Increased user satisfaction:* A memorable IoT interface ensures that users can swiftly regain familiarity after a period of non-use, fostering a sense of mastery and control over their interconnected devices.
- *Sustained user engagement:* Memorability is particularly important for IoT devices whose intricate functionalities or features are not engaged by users frequently. Devices that remain intuitive over time can sustain user engagement, ensuring they reap the benefits of their IoT ecosystem without becoming overwhelmed or discouraged.

IoT devices are typically set up once and used for an extended period without the need for reset or reconfiguration. Unlike traditional home appliances, infrequent and complicated configurations for IoT devices demand a clear and memorable setup process. Thus, the memorability of the setup process becomes a vital usability criterion.

In order to assess the memorability of the smart home devices, we use a two-phase testing approach in our study, to evaluate the ease with which users could recall the basic and advanced functionalities of each device after a period of disuse. The study is conducted as follows:

1) Initial testing: In the first phase, we thoroughly test each of the IoT devices, documenting our observations and experiences with their configuration and functionalities, including all the previously mentioned aspects. This preliminary assessment allows us to gain an in-depth understanding of the devices, their user interfaces, and the ease or difficulty in navigating their features.
2) Two-week break: After the initial testing, we take a break of two weeks. In this period, we do not use or interact with the device being tested. This pause simulates a real-life scenario where users might not use IoT devices or certain functionalities continuously.
3) Follow-up testing: After the two-week break, we conduct a follow-up test with each of the IoT devices. We attempt to recall and perform the features and functionalities that we learn from the initial testing, without referencing any resources. We record the ease of recalling and executing tasks, noting instances where consultation with guides or resources is required.

III. USABILITY ANALYSIS

In this section, we undertake a detailed analysis of the devices in our repository.

A. Privacy Concern

The permissions sought by an IoT application can, in many instances, elevate privacy concerns among users. If the application does not present good usability while requesting the approval of the permissions, it further compounds the issue of both usability and privacy, as users may struggle to comprehend the rationale behind such requests. Not understanding the intended use or the necessity of a permission request can amplify existing privacy apprehensions. Thus, poor usability can exacerbate privacy concerns, creating a barrier to user confidence and acceptance.

Tables II shows the comparisons in permissions requested by smart plugs and smart cameras. Users who are not aware of the technical aspects of a device are likely confused when the associated application asks for access to something that is not directly related to its main functions. SmartThings Wi-Fi Plug asks for microphone permissions even though it is simply a smart plug without a speaker, and other smart plugs like Gosund, SmartThings, and BN-LINK ask for camera access, the reason for these permissions may look redundant for users with a non-technical background. These plugs ask for mobile camera access to scan the QR codes to download the application for an easy setup process, and SmartThings asks for microphone access to enable voice control. Similarly, other privacy concerns arise when location and local network access are required by smart plugs and cameras, which may cause confusion for the users. Etekcity Smart Plug and Mi Smart Camera both request precise location information to enable additional features. For instance, the accompanying application utilizes this data to accurately determine sunrise and sunset times at the user's specific location, facilitating the activation and deactivation of certain functionalities tailored to individual preferences. To scan nearby Wi-Fi endpoints using a smartphone application, users must grant location permissions. Otherwise, they will have to manually enter the Wi-Fi SSID. This is due to the operating systems classifying nearby SSIDs as sensitive location data, making an application unable to read SSIDs if the location permission is not enabled. Yet, as many users perceive location permissions as highly sensitive private information [9], failing to explain the purpose of accessing location or its necessity might be problematic to usability.

To summarize, our findings suggest these usability concerns:

U1 Permissions may be requested without being clarified about their purpose and relevance.

U2 Broad requests for camera, microphone, and location permissions can raise privacy concerns.

U3 Confusion may be caused when devices request permissions intuitively unrelated to their primary functions.

B. Device Onboarding

Of the 13 Wi-Fi devices we evaluated, 12 exclusively support the 2.4GHz Wi-Fi connection, while only the Mi Home security camera offers support for both 2.4GHz and 5GHz frequencies, as detailed in Table III. While the 5GHz Wi-Fi promises faster data transmission rates, its coverage is notably less compared to the more extensive but slower 2.4GHz frequency. The device support suggests that device manufacturers are generally satisfied with the speed and coverage of 2.4GHz Wi-Fi, in order to maintain a robust and uninterrupted connection to deliver consistent and seamless services to users. It is noteworthy that during our evaluations, even the introduction of metal lamp shades impacted the Wi-Fi signal strength, as observed with the Tapo Smart Light Bulb. This emphasizes the sensitivity of these devices to environmental factors and the importance of their connectivity preferences.

TABLE III
SUMMARY OF NETWORK CONNECTIVITY METHODS ACROSS IOT DEVICE CATEGORIES

Network Type	Number of Devices
2.4GHz Wi-Fi	13
5GHz Wi-Fi	1
Bluetooth	6
Open Wi-Fi (Unsupported)	2

However, setting up the initial Wi-Fi connection can be quite different for each device, which yields a different user experience. We identify three primary approaches for this process: AP Mode, EZ Mode, and AutoScan.

- **AP Mode**: A prevalent approach adopted by most smart devices, where the mobile phone and the Wi-Fi chip of the device directly establish communication. In this mode, the device itself acts as a Wi-Fi access point. Users must manually connect to it via their Wi-Fi settings and provide the original Wi-Fi credentials. While this process can be time-consuming and somewhat confusing, AP Mode is still the most reliable and popular method. Most devices offer support for this mode or often use it as a fallback when their primary methods fail (e.g., when connecting to a public Wi-Fi).
- **EZ Mode**: The device sets itself to the monitor mode and captures Wi-Fi packets over the air [10]. The user needs to manually input the Wi-Fi credentials in the application, which then blindly sends the Wi-Fi credential over Wi-Fi for the device to intercept. To confirm the device's online status, mDNS is required, making this mode unsuitable for public Wi-Fi networks. Though it might expose security issues [11], EZ Mode offers an improved user experience, eliminating the need for users to connect to a separate hotspot.
- **AutoScan**: In this method, the mobile application detects nearby smart devices automatically, by using Bluetooth, mDNS, or lightning network for device discovery. Typically, we find this method exclusively available for devices equipped with both Wi-Fi and Bluetooth capabilities, and the application requests Bluetooth permission to scan the vicinity for compatible devices.

As illustrated in Table IV, it is evident that AP Mode has significant popularity, with 10 out of the 13 Wi-Fi devices supporting this mode. This preference can be attributed to the inherent security and reliability advantages previously discussed. Moreover, 4 devices provide the option of both EZ mode and AP mode, offering users a choice in their network connectivity approach. And 3 devices support all three connection methods. However, having multiple options may cause confusion for users who do not know what these modes actually mean. The TECKIN camera employs a QR code scanning method, which is generated by its accompanying application to encode the Wi-Fi credentials. Despite its certain convenience, the usability of the camera-based approach is substantially influenced by factors such as lens cleanliness, the distance or angle between the camera and the phone, as well as ambient lighting conditions.

TABLE IV
DEVICE NAMES AND CONNECTION METHODS

Device Name	Connection Methods
Tapo Smart Wi-Fi Light Bulb	AP Mode
LIFX - LED Smart Light	AP Mode, EZ Mode
Gosund Smart Plug	AP Mode, EZ Mode, Auto Scan
SmartThings Wi-Fi Smart Plug	AP Mode
Etekcity Voltson Smart Wi-Fi Outlet	EZ Mode, Auto Scan
Kasa Smart Wi-Fi Plug Lite	AP Mode
DSP-W320 Outdoor Wi-Fi Smart Plug	AP Mode, Auto Scan
BN-LINK Wi-Fi Smart Plug	AP Mode, EZ Mode, Auto Scan
Echo Flex	AP Mode, EZ Mode, Auto Scan
Blurams Smart Home Camera Home Pro	EZ Mode
Kasa Spot 24/7 Recording	AP Mode
Mi Home Security Camera	AP Mode, Auto Scan
TECKIN HD Wi-Fi Indoor Camera	QR Code
Etekcity Fitness Tracker	Bluetooth Connection
Wyze Fitness Tracker	Bluetooth Connection

To summarize, our findings suggest these usability concerns:

U4 Network onboarding is generally time-consuming and lacks user-friendliness or intuitiveness.
U5 Lack of clarity on 5GHz Wi-Fi and public Wi-Fi support.
U6 Insufficient guidance when connection methods fail.
U7 Absence of alternative Wi-Fi onboarding methods.
U8 Confusion and privacy concerns arise when users connect to the device's Wi-Fi and input their home Wi-Fi credentials in the associated application.
U9 Confusion arises when Bluetooth needs to be enabled to discover devices to be connected to Wi-Fi.
U10 Confusion arises when location permission is requested for scanning Wi-Fi endpoints.
U11 Technical terms and security details for the onboarding methods are not adequately explained.

C. Grant Device Access

Allowing multiple users to control smart home devices is a convenient feature, especially when family members or flat-mates need to use the same device simultaneously [12]. Unfortunately, we find limited support or flexibility in this regard in practice.

Gosund and BN-LINK devices allow sharing the device control with other users by entering a numeric code in the new user's account which is generated by the current user. In contrast, SmartThings generates a QR code instead of a numeric code for the same purpose. The new user will need to create an account and scan the QR code.

Etekcity, Blurams, Mi Home, Amazon Alexa, and Wyze allow device sharing using the user profiles. An existing user needs to enter the registered email address or account details of the user to grant access.

Additionally, devices like Mi Home, Blurams, and BN-Link allow two types of users: common users with partial permissions and admin users with complete permissions as the main user. This feature can be helpful if the user wants to grant access to others without letting them change or delete the device configurations set by the admin user.

However, devices like DSP Smart Plug and Kasa Smart Cameras cannot be controlled by multiple users. The only way to share the device access with other users is to share the original login information of the primary user or factory reset the device to register the device with a new account.

To summarize, our findings suggest these usability concerns:

U12 Device access sharing is often in an all-or-nothing manner or offers limited granularity.
U13 Users shared with limited access face the same intricate application interface as regular users.

D. Consistency Analysis

We scrutinize the consistency in the design and functionalities of the devices, and satisfactory consistency in the user interfaces is found. For example, by adding a device to an application, the user interface is designed as a + button, allowing the user to select the type of device from a list of devices the application supports. Most applications like Eteckcity, Tapo, Alexa, and Blurams have a consistent design in their icons, which clearly represent the physical device, making it easy for the user to identify. However, devices like Kasa and LIFX have some inconsistencies, which can make it difficult for users to navigate in their applications. Figure 2 shows notable inconsistencies between the Kasa Smart Wi-Fi Plug Lite device and its representation within the associated application. Firstly, the actual shape and the appearance of the device are not correctly mirrored in the application's iconography. Secondly, the name printed on the packaging of the device is not the same as the name displayed within the application. Users can get confused about which option to select, since neither the icon nor the text provides accurate information. Only after reading additional information in the manual, can the user know that "Smart Plug Mini" should be selected for "Smart Wi-Fi Plug Lite". Such inconsistencies can easily lead to confusion, as users might find it challenging to correlate the physical product with its digital representation.

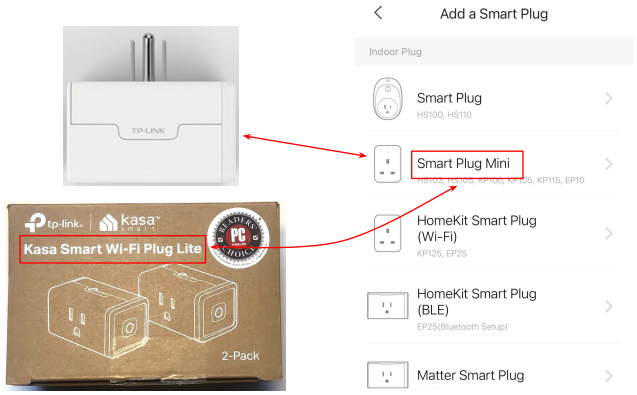

Fig. 2. Inconsistencies between the physical device, the package, and the associated application for Kasa Smart Plug Lite.

Other consistency issues are found where extra functionalities like setting a timer, connecting the device to Amazon Alexa or Google Assistant, and sharing the device access with other users. The procedures appear to be a bit inconsistent

when there is a failure in the initial attempt. Users are generally required to follow additional troubleshooting steps which can be quite different from the instructions outlined in user manuals, and the online resources for finding these solutions can be elusive. For instance, reconfiguring the Amazon Echo Flex to a different location and reconnecting it to an alternate user account deviate from the steps outlined in the initial setup instructions provided in the user manual, leading to inconsistency in user experience.

To summarize, our findings suggest these usability concerns:

U14 Inconsistency appears in the device name or model across packaging, device, manual, and application.

U15 Inconsistency appears in the device appearance across packaging, device, manual, and application.

U16 Inconsistency appears in mapping multiple sockets from a power strip into the application.

U17 Inconsistency arises in reattempting an operation deviating from the original procedure or following a failure.

E. Memorability

After concluding the *two-phase* testing process, we observe a congruent pattern to that noted in the consistency analysis of the devices. The majority of the basic features are easy to remember or recollect while using the application, mainly attributed to concise sequences of steps required to accomplish basic tasks. The primary challenges related to memorability stem from inconsistencies within the devices or their user manuals. Inconsistencies tend to catch users off guard, making them more difficult to remember. Additionally, certain memorability issues arise from the inherent complexity of advanced features in these devices, which may be challenging for non-technical users to understand, let alone remember.

Most of the devices which have consistency issues are harder to reuse after a long period of time. Devices with inconsistent names on the box and mobile application or with unfamiliar icons are harder to reconnect without looking up in the user manual again. The process of reconnecting Amazon Echo Flex to a new user account is difficult to remember, primarily attributed to inconsistencies observed during the initial setup and subsequent reconnection procedures. Recollecting the precise troubleshooting steps employed to address issues hindering the completion of specific tasks is generally harder to remember.

Some features like creating custom scenes and automation rules in smart plugs like Gosund or integrating the devices with Amazon Alexa or Google Home seem difficult to recall the clear procedures. Additional features like energy tracking and scheduling in power outlets for Etekcity and Kasa and advanced features like enabling night vision, accessing cloud storage, or taking a subscription for almost all of the smart cameras are also hard to remember. Such features however indeed require multiple steps to access, which makes them have reasonably poor memorability.

To summarize, our findings suggest these usability concerns:

U18 Numerous steps, particularly for advanced or seldom-used features, impair memorability.

U19 Overly ornate user interfaces hinder memorability.

IV. Conclusion

Usability challenges could deter users, especially those without technical expertise, from harnessing the IoT features, pushing them to fall back to using IoT devices merely as conventional devices. In this paper, we propose consistency and memorability as additional criteria for evaluating IoT usability. Through an examination of 15 smart home devices, we pinpoint 19 distinct usability concerns spanning privacy, device onboarding, access control, consistency, and memorability. Among them, device onboarding stands out as a significant area of usability concerns. To assist the research community, we have made our comprehensive report available as an open-source document, allowing for a thorough understanding without the need to purchase or have direct hands-on experience with the actual devices.

Acknowledgement

This work is supported by the National Science Foundation under grants CNS-1932418 and EEC-2133516. The authors would like to thank Kerim Kurttepeli and Daryl Chia Ler Choo for their early investigation of some of the devices.

Disclaimer: The findings and opinions in this paper result from the authors' research and are not representative of the views of any organization. These observations should not be construed as recommendations, advice, or guidance for consumers, nor should they influence consumer opinions.

References

[1] S. Vetrivel, V. van Harten, C. H. Gañán, M. van Eeten, and S. Parkin, "Examining consumer reviews to understand security and privacy issues in the market of smart home devices," in *USENIX Security Symposium*, 2023, pp. 1523–1540.

[2] E. Zeng and F. Roesner, "Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study," in *USENIX Security Symposium*, 2019, pp. 159–176.

[3] T. Jakobi, C. Ogonowski, N. Castelli, G. Stevens, and V. Wulf, "The catch(es) with smart home: Experiences of a living lab field study," in *ACM Conference on Human Factors in Computing Systems*, 2017, pp. 1620–1633.

[4] A. Nußbaum, J. Schütte, L. Hao, H. Schulzrinne, and F. Alt, "Tremble: Transparent emission monitoring with blockchain endorsement," in *IEEE International Conferences on Internet of Things*, 2021, pp. 59–64.

[5] V. Kumar, S. Mohan, and R. Kumar, "A voice based one step solution for bulk IoT device onboarding," in *IEEE Annual Consumer Communications & Networking Conference*, 2019.

[6] L. Hao and H. Schulzrinne, "Goldie: Harmonization and orchestration towards a global directory for IoT," in *IEEE International Conference on Computer Communications*, 2021.

[7] J. Nielsen, *Usability engineering*. Morgan Kaufmann, 1994.

[8] B. Shneiderman and C. Plaisant, *Designing the user interface: Strategies for effective human-computer interaction*. Pearson Education, 2010.

[9] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *ACM Symposium on Usable Privacy and Security*, 2012.

[10] Wikipedia, "Monitor mode," accessed: 09/02/2023. [Online]. Available: https://en.wikipedia.org/wiki/Monitor_mode

[11] G. Salzillo and M. Rak, "A (in) secure-by-design IoT protocol: the esp touch protocol and a case study analysis from the real market," in *Workshop on CPS&IoT Security and Privacy*, 2020, pp. 37–48.

[12] L. Hao, V. Naik, and H. Schulzrinne, "DBAC: Directory-based access control for geographically distributed IoT systems," in *IEEE Conference on Computer Communications*, 2022, pp. 360–369.